UNIVERSIDAD DE EL SALVADOR
Facultad de Ingenieria y Arquitectura
Departamento de Matematica

Seminario De Graduacion

APLICACIONES DEL ALGEBRA EN LA TEORIA DE LOS NUMEROS

Francisco Amaya Ventura

Diciembre de 1977

San Salvador, El Salvador Centro América

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERIA Y ARQUITECTURA

" APLICACIONES DEL ALGEBRA EN LA TEORIA DE LOS NUMEROS "

Trabajo Presentado Por:

FRANCISCO AMAYA VENTURA

Para Optar al Grado de:

LICENCIADO EN MATEMATICA

Diciembre de 1977.

San Salvador, El Salvador, Centro América.

UNIVERSIDAD DE EL SALVADOR

RECTOR: HONORABLE CONSEJO DE ADMINISTRACION PROVISIONAL DE LA UNIVERSIDAD DE EL SALVADOR.

SECRETARIO GENERAL: DR. EDMUNDO BARRERA RODRIGUEZ

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO: ARQ. MANUEL ENRIQUE ALFARO

SECRETARIO: ING. LUIS A. CARBAJAL VALDEZ

DEPARTAMENTO DE MATEMATICA

JEFE DEL DEPARTAMENTO: ING. GABRIEL MELENDEZ MAYORGA

SEMINARIO DE GRADUACION

ASESOR: LIC. JOSE JAVIER RIVERA LAZO

A MI MADRE Y

ESPOSA

CON AGRADECIMIENTO

CONTENIDO

APLICACIONES DEL ALGEBRA

EN LA TEORIA DE LOS NUMEROS

INTRODUCCION

En el primer capítulo se establecerán los conceptos que pueden considerarse como pre-requisitos para la lectura de este tópico.

La exposición es puramente enumerativa y se supone que el lector esté familiarizado con el material.

CAPITULO I

1.1 ANILLOS

DEFINICION DE ANILLO

Sea A un conjunto, $A \neq \phi$. En A se definen dos operaciones binarias internas:

$+: A \times A \longrightarrow A$

$(x,y) \rightsquigarrow +(x,y) = x+y$

$.: A \times A \longrightarrow A$

$(x,y) \rightsquigarrow .(x,y) = x.y$

Llamadas suma y producto respectivamente. Esta notación y terminología no quiere decir que las operaciones sean la adi-

ción y multiplicación de un sistema de números.

DEFINICION 1.1

Un conjunto A se dice que forma una estructura algebraica de ANILLO, si existen dos operaciones binarias sobre A, llamadas adición y multiplicación y que satisfacen las siguientes condiciones:

1o) La adición define un grupo conmutativo sobre el conjunto A.

2o) La multiplicación es asociativa, es decir,

$x.(y.z) = (x.y).z$

3o) Se cumplen las leyes distributivas, es decir,

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

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

Para cualesquiera x,y,z elementos de A.

Usaremos A para representar tanto el conjunto como el anillo. Cuando sea probable que esta notación cause confusión, indicaremos las operaciones escribiendo $(A,+,\cdot)$

Puede existir un elemento 1 en A tal que $x.1 = 1.x = x$ para todo x en A; si tal elemento existe diremos que A es un anillo unitario.

Representaremos por 0 el elemento identidad para la adición, y por 1 el elemento identidad para la multiplicación.

Por simplicidad en la expresión, prescindiremos de aquí en adelante del punto en x.y y escribiremos simplemente este producto como xy.

Si la multiplicación de A es tal que $xy = yx$ para todo x,y

en A entonces llamamos a A Anillo conmutativo.

DEFINICION 1.2

Si A es un anillo conmutativo, $x \in A$, $x \neq 0$ se dice que x es un divisor de cero si existe y en A, $y \neq 0$, tal que $xy = 0$.

Un anillo A es llamado DOMINIO DE INTEGRIDAD si es un anillo conmutativo y no tiene divisores de cero.

El anillo de los números enteros, es un ejemplo de dominio de integridad.

Se dice que un anillo A es un ANILLO CON DIVISION si sus elementos distintos de cero forman un grupo bajo la multiplicación.

DEFINICION 1.3

Un elemento x de un anillo unitario A, se dice inversible si existe un elemento $x^{-1} \in A$ tal que $xx^{-1} = x^{-1}x = 1$. El elemento x^{-1} es llamado el inverso de x.

Sea A un anillo, A es un CUERPO ó CAMPO si para todo $x \in A$, $x \neq 0$, existe $x^{-1} \in A$ tal que $xx^{-1} = x^{-1}x = 1$.

También se define un CAMPO como un anillo conmutativo con división. Observemos que por definición, un cuerpo posee al menos dos elementos 0 y 1.

Un subconjunto B de un anillo A se llama subanillo si es un subgrupo aditivo, y si $x, y \in B$ implica que $xy \in B$.

En tal caso, B es también un anillo, y las operaciones de B son las mismas que las de A.

Si A es un anillo y $B \subset A$, $D \subset A$, se forman los subconjuntos de A.

$B+D = \{x+y \;/\; x\in B,\ y\in D\}$

$BD = \{xy \;/\; x\in B,\ y\in D\}$

Si $x\in A$ se formas los conjuntos

$x+B = \{x+b \;/\; b\in B\}$

$xB = \{xb \;/\; b\in B\}$

$Bx = \{bx \;/\; b\in B\}$

1.2 MORFISMO E ISOMORFISMO

DEFINICION 1.2.1

Sean A y A' dos anillos, una aplicación ϕ del anillo A en el anillo A' se dice que es un morfismo o un morfismo de anillos si:

1) $\phi(a+b) = \phi(a) + \phi(b)$

2) $\phi(ab) = \phi(a)\phi(b)$

Para $a,b\in A$ cualesquiera.

Es importante hacer notar que: el + y el . que aparecen en los primeros miembros de las relaciones (1) y (2) son los de A, mientras que el + y el . que aparecen en los segundos miembros son los de A'.

Son importantes las propiedades siguientes:

Si ϕ es un morfismo de A en A', entonces

1) $\phi(0) = 0$

2) $\phi(-a) = -\phi(a)$

Si ϕ es un morfismo de A en A', entonces el núcleo de ϕ, $Ker(\phi)$, es el conjunto de todos los elementos $a\in A$ tales que $\phi(a) = 0$, el elemento cero de A', es decir,

$Ker(\phi) = \{a\in A \;/\; \phi(a) = 0,\ 0\in A'\}$

DEFINICION 1.2.1

Un morfismo ϕ de A en A' se dice que es un isomorfismo de anillos si ϕ es una aplicación biyectiva.

Dos anillos se dice que son ISOMORFOS si existe un isomorfismo de uno sobre el otro.

Sea ϕ un morfismo de anillos.

Entonces ϕ es inyectivo si y sólo si

$Ker(\phi) = \{0\}$

En efecto: si A y B son anillos y

$\phi: A \longrightarrow B$

$x \rightsquigarrow \phi(x)$

Veamos que si ϕ es inyectivo entonces

$Ker(\phi) = \{0\}$

Sabemos que $\phi(0) = 0$, $0 \in B$

Además si $x \neq 0$ es tal que $\phi(x)=0$,

tendríamos que ϕ no es inyectivo, por tanto

$Ker(\phi) = \{0\}$

Veamos que si $Ker(\phi) = \{0\}$, entonces ϕ es inyectivo.

Sea $\phi(x) = \phi(y)$, entonces $\phi(x)-\phi(y) = 0$

de donde $\phi(x-y) = 0$, por ser ϕ un morfismo.

Además $x-y = 0$ porque $Ker(\phi) = \{0\}$

Por tanto $x=y$.

De donde podemos afirmar que ϕ es inyectivo.

1.3 IDEALES Y ANILLOS COCIENTES

DEFINICION 1.3.1

Sean A un anillo, $I \subset A$. I es llamado un ideal del ani-

llo A si:

1) $AI \subset I$

2) $IA \subset I$

3) $(I,+)$ es un subgrupo de $(A,+)$

Donde $AI = \{ax / a \in A, x \in I\}$

$IA = \{xa / a \in A, x \in I\}$

Observemos que las condiciones (1) y (2) afirman que I absorve la multiplicación a la izquierda y a la derecha para elementos arbitrarios del anillo.

"Si A es un anillo conmutativo y $a \in A$ entonces Ax es un ideal de A".

Prueba

Debemos probar que:

1) $AAx \subset Ax$

2) $AxA \subset Ax$

3) $(Ax,+)$ es un subgrupo de $(A,+)$

Sabemos que $Ax = \{ax / a \in A\}$

Sean a,b elementos de A

1) Veamos si $AAx \subset Ax$

Sea $a(bx) \in AAx$

pero $a(bx) = (ab)x \in Ax$

Luego $a(bx) \in Ax$ de donde $AAx \subset Ax$

2) Veamos que $AxA \subset Ax$

Sea $(bx)a \in AxA$

Como $(bx)a = b(xa) = b(ax) = (ba)x \in Ax$

Luego $(bx)a \in Ax$ de donde $AxA \subset Ax$

3) Sean u,v elementos de Ax

Probemos que $u - v \in Ax$

Como u,v son elementos de Ax entonces

$u = ax$ y $v = bx$ con $a \in A$, $b \in A$

$u - v = ax - bx = (a-b)x \in Ax$

Luego $u-v \in Ax$ de donde $(Ax,+)$ es

subgrupo de $(A,+)$

Asf Ax es un ideal de A.

DEFINICION 1.3.2

Todo ideal de la forma Ax es llamado un IDEAL PRINCIPAL del anillo A.

Dado un ideal I de un anillo A, sea $\frac{A}{I}$ el conjunto de todas las distintas clases laterales de I en A que se obtienen al considerar I como un subgrupo aditivo de A. Es decir

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

El cociente $\frac{A}{I}$, es dotado de una estructura de anillo con las operaciones siguientes:

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

2) $(x+I)(y+I) = xy + I$

Probemos que estas operaciones estan bien definidas.

"$(x+I, y+I) = (x'+I, y'+I) \Rightarrow (x+y)+I = (x'+y')+I$"

$(x+I, y+I) = (x'+I, y'+I) \Rightarrow x+I = x'+I$ y $y+I = y'+I$

$x+I = x'+I \Rightarrow x = x'+i_1$ para $i_1 \in I$

$y+I = y'+I \Rightarrow y = y'+i_2$ para $i_2 \in I$

Luego $x+y = (x'+i_1)+(y'+i_2) = (x'+y')+i_3$ para $i_3 \in I$

$\Rightarrow (x+y)+I = [(x'+y')+i_3]+I = (x'+y')+i_3+I$

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

Luego $(x+y)+I = (x'+y')+I$

Lo cual prueba que la suma esta bien definida.

"$(x+I,y+I) = (x'+I,y'+I) \Rightarrow xy+I = x'y'+I$"

$(x+I,y+I) = (x'+I,y'+I) \Rightarrow x+I = x'+I \quad y \quad y+I = y'+I$

$x+I = x'+I \Rightarrow x=x'+i_1$ para $i_1 \in I$

$y+I = y'+I \Rightarrow y=y'+i_2$ para $i_2 \in I$

Luego $xy = (x'+i_1)(y'+i_2)$

$xy = x'y'+x'i_2+y'i_1+i_1 i_2$

$xy = x'y'+i_3$, por ser I un ideal de A.

$xy+I = (x'y'+i_3)+I$

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

Lo cual prueba que el producto esta bien definido.

Veamos ahora que $\frac{A}{I}$ es un anillo

P_1) Asociatividad para la suma.

"$[(x+I)+(y+I)] + (z+I) = (x+I) + [(y+I)+(z+I)]$"

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

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

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

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

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

P_2) Conmutatividad para la suma

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

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

$= (y+x)+I$

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

P_3) Existencia de un elemento neutro aditivo.

Sea $(x+I)+(a+I) = x+I$ es decir

$(x+a)+I = x+I$

Esto es cierto si $a=0$

Luego $a+I = 0+I = I$

De donde $a+I = I$

Por tanto el elemento neutro aditivo es I

P_4) Existencia de simétricos aditivos

$(x+I)+(b+I) = I$

$(x+I)+(b+I) = (x+b)+I = I \Rightarrow x+b \subset I$

Por ejemplo $x+b=0 \Rightarrow x=-b$ elemento

inverso o simétrico aditivo.

Luego el simétrico aditivo de $b+I$ es $-b+I$

P_5) Asociatividad para el producto.

"$\left[(x+I)(y+I)\right](z+I) = (x+I)\left[(y+I)(z+I)\right]$"

$$\begin{aligned}\left[(x+I)(y+I)\right](z+I) &= \left[xy+I\right](z+I)\\ &= \left[(xy)z\right]+I\\ &= \left[x(yz)\right]+I\\ &= (x+I)+(yz)+I\\ &= (x+I)+\left[(y+I)+(z+I)\right]\end{aligned}$$

P_6) Distributividad Derecha

"$(x+I)\left[(y+I)+(z+I)\right] = (x+I)(y+I)+(x+I)(z+I)$"

$$\begin{aligned}(x+I)\left[(y+I)+(z+I)\right] &= (x+I)\left[(y+z)+I\right]\\ &= \left[x(y+z)+I\right]\\ &= \left[(xy+xz)+I\right]\\ &= \left[xy+I\right]+\left[xz+I\right]\\ &= \left[(x+I)(y+I)\right]+\left[(x+I)(z+I)\right]\\ &= (x+I)(y+I)+(x+I)(z+I)\end{aligned}$$

P_7) Distributividad Izquierda.

"$\left[(y+I)(z+I)\right](x+I) = (y+I)(x+I)+(z+I)(x+I)$"

$$\begin{aligned}\left[(y+I)(z+I)\right](x+I) &= \left[(y+z)+I\right](x+I)\\ &= \left[(y+z)x\right]+I\\ &= \left[(yx)+(zx)\right]+I\end{aligned}$$

$$= [(yx)+I] + [(zx)+I]$$

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

Luego el cociente $\frac{A}{I}$ es un anillo.

$\frac{A}{I}$ es llamado el anillo de cocientes en el cual se cumplen las propiedades:

1) El elemento neutro es el conjunto I

2) Si A es unitario con identidad 1, entonces $1+I$ es la identidad de $\frac{A}{I}$.

3) Si $x \in A$ entonces $x+I = I \iff x \in I$

CAPITULO II

ANILLOS ENTEROS

2.1 DEFINICION DE ANILLO ENTERO

DEFINICION 2.1.1

Sea A un anillo, A será llamado ANILLO ENTERO, si es un dominio de integridad, es decir un anillo A tal que:

1) $A \neq 0$

2) A es conmutativo

3) A no tiene divisores de cero.

PROPOSICION 2-1.2

Si $A \neq 0$ y A es un anillo conmutativo, las condiciones que siguen son equivalentes:

1) A es entero

2) $(a \neq 0 \text{ y } ab=ac) \Rightarrow b=c$

DEMOSTRACION

1) => 2)

Por hipótesis tenemos que A es entero y asumiendo que $a \neq 0$ y $ab=ac$ es cierto, probemos que $b=c$.

Tenemos que $ab=ac$. Luego

$ab = ac \Rightarrow ab-ac = 0$

$\Rightarrow a(b-c)= 0$

como $a \neq 0$ tiene que ser $b-c=0$

de donde $b=c$.

2) => 1)

Tenemos por hipótesis que

$(a \neq 0 \ \text{y} \ ab = ac) \Rightarrow b=c$

Para todo a,b,c elementos de A.

Queremos probar que A es anillo entero.

Por el enunciado de la proposición tenemos que las condiciones 1) y 2) son satisfechas, es decir, $A \neq 0$ y A es conmutativo.

Probemos la condición 3) A no tiene divisores de cero. Se debe probar que

Si $a \neq 0$ y $ab=0$ entonces $b=0$

$ab=0 \Rightarrow ab=ao$ (porque $ao=0$)

$\Rightarrow b=0$ (por hipótesis)

Luego A es entero.

Lo que completa la demostración.

DEFINICION 2-1.3

Si A es un conjunto y R(x,y) es una relación, diremos que "R(x,y) es una relación de equivalencia sobre A" si se cumplen las condiciones:

1) La relación R(x,y) implica $x \in A$, $y \in A$

2) La relación R(x,x) es verdadera para todo $x \in A$.

3) La relación R(x,y) implica la relación R(y,x).

4) Las relaciones R(x,y) y R(y,z) implican la relación R(x,z).

La condición primera nos garantiza que los elementos que se relacionan son elementos del conjunto A. La segunda condición se llama reflexiva, la tercera simétrica y la cuarta transitiva.

DEFINICION 2-1.4

Si R es una relación de equivalencia sobre un conjunto A y x∈A, llamamos clase de equivalencia de x respecto a R al conjunto $P(x)=\{y\in A / R\ (x,y)\}$

2-2 CUERPO DE FRACCIONES DE UN ANILLO ENTERO

PROPOSICION 2-2.1

"Sea A un dominio entero.

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

En M denotaremos por $(a,b)\sim(c,d)$ la relación $ad=bc$.

Para todo a,b,c,d elementos de A.

Entonces:

1) $\sim$ es una relación de equivalencia en M.

2) Si $\frac{a}{b}$ denota la clase de equivalencia de un elemento (a,b) de M y $K=\{\frac{a}{b} /(a,b)\in M\}$

   Las operaciones siguientes estan bien definidas en K.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

3) Si $a,x\neq 0$, $y\neq 0$, son elementos de A,

$$\frac{ax}{x} = \frac{ay}{y} \quad \text{y definimos} \quad \frac{a\,x}{x} = \frac{a}{1}$$

4) $(k,+,\cdot)$ es un cuerpo

5) La función ψ: $A \longrightarrow K: a \rightsquigarrow \frac{a}{1}$ es un morfismo inyectivo.

6) Si A es unitario $\psi(1)=1$

DEMOSTRACION

Para 1 i) Reflexividad Si $(a,b)\in M$ entonces $(a,b)\sim(a,b)$ ya que $ab=ba$ por ser A conmutativo.

ii) Simétrica Si $(a,b),(c,d)\in M$ y $(a,b)\sim(c,d)$ entonces $ad=bc$, de donde $cb=da$ y por tanto $(c,d)\sim(a,b)$ es decir que $(a,b)\sim(c,d) \Rightarrow (c,d)\sim(a,b)$

iii) Transitividad Si $(a,b),(c,d),(e,f)$ estan todos en M, si $(a,b)\sim(c,d)$ y $(c,d)\sim(e,f)$ entonces $ad=bc$ y $cf=de$. Luego $bcf=bde$, y como $bc=ad$, de ello se sigue que $adf=bde$. Como A es conmutativo, esta relación se convierte en $afd=bed$; como, además, A es dominio entero y $d\neq 0$ esta relación implica, a su vez, que $af=be$. Pero entonces $(a,b)\sim(e,f)$ y nuestra relación es transitiva. Es decir que

$(a,b)\sim(c,d)$ y $(c,d)\sim(e,f) \Rightarrow (a,b)\sim(e,f)$

Luego $\sim$ es una relación de equivalencia.

Para 2 i) Probemos que la suma está bien definida en K

Sean $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$ probemos que

$$\frac{ad+bc}{bd} = \frac{a'd' + b'c'}{b'd'}$$

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = a'b \quad (1)$$

$$\frac{c}{d} = \frac{c'}{d'} \Rightarrow cd' = c'd \quad (2)$$

Como $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ si $b'd'(ad+bc)=bd(a'd'+b'c')$

Tenemos que $b'd'(ad+bc) = adb'd' + bcb'd'$

$= ab'dd' + cd'bb'$

$= a'bdd' + dc'bb'$ por (1)y(2)

$= bd(a'd'+b'c')$

de donde $b'd'(ad+bc) = bd(a'd'+b'c')$

Con lo cual queda probado que la suma esta bien definida.

ii) Probemos que el producto esta bien definido en K

Sean $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$ probemos que $\frac{ac}{bd} = \frac{a'c'}{b'd'}$

$\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = a'b$ (1)

$\frac{c}{d} = \frac{c'}{d'} \Rightarrow cd' = c'd$ (2)

Multiplicando miembro a micmbro (1) y (2) tenemos $ab'cd' = a'bc'd$, como A es conmutativo, luego tenemos $acb'd' = a'c'bd$ esta igualdad implica que

$\frac{ac}{bd} = \frac{a'c'}{b'd'}$

Con lo cual queda probado que el producto esta bien definido en K.

Para 3 $\frac{a}{x}\frac{x}{=} = \frac{ay}{y}$ es cierto ya que

$\frac{ax}{x} = \frac{ay}{y}$ si $(ax)y = (ay)x$

$(ax)y = a(xy) = a(yx) = (ay)x$ por ser A conmutativa.

Luego $(ax)y = (ay)x$

Asi definimos $\frac{ax}{x} = \frac{a}{1}$

Para 4 $(K,+,\cdot)$ es un campo o cuerpo

Recordemos que un cuerpo, es un anillo conmutativo-

con elemento unidad en el que todo elemento distinto de cero tiene un inverso multiplicativo.

* El elemento neutro para la adición en K es de la forma $\frac{0}{x}$ para todo $x \in A$, $x \neq 0$.

Prueba: " $\frac{a}{b} + \frac{0}{x} = \frac{a}{b}$ "

$\frac{a}{b} + \frac{0}{x} = \frac{ax+ob}{bx} = \frac{ax}{bx}$ por la definición de adición en K, luego hay que probar que

$\frac{ax}{x} = \frac{a}{b}$

$\frac{ax}{bx} = \frac{a}{b}$ si $(ax)b = a(bx)$

$(ax)b = a(xb) = a(bx)$ por ser A dominio entero,

luego $(ax)b = a(bx)$

de donde $\frac{ax}{bx} = \frac{a}{b}$

* El elemento negativo de $\frac{a}{b}$ es de la forma $\frac{-a}{b}$

Prueba "$\frac{a}{b} + (\frac{-a}{b}) = \frac{0}{b}$ " con $b \neq 0$

$\frac{a}{b} + (\frac{-a}{b}) = \frac{ab-ab}{b^2} = \frac{0}{b^2}$ como $b \neq 0$, también $b^2 \neq 0$

* La adición es asociativa en K

Prueba: "$(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$"

$$(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{(ad+bc)f+bde}{bdf}$$

$$= \frac{adf+bcf+bde}{bdf} \quad (1)$$

$$\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf+b(cf+de)}{bdf}$$

$$= \frac{adf+bcf+bde}{bdf} \quad (2)$$

De (1) y (2) se ve que la adición es asociativa.

* La adición es conmutativa en K.

Prueba: " $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$ "

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{bc+ad}{bd} = \frac{c}{d} + \frac{a}{b}$

de donde $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$

Lo cual prueba que la adición es conmutativa.

Así hemos probado que (K,+,·) es un grupo conmutativo.

* El elemento identidad para el producto en K es de la forma $\frac{z}{z}$, con z un elemento cualquiera en A.

Prueba: " $\frac{a}{b} \cdot \frac{z}{z} = \frac{a}{b}$ "

$$\frac{a}{b} \cdot \frac{z}{z} = \frac{az}{bz}$$

Probemos que $\frac{az}{bz} = \frac{a}{b}$

$\frac{az}{bz} = \frac{a}{b}$ si (az)b = a(bz)

(az)b = a(zb) = a(bz) por ser A dominio entero

Luego (az)b = a(bz)

Así $\frac{z}{z}$ es la identidad para el producto en K.

* En K los elementos diferentes de cero son de la forma $\frac{a}{b}$ con $a \neq 0$, $b \neq 0$.

Entonces si $\frac{a}{b} \in K$ es diferente de cero, su inverso multiplicativo es de la forma $\frac{b}{a}$ con

$a \neq 0$, $b \neq 0$.

Prueba: " $\frac{a}{b} \cdot \frac{b}{a} = \frac{z}{z}$ "

$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = 1$

Pero $1 = \frac{z}{z} \in K$

Asi $\frac{b}{a}$ es el inverso multiplicativo en K

* El producto es asociativo en K

Prueba: " $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = (\frac{a}{b} \cdot \frac{c}{d}) \frac{e}{f}$ "

$\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = \frac{a}{b} \cdot \frac{ce}{df} = \frac{ace}{bdf}$ (1)

$(\frac{a}{b} \cdot \frac{c}{d}) \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf}$ (2)

De (1) y (2) se ve que el producto es asociativo.

* El producto es conmutativo en K

Prueba: " $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$ "

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$

De donde $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$

Lo cual prueba que el producto en K es conmutativo.

* En K se cumplen las leyes distributivas.

Prueba: " $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$ "

$\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot \frac{cf+ed}{df} = \frac{a(cf+ed)}{bdf} = \frac{acf+aed}{bdf}$ (1)

$\frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{acbf+bdae}{bdbf}$

$= \frac{b(acf+aed)}{b(dbf)} = \frac{acf+aed}{bdf}$ (2)

De (1) y (2) se tiene que

$\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$

" $(\frac{a}{b} + \frac{c}{d}) \cdot \frac{e}{f} = \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f}$ "

$(\frac{a}{b} + \frac{c}{d}) \frac{e}{f} = \frac{ad+bc}{bd} \cdot \frac{e}{f} = \frac{(ad+bc)e}{bdf} = \frac{ade+bce}{bdf}$ (1)

$$\frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}=\frac{ae}{bf}+\frac{ce}{df}=\frac{aedf+cebf}{bfdf}$$

$$=\frac{f(ade+bce)}{f(bdf)}=\frac{ade+bcf}{bdf}\qquad(2)$$

De (1) y (2) se tiene que

$$(\frac{a}{b}+\frac{c}{d})\cdot\frac{e}{f}=\frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}\ .$$

Con lo cual queda probado que $(K,+,\cdot)$ es un cuerpo

Para 5 $\psi: A \longrightarrow K: a \rightsquigarrow \frac{a}{1}$

es un morfismo inyectivo

Debemos probar que: $\psi(a+b)=\psi(a)+\psi(b)$,

$\psi(ab)=\psi(a)\psi(b)$ y además que ψ es inyección.

* $\psi(a+b)=\frac{a+b}{1}=\frac{(a+b)x}{x}=\frac{ax+bx}{x}\qquad(1)$

$\psi(a)+\psi(b)=\frac{a}{1}+\frac{b}{1}=\frac{ax}{x}+\frac{bx}{x}=\frac{ax^2+bx^2}{x^2}\qquad(2)$

Probemos que $\frac{ax+bx}{x}=\frac{ax^2+bx^2}{x^2}$

$\frac{ax+bx}{x}=\frac{ax^2+bx^2}{x^2}$ si $(ax+bx)x^2=(ax^2+bx^2)x$

$(ax+bx)x^2=ax^3+bx^3\qquad(3)$

$(ax^2+bx^2)x=ax^3+bx^3\qquad(4)$

De (3) y (4) se ve que $(ax+bx)x^2=(ax^2+bx^2)x$

Luego se cumple que $\psi(a+b)=\psi(a)+\psi(b)$

* Probemos que $\psi(a)\psi(b)=\psi(ab)$

$\psi(ab)=\frac{ab}{1}=\frac{(ab)x}{x}\qquad(1)$

$\psi(a)\psi(b)=\frac{a}{1}\cdot\frac{b}{1}=\frac{ax}{x}\cdot\frac{bx}{x}=\frac{abx^2}{x^2}\qquad(2)$

Veamos que $\frac{(ab)x}{x}=\frac{(ab)x^2}{x^2}$

$$\frac{(ab)x}{x} = \frac{(ab)x^2}{xx^2} \quad \text{si} \quad [(ab)x]x^2 = [(ab)x^2]x$$

$$[(ab)x]x^2 = (ab)x^3 \qquad (3)$$

$$[(ab)x^2]x = (ab)x^3 \qquad (4)$$

De (3) y (4) se obtiene que $\frac{(ab)x}{x} = \frac{ax}{x} \cdot \frac{bx}{x}$

Luego se cumple que $\psi(ab) = \psi(a)\psi(b)$

* ψ es inyección; debemos probar que $\psi(x)=\psi(y) \Rightarrow x=y$

$\psi(x) = \frac{x}{1}$ y $\psi(y) = \frac{y}{1}$

$\psi(x) = \psi(y) \Rightarrow \frac{x}{1} = \frac{y}{1} \Rightarrow \frac{ax}{a} = \frac{ay}{a}$ con $a \neq 0$

$\frac{ax}{a} = \frac{ay}{a} \Rightarrow a(ax) = a(ay) \Rightarrow a^2x = a^2y$

$\Rightarrow x=y$ de donde ψ es inyección.

Luego ψ: A $\longrightarrow$ K es un morfismo inyectivo.

Para 6 Si A es unitario $\psi(1) = 1$

$\psi(1) = \frac{z}{z}$, $z \in A$, $z \neq 0$

$\psi(1) = \frac{1}{1} = \frac{1.z}{z} = \frac{z}{z} = 1 \in K$

De donde $\psi(1) = 1$

2-3 RELACION DE DIVISIBILIDAD EN UN ANILLO ENTERO

DEFINICION 2-3.1

Sean A un anillo entero; x,y elementos de A, $xy \neq 0$

Se dice que x divide a y si existe $a \in A$ tal que $y = ax$.

Enunciados sinónimos: x es divisor de y,

y es multiplo de x.

Notación: para indicar que x divide a y escribiremos $x|y$.

Si A es un anillo unitario, entonces definimos por

$A^{-1} = \{x \in A / \; xy = yx = 1 \text{ para algún } y \in A\}$.

al conjunto de elementos inversibles para el producto.

Ejemplo: Si A = Z entonces Z^{-1} se compone de

+ 1 y -1, es decir, $Z^{-1} = \{1,-1\}$

DEFINICION 2-3.2

Si A es un anillo entero; a,b dos elementos de A $d \in A$, $d \neq 0$. Se dice que d es un máximo común divisor de a y b si se cumplen:

1) $d|a$ y $d|b$

2) si $m \in A$ es tal que $m|a$ y $m|b$

entonces $m|d$.

para indicar que d es un máximo común divisor de a y b escribiremos d = m.c.d. (a,b)

DEFINICION 2-3.3

Si A es un anillo unitario, $a \in A$, $a \neq 0$. Se dice que a es un elemento primo de A si cumple que:

si m,n son dos elementos de A tales que

$a = mn$ entonces $m \in A^{-1}$ ó $n \in A^{-1}$ y $a \notin A^{-1}$

DEFINICION 2-3.4

Sean A un anillo entero unitario, a,b dos elementos de A. Se dice que a y b son Primos entre sí. Si 1 es un máximo común divisor de a y b.

Escribiremos 1=m.c.d(a,b) para indicar que a y b son primos entre sí.

DEFINICION 2-3.5

Sea A un anillo entero, $a \in A$, $a \neq 0$.

I) Se dice que a admite una factorización en elementos primos en A si:

Existen $P_1 , P_2 , \ldots , P_r$ elementos primos de A y $u \in A^{-1}$ tales que $a = u.P_1.P_2 \ldots P_r$

II) Se dice que a admite una factorización única en elementos primos si:

1) a admite otra factorización $a = v.q_1.q_2 \ldots q_s$ en elementos primos entonces:

1º) $r = s$

2º) para cada $i \leq r$ existe $u_i \in A^{-1}$ tal que $P_i = uq_i$ (Luego de ciertas permutaciones de los índices)

Un anillo entero A es llamado factorial si cada elemento $a \in A$, $a \neq 0$ admite una factorización en elementos primos en A.

PROPOSICION 2-3.6

Sean 1º) A un anillo unitario conmutativo

2º) $I \subset A$ un ideal

Entonces las condiciones que siguen son equivalentes:

1) $I \neq A$ y $\frac{A}{I}$ es un anillo entero

2) $I \neq A$ y si x,y son elementos de A tales que $xy \in I$ entonces $x \in I$ ó $y \in I$

DEMOSTRACION

1) $\Rightarrow$ 2) $\frac{A}{I}$ es un anillo entero por hipótesis y asumiendo cierto que $xy \in I$ probemos que $x \in I$ ó $y \in I$

$xy \in I \Rightarrow xy+I = I$

$\Rightarrow (x+I)(y+I) = I$

$\Rightarrow x+I = I$ ó $y+I = I$

$\Rightarrow x \in I$ ó $y \in I$

2) $\Rightarrow$ 1) Sean $x,y \in A$ tales que $(x+I)(y+I)=I$

$(x+I)(y+I) = I \Rightarrow xy+I = I$

$\Rightarrow xy \in I$

$\Rightarrow (x \in I$ ó $y \in I)$

$\Rightarrow x+I=I$ ó $y+I=I$

A los ideales I de un anillo conmutativo A que cumplen una de las dos condiciones anteriores se les llama IDEALES PRIMOS.

PROPOSICION 2-3.7

Sean 1) A un anillo entero unitario

2) $x \in A$, $x \neq 0$ tal que Ax es un ideal primo,

Entonces x es un elemento primo.

DEMOSTRACION

Sean m,n dos elementos de A tales que x=mn

probemos que $m \in A^{-1}$ ó $n \in A^{-1}$ y $x \notin A^{-1}$

$x \in Ax \Longrightarrow mn \in Ax \Longrightarrow (m \in Ax$ ó $n \in Ax)$

(por ser Ax un ideal primo)

Sea $m \in Ax$; entonces; existe $a \in A$ tal que $m=ax$

luego $x=axn=anx \Longrightarrow 1=an \Rightarrow n \in A^{-1}$.

si es el caso que $n \in Ax$; entonces; existe $a \in A$

tal que $n=ax$.

Luego $x=max=amx \Longrightarrow 1=am \Rightarrow m \in A^{-1}$

Veamos que $x \notin A^{-1}$ (por contradicción)

Supongamos $x \in A^{-1}$, sea $b \in A$, entonces $b=b(x^{-1}, x)$

$b=b(x^{-1} x) = (bx^{-1}) \; x \in Ax \Rightarrow A \subseteq Ax$

de donde $A=Ax$ (contradicción porque $Ax \neq A$)

Luego $x \in A^{-1}$

CAPITULO III

ANILLOS PRINCIPALES

DEFINICION 3-1.1

Sea A un anillo, A es llamado un anillo principal si se cumplen las condiciones siguientes:

1) A es unitario
2) A es entero
3) Todo ideal de A es principal.

Recordemos que llamamos ideal principal de A a un conjunto de la forma $\{ab/a\in A\} = Ab$ con $b\in A$.

Ejemplo:

Los enteros Z forman un anillo principal. Verifiquemos que todo ideal de Z es principal, es decir que es de la forma $\{ab/a\in Z\} = Ab$, con $b\in Z$

Sea $I \subset Z$ un ideal

Sea $b = \min\{p\in Z/p>0 \text{ y } p\in I\}$

Probemos que $I=Zb$

Sea $d\in I$

Si $d=0$ entonces $d=ob\in Zb$

Si $d>0$, entonces; existen e,r en Z tales que

$d= eb+r$, $0\leq r<b$; r es un elemento de I,

ya que $r= d-eb\in I$ de donde $r=0$

(por ser b minimal entre los elementos de I mayores que cero)

Por tanto $d \in Zb$

Si $d<0$, entonces $-d>0$

$-d>0 \Rightarrow -d = e'b \rightarrow d = (-e')b \in Zb$

de donde $d \in Zb$

Luego $I \subset Zb$, y como $Zb \subset I$, se da la igualdad, es decir $I=Zb$.

PROPOSICION 3-1.2

Sean i) A un anillo principal

ii) $a \in A$, $b \in A$, $a \neq 0$ y $b \neq 0$

Entonces:

1) Existe $d \in A$ tal que d es el máximo común divisor de a y de b.

2) Existen x,y en A tal que $xa+yb = d$.

DEMOSTRACION

Probaremos (1) y (2) simultáneamente.

Tomemos los ideales Aa y Ab

Luego $Aa+Ab$ es un ideal; asi existe $d \in A$

tal que $Aa+Ab=Ad$

Se debe probar que $d = m.c.d(a,b)$

Como Ad es un ideal entonces

$1a+0b \in Ad \Rightarrow$ existe $m \in A$ tal que $a=md \rightarrow d|a$

$0a+1b \in Ad \rightarrow$ existe $n \in A$ tal que $b=nd \Rightarrow d|b$

Sea $p \in A$ tal que $p|a$ y $p|b$ luego existen

r,s en A tal que $a=rp$ y $b=sp$

asi $d=1d \Rightarrow d \in Ad \Rightarrow d \in Aa+Ab$

entonces existen x,y en A tal que $d=xa+yb$

esto prueba la parte 2)

Ahora como $d=xa+yb \Rightarrow d=xrp+ysp$

$\Rightarrow d=(xr+ys)p$

$\Rightarrow p|d.$

Luego 1) queda probado ya que se tiene que $d|a$ y $d|b$ y además $p|d$.

PROPOSICION 3-1.3

Sean i) A un anillo principal

ii) $a \in A$, a un elemento primo

iii) $b \in A$, b no divide a b

Entonces: a y b son primos entre sí.

DEMOSTRACION

Demostrar que a y b son primos entre sí, es equivalente a demostrar que su máximo común divisor es 1.

Luego debemos demostrar que $1=m.c.d(a,b)$

Por ser A anillo principal existe 1 en A. Así

si $a \in A$, entonces $a=a1$ de donde $1|a$

si $b \in A$, entonces $b=b1$ de donde $1|b$

Sea $m \in A$ tal que $m|a$ y $m|b$ probemos que $m|1$

Existen r,s en A tal que $a=mr$, $b=ms$

Por ser a elemento primo, tenemos que $m \in A^{-1}$

ó $r \in A^{-1}$.

Si $r \in A^{-1}$, entonces $m=ar^{-1}$

Luego $b=(ar^{-1})s = a(r^{-1}s)$ de donde $b=a(r^{-1}s)$

o sea que $a|b$ (contradicción) ya que a no divide a b por hipótesis.

Por tanto $r \notin A^{-1}$. Luego debe ser $m \in A^{-1}$

Como $m \in A^{-1}$ entonces $1 = mm^{-1}$ esto implica que $m|1$.

Así el máximo común divisor de a y b es 1.

Luego a y b son primos entre sí.

PROPOSICION 3-1.4

Sean i) A un anillo principal

ii) a,b,c elementos de A tal que

a es primo y $a|bc$

Entonces: $a|b$ ó $a|c$

DEMOSTRACION

Supongamos que a no divide a b (a y b primos entre sí) entonces existen x,y en A tal que

$ax+by = 1$ (por proposición 3-1.2)

Multiplicando por c la ecuación $ax+by = 1$

tenemos $c(ax+by) = c1$ de donde

$$cax+cby = c$$

Por hipótesis tenemos que $a|bc$ entonces

existe $m \in A$ tal que $bc=am$

Luego de $c=cax+cby$ tenemos que

$$c = acx+bcy$$

$$c = acx+amy \text{ (por ser } bc=am)$$

$$c = a(cx+my)$$

de donde $a|c$

PROPOSICION 3-1.5

"Si A es un anillo principal, A es un anillo factorial".

DEMOSTRACION

Probaremos primero que todo elemento de A distinto de cero admite una factorización en elementos primos.

Sea $B \subset A$, formado por elementos distintos de cero que no admiten factorización en elementos primos y probemos que B es vacío.

Supongamos que B es no vacío,

Sean $a_1, a_2, a_3, \ldots, a_n, \ldots$ en B tales que

$$Aa_1 \subset Aa_2 \subset Aa_3 \subset \ldots \subset Aa_n \subset \ldots$$
$$\neq \quad \neq \quad \neq \quad \neq \quad \neq$$

Esta cadena es finita, ya que $\bigcup_{i \in N} Aa_i$ es un ideal

de A, que es principal.

En efecto

i) " $\bigcup_{i \in N} Aa_i$ es subgrupo "

Sean $x, y \in \bigcup_{i \in N} Aa_i$ entonces $x \in Aa_k$, $y \in Aa_n$

si $m \geq k$, entonces $Aa_k \subset Aa_n \Rightarrow x, y \in Aa_n$

$\Rightarrow x-y \in Aa_n \Rightarrow x-y \in \bigcup_{i \in N} Aa_i$

ii) " $A(\bigcup_{i \in N} Aa_i) \subset \bigcup_{i \in N} Aa_i$ y $(\bigcup_{i \in N} Aa_i)A \subset \bigcup_{i \in N} Aa_i$ "

Sea $\lambda \in A$, $x \in \bigcup_{i \in N} Aa_i$; entonces $x \in Aa_t$

$\lambda \in A$ y $x \in Aa_t \Rightarrow \lambda x \in Aa_t \Rightarrow \lambda x \in \bigcup_{i \in N} Aa_i$

de donde $A(\bigcup_{i\in N} Aa_i) \subset \bigcup_{i\in N} Aa_i$

En forma similar se prueba que $(\bigcup_{i\in N} Aa_i)A \subset \bigcup_{i\in N} Aa_i$

Si $\bigcup Aa_i = Aa$ (por ser anillo principal) existe n tal que $a \in Aa_n$, de donde $Aa \subset Aa_n$ lo que implica $Aa = Aa_n$

Entonces: Aa_n es el último elemento de la cadena

a_n no es elemento primo (si no admitiría la factorización $a_n = 1a_n$)

Luego existen b,c en A tal que

$a_n = bc$ y $b \notin A^{-1}$, $c \notin A^{-1}$

entonces $Aa_n \neq Ab$ y $Aa_n \neq Ac$

Probemos que $Aa_n \neq Ab$

Supongamos que $Aa_n = Ab$, entonces existen

$d \in A$, $e \in A$ tal que $a_n = db$ y $b = ea_n$

Luego $a_n = ea_n c = a_n(ec) \Rightarrow 1 = ec$ de

donde $c \in A^{-1}$ (contradicción) porque $c \notin A^{-1}$.

Probemos que $Aa_n \neq Ac$

supongamos que $Aa_n = Ac$, entonces existen

$d \in A$, $e \in A$ tal que $a_n = dc$ y $c = ea_n$

Luego $a_n = bea_n = a_n(be) \Rightarrow 1 = be$ de donde

$b \in A^{-1}$ (contradicción ya que $b \notin A^{-1}$)

Si $d \in A$: $da_n = dbc \Rightarrow da_n \in Ac \Rightarrow Aa_n \subset Ac$

$da_n = dbc \Rightarrow dcb \in Ab \Rightarrow da_n \in Ab$

$\Rightarrow Aa_n \subset Ab$

Luego $Aa_n \not\subset Ac$ y $Aa_n \not\subset Ab$

Entonces $c \notin B$, $b \notin B$ (porque no pueden ponerse en la cadena, ya que Aa_n es el último elemento de la cadena)

Esto implica que c y b admiten factorización en elementos primos. Luego $a_n = bc$ implica que a_n admite una factorización única en elementos primos, lo que contradice la hipótesis de que B es no vacío.

Luego $B = \phi$, ósea que $a \in A$, $a \neq 0$, a admite factorización en elementos primos.

"Probemos que la factorización es única"

Sean $a = up_1 p_2 \ldots p_r = vq_1 q_2 \ldots q_t$

dos factorizaciones en elementos primos

Debemos probar que r=t

La afirmación $up_1 p_2 \ldots p_r = vq_1 q_2 \ldots q_t$

implica que $p_1 \mid vq_1 q_2 \ldots q_t$

Por ser p_1 primo, p_1 divide a algún q_i

Supongamos que $p_1 \mid p_1$

Si $p_1 \mid q_1$ entonces existe $e \in A$ tal que $p_1 = eq_1$

$p_1 = eq_1 \Rightarrow e \in A^{-1}$.

Si tomamos $e = u_1$, entonces $p_1 = u_1 q_1$

sustituyendo p_1 en la afirmación tenemos

$uu_1 q_1 q_2 \ldots p_r = vq_1 q_2 \ldots q_t$

Aplicando la ley cancelativa obtenemos

$u\, u_1 p_2 \ldots\ldots p_r = vq_2 \ldots\ldots q_t$

Luego si hacemos este mismo proceso para p_2 tenemos:

$uu_1 u_2 q_2 p_3 \ldots\ldots = vq_2 q_3 \ldots\ldots q_t$

cancelando obtenemos $UU_1 U_2 P_3 \ldots = vq_3 \ldots q_t$

si $r < t$ y haciendo el mismo proceso anterior

tenemos $UU_1 U_2 U_3 \ldots U_r = vq_{r+1} q_{r+2} \ldots q_t$

haciendo $f = UU_1 U_2 \ldots U_3$ entonces $f \in A^{-1}$

así de $f = vq_{r+1} q_{r+2} \ldots q_t$ se obtiene

$1 = vq_{r+1} q_{r+2} \ldots q_t f^{-1}$ esto implica que

$q_{r+1} q_{r+2} \ldots q_t \in A^{-1}$ (contradicción)

Luego $r \geq t$

Si $r > t$ se encuentran ciertos P_i que son inversibles es decir que $P_{t+1}, P_{t+2}, \ldots, P_r$ estan en A^{-1}

Luego tiene que ser $r=t$

de donde $P_1 = U_1 q_1$, $P_2 = U_2 q_2$, $\ldots$, $P_r = U_t q_t$

Asi hemos probado que cada $a \in A$, $a \neq 0$ admite una factorización única.

PROPOSICION 3-1.6

"El anillo Z de los enteros es factorial"

DEMOSTRACION

Es una consecuencia de que Z es un anillo principal.

DEFINICION 3-1.7

Al cuerpo K de la proposición 2-2.1 le llamaremos EL CUERPO DE FRACCIONES del anillo A.

PROPOSICION 3-1.8

"Sean A un anillo entero unitario

K su cuerpo de fracciones

x,y elementos de K.

Entonces las condiciones que siguen son equivalentes:

1) $x|y$

2) $y \in Ax$

3) $Ay \subset Ax$"

DEMOSTRACION

1) $\Longrightarrow$ 2)

$x|y \Rightarrow y = ax$ con $x \in A$

$\Rightarrow y \in Ax$

Así $x|y \Rightarrow y \in Ax$

2) $\Longrightarrow$ 3)

$y \in Ax \Rightarrow y = ax$, $a \in A$

Sea $by \in Ay$ entonces $by = bax$

luego $by \in Ax$ de donde $Ay \subset Ax$

3) $\Longrightarrow$ 1)

Como $Ay \subset Ax \Rightarrow by \in Ax \Rightarrow by = cx$

con $b \in A$, $b \neq 0$. tomando $b = 1$ tenemos

$1y = cx \Rightarrow y = cx$ con $c \in A$

$\Rightarrow x|y$, $y \in K$

PROPOSICION 3-1.9

"Sean A un anillo entero unitario

K su cuerpo de fracciones

x,y,z elementos de K

Entonces:

1°) $x|x$

2°) $(x|y \ y \ y|z) \Rightarrow x|z$

3°) $(x|y \ y \ y|x) \Rightarrow Ay = Ax$'

DEMOSTRACION

Para 1°) Por ser A anillo entero unitario existe $1 \in A$ tal que $x = 1x$ luego $x|x$

Para 2°) $x|y \Rightarrow y = ax$, $a \in A$

$y|z \Rightarrow z = by$, $b \in A$

como $z = b\,y = bax$ entonces $z = bax$, $ba \in A$

de donde $x|z$

Para 3°) $x|y \Rightarrow y = ax$, $a \in A$

$y|x \Rightarrow x = by$, $b \in A$

Pero $Ay = Ax$ si y sólo si $Ay \subset Ax$ y $Ax \subset Ay$

Sea $u \in Ay$ entonces $u = my$ con $m \in A$

$my = max \Rightarrow my \in Ax$

de donde $Ay \subset Ax$

Sea $v \in Ax$ entonces $v = nx$ con $n \in A$

$nx = nby \Rightarrow nx \in Ay$, de donde $Ax \subset Ay$.

Luego $Ay = Ax$.

Es importante notar el hecho de que si $x|y$ y $y|x$ no se puede deducir, en general, que $x=y$; solamente es $Ax = Ay$.

PROPOSICION 3-1.10

Sean i) A un anillo unitario

ii) K su cuerpo de fracciones

iii) x,y en K, $y \neq 0$

Entonces las condiciones que siguen son equivalentes

1°) $Ay = Ax$

2°) $xy^{-1} \in A^{-1}$

DEMOSTRACION

1°) $\Rightarrow$ 2°)

Si $Ay = Ax$, entonces existen $a \in A$, $b \in A$ tales que $y=ax$, $x=by$

$y = ax \Rightarrow yx^{-1} = a \in A$

$x = by \Rightarrow xy^{-1} = b \in A$

Si $(xy^{-1})(yx^{-1}) = (yx^{-1})(xy^{-1}) = 1$, entonces $xy^{-1} \in A^{-1}$.

$(xy^{-1})(yx^{-1}) = x(y^{-1}y)x^{-1} = (xx^{-1}) = 1$

$(yx^{-1})(xy^{-1}) = y(x^{-1}x)y^{-1} = (yy^{-1}) = 1$

Así $xy^{-1} \in A^{-1}$.

2°) $\Rightarrow$ 1°)

Si $xy^{-1} \in A^{-1}$, entonces $Ay=Ax$ por definición de A^{-1}, entonces $xy^{-1} \in A$ y $(xy^{-1})^{-1} \in A$ tales que $(xy^{-1})(xy^{-1})^{-1} = 1$

Sea $a = (xy^{-1})^{-1}$ así se tiene que

$a(xy^{-1}) = (xy^{-1})a = 1$

Luego $a(xy^{-1}) = 1 \Rightarrow x = a^{-1}y$

$(xy^{-1})a = 1 \Rightarrow y = ax$

Si $b \in A$, entonces $by = b(ax) = (ba)x \Rightarrow Ay \subset Ax$

Si $d \in A$, entonces $dx = d(a^{-1}y) = (da^{-1})y \Rightarrow Ax \subset Ay$

de donde $Ay = Ax$.

3-2 DIVISIBILIDAD EN LOS ANILLOS PRINCIPALES

DEFINICION 3-2.1

Sean A un anillo principal, K su cuerpo de fracciones; x,y elementos de K. Se dice que x divide a y si existe $a \in A$ tal que $y = ax$.

La relación entre los elementos de K depende esencialmente del anillo A; es decir se trata de la relación de divisibilidad en K respecto al anillo A.

DEFINICION 3-2.2

Sean A un anillo principal, K su cuerpo de fracciones; x,y,d,m elementos de K.

i) Se dice que d es un máximo común divisor de x,y si:
   1) $d|x$, $d|y$
   2) si $h \in k$ es tal que $h|x$ y $h|y \Rightarrow h|d$.

ii) Se dice que m es un mínimo común multiplo de x,y si:
   1) $x|m$, $y|m$
   2) si $b \in K$ es tal que $x|b$ y $y|b \Rightarrow m|b$

PROPOSICION 3-2.3

"A un anillo, K su cuerpo de fracciones; x,y,m,d elementos de K.

Entonces:

i) Las condiciones que siguen son equivalentes:

1) d e s un m.c.d.(x,y)

2) si $b \in K$, entonces $b|x$ y $b|y \iff b|d$

ii) Las dos condiciones que siguen son equivalentes:

1) m e s un m.c.m(x,y)

2) si $b \in K$, entonces $x|b$ y $y|b \iff m|b$

DEMOSTRACION

Para i) 1) $\Rightarrow$ 2)

Como d e s m.c.d(x,y); entonces $d|x$, $d|y$

además $b \in K$ es tal que $b|x$ y $b|y$

Luego $b|d$.

Asi $b|x$ y $b|y \Rightarrow b|d$.

d e s m.c.d(x,y), entonces $d|x$ y $d|y$

$d|x \Rightarrow x = de'$, $e' \in A$

$d|y \Rightarrow y = de''$, $e'' \in A$

si $b|d$, entonces $d = be$, $e \in A$

Luego podemos escribir:

$x = bee' = b(ee'')$ de donde $b|x$

$y = bee'' = b(ee'')$ de donde $b|y$

asi $b|d \Rightarrow b|x$ y $b|y$

2) $\Rightarrow$ 1)

$(b|x \text{ y } b|y \Leftrightarrow b|d) \Rightarrow d = m.c.d(x,y)$

Por hipótesis tenemos que:

1) $b|x \text{ y } b|y \Rightarrow b|d$

2) $b|d \Rightarrow b|x \text{ y } b|y$

tomando b=d tenemos que $d|x$ y $d|y$

De 1) y 2) se tiene que $d=m.c.d(x,y)$

Para ii) 1) $\Longrightarrow$ 2)

Como m es $m.c.m(x,y)$, entonces $x|m$, $y|m$

además $b \in K$ es tal que $x|b$, $y|b$

Luego $m|b$.

asi $x|b$ y $y|b \Rightarrow m|b$.

m es $m.c.m(x,y)$, entonces $x|m$, $y|m$

$x|m \Rightarrow m = x\,e'$, $e' \in A$

$y|m \Rightarrow m = y\,e''$, $e'' \in A$

Si $m|b$ entonces $b = me$, $e \in A$

LUEGO podemos escribir:

$b = me = xe'e = x(e'e)$ de donde $x|b$

$b = me = ye''e = y(e''e)$ de donde $y|b$

asi $m|b \Rightarrow x|b$ y $y|b$.

2) $\Longrightarrow$ 1)

$(x|b \text{ y } y|b \Leftrightarrow m|b) \Rightarrow m = m.c.m(x,y)$

Por hipótesis tenemos que:

1) $x|b$ y $y|b \Rightarrow m|b$

2) $m|b \Rightarrow x|b$ y $y|b$

Tomando m=b tenemos $x|m$ y $y|m$

De 1) y 2) se tiene que $m=m.c.m(x,y)$

PROPOSICION 3-2.4

"Sea A un anillo principal

K s u cuerpo de fracciones

x,y en K.

Entonces existen m,d en K tal que

d = m.c.d(x,y)

m = m.c.m(x,y) "

DEMOSTRACION

Como x,y son elementos de K entonces son de la forma $x = \frac{a}{b}$, $y = \frac{m}{n}$ con a,b,m,n en A, $a \neq 0$, $n \neq 0$

por ser $x = \frac{a}{b}$ entonces $a = xb$

por ser $y = \frac{m}{n}$ entonces $m = yn$

Sea Aan + Abm un ideal de A; entonces existe

d' en A tal que Aan + Abm = Ad' .

Como a=xb y m=yn tenemos que

Abnx + Abny = Ad' además $b \neq 0$ y $n \neq 0$

Luego $\frac{Abnx+Abny}{bn} = \frac{Ad'}{bn}$. Llamemosle

d a $\frac{d'}{bn}$, Luego tenemos Ax+Ay = Ad.

Probemos q u e d e s m.c.d(x,y)

i) Como $x \in Ax+Ay$ entonces $x \in Ad$

$x \in Ad$ implica que x es de la forma

$x = qd$ con $q \in A$, Luego $d|x$

Como $y \in Ax+Ay$ entonces $y \in Ad$

$y \in Ad$ implica que y es de la forma

$y = pd$ con $p \in A$, luego $d|y$.

ii) "Si $h \in K$ es tal que $h|x$ y $h|y$ entonces $h|d$"

$h|x$ implica que $x=hh', h' \in A$

$h|y$ implica que $y=h h'', h'' \in A$

Sean $p \in A$, $t \in A$ y como $Ax+Ay = Ad$

entonces $d = px+ty$.

Luego $d = phh' + thh'' = h(ph' + th'')$ implica

que $d = h(ph' + th'')$ de donde $h|d$.

2) Probemos la existencia de $m=m.c.m(x,y)$

Se puede comprobar notando que el paso al inverso $t/ \longrightarrow t^{-1}$ invierte la relación de divisibilidad, lo que nos lleva al m.c.d.

Sea $t=m.c.d(x^{-1}, y^{-1})$ entonces $t^{-1}= m.c.m(x,y)$

Debemos probar que:

i) $x|t^{-1}$, $y|t^{-1}$

ii) si $h \in K$ es tal que $x|h$, $y|h$ entonces $t^{-1}|h$

Para i)

$t|x^{-1}$ y $t|y^{-1}$ por ser $t=m.c.d(x^{-1}, y^{-1})$

$t|x^{-1} \Rightarrow x^{-1} = at \Rightarrow t^{-1} = ax \Rightarrow x|t^{-1}$

$t|y^{-1} \Rightarrow y^{-1} = bt \Rightarrow t^{-1} = by \Rightarrow y|t^{-1}$

Para ii)

$$\left.\begin{array}{l} x|h \Rightarrow h^{-1}|x^{-1} \\ y|h \Rightarrow h^{-1}|y^{-1} \end{array}\right\} \Rightarrow h^{-1}|t \Rightarrow t^{-1}|h$$

PROPOSICION 3-2.5

"Sean A un anillo principal

K su cuerpo de fracciones

x,y en K, $d=m.c.d(x,y)$, $m=m.c.m(x,y)$.

Entonces: $xy=md$".

DEMOSTRACION

Esto es equivalente a probar que $xym^{-1} = d$,

siendo $m^{-1} = m.c.d(x^{-1},y^{-1})$

Como $m^{-1} = m.c.d(x^{-1},y^{-1})$ entonces existen

a,b en A tal que $m^{-1} = ax^{-1} + by^{-1}$.

Luego $xym^{-1} = xy(ax^{-1} + by^{-1}) = ay+bx$

de donde $xym^{-1} = ay+bx$.

Hay que probar que " $u|x$ y $u|y \iff u|(ay+bx)$"

$\Rightarrow$) $u|x \Rightarrow u = pu$ y $u|y \Rightarrow y = tu$

$x = pu \Rightarrow bx = bpu$ y $y = tu \Rightarrow ay = atu$

Sumando miembro a miembro obtenemos

$ay + bx = atu + bpu = u(at+bp)$

de donde $ay+bx = u(at+bp) \Rightarrow u|(ay+bx)$

$\Leftarrow$) $u|(ay+bx) \Rightarrow ay+bx = ur$, con $r \in A$.

como $ay+bx = xym^{-1}$ entonces $xym^{-1} = ur$

$xym^{-1} = ur \Rightarrow x = ury^{-1}m \Rightarrow u|x$, $ry^{-1}m \in A$

$xym^{-1} = ur \Rightarrow y = urx^{-1}m \Rightarrow u|y$, $rx^{-1}m \in A$

Probemos que $ry^{-1}m \in A$ y $rx^{-1}m \in A$

Sabemos que $m^{-1} = m.c.d(x^{-1}, y^{-1})$ entonces

$m^{-1}|x^{-1}$, $m^{-1}|y^{-1}$

$m^{-1} \mid x^{-1} \Rightarrow x^{-1} = m^{-1} z \Rightarrow x^{-1} m = z \in A$

$m^{-1} \mid y^{-1} \Rightarrow y^{-1} = m^{-1} t \Rightarrow y^{-1} m = t \in A$

y como $r \in A$ luego $rx^{-1} m \in A$ y $ry^{-1} m \in A$

Asi $xym^{-1} = d$.

DEFINICION 3-2.6

Sean A un anillo principal, K su cuerpo de fracciones; x,y,z,d elementos de K.

Se dice quedes el m.c.d(x,y,z) si:

1) $d|x$, $d|y$, $d|z$

2) si $m \in K$ es tal que $m|x$, $m|y$, $m|z$ entonces $m|d$.

PROPOSICION 3-2.7

"Sean A un anillo principal

K su cuerpo de fracciones

x,y,d,d' en K

d,d' dos m.c.d de x,y

Entonces: Existe $a \in A^{-1}$ tal que $d=ad'$ "

DEMOSTRACION

$d = m.c.d(x,y) \Rightarrow d|x$, $d|y$

$d' = m.c.d(x,y) \Rightarrow d' \mid x$, $d' \mid y$

$d|x$ y $d|y \Rightarrow d|d' \Rightarrow d' = xd$, $x \in A$

$d' \mid x$ y $d' \mid y \Rightarrow d' \mid d \Rightarrow d = yd'$, $y \in A$

$d' = xd = xyd' \Rightarrow xy = 1$ en tal caso $y \in A^{-1}$

Luego tomando y=a obtenemos $d=ad'$.

Si A=Z, tenemos que $d=1.d$

$-d=(-1)d$

De lo anterior concluímos que en los enteros Z el m.c.d no es único, mientras que en los naturales N el m.c.d es único.

PROPOSICION 3-2.8

" En el anillo Z; a,b enteros positivos
a par, b impar
d=m.c.d(a+b,a-b)
Entonces d=m.c.d(a,b)"

DEMOSTRACION

Como d=m.c.d(a+b,a-b) entonces d|a+b y d|a-b

$d|a+b \Rightarrow a+b = xd$ con $x \in Z$

$d|a-b \Rightarrow a-b = yd$ con $y \in Z$

Sumando miembro a miembro

$$\begin{array}{r} a+b = xd \\ a-b = yd \\ \hline 2a = (x+y)d \end{array}$$

$2a=(x+y)d \Rightarrow a=(\frac{x+y}{2})d$ de donde d|a.

Restando miembro a miembro

$$\begin{array}{r} a+b = xd \\ a-b = yd \\ \hline 2b = (x-y)d \end{array}$$

$2b=(x-y)d \Rightarrow b=(\frac{x-y}{2})d$ de donde d|b.

Si $m \in A$ es tal que m|a+b y m|a-b

entonces m|d.

En efecto.

$m|a+b \Rightarrow a+b = xm$ con $x \in Z$

$m|a-b \Rightarrow a-b = ym$

Luego $2a = (x+y)m$

Como $d|a \Rightarrow a=zd$ con $z \in A$

$2a = (x+y)m \Rightarrow 2(zd) = (x+y)m$

$\Rightarrow (2z)d = (x+y)m$

$\Rightarrow d = (\frac{x+y}{2z})m$

$\Rightarrow m|d$

Luego $d=m.c.d(a,b)$.

En forma general no se cumple.

Ejemplo: $m.c.d(7+3,7-3)=2$ a,b impares

$m.c.d(7,3)=1$

Ejemplo: $m.c.d(6+2,6-2)=4$ a,b pares

$m.c.d(6,2)=2$

Sin embargo obsérvese que si a,b son pares entonces d es par.

PROPOSICION 3-2.9

" En el anillo Z

a,b enteros positivos pares tales que

$2=m.c.d(a+b,a-b)$

Entonces: $2=m.c.d(a,b)$ "

DEMOSTRACION

Por ser a par y b par entonces $2|a$ y $2|b$

" si $m|a$ y $m|b$ entonces $m|2$ "

$m|a$ y $m|b \Rightarrow m|a+b$ y $m|a-b \Rightarrow m|2$

por ser $2 = m.c.d(a+b,a-b)$

PROPOSICION 3-2.10

" En el anillo Z; x,y dos enteros positivos

$d = m.c.d(x,y)$

$x' = \frac{x}{d}$, $y' = \frac{y}{d}$

Entonces x' ,y' son primos entre sí "

DEMOSTRACION

Es equivalente probar que $1 = m.c.d(x' ,y')$

Por hipótesis tenemos que $d|x$, $d|y$ ya que

$d = m.c.d(x,y)$ y que $x = x' d$, $y = y' d$

Supongamos que $m|x'$, $m|y'$, con $m \in Z$

$m|x' \Rightarrow x' = am$, $a \in Z$

$m|y' \Rightarrow y' = bm$, $b \in Z$

Como: $x = x' d = dx' = dam = a(dm)$

Luego $x = a(dm)$ de donde $dm|x$

$y = y' d = bmd = b(md) = b(dm)$

Luego $y = b(dm)$ de donde $dm|y$

$dm|x$ y $dm|y \Rightarrow dm|d$

$dm|d \Rightarrow m = 1 \Rightarrow m|1$

Asi $1 = m.c.d(x' ,y')$

PROPOSICION 3-2.11

" a,b,c enteros positivos

b,c primos entre sí, $a^2 = bc$

entonces b y c son de la forma $b = u^2$ y $c = v^2$,

u,v enteros positivos "

DEMOSTRACION

Si q es un factor primo de a, entonces $q|bc$

Luego $q|b$ ó $q|c$

Descompongamos a en sus factores primos, y sean $p_1, p_2, p_3, \ldots, p_m$ los factores primos que dividen a "b"; $q_1, q_2, q_3, \ldots, q_r$ los factores primos que dividen a "c", es decir

$a = p_1 \cdot p_2 \cdot p_3 \cdots p_m \cdot q_1 \cdot q_2 \cdots q_r$

Sea p un factor primo que divide a "b"

1 puede escribirse en la forma $1=xb+yc$

por que b y c son primos entre sí, luego

1=m.c.d(b,c), entonces I puede expresarse como combinación lineal.

De $1=xb+yc$ se obtiene $b=xb^2+ycb$

$p|b \Rightarrow b = pr \Rightarrow b^2 = p^2 r^2$

$p^2|b^2 \Rightarrow p^2|bc \Rightarrow bc=sp^2$

entonces ocurre que $b = xp^2r^2+ysp^2 = p^2(xr^2+ys)$

luego $b = (xr^2+ys)p^2$ de donde $p^2|b$.

Sean p,q dos factores primos de a que dividen a "b" entonces p y q son dos factores primos de b es decir:

$b = pqr$ de donde $b^2 = p^2q^2r^2$

$p^2q^2|bc \Rightarrow bc = tp^2q^2$

$b = xb^2+ybc \Rightarrow b = p^2q^2xr^2+p^2q^2ty$

$\Rightarrow b = p^2q^2(xr^2+ty)$

$\Rightarrow p^2q^2|b$

De igual manera se prueba que si p,q son dos factores primos que dividen a "c" entonces $p^2 q^2 | c$

Por inducción tendremos que

$p_1^2 \cdot p_2^2 \cdots p_m^2 | b$

$q_1^2 \cdot q_2^2 \cdots q_r^2 | c$

Además $p_1^2 \cdot p_2^2 \cdots p_m^2 \leq b$; $q_1^2 \cdot q_2^2 \cdots q_r^2 \leq c$

Si $p_1^2 \cdot p_2 \cdots p_m^2 < b$

$a^2 = p_1^2 \cdot p_2^2 \cdots p_m^2 \; q_1^2 \cdot q_2^2 \cdots q_r^2 < bc = a^2$

entonces $b = (p_1 \cdot p_2 \cdots p_m)^2 = u^2$

$c = (q_1 \cdot q_2 \cdots q_r)^2 = v^2$

3-3 ALGUNAS ECUACIONES DIOFANTINAS

Una de las partes más atrayentes de la teoría de números es el estudio de las ecuaciones diofantinas. Se trata de ecuaciones $p(x_1, x_2, \ldots, x_n) = 0$, siendo p un polinomio de coeficientes en Z (resp. en Q), de las que se buscan las soluciones (x_i) en números enteros (resp. en números racional). Es decir cualquier ecuación en la que sus soluciones se restrinjan a valores enteros o, en ocaciones, racionales, recibe el nombre de ecuación diofantina.

En este caso, existe la restrincción adicional de que los resultados no sólo deben ser enteros, sino que, además, no pueden ser negativos.

Existen variedades sin fin de las ecuaciones diofantinas y no se tiene un método general de solución.

Vamos a estudiar aquí dos casos particulares de la famosa ecuación de Fermat:

$x^n + y^n = z^n$. $x,y,z \in \mathbb{N}^*$ donde $\mathbb{N}^* = \mathbb{N} - \{0\}$

Fermat afirmó haber demostrado que, para $n \geq 3$, esta ecuación no tiene solución en números enteros todos distintos de cero; su demostración no ha sido hallada; a pesar de los esfuerzos de muchos matemáticos, nunca se ha probado para todo entero n.

PROPOSICION 3-3.1

" Sean x,y,z elementos de $\mathbb{N}^*$. Entonces:

$x^2 + y^2 = z^2 \iff$ existen un natural $d>0$ y u,v enteros primos entre sí tal que:

$x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$ ó

$y = d(u^2 - v^2)$, $x = 2duv$, $z = d(u^2 + v^2)$ "

DEMOSTRACION

$\Rightarrow$) Sea $d = m.c.d(x,y,z)$

Sean $x' = \frac{x}{d}$, $y' = \frac{y}{d}$, $z' = \frac{z}{d}$

$$x'^2 + y'^2 = z'^2$$

x', y', z' son primos entre sí (porque están divididos entre su m.c.d); entonces son primos entre sí dos a dos.

" Veamos que x', y' son primos entre sí "

Supongamos que no son primos entre sí.

Sea $m > 1$ tal que $m \mid x'$, $m \mid y'$

Si p es un factor primo de m entonces

$p|x'$, $p|y'$, también se va a tener que:

$p|x'^2$, $p|y'^2 \Rightarrow p|(x'^2+y'^2) \Rightarrow p|z'^2 \rightarrow p|z'$

Contradicción; porque $p|x'$, $p|y'$ y $p|z'$ no puede ser porque x' ,y' ,z' son primos entre sí.

En forma similar se prueba que:

x' ,y' son primos entre sí

y' ,z' son primos entre sí.

" Por ser x' ,y' ,z' primos entre sí; no pueden ser los tres números impares "

PRUEBA

Sean $x' = 2a+1$, $y' = 2b+1$, $z' = 2c+1$

Luego: $x'^2 = 4a^2+4a+1$; $y'^2 = 4b^2+4b+1$; $z'^2 = 4c^2+4c+1$

Así: $x'^2+y'^2 = z'^2$

$(4a^2+4a+1)+(4b^2+4b+1) = 4c^2+4c+1$

$4(a^2+a)+1+4(b^2+b)+1 = 4(c^2+c)+1$

$4k+1+4k'+1 = 4k''+1$

$4k+4k'+2 = 4k''+1$

$4(k+k')+2 = 4k''+1$ contradicción.

" No pueden ser los tres pares "

Por ser primos entre sí.

" No puede ser que dos sean pares y el otro impar"

PRUEBA

Sean $x' = 2a$,$y' = 2b+1$, $z' = 2c$

$x'^2 = 4a$, $y'^2 = 4b^2+4b+1$, $z'^2 = 4c^2$

$x'^2 + y'^2 = z'^2$

$4a^2 + 4b^2 + 4b + 1 = 4c^2$

$4(a^2 + b^2 + b) + 1 = 4c^2$

$4k + 1 = 4c^2$ contradicción

ya que $4k+1$ es impar y

$4c^2$ es par.

" No pueden ser x', y' impar y z' par "

PRUEBA

Sean $x' = 2a+1$, $y' = 2b+1$, $z' = 2c$

$x'^2 = 4a^2+4a+1$, $y'^2 = 4b^2+4b+1$, $z'^2 = 4c^2$

$x'^2 + y'^2 = z'^2$

$(4a^2 + 4a + 1) + (4b^2 + 4b + 1) = 4c^2$

$4(a^2 + a) + 1 + 4(b^2 + b) + 1 = 4c^2$

$4(a^2 + a + b^2 + b) + 2 = 4c^2$

$4t + 2 = 4c^2$

$2 = 4(c^2 - t)$ contradicción

(porque serían multiplos de 4)

Luego tiene que ser x' impar, y' par, z' impar

ó x' par, y' impar, z' impar.

Sea x' impar, y' impar, z' impar

$y' = 2y''$ (par)

Tenemos que $x'^2 + y'^2 = z'^2$

$\Rightarrow y'^2 = z'^2 - x'^2$

$\Rightarrow y'^2 = (z' + x')(z' - x')$ *

m.c.d$(2z', 2y') = 2$ y $2z' = (z' + x') + (z' - x')$

$2x' = (z' + x') - (z' - x')$

Luego tenemos que el m.c.d$(z' + x' , z' - x') = 2$

por proposición 3-2.9

Luego $z' + x' = 2x''$ (es par)

y $z' - x' = 2z''$ (es par)

Pero x'', z'' son primos entre sí

si no $2 \neq$ m.c.d$(z' + x' , z' - x')$

$y'^2 = 2x'' \cdot 2z'' = 4x'' z''$ (por $\star$)

$y' = 2y'' \Rightarrow 4y''^2 = 4x'' z'' \Rightarrow y''^2 = x'' z''$

x'' es de la forma $x'' = u^2$

z'' es de la forma $z'' = v^2$ (por proposición 3-2.11)

Luego $y''^2 = 4x'' z'' \Rightarrow y''^2 = 4u^2 v^2$

$\Rightarrow y'' = 2uv$

$2z' = 2u^2 + 2v^2 \Rightarrow z' = u^2 + v^2$

$2x' = 2u^2 - 2v^2 \Rightarrow x' = u^2 - v^2$

pero por hipótesis tenemos que

$x' = \frac{x}{d} \Rightarrow x = dx'$ de donde $x = d(u^2 - v^2)$

$y' = \frac{y}{d} \Rightarrow y = dy'$ de donde $y = d(2uv)$

$z' = \frac{z}{d} \Rightarrow z = dz'$ de donde $z = d(u^2 + v^2)$

$\Leftarrow$) En este sentido solamente hay que verificar

que $x^2 + y^2 = z^2$

Sean: $x = d(u^2 - v^2) = du^2 - dv^2$

$x^2 = (du^2 - dv^2)^2$

$x^2 = (du^2)^2 - 2(du^2)(dv^2) + (dv^2)^2$

de donde $x^2 = d^2 u^4 - 2d^2 u^2 v^2 + d^2 v^4$.

$y = 2duv \Rightarrow y^2 = 4d^2 u^2 v^2$

$z = d(u^2+v^2) = du^2+dv^2$

$z^2 = (du^2+dv^2)^2 = (du^2)^2+2(du^2)(dv^2)+(dv^2)^2$

de donde $z^2 = d^2u^4+2d^2u^2v^2+d^2v^4$

Así:

$d^2u^4-2d^2u^2v^2+d^2v^4+4d^2u^2v^2 = d^2u^4+2d^2u^2v^2+d^2v^4$

de donde $d^2u^4+2d^2u^2v^2+d^2v^4 = d^2u^4+2d^2u^2v^2+d^2v^4$

Luego $x^2+y^2 = z^2$

PROPOSICION 3.3.2

" La ecuación $x^4+y^4 = z^2$ no tiene solución en $\mathbb{N}^*$ "

DEMOSTRACION

Procedamos por reducción al absurdo.

Supongamos que sí existen soluciones para la ecuación.

Sea $z_0 = \min\{m \in \mathbb{N}^* \text{ / existen } x,y \text{ en } \mathbb{N}^* \text{ tal que } x^4+y^4 = m^2\}$

Existen x,y en $\mathbb{N}^*$ tal que $x^4+y^4 = z_0^2$ donde z_0 es minimal, entonces x,y,z_0 son primos entre sí dos a dos.

" x,y son primos entre sí "

En efecto:

Si $d>0$ tal que $d|x$, $d|y$ entonces $d^4 | x^4$, $d^4 | y^4$

$d^4 | x^4+y^4$ pero $x^4+y^4 = z_0^2$ entonces $d^4 | z_0^2$

por tanto $d^2 | z_0$ y $(\frac{x}{d})^4+(\frac{y}{d})^4 = (\frac{z_0}{d^2})^2$ sería una solución que contradice la minimidad de z_0

Porque $\frac{z_0}{d^2}$ es menor que z_0

De modo semejante se prueba que

" x, z_0 son primos entre sí "

" y, z_0 son primos entre sí"

Luego x^2, y^2, z_0 son primos entre sí.

Como nuestra ecuación puede escribirse en la forma $(x^2)^2+(y^2)^2 = z_0^2$ podemos aplicar la proposición 3-2.1: salvo permutaciones eventuales de x,y; luego existen u,v primos entre sí tal que $x^2 = u^2 - v^2$, $y^2 = 2uv$, $z_0 = u^2+v^2$ o bien $x^2 = 2uv$, $y^2 = u^2 - v^2$, $z_0 = u^2+v^2$

Según como lo hemos tomado si y^2 es par, entonces y es par.

Sea $y = 2a$ entonces $y^2 = 4a^2$

Si $4a^2 = 2uv$ entonces (u es par y v impar) o (u impar y v par)

u,v no pueden ser ambos pares, por que son primos entre sí.

" No puede ser u par, v impar "

Supongamos:

$$u = 2b, \quad v = 2c+1$$

$$x^2 = u^2 - v^2 = (2b)^2 - (2c+1)^2$$

$$= 4b^2 - (4c^2+4c+1)$$

Luego $x^2 = 4b^2 - 4c^2 - 4c - 1 = 4(b^2 - c^2 - c) - 1$

Llamándole t a $(b^2 - c^2 - c)$ tenemos

$x^2 = 4t-1$

x es par o impar

$x = 2d \Rightarrow x^2 = 4d \Rightarrow 4d^2 = 4t-1$

$x = 2d+1 \Rightarrow x^2 = 4d^2+4d+1 \Rightarrow 4d^2+4d+1 = 4t-1$

$\Rightarrow 4d^2+4d-4t = -2$

$\Rightarrow 4(d^2+d-t) = -2$

$\Rightarrow 4p = -2$

Luego tiene que ser u impar, v par.

Supongamos que $v=2v'$ entonces $y^2=4uv'$; u,v' primos entre sí $\Rightarrow (\frac{v}{2})^2 = uv'$, luego u,v' son de la forma $u = a^2$, $v' = b^2$

Como $x^2 = u^2-v^2$ entonces $x^2+v^2 = u^2$

Luego por la proposición 3-3.1 u es impar; x es impar. Luego existen c,d primos entre sí tal que $x = c^2-d^2$, $v = 2cd$, $u^2 = c^2+d^2$

Como: $v = 2v' = 2b^2 = 2cd \Rightarrow b^2 = cd$

Luego c,d son de la forma $c=h^2$, $d=r^2$

$a^2=u = h^4+r^4 \Rightarrow h^4+r^4 = a^2$

" Hay que probar que $a<z_o$ "

$u = a^2 \Rightarrow a<u \Rightarrow a<u^2 \Rightarrow a<u^2+v^2 = z_o$

$\Rightarrow a<z_o$ (Contradicción)

Luego $x^4+y^4 = z^2$ no tiene solución en $\mathbb{N}^*$.

PROPOSICION 3-3.3

" La ecuación $x^4+y^4 = z^4$ no tiene solución en $\mathbb{N}^*$ "

En efecto, esta ecuación puede escribirse en la forma $x^4+y^4 = (z^2)^2$ y aplicando la proposición 3-3.2 queda probado 3-3.3.

3-4 INDICADORES DE EULER

Sea $n \in \mathbb{N}^*$. Llamamos indicador de Euler de n, y notamos $\psi(n)$ el número de enteros P primos con n y tales que $0 \leq p \leq n$ es decir

$\psi(n) = \text{card}\{p \in \mathbb{N} / 0 \leq p \leq n;\ P,\ n \text{ primos entre si}\}$

También podemos escribir

$\psi(n) = \text{card}\{P \in \mathbb{N} / 1 \leq p \leq n-1;\ P,\ n \text{ primos entre sí}\}$

pues 0 y n no son primos con n.

Ejemplo: Sea n=12. Entre los números 1,2,3,4,5,6,7,8,9,10,11, solamente hay cuatro primos con 12: son ellos 1,5,7,11 por tanto $\psi(12) = 4$.

Convencionalmente definimos $\psi(1)=1$

Si n=p es un número primo, es evidente que todos los números de 1 a p-1 son primos con P.

luego $\psi(p) = p-1$.

PROPOSICION 3-4.1

" P un natural primo, $r \in \mathbb{N}^*$, $t \in \mathbb{N}^*$.
entonces t es primo con P^r <=> t no es multiplo de P ".

DEMOSTRACION

=>] Si t=mp, m>1 entonces $P|t$, $P|p^r$

$P|t$ y $P|p^r$ => P y t no son primos entre sí (lo cual no es posible)

$\Leftarrow$) Supongamos que t y p^r no son primos entre sí

y sea b>1 tal que $b|t$, $b|p^r$

entonces $t = mb$

$p^r = nb$

$p.p.p....p = nb$

$\Rightarrow P|b \Rightarrow b = pq$

luego $t = mb \rightarrow t = mpq$

de donde t es multiplo de P.

Para $n = p^r$, potencias de un número primo, $r \in \mathbb{N}^*$; los enteros primos con p^r son los enteros no multiplos de P; como hay p^{r-1} multiplos de P entre 1 y p^r entonces $\psi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$ en donde $p^r - p^{r-1}$ da la cantidad de números que no son multiplos de P.

A partir de esto nos proponemos calcular $\psi(n)$ utilizando la descomposición de n en factores primos.

PROPOSICION 3-4.2

" Sean $n \in \mathbb{N}^*$, $q \in \mathbb{N}^*$

Entonces las condiciones que siguen son equivalentes.

1) q y n son primos entre sí
2) $q+n\mathbb{Z}$ es inversible en el anillo $\frac{\mathbb{Z}}{n\mathbb{Z}}$
3) $q+n\mathbb{Z}$ es generador del grupo $\frac{\mathbb{Z}}{n\mathbb{Z}}$ "

DEMOSTRACION

1) $\Rightarrow$ 2) El conjunto $[nx/x\in Z] = nZ$ es un ideal de Z, luego podemos formar el anillo cociente $\frac{Z}{nZ}$ en donde nZ es la identidad para la suma y $1+nZ$ es la identidad para el producto.

Existen x,y en Z tales que $1=xq+yn$

$(x+nZ)(q+nZ) = xq+nZ$

$xq-1 = xq-xq-yn = -yn = n(-y)\in nZ$

$\Rightarrow \quad xq-1\in nZ \quad \Rightarrow xq+nZ= 1+nZ$

Luego $q+nZ$ es inversible.

2) $\Rightarrow$ 3) Sea $x\in Z$ tal que

$(q+nZ)(x+nZ) = 1+nZ$

Sea $a\in Z$ veamos que $a+nZ\in \left[\, q+nZ \,\right]$

$a+nZ = (a+nZ)(1+nZ) = (a+nZ)(qx+nZ)$

$= aqx+nZ = ax(q+nZ)\in \left[\, q+nZ \,\right]$

Luego $a+nZ\in \left[\, q+nZ \,\right]$

3) $\Rightarrow$ 1) Existe $x\in Z$ tal que

$1+nZ = x(q+nZ) = xq+nZ$

Luego $1+nZ = xq+nZ$

Existe $p\in Z$ tal que $1=xq+np$

Probemos que el m.c.d de n y q es 1.

Sea d tal que: $d|q$ y $d|n$

Por lo tanto $q=ad$, $n=bd$

Como $1=xq+np$ entonces

$1=xad+bdp = d(xa+bp)$

Luego $1=d(xa+bp) \Rightarrow d|1$

PROPOSICION 3-4.3

" Sea $n \in \mathbb{N}^*$. Entonces:

. $\psi(n)$ es igual a la cantidad de elementos $q+nZ$ tal que $q+nZ$ es un generador del grupo $\frac{Z}{nZ}$

. $\psi(n)$ es igual a la cantidad de elementos $q+nZ$ tal que $q+nZ$ es inversible en el anillo $\frac{Z}{nZ}$ "

DEMOSTRACION

Bastará probar quepara cada $q+nZ$ hay un único $x \in \mathbb{N}^*$ tal que $0 \leq x \leq n-1$: $x+nZ=q+nZ$

Sea $B=\{z \in Z / 0 \leq q+nz\}$

$z_0 = \min B$, $x = q+nz_0$

. $0 \leq x$ (por definición de B)

. " $x \leq n-1$ "

Supongamos $n-1<x$

$n-1<x \Rightarrow n \leq x$

$n \leq q+nz_0 \Rightarrow 0 \leq q+nz_0-n$

$\Rightarrow 0 \leq q+n(z_0-1)$ contradicción

Luego $0 \leq x \leq n-1$

" $x+nZ = q+nZ$ "

$x = q+nz_0 \Rightarrow x-q = nz_0 \in Z$

Probemos que x es único

Sea $p \in \mathbb{N}$ tal que $0 \leq p \leq n-1$ y $p+nZ=q+nZ$

$p+nZ = q+nZ \Rightarrow p-q \in nZ$

$\Rightarrow p-q = ny$, $y \in Z$

$\Rightarrow p = q+ny$

$0 < q+ny \Rightarrow z_0 \leq y$

si $p \neq x$ entonces $z_0 < y$

$z_0 < y \Rightarrow z_0 + 1 \leq y$

$0 < q+nz_0 \Rightarrow -1 < q+nz_0$

$\Rightarrow n-1 < q+nz_0+n$

$\Rightarrow n-1 < q+n(z_0+1)$

$\Rightarrow n-1 < q+ny$

$\Rightarrow n-1 < p$ (contradicción)

Porque pueden cumplirse al mismo tiempo las condiciones.

PROPOSICION 3-4.4

" A un anillo unitario conmutativo

I,J ideales de A

$I+J = A$

Entonces:

1) $I \cap J = [IJ]$

2) Hay un isomorfismo entre:

$$\frac{A}{[IJ]} \quad y \quad \frac{A}{I} \times \frac{A}{J} \quad "$$

DEMOSTRACION

Sabemos que $[IJ]$ es el más pequeño ideal que contiene a I,J.

$$\left[IJ\right]=\{\sum_{i=n}^{n} x_i y_i \,/\, n\in\mathbb{N}^*,\ x_i\in I,\ y_i\in J\}$$

Para 1) $I\cap J = \left[IJ\right] \Leftrightarrow I\cap J\subset \left[IJ\right]$ y $\left[IJ\right]\subset I\cap J$

" $I\cap J\subset \left[IJ\right]$ "

$x\in I\cap J \Rightarrow x\in I$ y $x\in J$

Como A es unitario entonces $1\in A$

$1\in A \Rightarrow 1\in I+J$ ya que $I+J = A$ por hipótesis

$1\in I+J$ implica que 1 es de la forma $a+y$

con $a\in I$, $y\in J$.

$1=a+y \Rightarrow x.1=x(a+y)$

$\Rightarrow x.1=xa+xy$

$\Rightarrow x=xa+xy\in \left[IJ\right]$

de donde $x\in \left[IJ\right]$

Luego $I\cap J\subset\left[IJ\right]$.

" $\left[IJ\right]\subset I\cap J$ " Basta probar que

" $IJ\subset I\cap J$" Sea $U\in IJ$ tal que $U=xy$

con $x\in I$, $y\in J$ entonces $xy\in I$ y $xy\in J$

de donde $xy\in I\cap J$

Luego $\left[IJ\right]\subset I\cap J$.

Para 2) $\psi: \dfrac{A}{\left[IJ\right]} \longrightarrow \dfrac{A}{I}\times\dfrac{A}{J}$ es isomorfismo

recordemos que

$\psi: A \longrightarrow \dfrac{A}{I}\times\dfrac{A}{J}$ tal que

$x \rightsquigarrow (x+I, x+J)$

es un morfismo de anillos.

$x \in Ker(\psi) \iff \psi(x)=0$

$\iff \psi(x)=(I,J)$

$\iff (x+I,x+J)=(I,J)$

$\iff x+I=I \quad y \quad x+J=J$

$\iff x \in I \quad y \quad x \in J$

$\iff x \in I \cap J$

Por lo tanto $Ker(\psi) = I \cap J$.

Veamos ahora que

$$\psi : \frac{A}{I \cap J} \longrightarrow \frac{A}{I} \times \frac{A}{J}$$

$x+(I \cap J) \rightsquigarrow (x+I,x+J)$ es un morfismo

Probemos que ψ esta bien definida o sea que

$x+(I \cap J) = y+(I \cap J) \Rightarrow \psi(x) = \psi(y)$

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

$\Rightarrow x-y \in Ker(\psi)$

$\Rightarrow \psi(x-y) = 0$

$\Rightarrow (x-y+I,x-y+J) = 0$

$\Rightarrow (x-y+I,x-y+J)=(I,J)$

$\Rightarrow x-y+I=I \quad y \quad x-y+J=J$

$\Rightarrow x-y \in I \quad y \quad x-y \in J$

$\Rightarrow x+I=y+I \quad y \quad x+J=y+J$

$\Rightarrow (x+I,x+J) = (y+I,y+J)$

$\Rightarrow \psi(x) = \psi(y)$

Probemos que ψ es morfismo de anillos.

i) "$\psi((x+(I \cap J))+(y+(I \cap J))) = \psi(x+(I \cap J))+\psi(y+(I \cap J))$"

$\psi((x+(I \cap J))+(y+(I \cap J))) = \psi((x+y)+I \cap J)$

$= ((x+y)+I,(x+y)+J)$

$= ((x+I)+(y+I),(x+J)+(y+J))$

$= (x+I,x+J)+(y+I,y+J)$

$= \psi(x+(I\cap J))+\psi(y+(I\cap J))$

ii) " $\psi(a(x+I\cap J))= a\psi(x+(I\cap J))$"

$\psi(a(x+I\cap J)) = (ax+I,ax+J)$

$= a(x+I,x+J)$

$= a\psi(x+(I\cap J))$

Probemos que ψ es inyectiva

Sean$x,y\in A$ tal que $\psi(x+(I\cap J))= \psi(y+(I\cap J))$

$\psi(x+(I\cap J)) = \psi(y+(I\cap J))$

$\Rightarrow (x+I,x+J) = (y+I,y+J)$

$\Rightarrow x+I = y+I \quad y \quad x+J = y+J$

$\Rightarrow x-y\in I \quad y \quad x-y\in J$

$\Rightarrow x-y\in I\cap J$

$\Rightarrow x+I\cap J = y+I\cap J$

de donde ψ es inyectiva.

Probemos que ψ es suryectivo

$1\in A \Rightarrow 1\in I+J \Rightarrow 1=a+y$ con $a\in I$, $y\in J$

Sea $(m+I,n+J)\in \frac{A}{I}\times\frac{A}{J}$, $z=my+na$

$\psi(z+(I\cap J)) = (z+I,z+J)$

Probemos que $(z+I,z+J)=(m+I,n+J)$

Debemos probar que $m+I=z+I \quad y \quad z+J=n+J$

Prueba: $m-z=m-(my+na) = m-my-na$

$=m(1-y)-na = m(a+y-y)-na$

$=ma-na = (m-n)a\in I$

Luego $m-z\in I$. de donde $m+I = z+I$.

Prueba: $z-n = my+na-n = my+n(a-1)$

$= my+n(a-a-y) = my-ny$

$= (m-n)y \in J$

Luego $z-n \in J$ de donde $z+J=n+J$

PROPOSICION 3-4.5

" A un anillo unitario conmutativo

$I_1, I_2, \ldots, I_r$ ideales de A tales que

$I_i + I_j = A$, si $i \neq j$.

Entonces hay un isomorfismo entre

$$\frac{A}{[I_1, I_2, \ldots, I_r]} \quad y \quad \frac{A}{I_1} \times \frac{A}{I_2} \times \ldots \times \frac{A}{I_r} \text{ "}$$

DEMOSTRACION (Por inducción)

Para n=2 tenemos el isomorfismo

$$\frac{A}{[I_1\ I_2]} \longrightarrow \frac{A}{I_1} \times \frac{A}{I_2}$$

Esto es cierto por proposición 3-4.4

Supongámoslo cierto para n=r-1

$J = [I_2\ I_3 \ldots I_r]$

Probemos que $I_1 + J = A$

$I_1 + I_2 = A \Rightarrow 1 = x_2 + y_2$

$I_1 + I_3 = A \Rightarrow 1 = x_3 + y_3$

.

.

.

.

.

$I_1 + I_r = A \Rightarrow 1 = x_r + y_r$

de donde obtenemos

$1 = (x_2 + y_2)(x_3 + y_3) \ldots\ldots (x_r + y'_{r-})$

$1 = x_2 x_3 \ldots x_r + \text{———} + y_2 y_3 \ldots y_r$

Luego $1 \in I_1 + J$

$x \in A \Rightarrow x.1 \in I_1 + J \Rightarrow A \subseteq I_1 + J$

y siempre se da $I_1 + J \subseteq A$

de donde $I_1 + J = A$

Luego hay un isomorfismo

$$f: \frac{A}{[I_1 J]} \longrightarrow \frac{A}{I_1} \times \frac{A}{J}$$

Además hay un isomorfismo

$$g: \frac{A}{J} \longrightarrow \frac{A}{I_2} \times \frac{A}{I_3} \times \ldots \times \frac{A}{I_r}$$

Por hipótesis inductiva

$$h: \frac{A}{I_1} \times \frac{A}{J} \longrightarrow \frac{A}{I_1} \times \frac{A}{I_2} \times \frac{A}{I_3} \times \ldots \times \frac{A}{I_r}$$

Asi tenemos

$$\frac{A}{[I_1 J]} \xrightarrow{f} \frac{A}{I_1} \times \frac{A}{J} \xrightarrow{h} \frac{A}{I_1} \times \frac{A}{I_2} \times \ldots \times \frac{A}{I_r}$$

es decir (hof) es el isomorfismo buscado.

Apliquemos ahora las proposiciones 3-4.4 y 3-4.5 al anillo Z.

PROPOSICION 3-4.6

" Si m,n son dos números de N* primos entre sí, entonces hay un isomorfismo entre:

$$\frac{Z}{mnZ} \quad y \quad \frac{Z}{mZ} \times \frac{Z}{nZ} \quad "$$

DEMOSTRACION

Esta proposición es un caso particular de la proposición 3-4.4. Luego basta probar que

$mZ+nZ = Z$

Como m y n son primos entre sí entonces

$1 = mx+ny$ con x,y en Z

Sea $z \in Z$ entonces $z = z.1 = z(mx+ny)$

$= mzx+nzy \in mZ+nZ$

de donde $Z \subset mZ+nZ$

Como es para cualquier Z entonces

$mZ+nZ = Z$

PROPOSICION 3-4.7

" S i m,n son naturales primos entre sí entonces:

$\psi(mn) = \psi(m)\psi(n)$ "

DEMOSTRACION

$\psi(mn) = card\{a+mnZ \;/\; a+mnZ$ es inversible en $\frac{Z}{mnZ}\}$

$$= \text{card}\{(x+mZ, y+nZ)/(x+mZ, y+nZ) \text{ es inversible en } \frac{Z}{mZ} \times \frac{Z}{nZ}\}$$

$$= \text{card}\{x+rZ/x+rZ \text{ es inversible en } \frac{Z}{mZ}\} \cdot \text{card}\{x+tZ/x+tZ \text{ es inversible en } \frac{Z}{nZ}\}$$

$$= \psi(m).\psi(n)$$

PROPOSICION 3-4.8

" Sean $n \in \mathbb{N}^*$, $n = p_1^{\alpha 1}.p_2^{\alpha 2} \ldots p_r^{\alpha r}$ su descomposición en factores primos. Entonces:

$$\psi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2}).....(1-\frac{1}{p_r}) \text{ "}$$

DEMOSTRACION

Por la proposición 3-4.7 tenemos

$$\psi(n) = \psi(p_1^{\alpha 1}).\psi(p_2^{\alpha 2}).\psi(p_3^{\alpha 3})\ldots\psi(p_r^{\alpha r})$$

$$= (p_1^{\alpha 1} - p_1^{\alpha 1 - 1})(p_2^{\alpha 2} - p_2^{\alpha 2 - 1})\ldots(p_r^{\alpha r} - p_r^{\alpha r - 1})$$

$$= p_1^{\alpha 1}(1-\frac{1}{p_1})p_2^{\alpha 2}(1-\frac{1}{p_2})\ldots p_r^{\alpha r}(1-\frac{1}{p_r})$$

$$= p_1^{\alpha 1}.p_2^{\alpha 2}\ldots p_r^{\alpha r}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_r})$$

$$= n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_r})$$

de donde obtenemos

$$\psi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_r})$$

3-5 MODULOS SOBRE ANILLOS PRINCIPALES

Con el fin de estudiar los módulos sobre un anillo principal, son necesarios algunos preliminares.

Sea A un anillo unitario conmutativo y (M,+) un grupo conmutativo. M es llamado un A-módulo a la izquierda si existe una aplicación μ: $A \times M \longrightarrow M$

$$(\alpha, x) \longmapsto \mu(\alpha, x) = \alpha x \quad (\alpha \in A, x \in M)$$

tal que los axiomas siguientes son satisfechos:

1) $\alpha(x+y) = \alpha x + \alpha y$

2) $(\alpha+\beta)x = \alpha x + \beta y$

3) $(\alpha\beta)x = \alpha(\beta x)$

4) $1x = x$ $\qquad (\alpha, \beta \in A; x, y \in M)$

Si el axioma 3) es sustituídos por $(\alpha\beta)x = \beta(\alpha x)$ Se tiene sobre M una estructura de A-módulo a la derecha.

Cuando se trabaja con A-módulos (a la izquierda ó a la derecha), los elementos de A son llamados escalares.

SUBMODULOS

Si A es un anillo y M es un A-módulo, un subconjunto E de M, diremos que E es un submódulo de M si:

1) E es un subgrupo del grupo (M,+)

2) $AE \subset E$

Es decir que E también es un A-módulo con las operaciones de M restrigidas a E.

Si M es un A-módulo y E es un subconjunto de M, se denotará por $[E]$ al subconjunto de E, formado por la intersección de todos los submódulos de M que contienen a E; $[E]$ es caracterizado por las propiedades siguientes:

1) $E \subset [E]$
2) $[E]$ es un submódulo de M
3) Si $H \subset M$ es un submódulo de M tal que $E \subset M$, entonces $[E] \subset H$.

Sea M un A-módulo y $E \subset M$, el conjunto

$\{ \sum_{i=1}^{n} \alpha_i x_i / n \in N^*, \alpha_i \in A, x_i \in E \}$ nos da la forma

de los elementos de $[E]$.

$E \subset M$, M un A-módulo, se dice que E es linealmente independiente si

$$\sum_{i=1}^{m} \beta_i x_i = 0 \Rightarrow \beta_1 = \beta_2 = \ldots \beta_m = 0$$

Para todo $m \in N$, para todo $x_i \in L$, para todo $\beta_i \in \lambda$

Sean $E \subset M$, M un A-módulo

E es una base de M si

1) $M = [E]$
2) E es linealmente independiente

Un A-módulo M se dice que es de tipo finito si existe $E \subset M$ tal que

E es finito y $[E] = M$

Un A-módulo M es llamado libre si posee una base.

Se llama dimensión o rango de un A-módulo libre M, al mayor cardinal de los conjuntos linealmente independientes.

MORFISMOS DE MODULOS

Sean M y N dos módulos sobre un mismo anillo A; una aplicación $f:M \longrightarrow N$ es llamada un morfismo (de módulos) si

1) $f(x+y) = f(x)+f(y)$
2) $f(\alpha x) = \alpha f(x)$

Para todo $\alpha \in A$ y todo $x,y \in M$.

PROPOSICION 3-5.1

"A Un anillo principal
M un A-módulo libre de dimensión finita n
$0 \neq E \subset M$ un sub-módulo de M.

Entonces:

1) E es libre y dim $E \leq n$
2) Existen $\{e_1, e_2, \ldots, e_n\}$ una base de M, un natural $r \leq n$, $\alpha_1, \alpha_2, \ldots, \alpha_r$ elementos no nulos de A tal que $\{\alpha_1 e_1, \alpha_2 e_2, \ldots, \alpha_r e_r\}$ es una base de E y α_i divide a α_{i+1} Para todo $i \leq r-1$.

DEMOSTRACION

Denotemos por M* al conjunto Mor(M,A), es decir al conjunto cuyos elementos son los morfismos de A módulo de M en A. Si $U \subset M^*$, U(E) es un ideal de A, y como A es principal existe $\alpha_u \in A$ tal que $U(E)=A\alpha_u$; luego la familia $(U(E))_{u \in M^*}$ esta formada por submódulos de A de tipo finito y por tanto admite un elemento máximal; sea $t \in M^*$ tal que t(E) es un elemento máximal de la familia $(U(E))_{u \in M^*}$. Sea $(x_1, x_2, \ldots, x_n)$ una base de M y consideremos los morfismos.

$$PJ: M \longrightarrow A: \sum_{i=1}^{n} \alpha_i x_i \rightsquigarrow \alpha_J \text{ para todo } J \leq n;$$

como $E \neq (0)$, existe algún $J \leq n$ tal que
$PJ(E) \neq (0)$, lo que significa que $\alpha_t \neq 0$;
como $\alpha_z \in A_{\alpha t}$ existe $e \in E$ tal que $\alpha_t = t(e)$.
Probemos que para todo $F \in M^*$, α_t divide a F(e):
si d es el máximo común divisor de α_t y F(e), existen α, b en A tales que $d=\alpha_{\alpha t}+bF(e)$, o sea
$d= (\alpha_t+bF)(e)$ implica $Ad \subset (\alpha_t+bF)(E)$;
como d divide a α_t, $A\alpha_t \subset Ad$;
$A\alpha_t$ máximal implica $A\alpha_t = (\alpha_t+bF)(E)$ de donde
$A\alpha_t = Ad$; luego α_t divide αd implica α_t divide a F(e).

En particular α_t divide a cada PJ(e), para todo $J \leq n$; sea $PJ(e)=\alpha_t b_j$; $bJ \in A$, $J \leq n$.

Si $x_o = \sum_{i=1}^{n} b_i x_i$ entonces $\alpha_t x_o = \sum_{i=1}^{n} \alpha_t b_i x_i = e$ y

$t(e)=t(\alpha_t x_o)=\alpha_t t(x_o)$, de donde $\alpha_t = \alpha_t t(x_o)$;

$\alpha_t (1-t(x_o))=0$, $\alpha_t (1-t(x_o))=0$, $\alpha_t \neq o$ implica $1=t(x_o)$

Probaremos que se cumple

I) $M = Ax_o \oplus Ker(t)$

II) $E = Ae \oplus E \cap Ker(t)$

donde las sumas son directas.

Si $x \in M$, x se puede escribir en la forma

$x = t(x)x_o+(x-t(x).x_o)$, y entonces tenemos

$t(x-t(x).x_o)=t(x)-t(x)t(x_o)=t(x)-t(x)=0$;

la suma es directa ya que $t(\alpha x_o)=0$,

$\alpha \in A$, implica $\alpha.1=0$, de donde $\alpha=0$;

luego $\alpha x_o = 0$.

Si x es un elemento de E, x puede escribirse

$x=t(x).x_o+(x-t(x).x_o)$;

$t(E)=A\alpha_t$ implica existe $B \in A$ tal que $t(x).x_o =$

$B\alpha_t .x_o = B.e \in Ae$; $x-t(x)x_o = x-Be \in E$;

$t(x-t(x).x_o) = t(x)-t(x).t(x_o) = t(x)-t(x_o)-t(x) = 0$

implica $x-t(x).x_o \in Ker(t)$; luego $E=Ae+E \cap Ker(t)$;

la suma es directa ya que si existe $\psi \in A$ tal que

$t(\psi(e))=0$, entonces $\psi e=\psi\alpha_t .x_o \in Ax_o$ implica

$\psi e=0$.

Demostraremos ahora la parte 1) de la proposición

Por inducción sobre la dimensión r de E.

si $r=0$, $E=\{o\}$ implica E libre y dim $E \leq n$.

Si $r>0$, $\dim(E \cap \mathrm{Ker}(t))=r-1$, según II), y luego es libre por inducción inductiva; luego si $\{e_1, e_2, \ldots, e_{r-1}\}$ es una base de $E \cap \mathrm{Ker}(t)$, entonces $\{e, e_1, e_2, \ldots, e_{r-1}\}$ es una base de E, ya que la suma II) es directa.

Probemos ahora la parte 2) por inducción sobre la dimensión n de M. Es tribial si $n=0$.

Para $n>0$, Ker(t) es libre (por parte 1) y dimensión $(n-1)$, ya que la suma I) es directa; podemos aplicar la hipótesis inductiva al módulo libre Ker(t) y al sub-módulo (de Ker(t))

$E \cap \mathrm{Ker}(t)$, es decir que existen $(e_2, e_3, \ldots, e_n)$ una base de Ker(t); $r \leq n$ un entero positivo, $\alpha_2, \alpha_3, \ldots, \alpha_r$ elementos no nulos de A tales que $(\alpha_2 e_2, \alpha_3 e_3, \ldots, \alpha_r e_r)$ es una base de $E \cap \mathrm{Ker}(t)$ y α_i divide a α_{i+1} para $2 \leq i \leq r-1$. Si ponemos $x_o = e_1$, $\alpha_u = \alpha_1$ entonces $(e_1, e_2, \ldots, e_n)$ es una base de M (según I) y $(\alpha_1 e_1, \alpha_2 e_2, \ldots, \alpha_r e_r)$ es una base de E (según II) y del hecho de que $e = \alpha_1 e_1$)

Falta sólo demostrar que α_1 divide a α_2

Sea $V \in M^*$ definida así:

$V(e_1)=V(e_2)=1$, $V(e_i)=0$, $i \geq 3$; se tiene que

$\alpha_1 = \alpha_u = V(\alpha_u e_1) = V(e) \in V(E)$, de donde

$A\alpha_u \subset V(E)$; como $A\alpha_u$ es máximal,

$V(E) = A\alpha_u = A\alpha_1$; como $\alpha_2 = V(\alpha_2 e_2) \in V(E)$,

se tiene $\alpha_2 \in A\alpha_1$, lo cual implica α_1 divide a α_2 .

PROPOSICION 3-5.2

"A un anillo principal

E un A-módulo de tipo finito.

Entonces:

E es isomorfo a un módulo de la forma:

$\frac{A}{I_1} \times \frac{A}{I_2} \times \cdots \times \frac{A}{I_n}$ en donde $I_1, I_2, \ldots, I_n$ son

ideales de A tal que $I_n \subset I_{n-1} \subset \ldots \subset I_2 \subset I_1$ "

DEMOSTRACION

Sea $\{x_1, x_2, \ldots, x_n\}$ un generador de E.

Existe una función $f: A^n \longrightarrow E : (\alpha_i)_{i \leq n} \rightsquigarrow \sum_{i=1}^{n} \alpha_i x_i$

tal que f es sobre y morfismo de módulo de modo que:

$\overline{f}: \frac{A^n}{Ker(f)} \longrightarrow E$ tal que $x + Ker(f) \rightsquigarrow f(x)$

es morfismo biyectivo.

A^n es un A-módulo libre

$(e'_1, e'_2, \ldots, e'_n)$ es una base de A^n, en donde

$e'_1 = (1,0,0,\ldots,0)$

$e'_2 = (0,1,0,\ldots,0)$

$e'_3 = (0,0,1,\ldots,0)$

.

.

.

.

.

$e'_n = (0,0,0,\ldots,1)$

Ker(f) es un submódulo de A^n

Existe una base $(e_1, e_2, \ldots, e_n)$ de A^n

un natural $r \leq n$.

$\alpha_1, \alpha_2, \ldots, \alpha_r$ elementos no nulos de A tal que

$(\alpha_1 e_1, \alpha_2 e_2, \ldots, \alpha_r e_r)$ es una base del Ker(f)

y α_1 divide α_{i+1} para todo $i<r$

Definamos $\alpha_{r+1} = \alpha_{r+2} = \ldots = \alpha_n = 0$

La función $g: \prod_{i=1}^{n} \frac{Ae_i}{A\alpha_i e_i} \longrightarrow \frac{A^n}{Ker(f)}$

$$(\beta_1 e_1 + A\alpha_1 e_1, \ldots\ldots, \beta_n e_n + A\alpha_n e_n)$$
$$\rightsquigarrow \left(\sum_{i=1}^{n} \beta_i e_i + Ker(f)\right)$$

es un morfismo biyectivo.

Probemos que "g esta bien definida"

" $(\beta_1 e_1 + A\alpha_1 e_1, \beta_2 e_2 + A\alpha_2 e_2, \ldots, \beta_n e_n + A\alpha_n e_n) =$

$(\gamma e_1 + A\alpha_1 e_1, \gamma_2 e_2 + A\alpha_2 e_2, \ldots, \gamma_n e_n + A\alpha_n e_n)$

$\Rightarrow \sum_{i=1}^{n} \beta_i e_i + Ker(f) = \sum_{i=1}^{n} \gamma_i e_i + Ker(f)$ "

$(\beta_1 e_1 + A\alpha_1 e_1, \ldots, \beta_n e_n + A\alpha_n e_n) = (\gamma_1 e_1 + A\alpha_1 e_1, \ldots, \gamma_n e_n + A\alpha_n e_n)$

$\Rightarrow \beta_1 e_1 + A\alpha_1 e_1 = \gamma_1 e_1 + A\alpha_1 e_1, \ldots, \beta_n e_n + A\alpha_n e_n = \gamma_n e_n + A\alpha_n e_n$

$\Rightarrow \beta_i e_i - \gamma_i e_i \in A\alpha_i e_i$

$\Rightarrow \beta_i e_i - \gamma_i e_i = \delta_i \alpha_i e_i$ para todo $i \leq n$ y $\delta_i \in A^n$

$\Rightarrow (\beta_i - \gamma_i)e_i = \delta_i \alpha_i e_i$

Queremos $\sum_{i=1}^{n} \beta_i e_i + Ker(f) = \sum_{i=1}^{n} \gamma_i e_i + Ker(f)$

esto es cierto si $\left(\sum_{i=1}^{n} \beta_i e_i - \sum_{i=1}^{n} \gamma_i e_i \right) \varepsilon\ Ker(f)$

y esto es cierto si "$f\left(\sum_{i=1}^{n} \beta_i e_i - \sum_{i=1}^{n} \gamma_i e_i\right) = 0$"

$$f\left(\sum_{i=1}^{n} \beta_i e_i - \sum_{i=1}^{n} \gamma_i e_i \right) = f\left(\sum_{i=1}^{n} (\beta_i - \gamma_i)e_i \right)$$

$= f\left(\sum_{i=1}^{n} \delta_i \alpha_i e_i \right) = 0$ porque $\alpha_i e_i$ son elementos de la base Ker(f).

"g es inyectiva"

$g\{(\beta_i e_i + A\alpha_i e_i)_{i \leq n}) = g((\gamma_i e_i + A\alpha_i e_i)_{i \leq n})$

$\Rightarrow \sum_{i=1}^{n} \beta_i e_i + Ker(f) = \sum_{i=1}^{n} \gamma_i e_i + Ker(f)$

$\Rightarrow \left(\sum_{i=1}^{n} \beta_i e_i - \sum_{i=1}^{n} \gamma_i . e_i . \right) \varepsilon\ Ker(f)$

$\Rightarrow \sum_{i=1}^{n} \beta_i e_i - \sum_{i=1}^{n} \gamma_i e_i = \sum_{i=1}^{n} \delta_i \alpha_i e_i$

$\Rightarrow \sum_{i=1}^{n} (\beta_i - \gamma_i)e_i = \sum_{i=1}^{n} \delta_i \alpha_i e_i$

$\Rightarrow$ Para todo i $\beta_i - \gamma_i = \delta_i \alpha_i$

$\Rightarrow$ Para todo i $(\beta_i - \gamma_i)e_i = \delta_i \alpha_i e_i$

$\Rightarrow$ Para todo i $\beta_i e_i - \gamma_i e_i \in A\alpha_i e_i$

$\Rightarrow$ Para todo i $\beta_i e_i + A\alpha_i e_i = \gamma_i e_i + A\alpha_i e_i$

$\Rightarrow$ $(\beta_i e_i + A\alpha_i e_i)_{i \leq n} = (\gamma_i e_i + A\alpha_i e_i)_{i \leq n}$

" g es sobre "

Sea $x \in A^n$ entonces x es de la forma $\sum_{i=1}^{n} \gamma_i e_i$

$$x + Ker(f) = \left(\sum_{i=1}^{n} \gamma_i e_i\right) + Ker(f)$$

$$= g((\gamma_i e_i) + A\alpha_i e_i)_{i \leq n}$$

para cada i

$$f_i : \frac{A}{A\alpha_i} \longrightarrow \frac{Ae_i}{A\alpha_i e_i}$$

$$a + A\alpha_i \rightsquigarrow a e_i + A\alpha_i e_i$$

f es morfismo biyectivo.

$$h: \prod_{i=1}^{n} \frac{A}{A\alpha_i} \longrightarrow \prod_{i=1}^{n} \frac{Ae_i}{A\alpha_i e_i}$$

$$(x_1, x_2, \ldots, x_n) \rightsquigarrow (f_1(x_1), f_2(x_2), \ldots, f_n(x_n))$$

es morfismo biyectivo con $x_i = a_i + A\alpha_i$

Definamos $I_1 = A\alpha_1, I_2 = A\alpha_2, \ldots, I_n = A\alpha_n$

$$\prod_{i=1}^{n} \frac{A}{I_i} \xrightarrow{h} \prod_{i=1}^{n} \frac{Ae_i}{A\alpha_i e_i} \xrightarrow{g} \frac{A^n}{\ker(f)} \xrightarrow{\bar{f}} E$$

$\bar{f}$ojoh: $\frac{A}{I_1} \times \frac{A}{I_2} \times \ldots \times \frac{A}{I_n} \longrightarrow E$

es morfismo biyectivo.

Probemos que $I_n \subset I_{n-1} \subset \ldots \subset I_2 \subset I_1$

Sabemos que $\alpha_1 \mid \alpha_2, \alpha_2 \mid \alpha_3, \ldots, \alpha_{r-1} \mid \alpha_r$

$I_n = A\alpha_n = A0 = (0)$

$I_{n-1} = A\alpha_{n-1} = A0 = (0)$

.
.
.
.
.

$I_{r+1} = A\alpha_{r+1} = A0 = (0)$

de donde $I_n \subset I_{n-1} \subset \ldots \subset I_r$

$\alpha_{r-1} \mid \alpha_r \Rightarrow A\alpha_r \subset A\alpha_{r-1} \Rightarrow I_r \subset I_{r-1}$

$\alpha_{r-2} \mid \alpha_{r-1} \Rightarrow A\alpha_{r-1} \subset A\alpha_{r-2} \Rightarrow I_{r-1} \subset I_{r-2}$

.
.
.
.
.

$\alpha_1 \mid \alpha_2 \Longrightarrow A\alpha_2 \subset A\alpha_1 \Longrightarrow I_2 \subset I_1$

Luego $I_n \subset I_{n-1} \subset \ldots \subset I_2 \subset I_1$

Sea $(G,+)$ grupo abeliano

G es un Z módulo

definamos una función $.: Z \times G \longrightarrow G$

$(n,x) \rightsquigarrow . \quad (n,x) = nx$

donde $nx=x+x+x+\ldots+x$ (n veces) si $n>0$

$nx=-x-x\ldots\ldots-x$ (-n veces) si $n<0$

$nx=0$, si $n=0$

$(G,+)$, $x\in G$, el orden de x es igual al menor número natural n tal que $nx=0$

$(G,\cdot)$, $x\in G$, el orden de x es igual al menor número natural n tal que $x^n=1$.

PROPOSICION 3-5.3

"Si $(G,+)$ es un grupo conmutativo finito entonces existe $x\in G$, $m\in\mathbb{N}^*$ tal que:

m = orden de x

m = m.c.m {t/t es el orden de algún $y\in G$}"

DEMOSTRACION

G es un Z módulo de tipo finito

G es isomorfo con un Z módulo de la forma

$\frac{Z}{I_1} \times \frac{Z}{I_2} \times \ldots \times \frac{Z}{I_n}$, en donde $I_1, I_2, \ldots, I_n$

son ideales de Z tal que $I_n \subset I_{n-1} \subset \ldots \subset I_1$

Existen $a_1, a_2, a_3, \ldots, a_n$ en $\mathbb{N}^*$ tal que

$I_1 = a_1 Z$, $I_2 = a_2 Z$, $\ldots$, $I_n = a_n Z$

ningún I_i es igual a cero, porque si alguno lo fuera entonces G sería infinito.

Existe un isomorfismo

$$f: G \longrightarrow \frac{Z}{a_1 Z} \times \frac{Z}{a_2 Z} \times \ldots \times \frac{Z}{a_n Z}$$

Sea x el elemento de G tal que

$f(x)= (a_1 Z,\ a_2 Z,\ \ldots,\ a_{n-1} Z,\ 1+a_n Z)$

"f es un isomorfismo"

$f(a_n x) = a_n f(x) = a_n(a_1 Z,\ a_2 Z\ ,\ \ldots a_{n-1} Z,\ 1+a_n Z)$

$= (a_1 Z,\ a_2 Z,\ \ldots,\ a_{n-1} Z,\ a_n + a_n Z)$

Pero $a_n + a_n Z = a_n Z$ porque $a_n \in a_n Z$ ya que

$a_n = a_n . 1 \in a_n Z.$

Como $(a_1 Z,\ a_2 Z,\ \ldots,\ a_n Z)$ es igual al cero del producto.

Entonces $a_n x=0$ con $a_n \neq 0$.

Hay que probar que a_n es el menor natural.

Supongamos que $rx=0$ con $r \in \mathbb{N}^*$

$f(rx) = 0 = (a_1 Z,\ a_2 Z,\ \ldots,\ a_{n-1} Z,\ r+a_n Z)$

$\Rightarrow \quad r+a_n Z = a_n Z \Rightarrow r \in a_n Z$

$\Rightarrow \quad r = a_n p, \quad$ con $p \in \mathbb{N}^*$

de donde $a_n \leq r$, luego a_n es el orden de x.

Probemos que a_n es m.c.m.

Sea $z \in G$ y probemos que $a_n z=0$

es decir "$f(a_n z)=0$"

$f(z)= (b_1+a_1 Z,\ b_2+a_2 Z,\ \ldots,\ b_n+a_n Z)$

$f(a_n z) = (a_n b_1 + a_1 Z,\ a_n b_2 + a_2 Z,\ \ldots,\ a_n b_n + a_n Z)$

Queremos que $(a_n b_1 + a_1 Z,\ \ldots\ldots,\ a_n b_n + a_n Z)$

Sea igual a cero para ello es necesario que

$a_n b_1 + a_1 Z = a_1 Z$, esto es cierto si $a_n b_1 \in a_1 Z$

por $I_n \subset I_{n-1} \subset \ldots \subset I_2 \subset I_1$

$a_n Z \subset a_1 Z \Rightarrow a_1 | a_n \Rightarrow a_n = a_1 p$

luego $a_n b_1 = a_1 p b_1 \in a_1 Z$

Luego a_n es más grande que el orden de z

si $a_n z = 0 \Rightarrow a_n$ es multiplo del orden de z.

ya que si $a_n = qr+t$, $0 \leq t < r$

entonces $0 = a_n z = qrz+tz = q(rz)+tz =$

$0+tz = tz$; $0 = tz \Rightarrow t = 0$

Como a_n = orden de un x en G y a_n es múltiplo común de { t/t es el orden de algun y G}

entonces a_n es m.c.m.

PROPOSICION 3-5.4

"K es un cuerpo

$H \subset K$ un subgrupo finito de $(K^*, \cdot)$ siendo $K^* = K - \{0\}$

Entonces:

1) Los elementos de H son raíces de 1

2) H es cíclico"

DEMOSTRACION

Para 1. Probemos que si $y \in H$ entonces $y^m = 1$ por ser H un grupo conmutativo finito, existen $x \in H$, $m \in N^*$ tal que m=orden de x y m=m.c.m. {$n \in N/n$ es el orden de algún y H} $x^m = 1$

si $y \in H$ entonces $y^m = 1$

Para 2 Probemos que para algún $a \in H$, todo $x \in H$ es de la forma a^m donde $m \in Z$.

Se sabe que un polinomio de grado m sobre un cuerpo K tiene a lo sumo m soluciones (x^m-1)

Sean $x, x^2, x^3, \ldots, x^{r-1}, x^m \in H$ y distintos

entonces $H=\{x, x^2, x^3, \ldots, x^{m-1}, 1\}$

de donde $H=[x]$

Luego x es un generador de H

asi H es ciclico.

PROPOSICION 3-5.5

" K un cuerpo

K poseen raíces de 1

$H=\{y \in K / y$ es raíz de 1$\}$

Entonces:

1) H es un grupo ciclico

2) H es isomorfo al grupo $\frac{Z}{nZ}$

3) H posee $\psi(n)$ generadores"

DEMOSTRACION

Para 1 Vamos a probar que H es subgrupo de $(K^*, \cdot)$

Para ello probaremos que si $x, y \in H$

entonces $xy^{-1} \in H$.

Existen $m \in N^*$, $r \in N^*$ tales que

$x^m = 1$ y $y^r = 1$

$(y^{-1})^r = 1$, $x^m = 1$

$y^r = 1 \Rightarrow (y^r)^{-1} = 1$

entonces multiplicando x con y^{-1} tenemos

$(xy^{-1})^{mr} = x^{mr}.(y^{-1})^{mr}$

$= (x^m)^r . ((y^{-1})^r)^m$

$= 1^r . 1^m$

$= 1 . 1 = 1$ luego $xy^{-1} \in H$

H por ser subgrupo de K es cíclico.

Para 2

H es isomorfo a $\frac{Z}{nZ}$

Sea x un generador de H

$f: H \longrightarrow \frac{A}{nZ}$

$x^m \rightsquigarrow m+nZ$

"f es morfismo de grupo"

$f(x^m . x^r) = f(x^{m+r}) = (m+r)+nZ$

$= m+nZ + r+nZ$

$= f(x^m) + f(x^r)$

"f es inyectiva"

Sean $y,z \in H$; $y = x^m$, $z = x^r$

"$f(y) = f(z) \Rightarrow y = z$"

$f(x^m) = f(x^r) \Rightarrow m+nZ = r+nZ \Rightarrow m-r \in nZ$

$\Rightarrow m-r = nw$, $w \in Z$

$\Rightarrow x^{m-r} = x^{nw} = (x^n)^w = 1^w = 1$

$\Rightarrow x^{m-r} = 1 \Rightarrow x^m . x^{-r} = 1 \Rightarrow x^m = x^r$

de donde y = z.

"f es sobre"

Para todo $m+nZ \in \frac{Z}{nZ}$, existe $x^m \in H$ tal que

$f(x^m) = m+nZ$, $m \in H$.

Para 3 H posee $\psi(n)$ generadores

por proposición 3-4.3 de indicadores de euler.

3-6 CUERPOS FINITOS

Sea K un cuerpo. Existe un único morfismo de anillos $f:Z \longrightarrow K$ tal que $f(1)=1$

DEMOSTRACION:

Definamos:

$f: Z \longrightarrow K$

$n \rightsquigarrow f(n)= 1+1+\ldots+1$ (n veces si $n>0$)

$n \rightsquigarrow f(n)= -1-1-\ldots-1$ ($-n$ veces si $n<0$)

$n \rightsquigarrow f(n)=0$ (si $n=0$)

Probemos que $f(1)=1$

$n>0$ $n = 1 \Rightarrow f(1)=1$ por definición.

Probemos que f es único

Supongamos que existe el morfismo

$g:Z \longrightarrow K$ tal que $g(1)=1$

si $n>0$. $g(n) = g(1+1+1\ldots+1)$

$= g(1)+g(1)+\ldots+g(1)$

$= 1+1+\ldots+1$

$= f(n)$

de donde $f(n) = g(n)$

Si $n<0$. $g(n) = (-1-1-\ldots-1)$

$= g(-(1+1+\ldots+1))$

$= -g(1+1+\ldots+1)$

$= -(g(1)+g(1)+\ldots+g(1))$

$= -(1+1+\ldots+1)$

$= -1-1-\ldots-1$

$= f(n)$

de donde $f(n) = g(n)$

Si $n=0$ entonces $g(n)=0$ por ser g morfismo por hipótesis.

Luego $f=g$.

de donde f es un morfismo único.

* Si f es inyectivo se dice que K es de carácterística cero.

* Si f no es inyectivo, su núcleo es un ideal de Z, es decir $Ker(f)=pZ$ con $p\in\mathbb{N}^*$.

Se dice entonces que K es de característica p.

PROPOSICION 3-6.1

"Sea $p\in\mathbb{N}^*$. Entonces $\frac{Z}{pZ}$ es un anillo entero si y sólo si p es un número primo."

DEMOSTRACION

$\Rightarrow$) Supongamos que p no es primo

Entonces existen $a\in\mathbb{N}^*$, $b\in\mathbb{N}^*$ tales que

$p = ab$. $p = ab \Rightarrow a|p$ con $a\neq p$

$\Rightarrow b|p$ con $b\neq p$

$a+pZ \neq pZ$. Porque si lo fuera

$a+pZ = pZ \Rightarrow a \in pZ \Rightarrow a = pd,\ d \in \mathbb{N}^*$

$\Rightarrow p|a$

$a|p$ y $p|a \Rightarrow a = p$ (contradicción)

luego tiene que ser $a+pZ \neq pZ$

De igual forma $b+pZ \neq pZ$

Porque si $b+pZ=pZ$ entonces $b \in pZ$

$\Rightarrow b = pc,\ c \in \mathbb{N}^*$

$\Rightarrow p|b \Rightarrow b = p$ (contradicción)

Luego $b+pZ \neq pZ$

$(a+pZ)(b+pZ) = ab+pZ = pZ$

Luego $\frac{Z}{pZ}$ no es entero

$\Leftarrow$) Sean a,b en Z tales que $(a+pZ) = pZ$

$(a+pZ)(b+pZ) = ab+pZ = pZ$

Luego $ab \in pZ$.

$ab \in pZ \Rightarrow ab$ se puede escribir en la forma

$ab = px,\ x \in Z$

$ab = px \Rightarrow p|ba$

Pero $p|ab \Rightarrow p|a$ ó $p|b$

Si $p|a$ entonces $a=py,\ y \in Z$

$a \in pZ \Rightarrow a+pZ = pZ$

Si $p|b$ entonces $b+pZ = pZ$

PROPOSICION 3-6.2

"K un cuerpo, K de característica $p \neq 0$

Entonces:

p es primo y $\frac{Z}{pZ}$ es un cuerpo"

DEMOSTRACION

Sabemos por proposición 3-6.1 que p e s primo si y sólo si $\frac{Z}{pZ}$ es un anillo entero.

$\frac{Z}{pZ}$ es isomorfo al anillo $\overline{f}(\frac{Z}{pZ})$; $\overline{f}:\frac{Z}{pZ} \longrightarrow K$.

Como K es anillo entero, todo subanillo, de K es entero. Luego $\overline{f}(\frac{Z}{pZ})$ es anillo entero.

$\frac{Z}{pZ}$ también es entero (Porque es isomorfo)

de donde p e s primo.

" $\frac{Z}{pZ}$ es un cuerpo"

Sea $a \in Z$ tal que $a+pZ \neq pZ$ entonces $a \notin pZ$

de donde a no divide a p.

a y p son primos entre sí.

$1 = m.c.d(a,p) \Rightarrow 1 = ax+py$

$$\begin{aligned}(a+pZ)(x+pZ) &= ax+pZ \\ &= (1-py)+pZ \\ &= (1+pZ)-(py+pZ) \\ &= 1+pZ-pZ \\ &= 1+pZ\end{aligned}$$

Luego $\frac{Z}{pZ}$ es inversible porque todo elemento distinto de cero tiene inverso.

PROPOSICION 3-6.3

"K un cuerpo, $p \neq 0$ la característica de K

Entonces:

1) $px=0$, para todo $x \in K$

2) $(x+y)^p = x^p + y^p$, para todo x,y en K"

DEMOSTRACION

El morfismo $f: Z \longrightarrow K$

$n \rightsquigarrow f(n) = 1+1+..,+1$ (n veces)

no es inyectivo porque $p \neq 0$

$Ker(f) = pZ$, $p>0$

Luego $px = x+x+..,+x$ (p veces)

$= (1.x)+(1.x)+...+(1.x)$ (p veces, $1 \in K$)

$= (1+1+...+1)x$

$= f(p)x$

$= 0\ x$

$= 0$

de donde $px = 0$

Para 2

Según la fórmula del binomio tenemos que

$$(x+y)^p = \sum_{j=o}^{p} \binom{p}{j} x^j \; y^{p-j}$$

el coeficiente binomial es un entero que vale

$$\frac{p!}{j!(p-j)!}$$

si $j = o$ tenemos

$$\binom{p}{o} x^o y^{p-o} = 1.y^p = y^p$$

si $j = p$ tendremos

$$\binom{p}{p} x^p y^{p-p} = 1.x^p .1 = x^p$$

$$(x+y)^p = \sum_{j=o}^{p} \binom{p}{j} x^j y^{p-j} = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j}$$

$$\binom{p}{j} x^j y^{p-j} = \frac{p!}{j!(p-j)!} x^j y^{p-j} = rpx^j y^{p-j}$$

$$= p(rx^j y^{p-j})$$

$$= 0 \text{ por parte 1}$$

Luego $(x+y)^p = \sum_{j=o}^{p} \binom{p}{j} x^j y^{p-j} = x^p + y^p + \sum_{1}^{p-1} \binom{p}{j} x^j y^{p-j}$

$$= x^p + y^p + 0$$

de donde $(x+y)^p = x^p + y^p$

PROPOSICION 3-6.4

"Sea K un cuerpo finito, q = card(k)

Entonces:

1) La Característica de K es un número primo

2) K es un espacio vectorial de dimensión finita m sobre $\frac{Z}{pZ}$

3) $q = p^m$

4) El grupo multiplicativo $(K^*, \cdot)$ es cíclico de orden q-1

5) $x^q = x$, para todo $x \in K$"

DEMOSTRACION

Para 1

Por ser K finito, $f: Z \longrightarrow K : z \rightsquigarrow f(z)$ no puede ser inyectivo. Luego la característica de K no puede ser cero.

Luego tiene que ser un número primo la característica de K.

Para 2

Como K es finito la dimensión de la base del espacio vectorial es finito.

Para 3

Sea $f: \frac{Z}{pZ} \times \frac{Z}{pZ} \times \ldots \times \frac{Z}{pZ} \longrightarrow K$ tal que

$$(\alpha_1, \alpha_2, \ldots, \alpha_m) \rightsquigarrow \sum_{i=}^{m} \alpha_i e_i$$

en donde $\{e_1, e_2, \ldots, e_n\}$ es una base

f es un isomorfismo.

Luego K tiene el mismo número de elementos

que $\frac{Z}{pZ} \times \frac{Z}{pZ} \times \ldots \times \frac{Z}{pZ}$

es decir $p^m = q$

Para 4

K* posee (q-1) elementos y es cíclico

por ser finito.

Para 5

Existe $z \in K^*$ tal que el orden de z es multiplo de

todos los elementos de K* y es un generador

$\{z, z^2, z^3, \ldots, z^{q-1}\} = K^*$

si $y \in K^*$ entonces $y^{q-1} = 1$

$y^q = y$

CAPITULO IV

ELEMENTOS ENTEROS SOBRE UN ANILLO

ELEMENTOS ALGEBRAICOS SOBRE UN CUERPO

4-1) ELEMENTOS ENTEROS SOBRE UN ANILLO

DEFINICION 4-1.1

Si x es un número complejo, se dice que x es un número algebraico si x satisface una igualdad de la forma:

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_0 = 0$$

donde cada a_i es un número racional.

Cuando los a_i son números enteros ($a_i \in Z$) el número algebraico x es llamado un entero algebraico.

Por ejemplo $\sqrt{2}$, $\sqrt{3}$, i. son enteros algebraicos.
En efecto.

* $x = \sqrt{2}$ $\qquad$ $x = \sqrt{2}$ es complejo

$x^2 = 2$ $\qquad$ $\sqrt{2} = \sqrt{2} + 0_i$

$x^2 - 2 = 0$

* $x = \sqrt{3}$ $\quad\quad$ $\sqrt{3}$ es complejo

$x^2 = 3$ $\quad\quad$ $\sqrt{3} = \sqrt{3} + 0_i$

$x^2 - 3 = 0$

* $i^2 = 1$ por definición

Luego $i^2 - 1 = 0$

No es evidente, a priori, que sumas o productos de números algebraicos (resp. de enteros algebraicos) sean también números algebraicos (resp. enteros algebraicos) observamos el ejemplo de

$x = \sqrt{2} + \sqrt{3}$;

$x^2 = (\sqrt{2}+\sqrt{3})^2 = 2+2\sqrt{6}+3$

$\Rightarrow \quad x^2 = 5+2\sqrt{6}$

$\Rightarrow \quad x^2 - 5 = 2\sqrt{6}$

$\Rightarrow \quad (x^2-5)^2 = 24$

$\Rightarrow \quad x^4 - 10x^2 + 25 - 24 = 0$

$\Rightarrow \quad x^4 - 10x^2 + 1 = 0$

de donde x es un número algebraico

Si tomamos $x = \sqrt[3]{5} + \sqrt[5]{7}$ nos damos cuenta de que la serie de astucias que lleva el resultado no es generalizable fácilmente.

Para superar esta dificultad, introducimos en dicho problema los módulos. Vamos a hacer la sustitución de Z (ó Q) por un anillo conmutativo cualquiera.

PROPOSICION 4-1.2

"A un anillo unitario conmutativo

. B C A un subanillo tal que $1 \in B$

. $x \in A$

Entonces, $B[x]$ es el subanillo cuyos elementos son de la forma $b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$

con $b_i \in B$, $n \in \mathbb{N}^*$

DEMOSTRACION

Sea $D = \{b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n / n \in \mathbb{N}^*, b_i \in B$

para todo $i \leq n\}$

. D es un subanillo de A

. $B[x]$ es subanillo de A generado por $B \cup \{x\}$

Probemos $B[x] = D$

$B[x] = D$ si y sólo si a) $B[x] \subset D$

b) $D \subset B[x]$

Prueba para a)

El anillo $B[x]$ tiene las siguientes propiedades:

1) Es un subanillo de A

2) $x \in B[x]$ y $B \subset B[x]$

3) si M C A es un subanillo de A tal que

$B \subset M$ y $x \in M$ entonces $B[x] \subset M$

Según lo anterior por la propiedad 3 basta probar que

$x \in D$ y $B \subset D$

esto es $B \cup \{x\} \subset D$

si $x \in D$ entonces

$x = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$

$\Rightarrow \quad b_1 = 1 \quad y \quad b_0 = b_2 = b_3 = \ldots = b_n = 0$

$B \subset D$

$b \in B \xrightarrow{?} b \in D$

$b = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$

$\Rightarrow \quad b_0 = b$

$b_1 = b_2 = b_3 = \ldots = b_n = 0$

Asi $B \cup \{x\} \subset D$

entonces $B[x] \subset D$

Prueba para b)

Sea $b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n \in D$

$b_0, b_1, b_2, \ldots, b_n \in B$ entonces $b_0, b_1, b_2, \ldots, b_n \in B[x]$

$x \in B[x] \Rightarrow x^2 \in B[x]$

$x^3 \in B[x]$

$\vdots$

$x^n \in B[x]$

$\Rightarrow b_1 x \in B[x]$

$b_2 x^2 \in B[x]$

$\vdots$

$b_n x^n \in B[x]$

de donde $b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n \in B[x]$

Luego $D \subset B[x]$

Asi tenemos que $B[x] = D$

Luego se cumple que D es subanillo de A.

PROPOSICION 4-1.3

"A un anillo unitario conmutativo

B C A un subanillo tal que $1 \in B$,

$x \in A$.

Entonces, las propiedades que siguen son equivalentes

1) Existen $b_0, b_1, b_2, \ldots, b_{n-1}$ en B tales que

$$x^n + b_{n-1} x^{n-1} + \ldots + b_2 x^2 + b_1 x + b_0 = 0$$

2) El anillo $B[x]$ es un B-módulo de tipo finito.

3) Existe D subanillo de A tal que $B \cup \{x\} \subset D$

y D es un B-módulo de tipo finito.

DEMOSTRACION

1) $\Longrightarrow$ 2) Sea M el subanillo generado por

$\{1, x, x^2, \ldots, x^{n-1}\}$

$M = B[x]$"

$$x^n = -b_0 1 - b_1 x - b_2 x^2 - \ldots - b_{n-1} x^{n-1} \in M$$

$$x^{n+1} = -b_0 x - b_1 x^2 - b_2 x^3 - \ldots - b_{n-1} x^n \in M$$

i) "$B[x] \subset M$"

para todo m: $x^m \in M$

para todo m, para todo subconjunto

$\{b_0, b_1, b_2, \ldots, b_m\}$ de B

$$b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m \in M$$

Luego $B[x] \subset M$

ii) "M C B[x]" es equivalente a probar que

$\{1, x, x^2, \ldots, x^{n-1}\} \subset B[x]$

¿ $1 \in B[x]$?

. $1 \in B$ y $B \subset B[x]$ luego $1 \in B[x]$

. $x \in B[x]$ por definición de $B[x]$ es cierto

$x^2 \in B[x]$

.

.

.

$x^{n-1} \in B[x]$

Luego $M \subset B[x]$

de donde $M = B[x]$

. Ahora probemos que es un B-módulo

. $B.B[x] \subset B[x]$. sea $b \in B$, $y \in B[x]$

Probemos que: $b.y \in B[x]$

Por ser anillo tenemos que si $p \in B[x]$, $t \in B[x]$

entonces $pt \in B[x]$

como $B \subset B[x]$, $b \in B \rightarrow b \in B[x]$

Luego es B-módulo.

2) $\Rightarrow$ 3) tomando $D = B[x]$

$B \cup \{x\} \subset B[x]$ por que $B \subset B[x]$ y

$x \in B[x]$ por definición de $B[x]$; y ya

se probó que $B[x]$ es un B-módulo.

3) $\Rightarrow$ 1) Sea $\{y_1, y_2, \ldots, y_n\}$ un generador

finito de D.

$D = By_1 + By_2 + \ldots + By_n$

1) " $D \subset By_1 + By_2 + \ldots + By_n$ "

Basta probar que

$\{y_1, y_2, \ldots, y_n\} \subset By_1 + By_2 + \ldots + By_n$

$y_1 = 1y_1 + 0y_2 + \ldots + 0y_n$

$y_2 = 0y_1 + 1y_2 + \ldots + 0y_n$

.

.

.

$y_n = 0y_1 + 0y_2 + \ldots + 1y_n$

si $y_1 \in B \Rightarrow y_1 \in By_1 + By_2 + \ldots + By_n$

$\vdots$

$y_n \in B \Rightarrow y_n \in By_1 + By_2 + \ldots + By_n$

Luego $\{y_1, y_2, \ldots, y_n\} \subset By_1 + By_2 + \ldots + By_n$

y como $\{y_1, y_2, \ldots, y_n\}$ es generador de D

se tiene que $D \subset By_1 + By_2 + \ldots + By_n$

ii) " $By_1 + By_2 + \ldots + By_n \subset D$ "

$b_1 y_1 + b_2 y_2 + \ldots + b_n y_n \in D$ cierto porque

$b_1 y_1 \in D$, $b_2 y_2 \in D$; ..., $b_n y_n \in D$

Luego su suma está en D.

También por que D es un B-módulo.

Luego $By_1 + By_2 + \ldots + By_n \subset D$

De i) y ii) se tiene que

$$D = By_1 + By_2 + \ldots + By_n$$

Como $x \in D$, $y_i \in D$ y D es subanillo de A. Se tiene

que $xy_1, xy_2, \ldots, xy_n$ pertenecen a D

$xy_1, xy_2, \ldots, xy_n$ son de la forma

$xy_1 = b_{11} y_1 + b_{12} y_2 + \ldots + b_{1n} y_n$

$xy_2 = b_{21} y_1 + b_{22} y_2 + \ldots + b_{2n} y_n$

.

.

.

$xy_n = b_{m1} y_1 + b_{m2} y_2 + \ldots + b_{mn} y_n$

en donde cada $b_{ij} \in B$

sea la matriz

$$M = \begin{bmatrix} x - b_{11} & -b_{12} & \cdots & -b_{1n} \\ -b_{21} & x - b_{22} & \cdots & -b_{2n} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ -b_{m1} & -b_{m2} & \cdots & x - b_{mn} \end{bmatrix}$$

El determinante d de la matriz asociada M es de la forma

$$d = x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0$$

" $d = o$ " para todo $i \leq n$

como $y_1 d = y_2 d = \ldots = y_n d = 0$ luego

para $b_1, b_2, \ldots, b_n$ en B tendremos

$b_1 y_1 d + b_2 y_2 d + \ldots + b_n y_n d = 0$

$(b_1 y_1 + b_2 y_2 + \ldots + b_n y_n)\, d = 0$

$(By_1 + By_2 + \ldots + By_n)\, d = \{0\}$

$D d = \{0\}$

Para todo $m \in D$: $md = 0$

$1.d = 0 \Leftrightarrow d = 0$.

DEFINICION 4-1.4

Si A es un anillo unitario conmutativo.

B C A un subanillo de A tal que $1 \in B$, $x \in A$

Se dice que x es entero sobre B si una de las condiciones 1), 2), ó 3) es verdadera (de la proposición anterior)

Si en esta definición tomamos A = C (C=complejo) y B = Z entonces tendríamos la definición de entero algebraico (ó sea que todo lo que se diga de los enteros sobre B vale para los enteros algebraicos).

PROPOSICION 4-1.5

"Sean A un anillo unitario conmutativo.

. B C A un subanillo tal que $1 \in B$

. $(x_i)_{i \in n}$ una familia finita de elementos de A tales que para todo $i \leq n$ x_i es entero sobre $B[x_1, x_2, \ldots, x_{i-1}]$

Entonces $B[x_1, \ldots, x_n]$ es un B-módulo de tipo finito".

DEMOSTRACION

Recordemos que $B[x_1, x_2, \ldots, x_{i-1}]$ es el anillo generado por $B \cup \{x_1, x_2, \ldots, x_{i-1}\}$ en donde

x_3 es entero sobre $B[x_1, x_2]$

x_2 es entero sobre $B[x_1]$

x_1 es entero sobre B.

Probando por inducción sobre n.

Para n=1.

x_1 es entero sobre B, lo que equivale a que $B[x_1]$ es un B-módulo de tipo finito.

Supongamos cierto para (n-1), esto equivale a afirmar que $B[x_1, x_2, \ldots, x_{n-1}] = D$ es un B-módulo de tipo finito.

Si es B-módulo de tipo finito.

Sea $\{y_1, y_2, \ldots, y_q\}$ un generador finito de D.

$D = By_1 + By_2 + \ldots + By_q$

x_n entero sobre D equivale a decir que $D[x_n]$ es un D-módulo de tipo finito; esto implica que existe $\{z_1, z_2, \ldots, z_p\} \subset D[x_n]$ un generador finito.

Es decir que:

$D[x_n] = Dz_1 + Dz_2 + \ldots + Dz_p$

$D[x_n] = By_1 z_1 + By_2 z_1 + \ldots + By_q z_1 + By_1 z_2 + \ldots + By_q z_2$

$+ \ldots + By_1 z_p + By_2 z_p + \ldots + By_q z_p$

$\{y_i z_j / i \leq q, j \leq p\}$ es un generador finito de $D[x_n]$

Como $B[x_1, x_2, \ldots, x_{n-1}] \cdot [x] = B[x_1, x_2, \ldots, x_n]$

entonces $D[x_n] = B[x_1, x_2, \ldots, x_n]$

Luego $B[x_1, x_2, \ldots, x_n]$ es B-módulo de tipo finito.

PROPOSICION 4-1.6

" Sean .A un anillo unitario conmutativo

.B C A un subanillo tal que $1_A \in B$

.B' = conjunto formado por los elementos de A que son enteros sobre B.

.x e y elementos de A enteros sobre B

Entonces:

1) x+y, x-y, xy son enteros sobre B

2) B' es un subanillo de A tal que B C B'

DEMOSTRACION

Para 1)

x+y, x-y, xy son elementos de $B[x,y]$

porque $B[x,y]$ es un subanillo

que contiene a x,y.

x es entero sobre B y y es entero sobre $B[x]$

Luego, $B[x,y]$ es un B-módulo de tipo finito

Entonces $B[x,y]$ es un B-módulo de tipo finito

tal que $B \cup \{x+y\} \subset B[x,y]$

$B \cup \{x-y\} \subset B[x,y]$

$B \cup \{xy\} \subset B[x,y]$

de donde x+y, x-y, xy son enteros sobre B

por la condición equivalente 3) de la proposición 4-1.3

Para 2)

Basta probar que B C B'

Por la definición de entero sobre B

$x \in B$, x es raiz del polinomio unitario

$1.x-x=0$ y es por tanto entero sobre B.

DEFINICION 4.1.7

A un anillo unitario conmutativo

B C A un subanillo tal que $1 \in B$

$B' = \{x \in A / x$ esentero sobre $B\}$

El subanillo B' es llamado cierre integral de B en A.

DEFINICION 4.1.8

Si A es un anillo entero y k es su cuerpo de fracciones; se llama clausura integral de A al cierre integral de A en k.

DEFINICION 4-1.9

A un anillo unitario conmutativo

B C A un subanillo tal que $1 \in B$

se dice que A es entero sobre B si $B'=A$

(dicho de otro modo, si el cierre integral de B en A es el mismo A)

PROPOSICION 4.1.10

" A un anillo unitario conmutativo

B y D subanillos de A tal que $1 \in B$, $1 \in D$, $D \subset B \subset A$

A entero sobre B

B entero sobre D

Entonces:

A es entero sobre D"

DEMOSTRACION

Sea $x \in A$. probemos que x es entero sobre D.

como A es entero sobre B, x es entero sobre B;

luego $x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_o = 0$

con $b_i \in B$

además B es entero sobre D; luego cada $b_i \in B$

es entero sobre D.

Pongamos $E = D[b_o, b_1, b_2, \ldots, b_{n-1}]$; entonces

x es también entero sobre E.

b_o entero sobre D

b_1 entero sobre $D[b_o]$

b_2 entero sobre $D[b_o, b_1]$

.

.

.

b_{n-1} entero sobre $D[b_o, b_1, \ldots, b_{n-1}]$

por tanto debido a la proposición 4-1.5

$E[x] = D[b_0, b_1, \ldots, b_{n-1}, x]$

es un D-módulo de tipo finito

por 3) de la proposición 4-1.3 se concluye

que x es entero sobre D.

es decir E es un D-módulo de tipo finito

tal que $D \subset E$, $x \in E$. $D \cup \{x\} \subset E$

por tanto A es entero sobre D.

PROPOSICION 4-1.11

" K un cuerpo

E,F dos K- e.v. de igual dimensión finita

$f: E \longrightarrow F$ un K- morfismo

Entonces:

Si f es inyectiva, f es isomorfismo"

DEMOSTRACION

Hay que probar que f es sobre.

por ser f una inyección entonces

E es isomorfo a f(E)

también E es isomorfo a F

F es isomorfo a f(E)

f(E) es un subespacio vectorial de F

isomorfo a F.

f(E) es un s.e.v. de F con igual dimensión que F.

esto implica que f(E)=F

de donde f es sobre

PROPOSICION 4-1.12

" A un anillo entero

B C A un subanillo tal que $1 \in B$

A entero sobre B

Entonces:

A es un cuerpo si y sólo si B es un subcuerpo de A"

DEMOSTRACION

Supongamos que A es un cuerpo y sea $b \in B$, $b \neq 0$. Probemos que $b^{-1} \in B$

Sabemos que $b^{-1} \in A$, por ser A un cuerpo.

b^{-1} es entero sobre B

Existen $b_0, b_1, b_2, \ldots, b_{n-1}$ en B tal que

$$(b^{-1})^n + b_{n-1}(b^{-1})^{n-1} + \ldots + b_1(b^{-1}) + b_0 = 0$$

con $b_i \in B$.

$$b^{-n} + b_{n-1}(b^{-n+1}) + b_{n-2}(b^{-n+2}) + \ldots + b_1(b^{-1}) + b_0 = 0$$

multiplicando por b^{n-1} tenemos

$$b^{-n+(n-1)} + b_{n-1}(b^{-n+1+(n-1)}) + \ldots + b_1(b^{n-2}) + b_0(b^{n-1}) = 0$$

$$b^{-1} + b_{n-1}(b^0) + b_{n-2}(b^1) + \ldots + b_1(b^{n-2}) + b_0(b^{n-1}) = 0$$

$$b^{-1} = -(b_{n-1} + b_{n-2}b + \ldots + b_1 b^{n-2} + b_0 b^{n-1})$$

de donde $b^{-1} \in B$ porque B es un anillo y cada uno de los términos es un producto de elementos de B.

Supongamos que B es un subcuerpo

Sea $a \in A$, $a \neq 0$

Probemos que a es inversible en A

a es entero sobre B

$B[a]$ es un B-e.v. de dimensión finita

" La función $f: B[a] \longrightarrow B[a]$

$x \rightsquigarrow xa$

es un morfismo de B-e.v inyectivo"

" f es morfismo"

$f(x+y) = (x+y)a = xa+ya = f(x)+f(y)$

$f(-x) = (-x)a = -(xa) = -f(x)$

asi f es morfismo.

" f es inyectivo "

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

$f(x)=F(y) \Rightarrow xa=ya \Rightarrow xa-ya = 0$

$\Rightarrow (x-y)a = 0 \Rightarrow x-y = 0$

$\Rightarrow x=y$

esto implica que f es isomorfismo.

Por tanto f es sobre. Luego existe y tal que

$f(y) = 1$. de donde $ya = 1$.

$ya = 1 \Rightarrow a = y^{-1}$ de donde $a \neq 0$ es inversible.

4-2 ANILLOS INTEGRAMENTE CERRADOS

DEFINICION 4-2.1

Si A es un anillo entero, se dice que A es integramente cerrado si su clausura integral es igual a A.

Dicho de otro modo, todo elemento x del cuerpo de fracciones K de A, que es entero sobre A, es elemento de A.

Ejemplo: Si A es anillo Entero

A' = clausura integral de A

Entonces

A' es integramente cerrado.

Si A" es la clausura integral de A', tenemos:

$A \subset A' \subset A''$

A' entero sobre A
A" entero sobre A' $\Rightarrow$ A" entero sobre A

$\Rightarrow A'' \subset A'$

$\Rightarrow A' = A''$

de donde A' es integramente cerrado.

PROPOSICION 4-2.2

" si A es un anillo principal, entonces A es integramente cerrado "

En efecto. Sea K el cuerpo de fracciones de A

A' = clausura integral de A, $x \in A'$.

Debemos probar que A = A'

. A C A' se tiene siempre

. "A' C A" es suficiente probar que $x \in A$.

Existen $a_0, a_1, a_2, \ldots, a_{n-1}$ en A tal que

$$x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 = 0$$

como $x \in K$, x es de la forma $\frac{a}{b}$, a,b en A, $b \neq 0$.

si d = m.c.d(a,b) y a = dm, b = dr entonces

$$\frac{a}{b} = \frac{m}{r}$$

en donde m y r son primos entre si.

$$\frac{m^n}{r^n} + a_{n-} \frac{m^{n-1}}{r^{n-1}} + \ldots + a_2 \frac{m^2}{r^2} + a_1 \frac{m}{r} + a_0 = 0$$

multiplicando por r^n tenemos

$$m^n + r(a_{n-1} m^{n-1}) + \ldots + r^{n-2}(a_2 m^2) + r^{n-1}(a_1 m) + r^n a_0 = 0$$

$$m^n + r(a_{n-1} m^{n-1} + \ldots + r^{n-3} a_2 m^2 + r^{n-2} a_1 m_1 + r^{n-1} a_0) = 0$$

$$m^n = -(a_{n-1} m^{n-1} + \ldots + r^{n-3} a_2 m^2 + r^{n-2} a_1 m + r^{n-1} a_0) r$$

$\Rightarrow$ $r \mid m^n$

$r \mid m^{n-1}$ (por ser m,r primos entre si)

$r \mid m^{n-2}$ (por ser m,r primos entre si)

$r \mid m$, $m = rt$, $t \in A$

$$x = \frac{m}{r} = \frac{rt}{r} = \frac{t}{1} = t$$

Luego x = t

de donde $x \in A$.

4.3 ELEMENTOS ALGEBRAICOS SOBRE UN CUERPO

DEFINICION 4-3.1

A un anillo unitario conmutativo
K C A un subcuerpo de A
$x \in A$.
Se dice que x es algebraico sobre K
si existen elementos $a_0, a_1, a_2, \ldots, a_n$ en K
no todos nulos tales que
$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$.
un elemento no algebraico sobre K se llama
trascendente sobre K.
Si en la definición 4-3.1 suponemos $a_n \neq 0$;
entonces admite un inverso a_n^{-1}, porque K es
un cuerpo; multiplicando por a_n^{-1} se obtiene
una ecuación de dependencia integral. Por tanto:
sobre un cuerpo, algebraico= entero.

PROPOSICION 4-3.2

" A un anillo unitario conmutativo
K C A un subc u erpo de A
$x \in A$.
Entonces
x es algebraico sobre K si y sólo si x es
entero sobre K. "

DEMOSTRACION

$\Rightarrow$) x es algebraico sobre K. Luego

$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$

Sea $m \leq n$ el mayor entero tal que $a_m \neq 0$

$x^m + a_m^{-1} a_{m-1} x^{n-1} + \ldots + a_m^{-1} a_2 x^2 + a_m^{-1} a_1 x +$

$a_m^{-1} a_0 = 0$

$x^m + (a_m^{-1} a_{m-1}) x^{n-1} + \ldots + (a_m^{-1} a_2) x^2 + (a_m^{-1} a_1) x$

$+ a_m^{-1} a_0 = 0$

Luego x es un entero sobre K.

$\Leftarrow$) x es entero sobre K, implica que

$1x^n + b_{n-1} x^{n-1} + \ldots + b_2 x^2 + b_1 x + b_0 = 0$

con $b_i \in K$ y $1 \neq 0$, el único que no puede ser cero.

Luego x es algebraico sobre K.

DEFINICION 4-3.3

A un anillo unitario conmutativo

K C A un subcuerpo de A

Se dice que A es algebraico sobre K

si todo elemento de A es Algebraico sobre K.

4.4 EXTENSIONES ALGEBRAICAS

DEFINICION 4.4.1

A un cuerpo
K C A un subcuerpo de A
Se dice que A es una extensión algebraica de K si A es algebraico sobre K.

DEFINICION 4-4.2

A un cuerpo
K C A un subcuerpo de A.
Llamaremos grado de A sobre K
a la dimensión de A considerado como
K- espacio vectorial.

PROPOSICION 4-4.3

" A un cuerpo
K C A un subcuerpo de A
Entonces
Si el grado de A sobre K es finito, A es extensión algebraica de K "

DEMOSTRACION

Debemos probar que A es algebraico sobre K.

O sea hay que probar que si $x \in A$ entonces

x es algebraico sobre K.

Basta probar que x es entero sobre K.

(Porque A es un cuerpo y en un cuerpo

algebraico es equivalente de entero)

Para ello basta que exista $D \subset A$, D subanillo

D un K-módulo de tipo finito tal que

$K \cup \{x\} \subset D$

$\dim_k A$ es finita (por hipótesis)

$\rightarrow$ que hay una base finita

hay un generador finito

A es de tipo finito

A es un K-módulo de tipo finito.

A toda extensión algebraica finita del cuerpo de los números racionales Q, le llamaremos cuerpo de números algebraicos (o cuerpo numérico)

PROPOSICION 4-4.4

" K un cuerpo

L una extensión algebraica de K

M una extensión algebraica de L

Entonces

1) M es una extensión algebraica de K

2) $\dim_k M = \dim_L M \cdot \dim_k L$

DEMOSTRACION

Para 1)

L una extensión algebraica de K
implica que L es algebraico sobre K.
L algebraico sobre K implica que todo
elemento de L es algebraico sobre K.
de donde $K \subset L$.
M una extensión algebraica de L
implica que M es algebraico sobre L
M algebraico sobre L implica que todo
elemento de M es algebraico sobre L
de donde $L \subset M$.
Luego tenemos $K \subset L \subset M$
de donde M es una extensión algebraica
sobre K.

Para 2)

Sean $\{e_1, e_2, \ldots, e_m\}$ una base de L
$\{d_1, d_2, \ldots, d_n\}$ una base de M

$x \in M$

entonces x es de la forma:

$$x = \sum_{i=1}^{n} a_i d_i, \quad a_i \in L,$$ cada a_i es de la forma

$$a_i = \sum_{j=1}^{m} b_{ij} e_j, \quad b_{ij} \in K$$

$$\Rightarrow \quad x = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} b_{ij}\, e_j \right) d_i$$

$$\Rightarrow \quad x = \sum_{\substack{i\leq n \\ j\leq m}} h_{ij}\, e_j\, d_i$$

esto significa que la familia

$\{e_j\, d_i / j\leq m,\ i\leq n\}$ es un K-generador de M

Veamos si $\{e_j\, d_i / j\leq m,\ i\leq n\}$ es K-linealmente independiente.

$$\sum_{\substack{i\leq n \\ j\leq m}} m_{ij}\, e_{ij}\, d_i = 0\ ,\ m_{ij} \in K$$

Hay que ver cada $m_{ij} = 0$

Pero $\sum_{\substack{i\leq n \\ j\leq m}} m_{ij}\, e_j\, d_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} m_{ij}\, e_j \right) d_i = 0$

$\Rightarrow$ Para todo i: $\sum_{j=1}^{m} m_{ij}\, e_j = 0$

$\Rightarrow$ $m_{ij} = 0$, para todo i, para todo j

$\Rightarrow$ que la dimensión de

$\{e_j\, d_i / j\leq m,\ i\leq n\}$ es mn

con $m = \dim_k L$ y $n = \dim_L M$

de donde $\dim_k M = \dim_k L \cdot \dim_L M$

4-5 ENTEROS DE LOS CUERPOS CUADRATICOS

DEFINICION 4-5.1

Sean K un cuerpo

M C K un subcuerpo

K una extensión algebraica de M

definamos

grado de K = $\dim_M K$

DEFINICION 4-5.2

Sean K un cuerpo, Q el cuerpo de los racionales

Q C K un subcuerpo

Se dice que K es un cuerpo cuadrático

si $\dim_Q K = 2$.

PROPOSICION 4-5.3

" K un cuerpo cuadrático

A el anillo formado por los elementos de K que son enteros sobre Z.

Entonces

I) Existe $d \in Z$, d sin factores primos cuadrados tal que para todo x: $x \in K$ si y sólo si x es de la forma $a+b\sqrt{d}$; $a,b \in Q$.

2) Si $x = a+b\sqrt{d}$, $a,b \in Q$ entonces

$x \in A$ si y sólo si $2a \in Z$ y $a^2 - db^2 \in Z$

DEMOSTRACION

Para 1) Si K es un cuerpo cuadrático, todo elemento x de K-Q es de grado 2 sobre Q.

Es decir si

$x \in K - Q$

$Q \subset Q[x] \subset K \quad , \quad x \notin Q$

$\dim_Q Q[x] = 2$

"$Q(x) = K$"

. $y \in K \Rightarrow y = a' + b' x \; ; \; a,b \in Q$

$Q[x] = \{a+bx / a,b \in Q\}$

. $x^2 \in K \Rightarrow x^2 = a+bx \; ; \; a,b \in Q$

$\Rightarrow x^2 - bx - a = 0$

$\Rightarrow 2x = b \pm \sqrt{b^2+4a}$

$b^2+4a \in Q$

$b^2+4a = \frac{u}{v} \; , \; u,v \in Z$

$b^2+4a = \frac{uv}{v^2}$

$\sqrt{b^2+4a} = \frac{1}{v}\sqrt{uv} \qquad u,v \in Z$

$uv = p_1^2 . p_2^2 \ldots . p_n^2 . q_1 . q_2 \ldots q_n$

$= p^2 . d$, d sin factores primos cuadrados

$\sqrt{uv} = P\sqrt{d}$

$y = a' + b' \left(\frac{b}{2} \pm \frac{1}{2v} P\sqrt{d}\right)$

$y = \left(a' + \frac{bb'}{2}\right) + \frac{b'p}{2v}\sqrt{d}$

Haciendo $a' + \frac{bb'}{2} = a$ y $\frac{b'p}{2v} = b$

Se obtiene $y = a+b\sqrt{d}$

Para 2) $\Rightarrow$ El elemento $\sqrt{d}$ admite un conjugado en K, a saber: $-\sqrt{d}$; luego $\sqrt{d} \notin Q$, $-\sqrt{d} \notin Q$

y $K = Q[\sqrt{d}] = Q[-\sqrt{d}]$

La función $f: Q[\sqrt{d}] \longrightarrow Q[-\sqrt{d}]$

$a' + b'\sqrt{d} \rightsquigarrow a' - b'\sqrt{d}$

es un isomorfismo, de cuerpos.

Supongamos que $x = a+b\sqrt{d} \in A$

a,b enteros sobre K.

Por definición de entero

Existen $z_0, z_1, z_2, \ldots, z_{n-1}$ en Z tal Que

$(a+b\sqrt{d})^n + z_{n-1}(a+b\sqrt{d})^{n-1} + \ldots + z_2(a+b\sqrt{d})^2 + z_1(a+b\sqrt{d}) + z_0 = 0$

Aplicando f a ambos miembros tenemos

$(a-b\sqrt{d})^n + z_{n-1}(a-b\sqrt{d})^{n-1} + \ldots + z(a-b\sqrt{d}) + z_0 = 0$

Luego $a-b\sqrt{d} \in A$

Como A es un anillo entonces:

$(a+b\sqrt{d})+(a-b\sqrt{d}) = 2a \in A$

$(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - b^2 d \in A$

Es decir que $2a$ y $a^2 - b^2 d$ pertenecen a Q y son enteros sobre Z.

Luego $2a$ y $a^2 - b^2 d$ pertenecen a la clausura integral de Z.

Como Z es anillo principal, Z es integramente cerrado. Luego $2a \in Z$, $a^2 - b^2 d \in Z$.

<=) " x entero sobre Z "

$x^2 - 2ax + a^2 - b^2 d = 0$ ya que

$(a+b\sqrt{d})^2 - 2a(a+b\sqrt{d}) + a^2 - b^2 d =$

$a2 + 2ab\sqrt{d} + b^2 d - 2a^2 - 2ab\sqrt{d} + a^2 - b^2 d = 0$

de donde $x \in A$.

PROPOSICION 4-5.4

" K un cuerpo cuadrático

A el anillo formado por los elementos de K que son enteros sobre Z.

Entonces:

1) Si $d \equiv 2(\text{mód}.4)$ ó $d \equiv 3(\text{mód}.4)$, todo elemento de A es de la forma $a+b\sqrt{d}$, con a,b en Z

2) Si $d \equiv 1(\text{mód}.4)$ todo elemento de A es de la forma $\frac{1}{2}a + \frac{1}{2}b\sqrt{d}$ con a,b enteros, ambos pares o ambos impares.

DEMOSTRACION

Sea $x = a+b\sqrt{d}$ en A; a,b en Q

$2a \in Z$, $a^2 - db^2 \in Z$

$4(a^2 - db^2) \in Z$

$(2a)^2 - d(2b)^2 \in Z$

$(2a)^2 \in Z$; $d(2b)^2 \in Z$;

$2b = \frac{m}{n}$, $m \in Z$, $n \in Z$

$d(\frac{m}{n})^2 = z \in Z$

$dm^2 = n^2 z$

Sea $n = q_1 . q_2 . q_3 \ldots . q_r$ (descomposición en sus factores primos)

$dm^2 = q_1^2 . q_2^2 \ldots . q_r^2 . z$

Si algún q_j no es factor primo de m, entonces q_j^2 no es un factor de m^2; luego sería un factor de d, lo cual no es posible.

Por tanto n divide a m y $2b = \frac{m}{n}$ es un entero.

$2a = u$, $2b = v$ enteros

$a = \frac{u}{2}$, $b = \frac{v}{2}$, u,v enteros

$a^2 - db^2 = z$ (un entero)

$\frac{u^2}{4} - d\frac{v^2}{4} = z$

$u^2 - dv^2 = 4z$

v par $\Rightarrow v^2$ par $\Rightarrow$ dv^2par $\Rightarrow u^2$ par $\Rightarrow$u par

si v impar, v = 2m+1

si u fuera par; u = 2n entonces

$4n^2 - d(2m+1)^2 = 4z$

$4n^2 - d(4m^2+4m+1) = 4z$

$d = 4(-z+n^2-dm^2-dm)$

Lo cual no es posible (porque $4 = 2^2$ y supusimos que no tenía factores primos)

Luego u es impar; sea u = 2n+1

$u^2 = 4n^2+4n+1$

Asi $4n^2+4n+1- d(4m^2+4m+1) = 4z$

$d = 4(n^2+n-dm^2-dm-z)+1$

de donde $d \equiv 1$(mód.4).

. $d \equiv 2$(mód.4) $\Rightarrow$ d es par $\Rightarrow$ dv^2 es par

$\Rightarrow u^2$ par $\Rightarrow$ u par $\Rightarrow$ v par.

(u par, v par) $\Rightarrow a,b \in Z$

. $d \equiv 3$(mód.4)

Si v fuera impar entonces $d \equiv 1$(mód.4)

es contradicción

Luego v es par y u es par; $a,b \in Z$

Para 2)

$d \equiv 1$(mód.4) $a,b \in Z$, ambos pares

ó ambos impares.

$x = \frac{1}{2} a + \frac{1}{2} b\sqrt{d}$; probar que $x \in A$

Si a,b son ambos pares, $\frac{a}{2}$, $\frac{b}{2}$ son números enteros y $x \in A$.

Si a,b son ambos impares

tendríamos $x = a+b\sqrt{d}$, $a\in Q$, $b\in Q$

$x\in A$ ssi $2a\in Z$, $a^2-b^2 d\in Z$

" $2.\frac{a}{2} \in Z$ y $(\frac{a}{2})^2 - d(\frac{b}{2})^2 \in Z$ "

$2.\frac{a}{2} = a\in Z$

a es de la forma $a=2m+1$

b es de la forma $b=2n+1$

d es de la forma $d=4t+1$

$$(\frac{a}{2})^2 - d(\frac{b}{2})^2 = \frac{1}{4}(a^2-db^2)$$

$$= \frac{1}{4}(4m^2+4m+1-16m^2t-16mt-4t-4n^2-4n-1)$$

$$= \frac{1}{4}(4m^2+4m-16n^2t-16nt-4t-4n^2-4n)$$

$$= m^2+m-4n^2t-4nt-t-n^2-n \in Z$$

de donde $(\frac{a}{2})^2 - d(\frac{b}{2})^2 \in Z$

B I B L I O G R A F I A

1º TEORIA ALGEBRAICA DE LOS NUMEROS .... PIERRE SAMUEL

2º ALGEBRA ..... SERGE LANG

3º A FIRST COURSE IN ABSTRACT ALGEBRA .. JOHN B. FRALEIGH

4º INTRODUCCION A LA TEORIA DE LOS NUMEROS ..... NIVEN Y ZUCKERMAN

5º TEORIA DE LOS NUMEROS ..... BURTON W. JONES