Universidad de El Salvador
Facultad de Ingeniería y Arquitectura
Departamento de Matemática

Tópico en Teoria de Campos: El Teorema de Kronecker.

TRABAJO DE GRADUACION PRESENTADO POR:

Delmy Angélica Duarte Sandoval

Jorge Alberto Martìnez Gutiérrez

PARA OPTAR AL TITULO DE:

Licenciado en Matemática.

OCTUBRE 1991

UNIVERSIDAD DE EL SALVADOR.-

RECTOR : DR. FABIO CASTILLO FIGUEROA

SECRETARIO GENERAL : LIC. MIGUEL ANGEL AZUCENA

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO : ING. JOSE FRANCISCO MARROQUIN

SECRETARIO : ING. JOSE RIGOBERTO MURILLO CAMPOS.

DEPARTAMENTO DE MATEMATICAS.-

JEFE : LIC. ALBA LILA RICO DE TEJADA

OCTUBRE DE 1991.-

ASESOR : LIC.- JOSE JAVIER RIVERA LAZO

COORDINADOR : LIC.- JOSE JAVIER RIVERA LAZO.-

DEDICATORIA

A DIOS TODOPODEROSO:

Por haber iluminado mi mente y poder así, escalar un peldaño más en mi vida.

Y porque

A MI MADRE:

Zoila Marina Sandoval

A MI ESPOSO:

Juan Antonio Alonzo

A MIS HERMANOS:

Wilfredó, Sandra, Chavy, Norma, Ovidio (Q.D.D.G.), Chema y Melvin

Los quiero mucho

Les dedico mi trabajo de Graduación

AGRADECIMIENTO

Al Licenciado Javier Rivera Lazo

Asesor del presente trabajo de grado

A Francisco Armando Moreno

Ana Gladys Avelar

Leticia Quiñónez H.

Compañeros y Amigos

DIDICATORIA

Este trabajo está dedicado a:

- DIOS TODOPODEROSO ya que El es el verdadero artífice de ésta y todas las obras sobre la tierra.

- A MIS PADRES: ANA VIRGINIA MARTINEZ Y ALEJANDRO GUTIERREZ como fruto de todo su esfuerzo y prueba de que todo el sacrificio hecho no ha sido en vano, ya que siempre estuvierón con migo moral y espiritualmente en todo momento.

- MIS HERMANOS: JOSE VIRGILIO, THELMA ORBELINA, MARIA GUADALUPE, por haber tenido fé y confianza en que saldría adelante.
  Por saber esperar durante todo tiempo este triunfo que es de ustedes.
  Por haberme acompañado día a día moral y económicamente en el largo trayecto de esta travesía.

- MIS TIOS: JUSTINIANO VIGIL Y GLADYS DURAN DE VIGIL que vivierón día a día, noche a noche los momentos de angustia de éste producto que hoy es palpable.
  Quienes sacaron tiempo de todos sus quehaceres para dedicarmelo y así poder salir adelante, quienes se convirtierón en mis padres y siempre estuvieron allí en el momento oportuno.
  Porque sin su ayuda jamás se hubiera logrado éste triunfo.

- MI HIJO: WILLIAM ROBERTO como un ejemplo de sacrificio y superación.

- LORENA que directamente se involucró desde el inicio de éste camino ya que se convirtió en impulso en momentos de tristezas y fracasos, porque siempre fue precisa, paciente, desinteresada y que tomó como suyos muchos problemas que surgieron en el largo camino y que hoy solamente hacemos una pausa.

- ANA EVELYN, ARELY CAROL que hicieron mucho para que llegara a sustituirlas por mis hermanos en muchas ocasiones porque supieron crear aquel ambiente familiar de tal manera que me sintiera como en casa lo cual contribuyó al buen estado de ánimo y siempre estar dispuesto a seguir adelante y nunca retroceder, para ellas con un tremendo amor fraternal.

- MIS TIOS PATERNOS Y MATERNOS con especial estima y admiración.

- MIS DEMAS FAMILIARES con el deseo de hacerles partícipes de lo que ha sido el fruto de todos como una sola familia.

- MIS AMIGOS como un recuerdo y muestra de que aquellos que siempre nos propusimos y soñamos hoy se cumple con la ayuda de nuestro Creador y el esfuerzo familiar.

- A Usted y todas aquellas personas que de una u otra forma me ayudaron a lograr este triunfo.

JORGE ALBERTO MARTINEZ GUTIERREZ

AGRADECIMIENTOS

- A todos los maestros que participaron en la formación básica que supieron conducirme por el buen camino y que siempre predicaron con el ejemplo.

- Al LIC. JOSE JAVIER RIVERA LAZO, con especial agradecimiento **Asesor y Coordinador** de éste trabajo, quien nunca le importó horarios para atender toda duda y problemática surgida en el trabajo, por haber tenido la paciencia y el esmero necesario para poder salir adelante con cada una de las metas propuestas.

- Al LIC. MARCELINO MEJIA GONZALEZ por sus aportes valiosos en todo el desarrollo del trabajo y porque siempre estuvo disponible y muchas veces hizo a un lado sus quehaceres para colaborar con migo, con mucha humildad pero muy sincero y seguro en sus opiniones.

- A todos los que estuvieron pendiente del desarrollo de cada una de las etapas ya que de esa forma colaboraron para impulsar este trabajo.

JORBE ALBERTO MARTINEZ GUTIERREZ

INTRODUCCION

La finalidad del presente trabajo es la de acrecentar el material bibliográfico en el área de álgebra. El aporte concreto es dentro de la Teoría de campos; siendo el objetivo primordial hacer una recopilación de conocimientos en el área de álgebra y dejar en el lector la inquietud de cuán amplio son los tópicos en la teoría de campos, concluyendo con el teorema de Kronecker.

Para la lectura de este trabajo se exige solamente conocimientos básicos de álgebra moderna como lo son Anillos, Ideales, Campos, polinomios y subcampos.

Sin embargo para el lector no familiarizado con estos conceptos se han presentado definiciones de los conceptos utilizados en la prueba de cada una de las proposiciones.

En cuanto al orden en la presentación los temas se han desarrollado de tal manera que el lector comienza con conceptos y propiedades elementales como campos, subcampos; luego extensiones de campos continuando con raíces de polinomios, además se desarrollan elementos básicos para la prue

ba del teorema de Kronecker.

Es claro que existe mucho más acerca de la teoría de campos de lo que aquí se encuentra, lo cual podría quedar como inquietud para el lector.

Esperamos que éste, preste alguna utilidad a los estudiosos del álgebra.

INDICE

UNIDAD I

UNIDAD II

UNIDAD III

UNIDAD IV

UNIDAD V

UNIDAD I

PROPIEDADES DE CAMPOS.

DEFINICION 1.1

Se dice que un conjunto no vacío A es un anillo si tiene dos operaciones + y . tales que:

a) a, b ε A implica que a + b ε A.

b) a + b = b + a para a, b ε A.

c) (a+b)+c = a+(b+c) para a, b, c ε A.

d) Existe un elemento 0 ε A tal que a + 0 = a para todo a ε A.

e) Dado a ε A existe un b ε A tal que a + b = 0 (donde b se expresa como -a).

f) a, b ε A implica que a.b ε A.

g) a.(b.c) = (a.b).c para a, b, c ε A.

h) a.(b+c) = a.b + a.c,
(b+c).a = b.a + c.a para a,b,c ε A.

DEFINICION 1.2

El anillo A es llamado unitario y conmutativo si:

i) Existe un elemento 1 ε A, tal que a.1 = 1.a = a para todo a ε A.

ii) Si a,b ε A entonces
a.b = b.a.

DEFINICION 1.3

Sea A un anillo; un subconjunto no vacío I de A, se llama ideal de A si:

a) I es un subgrupo aditivo de A.

b) Dados $r \in A$, $a \in I$ entonces:

i) $ra \in I$ y

ii) $ar \in I$.

DEFINICION 1.4

El ideal $I \neq A$ es llamado maximal, si para todo ideal J de A:

$$I \subset J \Rightarrow J = I \text{ ó } J = A$$

DEFINICION 1.5

Sea I un ideal de un anillo A; se dice que I es ideal primo si:

i) $I \neq A$.

ii) $xy \in I$ entonces $x \in I$ ó $y \in I$.

DEFINICION 1.6

Sea A un anillo.

Si $S \subset A$, existe un ideal I de A único que cumple las dos propiedades siguientes:

i) $S \subset I$.

ii) Si $F \subset A$ es un ideal tal que $S \subset F$ entonces $I \subset F$.

(Este ideal único se denota $[S]$ y es llamado ideal generado por S).

PROPOSICION 1.1

En un anillo A unitario y conmutativo todo ideal maximal es primo.

Pa.

Sea A un anillo unitario y conmutativo y sea $I \subset A$; I un ideal maximal probar que I es ideal primo.

Si $x, y \in A$ tales que $xy \in I$

entonces $x \in I$ ó $y \in I$. Supongamos que $x \notin I$ y

Sea $J = \{ z \in A / z = a+bx,\ a \in I,\ b \in A \}$.

a) Probemos que es un subgrupo.

a) $J \neq \emptyset$

$Z = 0 + 0x \Rightarrow Z = 0 \in J$

$\therefore \quad J \neq \emptyset$

b) Cierre para la suma

Si $z_1, z_2 \in J$ entonces $z_1 + z_2 \in J$, donde $z_1=a_1+b_1x$, $z_2=a_2+b_2x$.

$$z_1 + z_2 = (a_1 + b_1x) + (a_2+b_2x) = (a_1+a_2) + (b_1+b_2)x$$

$$= z_1 + z_2 \in J .$$

c) Dado $z \in J$, existe $-z \in J$

$z = a+bx \Rightarrow -z = -(a+bx) = -a-bx$, $-a \in I$, $-b \in A$

$\therefore \quad -Z \in J.$

ii) Si $t \in A$, $z \in J$, entonces $t.z \in J$

$t.z = t(a+bx) = ta + tbx$

$ta \in I$, $tb \in A$.

Luego J es ideal .

I C J.

Sea $z \in I$, si $b = 0$ entonces

$z = a+bx$

$= a + 0x$

$z = a$

Mostremos que $x \in J$.

Si $a = 0$ y $b = 1$ entonces

$z = 0 + 1x$

$z = x$

luego $x \in J$

$J \neq I$ porque $x \in I \wedge x \in J$

por tanto $J \neq I$.

J es un ideal que incluye propiamente al ideal I y como I es maximal entonces $J = A$.

Si $J = A$, el elemento $1 \in J$ ya que A es un anillo unitario.

Por tanto existe $a \in I$, $b \in A$ tal que

$1 = a + bx$

$1.y = (a+bx)y$

$y = ay + bxy$; $ay \in I$ porque $a \in I$ y $bxy \in I$ ya que $xy \in I$

$\therefore$ $y \in I$. Luego el ideal I es ideal primo.

DEFINICION 1.7

El anillo A es llamado "Dominio entero", si es unitario, conmutativo y si $xy = 0$ entonces $x=0$ ó $y=0$.

DEFINICION 1.8

Un dominio entero A, se llama dominio entero principal, si todo ideal I en A es de la forma

$I = \{xa / x \in A\}$ para algún $a \in I$.

Este ideal es denotado [a] .

PROPOSICION 1.2

En un dominio entero principal todo ideal primo es maximal.

Pa.

Sea D un dominio entero principal.

Probar que todo ideal primo es maximal.

Sea I un ideal primo.

Sea J un ideal de D tal que $I \subset J$.

Supongamos que $J \neq I$, y sean $I = [z]$ y $J = [w]$, ya que D es un dominio entero principal.

$z \in [z] \Longrightarrow z \in I$

$\Longrightarrow z \in J$

$\Longrightarrow z \in [w]$

como $[z] \subset [w] \wedge [z] \neq [w]$ entonces $w \notin [z]$

también $z \in [w] \Longrightarrow z = tw \qquad t \in D$

$z = tw \in [z] \Rightarrow t \in [z]$ por ser z, ideal primo y $w \notin [z]$.

$\Rightarrow t = yz$

$\Rightarrow z = yzw$

$\Rightarrow 1 = yw \in [w]$

$\Rightarrow 1 \in J$

$\Rightarrow J = D$

ya que todo ideal que contiene al 1 es todo el anillo.

$\therefore$ I es maximal.

PROPOSICION 1.3

El anillo $\mathbb{Z}$ de los números enteros es un dominio entero principal.

Pa.

Sea I un ideal en $\mathbb{Z}$

Con $I \neq \{0\}$ en el anillo de los enteros $\mathbb{Z}$

a probar que existe $a \in \mathbb{Z}$ tal que $I = \{ xa/x \in \mathbb{Z}\}$

Si $y \in I$, $y \neq 0$ entonces $-y \in I$ por ser I un ideal.

Luego I contiene enteros positivos y como $\mathbb{Z}^+$ es bien ordenado entonces I contiene un entero positivo mínimo; sea a el entero positivo mínimo de I. Sea $b \in I$,

$b = ax + r.$ $\quad x,r \in \mathbb{Z}$ $\quad 0 \leq r \leq a$

(utilizando el algoritmo de la división)

Pero $ax \in I$ ya que $a \in I$

$r = b-ax$

entonces r=0; ya que si fuera diferente de cero, ya no sería a el entero positivo mínimo de I, porque $0 \leq r \leq a$ como $r = 0$ entonces $b = ax$.

∴ I es ideal principal de $\mathbb{Z}$ entonces $\mathbb{Z}$ es dominio entero principal.

PROPOSICION 1.4

Si $p \in \mathbb{Z}$, $p > 0$ el ideal [p] es maximal si y solo si, p es número primo.

Pa

$\Rightarrow$

A probar que si [p] es maximal entonces p es primo. Supongamos que p no es primo, entonces existe un $m \in \mathbb{Z}$ tal que $1 < m < p$ y $m|p$.

$[p] \subset [m]$ ya que si $x \in [p]$ entonces $x = t_1 p$, $t_1 \in \mathbb{Z} \dashrightarrow (\alpha)$

pero $m \mid p$, es decir, que $p = t_2 m$, $t_2 \in \mathbb{Z} \dashrightarrow \beta$

sustituyendo β en α tenemos:

$$x = t_1 t_2 m \quad , \quad t_1, t_2 \in \mathbb{Z}$$

por lo tanto $x \in [m]$

$$\therefore \quad [p] \subset [m]$$

$[m] = [p]$ v $[m] = \mathbb{Z}$, por ser $[p]$ maximal.

Si $[m] = [p]$ entonces $p \mid m$ y como $m \mid p$ entonces $m = p$, lo que contradice la hipótesis por lo que $[m] = \mathbb{Z}$; lo que implica que:

$1 \in [m]$

$mk = 1$

$k = 1$ y $m = 1$, lo que contradice la hipótesis.

$\therefore$ p es primo.

Si p es primo, entonces el ideal $[p]$ es maximal.

Pa.

"$\Leftarrow$"

Sea I un ideal que contiene $[p]$. Como $\mathbb{Z}$ es un dominio entero de ideales principales se tiene que existe $m \in I$, tal que: $I = [m]$, $[p] \subset [m]$, por propiedad de ideales

luego $m \mid p$, lo que implica que:

$$m = 1 \quad \vee \quad m = p$$

Si $m = 1$ entonces $[m] = \mathbb{Z}$.

Si $m = p$ entonces $[p] = [m]$.

$\therefore$ $[p]$ es maximal.

DEFINICION 1.9

Sea A un anillo, $I \subset A$ un ideal; si $x \in A$ se define

$$x + I = \{z \in A / z = x+y,\ y \in I\}$$

el conjunto $\{T \subset A / T = x+I,\ x \in A\}$ es un anillo con las operaciones:

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

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

Este anillo se denota $\frac{A}{I}$ y se llama anillo cociente.

. Si A es unitario, $\frac{A}{I}$ es unitario

(Si 1 es la identidad de A entonces 1 + I es la identidad de $\frac{A}{I}$).

. El elemento cero es la clase 0 + I con 0 + I = I,

I es el elemento cero.

. El elemento identidad para $\frac{A}{I}$ es $1 + I$.

DEFINICION 1.10

Se dice que un anillo con unidad A, es un anillo con división, si para $a \neq 0$ en A existe un elemento $b \in A$. (que se expresa como a^{-1}) tal que $a.a^{-1} = a^{-1}.a = 1$.

DEFINICION 1.11

Se dice que un anillo A, es un campo, si A es un anillo con división conmutativo.

PROPOSICION 1.5

Sea A un anillo unitario y conmutativo y sea $I \subset A$, I un ideal.

1) Si I es ideal primo, $\frac{A}{I}$ es un dominio entero.

2) Si $\frac{A}{I}$ es un dominio entero, I es ideal primo.

3) Si I es ideal maximal, $\frac{A}{I}$ es un campo.

4) Si $\frac{A}{I}$ es un campo, I es ideal maximal.

Pa.

1) Si I es ideal primo $\frac{A}{I}$ es un dominio entero.

Sean $x + I, y + I \in \frac{A}{I}$ tal que

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

probar que $x + I = I$ ó $y + I = I$

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

$(x+I)(y+I) = xy + I$, por definición de anillo cociente.

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

$\Rightarrow xy + I = I$

$\Rightarrow xy \in I$

$\Rightarrow x \in I$ ó $y \in I$, por ser I un ideal primo

$\Rightarrow x + I = I$

ó $y + I = I$ $\therefore$ $\frac{A}{I}$ es un dominio entero.

2) Si $\frac{A}{I}$ es un dominio entero, I es ideal primo.

Pa. Sea $x, y \in A$ tal que $xy \in I$

Probar que $x \in I$ ó $y \in I$.

$xy \in I \Rightarrow xy + I = I$ por propiedad de ideales

$(x+I)(y+I) = I$, ya que

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

$\Rightarrow x+I = I$ ó $y + I = I$

por ser $\frac{A}{I}$ dominio entero, luego $x \in I$ ó $y \in I$.

$\therefore$ I es ideal primo.

3) Si I es ideal maximal, $\frac{A}{I}$ es un campo.

Pa.

i) Sean $x + I, y + I \in \frac{A}{I}$

$(x+I)(y+I) = xy + I$, por definición de anillo cociente.

$(x+I)(y+I) = yx+I$, ya que A es conmutativo.

$= (y+I)(x+I)$ por definición de anillo cociente.

$\therefore$ $\frac{A}{I}$ es conmutativo.

ii) Sea $x + I \in \frac{A}{I}$ tal que $x + I \neq I$

$x + I \neq I \Rightarrow x \notin I$

Sea $J = \{y \in A / y = z+ax, a \in A, z \in I\}$

un ideal

$I \subset J$

Sea $w \in I$

$w = w + 0.x$

$w \in J$

$\therefore$ $I \subset J$

Probemos que $J \neq I$

$x = 0 + 1$ por ser A unitario

$x \in J$

$\therefore$ $J \neq I$ pues $x \notin I$

por lo tanto $J = A$, (ya que I es maximal)

en particular $1 \in J$

ya que $1 \in A$, por ser A un anillo unitario;

$1 = a+bx$ $\quad a \in I, \quad b \in A$

$a \in I \Rightarrow -a \in I$

$\Rightarrow bx - 1 = -a \in I \quad (-a \in I)$

$\Rightarrow bx + I = 1 + I$

$\Rightarrow (b+I)(x+I) = 1 + I$, por propiedades de anillo cociente.

$\therefore$ $(x+I) = (b+I)^{-1}$

por lo que $\frac{A}{I}$ es inversible para el producto.

$\therefore$ $\frac{A}{I}$ es un campo.

4) Si $\frac{A}{I}$ es un campo, I es ideal maximal.

Pa.

Sea $J \subset A$ un ideal tal que $I \subset J$

Probemos que $J = I$ ó $J = A$

Supongamos que $J \neq I$ y probemos que $J = A$.

Sea $x \in J$, $x \notin I$

$x \notin I$ entonces $x+I \neq I$

por lo tanto existe $y + I \in \frac{A}{I}$ tal que

$(x+I)(y+I) = 1 + I$, ya que $\frac{A}{I}$ es un campo, tiene inverso multiplicativo.

lo que implica que $xy+I = 1+I$, por propiedades de anillo cociente

luego $xy - 1 \in I$

con lo que $xy - 1 = z$, $z \in I$

$1 = xy - z$

$xy \in J$ ya que $x \in J$

$z \in J$ porque $z \in I$ y $I \subset J$

$1 = xy - z \in J$

$\therefore 1 \in J$

Luego si $1 \in J$ entonces $J = A$.

DEFINICION 1.12

Sea D un dominio entero

$k = \{ \frac{m}{n} \ / \ m \in D, n \in D, n \neq 0 \}$

$\frac{m}{n}$ = clase de equivalencia del par (m, n)

por la relación (a,b) = (a,d) si ad = bc

1) $\frac{a}{b} + \frac{c}{d} = \frac{ad \text{ y } bc}{bd}$

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

entonces (k, +, .) es un campo llamado campo de fracciones asociados a D.

PROPOSICION 1.6

Si D es dominio entero finito, D es un campo.

Pa.

D es dominio entero si es anillo conmutativo unitario y sin divisores de cero.

D es un campo si D es un anillo de división conmutativo.

Sea D = $\{ x_1, x_2 \ldots\ldots x_n \}$ un dominio entero finito.

Sea a ε D, a $\neq$ 0 probar que a es inversible.

Sea L = $\{ ax_1, ax_2, \ldots . ax_n \}$

L $\subset$ D

Mostrar que L = D

Bastará probar que L tiene n elementos.

$$ax_i = ax_j$$

$$\Rightarrow \quad a(x_i - x_j) = 0$$

Como no hay divisores de cero

$$a = 0 \text{ ó } (x_i - x_j) = 0$$

como se tomó $a \neq 0$ entonces $xi - xj = 0$

$$xi = xj$$

por tanto, L tiene n elementos.

Todo elemento de D es de la forma

$$ax_i \text{ con } i \leq n$$

En particular existe j tal que:

$$1 = ax_j$$

$$x_j = a^{-1}$$

lo que implica que a es inversible.

∴ D es un campo.

DEFINICION 1.13

Una aplicación ϕ: $A \longrightarrow B$ de un anillo A en un anillo B es un homomorfismo si:

a) $\phi(x+y) = \phi(x) + \phi(y)$

b) $\phi(xy) = \phi(x)\phi(y)$

DEFINICION 1.14

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

PROPOSICION 1.7

f es inyectiva si y solo si ker f = {0}

Pa.

"$\Rightarrow$"

Sea f un homomorfismo

a probar que si f es inyectiva entonces

ker f = {0}

Sea $x \in \ker f$, luego $f(x) = 0$

lo que implica $f(x) = f(0)$, ya que $f(0) = 0$

$\Rightarrow$ $x = 0$ por ser f inyectiva.

$\therefore$ Cualquier elemento del ker f es el cero.

"$\Leftarrow$"

Si ker f = { 0 } entonces f es inyectiva.

Sean $x_1, x_2, \in A$ tal que: $f(x_1) = f(x_2)$

Probar que $x_1 = x_2$

$f(x_1) = f(x_2) \Rightarrow f(x_1) - f(x_2) = 0$

$\Rightarrow f(x_1 - x_2) = 0$, ya que f es un homomorfismo.

$\Rightarrow x_1 - x_2 \in \ker f$

$\Rightarrow \quad x_1 - x_2 = 0$, ya que ker f = {0}

$\Rightarrow \quad x_1 = x_2$ $\therefore$ f es inyectiva.

DEFINICION 1.15

Si una aplicación ϕ: A $\longrightarrow$ B de un anillo A en un anillo B es un homomorfismo biyectivo, entonces a esa aplicación se le llama Isomorfismo.

PROPOSICION 1.8

Sea D un dominio entero. Pruebe que existen un campo k y un homomorfismo de anillos f: D $\rightarrow$ k con las propiedades siguientes:

1) f es inyectiva.
2) Si L es un campo y g: D $\rightarrow$ L es un homomorfismo inyectivo entonces existe un homomorfismo inyectivo único $\hat{g}$: k $\rightarrow$ L tal que $\hat{g}$ o f = g.
3) Si M es un campo y m: D $\hookrightarrow$ m un morfismo inyectivo que cumplen las propiedades 1) y 2) entonces hay un isomorfismo ϕ : k $\rightarrow$ M tal que ϕ of = m.

(k es llamado campo de fracciones asociado a D).

Pa.

Sea k $\{ \frac{a}{b} / a,b \in D;\ b \neq 0 \}$

$\frac{a}{b}$ = clase de equivalencia del par (a,b)

Por la relación (c,d) = (c, f) si cf = dc

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

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

entonces (k, +, .) es un campo llamado campo de fracciones asociado a D.

. Probemos que k es campo bajo esas operaciones

Pa.

i) Sea $\frac{a}{b}, \frac{c}{d} \in k$, b, d $\neq 0$

probar que $\frac{a}{b} + \frac{c}{d} \in k$

$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$, por la forma en que esta definido k

como $\frac{a}{b}$, $\frac{c}{d} \in k$ entonces

$\frac{a}{b} + \frac{c}{d} \in k$

ii) Sea $\frac{a}{b}$, $\frac{c}{d} \in k$ probar que

$\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$ para $\frac{a}{b} \cdot \frac{c}{d} \in k$

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

$$= \frac{bc + ad}{ba}$$, por ser D un dominio entero es conmutativo

$$= \frac{cb + ad}{db}$$ D es un dominio entero entonces es conmutativo

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

$$\therefore \quad \frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$$

iii) Sea $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in k \quad b, d, f \neq 0$

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

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

$$= \frac{(ad + bc)f + bde}{bdf}$$ por la forma en que está definido k

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

$$= \frac{a(df) + (bcf + bed)}{b(df)}$$ asociando y conmutando

$$= \frac{a}{b} + (\frac{cf + ed}{df})$$

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

iv) Existe un elemento $0 \in k$ tal que:

$$\frac{a}{b} + 0 = \frac{a}{b} \quad \text{para todo } \frac{a}{b} \in k,\ b \neq 0$$

Pa.

$$\frac{a}{b} + 0 = \frac{a}{b} + \frac{0}{1}$$

ya que D es dominio entero, es anillo unitario

$$\Rightarrow \quad \frac{a}{b} + \frac{0}{1} = \frac{a.1 + b.0}{b.1}, \text{ por definición de k}$$

$$= \frac{a}{b} \qquad b \neq 0$$

v) Dado $\frac{a}{b} \in k$ existe un $\frac{c}{d} \in k$ tal que

$$\frac{a}{b} + \frac{c}{d} = 0, \text{ donde } \frac{c}{b} \text{ se expresará como } -(\frac{a}{b})$$

Pa.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = 0, \qquad bd \neq 0$$

$$\Rightarrow ad + bc = 0$$

$$\Rightarrow ad = -bc$$

$$\Rightarrow -\frac{a}{b} = \frac{c}{d}$$

$\therefore$ existe un $\frac{c}{d} = \frac{a}{b} \in k$

vi) $\frac{a}{b}$, $\frac{c}{d} \in k$, $b, d \neq 0$ implica que

$\frac{a}{b} \cdot \frac{c}{d} \in k$

Pa.

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ por la forma en que se definió k

como $\frac{a}{b}, \frac{c}{d} \in k$

entonces $\frac{ac}{bd} \in k$

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

$\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in k$ $b, d, f \neq 0$

Pa.

$\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = \frac{a}{b} \cdot (\frac{ce}{df})$ por la forma que se definió k

$= \frac{ace}{bdf}$, aplicando de nuevo definición

$= \frac{(ac)e}{(bd)f}$, asociando, ya que D es dominio entero

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

viii)

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

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

$\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in k, \quad b, d, f \neq 0$

Pa.

$\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot (\frac{cf + de}{df})$ aplicando definición

$= \frac{acf + ade}{bdf}$ aplicando definición

$= \frac{acf + aed}{bdf}$ conmutando ya que D es anillo conmutativo

$= \frac{(ac)f + (ae)d}{bdf}$ asociando, ya que D es dominio entero

$= \frac{(ac)f}{bdf} + \frac{(de)f}{bdf}$ distribuyendo, por ser D dominio entero

$= \frac{(ac)f}{bdf} + \frac{(ae)d}{bfd}$ conmutando en el denominador

$= \frac{(ac)f}{(bd)f} + \frac{(ac)d}{(bf)d}$ Asociando en el denominador por ser D dominio entero

$= \frac{ac}{bd} + \frac{ac}{bf}$ por ser D dominio entero tiene inverso.

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

viii)

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

Pa.

$(\frac{c}{d} + \frac{e}{f}) \cdot \frac{a}{b} = (\frac{cf + de}{df}) \cdot \frac{a}{b}$ aplicando definición de suma

$= \frac{(cf + de)\, a}{dfb}$ aplicando definición de productos

$= \frac{cfa + dea}{dfb}$ distribuyendo ya que D es dominio entero

$= \frac{caf + ead}{dfb}$ conmutando en el numerador, ya que D es conmutativo

$= \frac{(ca)f + (ea)d}{dfb}$ asociando, ya que D es dominio entero

$= \frac{(ca)f}{dfb} + \frac{(ea)d}{dfb}$ distribuyendo ya que D es dominio entero

$= \frac{(ca)f}{dbf} + \frac{(ea)d}{fbd}$ conmutando en el denominador ya que D es conmutativo

$= \frac{ca}{db} + \frac{ea}{fb}$ por ser D dominio entero posee inverso.

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

ix) Existe un elemento $1 \in k$ tal que $\frac{a}{b} \cdot 1 = 1 \cdot \frac{a}{b} = \frac{a}{b}$ para todo $\frac{a}{b} \in k$, $b \neq 0$

$\frac{a}{b} \cdot 1 = \frac{a}{b} \cdot \frac{1}{1}$, ya que D es unitario.

$= \frac{a.1}{b.1}$, aplicando definición.

$= \frac{1.a}{1.b}$, conmutando, ya que D es conmutativo.

$= 1.\frac{a}{b}$, ya que D es unitario.

$= \frac{a}{b}$

$\therefore$ Existe un elemento $1 \in k$, tal que

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

x) $\frac{a}{b}, \frac{c}{d} \in k$ implica $\frac{a}{b}.\frac{c}{d} = \frac{c}{d}.\frac{a}{b}$

con $b, d \neq 0$

Pa.

$$\frac{a}{b}.\frac{c}{d} = \frac{a.c}{b.d}, \text{ por definición.}$$

$$= \frac{c.a}{d.b}, \text{ conmutando, ya que D anillo es conmutativo.}$$

$$= \frac{c}{d}.\frac{a}{b}, \text{ por definición.}$$

xi) Sea $\frac{a}{b} \in k$ tal que $\frac{a}{b} \neq 0$ probar que existe $(\frac{a}{b})^{-1}$ con la propiedad que:

$$\frac{a}{b}(\frac{a}{b})^{-1} = \frac{1}{1}$$

$$\frac{a}{b} \neq \frac{0}{1} \Rightarrow a \neq 0$$

Sea $(\frac{a}{b})^{-1} = \frac{b}{a}$

$$(\frac{a}{b})(\frac{a}{b})^{-1} = (\frac{a}{b})(\frac{b}{a})$$

$$= \frac{ab}{ba} \text{ por definición}$$

$$= \frac{ab}{ab} \text{ conmutando ya que D es dominio entero}$$

$$(\frac{a}{b})(\frac{a}{b})^{-1} = 1$$

Pa.

Existe un homomorfismo $f: D \to k$

$$f: D \to k$$

$$x \rightsquigarrow \frac{x}{1} = (x, 1): \frac{x}{1} = \text{clase de } (x, 1)$$

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

$$f(x+y) = \frac{x+y}{1}$$

$$= \frac{x.1 + y.1}{1.1}$$

$$= \frac{x.1}{1.1} + \frac{y.1}{1.1}$$

$$= \frac{x}{1} + \frac{y}{1}$$

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

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

ii) $f(x,y) \stackrel{?}{=} f(x).f(y)$

$$f(x.y) = \frac{x-y}{1}$$

$$= \frac{x}{1} \cdot \frac{y}{1}$$

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

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

. Probar que f es inyectiva

Sean $x_1, x_2 \in A$ tal que: $f(x_1) = f(x_2)$

$f(x_1) = f(x_2)$

$f(x_1) - f(x_2) = 0$

$f(x-y) = 0$, ya que f es un homomorfismo

$\frac{x-y}{1} = 0$, por la forma en que se definió f

$\frac{x-y}{1} = \frac{0}{1} \Rightarrow ((x-y),1) = (0,1)$

$(x-y).1 = 1.0$

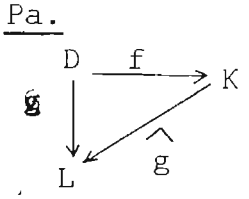
$x - y = 0$

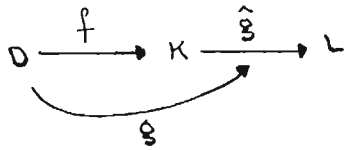
$\Rightarrow x = y$

. . f es inyectiva.

2) Si L es un campo y g: D $\longrightarrow$ L es un homomorfismo inyectiva entonces existe un homomorfismo inyectivo único $\hat{g}$: k$\longrightarrow$L tal que $\hat{g} \circ f = g$

Pa.





$\hat{g}$: k $\longrightarrow$ L: $\frac{m}{n} \longrightarrow g(m)\ g^{-1}(n)$

Probar si es homomorfismo

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

i) $\hat{g}(\frac{m_1}{n_1} + \frac{m_2}{n_2}) \stackrel{?}{=} \hat{g}(\frac{m_1}{n_1}) + g(\frac{m_2}{n_2})$ $\qquad (m_1, m_2, n_1, n_2) \in k$

$$\hat{g}(\frac{m_1}{n_1} + \frac{m_2}{n_2}) = \hat{g}\,(\frac{m_1 n_2 + m_2 n_1}{n_1 n_2})$$

$$= g(m_1 n_2 + m_2 n_1)\,[g(n_1 n_2)]^{-1}, \text{ por definición}$$

$$= [g(m_1 n_2) + g(m_2 n_1)][g(n_1 n_2)]^{-1}, \text{ ya que g es un homomorfismo}$$

$$= (g(m_1)g(n_2)+g(m_2)g(n_1))(g^{-1}(n_1)g^{-1}(n_2)) \text{ , por ser g un homomorfismo}$$

$$= (g(m_1)g(n_2)g^{-1}(n_1)g^{-1}(n_2)+(g(m_2)g(n_1)g^{-1}(n_1)g^{-1}(n_2))$$

distribuyendo, ya que L es campo y g es un homomorfismo $g: D \rightarrow L$

$$= g(m_1)g^{-1}(n_1)g(n_2)g^{-1}(n_2)+(g(m_2)g^{-1}(n_2)g(n_1)g^{-1}(n_1)$$

conmutando, ya que L es un campo y g es un homomorfismo $g: D \rightarrow L$

$$= (g(m_1)g^{-1}(n_1) + (g(m_2)g^{-1}(n_2))$$

$$= \hat{g}(\frac{m_1}{n_1}) + \hat{g}(\frac{m_2}{n_2})$$

ii) Probar

$$\hat{g}\left(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}\right) = \hat{g}\left(\frac{m_1}{n_1}\right)\ \hat{g}\left(\frac{m_2}{n_2}\right)$$

$$\hat{g}\left(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}\right) = g(m_1m_2)(g(n_1n_2))^{-1}$$

$$= (g(m_1)g(m_2))(g(n_1))^{-1}(g(n_2))^{-1}$$

$$= g(m_1)(g(n_1)^{-1}(g(m_2))(g(n_2))^{-1} \text{ conmutativo}$$

$$= \hat{g}\left(\frac{m_1}{n_1}\right)\ \hat{g}\left(\frac{m_2}{n_2}\right)$$

A probar inyectividad

Para que un homomorfismo sea inyectivo

el ker g = {0}

a probar que el ker $\hat{g}$ = {0}

Sea $\frac{m}{n} \in \ker \hat{g}$ entonces $\hat{g}\left(\frac{m}{n}\right) = 0$

$\hat{g}\left(\frac{m}{n}\right) = 0$

$g(m)\,[g(n)]^{-1} = 0$

como $[g(n)]^{-1} \neq 0$ entonces

$g(m) = 0$

Como g es homomorfismo inyectivo entonces m = 0

$\therefore \quad \frac{m}{n} = \frac{0}{n} = 0$

$\therefore \ker \hat{g} = \{0\}$

Ahora a probar que $\hat{g}_o f = g$

$(\hat{g}_o f)(x) = \hat{g}(f(x))$ por definición de composición

$= \hat{g}(\frac{x}{1})$

$= g(x)(g(1))^{-1}$

$= g(x)(1)^1$

$= g(x)(1^{-1})$

$= g(x)(1)$

$= g(x)$

$\therefore (\hat{g}_o f) = g$

PROPOSICION 1.9

El campo $\mathbb{Q}$ de los números racionales es el campo de fracciones asociado al anillo $\mathbb{Z}$ de los números racionales.

Pa.

. El anillo $\mathbb{Z}$ de los números enteros es un dominio entero, por proposición 1.3 $\mathbb{Q}$ es un campo.

$\mathbb{Z} \subset \mathbb{Q}$, $x \in \mathbb{Z}$ $\quad x = \frac{x}{1}$

$\mathbb{Q} = \{\frac{m}{n} / m,n \in \mathbb{Z}, n \neq 0\}$

$\frac{m}{n}$ es la clase de equivalencia del par (m,n) por la relación (a,b) = (c,d) si ad = bc

CONJUNTO DE ENTEROS MODULO P.

$a \equiv b \pmod p$ significa que $p/a-b$

se puede decir igualmente que:

$a \equiv b \pmod p$ cuando la diferencia $a-b$ pertenece al conjunto de los múltiplos de p ó $a \equiv b \pmod p$ si y solamente si a y b dejan el mismo residuo al ser divididos por p.

La relación $\equiv \bmod (p)$ sobre $\mathbb{Z}$ es una relación de equivalencia e indica una partición de los enteros en p clases de equivalencia $[\![0]\!]$, $[\![1]\!]$,... $[\![p-1]\!]$ que se llaman clases residuales módulo p siendo

$[\![r]\!] = \{a/a \in \mathbb{Z}, a \equiv r \bmod (p)\}$.

Denotaremos el conjunto de todas las clases residuales módulo p por $\frac{\mathbb{Z}}{[\![p]\!]}$.

DEFINICION 1.16

Sean (+) suma y

(.) producto definidos entre los elementos de $\frac{\mathbb{Z}}{[\![p]\!]}$ de la manera siguiente:

1) $(a \oplus b) = r$, donde r es el residuo de dividir a+b entre p es decir $a+b = pq + r$.

ii) $(a \odot b) = r$, donde r es el residuo de dividir a.b entre p es decir $a.b = pq + r$.

PROPOSICION 1.10

Sea $p \in \mathbf{Z}$, $p > 0$ y E = conjunto de enteros módulo p

1) Con las operaciones "suma módulo p" y "producto módulo p" E es un anillo.

2) Hay un isomorfismo entre E y $\frac{\mathbf{Z}}{[p]}$.

3) Si p es primo, E es un campo.

4) Si E es un campo, p es un número primo.

1) Con las operaciones "suma módulo p" y "producto módulo p" Es un anillo.

Solo se probará la ley distributiva para saber cuál es el proceso a seguir.

$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot C)$, $a,b,c \in \mathbf{Z}$

$a(+)b = r$, donde $a + b = pq_1 + r_1 \quad 0 < r_1 < p$

$(a \oplus b \odot c = r_2$

$r_1 \odot c = r_2$, donde $r_1 c = pq_2 + r_2 \quad 0 < r_2 < p$

$a \odot c = r_3$, donde $ac = pq_3 + r_3 \quad 0 < r_3 < p$

$b \odot c = r_4$, donde $bc = pq_4 + r_4 \quad 0 < r_4 < p$

$(a \odot c) \oplus (b \odot c) = r_5$

$r_3 \oplus r_4 = r_5$ donde $r_3 + r_4 = pq_5 + r_5 \quad 0 < r_5 < p$

$$r_2 \stackrel{?}{=} r_5$$

Supongamos que $r_2 \neq r_5$

$$r_2 < r_5 \implies 0 < r_5 - r_2 < p - r_2 \leq p$$

$$\implies 0 < r_5 - r_2 < p \dashrightarrow \alpha$$

pero $r_5 = r_3 + r_4 - pq_5$

y $r_2 = r_1 c - pq_2$ $\Big\}$ β

Sustituyendo β en α tenemos

$$0 < r_3 + r_4 - pq_5 - r_1 c + pq_2 < p \dashrightarrow \gamma$$

pero $r_3 + r_4 = ac - pq_3 + bc - pq_4 \dashrightarrow \sigma$

sustituyendo σ en γ nos queda

$$0 < ac - pq_3 + bc - pq_4 - pq_5 - r_1 c + pq_2 < p$$

$$0 < (a + b - r_1)\, c + (q_2 - q_3 - q_4 - q_5) < p$$

$$0 < \frac{(a+b-r_1)c}{p} + q_2 - q_3 - q_4 - q_5 < 1$$

como $q_1 = \dfrac{a + b - r_1}{p}$ nos queda

$$0 < q_1 + q_2 - q_3 - q_4 - q_5 < 1 \quad (\rightarrow \leftarrow)$$

ya que q_1, q_2, q_3, q_4, q_5 son enteros

$r_5 < r_2$ $\quad 0 < r_2 - r_5 < p - r_5 < p$

$$0 < r_2 - r_5 < p \text{ ---------- } (\Sigma)$$

Sustituyendo β en $\sum$ tenemos

$$0 < r_1c - pq_2 - r_3 - r_4 + pq_5 < p \longrightarrow (\text{ℵ})$$

Sustituyen α en ℵ nos queda:

$$0 < r_1c - pq_2 + pq_5 - ac + pq_3 - bc + pq_4 < p$$

asociando

$$0 < (r_1 - a - b)c + (-q_2 + q_3 + q_4 + q_5)p < p$$

$$0 < \frac{r_1 - a - b)}{p} + (-q_2 + q_3 + q_4 + q_5) < 1$$

dividiendo por p

pero como $\frac{r_1 - a - b}{p} = q_1$

entonces $0 < - q_1c - q_2 + q_3 + q_4 + q_5 < 1$

ya que $q_1, q_2, q_3, q_4, q_5 \in \mathbb{Z}$

luego $r_2 = r_5$

Hay un isomorfismo entre E y $\frac{\mathbb{Z}}{[p]}$

Pa.

$$\frac{\mathbb{Z}}{[p]} = \{ x + [p] / x \in \mathbb{Z} \}$$

$$\emptyset: E \longrightarrow \frac{\mathbb{Z}}{[p]}$$

$$x \rightsquigarrow x + [p]$$

Inyectividad

Sean $x, y \in E$ tal que:

$$\emptyset(x) = \emptyset(y)$$

a probar que $x = y$

$\emptyset(x) = \emptyset(y) \implies x + [p] = y + [p]$

$\implies (x-y) \in [p]$, por propiedad de ideales

$\implies x-y = kp \dashrightarrow (\not\downarrow)$

como $x-y = r$, donde r es el residuo de dividir x-y por p.

Como r es un resíduo entonces r tiene que ser menor p, entonces $k = 0$, ya que si $k \neq 0$ entonces $x-y = kp \geq p$

$\therefore x = y$.

Sobreyectividad

$$\frac{\mathbb{Z}}{[p]} = \{ x + [p] \; x \in \mathbb{Z} \}$$

$$\emptyset : E \longrightarrow \frac{\mathbb{Z}}{[p]}$$

$$x \rightsquigarrow x + [p]$$

Tenemos que probar que cualquier elemento de $\frac{\mathbb{Z}}{[p]}$ es imagen de algún elemento de E; x + [p] clases residuales.

Los elementos de $\frac{\mathbb{Z}}{[p]}$ son de la forma x + [p].

$x \mid p$
$r \quad q$ entonces $x = pq + r$

$x - r = pq$ $\qquad 0 \leq r \leq p$

$x - r \in [p]$

$\Rightarrow x + [p] = r + [p] \qquad r \in E$

Por tanto una imagen de $\frac{\mathbb{Z}}{[p]}$ es r + [p]

$\therefore$ Hay un isomorfismo entre E y $\frac{\mathbb{Z}}{[p]}$.

3) Si p es un número primo, E es un campo.

Pa.

Como hay un isomorfismo entre E y $\frac{\mathbb{Z}}{[p]}$ hereda todas las propiedades de $\frac{\mathbb{Z}}{[p]}$

Como p es primo entonces $\frac{\mathbb{Z}}{[p]}$ es un dominio entero entonces E, es dominio entero, por proposición 1.5 1

Por proposición 1.6, si D es dominio entero finito D es un campo.

Como E es dominio entero y tiene p-1 elemento entonces es dominio entero finito.

$\therefore$ E es un campo.

4) Si E es un campo, p es un número primo.

Pa.

Como hay un isomorfismo entre E y $\frac{\mathbb{Z}}{[p]}$ entonces $\frac{\mathbb{Z}}{[p]}$ hereda todas las propiedades de E.

$\frac{\mathbb{Z}}{[p]}$ es un campo entonces por proposición 1.5.4, [p] es maximal.

Ahora, por proposición 1.4 y como $p \in \mathbb{Z}$ y es maximal entonces D es primo.

$\therefore$ es un número primo.

U N I D A D II

SUBCAMPOS DE UN CAMPO.

DEFINICION 2.1

Sea A un campo, decimos que E es un subcampo de A, si E es un campo bajo las operaciones +, . de A.

PROPOSICION 2.1

$\mathbb{Q}$ es subcampo de $\mathbb{R}$ y $\mathbb{R}$ es subcampo de $\mathbb{C}$

Pa.

Sea $\mathbb{Q}$ el conjunto de los números racionales; $\mathbb{Q}$ es un campo, ya que cumple las propiedades de campo.

$\mathbb{R}$ es el conjunto de los números reales, cumple con las operaciones de campo, entonces $\mathbb{R}$ es un campo.

$\mathbb{C}$ el conjunto de números complejos, también cumple con las propiedades de campo, entonces $\mathbb{C}$ es un campo y como

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

es decir, que $\mathbb{Q}$ es subconjunto de un campo que cumple las propiedades de campo.

$\mathbb{R}$ es subconjunto del campo $\mathbb{C}$, donde $\mathbb{R}$ también cumple las propiedades de campo; entonces

$\mathbb{Q}$ es subcampo de $\mathbb{R}$ y $\mathbb{R}$ es subcampo de $\mathbb{C}$.

PROPOSICION 2.2

El conjunto $L = \{ x \in \mathbb{R} / x = a+b\sqrt{2},\ a,b, \in \mathbb{Q}\}$ es un subcampo de $\mathbb{R}$.

Pa.

$\mathbb{R}$ es un campo y $\mathbb{Q} \subset \mathbb{R}$.

$L = \{ x \in \mathbb{R} / x = a+b\sqrt{2},\ a,b, \in \mathbb{Q} \} \subset \mathbb{R}$.

Probar que L definida anteriormente cumple las propiedades de campo.

1) Si $x, y \in L$, entonces $x+y \in L$.

2) Si $x,y \in L$, entonces $xy \in L$.

3) Si $x \in L$, entonces $-x \in L$.

4) Si $x \in L$, $x \neq 0$ entonces $\frac{1}{x} \in L$.

Sólo se probará de 1 a 4, ya que por el teorema de caracterización, solo basta probar cerradura para la suma y el producto, y existencia de elementos inversos y opuesto.

1) Sea $x,y \in L$

$x = a+b\sqrt{2}$

$y = c+d\sqrt{2}$

$x+y = (a+c)+(b+d)\sqrt{2}$

como a+c son racionales, entonces $x+y \in L$.

2) Sea $x,y \in L$

$xy = (a+b\sqrt{2})(c+d\sqrt{2})$

$$xy = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$$

$$xy = ac + 2bd + ad\sqrt{2} + bc\sqrt{2}$$

$$xy = ac + 2bd + (ad + bc)\sqrt{2}$$

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2}$$

$\therefore$ $xy \in L$,

3) Si $x = a + b\sqrt{2} \in L$ entonces $-x \in L$

$$-x = -a-b\sqrt{2} \in L$$

$$-x = -(a+b\sqrt{2}) \in L$$

$\therefore$ $-x \in L$.

4) Si $x = a+b\sqrt{2} \in L$ entonces $\frac{1}{x} \in L$. (donde $\frac{1}{x}$ es el elemento inverso de L).

$$x = a+b\sqrt{2} \Rightarrow \frac{1}{x} = \frac{1}{a+b\sqrt{2}}$$

$$\frac{1}{x} = \frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$\frac{1}{x} = \frac{a}{(a^2-2b^2)} - \frac{(b)}{(a^2-2b^2)}\sqrt{2}$$

$$\frac{1}{x} = \frac{a}{(a^2 - 2b^2)} - \left(\frac{b}{a^2 - 2b^2}\right)\sqrt{2} \in L$$

$$a^2 - 2b^2 \neq 0$$

ya que $a^2 - 2b^2 = 0$

$$\Rightarrow \quad 2 = \frac{a^2}{b^2}$$

$$\sqrt{2} = \frac{a}{b} \in L$$

$$\therefore \quad \frac{1}{x} \in L .$$

PROPOSICION 2.4

El conjunto de matrices de la forma $\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$ $b \in \mathbb{Q}$ es un campo.

$$T = \{ M_2/M_2 = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} , b \in \mathbb{Q} \}$$

a probar:

i) $x,y \in T \Rightarrow x+y \in T$

ii) Si $x \in T \Rightarrow -x \in T$

iii) Si $x \in T \Rightarrow \frac{1}{x} \in T$

Pa.

i) $x = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$

$y = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$

$x+y = \begin{bmatrix} b+a & 0 \\ 0 & b+a \end{bmatrix} \in T$

ii) $x = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \Rightarrow -x = \begin{bmatrix} -b & 0 \\ 0 & -b \end{bmatrix} \in T$

iii) $x = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$ $b \neq 0$ a probar que tiene inverso.

Supongamos que $\frac{1}{x} = \begin{bmatrix} \frac{1}{b} & 0 \\ 0 & \frac{1}{b} \end{bmatrix}$ lo que implica que $x^{-1} = \begin{bmatrix} b^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix}$;

entonces $x.\frac{1}{x}$ tiene que ser igual a la matriz identidad

$$x.\frac{1}{x} = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} b^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} bb^{-1} + 0 & 00 + 0b^{-1} \\ 0b^{-1} + b0 & 0 + b^{-1}b \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

con lo que la matriz inversa de T es

$$x^{-1} = \begin{bmatrix} b^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix}$$

$\therefore$ T tiene inverso

PROPOSICION 2.3

a) En un campo k los únicos ideales son $\{0\}$ y k.

b) Si k es un anillo unitario y conmutativo cuyos únicos ideales son $\{0\}$ y k entonces k es un campo.

Solución:

a) En un campo k los únicos ideales son $\{0\}$ y k.

Pa.

Sea I un ideal de k tal que:

$I \neq \{0\}$,

A probar que $I = k$

Esto se reduce a verificar que $1 \in I$; como $I \neq \{0\}$, entonces, sea $y \in I$, $y \neq 0$.

Se tiene que k es un campo y $y \in K$; luego existe $y^{-1} \in k$ tal que:

$yy^{-1} = 1$ pero $y \in I$ e I es un ideal, teniéndose así:

$yy^{-1} = 1 \in I$

por lo tanto $I = k$

∴ los únicos ideales son $\{0\}$ y k.

b) Si k es un anillo unitario y conmutativo cuyos únicos ideales son $\{0\}$ y k entonces k es un campo.

Pa.

Sea $x \in k$, $x \neq 0$

a probar, que existe $x^{-1} \in k$

$I = \{y \in k / y = mx, m \in k\}$

i) $I \neq 0$

ya que al menos el cero está en I

ii) $y, z \in I$

$y = m_1 x$

$z = m_2 x$

$y + z = m_1x + m_2x$

$y + z = (m_1 + m_2)x$

$(m_1 + m_2)x \in I$ luego $y + z \in I$

iii) $y \in I$

$y = mx$

$-y = -mx$

$-y = (-m)x$

$-mx \in I$ ya que I es ideal

luego $-y \in I$.

iv) Si $y \in k$ y $z \in I$ entonces $yz \in I$

$z = mx$

$yz = y(mx)$

$= (ym)x$

$(ym)x \in I$, por ser I ideal y por la forma en que está definido,

$\therefore$ $yz \in I$.

v) $I \neq \{0\}$ porque $x \in I$

$x \neq 0$ por hipótesis

$\therefore\ I \neq \{0\}$

Si $I = k$ entonces $1 \in I$

luego, existe $m \in k$ tal que:

$1 = mx,\ m \in k,\ x \in I$

$\frac{1}{x} = m$

$x^{-1} = m$

por tanto k tiene elemento inverso

$\therefore$ k es un campo.

PROPOSICION 2.4

Sea k un campo.

1.- La intersección de dos subcampos de k es un subcampo de k.

Pa.

Sean F_1, F_2 dos subcampos de un campo k; probar que

$E = F_1 \cap F_2$ es un subcampo de k.

i) $E \neq \emptyset$, $1 \in E$ porque $1 \in F_1, F_2$.

ii) (E, +) es subgrupo de (k, +), porque F_1, F_2 es un subgrupo (por definición de subcampo) y la intersección de subgrupos es subgrupo.

iii) Sea $x,y \in E$, $x,y \in F_1 \wedge x,y \in F_2$ luego $xy \in F_1 \wedge xy \in F_2$ por ser F_1, F_2 subcampos, por tanto $xy \in E$.

iv) Sea $x \in E$, $x \neq 0$, $x \in F_1$, $x \in F_2$

F_1, F_2 son subcampos, lo que implica que $x^{-1} \in F_1$, F_2 luego $x^{-1} \in E$.

$\therefore$ E es un subcampo de k.

2.- La intersección de una familia $(Fi)i \in I$ de subcampos de k es un subcampo de k.

Pa.

Sea $(Fi)i \in I$, $I \neq 0$ una familia de subcampos de un campo k; probar que:

$$E = \bigcap_{i \in I} Fi \text{ es un subcampo de k.}$$

i) $E \neq \emptyset$, $1 \in E$ porque $1 \in Fi \ \underline{\forall}\ i$

ii) (E, +) es subgrupo de (k, +), porque cada Fi es un subgrupo y la intersección de subgrupos es subgrupo.

iii) Sea $x,y \in E$, $x, y \in Fi$, $\forall i$, luego $x\,y \in Fi$; por tanto $xy \in E$.

iv) Sea $x \in E$, $x \neq 0$, $x \in Fi$, $\forall i$ como Fi es subcampo, $x^{-1} \in Fi\ \forall i$ luego $x^{-1} \in E$.

$\therefore$ E un subcampo de k.

3. Si $S \subset k$, existe un subcampo L de k único que cumple las dos propiedades siguientes:

   i) $S \subset L$

   ii) Si $F \subset k$ es un subcampo tal que $S \subset F$ entonces $L \subset F$.

   (Este subcampo único se denota [S] y es llamado "subcampo generado por S")

Pa.

Existencia

i) El conjunto de subcampos de k que incluyen a S no es vacío, $S \subset k$

- Sea L = intersección de todos los subcampos de k, tal que $S \subset H$, H subcampo de k

$$L = \bigcap_{S \subset H} H$$

H subcampo de k;

como $S \subset H$ y $L = \bigcap H$ se tiene que $S \subset L$.

L es un subcampo de k, por ser intersección de subcampos (por prop. 2.4.2); además $S \subset L$.

$\therefore$ Existe un subcampo L.

Sea F un subcampo de k, tal que $S \subset F$;

probemos que $L \subset F$.

Como $S \subset F$, entonces F es uno de los H que forman L.

Así que $L = \bigcap_{S \subset H} H \subset F$

$\therefore$ $L \subset F$

ii) Unicidad

Sean I_1, I_2 subcampos de k tal que:

(1) $S \subset I$.

(2) Si L es subcampo de k tal que $S \subset L$ entonces $I_1 \subset L$.

(3) $S \subset I_2$

(4) Si L es un subcampo de k tal que $S \subset L$ entonces, $I_2 \subset L$.

Probar que $I_1 = I_2$

i) I_2 es un subcampo de k.

"$\subset$" verifiquemos que $I_1 \subset I_2$.

I_2 es un subcampo de k y $S \subset I_2$; por propiedad 2 se obtiene que $I_1 \subset I_2$

"$\supset$" Mostremos que $I_2 \subset I_1$.

I_1 es un subcampo de k y $S \subset I$; por 4 se tiene que $I_2 \subset I_1$

Sea k un campo

(4) K contiene un subcampo primo y solo uno

Pa.

Sea $S = \{0\}$

$L = \bigcap_{\{0\} \subset H} H$

L es la intersección de una familia de subcampos y es un subcampo, por propiedad 2.4.2; ahora como es la intersección de todos los - subcampos, entonces L, es un subcampo primo (por definición).

Por proposición 2.4.3, existe un subcampo L de k, único entonces L que es un subcampo primo, es único.

$\therefore$ k contiene un subcampo primo y solo uno.

Sea k un campo.

(5) El subcampo primo de k es el subcampo generado por $\{0\}$

Sea $S = \{0\}$

$L = \bigcap H$

$\{0\} \subset H$

Por proposición 2.4.4, L es subcampo primo de k;

i) A probar que $S \subset L$;

como $S = \{0\}$ y $L = \bigcap H$

$\{0\} \subset H$

entonces $\{0\}$ está contenido en todos los subcampos que forman la intersección de L, por lo que: $S \subset L$.

ii) Si $F \subset K$ es un subcampo tal que $S \subset F$, entonces, $L \subset F$.

Pa.

Como $S \subset F$ y $S = \{0\}$

F es uno de los H que forman L que contienen $\{0\}$

entonces $L = \bigcap H \subset F \Rightarrow L \subset F$

$\{0\} \subset H$

PROPOSICION 2.5

Sea $f: k \longrightarrow F$ un homomorfismo de campo.

Entonces, si $f \neq 0$

1) $f(1) \neq 0$

2) $f(1) = 1$

3) $x \in k$, $x \neq 0$, $\Longrightarrow f(x) \neq 0$

4) Si $x \in k$, $x \neq 0$, $f(x^{-1}) = f(x)^{-1}$

5) f es inyectivo

Pa.

1) $f(1) \neq 0$

Supongamos que $f(1) = 0$;

Sea $x \in f$

$f(x) = f(x.1) = f(x)f(1)$ por ser f un homomorfismo

$f(x).0$, ya que supusimos que $f(1) = 0$

Luego $f(x) = 0$ es una contradicción, ya que por hipótesis,

$f(x) \neq 0$

$\therefore$ $f(1) \neq 0$

2) $f(1) = 1$

$f(1) = f(1.1)$

$= f(1).f(1)$, por ser f un homomorfismo

$f(1)f^{-1}(1) = f(1).f(1).f^{-1}(1)$

$1 = f(1)$

por tanto: $f(1) = 1$

3) Si $x \in K$, $x \neq 0$, entonces $f(x) \neq 0$

Pa.

$f(1) = f(xx^{-1})$

$= f(x)f(x^{-1})$, por ser f un homomorfismo.

$f(x)f(x^{-1}) \neq 0$, ya que $f(1) \neq 0$

luego $f(x) \neq 0$

4) Si $x \in k$, $x \neq 0$, $f(x^{-1}) = f^{-1}_{(x)}$

Pa.

$1 = f(1)$

$= f(xx^{-1})$

$= f(x)f(x^{-1})$, por ser f un homomorfismo.

$1 = f(x)\ f(x^{-1})$

$f^{-1}_{(x)} = f^{-1}(x)\ f(x)\ f(x^{-1})$

$f^{-1}(x) = 1.f(x^{-1})$

$f^{-1}(x) = f(x^{-1})$

$\therefore\ f(x^{-1}) = f^{-1}(x)$

5) f es inyectivo

Pa.

Sea $x_1, x_2 \in k$ tal que: $f(x_1) = f(x_2)$

$f(x_1) = f(x_2)$

$f(x_1) - f(x_2) = 0$

$f(x_1 - x_2) = 0$, ya que f es un homomorfismo

$\Rightarrow\ x_1 - x_2 = 0$

$\Rightarrow\ x_1 = x_2$

$\therefore$ f es inyectivo.

DEFINICION 2.2

Anillo de polinomios. Sea F un campo, el anillo de polinomios en x sobre F, que siempre se expresará como F[x], es el conjunto de todas las expresiones formales $p(x) = a_o + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$, donde las a_i, llamados coeficientes del polinomio p(x), están en F.

En F[x] se definen igualdad, suma y producto de dos polinomios para hacer de F[x] un anillo conmutativo como sigue:

1) Igualdad. Se define que $P(x) = a_o + a_1x + \ldots + a_nx^n$ y $q(x) = b_o + b_1x + \ldots + b_mx^m$ son iguales si y solo si sus coeficientes correspondientes son iguales, es decir, si y solo si $a_i = b_i$ para todo $i > 0$

DEFINICION 2.3

Sea p(x) un polinomio enF[x]. Se dice que p(x) es irreducible si y solo si:

p(x) = q(x) r (x) implica que

grad (q(x)) = 0 V grad (r(x)) = 0

DEFINICION 2.4

El grado n = [u:F] de un elemento u algebraico sobre un campo F, es el grado n del único polinomio mónico irreducible con coefi-

cientes en F que tiene la raíz u.

n = grado de p(x).

2.- Adición: Si $p(x) = a_o + a_1x + \ldots + a_nx^n$ y

$q(x) = b_o + b_1x + \ldots + b_mx^m$, se define $p(x) + q(x) = c_o + c_1x + \ldots + c_sx^s$ donde para cada $c_i = a_i + b_i$

Así que los polinomios se suman sus coeficientes correspondientes.

3. Multiplicación. Si $p(x) = a_o + a_1x + \ldots + a_nx^n$ y

$q(x) = b_o + b_1x + \ldots + b_mx^m$ se define $p(x)q(x) = c_o + c_1x + \ldots + c_tx^t$, donde los c_i se determinan multiplicando la expresión formalmente (es decir, en cuanto a la forma), utilizando las leyes distributivas y las reglas de los exponentes $x^u x^v = x^{u+v}$, y reuniendo términos.

De manera más formal:

$c_i = a_ib_o + a_{i-1}b_1 + \ldots + a_1b_{i-1} + a_ob_i$, para todo i

PROPOSICION 2.6

Si F es un campo, el anillo de polinomios F[x] es un dominio entero principal.

Pa.

1) Si $p(x), q(x) \in F[x]$ y $p(x)\,q(x) = 0$; probar que

$p(x) = 0 \quad \vee \quad q(x) = 0$

Tomando los grados de cada polinomio

grado de $p(x) = 0$

grado de $q(x) = 0$

$p(x) = k_1$ y $q(x) = k_2$, porque son de grado cero

$k_1 k_2 = 0$, $k_1 = 0 \vee k_2 = 0$

$p(x) = 0$ ó $q(x) = 0$

2) Sea I un ideal de F[x] probar que existe $p(x) \in F[x]$ tal que

$I = [p(x)]$

a) Si $I = 0$, $p(x) = 0$

b) Si $I \neq 0$, sea $T = \{ q(x) \in I / \text{grado de } q(x) > 0 \}$

Sea $p(x) \in T$ un polinomio de grado mínimo

$q(x) \mid p(x)$ utilizando el algoritmo de la división,

$r(x) \quad s(x)$

grad de $r(x) <$ grad de $p(x)$

$q(x) = s(x)p(x) + r(x)$, $q(x) \in T$

y $p(x) \in T$ $\qquad$ $p(x)\,s(x) \in I$

$r(x) = q(x) - s(x)\,p(x)$ $\qquad$ ya que $p(x) \in I$

$r(x) \in I$

grado de $r(x)$ $<$ grado de $p(x)$

como $p(x)$ es de grado mínimo, y no puede haber otro polinomio de menor grado que $p(x) \in T$ entonces $r(x) \notin T$;

como $r(x) \notin T$, entonces por la forma en que se definió T, lo único que le queda al grad de $r(x) = 0$; que el grado de $r(x)$ sea igual a cero. Puede suceder:

i) $r(x) = k \neq 0$ como $k \in F$ y F es un campo, entonces tiene inverso multiplicativo; entonces $1 = k^{-1}k$, como $r(x) = k$ y $r(x) \in I$, entonces $1 \in I$; como $1 \in I$ y todo ideal que contiene al 1 es todo el anillo, entonces

$1 \in F[x]$

$\Rightarrow I = [1]$

ii) Si $r(x) = 0$ entonces $q(x) = s(x)p(x)$

como $q(x) \in I$, implica que $I = F[x]$

$\therefore$ $F[x]$ es dominio entero principal.

PROPOSICION 2.7

Sea F un campo y sea $p(x) \in F[x]$. Pruebe que el ideal generado por $p(x)$ es maximal si y solo si es irreducible.

Pa.

p(x) es irreducible si:

i) p(x) no es constante.

ii) $p(x) = q(x)t(x) \Rightarrow$ q(x) constante $\vee$ t(x) constante

Sea $I \subset F[x]$ un ideal maximal, y sea $p(x) \in F[x]$ tal que:

$I = [p(x)]$; probar que p(x) es irreducible;

si $p(x) = q(x)t(x)$ ----> (α)

entonces q(x) = constante $\vee$ t(x) = constante

$p(x) \in [q(x)] \Rightarrow [p(x)] \subset [q(x)]$;

por ser $I = [p(x)]$ maximal, entonces $[q(x)] = I$ ó

$[q(x)] = F[x]$;

Si $[q(x)] = [p(x)]$ entonces

$q(x) = s(x)\, p(x)$ ----> (β)

grado de p(x) = grado de q(x)

entonces s(x) = constante;

sustituyendo (α) en (β) tenemos

$q(x) = s(x)t(x)q(x)$;

como el grado de q(x) del miembro derecho es el mismo del q(x) de la izquierda entonces, de

$q(x) = s(x)t(x)q(x)$ no queda más que

$s(x)t(x)$ = constante

por tanto, t(x) = constante.

Si $[q(x)] = F[x]$ entonces

$1 \varepsilon [q(x)]$, lo que implica que

$1 = w(x)q(x)$

luego $q(x)$ = constante.

$\therefore$ $[p(x)]$ es irreducible.

"$\Leftarrow$"

F es un campo $p(x) \varepsilon F[x]$ un polinomio.

probar que el ideal generado por $p(x)$ es maximal si $p(x)$ es irreducible.

Pa.

i) Sea $T = [p(x)]$, T un ideal.

ii) $p(x) \varepsilon T$.

Sea I un ideal tal que $T \subset I$ probemos que $T = I$ ó $I = F[x]$

Si $T \neq I$ entonces $I = F[x]$;

como $T \neq I$, entonces, existe $q(x) \varepsilon I$ y $q(x) \notin T$;

además $I = [R(x)]$, $q(x) = s(x)\, R(x)$, como $T \subset I$, entonces $p(x) \varepsilon I$, ya que $T = [p(x)]$.

Si $p(x) \varepsilon I$, $p(x) \varepsilon [R(x)]$ entonces $p(x) = t(x)R(x)$; como $p(x)$ es irreducible, implica que $t(x)$ ó $R(x)$ son constantes.

1) Si $t(x) = k$, $k \varepsilon F$

$p(x) = kR(x)$, $R(x) = k^{-1}p(x)$; luego sustituyendo $R(x)$ tenemos:

$q(x) = s(x)\,[k^{-1}p(x)] = \frac{1}{k}\, s(x)p(x)$ lo que implica que

$q(x) \in [p(x)]$, y es una contradicción, ya que

$[p(x)] = T$ y $q(x) \notin T$

entonces $R(x)$ es constante.

2) Si $R(x) = k$, entonces $p(x) = kT(x)$

$1 = kk^{-1}$ como $k \in I \wedge k^{-1} \in F[x]$

entonces $kk^{-1} \in I$

$\therefore \quad 1 \in I$

DEFINICION 2.5

Se dice que un campo F tiene, ó es de característica $p \neq 0$, si para cierto entero positivo P, $px = 0$ para todo $x \in F$, y ningún entero positivo menor que p goza de esta propiedad.

DEFINICION 2.6

Si un campo F no es de característica $p \neq 0$ para ningún entero positivo p, se le llama campo de característica cero.

PROPOSICION 2.8

Sea F un campo de característica cero, $e \in F$ la identidad.

1) $D = \{ x \in F / x = me, m \in \mathbb{Z} \}$ es un dominio entero.

2) El campo de fracciones k asociado a D es el subcampo primo de F.

3) La función $\phi: \mathbb{Q} \to k: \frac{m}{n} \rightsquigarrow \frac{me}{ne}$ es un isomorfismo.

Pa.

Probar que es un subanillo

i) Sea $x,y \in D \longrightarrow x+y \in D$

$x = m.e \in D, m \in \mathbb{Z}$

$y = m_1 e, m \in Z$

$x+y = (m+m_1)e, (m+m_1) \in Z$

$(mx+nx) = x+x+....+x$ m veces + $(x+x+....+x)$n veces

$= (x+x+x+.....+x)(m+n)$ veces

ii) Sea $x \in D \wedge y \in D$

$x = m.e$

$y = m_1.e$

$xy = (m.e)(m_1.e)$

$= (m.m_1).e$, $m.m_1 \in \mathbb{Z}$

iii) Probar que D es dominio entero

Pa.

Si $x,y \in D$, si $xy = 0$ entonces $x=0 \vee y=0$

Sea $x = m_1 e$

$y = m_2 e$ donde $m_1, m_2 \in Z$

Luego, si $(m_1e)(m_2e) = 0$ entonces

$m_1e = 0 \vee m_2e = 0, m_1, m_2 \in Z$

$(m_1e)(m_2e) = 0$, donde e es la identidad

$(m_1e)(m_2e) = (m_1m_2)e = 0$

luego $(m_1m_2)e = 0$

$m_1m_2 = 0$, ya que e es la identidad de F y no puede ser $e = 0$.

Ahora, si $m_1m_2 = 0$, $m_1, m_2 \in Z$ y lo que implica que $m_1 = 0 \vee m_2 = 0$;

Si $m_1 = 0$ entonces $x = 0e$

$x = 0$, por ser F de característica cero.

$\therefore m_1e = 0$

Si $m_2 = 0$ entonces $y = 0e$

$y = 0$ por ser F de característica cero

$m_2e = 0$

por tanto D es dominio entero.

2) $k = \{ x \in F/x = yz^{-1}, y \in D, z^{-1} \in D \}$

$k = \{ x \in F/x = \frac{y}{z}, y \in D, z \in D \}$

$k = \{ x \in F/x = \frac{m.e}{n.e}, m,n \in Z, n \neq 0 \}$

Sea T un subcampo de F, probemos que k $\subset$ T

e ε T, m.e, n.e ε T

$$\frac{m.e}{n.e} \varepsilon T$$

3) La función $\phi : \mathbb{Q} \to k: \frac{m}{n} \rightsquigarrow \frac{m.e}{n.e}$ es un isomorfismo

$$\phi : \mathbb{Q} \to k$$

$$\frac{m}{n} \rightsquigarrow \frac{m.e}{n.e}$$

probar que existe un homomorfismo, $\Phi : Q \longrightarrow k$, es decir:

i) $\Phi\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) = \Phi\left(\frac{m_1}{n_1}\right) + \Phi\left(\frac{m_2}{n_2}\right)$

$\Phi\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) = \left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) e$ $\qquad \frac{m_1}{n_1}, \frac{m_2}{n_2} \varepsilon \mathbb{Q}$

$e \varepsilon F$

$= \left(\frac{m_1}{n_1}\right) e + \left(\frac{m_2}{n_2}\right) e,$ ya que e ε F y F es un campo.

$$= \frac{m_1 e}{n_1 e} + \frac{m_2 e}{n_2 e}$$

$$\therefore \quad \Phi\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) = \Phi\left(\frac{m_1}{n_1}\right) + \Phi\left(\frac{m_2}{n_2}\right)$$

ii) $\Phi(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}) \stackrel{?}{=} \Phi(\frac{m_1}{n_1}) \cdot \Phi(\frac{m_2}{n_2})$

$$\Phi(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}) = (\frac{m_1}{n_1} \cdot \frac{m_2}{n_2})\, e$$

$$= (\frac{m_1}{n_1} \cdot \frac{m_2}{n_2})(e.e) \qquad e \text{ es la identidad}$$

$$= (\frac{m_1}{n_1} \cdot e) \cdot (\frac{m_2}{n_2} \cdot e)$$

$$= \Phi(\frac{m_1}{n_1}) \cdot \Phi(\frac{m_2}{n_2})$$

$\therefore$ Existe un homomorfismo $\Phi: \mathbb{Q} \to k$

Ahora verifiquemos que es un homomorfismo biyectivo.

i) Inyectividad:

Sean $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in \mathbb{Q}$ tal que $\Phi(\frac{m_1}{n_1}) = \Phi(\frac{m_2}{n_2})$

$$\Phi(\frac{m_1}{n_1}) = \Phi(\frac{m_2}{n_2})$$

$$\Phi(\frac{m_1}{n_1}) - \Phi(\frac{m_2}{n_2}) = 0$$

$$\frac{m_1 e}{n_1 e} - \frac{m_2 e}{n_2 e} = 0$$

$(\frac{m_1}{n_1} - \frac{m_2}{n_2})e = 0$, como e es la identidad para F, e no puede ser cero, lo que implica que

$$\frac{m_1}{n_1} - \frac{m_2}{n_2} = 0$$

$$\Rightarrow \quad \frac{m_1}{n_1} = \frac{m_2}{n_2}$$

$\therefore$ Φ es inyectivo

ii) Sobreyectividad

$$\emptyset: \quad \mathbb{Q} \rightarrow k$$

$$\frac{m}{n} \rightsquigarrow \frac{m.e}{n.e}$$

Tenemos que probar que cualquier elemento de k, es imagen de algún elemento de $\mathbb{Q}$; los elementos de L son de la forma $\frac{m.e}{n.e}$

Existe un $\frac{k}{t} \in \mathbb{Q}$ tal que

$$\frac{m.e}{n.e} = \frac{k.e}{t.e}$$

luego se tiene que:

$$\Phi\left(\frac{k}{t}\right) = \frac{k.e}{t.e}$$

$$= \frac{m.e}{n.e}$$

$\therefore$ la preimagen buscada para

$$\frac{m.e}{n.e} \quad \text{es} \quad \frac{k}{t}$$

PROPOSICION 2.9.

Sea F un campo de característica p > 0 entonces

1) p es número primo.

2) L = { x ε F/x = m.e, m ε $\mathbb{Z}$} es un subcampo de F

3) L es un subcampo primo de F.

4) Hay un isomorfismo entre Jp y L .

Pa.

Sea F un campo de característica p > 0 entonces p es número primo.

P = caract (F), p.x = 0 ∀ x ε F

Supongamos que p no es primo.

P = m.n, m, n ε N, m< p, n < p

Sea x ≠ 0, luego px = (mn)x, se tiene que px = 0 y p = mn lo que

implica que (mn)x = 0 $\Rightarrow$ m(nx) = 0

como nx ε F, puede suceder que:

i) nx = 0

Sea y ≠ 0, luego (nx)y = y.0

(nx)y = 0

$\Longrightarrow$ x(ny) = 0

como x ≠ 0 implica que ny = 0 ∀ y ε F

con lo que p < n

pero n < p lo que implica que p = n y m = 1, por tanto p es

primo; lo que contradice la hipótesis.

ii) $nx \neq 0$

Sea $y \neq 0$, luego $(mn)(xy) = 0y$

$$(mn)(xy) = 0$$

$$\Longrightarrow \quad (my)(nx) = 0$$

como F es un campo, entonces es un dominio entero, y como $my, nx \in F$ y $(my)(nx) = 0$, implica que $my = 0 \vee nx = 0$ pero como $nx \neq 0$ lo único que queda es que $my = 0 \; \forall \; y \in F$ $my = 0 \Rightarrow p \leq m$ pero $m \leq p$, por tanto $m = p \wedge n = 1$, lo que se concluye que p es primo, luego ésto es una contradicción.

$\therefore$ p es primo.

2) Sea F un campo de característica $p > 0$ entonces $L = \{ x \in F / x = m.e, m \in \mathbb{Z} \}$ es un subcampo de F.

Pa.

$L = \{ 0, 1.e,, 3.e, \ldots . (p-1)e \}$

Sea $x \in L$, $x = m.e$, $m \in \mathbb{Z}$; utilizando el algoritmo de la división tenemos:

$$\begin{array}{c|c} m & p \\ \hline r & q \end{array}, \text{ luego } m = pq + r; \; 0 < r < p$$

$x = m.e$, sustituyendo el valor de m tenemos que:

$x = (pq + r)\, e$

$= p(qe) + r.e \qquad r < p$

$= r.e$ ya que $p(q.e) = 0$ por ser F un campo de característica $p > 0$

Como $x = r.e$ y $x \in L$ entonces L es finito.

Probemos que L es dominio entero.

Sean $y,z \in L$, tales que $y.z = 0$; como $y,z \in L$, entonces existen $m,n \in \mathbb{Z}$ tales que $y = m.e$ y

$z = n.e$

Luego se tiene que:

$(m.e)(n.e) = 0$

$(m.n)e = 0$

entonces $p \nmid m.n$, por ser F un campo de característica p.

Como p es primo, $p|m$ o $p|n$

Si $p \nmid m$ entonces $y = m.e = 0$

Si $p \nmid n$ entonces $z = n.e = 0$

Luego L es un dominio entero finito y por 1.6 L es un campo.

Como L es un campo y $L \subset F$ entonces L es un subcampo de F.

3) L es el subcampo primo de F.

$L \subset L_1$ es otro subcampo de F

Sea $x \in L$, $x = m.e$ $\quad e \in L_1$

$\Rightarrow x \in L_1$

Como L y L_1 son subcampos de F, y $x \in L_1$ y $x \in L$, entonces $x \in L_1 \cap L_2$; como $x \in L_1 \cap L_2$, podemos concluir que L es el subcampo primo de F.

Hay un isomorfismo entre Jp y L

$$Jp = \{ 0, 1, 2, \ldots . p-1 \}$$

$$\phi : Jp \longrightarrow L$$

$$m \rightsquigarrow m.e$$

Probemos que existe un homomorfismo de Jp L, es decir que:

i) $\Phi(m+n) = \Phi(m) + \Phi(n)$

$\Phi(m+n) = (m+n)e$, por definición

$= me + ne$, ya que $e \in F$ y F es un campo

$= \Phi(m) + \Phi(n)$

$\therefore \Phi(m+n) = \Phi(m) + \Phi(n)$

ii) $\Phi(m.n) = \Phi(m) \cdot \Phi(n)$

$\Phi(m\ n) = (m\ n)e$ por definición

$= (m.e)(n.e)$, ya que $e \in F$ y F es un campo

$= \Phi(m)\ \Phi(n)$

$\therefore \Phi(mn) = \Phi(m)\ \Phi(n)$

Por lo tanto, existe un homomorfismo de $Jp \longrightarrow L$

. Ahora probemos que el homomorfismo es biyectivo

i) Inyectividad

$\phi : Jp \longrightarrow L$

$m \rightsquigarrow m.e$

Sea $m, n \in Jp$ tal que $\phi(m) = \phi(n)$

$\Phi(m) = \Phi(n)$

$\phi(m) - \phi(n) = 0$

$(m.e)-(n.e) = 0$ aplicando definición

$(m-n)e = 0$ $m,n < p$

Luego $(m-n) = 0$ ya que $e \neq 0$, $e \neq p$, por ser

o $(m-n) = p$ la identidad de F

pero $(m-n) \neq p$ ya que $m, n < p$

Como $m-n = 0$ implica que $m = n$

$\therefore$ ϕ es inyectivo

ii) Sobreyectividad

$Jp = \{0, 1, 2, \ldots, p-1\}$

$\phi : Jp \longrightarrow L$

$m \rightsquigarrow m.e$ $m \in \mathbb{Z}$

tenemos que probar que cualquier elemento de L es imagen a algún elemento de Jp.

Los elementos de L son de la forma m.e

a) Si $0 \leq m \leq p-1$

entonces la imagen será m

b) Si $m > p-1$

Existe un $k \in Jp$ tal que

$$me = ke$$

luego se tiene que

$$\phi(k) = ke$$

$$= m.e$$

$\therefore$ la preimagen buscada para m.e es k.

por lo tanto hay un isomorfismo entre Jp y L.

DEFINICION 2.7

Un espacio vectorial $\mathbf{V}$ sobre un campo F es un grupo abeliano respecto a la adición "+ tal que, para todo $\alpha \in F$ y todo $v \in \mathbf{V}$, existe un elemento $\alpha v \in \mathbf{V}$ tal que:

a) $\alpha(V_1 + V_2) = \alpha V_1 + \alpha V_2$, para $\alpha \in F$, $V_1, V_2 \in \mathbf{V}$

b) $(\alpha + \beta)v = \alpha v + \beta v$, para $\alpha, \beta \in F$, $v \in \mathbf{V}$

c) $\alpha(\beta v) = (\alpha\beta)v$, para $\alpha \beta \in F$, $v \in \mathbf{V}$

d) $1v = v$, para todo $v \in \mathbf{V}$, donde 1 es el elemento unidad de F.

DEFINICION 2.8

Si $B = \{ b_1, b_2, \ldots\ldots, b_n \}$ es una base de un espacio vectorial V sobre un campo F, todas las bases del espacio vectorial V sobre F tienen el mismo número de elementos, a este número se le llama dimensión de V.

PROPOSICION 2.10

Sean F un campo, $P(x) \in F[x]$, n=grado de p(x)

Probar que el cociente $\frac{F[x]}{[p(x)]}$ es un F - e - v de dimensión n.

Pa.

Sean [p(x)]el ideal generado por p(x) entonces p(x)] = I

Probar que $\frac{F[x]}{I}$ es un F espacio vectorial de dimensión n.

Encontrar una base de n elementos

$B = \{ 1 + I, x + I, x^2 + I, \ldots x^{n-1} + I\}$ es una base de $\frac{F[x]}{I}$

B es l . i

Sean $\alpha_o, \alpha_1, \ldots \alpha_{n-1}$ escalares en F tal que

$$\alpha_o(1+I) + \alpha_1(x+I) + \ldots + \alpha_{n-1}(x^{n-1} + I) = 0$$

$$\alpha_o + I + \alpha_1 x + I + \alpha_2 x^2 + I + \ldots + \alpha_{n-1} x^{n-1} + I + 0$$

$$\alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1} + I = I$$

$$\alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1} \in I \text{ ------- } (\gamma)$$

$$\alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1} = \delta p(x)$$

$$p(x) = \beta_o + \beta_1 x + \beta_2 x^2 + \ldots + \beta_n x^n, \quad \beta_n \neq 0 \text{ ---- } (\theta)$$

igualando los polinomios (γ) y (θ) tenemos:

$$\alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1} = (\delta \beta_o) + (\delta \beta_1) x + \ldots + (\delta \beta_n) x^n$$

$$\alpha_o = \delta \beta_o, \quad \alpha_1 = \delta \beta_1, \quad \alpha_2 = \delta \beta_2 \ldots \alpha_{n-1} = \delta \beta_{n-1}$$

$$0 = \delta \beta_n$$

$$\delta \beta_n = 0 \text{ y } \beta_n \neq 0 \qquad \delta = 0$$

luego $\alpha_o = 0, \quad \alpha_1 = 0 \ldots\ldots \quad \alpha_{n-1} = 0$

Por tanto β es 1 , i

β es un generador de $\frac{F[x]}{I}$

Sea $q(x) \in \frac{F[x]}{I}$ probar que $q(x) + I \in [B]$

Encontrar escalares $\alpha_o, \alpha_1 \cdots \alpha_{n-1}$ tal que

$$q(x) + I = \alpha_o(1+I) + \alpha_1(x+I) + \ldots + \alpha_{n-1}(x^{n-1} + I)$$

Sea $q(x) = \gamma_1 + \gamma_2 x + \ldots + \gamma_n x^m$, $\gamma_m \neq 0$

$$q(x) + I = \gamma_o(1+I) + \gamma_1(x+I) + \ldots + \gamma_m(x^m+I)$$

Si $m < n$ queda probado

Si $m < n$ $q(x) \overline{|p(x)}$; $q(x) - t(x) = s(x)\, p(x)$

$t(x) \quad S(x)$

$q(x) - t(x) \in I$

$q(x) + I = t(x) + I \in [B]$

$$t(x) = \sum_{i=0}^{r} \alpha_i x^2 \qquad r < n$$

U N I D A D III

EXTENCIONES DE UN CAMPO.

DEFINICION 3.1.

Sean E, F dos campos. Se dice que F es una extensión de E, si E es un subcampo de F con las operaciones de F ($E \subset F$)

DEFINICION 3.2

Una aplicación $\emptyset$ del anillo $\mathbb{R}$ en el anillo $\mathbb{R}'$ se dice que es un homomorfismo si

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

2) $\emptyset(ab) = \emptyset(a)\,\emptyset(b)$

Para $a, b \in \mathbb{R}$ cualesquiera

PROPOSICION 3.1

Sea $f: A \longrightarrow B$ un homomorfismo de anillos.

Entonces:

a) Hay un homomorfismo sobreyectivo

$f_1: A \longrightarrow I_m(f)$

b) Hay un homomorfismo inyectivo

$f_2: \frac{A}{\ker f} \longrightarrow B$

c) Hay un isomorfismo

$f_3: \frac{A}{\ker f} \longrightarrow Im(f)$

Pa.

a) f_1: $A \longrightarrow Im(f)$

$x \rightsquigarrow f(x)$

El homomorfismo así definido es sobreyectivo ya que el conjunto de llegada se ha reducido estrictamente a las imágenes de cada x tomado en A de tal manera que el conjunto de llegada es igual al rango de f.

En general, la anterior es una forma de construir una función sobreyectiva para cualquier f.

b) f_2: $\frac{A}{\ker f} \longrightarrow B$

$x + \ker f \longrightarrow f(x)$

Demostrar que el homomorfismo está bien definido.

Sean $x_1 + \ker f \in \frac{A}{\ker f}$ y $x_2 + \ker f \in \frac{A}{\ker f}$

$$x_1 + \ker f = x_2 + \ker f$$

$$\Rightarrow x_1 - x_2 \in \ker f$$

$$\Rightarrow f(x_1 - x_2) = 0$$

$$\Rightarrow f(x_1) - f(x_2) = 0$$

$$\Rightarrow f(x_1) = f(x_2$$

Luego, el homomorfismo está bien definido, además es biyectivo.

DEFINICION 3.3 Un isomorfismo es un homomorfismo biyectivo.

c) $f_3: \frac{A}{\ker f} \longrightarrow Im(f)$

$x + \ker f \rightsquigarrow f(x)$

Este homomorfismo está bien definido como se comprobó en el literal anterior.

Hay que garantizar solamente que el homomorfismo así definido es inyectivo o sea

si $f_3(x_1+\ker f) = f_3(x_2+\ker f) \Longrightarrow x_1+\ker f = x_2+\ker f$

Pa.

Si $f_3(x_1+\ker f) = f_3(x_2 + \ker f)$

$\Longrightarrow f_3(x_1+\ker f) - f_3(x_2+\ker f) = 0$

$\Longrightarrow f(x_1) - f(x_2) = 0$

$\Longrightarrow f(x_1 - x_2) = 0$

$\Longrightarrow x_1 - x_2 \ \varepsilon \ \ker f$

$\Longrightarrow x_1 + \ker f = x_2 + \ker f$

Luego por el literal a) se puede asegurar que el homomorfismo f_3 es sobreyectivo con lo que se concluye que f_3 es un isomorfismo.

PROPOSICION 3.2

"Si E, F, H son campos tales que F es extensión de E y H extensión de F entonces H es extensión de E".

Por hipótesis tenemos $E \subset F \subset H$ entonces basta probar que $E \subset H$.

Como $E \subset F \subset H$ para la prueba vamos a analizar cada una de las inclusiones que se dan y con qué operaciones se cumple cada una.

i) F extensión de E entonces E es subcampo de F con las operaciones de F ($E \subset F$).

ii) H extensión de F entonces F es subcampo de H con las operaciones de H ($F \subset H$).

Por lo tanto E es un subcampo de H con las mismas operaciones de H ($E \subset H$).

PROPOSICION 3.3

"Si K es una extensión de F entonces k es un F-espacio vectorial".

$F \subset K$ hipótesis

Para demostrar que k es un F-espacio vectorial hay que garantizar que:

a) K es un grupo abeliano.

b) Si para todo $\alpha \in F$, $w \in K$ está definido un elemento escrito como $\alpha w \in k$ tq.

1) $\alpha (w + \ell) = \alpha w + \alpha \ell$

2) $(\alpha + \beta)(\omega) = \alpha\omega + \beta\omega$

3) $\alpha(\beta \omega) = (\alpha \beta)\omega$

4) $1 . \omega = \omega$

$\alpha, \beta \in F$

$w, \ell \in k$

para la parte a) está garantizada, ya que k es un campo y en particular grupo abeliano.

En el literal b) las propiedades de 1) a 4) se satisfacen todas ya que todos los elementos pertenecen a k y éste es un campo.

PROPOSICION 3.4.

"Sea V un k-espacio vectorial de dimensión finita m y sea F un subcampo de k tal que [k: F] = n finita, probar que V es un F-espacio vectorial de dimensión finita y además $\dim_F V = \dim_k V \ [k:F]$"

$F \subset K \subset V$

$\dim_F V = \dim_k V \ [k:F]$

Sean $[V:K] = m$ y $[k:F] = n$ demostrar $\dim_F V = m.n$

Como $[V:k] = m$ entonces hay una base de v con m elementos.

además como $[k:F] = n$ hay una base con n elementos

Sean $\{x_1, x_2, x_3, \ldots, x_m\}$ una base de $V \subset V$ y

$\{y_1, y_2, \ldots, y_n\}$ una base de $k \subset K$

dado $x \in V$ entonces $x = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \ldots + \alpha_m x_m$

$\tilde{\alpha}_i \in k$ los α_i por pertenecer a k se pueden escribir de la siguiente manera:

$$\alpha_i = \beta_{i1} y_1 + \beta_{i2} y_2 + \beta_{i3} y_3 + \ldots + \beta_{in} y_n$$

Luego:

$$x = (\beta_{11} y_1 + \beta_{12} y_2 + \ldots + \beta_{1n} y_n) x_1 +$$

$$(\beta_{21} y_1 + \beta_{22} y_2 + \ldots + \beta_{2n} y_n) x_2 +$$

$$\ldots\ldots\ldots + (\beta_{m1} y_1 + \ldots + \beta_{mn} y_n) x_m$$

$$\Longrightarrow x = \beta_{11} y_1 x_1 + \beta_{12} y_2 x_1 + \ldots + \beta_{1n} y_n x_1 + \beta_{21} y_1 x_2 +$$

$$\beta_{22} y_2 x_2 + \ldots + \beta_{2n} y_n x_2 + \ldots + \beta_{m1} y_1 x_m +$$

$$\beta_{m2} y_2 x_m + \ldots + \beta_{mn} y_n x_m$$

La base deseada es:

$$\{y_1x_1,\ y_2x_2,\ldots,y_1x_m,\ y_2x_1,\ y_2x_2,\ldots y_2x_m,\ldots,y_nx_1,\ldots,y_nx_m\}$$

para probar que son linealmente independientes

$$\text{Si} \quad \sum_{i=j=1}^{nm} \beta_{ij} y_i x_j = 0 \overset{?}{\Longrightarrow} \beta_{ij} = 0$$

La sumatoria anterior se puede escribir de la siguiente forma:

$$\sum_{j=1}^{m}\Big(\sum_{i=1}^{n} \beta_{ij}\, y_i\Big)\, x_j = 0 \Longrightarrow \sum_{i=1}^{n} \beta_{ij}\, y_i$$

$$\Longrightarrow \beta_{ij} = 0 \quad \forall \quad i = 1,2\ldots n$$

$$j = 1,2\ldots m$$

con lo anterior se ha demostrado que V es un F-espacio vectorial de dimensión finita y además

$$\dim_f V = \dim_k V\ [k:F]$$

PROPOSICION 3.5

"Sean F, K, L campos tales que K es una extensión finita de F y L extensión finita de K. Entonces:

a) L es extensión finita de F

b) [L:F] = [L:K] [K:F]

La idea de plantear y resolver la proposición 3.4 es poder utilizarla para campos que satisfacen las condiciones de esta propiedad, de tal manera que revisamos la demostración anterior y se observa que es suficiente identificar que se puede hacer la sustitución V=L y la demostración se repite paso a paso haciendo dicho cambio en donde aparezca V. En resumen esta propiedad es una consecuencia de la proposición 3.4

PROPOSICION 3.6.

"Sean F,K,L campos tales que K es una extensión de F y L extensión de K. Si L es extensión finita de F entonces K es extensión finita de F y L extensión finita de K".

Hipótesis $F \subset K \subset L$

Si L extensión finita de F probaremos que K es extensión finita de F.

L es un F-espacio vectorial de dimensión n.

Sean $x_1, x_2, \ldots, x_m$ vectores Li en k como F-espacio vectorial, los vectores $x_1, x_2, x_3, \ldots x_m$ son vectores Li en L como F-espacio vectorial, porque $K \subset L$.

En un espacio de dimensión n un conjunto L.i(linealmente

independiente) no puede tener más elementos que la dimensión del espacio, ésto implica que $m < n$.
Por lo tanto cualquier base de k como F-espacio vectorial no tiene más de n elementos o sea que

$$\dim_F K \leq n \quad \text{finita}$$

Si L es extensión finita de F a probar que L es extensión finita de k.

L es un F-espacio vectorial de dimensión n.

Sean $x_1, x_2, \ldots, x_r$ vectores linealmente independientes en L como K-espacio vectorial.

A probar que $x_1, x_2, \ldots, x_r$ son vectores linealmente independientes en L como F-espacio vectorial.

Sean $\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_r \in F$ y sea

$\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \ldots \alpha_r x_r = 0$ una combinación lineal nula de los vectores $x_1, x_2, \ldots, x_r$

A probar que $\alpha_1 = \alpha_2 = \alpha_3 = \ldots = \alpha_r = 0$

Por hipótesis de que $x_1, x_2, \ldots, x_r$ son vectores linealmente independientes en L como k espacio vectorial y además $F \subset K$ entonces $\alpha_1 = \alpha_2 = \alpha_3 = \ldots = \alpha_r = 0$ con -

lo que se concluye que $x_1, x_2, \ldots, x_r$ son L.i. en L como F espacio vectorial, pero lo anterior obliga a que $r \leq n$ por el mismo criterio utilizado en la parte anterior, de tal manera que

$$\dim_K^L = r \quad \text{finita}$$

con lo que se concluye la prueba.

DEFINICION 3.4

Un número es primo si y solo si es divisible solamente por él mismo y por la unidad.

PROPOSICION 3.7

Sean F,K,L campos tales que K es extensión de F y L es extensión de K. Si [L:F] es un número primo entonces K=F ó K=L.

Pa.

Usaremos en el desarrollo de la prueba el hecho de que [L:F] = [L:K][K:F] que ya fue probado en la proposición 3.5 en su parte b)

a) Si [L:F] es un número primo, sea n tal número primo

$\Rightarrow$ n = n.1

$\Rightarrow$ n = [L:K][K:F] = n-1

$\Rightarrow$ K = F

ó $n = 1.n$ entonces $n = [L:K][K:F] = 1.n$

luego $K=L$

con lo que la prueba queda completa.

PROPOSICION 3.8

Sean F_o, F_1, F_2,.....,F_n campos tales que para todo $i \geq 1$ Fi es una extensión finita de Fi-1. Entonces:

a) Fn es extensión finita de Fo

b) $[Fn:F_o] = [F_1:F_o][F_2:F_1]....[F_n:F_{n-1}]$.

Esta proposición es una generalización de la proposición 3.5, en donde se probó para n=2 y se obtuvo lo siguiente:

a) F_2 es extensión finita de F_o.

b) $[F_2:F_o] = [F_1:F_o][F_2:F_1]$.

Lo que haremos en éste caso es extender la prueba para - cualquier n; lo haremos por inducción sobre n.

Para n=1 se cumple que $[F_1:F_o] = [F_1:F_o]$.

Supongamos que se satisface para n=k entonces tenemos

$[F_k:F_o] = [F_1:F_o][F_2:F_1]....[F_k:F_{k-1}]$

probemos que se cumple para n= k+1

A probar que $[F_{k+1}: F_o] = [F_1:F_o][F_2:F_1][F_3:F_2]....[F_{k+1}:F_k]$

por hipótesis inductiva tenemos:

$$[F_k:F_o] = [F_o:F_1][F_1:F_2][F_3:F_2].....[F_k:F_{k-1}]$$

$$[F_k:F_o][F_{k+1}:F_k] = [F_1:F_o][F_2:F_1].....[F_k:F_{k-1}][F_{k+1}:F_k]$$

$$= [F_{k+1}:F_o] = [F_1:F_o][F_2:F_1][F_3:F_2]....[F_k:F_{k-1}][F_{k+1}:F_k]$$

con lo que se concluye la prueba.

PROPOSICION 3.9

"Si $f:E \longrightarrow F$ es un isomorfismo de anillos y E es un campo entonces F es un campo".

En un isomorfismo se cumplen las siguientes propiedades

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

$$f(1) = 1; \qquad f(e) = e$$

$$f(x)^{-1} = (f(x))^{-1}$$

Demostración

Por ser f sobreyectiva. Imf = F queremos demostrar que F es un campo.

Sea $x \in F$, $x \neq 0$, probar que existe $x^{-1} \in F$ tq $x.x^{-1} = e$

Por ser sobreyectiva f, para $x \in F$ existe $y \neq 0 \in E$ tal que $f(y) = x$, para $y \in E$ existe y^{-1} tal que $yy^{-1} = e$ porque E es un campo.

Aplicando f a ambos lados de $yy^{-1} = e$ tenemos:

$\Rightarrow f(yy^{-1}) = f(e)$

$\Rightarrow f(yy^{-1}) = e$

$\Rightarrow f(y).f(y^{-1}) = e$

$\Rightarrow x.\ (f(y))^{-1} = e$

$x.x^{-1} = e$

Luego F es un campo.

NOTA: Para la prueba de que F es un campo solamente se ha probado la existencia del inverso multiplicativo y es de notar que las otras condiciones de campo, las satisface F por ser un anillo.

DEFINICION 3.5

F(a) es el mínimo subcampo de k que contiene tanto a F como al elemento a. Llamaremos a F(a) el subcampo obtenido por adjunción del elemento a al campo F.

PROPOSICION 3.10

Sea k una extensión de F y sea $a \in K$.

Existe un subcampo único L de K con las dos propiedades siguientes:

1) $a \in L$ y $F \subset L$

2) Si T es un subcampo de k tal que $a \in T$ y $F \subset T$ entonces $L \subset T$

hipótesis $F \subset k$, $a \in k$

Sea $M = (Mi)i \in I$ la colección de todos los subcampos de k que contienen tanto a F como al elemento a.

$M \neq \emptyset$, ya que $k \in M$.

Se sabe que la intersección de cualquier familia de subcampos de un campo en particular k es también un subcampo de k.

Sea $L = \bigcap_{i \in I} Mi$, $(Mi)_{i \in I}$ definido como colección de subcampos de k que contienen a F como al elemento a.

1) $a \in L$ ya que $a \in Mi$; $\forall\, i \in I$

   $F \subset L$ ya que cada M contiene a F.

2) Si $T \subset K$ tal que $a \in T$ y $F \subset T$ entonces $L \subset T$

   $L \subset T$ ya que $\bigcap_{i \in I} Mi \subset T$

UNICIDAD

Sea L subcampo de k con las propiedades siguientes:

1) $a \in L$ y $F \subset L$

2) Si T es un subcampo de k tal que $a \in T$ y $F \subset T$ entonces $L \subset T$.

Tomemos además a w como otro subcampo de k que también cumple las condiciones (1) y (2) de L o sea

(1) $a \in w$ y $F \subset w$

(2) Si T es un subcampo de k tq $a \in T$ y $F \subset T$ entonces $w \subset T$

Vamos a probar que w=L para lo cual hay que garantizar que $w \subset L$ y $L \subset w$.

Por una parte para L tenemos $a \in L$ y $F \subset L$ por otro lado por (2) de w tenemos que si T es un subcampo de K tq $a \in T$ y $F \subset T$ entonces $w \subset T$. Se concluye bajo estas condiciones L es uno de los T de la propiedad (2) para w. Por tanto $w \subset L$.

Por otra parte tenemos utilizando (1) de w y (2) para L tenemos $a \in w$ y $F \subset w$ además si T subcampo de k tq $a \in T$ y $F \subset T$ entonces $L \subset T$.

Luego w es uno de los T por lo tanto $L \subset w$

con lo anterior se ha probado que L = w

por lo tanto L es único.

PROPOSICION 3.11

"Sea k una extensión de F y sean $a_1, a_2, a_3, \ldots a_n$ elementos de k. Existe un subcampo único L de k con las propiedades siguientes:

1) $a_1, a_2, \ldots a_n$ son elementos de L y $F \subset L$.
2) Si T es un subcampo de k tal que $a_1, a_2, \ldots a_n$ son elementos de T y $F \subset T$ entonces $L \subset T$

(Este subcampo único se denota por $F(a_1, a_2, \ldots, a_n)$

1) $L = \bigcap_{i \in I} Mi$ intersección de todos los subcampos de k que contienen tanto a F como a los elementos $a_1, a_2, \ldots, a_n$.

Para cada a_i, $a_i \in k$, $a_1, a_2, \ldots a_n \in Mi$ para cada i

$\Rightarrow a_1, a_2, a_3 \ldots a_n \in L$

del mismo modo como cada Mi contiene a F entonces $F \subset L$.

2) T es subcampo de k que contiene tanto a los elementos $a_1, a_2, \ldots a_n$ como a F entonces $T \in (Mi)i \in I$

Luego $L \subset T$.

Al subcampo así construido L de K se denota por $F(a_1, a_2, a_3 \ldots\ldots, a_n)$.

Unicidad

Para garantizar la unicidad en esta propiedad que es una generalización de la proposición 3.10 hay que suponer que existe otro subcampo de k que también satisface las condiciones dadas.

Por una parte tenemos el subcampo L con las propiedades

1.- $a_1, a_2, a_3, \ldots, a_n$ son elementos de L y $F \subset L$.

2.- Si T es un subcampo de k tal que $a_1, a_2, a_3, \ldots a_n$ son elementos de T y $F \subset T$ entonces $L \subset T$

Por otro lado sea w subcampo de k tal que:

1) $a_1, a_2, a_3, \ldots, a_n$ son elementos de w y $F \subset w$

2) Si T es subcampo de k tal que $a_1, a_2, a_3, \ldots, a_n$ pertenecen a T y $F \subset T$ entonces $w \subset T$.

A probar que w = L.

Esta es una generalización de la proposición y se hará un análisis similar para su comprobación.

En primer lugar tenemos

$a_1, a_2, a_2, \ldots, a_n$ elementos de L y $F \subset L$

por otra parte para T subcampo de k tal que

$a_1, a_2, \ldots, a_n$ son elementos de T y $F \subset T$ entonces L = T y $w \subset L$.

En segundo lugar tenemos:

$a_1, a_2, a_3, \ldots, a_n$ elementos de w y $F \subset w$ y para T subcampo de k tal que $a_1, a_2, \ldots, a_n$ son elementos de T y $F \subset T$ entonces w = T y $L \subset w$

Por tanto w = L

de lo anterior se concluye que L es único.

PROPOSICION 3.12

"Sean k una extensión de F y a,b $\in$ K.

Entonces:

$F(a,b) = F(b)(a) = F(a)(b) = F(b,a)$

Solamente probaremos

$F(a,b) = F(a)(b)$ y $F(a,b) = F(b)(a)$

"$F(a,b) \subset F(a)(b)$"

$b \in F(a)(b)$ (por definición de $F(a)(b)$)

$F(a) \subset F(a)(b)$ (por definición de $F(a)(b)$

$a \in F(a)$

$F \subset F(a)$

Con lo anterior se tiene que:

$a,b \in F(a)(b)$

$F \subset F(a)(b)$

por lo tanto $F(a,b) \subset F(a)(b)$

"$F(a)(b) \subset F(a,b)$"

bastará probar que $b \in F(a,b)$ y $F(a) \subset F(a,b)$

$b \in F(a,b)$ por definición de $F(a,b)$

$F \subset F(a,b)$ y $a \in F(a,b)$ por definición de $F(a,b)$

por lo tanto $F(a) \subset F(a,b)$.

Luego $F(a)(b) \subset F(a,b)$ y al final se concluye que

$F(a,b) = F(a)(b)$

** $F(a,b) = F(b)(a)$

"$F(a,b) \subset F(b)(a)$"

hay que probar que $a,b \in F(b)(a)$

$a \in F(b)$ por definición de $F(b)(a)$

$F(b) \subset F(b)(a)$

$b \in F(b)$ por definición de $F(b)$

$F \subset F(b)$

entonces $a,b \in F(b)(a)$

$F \subset F(b)(a)$

por lo tanto $F(a,b) \subset F(b)(a)$

"$F(b)(a) \subset F(a,b)$"

A mostrar que $a \in F(a,b)$ y $F(b) \subset F(a,b)$

$a \in F(a,b)$ por definición de $F(a,b)$

$F \subset F(a,b)$ y $b \in F(a,b)$ por definición de $F(a,b)$

entonces $F(b) \subset F(a,b)$

Luego $F(b)(a) \subset F(a,b)$

por lo tanto se concluye que:

$$F(a,b) = F(b)(a)$$

NOTA: Las otras igualdades de esta propiedad se demuestra en forma similar utilizando las mismas definiciones de $F(a)$, $F(b)$, $F(a,b)$, $F(b,a)$ y $F(a)(b)$

PROPOSICION 3.13

Si k es una extensión de F y $a \in k$, las condiciones que se presentan a continuación son equivalentes.

1.- Para cierto $n \in \mathbb{N}$, $n > 0$, existen $\lambda_0, \lambda_1, \lambda_2 \cdots \lambda_n$ no todos nulos en F tales que

$$\lambda_o + \lambda_1 a + \lambda_2 a^2 + \lambda_3 a^3 + \ldots + \lambda_n a^n = 0$$

2.- Existe $p(x) \in F[x]$ de grado $m > 0$ tq $p(a) = 0$

Pa.

"1 $\Longrightarrow$ 2"

Supongamos que para $n \in \mathbb{N}$, $n > 0$ existen $\lambda_o, \lambda_1, \ldots, \lambda_n$ no todos nulos tales que:

$\lambda_o + \lambda_1 a + \lambda_2 a^2 + \lambda_3 a^3 + \ldots + \lambda_n a^n = 0$ y probemos que existe $p(x) \in F[x]$ de grado $m > 0$ tq $p(a) = 0$

Sea $p(x) = \lambda_o + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n$

entonces $p(a) = \lambda_o + \lambda_1 a + \lambda_2 a^2 + \ldots + \lambda_n a^n = 0$

Si el grado de p(x) fuera cero

$p(x) = \lambda_o$; $\lambda_1 = \lambda_2 = \lambda_3 = \ldots = \lambda_n = 0$

entonces: $p(a) = \lambda_o$

$\Rightarrow \lambda_o = 0$

$\Rightarrow \lambda_i = 0, \forall\ i = 0, 1, 2, 3, \ldots, n$

Pero la última implicación es una contradicción ya que por nuestra hipótesis los $\lambda_o, \lambda_1, \lambda_2, \ldots, \lambda_n$ no todos son nulos, por lo tanto, el grado de p(x) no puede ser cero de aquí que grado de p(x) > 0

"2 $\Longrightarrow$ 1"

Supongamos que existe p(x) de grado m > 0 con p(x) ε [x] tq p(a) = 0 a probar que para cierto n ε N, n > 0, existen $\lambda_o, \lambda_1, \lambda_2, \ldots, \lambda_n$ no todos nulos en F tales que

$$\lambda_o + \lambda_a + \lambda_2 a^2 + \ldots + \lambda_n a^n = 0$$

Sea $p(x) = \alpha_o + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \ldots + \alpha_m x^m$

tal que $p(a) = \alpha_o + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 + \ldots + \alpha_m a^m = 0$

Si $\alpha_i = 0$ para i = 0,1,2,3,...,m

entonces grado de p(x) es cero, pero esto es una contradicción ya que p(x) tiene grado m > 0 por hipótesis.

Por la contradicción anterior puede concluirse que no todos los escalares son nulos.

Con lo que se concluye la prueba.

NOTA Al elemento a ε k se le llama elemento algebraico sobre F cuando satisface estas condiciones equivalentes.

PROPOSICION 3.14.

"Sea k una extensión de F y aε k. El conjunto
$L = \{ q(x) \varepsilon P[x]/q(a) = 0 \}$ es un ideal de F[x]."

hipótesis $F \subset k$; $a \varepsilon k$; F,k campos.

L será un ideal de F[x] si satisface las siguientes condiciones:

(1) L es un subgrupo de F[x] bajo la suma

(2) Para todo $q(x) \varepsilon L$ y $p(x) \varepsilon F[x]$ tanto $q(x)\,p(x)$ como $p(x)\,q(x) \varepsilon L$.

Pa.

(1) i) $L \neq \emptyset$ ya que $q(x) = 0 \varepsilon L$

ii) Sean $p(x), q(x) \varepsilon L$ probar que $p(x) + q(x) \varepsilon L$

Sean $p(x) = \alpha_o + \alpha_1 x^1 + \alpha_2 x^2 + \ldots + \alpha_n x^n$

$q(x) = \beta_o + \beta_1 x^1 + \beta_2 x^2 + \ldots + \beta_n x^n$

$p(x)+q(x) = (\alpha_o + \alpha_1 x^1 + \alpha_2 x^2 + \ldots + \alpha_n x^n) +$

$(\beta_o + \beta_1 x + \ldots + \beta_n x^n)$

$= \alpha_o + \beta_o + (\alpha_1 + \beta_1)x + (\alpha_2 + \beta_2)x^2 +$

$\ldots\ldots + (\alpha_n + \beta_n)x^n$

$$p(x)+q(x) = \sum_{i=0}^{n} (\alpha_i + \beta_i)x^i$$

$$p(a) + q(a) = \sum_{i=0}^{n} (\alpha_i + \beta_i)a^i = \sum_{i=0}^{n} (\alpha_i a^i + \beta_i a^i)$$

$$= \sum_{i=0}^{n} \alpha_i a^i + \sum_{i=0}^{n} \beta_i a^i = p(a) + q(a) = 0$$

entonces $p(x) + q(x) \in L$

con lo anterior se tiene que L es un subgrupo bajo la suma.

(2) Sea $q(x) \in L$, $p(x) \in F[x]$

$q(x) \in L \Longrightarrow q(x) \in F[x]$ t.q $q(a) = 0$

Si $q(x) = \alpha_o + \alpha_1 x + \alpha_2 x + \ldots + \alpha_n x^n = 0$

$q(a) = \alpha_o + \alpha_1 a + \alpha_2 a + \ldots + \alpha_n a^n = 0$

además $p(x) = \alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_m x^m$

queremos probar que para $q(x) \in L$ y $p(x) \in F[x]$ el producto $p(x)\,q(x) \in L$.

$$p(x) = \sum_{i=0}^{n} \beta_i x^i, \qquad q(x) = \sum_{j=0}^{m} \alpha_j x^j$$

$q(x) \in L$ tal que $q(a) = 0$

$$p(x)q(x) = t(x) = \left(\sum_{i=1}^{n} \beta_i x^i\right) \left(\sum_{j=1}^{m} \alpha_j x^j\right) = t(x) = \sum_{t=0}^{n} c_t x^t$$

donde $C_t = \alpha_t \beta_o + \alpha_{t-1}\beta_1 + \alpha_{t-2}\beta_2 + \ldots + \alpha_o \beta_t$

$$t(x) = (\beta_o + \beta_1 x + \beta_2 x^2 + \ldots + \beta_n x^n)(\alpha_o + \alpha_1 x + \ldots + \alpha_m x^m)$$

$$t(a) = (\beta_o + \beta_1 a + \beta_2 a^2 + \ldots + \beta_n a^n)(\alpha_o + \alpha_1 a + \ldots + \alpha_m a^m)$$

$$t(a) = p(a)\, q(a)$$

$$= (\beta_o + \beta_1 a + \beta_2 a^2 + \ldots + \beta_n a^n).q(a)$$

$$= (\beta_o + \beta_1 a + \beta_2 a^2 + \ldots + \beta_n a^n).\ 0$$

$$t(a) = 0 \implies t(x) \in L \implies p(x)q(x) \in L$$

$$q(x)p(x) = t(x) = (\alpha_o + \alpha_1 x + \ldots + \alpha_m x^m)(\beta_o + \beta_1 x + \ldots + \beta_n x^n)$$

$$t(a) = (\alpha_o + \alpha_1 x + \ldots + \alpha_m a^m)(\beta_o + \beta_1 a + \ldots + \beta_n a^n)$$

$$= q(a)\, p(a)$$

$$= 0(\beta_o + \beta_1 a + \ldots + \beta_n a^n)$$

$$t(a) = 0 \Rightarrow t(x) \in L$$

$$\Rightarrow q(x)p(x) \in L$$

por lo tanto L es un ideal.

PROPOSICION 3.15

"Sea k una extensión de F y $a \in k$. La función

$\Phi : F[x] \longrightarrow F(a)$

$p(x) \rightsquigarrow p(a)$ es un homomorfismo de anillos"

A probar que para $p(x), q(x) \in F[x]$ se cumple que:

i) $\Phi(p(x) + q(x)) = \Phi(p(x) + \Phi(q(x))$

ii) $\Phi(p(x).q(x) = \Phi(p(x). \Phi q(x))$

Sean $p(x) = \sum \alpha_i x^i$

$q(x) = \sum \beta_i x^i$

$$\Phi(p(x) + q(x)) = \Phi(\alpha_i x^i + \beta_i x^i)$$

$$= \Phi((\alpha_i + \beta_i)x^i)$$

$$= \sum (\alpha_i + \beta_i)a^i = \sum (\alpha_i a^i + \beta_i a^i)$$

$$= \sum \alpha_i a^i + \sum \beta_i a^i$$

$$= \Phi(p(x)) + \Phi(p(x))$$

$$\Phi(p(x)q(x)) = \Phi\left(\sum_{i=0}^{n} \alpha_i x^i \sum_{i=0}^{m} \beta_i x^i\right)$$

$$= \Phi\left(\sum_{t=0}^{k} ctx^t\right)$$

donde:

$$Ct = \alpha_t \beta_o + \alpha_{t-1} \beta_1 + \alpha_{t-2} \beta_2 + \ldots + \alpha_o \beta_t$$

$$= \Phi\left(\sum_{t=0}^{k} C_t x^t\right)$$

$$= \sum_{t=0}^{k} Cta^t$$

$$= \sum \alpha_i a^i \cdot \sum \beta_i a^i$$

$$= \Phi(p(x) \cdot \Phi(q(x))$$

luego:

$$\Phi : F[x] \longrightarrow F(a)$$

$$p(x) \rightsquigarrow p(a)$$

es un homomorfismo de anillos.

PROPOSICION 3.16

"Sea k una extensión de F y a ε k.

a) El subconjunto L de k formado por los elementos de la forma xy^{-1} en donde $x = \sum_{i=0}^{m} \alpha_i a^i$ y $= \sum \beta_i a^i$ $\alpha_i \varepsilon F$, $y \neq 0$ es un subcampo de k $\beta_i \varepsilon F$

b) L = F(a)"

Pa.

$$L = \{ xy^{-1} / x = \sum_{i=0}^{m} \alpha_i a^i \quad y \; y = \sum \beta_i a^i, \quad \alpha_i \; \beta_i \varepsilon F$$

Demostrar que L es campo con las operaciones de k.

(1) Sea w ε L, w ≠ 0 probar que existe w^{-1} ε L tal que $w.w^{-1} = 1$

como $y \neq 0$ $\quad y^{-1} = \frac{1}{y} = \frac{1}{\sum_{i} \beta_i a^i}$

luego $w = xy^{-1} = \frac{x}{y} = \frac{\sum_{i=1}^{m} \alpha_i a^i}{\sum_{i} \beta_i a^i}$

$$w = xy^{-1} \Longrightarrow w^{-1} = (xy^{-1})^{-1} = \frac{y}{x}$$

$$\Longrightarrow w^{-1} = \frac{\sum_{i} \beta_i a^i}{\sum_{i=0}^{m} \alpha_i a^i} \qquad \alpha_i, \beta_i \in F$$

$$w.w^{-1} = \frac{\sum_{i=1}^{m} \alpha_i a^i}{\sum \beta_i a^i} \cdot \frac{\sum \beta_i a^i}{\sum \alpha_i a^i} = 1$$

$$\Longrightarrow w.w^{-1} = 1$$

(2) $L \neq 0$ ya que $0 = 0.y^{-1} \Longrightarrow 0 \in L$

$1 \in L$ ya que $1 = 1.1^{-1}$

(3) si $w_1, w_2 \in L$ probar que $w_1 + w_2 \in L$

$$\therefore \quad w_1 = \left(\sum_{i=0}^{m} \alpha_i a^i\right)\left(\sum \beta_i a^i\right)^{-1} \qquad \alpha_i, \alpha_i', \beta_i, \beta_i' \in F$$

$$w_2 = \left(\sum_{i=0}^{m} \alpha_i' a^i\right)\left(\sum \beta_i' a^i\right)^{-1}$$

$$w_1 = \frac{x}{y};\ w_2 = \frac{x_1}{y_1} \qquad w_1+w_2 = \frac{y_1x + yx_1}{yy_1}$$

$$w_1+w_2 = \frac{y_1x+yx_1}{yy_1} = \frac{\left(\sum \beta'_i a^i\right)\left(\sum \alpha_i a^i\right) \quad \left(\sum \beta_i a^i\right)\left(\sum \alpha'_i a^i\right)}{\left(\sum \beta_i a^i\right)\left(\sum \beta'_i a^i\right)}$$

$$= \frac{\sum_{\substack{i<m \\ j<n}} (\alpha_i a^i\ \beta'_j a^j) + \sum_{\substack{i<m \\ j<n}} (\alpha'_i a^i\ \beta_j a^j)}{\sum_{\substack{i<m \\ j<n}} (\beta_i a^i\ \beta'_j a^j)}$$

$$= \frac{\sum_{\substack{i<m \\ j<n}} (\alpha_i\ \beta'_j a^i a^j + \alpha'_i\ \beta_j a^i a^j)}{\sum_{\substack{i<m \\ j<n}} (\beta_i\ \beta'_j\ a^{i+j})}$$

$$w_1 + w_2 = \frac{\sum_{\substack{i<m \\ j<n}} (\gamma_{i,j} a^{i+j} + \gamma'_{i,j} a^{i+j})}{\sum_{\substack{i<m \\ j<n}} (\gamma_{i,j} a^{i+j})}$$

$$\Rightarrow w_1 + w_2 \in L$$

Para el producto hay que darse $w_1, w_2 \in L$ y probar que $w_1 \cdot w_2 \in L$

$$\frac{\sum_{o}^{m} \alpha_i a^i}{\sum_{o}^{n} \beta_i a^i} \cdot \frac{\sum_{o}^{m} \alpha'_i a^i}{\sum_{o}^{n} \beta'_i a^i} = \frac{\sum_{o}^{m} \alpha_i a^i \sum_{o}^{n} \alpha'_i a^i}{\sum_{o}^{n} \beta_i a^i \sum_{o}^{n} \beta'_i a^i} = \frac{\sum_{\substack{i<m \\ j<n}} (\alpha_i a^i)(\alpha'_j a^j)}{\sum (\beta_i a^i)(\beta'_j a^j)}$$

$$= \frac{\sum_{\substack{i<m \\ j<n}} (\alpha_i \alpha'_j) a^i a^j}{\sum_{\substack{i<m \\ j<n}} (\beta_i \beta'_j) a^i a^j} = \frac{\sum_{\substack{i<m \\ j<n}} \gamma_{i,j} a^{i+j}}{\sum_{\substack{i<m \\ j<n}} \lambda_{i,j} a^{i+j}}$$

$$\Rightarrow w_1 \cdot w_2 \in L .$$

con lo anterior se ha probado que el subconjunto L de k formado por los elementos de la forma xy^{-1} en donde $x = \sum_{i=0}^{m} \alpha_i a^i$ y $y = \sum \beta_i a^i$, $\alpha_i, \beta_i \in F$, $y \neq 0$ es un subcampo de k.

b) Probar que L = F(a)

(1) Sea $x \in F$;

$x \quad F \subset F(a)$

pero $x = \dfrac{\sum_{i=0}^{m} \alpha_i a^i}{\sum_{i=0}^{n} \beta_i a^i}$; $\alpha_i=0$; $i=1,2,3,.....m$ $\quad \alpha_o=x$

$\beta_i=0$ $\quad i=1,2,3,.....n$ $\quad \beta_o=1$

ya que $\dfrac{\sum_{o}^{m} \alpha_i a^i}{\sum \beta_i a^i} = \dfrac{\alpha_o a^o+\alpha_q a^1+\ldots+\alpha_m a^m}{\beta_o a^o+\beta_1 a^1+\ldots+\beta_n a^n} = \dfrac{\alpha_o a^o}{\beta_o a^o} = \dfrac{\alpha_o}{\beta_o} = \dfrac{x}{1} = x$

luego $x \in L$, de donde $F \subset L$

(2) $a \in L$ ya que $a = \dfrac{\sum_{i=0}^{m} \alpha_i a^i}{\sum_{i=0}^{n} \beta_i a^i}$ haciendo $\alpha_o = 0$, $\alpha_1 = 1$,

$\alpha_i = 0$ para $i=1,2,3....m$

$\beta_o = 1$; $\beta_i=0$, $i=1,2,3....n$

(3) $T \subset K$ subcampo tal que $a \in T$ y $F \subset T$ a probar que

$L \subset T$

$x \in L \Longrightarrow x = \dfrac{\sum_{i=0}^{m} \alpha_i a^i}{\sum_{i=0}^{n} \beta_i a^i}$ $\alpha_i, \beta_i \in F$ como además

$F \subset T$, $\alpha_i \beta_i \in T, \forall\ i$

además $a \in T$ entonces $a^i \in T$, $\forall\ i$ (T es subcampo)

de aquí que $\sum_{i=0}^{m} \alpha_i a^i \in T$ y $\sum_{i=0}^{n} \beta_i a^i \in T$ de donde se tiene

que $x \in T$, es decir $L \subset T$

por (1), (2) y (3) se concluye que $F(a) = L$.

DEFINICION 3.6

Un polinomio p(x) se dice que es irreducible

si: 1) p(x) no es constante

2) $p(x) = q(x)\ t(x)$

$\Longrightarrow$ q(x) es constante o t(x) es constante.

PROPOSICION 3.17

Si F es un campo y si $p(x) \in F[x]$.

El ideal generado por p(x) es máximal si y solo si

p(x) es irreducible.

Pa. " $\Longrightarrow$ " Sea $I \subset F[x]$ un ideal maximal y sea $p(x) \in$

$[x]$ tal que $I = [p(x)]$ probar que p(x) es irreducible.

Sea $p(x) = q(x)t(x)$, $p(x) \in [q(x)]$, ya que es múltiplo,

entonces $[p(x)] \subset [q(x)]$, por ser $I = [p(x)]$ maximal

entonces $[q(x)] = I$ ó $[q(x)] = F[x]$

i) Si $[q(x)] = [p(x)]$; $q(x) = s(x)\ p(x)$

grado de $p(x)$ = grado $q(x)$ entonces $t(x)$ es constante

ii) Si $[q(x)] = F[x]$; $1 \in [q(x)]$

$1 = q(x)\ s(x) \Longrightarrow q(x)$ es constante

de i) y ii) tenemos que $p(x)$ es irreducible.

" $\Longleftarrow$ " F es un campo, $p(x) \in F[x]$ un polinomio probar que el ideal generado por $p(x)$ es maximal si $p(x)$ es irreducible.

Sea $T = [p(x)]$ entonces i) $T \neq \emptyset$, T es un ideal

ii) $p(x) \in T$

iii) Si L es un ideal tal que $p(x) \in L$ entonces $T \subset L$.

Sea I un ideal tal que $T \subset I$ probemos que $T = I$ ó $I = F[x]$

Supongamos que $T \neq I$ y probemos que $I = F[x]$

Veamos que $1 \in F[x]$, $1 \in 1$, como $I \neq T$ entonces existe $q(x) \in I \wedge q(x) \notin T$, además como $I = [R(x)]$ entonces $q(x) = s(x)R(x)$ como $T \subset I \Longrightarrow p(x) \in I$, ya que $T = [p(x)]$ y $T \subset I$. Si $p(x) \in I$, $p(x) \in [R(x)]$ entonces $p(x) = t(x)R(x)$

ya que p(x) es irreducible, luego t(x) o R(x) son constantes

(1) Si $t(x) = k$, $p(x) = kR(x)$

$$\Rightarrow q(x) = s(x)\left(\frac{p(x)}{k}\right) = \frac{1}{k}\ s(x)\ R(x)$$

$$\Rightarrow q(x) \in [p(x)]$$

la anterior es una contradicción, ya que

$$q(x) = s(x)\ R(x)$$

$$\Rightarrow q(x) \in [R(x)].$$

(2) Si $R(x) = k$

$1 = k.k^{-1}$ como $k \in I \wedge k^{-1} \in F[x]$

entonces $kk^{-1} \in I$

$$\therefore\ 1 \in I$$

con lo que se concluye que el ideal generado por p(x) es maximal.

DEFINICION 3.7

Se dice que un polinomio p(x) es mónico si el coeficiente de su máxima potencia es igual a uno.

DEFINICION 3.8

Un elemento $a \in K$ donde K es un campo se dice que es alge-

braico sobre F si existen elementos $\alpha_o, \alpha_1, \ldots, \alpha_n$ en F. no todos 0, tales que:

$$\alpha_o a^n + \alpha_1 a^{n-1} + \ldots \alpha_n = 0$$

DEFINICION 3.9

Ideal máximo; un ideal $M \neq A$, A es un anillo, se dice que M es un ideal máximo de A si siempre que U es un ideal de A tal que $M \subset U \subset A$ se tiene que $A = U$ ó $M = U$

PROPOSICION 3.18

Sea k una extensión de F y $a \in k$ un elemento algebraico sobre F. Entonces:

(1) "Todo polinomio $q(x) \in F[x]$ de grado mínimo $m > 0$ tal que $q(a) = 0$ es un polinomio irreducible".

Pa.

Sea $q(x) \in F[x]$ de grado mínimo $m > 0$ tal que $q(a) = 0$ a probar que q(x) es irreducible.

Si $q(x) = p(x)\, T(x)$

$q(a) = p(a)\, T(a) = 0$

$\Longrightarrow p(a) = 0$ ó $T(a) = 0$

además grado $(p(x)) \leq$ grado $(q(x))$

grado $(T(x)) \leq$ grado $(q(x))$

Si p(a) = 0 entonces grado (p(x)) = 0 o grado (p(x))= grado (q(x))

$\Rightarrow$ p = c; donde c es una constante.

Si T(a) = 0 entonces grado (T(x)) = 0

ó grado (T(x)) = grado (q(x))

T = c; donde c es una constante.

Luego p = c ó T = c entonces q(x) es irreducible.

(2) "Existe un único polinomio mínico p(x) ε F[x] de grado m > 0 minimo tal que p(a) = 0 (Este polinomio único es llamado polinomio mínimo de a)."

Sean r, t dos polinomios mónicos de grado mínimo tales que r(a) = t(a) = 0 probemos que r = t

$r(x) = \alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots + x^m$

$t(x) = \beta_o + \beta_1 x + \beta_2 x^2 + \ldots\ldots + x^m$

haciendo s(x) = r(x) - t(x)

$$S(x) = (\alpha_o - \beta_o) + (\alpha_1 - \beta_1)x + (\alpha_2 - \beta_2)x^2 + \ldots + (\alpha_{m-1} - \beta_{m-1})x^{m-1}$$

$$\Rightarrow s(a) = (\alpha_o - \beta_o) + (\alpha_1 - \beta_1)a + (\alpha_2 - \beta_2)a^2 + \ldots + (\alpha_{m-1} - \beta_{m-1})a^{m-1}$$

como grado (s(x)) $\leq$ m-1

$\Rightarrow$ grado (s(x) = 0

entonces $s(x) = r(x) - t(x) = c$

$\Rightarrow r(x) - t(x) = c$

$\Rightarrow \alpha_i = \beta_i$ para $i \geq 1$

de $r(x) - t(x) = c$

$r(a) - t(a) = c$

$0 - 0 = c$

$\Rightarrow c = 0$

$\Rightarrow \alpha_o - \beta_o = 0 \Rightarrow \alpha_o = \beta_o$

con lo que se concluye que $r(x) = t(x)$ por lo tanto $p(x)$ es único.

3). El polinomio mínimo de a es un generador del ideal de $F[x]$.

$$L = \{q(x) \in F[x] / q(a) = 0\}$$

Sea $L = \{q(x) \in F[x]/q(a) = 0\}$ un ideal de $F[x]$ probar que L es un generado por el polinomio mínimo de a.

- Por la proposición 3.17 "Si F es un campo y si $p(x)$ pertenece a $F[x]$. El ideal generado por $p(x)$ es maximal si y solo si $p(x)$ es irreducible."

Además todo polinomio mínimo $p(x)$ es irreducible probado en (1) de ésta proposición, entonces el ideal generado por $p(x)$ es maximal, por definición de polinomio mínimo de a, $p(x) \in F[x]$ tal que $p(a) = 0$ entonces $p(x) \in L$, el ideal gene-

rado por p(x), $[p(x)] \subset L$

Luego $[p(x)] \subset L \subset F[x]$, por definición de ideal maximal se tiene que $L = [p(x)]$ ó $L = F[x]$.

$L \neq F[x]$ ya que existen polinomios de los cuales a no es raíz (ejemplo $t(x) = 1+x$)

entonces $L = [p(x)]$ lo que prueba que L es generado por el polinomio mínimo.

4) "El núcleo del homomorfismo $\phi : F[x] \longrightarrow F(a)$

$q(x) \rightsquigarrow q(a)$

es un ideal maximal de F[x]."

Sea $p(x) \in F[x]$ el polinomio mínimo de a sobre F, p(x) es irreducible y aprobado en (1) de esta proposición

La función $\Phi : F[x] \longrightarrow F(a)$

$q(x) \rightsquigarrow q(a)$ es un morfismo de anillos.

Sea $V = \text{Ker}(\Phi)$ entonces $V = [p(x)]$ porque p(x) es el polinomio mínimo de $\underline{a}$ y p(x) es el generador del ideal,

$L = \{ q(x) \in F[x] / q(a) = 0 \}$

como p(x) es irreducible [p(x)] es maximal ya probado en la proposición 3.17.

$$\Phi_1 : \frac{F[x]}{\ker \Phi} \longrightarrow \text{Im } \Phi_1 \quad \text{es un isomorfismo}$$

$\ker \Phi = [p(x)]$ entonces $\ker \Phi$ es maximal, con lo que se concluye la prueba.

PROPOSICION 3.19

"F un campo, F[x] el anillo de polinomios en x sobre F, $p(x) \in F[x]$.

I = ideal de F[x] generado por p(x) donde grado de p(x) es n. probar que $\frac{F[x]}{I}$ es un F-espacio vectorial de dimensión n".

El camino para la prueba será encontrar una base que contenga n elementos.

Usaremos $B = \{ 1+I, x+I, x^2+I, \ldots\ldots, x^{n-1}+I \}$ y el propósito es mostrar que B es una base de $\frac{F[x]}{I}$.

a) B es linealmente independiente?

Sean $\alpha_o, \alpha_1, \alpha_2, \ldots\ldots, \alpha_{n-1}$ escalares en F tq .

$$\alpha_o(1+I)+ \alpha_1(x+I)+ \alpha_2(x^2+I)+\ldots\ldots+ \alpha_{n-1}(x^{n-1}+I) = 0 = I$$

de donde:

$$(\alpha_o+I)+(\alpha_1 x+I) + (\alpha_2 x^2+I)+\ldots\ldots+(\alpha_{n-1}x^{n-1}+I) = I$$

por tanto

$$(\alpha_o+\alpha_1 x+\alpha_2 x^2+\ldots\ldots+\alpha_{n-1}x^{n-1}) + I = I$$

de donde:

$$\alpha_o + \alpha_1 x + \alpha_2 x^2 +\ldots\ldots+ \alpha_{n-1}x^{n-1} \in I$$

pero como I es el generado por p(x) tenemos:

(1) $\alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots + \alpha_{n-1} x^{n-1} = \delta\, p(x)$

Sea $p(x) = \beta_o + \beta_1 x + \beta_2 x^2 + \ldots + \beta_n x^n$; $\beta_n \neq 0$

Luego (1) se puede escribir como

$$\alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1} =$$

$$\delta(\beta_o) + (\delta\beta_1)x_1 + \ldots\ldots + (\delta\beta_n)x^n$$

de donde $\alpha_o = \delta\beta_o$; $\alpha_1 = \delta\beta_1, \ldots\ldots\ldots, \alpha_{n-1} = \delta\beta_{n-1}$

$$0 = \delta\beta_n$$

de $\delta\beta_n = 0$ ya que $\beta_n \neq 0$ tenemos que $\delta = 0$

luego $\alpha_o = 0$; $\alpha_1 = 0 \ldots\ldots$, $\alpha_{n-1} = 0$

por lo tanto B es linealmente independiente.

b) B es generador de $\dfrac{F[x]}{I}$?

Sea $q(x) \in F[x]$ probar que $q(x) + I \subset [B]$

encontrar escalares $\alpha_o, \alpha_1, \ldots\ldots, \alpha_{n-1}$, tq

$q(x) + I = \alpha_o(1+I) + \alpha_1(x+I) + \ldots\ldots + \alpha_{n-1}(x^{n-1}+I)$

Sea $q(x) = \gamma_o + \gamma_1 x + \ldots\ldots + \gamma_m x^m$; $\gamma_m \neq 0$

$$q(x) + I = \gamma_o + \gamma_o + I + (\gamma_1 x + I) + (\gamma_2 x^2 + I) + \ldots + (\gamma_m x^m + I)$$

Si $m \leq n$ la solución es inmediata.

Supongamos que $m > n$ entonces

$$\begin{array}{c|c} q(x) & p(x) \\ \hline t(x) & s(x) \end{array}$$

donde $t(x)$ es un residuo y grad $t(x) < p(x)$

entonces $q(x) - t(x) = p(x)\, s(x) \in I$

$$\Rightarrow q(x) - t(x) \in I$$

$$\Rightarrow q(x) + I = t(x) + I \in [B]$$

donde $t(x) = \sum_{o}^{r} \alpha_i x^i$ con $r < n$.

Luego B es un generador de $\frac{F[x]}{I}$

con lo que se concluye que $\frac{F[x]}{I}$ es un F-espacio vectorial de dimensión finita n y se probó encontrando una base que contiene n elementos.

PROPOSICION 3.20

"Sea k una extensión de F y $\underline{a} \in k$ un elemento algebraico sobre F.

1) Si el polinomio mínimo de $\underline{a}$ es de grado n entonces F(a) es una extensión finita de F de grado n.

2) F(a) es una extensión finita de F."

1) Sea $p(x) \in F[x]$ el polinomio mínimo de a sobre F. p(x) es irreducible probado en proposición (3.18 - (1))

Sea $\Phi : F[x] \longrightarrow F(a)$

$q(x) \rightsquigarrow q(a)$ morfismo de anillos

Sea $V = \ker \Phi \Rightarrow V = [p(x)]$ como p(x) es irreducible entonces [p(x)] es un ideal maximal, o sea v es maximal.

Luego $\frac{F[x]}{V}$ es un campo.

Sea $\Phi_1 : \frac{F[x]}{V} \longrightarrow \text{Im}(\Phi)$

Φ_1 es un isomorfismo entonces $\text{Im}(\Phi)$ es un campo $F \subset \text{Im}(\Phi)$ porque F es el mínimo, $a \in \text{Im}(\Phi)$ por definición de Φ entonces $F(a) \subset \text{Im}(\Phi)$ ya que F(a) es el menor subcampo que contiene tanto a F como al elemento a, (además único) y $\text{Im}\,\Phi \subset F(a)$ por definición de Φ

de donde $F(a) = \text{Im}\,\Phi$

Además $\frac{F[x]}{V}$ es un espacio vectorial de dimensión n sobre F probado en (3.19)

también n = dim(F(a)) (ya que $\text{Im}(\Phi)$ es de dimensión n)

Luego $F(a) = \text{Im}\,\Phi$

por lo tanto F(a) es de dimensión n.

Para 2) si F(a) es de dimensión n como una consecuencia F(a) es una extensión finita de F con lo que se concluye la prueba.

PROPOSICION 3.21

Sea k una extensión de F y $a \in k$ un elemento algebraico sobre F y sea $p(x) = \sum_{i=0}^{n} \alpha_i x^i$ el polinomio mínimo de a, n = grado de p(x).

(1) Para todo $k \geq 0$, a^k es combinación lineal de $1, a_1, a^2, \ldots, a^{n-1}$

Pa.

Sea $p(x) = 0$

$$\alpha_o a^o + \alpha_1 a^1 + \alpha_2 a^2 + \ldots + \alpha_n a^n = 0, \text{ mónico}$$

$$\Rightarrow a^n = -\alpha_o - \alpha_1 a^1 - \alpha_2 a^2 - \ldots\ldots - \alpha_{n-1} a^{n-1}$$

pero ésto no es otra cosa más que decir
a^n es combinación lineal de $1, a, a^2, \ldots, a^{n-1}$ o sea se ha probado lo requerido para n=k.

Si $k > n$

supongamos que a^k es combinación lineal de los elementos a^i con $i = 0, 1, 2, 3, \ldots, n-1$.

esto es $a^k = \beta_o + \beta_1 a^1 + \ldots\ldots + \beta_{n-1} a^{n-1}$

$$a^{k+1} = \beta_o a + \beta_1 a^2 + \beta_2 a^3 + \ldots\ldots + \beta_{n-1} a^n$$

$$= \beta_o a + \beta_1 a^2 + \beta_2 a^3 + \ldots\ldots + \beta_{n-1} \left(- \sum_{i=0}^{n-1} \alpha_i a^i\right)$$

por lo tanto a^k es combinación lineal de $1, a, a^2, a^3 \ldots a^{n-1}$

(2) $T = \{ z \in k / z = \sum_{0}^{n-1} \beta_i a^i, \beta_i \in F \}$ es un subcampo de k

Sea $z \in T$, $z \neq 0$ a probar que $Z^{-1} \in T$

como $z \in T$, $z \neq 0$, entonces $z = \sum_{i=0}^{n-1} \beta_i a^i \neq 0$

Sea $y(x) = \sum_{o}^{n-1} \beta_i x^i \neq 0$ pero grad $y(x) <$ grad $p(x)$

entonces $p(x) \neq y(x)\, s(x)$

por lo tanto $p(x)$ no es divisible por $y(x)$ entonces existen $s(x)$, $j(x)$, $\in F[x]$ tq.

$1 = s(x)\, p(x) + j(x) y(x)$

$1 = s(a)\, p(a)^o + j(a)\, y(a)$

$1 = j(a)\, y(a)$

$1 = j(a)\, z$

$\Longrightarrow$ $j(a)$ es el inverso para z.

Hay que ver ahora si $j(a) \in T$

$j(x) \in F(x)$

$j(x) = \lambda_o + \lambda_1 x + \lambda_2 x^2 + \ldots\ldots + \lambda_r x^r$

$j(a) = \lambda_o + \lambda_1 a + \lambda_2 a^2 + \ldots\ldots + \lambda_r a^r$

i) Si $r \leq n-1$ entonces $j(a) \in T$.

ii) Si $r > n-1$ entonces $j(a)$ es combinación lineal de los elementos es decir

$j(a) = \lambda_o + \lambda_1 a + \lambda_2 a^2 + \ldots\ldots + \lambda_{n-1} a^{n-1} + \lambda_r a^r$

con $a^r = -\alpha_o - \alpha_1 a - \alpha_2 a^2 - \ldots\ldots - \alpha_{n-1} a^{n-1}$

$j(a) = \gamma_o + \gamma_1 a_1 + \gamma_2 a^2 + \ldots\ldots + \gamma_{n-1} a^{n-1} \in T$

por lo tanto $j(a) \in T$

con lo que se tiene que $x^{-1} \in T$

con lo anterior es suficiente para garantizar que T es un subcampo de k.

3). $T = F(a)$

a probar i) $a \in T$

ii) $F \subset T$

iii) Si L es subcampo de k tq $a \in L$ y $F \subset L$ entonces $F(a) = T \subset L$

i) $a \overset{?}{\in} T$

$a = \sum_{0}^{n-1} \beta_i a^i$ haciendo $\beta_o = 0$, $\beta_1 = 1$; $\beta_i = 0$ para $i = 1, 2, \ldots$.

entonces $a \in T$

ii) $F \subset T$

Si $x \in F$ probar que $x \in T$

$x \in F$; $x = \sum_{o}^{n-1} \beta_i a^i$; $\beta_o = x$; $\beta_i = 0$, $\forall i=1,2....$

$\beta_i \in F$

entonces $x \in T$

$\therefore$ $T \subset F(a)$

iii) L subcampo de k tq $a \in L$ y $F \subset L$ entonces $T \subset L$

Sea $x \in T$ entonces $x = \sum_{o}^{n-1} \beta_i a^i$ como $a \in L$,

$a^i \in L$, $\beta_i \in F \subset L$ entonces $\beta_i \in L$

por lo tanto $\beta_i a^i \in L$ de aquí que

$$x = \sum_{o}^{n-1} \beta_i a^i \in L \Rightarrow x \in L$$

- luego $T \subset L$

con lo que se concluye que $T = F(a)$

4)- $\{1, a, a^2 .....a^{n-1}\}$ son linealmente independientes sobre F.

Sea $\delta_o + \delta_1 a + \delta_2 a^2 + ...+ \delta_{n-1} a^{n-1} = 0$ con $\delta_i \in F$

como $p(a) = 0$

$\alpha_o 1 + \alpha_1 a_1 + ...+ \alpha_n a^n = 0$

Sea $Q(x) = \sum_{i=0}^{n-1} \delta_i x^i$

grado de $Q(x)$ < grado $p(x)$

$Q(a) = 0 \Longrightarrow$ grado de $Q(x) = 0$

$\Longrightarrow Q(x) = 0$

$\Longrightarrow \delta_i = 0, \forall i = 1,2,\ldots,n-1 \Longrightarrow \delta_0 = 0$

Luego $1, a, a^2, \ldots .a^{n-1}$ son linealmente independientes sobre F.

(5) $[F(a):F] = n$

Pa.

Por la forma como se ha definido T en el numeral (2) de esta propiedad tenemos que $x = \sum_{\sigma}^{n-1} \beta_i a^i$ para $\beta_i \cdot \epsilon$ F los elementos $1, a, a^2 \ldots .., a^{n-1}$ son generadores de T o sea de F(a) ya que T = F(a).

Además $\{1, a, a^2, \ldots, a^{n-1}\}$ son linealmente independientes probado en (4), por lo tanto $\{1, a, a^2, a^3 \ldots a^{n-1}\}$ son una base de F(a) con lo que se concluye que

$$\dim_F F(a) = n$$

PROPOSICION 3.22

"Sea k una extensión de F y sea $a \in k$. Si F(a) es una extensión finita de F entonces a es algebraico sobre F."

Pa.

Sea $n = \dim_F F(a)$

Como F es un espacio vectorial, podemos tomar 1, a, a^2..... a^n que son n+1 elementos de F(a), luego estos elementos son linealmente dependientes por tanto existen $\lambda_o, \lambda_1, \lambda_2, .., \lambda_n$ no todos nulos tales que $\lambda_o 1 + \lambda_1 a + \lambda_2 a^2 + ... + \lambda_n a^n = 0$

Luego a es una raíz del polinomio $p(x) \neq 0$ con

$p(x) = \sum_{i=0}^{n} \lambda_i x^i$, por lo tanto

a es algebraico sobre F.

PROPOSICION 3.23

"Sea k una extensión de F. Las condiciones que siguen son equivalentes:

1) a es un elemento algebraico sobre F.

2) F(a) es una extensión finita de F."

Para esta propiedad revisaremos condiciones de la proposición 3.20-1 y a continuación haremos uso de la proposición 3.22 para concluir la prueba.

"1 $\Longrightarrow$ 2" Revisando el numeral 1) de la proposición 3.20 observamos que si $\underline{a}$ es un elemento algebraico sobre F - entonces F(a) es una extensión finita de F y además de - grado n.

"2 $\Longrightarrow$ 1" Si F(a) es una extensión finita de F a probar que $\underline{a}$ es un elemento algebraico sobre F.
Pero esto es justamente lo que se demostró en la propiedad (3.22).
Con las dos implicaciones anteriores, se completa la - prueba.

PROPOSICION 3.24

"Sea k una extensión finita de un campo F"
Si $\underline{a} \in K$ entonces $\underline{a}$ es algebraico sobre F.

Pa.

Sea $\underline{a} \in k$ a probar que $\underline{a}$ es un elemento algebraico de F.
Basándonos en el numeral 2 de la proposición 3.23 para demostrar esta propiedad bastará probar que F(a) es extensión finita de F.
Por la definición de F(a) tenemos que F(a) contiene tanto a F como al elemento $\underline{a}$ por lo tanto $F \subset F(a)$, esto nos conduce a que F(a) es extensión de F.

Ahora para garantizar que F(a) no es solamente una extensión de F si no además una extensión finita lo hacemos de la siguiente manera:

F(a) además de contener a F y al elemento a es el subcampo mínimo de k , donde k es una extensión finita de un campo F, por tanto

$F(a) \subset K$ por otra parte $F \subset F(a)$.

Luego $F \subset F(a) \subset K$, haciendo uso del (Ej.3.5) podemos concluir que F(a) es extensión finita de F, con lo que se concluye la prueba.

PROPOSICION 3.25

"Sea k una extensión de F y $a \in k$ un elemento algebraico sobre F.

1) Si $x \in F(a)$ entonces x es algebraico sobre F.

2) -a y a^{-1} son algebraicos sobre F."

Pa.

1) Sea $x \in F(a)$ probaremos que x es algebraico sobre F. como $x \in F(a)$ y además sabemos que $F \subset F(a)$ entonces tenemos que $F(x) \subset F(a)$

Resumiendo lo anterior tenemos:

$F \subset F(x) \subset F(a)$; ya que $F \subset F(a)$, $F(x) \subset F(a)$ y $F \subset F(x)$ por definición, a su vez apoyándonos en el (ej.3.2) lo podemos escribir de la siguiente manera:

$[F(a):F] = [F(x):F]\,[F(a):F(x)]$

como a es un elemento algebraico sobre F tenemos

$[F(a):F] = n$ = grado de a que no es otra cosa más que una aplicación de proposición 3.23 específicamente la implicación $1) \Longrightarrow 2)$.

Luego $[F(a):F]$ es finita, ésto obliga a que $[F(x):F]$ es finita y como consecuencia F(x) extensión finita de F (grado x $\leq$ grado a).

Pero ésto es suficiente para decir que x es algebraico sobre F.

2) Dado $a \in k$ un elemento algebraico queremos probar que -a y a^{-1} también son elementos algebraicos sobre F.

$a \in F(a)$, como F(a) es un subcampo de k entonces $-a \in F(a)$ y $a^{-1} \in F(a)$, por tanto -a y a^{-1} son algebraicos sobre F ya que F(a) es extensión finita de F.

PROPOSICION 3.26

"Sea k una extensión de F y sean $a,b \in k$.

1) Si a y b son algebraicos sobre F entonces F(a,b) es extensión finita de F.

2) Si F(a,b) es extensión finita de F entonces a y b son algebraicos sobre F."

Pa.

1) Sean a y b elementos algebraicos sobre F.
a probar que F(a,b) es extensión finita de F.
En otras palabras lo que queremos demostrar es que
[F(a,b):F] es finita.

$F \subset F(a) \subset F(a,b)$ ésto lo podemos escribir de otra forma apoyados en la proposición 3.5 literal b).

$[F(a,b):F] = [F(a,b):F(a)][F(a):F]$
para que $[F(a,b):F]$ sea finita bastará garantizar que $[F(a,b):F(a)]$ es finita ya que $[F(a):F]$ es finita.
$[F(a,b):F(a)] = [F(a)(b):F(a)]$ esta igualdad es válida, ya que $F(a,b) = F(a)(b)$.

Se tendrá entonces que $[F(a)(b):F(a)]$ es finita si b es algebraico sobre F(a), ésto es cierto porque b es algebraico sobre hipótesis; pero $F \subset F(a)$ entonces lo es algebraico sobre F(a).
Por lo tanterior se concluye que $[F(a,b):F]$ es finita.

2) Si F(a,b) es extensión finita de F a probar que a y b son elementos algebraicos sobre F.
Será suficiente mostrar que $[F(a):F]$ y $[F(b):F]$ son extensiones finitas de F.

i) $F \subset F(a) \subset F(a,b)$

$[F(a,b):F] = [F(a,b):F(a)][F(a):F]$

$[F(a,b):F]$ es extensión finita de F por hipótesis de ésto tenemos que $[F(a,b):F(a)][F(a):F]$ también es finita en particular $[F(a):F]$ es finita entonces a es algebraico sobre F.

ii) Si $F \subset F(b) \subset F(a,b)$ entonces

$[F(a,b):F] = [F(a,b):F(b)]\ [F(b):F]$

por hipótesis $[F(a,b):F]$ es una extensión finita de F. Luego $[F(a,b):F(b)]\ [F(b):F]$ debe ser finita en particular $[F(b):F]$ es finita, por lo tanto, b es un elemento algebraico sobre F.

En resumen lo que se ha probado es que si F(a,b) es una extensión finita de F entonces a,b, son algebraicos sobre F.

PROPOSICION 3.27

"Sea k una extensión de F y sean $a_1, a_2, \ldots, a_n$ elementos de k. Entonces $a_1, a_2, \ldots, a_n$ son algebraicos sobre F si y solo si $F(a_1, a_2, \ldots, a_n)$ es extensión finita de F"

" $\Longrightarrow$ "

Supongamos que $a_1, a_2, \ldots, a_n$ son algebraicos sobre F y probemos que $F(a_1, a_2, \ldots a_n)$ es extensión finita de F.

La demostración se hará por inducción sobre n.

Para n=1; F(a) es extensión finita de F ya que a es algebraico sobre F. (probado en proposición 3.23).

Para n=2; F(a,b) es extensión finita de F ya que a y b son elementos algebraicos sobre F(probado en proposición 3.26)

Supongamos que se cumple para n=k o sea que

$F(a_1, a_2, \ldots a_k)$ es extensión finita de F, con $a_1, a_2, \ldots a_k$ algebraicos.

Probemos que se cumple para n = k+1

debemos probar que $F(a_1, a_2, \ldots, a_{k+1})$ es extensión finita de F, con $a_1, a_2, a_3, \ldots . a_{k+1}$ elementos algebraicos.

$F \subset F(a_1, a_2, \ldots . a_k) \subset F(a_1, a_2, \ldots . , a_k, a_{k+1})$

Aplicando la propiedad 3.5 tenemos lo siguiente:

$$[F(a_1 a_2, \ldots, a_{k+1}):F]=[F(a_1,a_2,\ldots a_{k+1}:F(a_1,a_2,\ldots a_k)]$$
$$[F(a_1,a_2,\ldots a_k) : F]$$

Habría que probar que

$[F(a_1,a_2,\ldots a_{k+1}):F(a_1,a_2,\ldots a_k)]$ es finita ya que $[F(a_1,a_2,\ldots a_k):F]$ por hipótesis inductiva, es finita y de esta forma estaríamos garantizando que

$F[(a_1,a_2,\ldots a_{k+1}):F]$ es finita

$[F(a_1,a_2,\ldots a_{k+1}):F(a_1,a_2 \ldots a_k)] =$

$[F(a_1)(a_2)(a_3) \ldots . (a_k)(a_{k+1}):F(a_1, \ldots . a_k)]$

El miembro derecho será finito si a_{k+1} es algebraico sobre $F(a_1,a_2,....a_k)$, pero esto es cierto ya que a_{k+1} es algebraico sobre F y como $F \subset F(a_1,a_2,....a_k)$ entonces a_{k+1} es algebraico sobre $F(a_1,a_2,....a_k)$.

Luego $[F(a_1, a_2,....a_{k+1}):F(a_1,a_2,....a_k)$ es finita por tanto $[F(a_1,a_2.....a_{k+1}):F]$ es finita.

"$\Longleftarrow$"

Supongamos que $F(a_1, a_2.....a_n)$ es extensión finita de F

A probar que $a_1, a_2.....a_n$ son elementos algebraicos sobre F.

Continuaremos la prueba por inducción sobre n.

para n = 1; F(a) es extensión finita de F entonces a es algebraico sobre F por proposición 3.23.

para n = 2; F(a,b) es extensión finita de F entonces a,b son elementos algebraicos sobre F. probado en proposición 3.26.

Supongamos que se cumple para n = k

Si $F(a_1, a_2,....a_k)$ es extensión finita de F entonces $a_1, a_2,.....a_k$ son algebraicos sobre F.

Probemos que se satisface para n = k+1

Si $F(a_1, a_2,.....a_{k+1})$ es extensión finita de F a probar que $a_1, a_2,....a_{k+1}$ son elementos algebraicos de F.

Tenemos que

$$F \subset F(a_1,a_2,....a_k) \subset F(a_1,a_2,.....a_{k+1})$$

por hipótesis $F(a_1, a_2,....a_k)$ extensión finita de F y $a_1, a_2,....a_k$ elementos algebraicos, además $F(a_1,a_2....a_{k+1})$ es extensión de $F(a_1, a_2,....,a_k)$. Luego $F(a_1, a_2.....a_{k+1})$ es extensión finita de F, por lo tanto - $a_1, a_2,.....a_{k+1}$ son elementos algebraicos sobre F.

En general se ha probado que si $F(a_1, a_2,....a_n)$ es extensión finita de F entonces $a_1, a_2,....,a_n$ son algebraicos.

PROPOSICION 3.28

"K una extensión de F, $a,b \in k$, a y b elementos algebraicos sobre F entonces

1) Todo elemento $x \in F(a,b)$ es algebraico sobre F.

2) a + b y ab son algebraicos sobre F."

1) Sea $x \in F(a,b)$ vamos a probar que x es algebraico sobre F.

$x \in F(a,b)$ y sabemos que $F \subset F(a,b)$

entonces $F(x) \subset F(a,b)$; (F(x), es el menor subcampo de k que contiene tanto a F como al elemento x)

es decir $F \subset F(x) \subset F(a,b)$

$[F(a,b):F] = [F(a,b):F(x)][F(x):F]$

$[\Gamma(a,b):F]$ es finita ya probado en proposición 3.26.
Esto obliga a que $[F(a,b):F(x)][F(x):F]$ sea finita en particular $[F(x):F]$ es finita, entonces x es algebraico sobre F.

2) $a,b \in k$ tales que a y b son elementos algebraicos sobre F a probar que a+b y ab son elementos algebraicos sobre F.

$a,b \in F(a,b)$ ésto por definición de F(a,b) que es el menor subcampo de k que contiene tanto a F como a los elementos a,b

$a+b \in F(a,b)$ ya que F(a,b) es subcampo de k

$a,b \in k$ por la prueba 1).

Además, si $a,b \in F(a,b)$ entonces $ab \in F(a,b)$ por la razón anteriormente expuesta y como F(a,b) extensión finita de F entonces a+b, ab son algebraicos sobre F.

PROPOSICION 3.29

"Sea k una extensión de F. El conjunto $\{ x \in k/x$ algebraico sobre F $\}$ es un subcampo de k".

- Para demostrar que el conjunto $\{ x \in k/x$ es algebraico sobre F $\}$ es un subcampo de k deben cumplirse las siguientes propiedades:

Sea $S = \{ x \in k/x$ es algebraico sobre $F\}$

Si $a \in s$, $b \in s$ entonces $-a$, a^{-1}, $a+b$, $a.b$ deben pertenecer a s, de tal manera que $-a$, a^{-1}, $a+b$, $a.b$ son algebraicos sobre F.

En este momento haremos una revisión de lo que se probó en las proposiciones 3.25 y 3.28 de donde se tiene garantía - por una parte que para $a \in k$ un elemento algebraico entonces $-a$, a^{-1}, son también elementos algebraicos sobre F.

Por otra parte si $a,b \in k$, a y b elementos algebraicos sobre F entonces $a+b$ y $a.b$ son también elementos algebraicos sobre F.

Como consecuencia de este análisis hemos logrado probar que $-a$, a^{-1}, $a+b$, $a.b$ son elementos algebraicos que es justamente lo que garantiza que el conjunto

$S = \{ x \in k/x$ es algebraico sobre $F \}$ es un subcampo de k.

DEFINICION 3.9

Sea k una extensión de F, se dice que k es una extensión algebraica de F si todo elemento de k es algebraico sobre F.

DEFINICION 3.10

Un elemento $\underline{a} \in \mathbb{C}$ es algebraico si existe un polinomio con coeficientes en $\mathbb{Q}$ del cual el elemento $\underline{a}$ es una raíz. En otras palabras si $\underline{a}$ es algebraico entonces existe $p(x)$ tq $p(a) = 0$.

PROPOSICION 3.30

"Si k es una extensión algebraica de F y L es extensión algebraica de k entonces L es extensión algebraica de F."

Pa.

k una extensión algebraica de F implica que k es algebraico sobre F.

k algebraico sobre F implica que todo elemento de k es algebraico sobre F de donde $F \subset K$.

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 $K \subset L$.

Luego tenemos $F \subset K \subset L$ de donde por propiedades de inclusiones, L es una extensión algebraica sobre F, que es lo que se necesitaba probar.

PROPOSICION 3.31

"Los números $\sqrt{2}$, $\sqrt{3}$, $\sqrt{2} + \sqrt{3}$, $\sqrt{2} \cdot \sqrt{3}$ son números algebraicos."

De acuerdo a la definición de número algebraico debemos encontrar un polinomio con coeficientes en $\mathbb{Q}$ para cada uno de los números $\sqrt{2}$, $\sqrt{3}$, $\sqrt{2} + \sqrt{3}$, $\sqrt{2}\ \sqrt{3}$

a) $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$ ya que para $x = \sqrt{2}$ tenemos

$$x^2 = 2$$

$$\Rightarrow x^2 - 2 = 0$$

$\Rightarrow \sqrt{2}$ es raíz del polinomio $p(x) = x^2 - 2$

b) Sea $x = \sqrt{3}$ probar que x es algebraico

$$x = \sqrt{3} \Rightarrow x^2 = 3 \Rightarrow x^2 - 3 = 0$$

$\sqrt{3}$ es raíz del polinomio $p(x) = x^2 - 3$

c) Sea $x = \sqrt{2} + \sqrt{3}$ probar que x es algebraico sobre $\mathbb{Q}$.

$$x = \sqrt{2} + \sqrt{3}$$

$x^2 = 5 + 2\sqrt{6} \Rightarrow x^2 - 5 = 2\sqrt{6}$ elevando al cuadrado ambos miembros de la última ecuación tenemos:

$$x^4 - 2x^2(5) + 25 = 4(6)$$

$$x^4 - 10x^2 + 25 = 24$$

$$\Rightarrow x^4 - 10x^2 + 1 = 0$$

$\Rightarrow \sqrt{2} + \sqrt{3}$ es raíz del polinomio $p(x) = x^4 - 10x^2 + 1$

luego $\sqrt{2} + \sqrt{3}$ es algebraico.

d) Sea $x = \sqrt{2}.\ \sqrt{3}$

$= x = \sqrt{6}$

$\Rightarrow x^2 = 6$

$\Rightarrow x^2 - 6 = 0$ $\sqrt{2}.\ \sqrt{3}$ es raíz del polinomio

$$p(x) = x^2 - 6$$

por lo tanto $\sqrt{2}.\ \sqrt{3}$ es algebraico.

PROPOSICION 3.32

"El conjunto de los números algebraicos es un subcampo del campo de los números complejos"

Pa.

Sea $S = \{ x \in k / x$ es algebraico$\}$

Vamos a probar que S es un subcampo del campo de los números complejos.

Practicamente la prueba es una aplicación directa de la proposición 3.29 que es una propiedad que satisfacen los números algebraicos.

Asociando $\mathbb{C}$ con el k y $\mathbb{Q}$ con el F. ya que el campo de los números complejos es una extensión del campo de los números racionales o sea $\mathbb{Q} \subset \mathbb{C}$.

De tal forma que el conjunto

$\{ x \in \mathbb{C} / x$ es algebraico sobre $\mathbb{Q}\}$ es un subcampo de $\mathbb{C}$, haciendo énfasis en que se trata de una aplicación directa

de la proposición 3.29.

Por lo tanto, hemos probado de manera general que el conjunto de números algebraicos es un subcampo del campo de los números complejos.

U N I D A D IV

R A I C E S D E P O L I N O M I O S.

DEFINICION 4.1

Si $p(x) \in F[x]$ entonces un elemento a que se encuentra en algún campo extensión del F se llama raíz de $p(x)$ si $p(a)=0$.

PROPOSICION 4.1

Sea $p(x) \in \mathbb{C}[x]$ tal que sus coeficientes son números algebraicos. Si m es una raíz de $p(x)$ entonces m es un número algebraico.

Pa.

Sea $p(x) = \sum_{i=0}^{n} \alpha_i x^i$ tal que cada α_i es un número algebraico.

Como cada α_i es algebraico sobre $\mathbb{Q}$ tenemos $\mathbb{Q}(\alpha_o, \alpha_1, \ldots \alpha_n)$ es una extensión finita de $\mathbb{Q}$ ésto como una aplicación de la proposición 3.27.

$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_n)(m)$ es una extensión finita de $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$; pero ésto es cierto ya que m es una raíz de $p(x)$ por lo tanto algebraico sobre $\mathbb{Q}$ pero como $\mathbb{Q} \subset \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ entonces m es algebraico sobre $\mathbb{Q}(\alpha_1, \alpha_2, \ldots \alpha_n)$

Luego siempre aplicando la propiedad 3.27 tenemos

$\mathbb{Q} \subset \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{Q}(\alpha_o, \alpha_1, \ldots, \alpha_n, m)$

entonces $\mathbb{Q} \subset \mathbb{Q}(\alpha_o, \alpha_1, \ldots \alpha_n, m)$

por lo tanto m es un número algebraico que es lo que se necesitaba probar.

DEFINICION 4.2

X ε $\mathbb{C}$ es un entero algebraico si x es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$.

PROPOSICION 42

"Si a ε $\mathbb{C}$ es un entero algebraico existe m ε $\mathbb{N}$, m > 0 tal que ma es un entero algebraico."

Si a ε $\mathbb{C}$ es un número algebraico entonces a es algebraico sobre $\mathbb{Q}$.

Sea $p(x) = \sum_{i=0}^{n} \alpha_i x^i$, $\alpha_i \varepsilon \mathbb{Q}$

$$\Rightarrow p(a) = \sum_{i=0}^{n} \alpha_i a^i = 0$$

$\Rightarrow \alpha_o + \alpha_1 a + \alpha_2 a^2 + \ldots\ldots + a^n = 0$, ya que p(x) es mónico, $\alpha_n = 1$

$$\Rightarrow \frac{c_o}{d_o} + \frac{c_1}{d_1} a + \frac{c_2}{d_2} a^2 + \ldots\ldots + a^n = 0$$

ya que $\alpha_i \varepsilon \mathbb{Q}$

donde c_i y d_i son enteros

Si hacemos $c = \prod_{i=0}^{n} d_i$, tenemos

$$(1)\ldots\ldots C\left(\frac{c_o}{d_o}\right) + c\left(\frac{c_1}{d_1}\right)a + c\,\frac{c_2}{d_2}\,a^2 + \ldots\ldots + ca^n = 0$$

para el producto $c\left(\frac{c_i}{d_i}\right) = (d_o.d_1.d_2.d_3\ldots d_i\ldots d_n)\left(\frac{c_i}{d_i}\right)$

Cada d_i es un entero, c_i es entero y c es también un entero, luego podemos escribir (1) como

$\beta_1 + \beta_2 a + \beta_3 a^2 + \ldots\ldots + \beta_n a^n = 0$ notando que $\beta_i \in \mathbb{Z}$

multiplicando esta ecuación por β_n^{n-1} tenemos:

$$\beta_n^{n-1} (\beta_1 + \beta_2 a + \beta_3 a^2 + \ldots\ldots + \beta_n a^n) = 0$$

$$\Longrightarrow \beta_n^{n-1} \beta_1 + \beta_n^{n-2} \beta_n (\beta_2 a) + \beta_n^{n-3} \beta_n^2 (\beta_3 a^2) + \ldots\ldots (\beta_n a)^n = 0$$

$$\Longrightarrow \beta(\beta_n a) = 0, \text{donde } \beta = \beta_n^{n-1} + \beta_n^{n-2} \beta_n + \ldots\ldots \beta_n$$

haciendo $m = \beta_n$ se tiene que $\beta_n a = ma$ es entero algebraico ya que es raíz de β un polinomio con coeficientes en $\mathbb{Z}$, que es lo que se quería probar.

PROPOSICION 4.3

"Dada la ecuación $\alpha_o x^n + \alpha_1 x^{n-1} + \ldots\ldots + \alpha_n = 0$ con $\alpha_o, \alpha_1, \ldots\ldots, \alpha_n$ enteros y α_o y $\alpha_n \neq 0$. Mostrar que si la ecuación anterior tiene una raíz racional p/q, entonces p divide a α_n y q divide a α_o".

Como $x = \frac{p}{q}$ es una raíz de la ecuación

$x^m + \alpha_1 x^{m-1} + \alpha_2 x^{m-2} + \ldots\ldots + \alpha_m = 0$ sustituyéndolo y multiplicando por q^n se tiene:

$$\alpha_o\left(\frac{p}{q}\right)^n q^n + \alpha_1\left(\frac{p}{q}\right)^{n-1} q^n + \ldots\ldots + \alpha_n q^n = 0$$

$$(1) = \alpha_o p^n + \alpha_1 p^{n-1} q + \alpha_2 p^{n-2} q^2 + \ldots\ldots + \alpha_{n-1} p q^{n-1} + \alpha_n q^n = 0$$

dividiendo por p la ecuación anterior tenemos:

$$\frac{\alpha_o p^n}{p} + \frac{\alpha_1 p^{n-1} q}{p} + \frac{\alpha_2 p^{n-2} q^2}{p} + \ldots\ldots + \frac{\alpha_{n-1} p p^{n-1}}{p} + \frac{\alpha_n q^n}{p} = 0$$

$$\alpha_o p^{n-1} + \alpha_1 p^{n-2} q + \alpha_2 p^{n-3} q^2 + \ldots\ldots + \alpha_{n-1} q^{n-1} + \frac{\alpha_n q^n}{p} = 0$$

$$= \alpha_o p^{n-1} + \alpha_1 p^{n-2} q + \alpha_2 p^{n-3} q^2 + \ldots\ldots + \alpha_{n-1} q^{n-1} = -\frac{\alpha_n q^n}{p}$$

El primer miembro de la ecuación anterior es un entero, ya que α_i; $i = 0,1,\ldots\ldots n$ son enteros, p, q también son enteros por consiguiente ha de serlo el segundo miembro.

Como p, q son primos entre sí, p no divide a q^n, por lo tanto p divide a α_n.

Por otra parte si en la ecuación (1) pasamos el primer término al de la derecha, y luego dividimos por q tenemos la siguiente ecuación:

$$\alpha_1 p^{n-1} + \alpha_2 p^{n-2} q + \ldots\ldots + \alpha_{n-1} p q^{n-2} + \alpha_n q^{n-1} = -\frac{\alpha_o p^n}{q}$$

haciendo un análisis similar al anterior, tenemos que q divide a α_o.

Con lo anterior se ha probado que para $a = \frac{p}{q}$ perteneciente a los racionales y siendo raíz de la ecuación $\alpha_o x^n + \alpha_1 x^{n-1} + \ldots\ldots + \alpha_n = 0$ entonces p divide a α_n y q divide a α_o.

PROPOSICION 4.4

" Si $a \in \mathbb{Q}$ es un entero algebraico entonces a es un número entero"

Para la demostración de esta proposición haremos uso de la propiedad anterior, proposición 4.3, que se hizo en forma general.

Como a es un entero algebraico entonces satisface una ecuación de la forma

$$\alpha_o x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \ldots\ldots + \alpha_n = 0$$

con $\alpha_o = 1$ ya que $\alpha_o x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \ldots + \alpha_n$ es un polinomio mónico.

Para probar que $a = \frac{p}{q}$ es entero, hay que probar que q divide a p; como en el caso general q divide a α_o aquí $\alpha_o = 1$, entonces q toma únicamente los valores de 1 ó -1 con lo que $a = \frac{p}{q}$ es un entero que es precisamente lo que se quería probar.

"ELEMENTOS ENTEROS SOBRE

UN ANILLO "

DEFINICION 4.2.1

Dados un anillo B, un sub-anillo A de B y un elemento $x \in B$ indicamos por A[x] el subanillo de B engendrado por A y x, es decir, la intersección de los subanillos de B que contienen a A y al elemento x.

Es el conjunto de sumas de la forma

$$a_o + a_1x + a_2x^2 + \ldots\ldots + a_nx^n; \qquad a_i \in A$$

La noción de A-módulo (módulo sobre un anillo) es la generalización directa de la noción de espacio vectorial sobre un campo.

DEFINICION 4.2.2

Un A-módulo M es un grupo abeliano (aditivo) provisto de una aplicación $A \times M \longrightarrow M$ (multiplicativamente) tal que

$$a(x+y) = ax + ay$$

$$(a+b)x = ax + bx$$

$$a(bx) = (ab)x$$

$$1x = x$$

con $a,b \in A$, A un anillo

$x,y \in M$

TEOREMA (1) Sean $\mathbb{R}$ un anillo, A un sub-anillo de $\mathbb{R}$ y x un elemento de $\mathbb{R}$. Las propiedades que siguen son equivalentes.

a) Existen $a_o, a_1, \ldots . a_{n-1} \in A$ tales que

$$x^n + a_{n-1}x^{n-1} + \ldots . + a_1 x + a_o = 0$$

b) El anillo A[x] es un A-módulo de tipo finito.

c) Existe un sub-anillo B de $\mathbb{R}$ que contiene a A y aX, y que es un A-módulo de tipo finito.

DEMOSTRACION

"a $\Longrightarrow$ b" Sea M el sub-anillo generado por

$$\{1, x_1\ x_2, \ldots . , x^{n-1}\}$$

a probar $M = A[x]$

$$x^n = -a_o 1 - a_o x - a_2 x^2 - \ldots . - a_{n-1} x^{n-1} \in M$$

$$x^{n+1} = -a_o x - a_1 x^2 - a_2 x^3 - \ldots . - a_{n-1}\ x^n \in M$$

i) "A[x] $\subset$ M"

para todo m: $x^m \in M$

para todo m, para todo subconjunto

$\{ a_o, a_1, a_2, \ldots\ldots, a_m \}$ de A

$a_o + a_1 x + a_2 x^2 + \ldots\ldots + a_m x^m \in M$

luego $A[x] \subset M$.

ii) "$M \subset A[x]$" es equivalente a probar que:

$\{1, x, x^2, \ldots\ldots, x^{n-1}\} \subset A[x]$

a probar que $1 \in A[x]$, $1 \in A$ y $A \subset A[x]$ luego $1 \in A[x]$

$x \in A[x]$, por definición de $A[x]$ es cierto.

$x^2 \in A[x]$

.
.
.
.
.

$x^{n-1} \in A[x]$

Luego $M \subset A[x]$

por lo tanto $M = A[x]$

Ahora probaremos que es un A-módulo

$A.A[x] \subset A[x]$. Sea $a \in A$, y $\in A[x]$

probamos que $a.y \in A[x]$

por tratarse de un anillo tenemos que si $p \in A[x]$;

$t \in A[x]$ entonces $pt \in A[x]$, como $A \subset A[x]$,

si $a \in A \Rightarrow a \in A[x]$; luego es A-módulo.

"b $\Longrightarrow$ c"

tomando B = A[x]

AU { x } $\subset$ A[x] porque A $\subset$ A[x] y x ε A[x] por definición de A[x]; y ya se probó que A[x] es un A-módulo

"c $\Longrightarrow$ a"

Sea $\{y_1, y_2, y_3, \ldots\ldots, y_n\}$ un generador finito de B

$$B = Ay_1 + Ay_2 + Ay_3 + \ldots\ldots + Ay_n$$

i) "B $\subset$ $Ay_1 + Ay_2 + Ay_3 + \ldots\ldots + Ay_n$"

basta probar que

$$\{y_1, y_2, y_3, \ldots\ldots y_n\} \subset Ay_1, + Ay_2 + Ay_3 + \ldots\ldots + Ay_n$$

$$y_1 = 1y_1 + 0y_2 + 0y_3 + \ldots\ldots + 0y_n$$

$$y_2 = 0y_1 + 1y_2 + 0y_3 + \ldots\ldots + 0y_n$$

$$\vdots$$

$$y_n = 0y_1 + oy_2 + 0y_3 + \ldots\ldots + 1y_n$$

Si $y_1 \varepsilon A \Longrightarrow y_1 \varepsilon Ay_1 + Ay_2 + Ay_3 + \ldots\ldots + Ay_n$

$$\vdots$$

$y_n \varepsilon A \Longrightarrow y_n \varepsilon Ay_1 + Ay_2 + Ay_3 + \ldots\ldots + Ay_n$

Luego $\{y_1, y_2, y_3, \ldots\ldots, y_n\} \subset Ay_1 + Ay_2 + \ldots\ldots Ay_n$

y como $\{ y_1\ y_2, y_3, \ldots\ldots, y_n\}$ es generador de B se tiene que $B \subset Ay_1 + Ay_2 + \ldots\ldots + Ay_n$

ii) "$Ay_1 + Ay_2 + Ay_3 + \ldots\ldots + Ay_n \subset B$"

$a_1y_1 + a_2y_2 + a_3y_3 + \ldots\ldots + a_ny_n \in B$ es cierto porque

$a_1y_1 \in B$; $a_2y_2 \in B, \ldots\ldots, a_ny_n \in B$

Luego su suma está en B.

También porque B es un A-módulo

Luego $Ay_1 + Ay_2 + Ay_3 + \ldots\ldots + Ay_n \subset B$

De i) y ii) se tiene que $B = Ay_1 + Ay_2 + \ldots\ldots + Ay_n$

Como $x \in B$, $y_i \in B$ y B es sub-anillo de $\mathbb{R}$. Se tiene que

$xy_1, xy_2, xy_3, \ldots\ldots, xy_n$ pertenecen a B

$xy_1, xy_2, xy_3, \ldots\ldots, xy_n$ son de la forma

$$xy_1 = a_{11}y_1 + a_{12}y_2 + \ldots\ldots + a_{1n}y_n$$

$$xy_2 = a_{21}y_1 + a_{22}y_2 + \ldots\ldots + a_{2n}y_n$$

.
.
.
.
.

$$xy_n = a_{n1}y_1 + a_{n2}y_2 + \ldots\ldots + a_{nn}y_n$$

de

$$xy_i = \sum_{j=1}^{n} a_{ij}y_j$$

$$xy_i = \sum_{j=1}^{n} a_{ij}y_j \Longrightarrow xy_i - \sum_{j=1}^{n} a_{ij}y_j = 0$$

$$\Longrightarrow (x - \sum_{j=1}^{n} a_{ij})y_j = 0$$

$$= (\sum_{j=1}^{n} x\delta ij - \sum_{j=1}^{n} aij)\ y_j = 0$$

donde $\delta_{ij} = \begin{cases} 1, & j=i \\ 0, & j \neq i \end{cases}$ $= \sum_{j=1}^{n} (\delta_{ij}x - a_{ij})y_j = 0$

$i = 1,2,3...,n$

cada $aij \in A$

desarrollando $\sum_{j=1}^{n} (\delta_{ij}x - a_{ij})yi = 0$

se tienen las siguientes ecuaciones

$$(x - a_{11})y_1 - a_{12}y_2 -.....- a_{1n}y_n = 0$$

$$- a_{21}y_1 + (x - a_{22})y_2 -..... - a_{2n}y_n = 0$$

$$- a_{31}y_1 - a_{32}y_2 + (x - a_{33})y_3 - a_{3n}y_3 = 0$$

$$\vdots$$

$$-a_{n1}y_1 - a_{n2}y_2 - a_{n3}y_3 -.... +(x - a_{nn})y_n = 0$$

Sea la matriz de coeficientes del sistema de ecuaciones anteriores

$$T = \begin{bmatrix} (x-a_{11}) & -a_{12} & -a_{13} \ldots\ldots & -a_{1n} \\ -a_{21} & (x-a_{22}) & -a_{23} \ldots\ldots & -a_{2n} \\ -a_{31} & -a_{32} & (x-a_{33}) \ldots\ldots & -a_{3n} \\ \vdots & & & \\ -a_{n1} & -a_{n2} & -a_{n3} -\ldots\ldots & (x-a_{nn}) \end{bmatrix}$$

El determinante de la matriz asociada es de la forma

$$d = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots\ldots + a_1 x + a_o$$

que es una ecuación de la forma $p(x) = 0$, donde $p(x)$ es un polinomio de grado n sobre A; este polinomio es unitario ya que el término de x^n proviene únicamente del producto $\prod_{i=1}^{n}(x-a_{ii})$ de los elementos de la diagonal principal de la matriz asociada al sistema de ecuaciones.

Faltaría probar que $d=0$ para todo $i \leq n$.

El objetivo es probar que $d=0 \ \forall i \leq n$.

Supongamos que $d \neq 0 \ \forall \ i \leq n$, si $d \neq 0$ entonces aplicando la regla de cramer tenemos que para

$$y_1 d = 0 \Longrightarrow y_1 = \frac{|T_1|}{d}$$

donde T_1 es la matriz asociada adjunta que tiene la forma

$$T_1 = \begin{pmatrix} 0 & -a_{12} & -a_{13} \cdots\cdots & -a_{1n} \\ 0 & (x-a_{22}) & -a_{23} \cdots\cdots & -a_{2n} \\ \vdots & & & \\ 0 & -a_{n2} & -a_{n3} \cdots\cdots & (x-a_{nn}) \end{pmatrix}$$

Y $|T_1|$ denota el determinante de T_1.

Por propiedades de determinantes "si todos los componentes de una fila o columna de una matriz cuadrada T_1 son todos nulos, el determinante de $T_1 = 0$"

Luego mediante esta propiedad tenemos $y_1 = \frac{|T_1|}{d}$ son todos nulos, el determinante de $T_1 = 0$"

Luego mediante esta propiedad tenemos $y_1 = \frac{|T_1|}{d} = 0$

lo que implica que $y_1 = 0$

Realizando el mismo proceso para $y_2 d = 0$ se obtiene que $y_2 = 0$ continuando con este proceso tenemos que $y_1 = y_2 = y_3 \cdots\cdots = y_n = 0$

pero lo anterior es una contradicción, ya que

$y_1, y_2, \ldots, y_n$ es un generador finito de B.

Por lo tanto $d=0 \ \forall \ i \leq n$ que es precisamente lo que se necesitaba probar.

DEFINICION 4.2.3

Sean $\mathbb{R}$ un anillo y A un sub-anillo de $\mathbb{R}$.
Se dice que un elemento x de $\mathbb{R}$ es entero sobre A si satisface las condiciones equivalentes a), b), c) del teorema (1).

DEFINICION 4.2.4

Sea $p \in A[x]$ un polinomio unitario tal que $p(x) = 0$ (polinomio cuya existencia es afirmada por a)); la relación $p(x)=0$ es llamada ecuación de dependencia integral de x sobre A.

PROPOSICION 4.2.1

Sean $\mathbb{R}$ un anillo, A un sub-anillo de $\mathbb{R}$ y $(x_i)_1,....i...n$ una familia finita de elementos de $\mathbb{R}$. Si para todo i, x_i es entero sobre $A[x_1, x_2,....x_{i-1}]$ (en particular, si todos los xi son enteros sobre A), entonces $A[x_1,....,x_n]$ es un A-módulo de tipo finito.

Demostración: Recordemos que $A[x_1,x_2,....x_{i-1}]$ es el anillo generado por AU $\{x_1,x_2,....,x_n\}$ en donde:

x_3 es entero sobre $A[x_1,x_2]$

x_2 es entero sobre $A[x_1]$

x_1 es entero sobre A

probando por inducción sobre n

para n=1

x_1 es entero sobre A, lo que es equivalente a que $A[x_1]$ es un A-módulo de tipo finito.

por la equivalencia entre a $\Longrightarrow$ b del teorema 1.

Supongamos cierto para (n-1), esto equivale a afirmar que $A[x_1, x_2 \ldots\ldots x_{n-1}] = B$ es un A-módulo de tipo finito.

Si es A-módulo de tipo finito.

Sea $\{ y_1, y_2, y_3, \ldots, y_q \}$ un generador finito de B

$$B = Ay_1 + Ay_2 + \ldots\ldots + Ay_q$$

x_n entero sobre B equivale a decir que $B[x_n]$ es un B-módulo de tipo finito; ésto implica que existe $\{ z_1, z_2, \ldots, z_p \} \subset B[x_n]$ un generador finito.

Es decir que:

$$B[x_n] = Bz_1 + Bz_2 + Bz_3 + \ldots + Bz_p$$

$$B[x_n] = Ay_1z_1 + Ay_2z_1 + \ldots\ldots + Ay_qz_1 + Ay_1z_2 + \ldots\ldots + Ay_qz_2 +$$

$$\ldots\ldots Ay_1z_p + Ay_2z_p + \ldots\ldots + Ay_qz_p$$

$\{ y_iz_j \mid i \leq q, \quad j \leq p \}$ es un generador finito de B[x]

como $A[x_1x_2, \ldots\ldots, x_{n-1}].[x] = A[x_1, x_2, \ldots, x_n]$

entonces $B[x_n] = A[x_1, x_2, \ldots, x_n]$

Luego $A[x_1, x_2, \ldots x_n]$ es un A-módulo de tipo finito

con que se concluye la prueba.

PROPOSICION 4.2.2

Sean $\mathbb{R}$ un anillo, A un sub-anillo de $\mathbb{R}$, x e y elementos de $\mathbb{R}$ enteros sobre A. Entonces x+y, x-y y xy son enteros sobre A.

Demostración: x+y, x-y, xy son elementos de A[x,y] porque A[x,y] es un sub-anillo que contiene a x,y.

x es un entero sobre A y y es entero sobre A[x], luego A[x,y] es un A-módulo de tipo finito.

Entonces A[x,y] es un A-módulo de tipo finito tal que

$A \cup \{x+y\} \subset A[x,y]$

tal que $A \cup \{ x+y \} \subset A[x,y]$

$A \cup \{ x-y \} \subset A[x,y]$

$A \cup \{ xy \{ \subset A[x,y]$

de donde x+y, x-y, xy son enteros sobre A por la condición equivalente c) $\Rightarrow$ a) del teorema 1 con lo que se concluye la prueba.

U N I D A D V

TEOREMA DE KRONECKER.

ANILLOS DE POLINOMIOS

LEMA (ALGORITMO DE LA DIVISION)

Dados dos polinomios $p(x)$ y $q(x)$ de $F[x]$ con $q(x) \neq 0$, existen entonces dos polinomios $t(x)$ y $r(x)$ en $F[x]$ tales que:

$p(x) = t(x)q(x) + r(x)$ donde $r(x) = 0$

ó grado $(r(x)) <$ grado$(q(x))$

Pa.

La prueba no es otra cosa más que el proceso de la división larga de polinomios que usamos para dividir un polinomio entre otro.

Si el grado de $p(x)$ es menor que el de $q(x)$ nada hay que probar, ya que solamente hay que poner $t(x) = 0$, $r(x) = p(x)$ y ciertamente, tenemos $p(x) = 0\ q(x) + p(x)$ donde grad $(p(x)) <$ grad $(q(x))$ ó $p(x) = 0$

Supongamos que $p(x) = a_o + a_1x + \ldots\ldots + a_mx^m$ y $q(x) = b_o + b_1x + \ldots\ldots + b_nx^n$ con $a_m \neq 0$ y $b_n \neq 0$ y además $m \geq n$.

Sea $p_1(x) = p(x) - (a_m | b_n)x^{m-n}(q)$; entonces grad $(p_1(x)) \leq m-1$, de donde por inducción sobre el grado de $p(x)$ podemos suponer que $p_1(x) = t_1(x)\ q(x) + r(x)$ donde $r(x) = 0$ ó grad $(r(x)) <$ grad $q(x)$. pero entonces $p(x) - (a_m | b_n)x^{m-n} \cdot q(x) = t_1(x)q(x) + r(x)$, lo cual, por transposición, nos da

$$p(x)=((a_m|b_n)x^{m-n} + t_1(x)q(x)+r(x)$$

Si hacemos $t(x) = (a_m|b_n)x^{m-n} + t_1(x)$ tendremos que

$p(x) = t(x)q(x) + r(x)$

donde $t(x), r(x) \in F[x]$ y $r(x) = 0$

o grado $r(x) <$ grado $(q(x))$

lo que completa la prueba.

DEFINICION 5.1

El elemento $a \in k$ es una raíz de $p(x) \in F[x]$ de multiplicidad m si $(x-a)^m$ divide a $p(x)$, mientras que $(x-a)^{m+1}$ no divide a $p(x)$.

PROPOSICION 5.1

"Si $p(x) \in F[x]$ y si k es una extensión de F entonces para todo $b \in k$, $p(x)=(x-b)q(x)+p(b)$ en donde $q(x) \in k[x]$ y grado de $q(x) = n-1$, n=grado de $p(x)$"

Pa. Ya que k es extensión de F entonces $F \subset k$.

Además $F[x] \subset k[x]$ por definición de F[x] y k[x], de donde podamos considerar p(x) se encontrará en k[x].

Por el algoritmo de la división para polinomios en k[x]

tenemos $p(x) = (x-b)q(x) + r$ donde $q(x) \in k[x]$
y $r=0$ ó grado de $r <$ grado de $(x-b) = 1$.
Así pues $r=0$ ó grado de $r=0$; en cualquiera de los casos
r debe ser un elemento de k.
Como $p(x) = (x-b)q(x)+r$, $p(b) = (b-b)q(b) + r = r$
o sea $r = p(b)$,
por tanto $p(x) = (x-b)\, q(x) + p(b)$;
Para verificar que el grado de q(x) es menor en una unidad
que el de p(x) basta con observar que
$p(x) = (x-b)q(x) + p(b)$ y como grado de $p(x)=n$;
grado $p(b) = 0$ debe ser que grado de $(x-b)$ + grado de $q(x)$
sea igual a n, grado de $(x-b) = 1$ entonces tiene que ser
grado de $q(x) = n-1$ ya que grado de $(x-b)$ + grado de $q(x)$
$= 1 + n-1 = n$
con lo que se prueba que grado de $q(x) = n-1$.

PROPOSICION 5.2

Si $p(x) \in F[x]$ y $a \in k$ es una raíz de p(x), k una extensión de F, entonces en k[x], x-a es un divisor de p(x).

Pa.

De acuerdo con la propiedad anterior en k[x] $p(x) = (x-a)q(x) + p(a) = (x-a)q(x)$ ya que $p(a) = 0$ por ser una raíz de p(x) por tanto $p(x) = (x-a)q(x)$

ésto significa, (x-a) divide a p(x) en k[x] con lo que se concluye la prueba.

PROPOSICION 5.3

Sea $p(x) \in F[x]$ un polinomio de grado n y sea k una extensión de F. Entonces, en k, p(x) tiene a lo sumo n raíces.

Procedemos para la prueba por inducción sobre n, el grado del polinomio p(x).

Si p(x) es de grado 1, entonces debe ser de la forma $\alpha x + \beta$, donde α, β están en un campo F y donde $\alpha \neq 0$. Para cualquier a tal que $p(a) = 0$ debe entonces implicar que $\alpha a + \beta = 0$ de donde se concluye que $a = -\beta / \alpha$, es decir, p(x) tiene la raíz única $-\beta / \alpha$ de donde la conclusión es válida en este caso.

Suponiendo que el resultado sea cierto en cualquier campo para todos los polinomios de grado menor que n, supongamos que p(x) es de grado n sobre F. Sea k una extensión cualquiera de F. Si p(x) no tiene ninguna raíz en k entonces lo afirmado es cierto, pues el número de raíces en k, cero, es definitivamente cuando más n.

Supongamos que p(x) tiene al menos una raíz $a \in k$ y que a es de multiplicidad m, por la propiedad (5.2) $(x-a)^m$ divide a p(x), de ello se sigue que $m \leq n$.

Ahora $p(x) = (x-a)^m q(x)$ donde $q(x) \in k[x]$ es de grado $n-m$ (por tratarse de un producto de polinomios)
Del hecho de que $(x-a)^{m+1}$ no divide a $p(x)$, (también como una aplicación de la propiedad (5.2) deducimos que $(x-a)$ no divide a $q(x)$, de donde se tiene que a no es una raíz de $q(x)$. Si $b \neq 0$ es una raíz en k, de $p(x)$ entonces $0 = p(b) = (b-a)^m q(b)$; como $b-a \neq 0$ y como estamos en un campo concluimos que $q(b) = 0$.

Es decir, cualquier raíz de $p(x)$ en k distinta de a debe ser una raíz de $q(x)$. Como $q(x)$ es de grado $n-m < n$, $q(x)$ tiene, de acuerdo con nuestra hipótesis de inducción, cuando más $n-m$ raíces en k, que junto con la otra raíz, a, contada m veces, nos dice que $p(x)$ tiene cuando más $m+(n-m)=n$ - raíces en k. Esto completa la prueba.

PROPOSICION 5.4

Sea $p(x) \in F[x]$ un polinomio de grado $n \geq 1$, irreducible sobre F. Entonces existe una extensión E de F en la cual $p(x)$ tiene una raíz y $[E:F] = n$

Pa.

Por ser $p(x)$ irreducible, $[p(x)]$ es un ideal maximal en $F[x]$, luego $\frac{F[x]}{[p(x)]}$ es un campo.

Mostraremos que $\frac{F[x]}{[p(x)]}$ satisface las conclusiones del teorema.

La función $\Phi : F \longrightarrow \frac{F[x]}{[p(x)]}$

$$\alpha \rightarrow \alpha + [p(x)], \quad \alpha \in F$$

es un homomorfismo inyectivo.

F es isomorfo a $\Phi(F)$ o sea F es isomorfo a un subcampo de $\frac{F[x]}{[p(x)]}$.

Solamente hay que probar que p(x) tiene una raíz en $\frac{F[x]}{[p(x)]}$.

Sea $x + [p(x)] = a$ en $\frac{F[x]}{[p(x)]}$

$p(a) = p(x + [p(x)]) = [p(x)]$

En general sea $q(x) \in F[x]$, con grado de $q(x) = m$

$$q(x) = \alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots + \alpha_m x^m$$

$$q(a) = \alpha_o + \alpha_1 a + \alpha_2 a^2 + \ldots\ldots + \alpha_m a^m$$

$$q(a) = \alpha_o + \alpha_1 (x+[p(x)] + \alpha_2 (x+[p(x)])^2 + \ldots\ldots$$

$$+ \alpha_m (x + [p(x)])^m$$

entonces $q(a) = \alpha_o + \alpha_1 x + [p(x)] + \alpha_2 x^2 + [p(x)] +$

$$\ldots\ldots + \alpha_m x^m + [p(x)]$$

por lo tanto $q(a) = \alpha_o + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_m x^m + [p(x)]$

entonces $q(a) = q(x) + [p(x)$

$$\text{luego } q(x) + [p(x)] \in \frac{F[x]}{[p(x)]}$$

$$\forall\ q(x) \in F[x]$$

por lo tanto $p(a) = p(x) + [p(x)] = [p(x)] = 0$

lo que se tiene es que $a = x + [p(x)]$ es una raíz de $p(x)$ en $\frac{F[x]}{[p(x)]}$

Luego la extensión formada $\frac{F[x]}{[p(x)]}$ es la buscada y se puede denotar por E y se obtienen las conclusiones del teorema.

PROPOSICION 5.5

Si $p(x) \in F[x]$, hay una extensión E de F en la cual $p(x)$ tiene una raíz, y además $[E:F] \leq n$, n=grado de $p(x)$.

Pa.

Sea $t(x)$ un factor irreducible de $p(x)$; cualquier raíz de $t(x)$ es una raíz de $p(x)$. De acuerdo con la propiedad 5.4 hay una extensión E de F con $[E:F]$ = grado $t(x) \leq$ grado de $p(x)$ en que $t(x)$ y, por lo tanto, $p(x)$ tiene una raíz.

PROPOSICION 5.6 (TEOREMA DE KRONECKER)

Sea $p(x) \in F[x]$ un polinomio de grado $n \geq 1$.
Entonces existe una extensión E de F en la cual p(x) tiene n raíces, además $[E:F] \leq n!$.

Pa.

En el enunciado de este teorema una raíz de multiplicidad m se cuenta como m raíces.
Según la proposición anterior 5.5 hay una extensión E_o de F con $[E_o:F] \leq n$ en que p(x) tiene una raíz denotémosla por α. Así, pues, en $E_o[x]$, p(x) se factoriza como $p(x) = (x - \alpha)q(x)$ donde q(x) es de grado n-1 por la proposición 5.1.

Continuando con este proceso hay una extensión E de E_o de grado cuando más (n-1)! en que q(x) tiene n-1 raíces, teniéndose $[E_o:E] \leq (n-1)!$

Ahora como cualquier raíz de p(x) es α o una raíz de q(x)
y $q(x) = (x-\alpha_1)(x-\alpha_2).....(x-\alpha_{n-1})C$
Luego $p(x) = (x-\alpha)(x-\alpha_1)(x-\alpha_2).....(x-\alpha_{n-1})C$
obteniéndose de esta manera en E todas las n raíces de p(x)
y tenemos además $[E:F] = [E:E_o][E_o:F]$

$$\leq (n-1)!\ n$$

$$= n!$$

por lo tanto $[E:F] \leq n!$

con lo que todas las partes del teorema han quedado demostradas.

BIBLIOGRAFIA

- FRANK A.

" Algebra Moderna, Teoría y Problemas"

Serie Schawn, McGraw-Hill Publicacionses USA 1965

- GARRET B. E SAUDERS M.

"Algebra Moderna"

Editorial Vicens-Vives,

Barcelona, 1953

- I.N. HERSTEIN

"Algebra Abstracta"

Grupo Editorial Iberoamericana, USA, 1986

- PIERRE SAMUEL

"Teoría Algebraica de Números"

Omega, Barcelona, Colección Métodos

*****