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

SEMINARIO DE GRADUACION

T E O R I A   D E   G A L O I S

(Breve estudio)

DICIEMBRE DE 1977

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA.

UNIVERSIDAD DE EL SALVADOR

RECTOR	HONORABLE CONSEJO DE ADMINISTRACION PROVISIONAL DE LA UNIVERSIDAD DE EL SALVADOR.
SECRETARIO	Dr. EDMUNDO BARRERA RODRIGUEZ

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO	Arq. MANUEL ENRIQUE ALFARO
SECRETARIO	Ing. LUIS A. CARBAJAL VALDEZ

DEPARTAMENTO DE MATEMATICA

JEFE DEL DEPARTAMENTO	Ing. GABRIEL MELENDEZ MAYORGA

SEMINARIO DE GRADUACION

ASESOR *Lic. JOSE JAVIER RIVERA LAZO*

Trabajo desarrollado por

RAUL AGUILERA LIBORIO

previo a la opción de su

Título de

LICENCIADO EN MATEMATICA

I N D I C E

Página

****

I N T R O D U C C I O N

El presente trabajo no es Teoría de Galois en el sentido estricto de la palabra, es más bien un breve estudio de dicha Teoría.

Es así como el Capítulo I está formado sólo por conceptos elementales, siendo hasta en el Capítulo II que se estudia Teoría de Galois; para terminar en una aplicación de dicha Teoría en el Capítulo III.

Las proposiciones, definiciones y corolarios, no se han separado por Capítulos, sino que se numeran en forma correlativa.

CAPITULO I
CONCEPTOS ELEMENTALES

1- GRUPOS

Sea S un conjunto. Se llama ley de composición (de S en si mismo) a una aplicación

$$S \times S \longrightarrow S .$$

DEFINICION 1

Un monoide es un conjunto G, con una ley de composición asociativa, y que posee un elemento e llamado neutro, tal que $x\,e = e\,x = x$, para todo $x \in G$.

DEFINICION 2

Un grupo G es un monoide tal que para todo elemento $x \in G$, existe un elemento $x \in G$, para el cual

$$x\,y = y\,x = e$$

este elemento y se llama inverso de x.

El inverso es único, ya que si y' es también inverso de x,

$$y' = y'\,e = y'(x\,y) = (y'\,x)y = e\,y = y .$$

Un grupo G es abeliano si para cualesquiera $a, b \in G$; se cumple que $a\,b = b\,a$.

NOTACION

Representaremos el inverso de x por x^{-1} (ó por -x cuando la ley de composición es aditiva).

DEFINICION 3

Sean G, F grupos.

Un homomorfismo de grupos de G en F es una aplicación

$$f : G \longrightarrow F$$

tal que $f(xy) = f(x)\,f(y)$ para todo par $x, y \in G$.

Observamos que f aplica el elemento neutro de G en el de F, ya que

$$f(e) = f(e\,e) = f(e)\,f(e) .$$

Si $f : G \longrightarrow F$ es un homomorfismo de grupos entonces

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

ya que si e, e' son los respectivos elementos unidad de G, F

$$e' = f(e) = f(xx^{-1}) = f(x)\, f(x^{-1}) \; .$$

DEFINICION 4

Sean G, F dos grupos.

Un homomorfismo $f : G \longrightarrow F$ se llama isomorfismo si f es biyectiva, es decir si f es inyectiva y sobreyectiva.

Si $G = F$ entonces llamaremos al isomorfismo, automorfismo.

Sea G un grupo y S un subconjunto de G. Diremos que S engendra a G (ó que S es un conjunto de generadores de G) si todo elemento de G se puede expresar como producto de elementos de S ó de sus inversos.

DEFINICION 5

Un subconjunto H de un grupo G, es un subgrupo de G si respecto a la operación definida en G, H es un grupo.

PROPOSICION 1

Un subconjunto no vacío H del grupo G, es un subgrupo de G si y sólo si

i) Para a y b que pertenecen a H, tenemos que ab pertenece a H.

ii) Para un elemento a que pertenece a H, se cumple que a^{-1} pertenece también a H.

Prueba

($\Longrightarrow$) Trivial.

($\Longleftarrow$)

Como la ley asociativa es válida para G, es claro que -- también es válida para H.

Si $a \in H$, tenemos por ii) que $a^{-1} \in H$, luego por i) $a\,a^{-1} \in H$; pero $a\,a^{-1} = e$.

PROPOSICION 2

Si H es un subconjunto finito no vacío de un grupo G y H es cerrado respecto a la multiplicación, entonces H es un subgrupo de G.

Prueba

Sea $a \in H$, entonces

$$a^2 = a\,a \in H$$
$$a^3 = a^2 a \in H$$
$$\vdots$$
$$a^n = a^{n-1}\,a \in H\,.$$

Luego la colección infinita de elementos

$$a,\ a^2,\ a^3,\ \ldots,\ a^n,\ \ldots$$

debe estar contenida en H.

Por lo tanto debe haber repeticiones de elementos; es decir, para algunos enteros r, s con $r > s > 0$

$$a^r = a^s$$

entonces

$$a^{r-s} = e$$

ó sea que $e \in H$

$$e = a^{r-s} = a\,a^{r-s-1}$$

entonces

$$a^{r-s-1} \in H\,,$$

así

$$a^{-1} = a^{r-s-1}$$

de donde $a^{-1} \in H$.

DEFINICION 6

Sea G un grupo y H un subgrupo.

Una clase lateral izquierda de H en G es un subconjunto de G de la forma $a H$, para cierto elemento $a \in G$.

Un elemento de $a H$ recibe el nombre de representante de la clase $a H$.

La aplicación

$$\begin{aligned} * : H &\longrightarrow a H \\ x &\rightsquigarrow a x \end{aligned}$$

induce una biyección de H en $a H$. De lo que resulta que dos clases laterales izquierdas tienen el mismo cardinal, es decir el -- mismo número de elementos.

Si a y b son elementos de G y las clases $a H$ y $b H$ tienen un elemento común, $a H$ y $b H$ coinciden. En efecto, sea

$$a x = b y \qquad \text{con } x, y \in H$$

$$a = b y x^{-1}$$

pero $y x^{-1} \in H$ y por lo tanto

$$a H = b(y x^{-1}) H = b H$$

ya que para todo $z \in H$, tenemos que $z H = H$.

DEFINICION 7

Si H es un subgrupo de G, el índice de H en G es el número de distintas clases laterales derechas de H en G.

Como cualquier $a \in G$ está en una única clase lateral, las clases laterales izquierdas (ó derechas) saturan a G. Luego si n representa el número de distintas clases laterales de H en G, debemos tener que

$$n \cdot o(H) = o(G) \qquad\qquad o(H) = \text{orden de } H.$$

Tenemos así que si G es un grupo finito

$$\text{índice de } H \text{ en } G = \frac{o(G)}{o(H)} \quad .$$

DEFINICION 8

Un subgrupo N de G decimos que es un subgrupo normal de G, si para todo $x \in G$ y todo $n \in N$, $x\, n\, x^{-1} \in N$.

PROPOSICION 3

N es un subgrupo normal de G si y sólo si

$$a N a^{-1} = N \quad \text{para todo} \quad a \in G .$$

Prueba

($\Longrightarrow$)

Para $a \in G$, tenemos

$$a N a^{-1} \subset N$$

como $a^{-1} \in G$, entonces

$$a^{-1} N (a^{-1})^{-1} \subset N$$

y como

$$a^{-1} N (a^{-1})^{-1} = a^{-1} N a , \qquad \text{entonces}$$

$$a^{-1} N a \subset N .$$

Tenemos así que

$$N = a (a^{-1} N a) a^{-1} \subset a N a^{-1} \subset N$$

luego

$$N = a N a^{-1} .$$

($\Longleftarrow$)

Si $a N a^{-1} = N$, para todo $a \in G$, entonces

$$a N a^{-1} \subset N$$

por lo tanto N es normal en G.

PROPOSICION 4

El subgrupo N de G es un subgrupo normal de G, si y sólo si toda clase lateral izquierda de N en G es una clase lateral derecha de N en G.

Prueba

Por la proposición 3, sabemos que $a N a^{-1} = N$ para todo $a \in G$. Luego

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

$$a N = N a .$$

($\Longleftarrow$)

Supongamos que toda clase lateral izquierda de N en G es una clase lateral derecha de N en G. Como

$$a = a e \in a N$$

cualquiera que sea la clase lateral derecha que resulte ser $a N$, debe contener a a pero a está en la clase lateral derecha $N a$ y dos clases laterales derechas (ó izquierdas) distintas no tie-- nen elementos en común, luego

$$a N = N a$$

$$a N a^{-1} = N a a^{-1} = N .$$

PROPOSICION 5

Si un subgrupo N de G, es un subgrupo normal de G entonces el producto de dos clases laterales derechas de N en G es de nuevo una clase lateral derecha de N en G.

Prueba

Sean $N a$ y $N b$ dos clases laterales derechas de N en G, entonces

$$\begin{aligned} N a N b &= N(a N) b \\ &= N(N a) b \\ &= N N a b \\ &= N a b . \end{aligned}$$

NOTACION

Representaremos por $\frac{G}{N}$ el conjunto de clases laterales del subgrupo normal N en G, es decir que

$$\frac{G}{N} = \{ N a \mid a \in G \} .$$

El conjunto $\frac{G}{N}$ cumple ser un grupo para la operación -- producto que definimos $N a N b = N a b$, a este grupo le llamaremos, el grupo cociente de G por N.

La aplicación

$$\alpha : G \longrightarrow \frac{G}{N}$$

$$x \rightsquigarrow \alpha(x) = N x$$

cumple ser un homomorfismo sobreyectivo.

DEFINICION 9

El núcleo del homomorfismo $\alpha : G \longrightarrow H$, del grupo G en el grupo H, es el conjunto

$$N = \{ x \in G \mid \alpha(x) = e, \text{ e identidad de } H \} .$$

PROPOSICION 6

Si $\alpha : G \longrightarrow H$ es un homomorfismo sobreyectivo de núcleo K, entonces K es un subgrupo normal de G.

Prueba

i) Si $x, y \in K$, tenemos que
$\alpha(xy) = \alpha(x)\ \alpha(y) = e\ e = e$, donde e es la identidad de H
por lo tanto $x\,y \in K$.
Además
$$\alpha(x^{-1}) = (\alpha(x))^{-1} = e^{-1} = e ,$$
así $x^{-1} \in K$.

ii) Sea $a \in G$ y $x \in K$
$$\alpha(a\ x\ a^{-1}) = \alpha(a)\ \alpha(x)\ \alpha(a^{-1})$$

$$= \alpha(a) \ e \ (\alpha(a))^{-1}$$
$$= e \ .$$

PROPOSICION 7

Si α es un homomorfismo sobreyectivo de G sobre H con núcleo K, entonces $\frac{G}{K}$ es isomórfico con H.

Prueba

Sea

$$\lambda : \frac{G}{K} \longrightarrow H$$

$$K\,a \rightsquigarrow \lambda(K\,a) = \alpha(a) \ .$$

i) Si $K\,a = K\,b$, entonces $a = k\,b$, con $k \in K$

como $a = k\,b$

$$\alpha(a) = \alpha(k\,b) = \alpha(k)\,\alpha(b) = \alpha(b).$$

ii) Para $x \in H$, $x = \alpha\,(a)$; $a \in G$

$$x = \alpha\,(a) = \lambda(K\,a) \ .$$

iii)
$$\begin{aligned} \lambda(K\,a\,K\,b) &= \lambda(K\,a\,b) \\ &= \alpha(a\,b) \\ &= \alpha(a)\,\alpha(b) \\ &= \lambda(K\,a)\,\lambda(K\,b). \end{aligned}$$

iv) Para probar que λ es inyectiva es suficiente demostrar que el núcleo es igual a la identidad del conjunto de partida

$$\lambda(K\,a) = e \qquad e \text{ identidad en } H$$

$$\alpha(a) = e \ .$$

Por lo tanto a está en el núcleo de α, ó sea, en K; pero esto implica que $K\,a = K$ y ya sabemos que K es la identidad de $\frac{G}{K}$.

DEFINICION 10

Sea S un conjunto que posee n elementos.

Llamaremos grupo simétrico de grado n y lo denotaremos S_n, al conjunto de todas las aplicaciones biyectivas del conjunto S sobre si mismo.

2- ANILLOS E IDEALES

DEFINICION 11

Una terna $(R, +, .)$ es un anillo si

i) R es un conjunto (no vacío).

ii) $(R, +)$ es un grupo conmutativo.

iii) $(R, .)$ es un semigrupo.

iv) Para a, b, c que pertenecen a R, tenemos

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

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

El anillo se llamará conmutativo si para cualesquiera elementos a, b en R, se cumple $a \cdot b = b \cdot a$.

DEFINICION 12

Si A es un anillo conmutativo, entonces $0 \neq a \in A$ decimos que es un divisor de cero si existe un $b \in A$, $b \neq 0$, tal que $a\, b = 0$.

DEFINICION 13

Un anillo R con elemento unidad, se llama anillo unitario.

DEFINICION 14

Un anillo conmutativo unitario es un dominio entero si no tiene divisores de cero.

DEFINICION 15

Un anillo recibe el nombre de anillo con división si sus elementos distintos de cero forman un grupo bajo la multiplicación.

DEFINICION 16

Un campo es un anillo conmutativo con división.

DEFINICION 17

Un ideal I a la izquierda en un anillo A, es un subgrupo del grupo aditivo de A, tal que para $i \in I$ y $a \in A$, $a\,i \in I$.

Si $i\,a \in I$ entonces decimos que I es un ideal a la derecha y si tanto $a\,i$ como $i\,a$ están en I, entonces diremos -- simplemente que I es un ideal de A.

DEFINICION 18

Llamaremos ideales principales de A, a los ideales de la forma $(a) = \{\, x\,a \mid x \in A \,\}$.

DEFINICION 19

Una aplicación α del anillo A en el anillo R decimos que es un homomorfismo si

i) $\alpha(a + b) = \alpha(a) + \alpha(b)$

ii) $\alpha(a\ \ b) = \alpha(a)\ \ \alpha(b)$ para $a, b \in A$.

PROPOSICION 8

Sean A y R anillos y α un homomorfismo sobreyectivo de A sobre R de núcleo K. Entonces R es isomorfo a $\frac{A}{K}$, donde $\frac{A}{K} = \{\, a + K \mid a \in A \,\}$.

Además hay una correspondencia biyectiva entre el conjunto de ideales de R y el conjunto de ideales de A que contienen a K. Esta correspondencia puede obtenerse asociando a cada ideal J en R, el ideal I de A definido por $I = \{\, x \in A \mid \alpha(x) \in J \,\}$. Con I así definido $\frac{A}{I}$ es isomorfo a $\frac{R}{J}$.

Prueba

1) Sea $\phi : \frac{A}{K} \longrightarrow R$

$a+K \rightsquigarrow \alpha(a)$.

i) $a + K = b + K \Longrightarrow a = b + k , \quad k \in K$

$$\alpha(a) = \alpha(b + k) = \alpha(b) + \alpha(k) = \alpha(b)$$

es decir que $\phi(a + K) = \phi(b + K)$

ii) $\Phi((a + K) + (b + K)) = \phi((a + b) + K)$

$= \alpha(a + b)$

$= \alpha(a) + \alpha(b)$

$= \phi(a + K) + \phi(b + K)$.

iii) $\phi((a + K)(b + K)) = \phi((a\,b) + K)$

$= \alpha(a\,b)$

$= \alpha(a)\,\alpha(b)$

$= \phi(a + K)\,\phi(b + K)$.

iv) $x \in R \Longrightarrow x = \alpha(a) \quad , \quad a \in A.$

$x = \alpha(a) = \phi(a + K)$.

v) $\phi(a + K) = e \quad , \quad e$ identidad en R

$\alpha(a) = e$

$\Longrightarrow \quad a \in K$

$\Longrightarrow \quad a + K = K$.

2) $J \rightsquigarrow I = \{ x \in A \mid \alpha(x) \in J \}$.

i) Probaremos que I es un ideal de A.
Sea $a \in A$; $i \in I \Longrightarrow a\,i \in A$.
Además $\alpha(a\,i) = \underset{\in R}{\alpha(a)}\ \underset{\in J}{\alpha(i)} \in J$

Para que I sea ideal bastará que sea cerrado para la suma

$a \in I \Longrightarrow a \in A \quad y \quad \alpha(a) \in J$

$b \in I \Longrightarrow b \in A \quad y \quad \alpha(b) \in J$

$(a+b) \in A \quad y \quad (\alpha(a) + \alpha(b)) \in J$

$\alpha(a + b) \in J$

$\Longrightarrow \quad (a + b) \in I$.

Por lo tanto I es un ideal de A.

ii) Veremos si $K \subset I$.

$$k \in K \Longrightarrow \alpha(k) = 0.$$

Como J es un grupo $0 \in J$, es decir $\alpha(k) \in J$ y como $k \in A$, tenemos que $k \in I$, ó sea $K \subset I$.

iii) Sea L un ideal de A tal que $K \subset L$ y sea $J = \{ r \in R \mid r = \alpha(\ell), \ \ell \in L \}$

Tenemos para $j \in J$ y $g \in R$ que $j\, g \in R$.
Además

$$\begin{aligned} j\, g &= \alpha(\ell)g \quad \text{para algún } \ell \in L \\ &= \alpha(\ell)\, \alpha(a) \quad \text{para algún } a \in A \\ &= \alpha(\ell a) \quad \text{con } \ell a \in L \end{aligned}$$

por lo tanto $j\, g \in J$, es decir J cumple ser un ideal de R.

iv) Para probar la sobreyectividad de la función que hemos de_ finido, veremos que todo ideal L de A tal que $K \subset L$, es de la forma $I = \{ x \in A \mid \alpha(x) \in J \}$.

Sea $i \in I$, entonces $\alpha(i) \in J$.
Por la definición de J, $\alpha(i) = \alpha(\ell)$ para algún $\ell \in L$ por lo tanto

$$\begin{aligned} \alpha(i) - \alpha(\ell) &= e \\ \alpha(i - \ell) &= e \\ \Longrightarrow (i - \ell) &\in K \subset L \\ \Longrightarrow i &\in K \subset L \\ \Longrightarrow i &\in L\,. \end{aligned}$$

Sea $\ell \in L$, entonces $\ell \in A$, además $\alpha(\ell) = r$ para algún $r \in R$, por ser α sobreyectiva, es decir $\ell \in I$.

v) La inyectividad es trivial.

3) Para probar que $\frac{A}{I} \simeq \frac{R}{J}$, bastará demostrar que $\Psi : A \longrightarrow \frac{R}{J}$ es un homomorfismo sobreyectivo y luego aplicar la primera parte del teorema

$$\Psi : A \longrightarrow \frac{R}{J}$$
$$a \rightsquigarrow \alpha(a) + J .$$

i) Para $m \in R$, existe $a \in A$ tal que $\alpha(a) = m$, es decir para $\alpha(a) + J$, existe $a \in A$ tal que $\Psi(a) = \alpha(a) + J$.

ii) $$\begin{aligned} \Psi(a + b) &= \alpha(a + b) + J \\ &= (\alpha(a) + J) + (\alpha(b) + J) \\ &= \Psi(a) + \Psi(b) . \end{aligned}$$

iii) $$\begin{aligned} \Psi(a\, b) &= \alpha(a\, b) + J \\ &= (\alpha(a) + J)\ (\alpha(b) + J) \\ &= \Psi(a)\ \ \Psi(b) \end{aligned}$$

iv) Probaremos que $I =$ núcleo de Ψ .

$$\begin{aligned} i \in I &\Longrightarrow \alpha(i) \in J \\ &\Longrightarrow \Psi(i) = \alpha(i) + J = J \\ &\Longrightarrow i \in \text{Núcleo} \\ &\Longrightarrow I \subset N . \end{aligned}$$

Además si $n \in N$, tenemos que

$$\Psi(n) = 0$$
$$\alpha(n) + J = 0$$
$$\begin{aligned} &\Longrightarrow \alpha(n) \in J \\ &\Longrightarrow n \in I \\ &\Longrightarrow N \subset I . \end{aligned}$$

$$\therefore I = N , \text{ luego } \frac{A}{I} \simeq \frac{R}{J} .$$

PROPOSICION 9

Si I es un ideal del anillo R, entonces

$$\alpha : R \longrightarrow \frac{R}{I}$$

$$x \rightsquigarrow x + I$$

es un homomorfismo sobreyectivo con núcleo I.

Prueba

trivial.

DEFINICION 20

Sea I un ideal en un anillo R. Diremos que I es un ideal maximal si $I \neq R$ y si no hay un ideal $M \neq R$ que contenga a I y sea distinto de I.

PROPOSICION 10

Sea A un anillo conmutativo con elemento unitario cuyos únicos ideales son (0) y el mismo A. Entonces A es un campo.

Prueba

Sea $0 \neq a \in A$.

Consideremos el conjunto $Aa = \{ x a \mid x \in A \}$.

Si $m, n \in Aa$ entonces

$$m = x_1 a \qquad x_1 \in A$$

$$n = x_2 a \qquad x_2 \in A$$

$$m + n = x_1 a + x_2 a = (x_1 + x_2)a \in Aa$$

también

$$- m = -x_1 a = (-x_1)a \in Aa .$$

Luego Aa es un subgrupo aditivo de A.

Además para $y \in A$ tenemos que

$$ym = y(x_1 a) = (yx_1)a \in Aa .$$

Por lo tanto Aa es un ideal de A.

Tenemos entonces por hipótesis que $Aa = (0)$ ó $Aa = A$

como $0 \neq a = 1a \in Aa$

afirmamos que $Aa \neq (0)$ y que $Aa = A$.

Por lo tanto todo $y \in A$ se puede expresar

$$y = x\,a \quad \text{con} \quad x \in A$$

como $1 \in A$, debe existir un $b \in A$ tal que $a\,b = 1$.

PROPOSICION 11

Si A es un anillo conmutativo con elemento unidad y I es un ideal de A, entonces I es un ideal maximal de A si y solo si $\frac{A}{I}$ es un campo.

Prueba

($\Longrightarrow$)

I es un ideal maximal de A; pero por las proposiciones 8 y 9, existe una correspondencia biyectiva entre el conjunto de ideales de A que contienen a I y el conjunto de ideales de $\frac{A}{I}$ por lo que $\frac{A}{I}$ sôlo puede tener 2 ideales, (0) y êl mismo.

Ademâs $\frac{A}{I}$ es conmutativo y posee un elemento unidad, ya que A posee esas dos propiedades.

Luego por la proposiciôn 10 concluimos que $\frac{A}{I}$ es un campo.

($\Longleftarrow$)

Si $\frac{A}{I}$ es un campo, tenemos para $(0) \neq I$ un ideal de $\frac{A}{I}$ que $I \subset \frac{A}{I}$.

Ademâs si $x \in \frac{A}{I}$, entonces $i\,x \in I$, con $i \in I$ asî

$$(i\,x)\,i^{-1} \in I$$

$$x \in I$$

de donde concluimos que los ûnicos ideales de un campo son (0) y êl mismo.

Por las proposiciones 8 y 9 existe una correspondencia biyectiva entre el conjunto de ideales de $\frac{A}{I}$ y el conjunto de ideales de A que contienen a I.

El ideal I de A se corresponde con el ideal (0) de $\frac{A}{I}$ y y el ideal A de A se corresponde con el ideal $\frac{A}{I}$ de $\frac{A}{I}$.

Por lo tanto no existe ideal entre I y A.

DEFINICION 21

Si $D \neq 0$ es un dominio de integridad contenido en un campo F, entonces

$$K = \{ a\, b^{-1} \mid a, b \in D,\ \ b \neq 0 \}$$

es el campo cociente o campo de cocientes de D en F.

PROPOSICION 12

Sean D y D' dominios de integridad isomórficos, con isomorfismo $\alpha : D \longrightarrow D'$, contenidos respectivamente en campos F y F' y sean K, K' los respectivos campos cocientes.

Entonces α puede ser extendido de una única manera a un isomorfismo $\alpha' : K \longrightarrow K'$.

Prueba

Si existe una extensión α' de α , entonces para cualquier $a\, b^{-1} \in K$, tenemos

$$\begin{aligned}\alpha'(a\, b^{-1}) = \alpha'(a)\, \alpha'(b^{-1}) &= \alpha'(a)\ \ \alpha'(b)^{-1}\\ &= [\alpha'(a)]\ [\alpha'(b)]^{-1}\\ &= [\alpha(a)]\ [\alpha(b)]^{-1}\end{aligned}$$

por lo que si α' existe debe ser única.

Sea $\alpha' : K \longrightarrow K'$

$$ab^{-1} \rightsquigarrow \alpha'(ab^{-1}) = \alpha(a)\ \ \alpha(b)^{-1} .$$

$$\begin{aligned} \text{i) } \alpha'(a\, b^{-1}) &= \alpha'(c\, d^{-1})\\ \alpha(a)\, \alpha(b)^{-1} &= \alpha(c)\, \alpha(d)^{-1}\\ \Longrightarrow \alpha(a)\, \alpha(d) &= \alpha(c)\, \alpha(b)\end{aligned}$$

$$\Longrightarrow \quad \alpha(a\,d) = \alpha(c\,b)$$

$$\Longrightarrow \quad a\,d = c\,b$$

$$\Longrightarrow \quad a\,b^{-1} = c\,d^{-1} \quad .$$

ii) Si $xy^{-1} \in K'$ $\Longrightarrow$ $x, y \in D'$

$$\Longrightarrow \quad x = \alpha(a) \qquad y = \alpha(b) \qquad a, b \in D$$

$$\Longrightarrow \quad \alpha'\,(a\,b^{-1}) = x\,y^{-1} \; .$$

iii) $\alpha'(a\,b^{-1} + c\,d^{-1}) = \alpha'\left[(a\,d + b\,c)(b\,d)^{-1}\right]$

$$= \alpha(a\,d + b\,c)\,\alpha(b\,d)^{-1}$$

$$= \left[\alpha(a)\,\alpha(d) + \alpha(b)\,\alpha(c)\right]\left[\alpha(b)^{-1}\,\alpha(d)^{-1}\right]$$

$$= \alpha(a)\,\alpha(b)^{-1} + \alpha(c)\,\alpha(d)^{-1}$$

$$= \alpha'(a\,b^{-1}) + \alpha'(c\,d^{-1}).$$

iv) $\alpha'\left[(a\,b^{-1})(c\,d^{-1})\right] = \alpha'\left[(a\,c)\,(b\,d)^{-1}\right]$

$$= \alpha(a\,c)\;\;\alpha(b\,d)^{-1}$$

$$= \alpha(a)\;\;\alpha(c)\,\alpha(b)^{-1}\,\alpha(d)^{-1}$$

$$= \alpha(a)\;\;\alpha(b)^{-1}\,\alpha(c)\,\alpha(d)^{-1}$$

$$= \alpha'(a\,b^{-1})\;\;\alpha'(c\,d^{-1}) \quad .$$

DEFINICION 22

Un dominio entero D es de características 0 si la relación $m\,a = 0$ donde $0 \neq a \in D$ y m es un entero , puede solamente verificarse si $m = 0$.

D es de característica finita si para algún $a \neq 0$ en D y algún entero $m \neq 0$, $m\,a = 0$. Definimos entonces la característica de D como el mínimo entero positivo P tal que $p\,a = 0$ para algún $a \neq 0$ en D.

PROPOSICION 13

Un anillo unitario F de característica 0 posee un número infinito de elementos.

Prueba

Sea $\beta : Z \longrightarrow F$

$$n \rightsquigarrow \beta(n) = n.1 = \overbrace{1 + 1 + \ldots\ldots. + 1}^{n \text{ veces}}$$

i) $n = m \Longrightarrow n . 1 = m . 1$

ii) $\beta(n) = \beta(m)$

$n . 1 = m . 1$

$(n-m)1 = 0$.

Como F es de característica 0, tenemos que

$$n - m = 0$$

$$n = m .$$

Existe por lo tanto una inyección entre Z y un subconjunto A de F; por lo tanto A es infinito, tenemos entonces que F es infinito.

PROPOSICION 14

Sea R un anillo conmutativo en donde todo ideal es principal, $a, b \in R$. Entonces existen $d, r, s \in R$ tal que d es un máximo divisor de a y b y $d = a r + b s$.

Prueba

Como R es un anillo de ideales principales, el ideal $[a, b]$ (generado por a y b) debe ser un ideal principal (d) para algún d en R.

Entonces

$$a = g d \quad y \quad b = h d$$

para algunos g, h en R y d es común divisor de a y b.

Como $d \in [a, b]$, entonces $d = a r + bs$ para r, s en R. Si d' es un común divisor de a y b, entonces

$$a = g' d' \quad y \quad b = h' d' \qquad \text{para } g', h' \text{ en } R$$

tenemos entonces que

$$d = g'd'r + h'd's = d'(g'r + h's)$$

luego $d' \mid d$.

DEFINICION 23

Sea R un anillo conmutativo con unidad. Un elemento p de R es primo si siempre que p divide un producto a b de elementos de R, entonces p divide al menos uno de los dos.

DEFINICION 24

Para un anillo conmutativo R; un ideal P de R decimos que es un ideal primo de R si $a\,b \in P$, $a, b \in R$ implica que $a \in P$ ó $b \in P$. Esto es equivalente a decir que P es un ideal primo de R si $\frac{P}{R}$ es un dominio de integridad.

PROPOSICION 15

Si el ideal principal $I = (p)$ es primo, entonces p es primo.

Prueba

Sea $\frac{ab}{p} = r$ para algûn r

$\Longrightarrow$ $a\,b = p\,r$

$\Longrightarrow$ $a\,b \in I$ por ser I primo, tenemos que $a \in I$ ó $b \in I$.

Si $a \in I$,

$a = p\,k$

$\Longrightarrow$ p divide a "a"

de manera semejante para b.

PROPOSICION 16

Sea R un dominio de integridad de ideales principales. Si I es un ideal primo, entonces I es maximal.

Prueba

$I = (p)$ para algûn elemento primo $p \in R$.

Si a es cualquier elemento de R que no está en I, entonces el máximo común divisor de a y p es el elemento unidad e y por la proposición 14, tenemos que

$$e = r a + s p$$

para algunos $r, s \in R$.

Entonces

$$(e) = R \subseteq [a, I] \subseteq R$$

$\Longrightarrow$ $[a, I] = R$ y I es maximal.

3- ANILLO DE POLINOMIOS

DEFINICION 25

Sea F un campo. Llamaremos a

$$F[x] = \{ a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in F,\ i = 0,1,2,\dots,n \}$$

el anillo de polinomios sobre F.

Si $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$

$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$

definimos las operaciones suma y producto, así

$$f(x)+g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots.$$

$$f(x)g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \dots$$

$$= C_0X^0 + C_1X + \dots. + C_{n+m}X^{n+m}$$

donde

$$C_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-1} .$$

DEFINICION 26

Si en el polinomio $f(x) = a_0 + a_1x + \dots. + a_nx^n$, tenemos que $a_n \neq 0$, entonces diremos que $f(x)$ es de grado n; a_nx^n será llamado el término principal y a_n coeficiente principal.

El polinomio cero, es aquel en que todos sus coeficientes son cero.

Un polinomio $f(x) \in F[x]$ se llamará mónico si su coeficiente principal es la unidad.

PROPOSICION 17

Dados dos polinomios $f(x)$ y $g(x)$ de $F[x]$, con $g(x) \neq 0$, existen entonces dos polinomios $t(x)$ y $r(x)$ en $F[x]$ tales que

$$f(x) = t(x)\,g(x) + r(x) \qquad \text{donde } r(x) = 0$$
$$\text{ó grado } r(x) < \text{grado } g(x)$$

Prueba

Si grado $f(x)$ < grado $g(x)$, basta hacer $t(x) = 0$ y $r(x) = f(x)$, logrando entonces lo deseado, es decir

$$f(x) = 0g(x) + f(x).$$

Supongamos que

$$f(x) = a_0 + a_1 x + \dots + a_m x^m \qquad \text{con } a_m \neq 0$$

$$g(x) = b_0 + b_1 x + \dots + b_n x^n \qquad \text{con } b_n \neq 0 \text{ y } n \leq m$$

procederemos por inducción sobre el grado de $f(x)$.

Supongamos que el resultado es válido para cualquier polinomio de grado menor que m.

Sea

$$f_1(x) = f(x) - (a_m b_n^{-1})x^{m-n}\,g(x)$$

es claro que grado $f_1(x) \leq m - 1$, entonces tenemos por nuestra hipôtesis inductiva que

$$f_1(x) = t_1(x)\,g(x) + r(x)$$

donde grado $r(x) = 0$ ó grado $r(x)$ < grado $g(x)$ entonces

$$f_1(x) = t_1(x)\,g(x) + r(x)$$
$$= f(x) - (a_m b_n^{-1})\,x^{m-n}\,g(x)$$

así

$$f(x) = (t_1(x) + a_m b_n^{-1} x^{m-n})\ g(x) + r(x)$$

$$f(x) = t(x)\ g(x) + r(x) \qquad \text{con } t(x) = t_1(x) + a_m b_n^{-1} x^{m-n}\ .$$

Vemos que $t(x)$ y $r(x)$ pertenecen a $F[x]$ y además $r(x) = 0$ ó grado $r(x) <$ grado $g(x)$.

PROPOSICION 18

$F[x]$ es un anillo de ideales principales.

Prueba

Sea I un ideal de $F[x]$.

Si I consiste solamente del elemento 0, tenemos

$$I = (0) = \{\ p(x)0 \mid p(x) \in F[x]\ \}$$

Si $I \neq (0)$, entonces existe $p(x) \in F[x]$, $p(x) \neq 0$ tal que $p(x) \in I$.

Consideremos un polinomio $q(x) \in I$ de grado mínimo, tenemos entonces por la proposición 17 que existen polinomios $t(x), r(x) \in F[x]$ tal que

$$p(x) = t(x)\ q(x) + r(x)$$

donde $r(x) = 0$ ó grado $r(x) <$ grado $q(x)$.

Como $q(x) \in I$ e I es un ideal de $F[x]$, tenemos que

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

Como además $p(x) \in I$, entonces

$$[p(x) - t(x)\ q(x)] \in I$$

y como

$$r(x) = p(x) - t(x)\ q(x)$$

concluimos que $r(x) \in I$.

Si $r(x) \neq 0$, entonces grado $r(x) <$ grado $q(x)$ y esto contradice el hecho de que $q(x)$ es el polinomio de grado mínimo en I.

Por consiguiente $r(x) = 0$.

y

$$p(x) = t(x)\, q(x)\ .$$

Luego $F[x]$ es un anillo de ideales principales.

DEFINICION 27

Un polinomio $p(x)$ de $F[x]$ decimos que es irreducible sobre F, si siempre que $p(x) = q(x)\, t(x)$ entonces uno de los dos $q(x)$ ó $t(x)$ tiene grado cero.

PROPOSICION 19

Todo elemento en $F[x]$ ó es una constante en $F[x]$ ó puede escribirse como el producto de un número finito de elementos irreducibles de $F[x]$.

Prueba

Sea $f(x) \in F[x]$.

La prueba la haremos por inducción sobre el grado de $f(x)$.

Si el grado de $f(x)$ es 0, entonces $f(x)$ es constante. Supongamos que la proposición es cierta para los elementos $g(x) \in F[x]$ tal que grado $g(x) <$ grado $f(x)$.

Lo probaremos para $f(x)$.

Si $f(x)$ es irreducible sobre F no hay nada que probar.

Supongamos pues que

$$f(x) = q(x)\, r(x)$$

donde tanto $q(x)$ como $r(x)$ no son constantes.

Sabemos que

$$\text{grado } q(x) < \text{grado } (q(x)\, r(x)) = \text{grado } f(x)$$

y $$\text{grado } r(x) < \text{grado } (q(x)\, r(x)) = \text{grado } f(x)$$

entonces por la hipótesis inductiva, $q(x)$ y $r(x)$ pueden escribirse como un producto de factores irreducibles de $F[x]$, es decir

$$q(x) = m_1(x)\, m_2(x) \,\ldots\ldots\, m_n(x)$$

$$r(x) = K_1(x)\, K_2(x) \,\ldots\ldots\, K_s(x)$$

donde los $m_i(x)$ y los $K_j(x)$ son elementos irreducibles de $F[x]$. Por lo tanto

$$f(x) = q(x)\, r(x) = m_1(x)\, m_2(x) \,\ldots\, m_n(x)\, K_1(x)\, K_2(x) \,\ldots\, K_s(x)$$

y así $f(x)$ se descompone en factores irreducibles.

PROPOSICION 20

El ideal $A = (p(x))$ en $F[x]$ es un ideal maximal si y sólo si $P(x)$ es irreducible sobre F.

Prueba

($\Longrightarrow$)

Supongamos que $p(x)$ no es irreducible sobre F, entonces

$$p(x) = t(x)\, q(x)$$

con $t(x), q(x) \in F[x]$ y ni $t(x)$, ni $q(x)$ constantes.

Sea

$$I = (t(x))$$

entonces $p(x) \in I$, de modo que $(p(x)) \subset I$.

Además $I \neq F[x]$ y $(p(x)) \neq I$ ya que si $I = F[x]$, entonces $1 \in I$, de modo que

$$1 = r(x)\, t(x) \qquad \text{para algún } r(x) \in F[x]$$

entonces $t(x)$ sería de grado 0, lo que contradice la hipótesis.

Por otra parte si $(p(x)) = I$.

entonces

$$t(x) \in (p(x))$$

de donde

$$t(x) = r(x)\, p(x)$$

para algún $r(x) \in F[x]$,

luego

$$p(x) = r(x)\, q(x)\, p(x)$$

de donde $r(x)\, q(x) = 1$

pero entonces $q(x)$ es constante y esto es nuevamente contradicción.

Por lo tanto ni A, ni $F[x]$ son iguales a I y como $A \subset I$, entonces A no puede ser un ideal maximal de $F[x]$.

($\Longleftarrow$)

Sea U un ideal tal que

$$A = (p(x)) \subset U \subset F[x] \quad .$$

Por ser $F[x]$ un anillo de ideales principales

$$U = (q(x)) \qquad q(x) \in F[x] \; .$$

Como $p(x) \in A \Longrightarrow p(x) \in U$

$$\Longrightarrow p(x) = q(x)\, m(x)$$

como $p(x)$ es irreducible, $q(x)$ ó $m(x)$ es constante si $q(x)$ es constante, para el caso c, entonces

$$U = (q(x)) = (c)$$

luego para cualquier polinomio $f(x) \in F[x]$

$$f(x) = c^{-1} f(x)\, c \Longrightarrow f(x) \in U$$

$$\Longrightarrow F[x] \subset U$$

$$\Longrightarrow F[x] = U \; .$$

Si $m(x) = c$ constante

entonces

$$p(x) = q(x)\, c$$

$$\Longrightarrow c^{-1} p(x) = q(x)$$

$$\Longrightarrow q(x) \in (p(x))$$

$$\Longrightarrow U \subset A$$

$$\Longrightarrow A = U .$$

DEFINICION 28-A

Si $p(x) \in F[x]$, llamaremos raíz de $p(x)$ a un elemento r que pertenece a un campo que incluye a F, si $p(r) = 0$.

PROPOSICION 21

Si $p(x) \in F[x]$ y si K es un campo tal que $F \subset K$, entonces para cualquier elemento $b \in K$, $p(x) = (x-b)\, q(x) + p(b)$ donde $q(x) \in K[x]$ y donde grado $q(x)$ = grado $p(x) - 1$.

Prueba

Como $F \subset K$, $F[x] \subset K[x]$ de donde podemos considerar que $p(x) \in K[x]$.

Tenemos por la proposición 17 que

$p(x) = (x - b)\, q(x) + r(x)$ donde $q(x) \in K[x]$ y $r(x) = 0$ ó grado $r(x) <$ grado $(x - b)$.

Entonces $r(x) = 0$ ó grado $r(x) = 0$.

Como

$$p(x) = (x - b)\, q(x) + r(x)$$

$$p(b) = (b - b)\, q(b) + r(b)$$

luego

$$p(x) = (x - b)\, q(x) + p(b) .$$

COROLARIO 1

Si r es una raíz de $p(x) \in F[x]$, donde $F \subset K$ enton ces en $K[x]$, $(x - r)$ divide a $p(x)$.

Prueba

$$p(x) = (x - r)\, q(x) + p(r)$$

como

$$p(r) = 0$$

$$p(x) = (x - r)\, q(x)\ .$$

DEFINICION 28-B

El elemento $r \in K$ es una raíz de $p(x) \in F[x]$ de multiplicidad m si $(x - r)^m$ divide a $p(x)$ y $(x - r)^{m+1}$ no divide a $p(x)$.

PROPOSICION 22

Si $r_1, r_2, \ldots, r_k \in F$ son distintas raíces de $p(x) \in F[x]$, entonces $p(x)$ es divisible por el producto $(x - r_1)(x - r_2) \ldots (x - r_k)$.

Prueba

Por el corolario 1, sabemos que el resultado es válido para $k = 1$.

Procederemos por inducción sobre k.

Supongamos que el resultado es válido para $k = i - 1$, $i > 1$, de modo que

$$p(x) = (x - r_1)(x - r_2) \ldots (x - r_{i-1})\, q(x)$$

entonces

$$p(r_i) = (r_i - r_1)(r_i - r_2) \ldots (r_i - r_{i-1}) q(r_i) = 0$$

como las r_j son todas distintas y F no posee divisores de cero, tenemos que $q(r_i) = 0$, por lo tanto

$$q(x) = (x - r_i)\, h(x)$$

así

$$p(x) = (x - r_1)(x - r_2) \ldots (x - r_{i-1})(x - r_i)\, h(x).$$

PROPOSICION 23

Un polinomio $p(x)$ de grado n sobre un campo F tiene cuando más n raíces en cualquier campo extensión de F.

Prueba

Si $p(x)$ es de grado 1, entonces debe ser de la forma $ax + b$ donde a, b están en F y donde $a \neq 0$ cualquier r tal que $p(r) = 0$ debe implicar que

$$ar + b = 0 \text{ , es decir } r = -\frac{b}{a} .$$

O sea que $p(x)$ tiene la única raíz $-\dfrac{b}{a}$.

Supongamos que el resultado es válido 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 cualquier de F.

Si $p(x)$ no tiene ninguna raíz en K, entonces la proposición es cierta.

Supongamos que $p(x)$ tiene al menos una raíz $r \in K$ y que r es una raíz de multiplicidad m.

Como $(x - r)^m$ divide a $p(x)$, tenemos que $m \leq n$. Así

$$p(x) = (x - r)^m q(x) \qquad \text{donde } q(x) \in K[x]$$

con grado de $q(x) = n - m$.

Como $(x - r)^{m+1}$ no divide a $p(x)$, concluimos que $(x - r)$ no divide a $q(x)$, es decir que r no es raíz de $q(x)$.

Si $r_2 \neq r$ es una raíz en K de $p(x)$, entonces

$$0 = p(r_2) = (r_2 - r)^m \; q(r_2)$$

y como $(r_2 - r) \neq 0$ concluimos que $q(r_2) = 0$.

Es decir cualquier raíz de $p(x)$ en K distinta de r debe ser una raíz de $q(x)$.

Como $q(x)$ es de grado $n - m < n$, $q(x)$ tiene de acuerdo a nuestra hipótesis de inducción, cuando más $n - m$ raíces en K, que junto con la otra raíz r, contada m veces nos da que $p(x)$ tiene cuando más $m + (n - m) = n$ raíces en K.

DEFINICION 29

Un conjunto no vacío V decimos que es un espacio vectorial sobre un campo F si V es un grupo abeliano respecto a una operación que denotaremos +, y si para todo $a \in F$, $v \in V$ está definido un elemento, escrito como $a\,v$ de V, con las siguientes propiedades

1) $a(v + w) = a\,v + a\,w$

2) $(a + b)v = a\,v + b\,v$

3) $a(bv) = (ab)v$

4) $1\,v = v$.

DEFINICION 30

Si V es un espacio vectorial y si $v_1, v_2, \ldots, v_n$ están en V diremos que tales elementos son linealmente dependientes sobre F si existen elementos $a_1, a_2, \ldots, a_n$ en F no todos cero, tales que $a_1v_1 + a_2v_2 + \ldots. + a_nv_n = 0$.

Si los elementos $v_1, \ldots., v_n$ no son linealmente dependientes, entonces son linealmente independientes.

Un subconjunto B de un espacio vectorial V, se llama base de V, si B consiste en elementos linealmente independientes que generan a B.

PROPOSICION 24

Si $v_1, v_2, \ldots, v_n$ están en V, entonces ó son linealmente independientes o algún v_k es una combinación lineal de los que le preceden $v_1, v_2, \ldots, v_{k-1}$.

Prueba

Si $v_1, v_2, \ldots, v_n$ son linealmente independientes no hay nada que probar.

Supongamos que $a_1v_1 + \ldots + a_nv_n = 0$ donde no todos los a_i son cero.

Sea k el mayor entero para el que $a_k \neq 0$.

Como $a_i = 0$ para $i > k$

$$a_1v_1 + \ldots + a_kv_k = 0 \qquad \text{con } a_k \neq 0$$

luego

$$v_k = a_k^{-1}(-a_1v_1 - a_2v_2 - \ldots - a_{k-1}v_{k-1}$$

$$= (-a_k^{-1}a_1)v_1 + (-a_k^{-1}a_2)v_2 + \ldots + (-a_k^{-1}a_{k-1})v_{k-1} .$$

COROLARIO 2

Si $v_1, v_2, \ldots, v_n$ de V generan a W y si $v_1, \ldots, v_k$ son linealmente independientes, entonces podemos encontrar un subconjunto de $v_1, \ldots, v_n$ de la forma $v_1, \ldots, v_k, v_{i_1}, \ldots, v_{i_r}$ consistente de elementos linealmente independientes que generan también a W.

Prueba

Si $v_1, \ldots, v_n$ son linealmente independientes, no hay nada que probar.

Si $v_1, \ldots, v_n$ no son linealmente independientes, saquemos de este conjunto la primera v_j que sea combinación lineal de los -- elementos que la preceden.

Como $v_1, \ldots, v_n$ son linealmente independientes, $j > k$; el subconjunto

$$v_1, \ldots, v_k, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n \quad \text{tiene}$$

$n - 1$ elementos, por lo tanto el subespacio que generan está contenido en W; pero en realidad es igual a W, ya que para todo $m \in W$, m puede escribirse como una combinación lineal de $v_1, \ldots, v_n$; pero en esta combinación lineal podemos reemplazar v_j por una combinación lineal de $v_1, \ldots, v_{j-1}$. Entonces m es una combinación lineal de $v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n$. Continuando con este proceso, llegamos a un subconjunto $v_1, \ldots, v_k, v_{i_1}, \ldots, v_{i_r}$ que todavía generan a W; pero en el que no hay elemento que sea una combinación lineal de los - que le preceden. Entonces por la proposición 24, los elementos $v_1, \ldots, v_k, v_{i_1}, \ldots, v_{i_r}$ deben ser linealmente independientes.

PROPOSICION 25

Si $v_1, \ldots, v_n$ es una base de V sobre F y $w_1, \ldots w_m$ son elementos linealmente independientes de V, entonces $m \leq n$.

Prueba

Todo vector en V y, en particular w_m, es una combinación lineal de $v_1, \ldots, v_n$. Por lo tanto los vectores $w_m, v_1, \ldots, v_n$ son linealmente dependientes y generan a V.

Por lo tanto existe algún subconjunto propio de dicho conjunto;

$$w_m, v_{i_1}, \ldots, v_{i_k} \quad \text{con} \quad k \leq n - 1$$

que forma una base de V.

Para formar esta nueva base hemos cambiado un w por al menos un v_i.

Vemos que del conjunto $w_{m-1}, w_m, v_{i_1}, \ldots, v_{i_k}$ linealmente dependiente, podemos extraer, según el corolario 2, una base de la forma

$$w_{m-1}, w_m, v_{j_1}, \ldots, v_{j_s} \quad ; \quad s \leq n-2 .$$

Repitiendo este proceso llegaremos a obtener una base de V de la forma $w_2, \ldots, w_{m-1}, w_m, v_\alpha, v_\beta, \ldots$ Como w_1 no es una combinación lineal de $w_2, \ldots, w_{m-1}, w_m$ la anterior base debe incluir algún v.

Para llegar a esta base hemos introducido $m-1$ elementos w y en cada una de estas introducciones hemos eliminado al menos una v y sin embargo nos queda al menos una v, por lo tanto $m-1 \leq n-1$ luego $m \leq n$.

COROLARIO 3

Sea $c_1a_{i_1} + c_2a_{i_2} + \ldots + c_ra_{i_r} = 0 \quad i = 1, 2, \ldots n < r$ un sistema de n ecuaciones lineales homogéneas en r incógnitas con coeficientes a_{i_j} en un anillo de división D. Entonces existen elementos $c_1, c_2, \ldots, c_r$ en D no todos cero, que son una solución para este sistema de ecuaciones.

Prueba

Consideremos el espacio vectorial sobre D, cuya base es

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, \ldots, 0), \ldots e_r,$$
$$\ldots, \quad e_n = (0, \ldots, 0, 1).$$

Sea

$$y_i = a_{1_i}e_1 + a_{2_i}e_2 + \ldots + a_{n_i}e_n = (a_{1_i}, a_{2_i}, \ldots, a_{n_i})$$

tenemos que

$$c_1y_1 + c_2y_2 + \ldots + c_ry_r = 0$$

si y sólo si

$$c_1a_{i_1} + \ldots + c_ra_{i_r} = 0 \quad i = 1, 2, \ldots, n.$$

Pero si $r > n$, entonces $\{y_1, y_2, \ldots, y_r\}$ es linealmente dependiente y por lo tanto existen $c_1, c_2, \ldots, c_r$ en D no todos cero que satisfacen la ecuación.

CAPITULO II
EXTENSIONES DE CAMPOS

1- EXTENSIONES ALGEBRAICAS

DEFINICION 31

Si F es un subcampo de un campo K, entonces K es un campo extensión de F.

DEFINICION 32

Si M es algún conjunto de elementos de K, entonces por F(M) representaremos la intersección de todos los subcampos de K que contienen a F y M.

Si el conjunto M consta de un solo elemento c y $c \notin F$, entonces F(c) es una extensión simple de F.

Si tomamos los elementos de K que pueden expresarse en la forma $a_0 + a_1c + \ldots + a_nc^n$ con $a_i \in F$ y $n \geq 1$ como este es un elemento de K, puede multiplicarse por cualquier inverso (lo que se tomará como una división); siempre que sea distinto de cero.

Sea U el conjunto de todos los cocientes.

Claramente U contiene a F y c, es decir $F(c) \subset U$. Además cualquier subcampo de K que contiene a F y c debe ser cerrado respecto a la suma y la multiplicación; debe contener entonces todos los elementos $a_0 + a_1x + \ldots + a_nx^n$ para $a_i \in F$ cualesquiera.

Así F(c) debe contener todos esos elementos y por ser un subcampo de K, también debe contener a los cocientes de dichos -- elementos. Luego $U \subset F(c)$.

DEFINICION 33

Sea $r \neq 0$ un elemento de K.

K un campo extensión del campo F.

El elemento r es algebraico sobre F, si existen elementos $a_0, a_1, \ldots, a_n$ $(n \geq 1)$ de F, no todos iguales a cero, tales que $a_0 + a_1r + \ldots + a_nr^n = 0$.

PROPOSICION 26

Sea x una variable sobre F, entonces r es algebraico sobre F, si el homomorfismo

$$\alpha : F[x] \longrightarrow K \quad ; \quad K \text{ campo extensión de } F$$

que es la identidad sobre F y aplica x sobre r tiene un núcleo distinto de cero.

Prueba

Como

$$\text{Núcleo de } \alpha = \{ f \mid f(r) = 0 \} \neq 0$$

debe existir al menos un $f(x) \neq 0$ tal que $f(r) = 0$ es decir hay elementos a_0 , a_1 , ... , a_n no todos cero en F tal que

$$f(r) = a_0 + a_1 r + a_2 r^2 + \ldots + a_n r^n = 0 \quad .$$

DEFINICION 34

Si un elemento c no es algebraico sobre F, entonces es trascendental sobre F.

DEFINICION 35

El campo K es una extensión algebraica del campo F, si todo elemento de K es algebraico sobre F.

Si F(r) es una extensión simple de F, entonces F(r) es algebraica o trascendental de acuerdo a que el elemento r sea algebraico o trascendental.

Si por ejemplo Q es el campo de los números racionales, entonces $Q(\sqrt{2})$ es una extensión algebraica de Q, ya que $\sqrt{2}$ satisface $x^2 - 2 = 0$; mientras que $Q(\Pi)$ es una extensión trascendental de Q.

Es claro que todo campo es una extensión algebraica de él mismo.

PROPOSICION 27

Si M y N son dos partes cualesquiera del campo K, entonces $F(M \cup N) = F(M)(N) = F(N)(M)$.

Prueba

$F(M \cup N)$ es un campo que contiene a F y $M \cup N$, es decir contiene a F, M y N.

Como $F(M)$ es el menor campo que contiene a F y M entonces $F(M) \subset F(M \cup N)$. Por lo tanto $F(M \cup N)$ contiene a $F(M)(N)$.

Además $F(M)(N)$ es un campo que contiene a $F \cup M \cup N$ y por lo tanto contiene a $F(M \cup N)$.

PROPOSICION 28

Si K es una extensión de F y c un elemento de K trascendental sobre F. Entonces la extensión simple $F(c)$ $(c \notin F)$ es isomórfica a $F(x)$ (campo de todas las funciones racionales en la indeterminada x con coeficientes en F) y el isomorfismo α puede ser escogido de modo que F permanezca fijo para cada elemento, es decir $\alpha(m) = m$ para todo $m \in F$.

Prueba

Consideremos la función

$$\alpha : F[x] \longrightarrow F[c]$$

$$f(x) \rightsquigarrow \alpha(f(x)) = f(c).$$

i) Dos elementos distintos $f(x)$ y $g(x)$ de $F[x]$ no pueden tener la misma imagen bajo α puesto que si así fuera, tendríamos

$$f(c) = g(c) \Longrightarrow f(c) - g(c) = 0$$

lo que implicaría que c es algebraico sobre F, y esto contradice nuestra hipótesis. Por lo tanto α es inyectiva.

ii) Para $f(c) = a_0 + a_1c + a_2c^2 + \dots + a_nc^n$ que pertenece a $F[c]$ existe $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ tal que $\alpha(f(x)) = F(c)$.

Esta propiedad vale para todo c ya sea algebraico ó no.

iii) $\alpha(f(x) + g(x)) = \alpha((f + g)(x)) = (f + g)(c)$

$$= f(c) + g(c)$$

$$= \alpha(f(x)) + \alpha(g(x)).$$

iv) $\alpha(f(x)g(x)) = f(c)g(c) = \alpha(f(x))\alpha(g(x))$.

Luego α es un isomorfismo.

Como para $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ en $F[x]$, se tiene $\alpha(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1c + \ldots + a_nc^n$ vemos que el elemento a_0 se mantiéne sin variación, luego si el polinomio está constituido sólo por el elemento $a \in F$, entonces $\alpha(a) = a$ para todo $a \in F$.

Por la proposición 12 el isomorfismo α entre los dominios de integridad $F[x]$ y $F[c]$ puede ser extendido únicamente al isomorfismo

$$\alpha_1 : F(x) \longrightarrow F(c)$$

considerados $F(x)$ y $F(c)$ como campos cocientes.

PROPOSICION 29

Sea r un elemento del campo K, algebraico sobre el campo F, siendo K un campo extensión de F. Entonces $F(r) = F[r]$ y es isomórfico a $\dfrac{F[x]}{(p(x))}$, donde $p(x)$ es el único polinomio mónico irreducible, teniendo r como una raíz (en K).

r es una raíz de un polinomio $g(x)$ en $F[x] \Longleftrightarrow g(x)$ es divisible en $F[x]$ por $p(x)$.

Prueba

Consideremos la función

$$\alpha : F[x] \longrightarrow F[r]$$

$$f(x) \rightsquigarrow f(r)$$

α cumple ser un morfismo sobreyectivo.

Si N es el núcleo de α, entonces por la proposición 8 vemos que $\dfrac{F[x]}{N}$ y $F[r]$ son isomórficos.

Como sabemos que r es algebraico sobre F, entonces N no puede constar sólo del elemento 0, además no puede ser que $N = F[x]$ ya que si ese fuera el caso $F[r]$ constaría sólo del elemento 0, lo que no puede ser porque $r \neq 0$ y $r \in F[r]$.

Por lo tanto N es un ideal propio de $F[x]$.

Como $F[x]$ es un dominio de integridad en donde todo ideal es principal, N debe ser un ideal principal, es decir $N = (p(x))$.

Como el anillo $F[r]$ es un subconjunto del campo F(r), entonces $F[r]$ es un dominio de integridad.

Además como $\dfrac{F[x]}{N}$ y $F[r]$ son isomórficos, entonces $\dfrac{F[x]}{N}$ cumple ser un dominio de integridad, pero si $\dfrac{F[x]}{N}$ es un dominio de integridad, entonces N es un ideal primo y como $N = (p(x))$ entonces por las proposiciones 16 y 20 concluimos que p(x) es irreducible. F es un campo por lo que podemos escoger a p(x) mónico. Un elemento $g(x) \in F[x]$ tiene r como raíz si y sólo si $g(x) = p(x)q(x)$ para $q(x) \in F[x]$, es decir si y sólo si g(x) es divisible en $F[x]$ por p(x), entonces sí

m(x) es un polinomio mónico irreducible en $F[x]$ que tiene r como raíz, tenemos que p(x) y m(x) se dividen mutuamente, como ambos son mónicos, esto es posible sólo si p(x) = q(x), luego p(x) es único.

Como $F[x]$ es un dominio de integridad en donde todo ideal es principal y el ideal (p(x)) es primo, entonces tenemos por la proposición 16 que (p(x)) es maximal y por la proposición 11 afirmamos que $\dfrac{F[x]}{(p(x))}$ es un campo, luego $F[r]$ es un campo y como F(r) es el más pequeño campo que contiene a F y r concluimos que $F[r] = F(r)$.

DEFINICION 36

Para un elemento r algebraico sobre F, al único polinomio mónico irreducible $p(x)$ en $F[x]$ que tiene r como raíz le llamamos el polinomio mínimo de r sobre F y al grado de $p(x)$ le llamamos el grado de r sobre F.

PROPOSICION 30

Sean r y m dos raíces del polinomio $p(x)$, irreducible sobre el campo F. Entonces $F(r)$ y $F(m)$ son isomórficos bajo un isomorfismo tal que a m le corresponde r y todos los elementos de F permanecen fijos.

Prueba

Sean $f(r)$ en $F(r)$ y $f(m)$ en $F(m)$, con $\alpha(f(m)) = f(r)$ es decir que a un polinomio le corresponderá otro que tenga exactamente los mismos coeficientes.

Tenemos que cuando

$$f(r) = g(r)$$

$$f(r) - g(r) = 0$$

pero como ya vimos en la proposición 29, debe entonces cumplirse que $p(x)$ divide a $f(x) - g(x)$ lo que implica que

$$f(m) - g(m) = 0$$

$$f(m) = g(m)$$

por tanto cumple ser inyectiva la aplicación.

Las otras propiedades de un isomorfismo son triviales por la definición de $F(r)$ y $F(m)$.

PROPOSICION 31

Bajo las operaciones ordinarias del campo K, K es un espacio vectorial sobre F.

Prueba

Trivial.

DEFINICION 37

Considerando a K como espacio vectorial sobre F, diremos que K es una extensión finita ó infinita de F, según que la dimensión de este espacio vectorial sea finita o infinita.

NOTACION

Por $[K : F]$ denotaremos la dimensión de K como espacio vectorial sobre F.

PROPOSICION 32

Sea $K = F(r)$ una extensión simple algebraica del campo F, donde el polinomio mínimo de r sobre F es de grado n. Entonces $[K : F] = n$ y todo elemento de K puede ser representado únicamente en la forma

$$a_0 + a_1 r + \ldots + a_{n-1} r^{n-1} \qquad a_0, a_1, \ldots, a_{n-1} \in F.$$

Prueba

Lo único que necesitamos probar es que el conjunto $\{ 1, r, \ldots, r^{n-1} \}$ es una base de K sobre F.

Si $a_0 + a_1 r + a_2 r^2 + \ldots + a_{n-1} r^{n-1} = 0$

con $a_0, a_1, \ldots, a_{n-1} \in F$, es claro que $a_0 = a_1 = \ldots = a_{n-1} = 0$ ya que el polinomio mínimo satisfecho por r es de grado n y $a_0 + a_1 r + a_2 r^2 + \ldots + a_{n-1} r^{n-1}$ es de grado $n - 1$.

Además como r es de grado n sobre F, tenemos que para $k \geq n$; r^k debe ser una combinación lineal de $1, r, \ldots, r^{n-1}$, es decir que $\{ 1, r, \ldots, r^{n-1} \}$ es un conjunto generador linealmente independiente de K sobre F ó sea es una base.

PROPOSICION 33

Si K es una extensión finita de F, entonces K es algebraico sobre F.

Prueba

Sea $c \in K$, $c \neq 0$.

Las potencias de c : $1, c, c^2, \ldots, c^n, \ldots$ no pueden ser linealmente independientes sobre F para todo entero positivo n, pues si así fuera, la dimensión de K sobre F sería infinita. Existe pues un entero m tal que $1, c, c^2, \ldots, c^m$ son linealmente dependientes, es decir

$$a_0 + a_1 c + a_2 c^2 + \ldots + a_m c^m = 0$$

en donde no todos los a_i son iguales a cero.

PROPOSICION 34

Si F es un campo y $K \subset E$ son campos extensiones de F, se verifica que

$$[E : F] = [E : K][K : F].$$

Si $\{X_i\}_{i \in I}$ es una base de K sobre F.

$\{Y_j\}_{j \in J}$ es una base de E sobre K

entonces

$\{X_i Y_j\}_{(i,j) \in I \times J}$ es una base de E sobre F.

Prueba

Sea $z \in E$.

Por hipótesis existe un número finito de elementos ℓ_j distintos de cero, en K tales que

$$z = \sum_{j \in J} \ell_j Y_j .$$

Además, para cada $j \in J$ hay elementos $b_{ji} \in F$, casi todos cero, tales que

$$\ell_j = \sum_{i \in I} b_{ji} X_i$$

y, por tanto,

$$z = \sum_{j\in J} \sum_{i\in I} b_{j_i} X_i Y_j$$

tenemos así que $\{X_i Y_j\}$ es una familia de generadores de E sobre F, ya que $z \in E$ y $b_{j_i} \in F$.

Para que $\{X_i Y_j\}_{(i,j)\in I\times J}$ cumpla ser una base, falta probar que es linealmente independiente.

Sea $\{C_{i_j}\}$ una familia de elementos de F, casi todos nulos, tal que

$$\sum_{j\in J} \sum_{i\in I} C_{i_j} X_i Y_j = 0$$

entonces, para cada j,

$$\sum_{i\in I} C_{i_j} X_i = 0$$

ya que los elementos Y_j son linealmente independientes sobre K.

Como $\{X_i\}$ es una base de K sobre F, tenemos que $\{X_i\}$ es linealmente independiente, luego $C_{i_j} = 0$ para cada i.

Por lo tanto $\{X_i Y_j\}_{(i,j)\in I\times J}$ cumple ser una base de E sobre F.

COROLARIO 4

Si E es una extensión finita de F y si K es un subcampo de E que contiene a F, entonces

$$[K : F] \text{ divide a } [E : F] \text{ .}$$

De aquí concluimos que cuando $[E : F]$ es un número primo, no existe un campo entre E y F.

COROLARIO 5

La extensión E de F es finita si y sólo si E es finita sobre K y K es finita sobre F.

COROLARIO 6

Si E es una extensión de F de grado finito, un cuerpo intermedio K entre E y F, la relación $[E : F] = [K : F]$ es equivalente a $K = E$ y la relación $[E : K] = [E : F]$ es equivalente a $K = F$.

Prueba

Sabemos que $[E : F] = [E : K][K : F]$

como $[E : F] = [K : F]$

tenemos $[E : F] = [E : K][E : F]$

luego $[E : K] = 1 \Longrightarrow E = K.$

PROPOSICION 35

Si F(r) es una extensión finita de F, entonces el elemento r es algebraico sobre F.

Prueba

Sea F(r) una extensión finita de F, tal que

$$[F(r) : F] = n$$

consideremos los elementos

$$1, r, r^2, \ldots, r^n$$

todos están en F(r) y son en número de $n + 1$ y por lo tanto linealmente dependientes sobre F.

Hay por lo tanto elementos $b_0, b_1, \ldots, b_n \in F$ no todos 0 tales que

$$b_0 + b_1 r + b_2 r^2 + \ldots + b_n r^n = 0$$

luego r es algebraico sobre F y satisface el polinomio distinto de cero

$$p(x) = b_0 + b_1 x + \dots + b_n x^n \quad \text{con coeficientes en F.}$$

NOTACION

Siendo F un subcuerpo de K y $a_1, a_2, \dots, a_n$ elementos de K, representaremos por $F(a_1, a_2, \dots, a_n)$ el subcuerpo más pequeño de K que contiene a F y $a_1, a_2, \dots, a_n$.

Sus elementos son todos los cocientes

$$\frac{f(a_1, a_2, \dots, a_n)}{g(a_1, a_2, \dots, a_n)}$$

donde f y g son polinomios en n variables con coeficientes en F, siendo $g(a_1, a_2, \dots, a_n) \neq 0$.

DEFINICION 38

Decimos que el campo K es de generación finita sobre F si hay una familia finita de elementos $a_1, a_2, \dots, a_n$ de K tal que $K = F(a_1, a_2, \dots, a_n)$.

PROPOSICION 36

Si K es un campo extensión del campo F, con a, b que pertenecen a K, tenemos que $F(a, b) = (F(a))(b)$.

Prueba

$F \subset F(a)$.

$a \in F(a)$.

$b \in (F(a))(b)$.

$\Longrightarrow \quad F(a, b) \subset (F(a))(b)$

ya que $F(a, b)$ es el menor campo que contiene a F, a y b.

Además, para $m \in (F(a))(b)$, tenemos

$$m = f_0(a) + f_1(a)b + f_2(a)b^2 + \dots + f_n(a)b^n$$

por ser $F(a, b)$ un campo, cumple la propiedad de cláusura para las operaciones suma y producto, luego $m \in F(a, b)$

$\Longrightarrow$ $(F(a))(b) \subset F(a, b)$

por lo tanto $F(a, b) = (F(a))(b)$.

PROPOSICION 37

Si E es una extensión algebraica del campo K y si K es una extensión algebraica del campo F, entonces E es una extensión algebraica de F.

Prueba

Sea r un elemento cualquiera de E.

Por ser E una extensión algebraica de K, existen elementos $a , a , \ldots, a_n \in K$ tal que r satisface el polinomio $X^n + a_1X^{n-1} + \ldots + a_n$. Como $a_1, a_2, \ldots , a_n$ pertenecen a K y K es algebraico sobre F, entonces los elementos $a_i \in K$ $i = 1, 2, \ldots, n$; son algebraicos sobre F.

Por la proposición 32 tenemos que $[F(a_i) : F]$ es finita para cada $i = 1, 2, \ldots, n$ y siendo n un número natural conocido concluimos que

$$M = F(a_1, a_2, \ldots, a_n) = (F(a_1, a_2, \ldots, a_{n-1})(a_n))$$

es una extensión finita de F, ya que a_n es algebraico sobre F y con mayor razón lo es sobre $F(a_1, a_2, \ldots , a_{n-1})$.

Como r satisface el polinomio $X^n + a_1X^{n-1} + \ldots + a_n$ y sabemos que $a_1, a_2, \ldots, a_n \in M$ concluimos que r es algebraico sobre M, pero entonces por la proposición 32 tenemos que M(r) es una extensión finita de M.

Como $[M : F]$ y $[M(r) : M]$ son finitos, también lo es $[M(r) : M][M : F]$.

Tenemos entonces por la proposición 32 que $[M(r) : F]$ es finita y como $[M(r) : F] = [M(r) : F(r)][F(r) : F]$. Concluimos que $[F(r) : F]$ es finita y por la proposición 33 afirmamos que r es algebraica sobre F.

2- CAMPOS DE DESCOMPOSICION

DEFINICION 39

Sea p(x) un polinomio sobre el campo F y K un campo extensión de F.

Decimos que p(x) se descompone en K si p(x) puede ser escrito como un producto de factores lineales sobre K; pero no en ningún subcampo propio de K, es decir si existen elementos $r_1, r_2, \ldots, r_n$ en K tal que $p(x) = a_n(x - r_1)(x - r_2)\ldots(x - r_n)$ donde a_n es el coeficiente principal de p(x) y tal que $K = F(r_1, r_2, \ldots, r_n)$ está engendrado por todas las raíces de p(x). K recibe el nombre de campo de descomposición de p(x).

PROPOSICION 38

Si p(x) es un polinomio en $F[x]$ de grado mayor ó igual a 1 y es irreducible sobre F, entonces p(x) tiene una raíz en un campo K extensión de F, tal que $[K : F]$ = grado de p(x).

Prueba

Sea $F[x]$ el anillo de polinomios en **x** sobre F y sea $I = (p(x))$ el ideal de $F[x]$ generado por p(x), tenemos por la proposición 20 que I es un ideal máximo de $F[x]$, entonces por proposición 11,

$$K = \frac{F[x]}{I}$$

es un campo.

i) K es una extensión de F.

Sea la función

$$\alpha : F[x] \longrightarrow \frac{F[X]}{I}$$

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

restringiendo α a F tenemos:

$$\alpha|_F : F \longrightarrow \overline{F} \text{ en donde } \overline{F} = \{a + I \mid a \in F\}.$$

Probaremos que α cumple ser un isomorfismo

$$\alpha|_F(a) = \alpha|_F(b)$$

$$a + I = b + I$$

$$\Longrightarrow a - b \in I.$$

Como los elementos de I son de la forma

$$a - b = q(x)\, p(x)$$

con grado $p(x) \geq 1$, esta igualdad puede darse sólo cuando $q(x) = 0$, es decir si

$$a - b = 0$$

luego $a = b$.

Sea $m \in \overline{F}$, entonces $m = a + I$, es decir existe $a \in F$ tal que $\alpha(a) = m$.

$$\begin{aligned} \alpha|_F(a + b) &= (a + b) + I \\ &= (a + I) + (b + I) \\ &= \alpha|_F(a) + \alpha|_F(b) . \end{aligned}$$

$$\begin{aligned} \alpha|_F(a\, b) &= a\, b + I \\ &= (a + I)(b + I) \\ &= \alpha|_F(a)\, \alpha|_F(b). \end{aligned}$$

Tenemos así que F y $\overline{F}$ son isomorfos, como además K es una extensión de $\overline{F}$, podemos considerar a K como una extensión de F, aunque en realidad no lo es.

Denotemos el elemento $\alpha(x) = x + I$ en el campo K por r. Dado $f(x) \in F[x]$, tenemos que si

$$f(x) = b_0 + b_1 x + \ldots + b_s x^s$$

entonces

$\alpha(f(x)) = \alpha(b_0) + \alpha(b_1)\ \alpha(x) + \dots + \alpha(b_s)\ \alpha(x^s)$

$\alpha(f(x)) = b_0 + b_1\alpha(x) + b_2\alpha(\ x^2\ ) + \dots + b_s\ \alpha(x^s)$

$\alpha(f(x)) = b_0 + b_1\alpha(x) + b_2(\alpha(x))^2 + \dots + b_s(\alpha(x))^s$

$\alpha(f(x)) = f(r)$

en particular como $p(x) \in I$

$$\alpha(p(x)) = 0 \quad \text{(cero del cociente)}$$

pero $\qquad \alpha(p(x)) = p(r)$

luego el elemento $\alpha\ (x) = r$ en K es una raíz de p(x).

Sabemos por la proposición 29 que F(r) y K son isomorfos.

Por la proposición 32, tenemos que

$$[F(r) : F] = n$$

donde n = grado del polinomio mínimo de r sobre F, luego, entonces

$$[K : F] = n\ .$$

COROLARIO 7

Si $p(x) \in F[x]$, entonces hay una extensión finita K de F en que p(x) tiene una raíz.

Además $[K : F] \leq$ grado $p(x)$.

Prueba

Basta que p(x) se exprese como un producto de factores irreducibles y apliquemos la proposición 38 a uno de los factores.

PROPOSICION 39

Sea $f(x) \in F[x]$ de grado $n \geq 1$. Entonces hay una extensión K de F de grado cuando más n! en que f(x) tiene a lo más n raíces.

Prueba

Según el corolario 7 hay una extensión K de F con $[K : F] \leq n$ en que f(x) tiene una raíz r.

Entonces en $K[x]$, f(x) se factoriza como $f(x) = (x - r)\, q(x)$ donde q(x) es de grado n - 1. Continuando con el mismo proceso anterior nos damos cuenta que hay una extensión E de K de grado menor o igual que $(n - 1)!$ en que q(x) tiene n - 1 raíces. Como cualquier raíz de f(x) es r ó una raíz de q(x), vemos que en E se encuentran todas las raíces de f(x). Además

$$[E : F] = [E : K][K : F] \leq (n - 1)!\, n = n!\ .$$

PROPOSICION 40

Cualquier polinomio p(x) sobre un campo F tiene un campo de descomposición K.

Prueba

Haremos la prueba por inducción sobre el grado de p(x). Si el grado de p(x) es 1, entonces la proposición no es más que una reafirmación del corolario 7.

Supongamos entonces que el resultado es válido para todo polinomio de grado menor que n.

Sea p(x) un polinomio de grado n.

Como n es mayor que 1, entonces p(x) debe tener algún factor irreducible f(x), entonces por el corolario 7, existe un campo extensión F(r) de F donde r es una raíz de f(x), por lo tanto p(x) tiene la raíz r en F(r) y por la proposición 20 tenemos que $p(x) = (x - r)\, q(x)$ con p(x) en $F(r)[x]$. Como el grado de q(x) es n - 1 tenemos por la hipótesis inductiva que existe un campo extensión

$$K = F(r)\,(r_2, r_3, \ldots, r_n)$$
$$= F(r, r_2, r_3, \ldots, r_n)$$

de $q(x)$ sobre $F(r)$, donde $r_2, r_3, \ldots, r_n$ son las raíces de $q(x)$.

Entonces en $K[x]$ tenemos

$$p(x) = (x - r)q(x) = (x - r)a_n(x - r_2) \ldots (x - r_n)$$

$$p(x) = a_n(x - r)(x - r_2) \ldots (x - r_n)$$

y tenemos así que K es el campo de descomposición de p(x).

PROPOSICION 41

Sea p(x) un polinomio sobre el campo F y sea $\overline{p}(x)$ el correspondiente polinomio sobre un campo isomórfico $\overline{F}$, con K y $\overline{K}$ los campos de descomposición de p(x) y $\overline{p}(x)$ respectivamente. Entonces el isomorfismo entre F y $\overline{F}$ puede ser extendido a los campor K y $\overline{K}$.

Prueba

$$\text{Sea } \Psi : F \longrightarrow \overline{F}$$

$$a \rightsquigarrow \overline{a}$$

tenemos así que

$$\Psi(p(x)) = \overline{p}(x)$$

es decir

$$\Psi(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) = \overline{a}_0 + \overline{a}_1x + \ldots + \overline{a}_nx^n .$$

Procederemos para la prueba por inducción sobre el grado $[K : F] = m$.

Si $m = 1$ el isomorfismo existe y es el mismo Ψ ya que entonces $K = F$.

Supongamos que el resultado es válido para p(x) sobre F y $\overline{p}(x)$ sobre $\overline{F}$ en donde K y $\overline{K}$ son sus respectivos campos de descomposición y el grado de p(x) y $\overline{p}(x)$ es menor que $m > 1$.

Como $[K : F] > 1$, concluimos de que no todas las raíces de p(x) están en F y por lo tanto debe existir un factor irreducible q(x) de p(x) sobre F de grado $d > 1$.

Sea $\overline{q}(x)$ el polinomio sobre $\overline{F}$ que corresponde a $q(x)$, - también el grado de $\overline{q}(x) = d$.

Sea además r una raíz de $q(x)$ y $\overline{r}$ una raíz de $\overline{q}(x)$, entonces K y $\overline{K}$ contienen a r y $\overline{r}$ respectivamente.

Definamos

$$\alpha : \quad F(r) \longrightarrow \overline{F}(\overline{r})$$
$$a_0 + a_1 r + \ldots + a_{d-1} r^{d-1} \rightsquigarrow \overline{a}_0 + \overline{a}_1 \overline{r} + \ldots + \overline{a}_{d-1} \overline{r}^{d-1}$$

Probaremos que α es un isomorfismo y para ello nos bastará que sea inyectiva ya que las demás condiciones son semejantes a las vistas en proposiciones anteriores.

$$\begin{aligned}
\overline{f}(\overline{r}) = \overline{g}(\overline{r}) &\Longrightarrow \overline{f}(\overline{r}) - \overline{g}(\overline{r}) = 0 \\
&\Longrightarrow \overline{q}(x) \text{ divide a } \overline{f}(x) - \overline{g}(x) \quad \text{(Prop. 27)} \\
&\Longrightarrow q(x) \text{ divide a } f(x) - g(x) \\
&\Longrightarrow f(r) - g(r) = 0 \\
&\Longrightarrow f(r) = g(r) .
\end{aligned}$$

Como K es un campo de descomposición de $p(x)$ sobre $F(r)$ y $[K : F(r)] = \frac{m}{d} < m$.

Además $\overline{K}$ es un campo de descomposición de $\overline{p}(x)$ sobre $\overline{F}(\overline{r})$ y $[\overline{K} : \overline{F}(\overline{r})] = \frac{m}{d} < m$.

Entonces por la hipótesis inductiva, el isomorfismo α que es una extensión de Ψ puede extenderse a un isomorfismo Ω entre K y $\overline{K}$.

Es claro que

$$\Omega\big|_{F(r)} = \alpha$$

$$\alpha\big|_{F} = \Psi .$$

PROPOSICION 42

Si el polinomio $f(x) \in F[x]$ tiene una raíz múltiple, entonces $f(x)$ y $f'(x)$ (la derivada de $f(x)$) tienen un factor común de grado positivo.

Prueba

Sea r una raíz múltiple de f(x), entonces

$$f(x) = (x - r)^n \ p(x) \qquad \text{donde} \quad n > 1$$

derivando esta igualdad tenemos

$$f'(x) = n(x - r)^{n-1}p(x) + (x - r)^n \ p'(x)$$

$$f'(x) = (x-r)\left[n(x-r)^{n-2}p(x) + (x-r)^{n-1} \ p'(x)\right]$$

Por lo tanto f(x) y f'(x) tienen a (x - r) como factor común.

COROLARIO 8

Para $f(x) \in F[x]$, irreducible, se cumple que si la característica de F es 0, entonces f(x) no tiene raíces múltiples.

Prueba

Por ser f(x) irreducible, sus únicos factores en $F[x]$ son 1 y f(x).

Supongamos que f(x) tiene una raíz múltiple, entonces por la proposición 42, f(x) y f'(x) deben tener un factor común de grado positivo y como f(x) es irreducible, debe cumplirse que

$$f(x) \mid f'(x)$$

pero como el grado de f'(x) es menor que el grado de f(x), esto sólo puede ser posible si $f'(x) = 0$ y como la característica de F es 0, entonces

$$f(x) = \text{constante}$$

y por lo tanto no tiene ninguna raíz, con lo que queda probado el corolario.

3- EXTENSIONES SEPARABLES

DEFINICION 40

El polinomio irreducible $p(x)$ en $F[x]$ es separable si no tiene raíces múltiples en su campo de descomposición, es decir, si al factor $p(x)$ sobre su campo de descomposición en factores de grado uno, no existen factores repetidos.

DEFINICION 41

Un polinomio arbitrario $f(x) \in F[x]$ es separable si cada uno de sus factores irreducibles es separable.

DEFINICION 42

Un elemento r, algebraico sobre F, es separable si su polinomio mínimo sobre F es separable. Una extensión algebraica K de F se llama separable sobre F si todos sus elementos son separables. Un elemento r algebraico sobre F decimos que es separable sobre F si F(r) es separable sobre F.

PROPOSICION 43

Si F es de característica 0, y si r, s son algebraicos sobre F, entonces existe un elemento t en F(r, s) tal que $F(r, s) = F(t)$.

Prueba

Sean $f(x)$ y $g(x)$, de grados m y n los polinomios irreducibles sobre F satisfechos por r y s respectivamente.

Sea K una extensión de F en que tanto $f(x)$ como $g(x)$ se descomponen completamente con

$$r = r_1 , r_2 , \ldots , r_m \quad y \quad s = s_1 , s_2 , \ldots , s_n$$

sus raíces respectivas, todas distintas por corolario 8.

Podemos escoger c en F tal que

$$t = r + cs \neq r_i + c s_j$$

es decir

$$c \neq \frac{r_i - r}{s - s_j}$$

para todo i y todo j mayores que 1. Como g(x) es irreducible y s es separable, tenemos la garantía de que $s - s_j \neq 0$, además por ser F de característica 0 tiene un número infinito de elementos. Los polinomios g(x) y f(t - cx) son satisfechos por s, considerando a g(x) y f(t - cx) como polinomios sobre F(t)[x] por lo que g(x) y f(t - cx) tienen un máximo común divisor h(x) que tiene a s como raíz. Pero g(x) y f(t - cx) no tienen otra raíz en común en ningún campo, ya que ninguna de las otras raíces de g(x); $s_2, s_3, \ldots, s_n$ es raíz de f(t - cx), por la escogencia de c entonces la única raíz de h(x) en cualquier campo, es la raíz simple s y h(x) debe por lo tanto ser de grado 1, es decir

$$h(x) = (x - s).$$

Así tenemos que $(x - s) \in F(t)[x]$, es decir $s \in F(t)$ y como $r = t - cs$, entonces $r \in F(t)$, es decir

$$F(r, s) \subset F(t)$$

y como $t = r + cs$, tenemos que $t \in F(r, s)$ ó sea $F(t) \subset F(r, s)$, así

$$F(r, s) = F(t).$$

DEFINICION 43

Diremos que un cuerpo K es algebraicamente cerrado si todo polinomio de K[x], de grado $n \geq 1$ tiene una raíz en K.

Observemos que si $p(x) \in K[x]$, entonces existe $a \in K$ tal que $p(a) = 0$, es decir

$$p(x) = (x - a)\, q(x)$$

donde q(x) es un polinomio en K[x], para el que a su vez existe $b \in K$ tal que $q(b) = 0$, ó sea

$$q(x) = (x - b)\, r(x)$$

si seguimos este razonamiento, nos damos cuenta que para un polinomio $p(x) \in K[x]$ todas sus raíces están en K.

Sea F un cuerpo y $\alpha : F \longrightarrow K$ un homomorfismo inyectivo de F en un cuerpo algebraicamente cerrado K. Analizaremos las extensiones de α a extensiones algebraicas E de F.

PROPOSICION 44

El número de posibles extensiones de α a F(r), donde r es algebraico sobre F, es menor o igual que el número de raíces del polinomio mónico irreducible de r sobre F, p(x), y es igual al número de raíces distintas de p(x).

Prueba

Sea b una raíz de $\alpha(p)$ en K.

Dado un elemento de $F(r) = F[r]$, podemos expresarlo en la forma f(r) para cierto polinomio $f(x) \in F[x]$.

Definamos una extensión de α aplicando

$$f(r) \rightsquigarrow (\alpha(f))(b)$$

veamos si está bien definida.

Si g(x) está en $F[x]$ y es tal que

$$g(r) = f(r)$$

$$\Longrightarrow g(r) - f(r) = 0$$

$$\Longrightarrow (g - f)(r) = 0$$

entonces por proposición 29, tenemos que p(x) divide a g(x) - f(x).

Por tanto $(\alpha(p))(x)$ dividirá a $(\alpha(g))(x) - (\alpha(f))(x)$ y $(\alpha(g))(b) = (\alpha(f))(b)$.

Esta aplicación es además un homomorfismo que induce α sobre F y es una extensión de α a F(r).

PROPOSICION 45

Sea F un cuerpo, E una extensión algebraica de F y $\alpha : F \longrightarrow K$ un homomorfismo inyectivo de F en un cuerpo algebraicamente cerrado K. Existe entonces una extensión de α a un homomorfismo inyectivo de E en K. Si E es algebraicamente cerrado y K es algebraico sobre $\alpha(F)$; toda extensión de este tipo de α es un isomorfismo de E en K.

Sea S el conjunto de todos los pares (L, τ), donde L es un subcuerpo de E que contiene a F, y τ , una extensión de α a un homomorfismo inyectivo de L en K.

Si (L, τ) y (L', τ') son dos de tales pares, escribiremos $(L, \tau) \leq (L', \tau')$ si $L \subset L'$ y $\tau'|_L = \tau$.

Observemos que S es no vacío ya que contiene al menos a (F, α).

Sea $\{(L_i , \tau_i)\}$ un subconjunto totalmente ordenado de S. Si hacemos $L = \cup L_i$ y definimos τ sobre L como igual a τ_i sobre cada L_i , tenemos que (L, τ) es un mayorante para el subconjunto totalmente ordenado, por lo tanto S es inductivo. Tenemos entonces por el lema de Zorn, que existe un elemento maximal (H, λ) de S, donde λ es una extensión de α.

Probaremos que $H = E$.

Si $H \neq E$, debe existir r en E, tal que r no pertenece a H, entonces por la proposición 44, el homomorfismo inyectivo λ tendría una extensión a H(r) lo que contradice el hecho de que (H, λ) es maximal. Por lo tanto existe una extensión de α a E.

Si E es algebraicamente cerrado, y K es algebraico sobre $\alpha(F)$, entonces $\lambda(E)$ es algebraicamente cerrado y K es algebraico sobre $\lambda(E)$, tenemos así que

$$K = \lambda(E)$$

ya que para $k \in K$, existen $\lambda(e_0), \lambda(e_1), \ldots, \lambda(e_n)$ en $\lambda(E)$ tal que $\lambda(e_0) + \lambda(e_1)k + \lambda(e_2)k^2 + \ldots + \lambda(e_n)k^n = 0$ y por ser $\lambda(E)$ algebraicamente cerrado $k \in \lambda(E)$.

COROLARIO 9

Sea F un cuerpo y E, H extensiones algebraicas de F.

Si E, H son algebraicamente cerrados, existe entonces un isomorfismo $\tau : E \longrightarrow H$ que induce la identidad sobre F.

Prueba

Sea $\alpha : F \longrightarrow H$

$a \rightsquigarrow a$

extendemos α al cuerpo E y aplicando el teorema tenemos el isomorfismo deseado.

DEFINICION 44

Una extensión algebraica y algebraicamente cerrada de F está determinada por un isomorfismo. Esta extensión se llama cláusura algebraica de F.

DEFINICION 45

Sea K una extensión algebraica de un cuerpo F, y sea

$$\alpha : F \longrightarrow L$$

un homomorfismo inyectivo de F en un cuerpo algebraicamente cerrado, L. Con L cláusura algebraica de $\alpha(F)$.

Sea S_α el conjunto de extensiones de α a un homomorfismo inyectivo de E en L.

Sea H otro cuerpo algebraicamente cerrado y

$$\tau : F \longrightarrow H$$

un homomorfismo inyectivo, con H una cláusura algebraica de $\tau(F)$.

Por la proposición 45, existe un isomorfismo

$$\lambda : L \longrightarrow H$$

que extiende la aplicación $\tau_{\,o}\,\alpha^{-1}$ al cuerpo $\alpha(F)$.

Esto se aclara con el siguiente diagrama

$$\begin{tikzcd}
H \arrow[dd, dash] & & L \arrow[ll, "\lambda"'] \arrow[dd, dash] \\
 & E \arrow[ul, "\tau^*"'] \arrow[ur, "\alpha^*"] \arrow[d, dash] & \\
\tau(F) & F \arrow[l, "\tau"] \arrow[r, "\alpha"'] & \alpha(F)
\end{tikzcd}$$

Sea S_τ el conjunto de extensiones de τ a un homomorfismo inyectivo de E en H.

Si $\alpha^* \in S_\alpha$ es una extensión de α a un homomorfismo inyectivo de E en L, entonces $\lambda \circ \alpha^*$ será una extensión de τ a un homomorfismo inyectivo de E en H, ya que restringiendo α^* a F tenemos

$$\begin{aligned}
\lambda \circ \alpha^* &= \lambda \circ \alpha \\
&= \tau \circ \alpha^{-1} \circ \alpha \\
&= \tau .
\end{aligned}$$

Vemos entonces que λ induce una aplicación de S_α en S_τ.

Además si $\tau^* \in S_\tau$ con las mismas condiciones anteriores tenemos

$$\begin{aligned}
\lambda^{-1} \circ \tau^* &= \lambda^{-1} \circ \tau \\
&= \alpha \circ \tau^{-1} \circ \tau \\
&= \alpha .
\end{aligned}$$

Así λ^{-1} induce una aplicación de S_τ en S_α, por lo tanto S_α y S_τ están en biyección por la aplicación

$$\alpha^* \rightsquigarrow \lambda \circ \alpha^* \quad .$$

Tenemos así que el cardinal de S_α coincide con el cardinal de S_τ. Este cardinal que depende sólo de la extensión $\frac{E}{F}$, lo simbolizaremos por

$$[E : F]_s$$

y le llamaremos grado de separabilidad de E sobre F.

PROPOSICION 46

Sean $F \subset K \subset E$ cuerpos. Se tiene

$$[E : F]_s = [E : K]_s \, [K : F]_s \; .$$

Además, si E es finita sobre F, $[E : F]_s$ es finito y

$$[E : F]_s \leq [E : F]$$

el grado de separabilidad es a lo sumo igual al grado.

Prueba

Sea $\alpha : F \longrightarrow L$

un homomorfismo inyectivo de F en un cuerpo algebraicamente cerrado L.

Sea $\{\alpha_i\}_{i \in I}$ la familia de extensiones distintas de α a K y sea $\{\tau_{i_j}\}$ para cada i la familia de extensiones distintas de α_i a E.

Tenemos entonces que cada α_i tiene $[E : K]_s$ extensiones a homomorfismos inyectivos de E en L; el conjunto $\{\tau_{i_j}\}$ tiene $[E : K]_s \, [K : F]_s$ elementos.

En cuanto a los homomorfismos inyectivos de E en L sobre α, vemos que cualquiera de ellos debe ser uno de los τ_{i_j}, por lo tanto

$$[E : F]_s = [E : K]_s \, [K : F]_s \; .$$

Supongamos ahora que $\frac{E}{F}$ es finito.

Podemos obtener entonces E como una sucesión de extensiones, en la que cada componente está engendrado por un único elemento:

$$F \subset F(a_1) \subset F(a_1, a_2) \subset \ldots \subset F(a_1, a_2, \ldots a_r) = E \; .$$

Definamos inductivamente $K_{n+1} = K_n(a_{n+1})$, tenemos entonces por la proposición 44, que

$$[K_n(a_{n+1}) : K_n]_s \leq [K_n(a_{n+1}) : K_n] .$$

Resulta así que la desigualdad es cierta para cada componente de la sucesión; por la multiplicabilidad, vemos también que lo es para la extensión $\frac{E}{F}$.

COROLARIO 10

Sea E finita sobre F, y $F \subset K \subset E$. Se verifica la igualdad $[E : F]_s = [E : F]$ si y sólo si la igualdad correspondiente es válida para cada componente de la sucesión, es decir, para $\frac{E}{K}$ y $\frac{K}{F}$.

Prueba

($\Longrightarrow$)

$$[E : F]_s = [E : F]$$

$$[E : K]_s [K : F]_s = [E : K][K : F]$$

Si $[E : K]_s = [E : K]$ tenemos lo deseado

Si $[E : K]_s < [E : K]$

tendría que ser necesariamente

$$[K : F]_s > [K : F]$$

lo que es imposible, por lo tanto

$$[E : K]_s = [E : K]$$

$$[K : F]_s = [K : F] .$$

($\Longleftarrow$)

$$[E : K]_s = [E : K]$$

$$[K : F]_s = [K : F]$$

entonces

$$[E : F]_s = [E : F]$$

repetimos ahora la siguiente

DEFINICION 46

Sea K una extensión finita de F, diremos que K es separable sobre F si $[K : F]_s = [K : F]$.

PROPOSICION 47

Una extensión finita K de F es separable sobre F si y sólo si cada elemento de K es separable sobre F.

Prueba

Supongamos que K es separable sobre F y sea $r \in K$.

Consideremos

$$F \subset F(r) \subset K$$

tenemos por la proposición 46 que

$$[F(r) : F]_s = [F(r) : F]$$

de donde concluimos que r es separable sobre F, ya que el número de factores de descomposición coincide con el grado.

($\Longleftarrow$)

Supongamos que cada elemento de K es separable sobre F.

Como K es finita podemos escribir $K = F(r_1, r_2, \ldots r_n)$ donde cada r_i es separable sobre F.

Consideremos la sucesión

$$F \subset F(r_1) \subset F(r_1, r_2) \subset \ldots \subset F(r_1, r_2, \ldots, r_n)$$

como cada r_i es separable sobre F, cada r_i será separable sobre $F(r_1, \ldots, r_{i-1})$ para $i \geq 2$; tenemos que K es separable sobre F.

Vemos, pues, que si K está engendrado por un número finito de elementos, cada uno de los cuales es separable sobre F; K es también separable sobre F.

4- EXTENSIONES NORMALES

PROPOSICION 48

Sean K y K_1 campos y $\alpha_1, \alpha_2, \ldots, \alpha_n$ distintos isomorfismos de K hacia K_1. Entonces

$$a_1\alpha_1(k) + a_2\alpha_2(k) + \ldots + a_n\alpha_n(k) = 0 \quad \text{para todo} \quad k \in K$$

y las constantes $a_1, a_2, \ldots, a_n$ en K_1

$\Longrightarrow \quad a_1 = a_2 = \ldots = a_n = 0$.

Prueba

Procederemos por inducción sobre n.

Si $n = 1$ y $a_1\,\alpha_1(k) = 0$ para todo $k \in K$ entonces

$$a_1\,\alpha_1(1) = a_1 = 0$$

puesto que $\alpha_1(1)$ es el elemento identidad de K_1 asumamos ahora que el resultado es válido para m distintos isomorfismos, con $1 \leq m < n$.

Supongamos

$$a_1\,\alpha_1(k) + a_2\,\alpha_2(k) + \ldots + a_n\,\alpha_n(k) = 0$$

para todo $k \in K$ y $a_1, a_2, \ldots, a_n$ no todos cero en K_1.

Implicamos de nuestra asunción que $a_i \neq 0$ para todo i. Como α_1 y α_n son distintos, debe existir algún $h \in K$ tal que

$$\alpha_1(h) \neq \alpha_n(h).$$

Hagamos $k = h\,g$ para algún $g \in K$.

Tenemos

$$a_1\,\alpha_1(h)\,\alpha_1(g) + a_2\,\alpha_2(h)\,\alpha_2(g) + \ldots + a_n\alpha_n(h)\alpha_n(g) = 0$$

multiplicando por $\alpha_n^{-1}(h)$, tenemos

(1) $b_1\alpha_1(g) + b_2\alpha_2(g) + \ldots + b_n\alpha_n(g) = 0$ $\qquad b_i = a_i\alpha_i(h)\alpha_n^{-1}(h)$

entonces $b_n = a_n$ y si a

$$a_1\alpha_1(g) + a_2\alpha_2(g) + \ldots + a_n\alpha_n(g) = 0$$ le restamos (1)

tenemos

$$(a_1 - b_1)\alpha_1(g) + (a_2 - b_2)\alpha_2(g) + \ldots + (a_{n-1} - b_{n-1})\alpha_{n-1}(g) = 0$$

y

$$(a_1 - b_1) = a_1\left[1 - \alpha_1(h)\,\alpha_n^{-1}(h)\right] \neq 0$$

puesto que $\alpha_1(h) \neq \alpha_n(h)$. Pero esto contradice nuestra hipótesis inductiva. Por lo tanto el resultado es válido para todo n.

DEFINICION 47

Los isomorfismos $\alpha_1, \alpha_2, \ldots, \alpha_n$ de el campo K hacia el campo K_1 tal que cuando

$$a_1\alpha_1(k) + a_2\alpha_2(k) + \ldots + a_n\alpha_n(k) = 0 \quad \text{para todo } k \in K$$

entonces $a_1 = a_2 = \ldots = a_n = 0$ son llamados linealmente independientes sobre K_1.

DEFINICION 48

Sean K y K_1 campos y sea $A = \{\alpha_i \mid i \in I\}$ un conjunto de isomorfismos de K hacia K_1.

Un elemento $k \in K$ es llamado fijo para A si

$$\alpha_i(k) = \alpha_j(k) \quad \text{para todo } i, j \in I.$$

El conjunto de todos los $k \in K$ que son fijos para A lo denotaremos K_A.

PROPOSICION 49

Sean K, K_1 y A los elementos de la definición 48. Entonces K_A es un subcampo de K.

[illegible]

Prueba

Sean $r, k \in K_A$ y $\alpha, \beta \in A$ entonces

$$\alpha(r - k) = \alpha(r) - \alpha(k) = \beta(r) - \beta(k) = \beta(r - k)$$

luego K_A es un subgrupo aditivo de K.

Si $k \neq 0$, entonces

$$\alpha(rk^{-1}) = \alpha(r)\,\alpha(k^{-1}) = \alpha(r)\,\alpha(k)^{-1} = \beta(r)\,\beta(k)^{-1}$$

$$= \beta(r)\,\beta(k^{-1}) = \beta(rk^{-1}).$$

Por lo tanto los elementos distintos de cero de K_A forman un subgrupo multiplicativo de el grupo multiplicativo de K.

Así K_A es un subcampo de K.

DEFINICION 49

K_A será llamado el campo fijo de K por A.

PROPOSICION 50

Sea $A = \{\alpha_1, \alpha_2, \ldots \alpha_n\}$ un conjunto de n distintos isomorfismos de un campo K hacia un campo K_1. Entonces $n \leq [K : K_A]$.

Prueba

Supongamos que nuestra conclusión es falsa, de modo que K tiene una base $\{U_1, U_2, \ldots, U_m\}$ donde $m < n$.

Entonces por corolario 3 existen $c_1, c_2, \ldots, c_n$ no todos cero en K_1 tal que

$$c_1\alpha_1(u_i) + c_2\alpha_2(u_i) + \ldots + c_n\alpha_n(u_i) = 0 \qquad i = 1, 2, \ldots, m$$

Sea k un elemento cualquiera de K y

$$k = b_1u_1 + b_2u_2 + \ldots + b_mu_m \text{ para algunos } b_1, b_2, \ldots b_m \text{ en } K_A$$

como $\alpha_j(b_i) = g_i$ para algún $g_i \in K_1$ y todo $j = 1, 2, \ldots, n$.

Sea $\alpha_j(b_i) = g_i$ para algún $g_i \in K_1$ y todo $j = 1, 2, \ldots, n$ tenemos

$$c_1\alpha_1(k) + c_2\alpha_2(k) + \ldots + c_n\alpha_n(k)$$

$$= c_1\alpha_1(b_1u_1 + \ldots + b_m u_m) + \ldots + c_n\alpha_n(b_1u_1 + \ldots + b_mu_m)$$

$= [c_1 g_1 \alpha_1(u_1) + \dots + c_1 g_m \alpha_1(u_m)] + \dots + [c_n g_1 \alpha_n(u_1) + \dots +$

$\dots + c_n g_m \alpha_n(u_m)]$

$= g_1 [c_1 \alpha_1(u_1) + \dots + c_n \alpha_n(u_1)] + \dots + g_m [c_1 \alpha_1(u_m) + \dots +$

$\dots + c_n \alpha_n(u_m)]$

$= 0$.

Pero esto contradice la proposición 48, por lo que concluimos que nuestra suposición es falsa y por lo tanto

$$n \leq [K : K_A] .$$

COROLARIO 11

Sea $A = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ un conjunto de distintos automorfismos de un campo K. Entonces

$$n \leq [K : K_A].$$

DEFINICION 50

Sea K un campo y sea F un subcampo de K.

El grupo de todos los automorfismos α de K para los cuales $F \subseteq K_\alpha$ lo llamaremos el grupo de automorfismos de K sobre F y lo denotaremos $G_{K|_F}$.

PROPOSICION 51

Sea K_A el campo fijo del campo K por un grupo

$$A = \{\alpha_1 = e, \alpha_2, \dots, \alpha_n\}$$

de automorfismos de K. Entonces $[K : K_A] = n$.

Prueba

Sabemos que $n \leq [K : K_A]$.

Supongamos que $n < [K : K_A]$, es decir que existen $u_1, u_2, \dots, u_{n+1}$ elementos de K, linealmente independientes sobre K_A .

Existen entonces $c_1, c_2, \ldots, c_{n+1}$ en K, no todos cero, que satisfacen el sistema de n ecuaciones lineales homogéneas en $n + 1$ incógnitas:

(1) $x_1\alpha_i(u_1) + x_2\alpha_i(u_2) + \ldots + x_{n+1}\alpha_i(u_{n+1}) = 0 \quad i = 1, 2, \ldots, n$.

De entre todas las soluciones no triviales de (1), seleccionemos una que tenga el mínimo número posible m, de miembros distintos de cero.

Tenemos entonces que $1 < m$, ya que si $m = 1$ tendríamos

$$c_1 \, \alpha_1 \, (u_1) = 0$$

y entonces c_1 sería cero, lo que sería contrario a nuestra condición de que los c_j no son todos ceros $(\alpha_i(u_1) \neq 0$ puesto que $u_1 \neq 0$ y α_1 es un automorfismo).

Podemos entonces asumir que $c_1, c_2, \ldots, c_m$ son distintos de cero y $c_{m+1} = \ldots = c_{n+1} = 0$.

Mutliplicando todos los c_j por c_m^{-1} tenemos

(2) $c_1\alpha_i(u_1) + c_2\alpha_i(u_2) + \ldots + c_{m-1}\alpha_i(u_{m-1}) + \alpha_i(u_m) = 0$

$$i = 1, 2, \ldots, n.$$

Cuando $i = 1$, tenemos que $\alpha_i = e$, así

$$c_1u_1 + c_2u_2 + \ldots + c_{m-1}\, u_{m-1} + u_m = 0$$

de aquí concluimos que $c_1, c_2, \ldots, c_{m-1}$ no están todos en K_A, puesto que $u_1, \ldots, u_m$ son linealmente independientes sobre K_A.

Supongamos que $c_1 \notin K_A$, entonces

$$c_1 - \alpha_j(c_1) \neq 0 \qquad \text{para algún } \alpha_j$$

aplicando este α_j a (2) tenemos

$$\alpha_j(c_1\alpha_i(u_1)) + \alpha_j(c_2\alpha_i(u_2)) + \ldots + \alpha_j(\alpha_i(u_m)) = 0 \qquad i = 1,2,..,n$$

es decir

$$(3) \quad \alpha_j(c_1)\alpha_{i_j}(u_1) + \ldots + \alpha_j(c_{m-1})\alpha_{i_j}(u_{m-1}) + \alpha_{i_j}(u_m) = 0$$

$$i = 1,2,..,n$$

donde $\alpha_{i_j} = \alpha_j(\alpha_i)$.

Como A es un grupo, los elementos $\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}$ son simplemente una permutación de $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Restando (3) de (2) tenemos

$$(c_1 - \alpha_j(c_1))\alpha_i(u_1) + \ldots + (c_{m-1} - \alpha_j(c_{m-1}))(\alpha_i(u_{m-1})) = 0$$

$$l = 1,2,..,n$$

Pero entonces

$$c_1 - \alpha_j(c_1), \ldots, c_{m-1} - \alpha_j(c_{m-1}), \quad 0, \ldots, 0$$

es una solución no trivial de (1) que posee menos de m elementos distintos de cero. Entonces nuestro supuesto de que $n < [K : K_A]$ es falso y por lo tanto $[K : K_A] = n$.

<u>*PROPOSICION 52*</u>

$G_{K|F}$ es un subgrupo del grupo de todos los automorfismos de K.

<u>*Prueba*</u>

Para $\alpha, \beta \in G_{K|F}$ y $a \in F$, tenemos

$$\begin{aligned}(\alpha_0\beta)(a) &= \alpha(\beta(a)) \\ &= \alpha(a) \\ &= a\end{aligned}$$

el automorfismo identidad, evidentemente pertenece a $G_{K|F}$ y la composición de funciones es asociativa, además

$$\begin{aligned} \alpha(a) &= a \\ \alpha^{-1}(\alpha(a)) &= \alpha^{-1}(a) \\ a &= \alpha^{-1}(a) \end{aligned}$$

luego para $\alpha \in G_{K|F}$ tenemos que $\alpha^{-1} \in G_{K|F}$.

<u>*DEFINICION 51*</u>

Si $[K : F]$ es finito y $K_{G_{K|F}} = F$, entonces decimos que K es una extensión normal de F y $G_{K|F}$ es llamado el grupo de Galais de K sobre F.

<u>*PROPOSICION 53*</u>

Sea K normal sobre F. Entonces K es separable sobre F y todo elemento $k \in K$ es una raíz de un polinomio f(x) en $F[x]$, el cual se descompone en K.

<u>*Prueba*</u>

Sea $G_{K|F} = \{\alpha_1 = e, \alpha_2, \ldots, \alpha_n\}$, donde $[K : F] = n$.

Para $k \in K$, sean $k = k_1, k_2, \ldots , k_m$ los distintos elementos del conjunto $\{\alpha_i(k) \mid i = 1, 2, \ldots, n\}$.

Como $G_{K|F}$ es un grupo, tenemos

$$\alpha_j(k_i) = \alpha_j(\alpha_i(k)) = k_r \quad \text{para algún } r.$$

Además

$$\alpha_r(k_i) = \alpha_r(k_j)$$

implica que

$$k_i = \alpha_r^{-1}(\alpha_r(k_i)) = \alpha_r^{-1}(\alpha_r(k_j)) = k_j$$

por lo tanto $\alpha_j(k_1), \alpha_j(k_2), \ldots, \alpha_j(k_m)$ son distintos, entonces los factores de

$$f(x) = (x - k_1)(x - k_2) \ldots (x - k_m)$$

son simplemente permutaciones para algún α_i de $G_{K|F}$.

Así los coeficientes de f(x) permanecen inalterables para cualquier α_i de $G_{K|F}$ y deben por tanto estar en F, ya que K es normal sobre F.

Además $k = k_1$ es una raíz de un polinomio separable f(x) en $F[x]$ y f(x) se descompone en K.

PROPOSICION 54

Sea K una extensión normal de F y sea A un subgrupo de $G_{K|F}$.

Sea $K_A = \{x \in K \mid \alpha(x) = x, \text{ para toda } \alpha \in A\}$ el campo fijo de A. Entonces

$$G_{K|K_A} = A .$$

Prueba

Como todos los elementos de A dejan fijos a todos los elementos de K_A, tenemos que

$$A \subset G_{K|K_A} .$$

Sabemos por la proposición 50 que el orden de $G_{K|K_A}$ es menor o igual que $[K : K_A]$($0\, G_{K|K_A} \leq [K : K_A]$) y como

$$0\, A \leq 0\, G_{K|K_A}$$

tenemos

$$0\, A \leq 0\, G_{K|K_A} \leq [K : K_A] .$$

Además por la proposición 51, sabemos que

$$0\,A = [K : K_A]$$

por lo tanto

$$0\,A = 0\,G_{K|K_A}$$

de aquí tenemos que

$$A = G_{K|K_A}$$

ya que A es un subgrupo de $G_{K|K_A}$.

DEFINICION 52

Sea S_n el grupo simétrico de grado n, considerado como si actuara sobre el conjunto $\{1, 2, \ldots, n\}$; para $\alpha \in S_n$ e i entero, con $1 \leq i \leq n$; sea $\alpha(i)$ la imagen de i bajo α.

Podemos hacer actuar a S_n sobre $F(x_1, x_2, \ldots, x_n)$ de la siguiente manera: para $\alpha \in S_n$ y $f(x_1, x_2, \ldots, x_n) \in F(x_1, x_2, \ldots, x_n)$ definimos la aplicación que lleva $f(x_1, x_2, \ldots, x_n)$ sobre $f(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$.

El campo fijo de $F(x_1, x_2, \ldots, x_n)$ respecto a S_n, consiste entonces de todas las funciones racionales $f(x_1, x_2, \ldots, x_n)$ tales que

$$f(x_1, x_2, \ldots, x_n) = f(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) \quad \text{para todo } \alpha \in S_n$$

A estos elementos fijos en $F(x_1, x_2, \ldots, x_n)$ les llamaremos funciones racionales simétricas.

Como son el campo fijo de S_n forman un subcampo de $F(x_1, x_2, \ldots, x_n)$ al que llamaremos el campo de las funciones racionales simétricas y lo representaremos por S.

Veamos algunas funciones de S construidas con $x_1, x_1, \ldots, x_n$ conocidas como funciones simétricas elementales en $x_1, x_2, \ldots, x_n$; las definimos:

$$a_1 = x_1 + x_2 + \dots + x_n = \sum_{i=1}^{n} x_i$$

$$a_2 = \sum_{i<j} x_i\, x_j$$

$$a_3 = \sum_{i<j<k} x_i\, x_j\, x_k$$

$$\vdots$$

$$a_n = x_1\, x_2 \dots x_n \,.$$

PROPOSICION 55

Sea F un campo y $F(x_1, x_2, \dots, x_n)$ el campo de las funciones racionales en $x_1, x_2, \dots, x_n$ sobre F. Supongamos que S es el campo de las funciones racionales simétricas, entonces

$$G_F(x_1, x_2, \dots, x_n)_{|S} = S_n \,.$$

Prueba

Como el grupo S_n es un grupo de automorfismos de $F(x_1, x_2 \dots, x_n)$ que deja a S fijo, entonces $S_n \subset G_{F(x_1, x_2, \dots x_n)|S}$ por la proposición 50 afirmamos que

$$n! = O(S_n) \leq OG_{F(x_1, x_2, \dots, x_n)|S} < [F(x_1, x_2, \dots, x_n) : S]$$

construyamos ahora el polinomio

$$p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \dots + (-1)^n a_n .$$

Vemos que p(t) toma sus coeficientes en $F(a_1, a_2, \dots, a_n)$ y se factoriza sobre $F(x_1, x_2, \dots, x_n)$ de la siguiente manera

$$p(t) = (t - x_1)(t - x_2) \dots (t - x_n) \,.$$

Así tenemos que p(t) de grado n sobre $F(a_1, a_2, \dots, a_n)$ se descompone en un producto de factores lineales sobre $F(x_1, x_2, \dots, x_n)$.

No puede descomponerse sobre un subcampo propio de

$F(x_1, x_2, \ldots, x_n)$ que contenga a $F(a_1, a_2, \ldots, a_n)$ pues este subcampo tendría entonces que contener tanto a F como a cada una de las raíces de p(t), es decir a $x_1, x_2, \ldots, x_n$; pero entonces este subcampo sería todo $F(x_1, x_2, \ldots, x_n)$.

Vemos pues que $F(x_1, x_2, \ldots, x_n)$ es el campo de descomposición del polinomio $p(t) = t^n - a_1 t^{n-1} + \ldots + (-1)^n a_n$ sobre $F(a_1, a_2, \ldots, a_n)$.

Como p(t) es de grado n, tenemos según la proposición 39 que

$$[F(x_1, x_2, \ldots, x_n) : F(a_1, a_2, \ldots, a_n)] \leq n! = O(S_n)$$

y por ser $F(a_1, a_2, \ldots, a_n)$ un subcampo de S

$$O(S_n) = n! \geq [F(x_1, x_2, \ldots, x_n) : F(a_1, a_2, \ldots, a_n)]$$

$$= [F(x_1, x_2, \ldots x_n) : S]\,[S : F(a_1, a_2, \ldots, a_n)] \geq n!$$

$$= O(S_n)$$

por lo tanto

$$[F(x_1, x_2, \ldots, x_n) : S] = n! = O(S_n)$$

$$\Longrightarrow \quad O\, G_{F(x_1, x_2, \ldots, x_n)|S} = O(S_n)$$

$$\Longrightarrow \quad G_{F(x_1, x_2, \ldots, x_n)|S} = S_n .$$

PROPOSICION 56

K es una extensión normal de F si y sólo si K es el campo de descomposición de un polinomio en $F[x]$.

Prueba

($\Longrightarrow$) Como K es normal sobre F, entonces

$$[K : F] = n \quad \text{para algún } n.$$

Tomemos $\{u_1, u_2, \ldots, u_n\}$ como una base de K sobre F.

Por la proposición 53, tenemos que cada u_i es raíz de un polinomio irreducible $f_i(x)$ en $F[x]$, que es separable y se descompone en K.

Sea $f(x) = f_1(x)\, f_2(x) \ldots f_n(x)$.

Como f(x) tiene las raíces $u_1, u_2, \ldots, u_n$, el campo de descomposición K_0 de f(x) debe contener a

$$K = F(u_1, u_2, \ldots, u_n)$$

y como además todas las raíces de f(x) están en K tenemos que $K_0 \subset K$, luego $K_0 = K$.

$(\Longleftarrow)$

Asumamos ahora que K es el campo de descomposición de un polinomio separable en $F[x]$.

Procederemos por inducción sobre $[K : F]$, suponiendo que para cualquier par de campos K_1, F_1 con $[K_1 : F_1]$ menor que $[K : F]$, siempre que K_1 es el campo de descomposición sobre F_1 de un polinomio en $F_1[x]$, entonces K_1 es normal sobre F_1.

i) $[K : F] = 1$.

Si $f(x) \in F[x]$ se descompone en factores lineales sobre F, entonces $K = F$ y K es normal sobre F puesto que entonces $G_{K|F} = \{e\}$, y $K = F$ es el campo fijo por el automorfismo identidad e.

Supongamos ahora que el resultado es válido para todos los pares de campos tales que f(x) posee $m > 1$ raíces fuera del campo base.

$f(x) = p_1(x)\, p_2(x) \ldots p_r(x)$ para $p_i(x)$ irreducible y separable en $F[x]$ y como $m > 1$, podemos asumir que $p_1(x)$ posee grado d mayor que 1.

Sea r una raíz de $p_1(x)$, de modo que $[F(r) : F] = d$. Como $p_1(x)$ es irreducible y separable, sus raíces $r = r_1, \ldots, r_d$ son todas distintas.

Entonces por la proposición 30, existen isomorfismos $\alpha'_1, \alpha'_2, \ldots, \alpha'_d$ tal que

$$\alpha'_i : F(r) \longrightarrow F(r_i)$$

con $\alpha'_i(r) = r_i$ y F fijo bajo α'_i.

Como K es un campo de descomposición de f(x) sobre F(r) y $F(r_i)$, por la proposición 41, el isomorfismo α'_i puede ser extendido a un automorfismo α_i de K, el cual lleva r sobre r_i y deja a F fijo, con $i = 1, 2, \ldots, d$.

Supongamos que t es un elemento de K que se mantiene fijo para todos los automorfismos en $G_{K|F}$.

Como f(x) posee m raíces fuera de F(r), por nuestra hipótesis inductiva K es normal sobre F(r) y por lo tanto, cualquier elemento fijo bajo $G_{K|F(r)} \subset G_{K|F}$ debe estar en F(r).

t entonces es de la forma

$$t = a_0 + a_1 r + \ldots + a_{d-1} r^{d-1} \qquad a_0, a_1, \ldots, a_{d-1} \in F$$

aplicando α_i a ambos lados tenemos

$$\alpha_i(t) = t = a_0 + a_1 r_i + \ldots + a_{d-1} r_i^{d-1} \qquad i = 1, 2, \ldots, d$$

pero esto implica que

$$g(x) = (a_0 - t) + a_1 x + \ldots + a_{d-1} x^{d-1}$$

tiene las d distintas raíces $r_1, r_2, \ldots, r_d$ en K, lo que implica que g(x) es el polinomio cero y $t = a_0$ está en F.

Por lo tanto F es el campo fijo de $G_{K|F}$ y K es normal sobre F.

PROPOSICION 57

Sea K una extensión finita de F.

K es normal sobre F si y sólo si todo elemento de K es una raíz de un polinomio separable f(x) en F[x] el cual se descompone en K.

Prueba

($\Longrightarrow$)

Está dada por la proposición 53.

($\Longleftarrow$)

Sea $\{u_1, u_2, \ldots, u_n\}$ una base de K sobre F y supongamos que la condición sobre los elementos de K es satisfecha, donde u_i es una raíz de el polinomio separable $f_i(x)$ en F[x] y $f_i(x)$ se descompone en K.

Entonces $f(x) = f_1(x) f_2(x) \ldots f_n(x)$ es separable, K es el campo de descomposición de f(x) y K es normal sobre F por la proposición 56.

COROLARIO 12

Sean $F \subset H \subset K$ campos con K normal sobre F. Entonces K es normal sobre H.

Prueba

Como $F[x] \subset H[x]$, aplicamos la proposición 57 ya que el polinomio separable en F[x] puede considerarse sobre H.

DEFINICION 53

Sea f(x) un polinomio en F[x] y sea K su campo de descomposición sobre F. El grupo de Galois de f(x) es el grupo $G_{K|F}$ de todos los automorfismos de K que dejan fijos los elementos de F.

El grupo de Galois de f(x) puede considerarse como un grupo de permutaciones de sus raíces ya que si r es una raíz de f(x) y si $\alpha \in G_{K|F}$ entonces $\alpha(r)$ es también una raíz de $f(x)$.

PROPOSICION 58

Sea $f(x)$ un polinomio en $F[x]$.

K su campo de descomposición sobre F.

$G_{K|F}$ su grupo de Galois.

Para cualquier subcampo H de K que contiene a F sea $G_{K|H} = \{\alpha \in G_{K|F} \mid \alpha(h) = h$ para todo $h \in H\}$ y para cualquier subgrupo A de $G_{K|F}$.

Sea $K_A = \{x \in K \mid \alpha(x) = x$ para todo $\alpha \in A\}$.

Entonces la asociación de H con $G_{K|H}$ establece una correspondencia biyectiva del conjunto de subcampos de K que contienen a F sobre el conjunto de subgrupos de $G_{K|F}$ tal que

i) $H = K_{G_{K|H}}$

ii) $A = G_{K|K_A}$

iii) $[K : H] = OG_{K|H}$, $[H : F]$ = índice de $G_{K|H}$ en $G_{K|F}$.

iv) H es una extensión normal de F si y sólo si $G_{K|H}$ es un subgrupo normal de $G_{K|F}$.

v) Cuando H es una extensión normal de F, entonces $G_{H|F}$ es isomorfo a $\dfrac{G_{K|F}}{G_{K|H}}$.

Prueba

i) Por ser K el campo de descomposición de f(x) sobre F es también el campo de descomposición de f(x) sobre cualquier subcampo H que contenga a F, luego por la proposición 56, K es una extensión normal de H y por la definición de normalidad H es el campo fijo de $G_{K|H}$, es decir

$$H = K_{G_{K|H}} .$$

ii) Como K es una extensión normal de F, por proposición 54, dado un subgrupo A de $G_{K|F}$, entonces

$$A = G_{K|K_A} .$$

iii) Tenemos por la proposición 51 que

$$[K : H] = OG_{K|H}$$

tenemos entonces que

$$OG_{K|F} = [K : F] = [K : H][H : F]$$

de donde

$$[H : F] = \frac{OG_{K|F}}{OG_{K|H}} = \text{índice de } G_{K|H} \text{ en } G_{K|F} .$$

iv) Haremos primero la siguiente observación: H es una extensión normal de F, si y sólo si, para cada $\alpha \in G_{K|F}$, $\alpha(H) \subset H$.

Sabemos por la proposición 43, que existe $a \in H$ tal que $H = F(a)$.

Si $\alpha(H) \subset H$, entonces $\alpha(a) \in H$ para todo $\alpha \in G_{K|F}$, Consideremos el polinomio sobre H

$p(x) = (x - \alpha_1(a))(x - \alpha_2(a))\dots(x - \alpha_n(a))$

donde $\alpha_1, \alpha_2, \dots, \alpha_n$ son todos los elementos de $G_{H|F}$

Vemos que H es el campo de descomposición de p(x), que tiene sus coeficientes en F, y por la proposición 56 tenemos que H es una extensión normal de F.

Reciprocamente si H es una extensión normal de F entonces H = F(a), donde el polinomio mínimo de a, p(x), sobre F tiene todas sus raíces en H, pero para cualquier $\alpha \in G_{K|F}$, $\alpha(a)$ es también una raíz de p(x), de donde $\alpha(a)$ debe estar en H.

Como H está generado por a sobre F tenemos que

$$\alpha(H) \subset H \qquad \text{para todo } \alpha \in G_{K|F} .$$

Tenemos así que H es una extensión normal de F, si y sólo si, para todo $\alpha \in G_{K|F}$, $\tau \in G_{K|H}$ y $a \in H$, $\alpha(a) \in H$ y por lo tanto

$$\tau(\alpha(a)) = \alpha(a)$$

es decir si y sólo si

$$\alpha^{-1} \circ \tau \circ \alpha(a) = a .$$

Pero esto es lo mismo que decir que H es normal sobre F si y sólo si

$$\alpha^{-1} G_{K|H} \alpha \subset G_{K|H} \quad \text{para todo } \alpha \in G_{K|F} .$$

Entonces $G_{K|H}$ es un subgrupo normal de $G_{K|F}$.

v) Si H es normal sobre F, para $\alpha \in G_{K|F}$, como $\alpha(H) \subset H$, tenemos que α induce un automorfismo α_* de H definido por

$$\alpha_*(a) = \alpha(a) \qquad \text{para todo } a \in H .$$

Como α_* deja a todo elemento de F fijo, α_* debe estar en $G_{H|F}$.

Además para cualquier $\alpha,\Psi \in G_{K|F}$

$$(\alpha\,\Psi)_* = \alpha_*\,\Psi_*$$

de donde la aplicación

$$\begin{array}{ccc} G_{K|F} & \longrightarrow & G_{H|F} \\ \alpha & \rightsquigarrow & \alpha_* \end{array}$$

cumple ser un homomorfismo.

El núcleo de este homomorfismo consiste en todos los elementos $\alpha \in G_{K|F}$ tal que α_* es la aplicación identidad sobre H.

El núcleo es pues, el conjunto de todos los $\alpha_* \in G_{K|F}$ tales que

$$a = \alpha_*(a) = \alpha(a)$$

tenemos entonces que el núcleo es $G_{K|H}$.

Por la proposición 7 existe un isomorfismo entre la imagen de $G_{K|F}$ en $G_{H|F}$ y $\dfrac{G_{K|F}}{G_{K|H}}$.

Por iii) tenemos que

$$\frac{0\;G_{K|F}}{0\;G_{K|H}} = [H : F] .$$

Por la proposición 54

$$[H : F] = 0\;G_{H|F} .$$

Por lo tanto

$$\frac{0\ G_{K|_F}}{0\ G_{K|_H}} = 0\ G_{H|_F} \quad .$$

Tenemos así que la imagen de $G_{K|_F}$ en $G_{H|_F}$ es todo $G_{H|_F}$

y por lo tanto

$$G_{H|_F} \simeq \frac{G_{K|_F}}{G_{K|_H}} \quad .$$

CAPITULO III
SOLUBILIDAD POR MEDIO DE RADICALES

1- IRRESOLUBILIDAD DEL POLINOMIO DE GRADO 5 POR MEDIO DE RADICALES

DEFINICION 54

Dado un campo F y un polinomio $p(x) \in F[x]$ diremos que p(x) es soluble por radicales sobre F, si podemos encontrar una sucesión finita de campos.

$F_1 = F(w_1),\ F_2 = F_1(w_2),\ \ldots,\ F_k = F_{k-1}(w_k)$

donde $w_1^{r_1} \in F,\ w_2^{r_2} \in F_1,\ \ldots,\ w_k^{r_k} \in F_{k-1}$

tal que las raíces de p(x) se encuentran todas en F_k.

Si K es el campo de descomposición de p(x) sobre F, entonces p(x) es soluble por radicales sobre F, si puede encontrarse una sucesión de campos como los anteriores tal que $K \subset F_k$.

Sea $F(a_1, a_2, \ldots, a_n)$ el campo de las funciones racionales en las n variables $a_1, a_2, \ldots, a_n$ sobre F y consideremos el polinomio particular $p(x) = x^n + a_1x^{n-1} + \ldots + a_n$ sobre el campo $F(a_1, a_2, \ldots, a_n)$, p(x) es soluble por radicales, si es soluble por radicales sobre $F(a_1, a_2, \ldots, a_n)$.

DEFINICION 55

Un grupo G es soluble si puede encontrarse una cadena finita de subgrupos

$$G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k = (e)$$

donde cada N_i es un subgrupo normal de N_{i-1} y tal que cada grupo cociente $\dfrac{N_{i-1}}{N_i}$ es abeliano.

PROPOSICION 59

Si G es un grupo, entonces G' es normal sobre G.

Prueba

Sea $S = \{ x^{-1} y^{-1} x y \mid x, y \in G\}$.

Para $m \in G$, tenemos

$$\begin{aligned} m(x^{-1} y^{-1} x y)m^{-1} &= m(x^{-1} e y^{-1} e x e y)m^{-1} \\ &= m(x^{-1}m^{-1}my^{-1}m^{-1}mxm^{-1}my)m^{-1} \\ &= (mx^{-1}m^{-1})(my^{-1}m^{-1})(mxm^{-1})(mym^{-1}) \\ &= (mxm^{-1})^{-1}(mym^{-1})^{-1}(mxm^{-1})(mym^{-1}) \end{aligned}$$

este último producto pertenece a S, por lo tanto S es normal sobre G.

Si $[S]$ es el conjunto generado por S, es decir $G' = [S]$ entonces para $g \in G$, tenemos

$$g[S]g^{-1} = [gSg^{-1}] = [S]$$

por lo tanto G' es normal sobre G.

DEFINICION 56

Dado el grupo G y los elementos a y b de G, diremos que el conmutador de a y b es el elemento $a^{-1} b^{-1} a b$.

El subgrupo conmutador, G' de G, es el subgrupo de G generado por todos los conmutadores de G.

El conmutador de G' se denotará $(G')' = G^{(2)}$ y del mismo modo $(G^{(i-1)})' = G^{(i)}$.

PROPOSICION 60

G es soluble si y sólo si $G^{(k)} = (e)$ para algún entero K.

Prueba

($\Longrightarrow$)

Si G es un grupo soluble, existe una cadena

$$G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k = (e)$$

donde cada N_i es normal en N_{i-1} y donde

$\frac{N_{i-1}}{N_i}$ es abeliano. Pero entonces, el subgrupo conmutador N'_{i-1}

de N_{i-1} debe estar contenido en N_i , ya que para cualquier

$a, b \in N_{i-1}$, tenemos

$$(a\, N_i)(b\, N_i) = (b\, N_i)(a\, N_i)$$

$$a\, b\, N_i = b\, a\, N_i$$

$$a^{-1}b^{-1}a\, b\, N_i = N_i$$

$$\Longrightarrow a^{-1}\, b^{-1}\, a\, b \in N_i .$$

Así, pues,

$N_1 \supset N'_0 = G'$, $N_2 \supset N'_1 \supset (G')' = G^{(2)}$, $N_3 \supset N'_2 \supset (G^{(2)})' = G^{(3)} \ldots$

$N_i \supset G^{(i)}$, $(e) = N_k \supset G^{(k)}$

por lo tanto $G^{(k)} = (e)$.

($\Longleftarrow$)

Si $G^{(k)} = (e)$.

$$\begin{aligned} \text{Sea } N_0 &= G \\ N_1 &= G' \\ N_2 &= G^{(2)} \\ &\vdots \\ N_k &= G^{(k)} = (e) . \end{aligned}$$

Vemos que $G = N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_k = (e)$

donde cada N_i es normal en N_{i-1} .

Además, el grupo $\frac{N_{i-1}}{N_i}$ es abeliano, ya que para a, b $\in$ G, tenemos

$$
\begin{aligned}
(a\,G')(b\,G') &= a\,b\,G' = e\,a\,b\,G' \\
&= b\,a\,a^{-1}\,b^{-1}\,a\,b\,G \\
&= b\,a\,(a^{-1}\,b^{-1}\,a\,b)G' \\
&\quad \text{como } (a^{-1}\,b^{-1}\,a\,b) \in G' \\
&= b\,a\,G' \\
&= (b\,G')(a\,G')
\end{aligned}
$$

es decir $\frac{G}{G}$,es abeliano y $\frac{N_{i-1}}{N_i} = \frac{G^{(i-1)}}{G^{(i)}} = \frac{G^{(i-1)}}{(G^{(i-1)})'}$ es abeliano. Por lo tanto G es soluble.

COROLARIO 13

Si G es un grupo soluble y si $\overline{G}$ es una imagen homomórfica de G, entonces $\overline{G}$ es soluble.

Prueba

Por ser $\overline{G}$ imagen homomórfica de G, tenemos que $(\overline{G})^{(k)}$ es la imagen de $G^{(k)}$.

Como $G^{(k)} = (e)$ para algún k, tenemos $(\overline{G})^{(k)} = (e)$ para la misma k, por lo tanto $\overline{G}$ es soluble.

PROPOSICION 61

Sea $G = S_n$, $n \geq 5$, S_n es el grupo simétrico de grado n, entonces $G^{(k)}$ para k = 1, 2, ... contiene todo ciclo de orden 3 de S_n .

Prueba

Si N es un subgrupo normal de $G = S_n$ donde $n \geq 5$, que contiene todo ciclo de orden 3 en S_n, entonces N' debe también contener todo ciclo de orden 3. Pues supongamos

$$a = (1, 2, 3)$$

$$b = (1, 4, 5)$$

con a y b en N.

Entonces

$$a^{-1}b^{-1}ab = (3, 2, 1)(5, 4, 1)(1, 2, 3)(1, 4, 5)$$

$$= (1, 4, 2).$$

Vemos que $(a^{-1} b^{-1} a b) \in N'$. Es decir $(1, 4, 2) \in N'$.

Así para cualquier $\alpha \in S_n$

$\alpha^{-1} (1, 4, 2)\alpha$ debe estar en N'.

Escojamos $\alpha \in S_n$ de la siguiente manera

$$\alpha(1) = i_1$$

$$\alpha(4) = i_2$$

$$\alpha(2) = i_3$$

donde i_1, i_2, i_3 son tres enteros distintos en el rango de 1 a n.

Entonces $\alpha^{-1}(1, 4, 2)\alpha = (i_1, i_2, i_3)$ está en N'.

Por lo tanto N' contiene todos los ciclos de orden 3. Haciendo N = G, que es normal en G y contiene todos los ciclos de orden 3, tenemos que G' contiene todos los ciclos de orden 3.

Como G' es normal en G; $G^{(2)}$ contiene todos los ciclos de orden 3.

Como $G^{(2)}$ es normal en G, $G^{(3)}$ contiene todos los ciclos de orden 3.

Continuando así concluimos que $G^{(k)}$ contiene todos los ciclos de orden 3 para cualquier k.

DEFINICION 57

Un elemento ξ de un cuerpo K tal que existe un entero $n \geq 1$; para el cual $\xi^n = 1$, se llama raíz de la unidad o más exactamente raíz n-ésima de la unidad. Así, el conjunto de las raíces n-ésimas de la unidad es el conjunto de las raíces del polinomio $X^n - 1$.

DEFINICION 58

Si $z = x + iy$ $(i = \sqrt{-1})$, definimos $e^z = e^{x+iy}$ como el número complejo

$$e^z = e^x (\cos y + i \operatorname{sen} y).$$

PROPOSICION 62

S_n no es soluble para $n \geq 5$.

Prueba

Si $G = S_n$, según la proposición 61, tenemos que $G^{(k)}$ contiene todos los ciclos de orden 3 de S_n para todo k, por lo tanto $G^{(k)} \neq (e)$ para toda k, luego por la proposición 60 concluimos que G no es soluble.

PROPOSICION 63

Sea F un campo que contiene todas las raíces n-ésimas de la unidad (para n fijo) y sea $a \neq 0$, $a \in F$. Sea además $(X^n - a) \in F[x]$ y sea K su campo de descomposición sobre F, entonces:

i) $K = F(u)$, donde u es cualquier raíz de $X^n - a$.

ii) El grupo de Galois de $X^n - a$ sobre F, es abeliano.

Prueba

i) Como F contiene a todas las raíces n-ésimas de la unidad, contiene a $\xi = e^{2\Pi i/n}$ ya que $\xi^n = 1$ pero $\xi^m \neq 1$ para $0 < m < n$.

Sea $u \in K$, una raíz cualquiera de $X^n - a$, entonces $u, \xi u, \xi^2 u, \ldots, \xi^{n-1} u$ son todas las raíces distintas de $X^n - a$; ya que si

$$\xi^i u = \xi^j u \quad \text{con} \quad 0 \leq i < j < n$$

como $u \neq 0$ y $(\xi^i - \xi^j)u = 0$ debe ser $\xi^i = \xi^j$ es decir

$$\xi^{j-1} = 1 \qquad \text{con} \quad 0 < j-i < n$$

lo que es imposible.

$\xi \in F$ por lo tanto $u, \xi u, \ldots, \xi^{n-1} u$ están en $F(u)$ luego $F(u)$ descompone a $X^n - a$.

Como ningún subcampo propio de $F(u)$ que contenga a F contiene a u, ningún subcampo propio de $F(u)$ puede descomponer a $X^n - a$. Por tanto $F(u)$ es el campo de descomposición de $X^n - a$, ó sea $K = F(u)$.

ii) Si α, τ son dos elementos cualesquiera del grupo de Galois de $X^n - a$, es decir, si α, τ son automorfismos de $K = F(u)$ que dejan todos los elementos de F fijos, entonces como $\alpha(u)$ y $\tau(u)$ son raíces de $X^n - a$, tenemos que

$$\alpha(u) = \xi^i u \quad \text{y} \quad \tau(u) = \xi^j u$$

para algunos i y j.

Luego

$$\begin{aligned} \alpha(\tau(u)) = \alpha(\xi^j u) &= \xi^j \alpha(u) \quad \text{porque } \xi^j \in F \\ &= \xi^j \xi^i u \\ &= \xi^{i+j} u \end{aligned}$$

además

$$\tau(\alpha(u)) = \xi^{i+j}u \quad .$$

Por lo tanto $\alpha\tau$ y $\tau\alpha$ coinciden sobre u y sobre F, es decir cocinciden sobre $K = F(u)$.

Luego entonces $\alpha\tau = \tau\alpha$, es decir que el grupo de Galois es abeliano.

PROPOSICION 64

Si $p(x) \in F[x]$ es soluble por radicales sobre F, con F un campo que contiene todas las raíces n-ésimas de la unidad, entonces el grupo de Galois sobre F de p(x) es un grupo soluble.

Prueba

Sea K el campo de descomposición de p(x) sobre F.

El grupo de Galois de p(x) sobre F es $G_{K|F}$.

Como p(x) es soluble por radicales existe una sucesión de campos

$$F \subset F_1 = F(w_1) \subset F_2 = F_1(w_2) \subset \ldots \subset F_k = F_{k-1}(w_k)$$

donde

$$w_1^{r_1} \in F, \quad w_2^{r_2} \in F_1 \; , \; \ldots \; , \; w_k^{r_k} \in F_{k-1} \text{ y donde } K \subset F_k \; .$$

Podemos suponer, sin pérdida de generalidad, que F_k es una extensión normal de F.

Como extensión normal de F, F_k es también una extensión normal de cualquier campo intermedio, de donde F_k es una extensión normal de cada una de las F_i.

Según la proposición 63 toda F_i es una extensión normal de F_{i-1} , como además F_k es normal sobre F_{i-1} , tenemos por la proposición 58 que $G_{F_k|F_i}$ es un subgrupo normal en $G_{F_k|F_{i-1}}$.

Consideremos la sucesión

$$G_{F_k|F} \supset G_{F_k|F_1} \supset G_{F_k|F_2} \supset \cdots \supset G_{F_k|F_{k-1}} \supset (e) \; .$$

Cada grupo de estos es un subgrupo normal en el que le precede.

Como F_i es una extensión normal de F_{i-1}, tenemos por la proposición 58 que

$G_{F_i|F_{i-1}}$ es isomorfo a $\dfrac{G_{F_k|F_{i-1}}}{G_{F_k|F_i}}$ y por la proposición 63, $G_{F_i|F_{i-1}}$ es abeliano; es decir que todo grupo cociente

$\dfrac{G_{F_k|F_{i-1}}}{G_{F_k|F_i}}$ es abeliano.

Así, el grupo $G_{F_k|F}$ es soluble.

Como $K \subset F_k$ es una extensión normal de F (por ser un campo de descomposición), según la proposición 58, $G_{F_k|K}$ es un subgrupo normal de $G_{F_k|F}$ y $G_{K|F}$ es isomorfo a

$\dfrac{G_{F_k|F}}{G_{F_k|K}}$. Tenemos así que $G_{K|F}$ es una imagen homomórfica de

$G_{F_k|F}$ que es un grupo soluble por el corolario 13, tenemos que

$G_{K|F}$ es un grupo soluble.

PROPOSICION 65

El polinomio general de grado $n \geq 5$ no es soluble por radicales.

Prueba

En la proposición 55 se demostró que si $F(a_1, a_2, .., a_n)$ es el campo de las funciones racionales en las n variables $a_1, a_2, ... , a_n$ entonces el grupo de Galois del polinomio $p(t) = t^n + a_1t^{n-1} + ... + a_n$ sobre $F(a_1, a_2, ..., a_n)$ es S_n (Grupo simétrico de grado n).

Por la proposición 62 sabemos que S_n no es un grupo soluble cuando $n \geq 5$ y por la proposición 64 concluimos que p(t) no es soluble por radicales sobre $F(a_1, a_2, ..., a_n)$ para $n \geq 5$.

B I B L I O G R A F I A

1) Barnes, Wilfred E., INTRODUCTION TO ABSTRACT ALGEBRA. Washington State University, 1965.

2) Herstein, I. N., ALGEBRA MODERNA, Editorial Trillas, 1973.

3) Lang, Serge, ALGEBRA. Universidad de Columbia, Nueva York. Editorial Aguilar.

4) Boubarki, N., ELEMENTS DE MATHEMATIQUE, FASCICULE XI, ALGEBRE. CHAPITRE 4. POLYNOMES ET FRACTIONS RATIONNELLES. CHAPITRE 5. CORPS CONMUTATIFS. Editorial Hermann.

5) McDuffee, INTRODUCTION TO ABSTRACT ALGEBRA, John Wiley and Sons.

6) Robinson, Abraham, NUMBERS AND IDEALS, Yale University, 1965.