UNIVERSIDAD AUTONOMA DE QUERETARO.
DIRECCION DE ESTUDIOS DE POSGRADO.
SECC. DOCENCIA DE LAS MATEMATICAS.

CAMPOS FINITOS

T E S I S

Que para obtener el grado de

MAESTRO EN DOCENCIA DE LAS MATEMATICAS

p r e s e n t a

ALFREDO CASTANEDO ESCOBEDO

bajo la dirección del Dr,

ALEJANDRO DIAZ BARRIGA CASALES

CREDITOS ASIGNADOS A LA TESIS: 110

JURADO:

DR. ALEJANDRO DIAZ BARRIGA CASALES — PRESIDENTE

DR. EMILIO LLUIS RIERA — SECRETARIO

M. CESAR RINCON ORTA — VOCAL

M. ALEJANDRO PADILLA GONZALEZ — SUPLENTE

M. JORGE MARTINEZ SANCHEZ — SUPLENTE

COORDINADOR DE LA SECCION

M. Alejandro Padilla G.

DIRECTOR DE ESTUDIOS DE POSGRADO

M. en I. José Alfredo Zepeda G.

Querétaro, Qro., Agosto de 1989.

A MI ESPOSA SARITA Y A MI
HIJO ALFREDO CON TODO MI
AMOR.

ALGUNAS PALABRAS PRELIMINARES

Los campos finitos juegan un papel importante en algunas de las ramas de las Matemáticas, como por ejemplo: la Teoría de Números, la Geometría Proyectiva, la Teoría Algebráica de los números, etc.; los ejemplos más familiares que tenemos de ellos son los enteros módulo p, con p un número primo, aunque éstos no - son todos los campos finitos.

En este trabajo clasificamos de una manera completa a los campos finitos y hacemos una discusión sobre su estructura interna. Se estudian también las raíces de un polinomio con coeficientes en algunos de estos campos, así como la relación que éstas guardan con las extensiones finitas de dichos campos finitos.

Por otro lado se intenta que este trabajo, por su forma, sea - accesible a un lector que haya tomado un primer curso de Algebra - abstracta, pretendiendo además que dicho lector encuentre en esta obra el material y apoyo necesarios para la comprensión de aquellos temas que requieren los conceptos y en general la Teoría de los campos finitos.

INDICE

CAPITULO I.

ANTECEDENTES

CAMPOS.

Comenzaremos recordando los canceptos de operación binaria y campo.

DEFINICION. Una operación binaria en un conjunto no vacío A es una función de dominio A^2 y codominio A.

Generalmente se usan símbolos tales como $*, \#, \times, +, \cdot, \circ$, etc., para denotar operaciones binarias, de esta forma podríamos representar a una de ellas así:

$$*: A^2 \longrightarrow A$$

NOTACION: Si $* : A^2 \longrightarrow A$ es una operación binaria y si:

$$((a,b),c) \in *$$

de acuerdo a la notación de funciones esto lo podemos escribir así $(a,b) \xrightarrow{*} c$, pero usualmente preferimos escribirlo como: $a*b=c$.
Así por ejemplo en $+: \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ a $((3,2),5) \in +$, o bien $(3,2) \xrightarrow{+} 5$, lo escribiremos como es usual: $3+2=5$.

DEFINICION. Un campo es una estructura que consiste en un conjunto A, y dos operaciones binarias en A, denotadas como + y $\cdot$, llamadas suma y producto respectivamente, para las cuales se cumplen las siguientes propiedades:

- $(a+b)+c=a+(b+c)$ y $(a\cdot b)\cdot c=a\cdot(b\cdot c)$, $\forall\ a,b,c \in A$
- $a+b=b+a$ y $a\cdot b=b\cdot a$ $\forall\ a,b \in A$.
- Existen elementos distintos o y 1 en A tales que $o+a=a+o=a$ y $1\cdot a=a\cdot 1=a$ $\forall\ a \in A$.
- $\forall\ a,b \in A$ con $b \neq o$ existen elementos c y d $\in A$ tales que $a+c=o$ y $b\cdot d=1$.
- $a\cdot(b+c)=a\cdot b+a\cdot c$ $\forall\ a,b,c \in A$.

Los elementos $a+b$ y $a\cdot b$ se llaman suma y producto de a y b respectivamente.
Los elementos 0 y 1 se llaman idéntico aditivo e idéntico multiplicativo respectivamente.
Los elementos c y d mencionados en la cuarta propiedad se llaman - inverso aditivo de a e inverso multiplicativo de b respectivamente

Algunos ejemplos de campos son los siguientes:

- El conjunto de números racionales con las operaciones de suma y producto definidas en forma usual.
  Este campo lo denotamos como $(\mathbb{Q},+,\cdot)$.

- El conjunto de números reales con las operaciones de suma y - producto definidas en forma usual.
  Este campo lo denotamos como $(\mathbb{R},+,\cdot)$.
- El conjunto de números reales de la forma $a+b\sqrt{2}$ donde $a,b \in \mathbb{Q}$ con la suma y producto como en $(\mathbb{R},+,\cdot)$.
  Este campo lo denotamos como $(\mathbb{Q}(\sqrt{2}),+,\cdot)$.
- El conjunto de números complejos cuyos elementos son de la forma $a+bi$ donde a,b estan en $\mathbb{R}$, con la suma y el producto definidas como sigue:

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i$$

  y donde

$$a+bi=c+di \iff a=c, \text{ y } b=d.$$

  Este campo lo denotamos como $(\mathbb{C},+,\cdot)$.
- El conjunto cuyos elementos sean los enteros módulo p, con p - un número primo, con las operaciones de suma y producto módulo p usuales.
  Este campo lo denotamos como $(\mathbb{Z}_p,+,\cdot)$.
  Por mencionar alguno: $(\mathbb{Z}_2,+,\cdot)$ donde $\mathbb{Z}_2=\{0,1\}$ y $0+0=0$, $0+1=1+0=1$, $1+1=0$, $0\cdot 0=0$, $0\cdot 1=1\cdot 0=0$ y $1\cdot 1=1$.

DEFINICION. Un Campo Finito es un Campo que tiene un número finito de elementos.

NOTACION. En el presente trabajo denotaremos un campo $(K,+,\cdot)$ simplemente como K.

EL ANILLO K[x] DE POLINOMIOS SOBRE UN CAMPO K.

Dado un campo K consideremos el conjunto :

$$K[x]=\{s:\mathbb{N}\cup\{o\}\longrightarrow K/s(n)=o \text{ para casi toda } n\in\mathbb{N}\cup\{o\}\}$$

En este conjunto definimos dos operaciones como sigue :

DEFINICION 1. Si s_1, $s_2 \in K[x]$ entonces $s_1+s_2:\mathbb{N}\cup\{o\}\longrightarrow K$ es tal que:

$$(s_1+s_2)(n)=s_1(n)+s_2(n)$$

s_1+s_2 se llama la suma de s_1 y s_2.

DEFINICION 2. Si $s_1, s_2 \in K[x]$ entonces $s_1\cdot s_2$: $\mathbb{N}\cup\{o\}\longrightarrow K$ es tal que :

$$(s_1\cdot s_2)(n)=\sum_{i+j=n} s_1(i)s_2(j)$$

$s_1\cdot s_2$ se llama producto de s_1 y s_2.

Es fácil ver que $s_1+s_2 \in K[x]$, por lo que sólo se demostrará el siguiente lema.

LEMA. Si $s_1 \in K[x]$ y $s_2 \in K[x]$ entonces $s_1s_2 \in K[x]$.

Demostración. Ya que $s_1 \in K[x]$ entonces existe $n_1 \in \mathbb{N}\cup\{o\}$ tal que si $N>n_1$ entonces $s_1(N)=o$. Análogamente existe $n_2 \in \mathbb{N}\cup\{o\}$ tal que si $N>n_2$ entonces $s_2(N)=o$. Sea $N>n_1+n_2$ y supongamos que $i+j=N$. Si $i>n_1$ entonces $s_1(i)=0$ por lo que $s_1(i)s_2(j)=o$. Si $i\leq n_1$ entonces $j>n_2$ por lo que $s_2(j)=0$ y entonces $s_1(i)s_2(j)=o$. Por lo tanto $(s_1s_2)(N)=\sum_{i+j=N} s_1(i)s_2(j)=0 \quad \forall\, N>n_1+n_2$ y por lo tanto:

$$s_1s_2 \in K[x]. \blacksquare$$

NOTA: $\blacksquare$ quiere decir que la demostración ha terminado.

PROPOSICION. $(K[x],+,\cdot)$ es un dominio entero con 1.

Es fácil probar que es un anillo conmutativo con 1, por lo que se demostrará aquí solamente que no tiene divisores de cero.

Demostración. Sean $s_1, s_2 \in K[x]$ tales que $s_1\neq o$, $s_2\neq o$ entonces existen $n,m \in \mathbb{N}\cup\{o\}$ tales que $s_1(n)\neq o$ y $s_1(N)=o \ \forall\, N>n$ y $s_2(m)\neq o$ con $s_2(N)=o \ \forall\, N>m$, entonces :

$$(s_1 s_2)(n+m) = \sum_{i+j=n+m} s_1(i)s_2(j)$$

pero si $i<n$ entonces $j>m$, de donde $s_1(i)s_2(j)=0$ y si $i>n$ entonces $s_1(i)s_2(j)=0$ y si $i=n$ entonces $j=m$ y $s_1(n)s_2(m)\neq 0$ por lo tanto $(s_1 s_2)(n+m)=s_1(n)s_2(m)\neq 0$, por lo que $s_1 s_2 \neq 0$. ■

NOTACION. Al dominio entero $(k[x],+,\cdot)$ se le acostrumba llamar Anillo de Polinomios en la indeterminada x con coeficientes en K y se denota simplemente como $K[x]$.
Definimos a continuación una función que va del Campo K en el Anillo $K[x]$.

DEFINICION. Sea $\phi: K \longrightarrow K[x]$ tal que $\phi(a): \mathbb{N} \cup \{0\} \longrightarrow K$ y tal que $(\phi(a))(0)=a$ y $(\phi(a))(n)=0$ $\forall$ $n \in \mathbb{N}$.
Si al elemento $s \in K[x]$ tal que $s(0)=a$ y $s(n)=0$ $\forall$ $n\neq 0$ lo denotamos como :

$$(a,0,0,0,\ldots)=\bar{0}$$

Podemos ver que ϕ es un monomorfismo de anillos ya que:

$$\phi(a+b)=(a+b,0,0,\ldots)=(a,0,0,\ldots)+(b,0,0,\ldots)=\phi(a)+\phi(b)$$

y además

$$\phi(ab)=(ab,0,0,\ldots)=(a,0,0,\ldots)(b,0,0,\ldots)=\phi(a)\phi(b)$$

y además si

$$\phi(a)=\bar{0}=(0,0,\ldots) \text{ entonces } a=0. \blacksquare$$

Esto nos permite identificar a K como un subcampo del Anillo $k[x]$.
Así, las sucesiones de la forma

$$(a,0,0,\ldots)$$

las identificamos con a.
Se dará a continuación una definición que nos permitirá, por un lado aclarar el significado de la frase " la indeterminada x ", y por otro lado nos permitirá recuperar la forma que generalmente se les dá a los polinomios.

DEFINICION. Al elemento $(0,1,0,0,\ldots) \in K[x]$ se le llama x, es decir:

$$(0,1,0,0,\ldots)=x.$$

Se puede probar por inducción que si $n>0$ y

$$s(j)=\begin{cases} 1 \text{ para } j=n \\ 0 \text{ para } j\neq n \end{cases}$$

entonces $s=x^n$ y en consecuencia se puede probar que todo elemento de $K[x]$ se puede escribir como

$$f(x)=a_0+a_1x+\ldots+a_nx^n$$

con $a_i \in K$, para $i=1,2,\ldots,n$.
A los elementos de $K[x]$ les llamaremos como es usual, polinomios en la indeterminada x, y a los que estan en la imagen de K bajo ϕ les llamaremos polinomios constantes.

DEFINICION. Supongamos que $f(x)=a_0+a_1x+\ldots+a_nx^n$ con $a_n\neq 0$ entonces el grado de $f(x)$ es n y lo denotamos como $grd(f(x))=n$, $grd(\bar{0})=-\infty$ y definimos $n+(-\infty)=(-\infty)+n=(-\infty)+(-\infty)=n(-\infty)=(-\infty)n=-\infty$ y $-\infty<n$ --

$$\forall\ n \in \mathbb{N} \cup \{0\} \circ (-\infty)$$

Las siguientes proposiciones son consecuencia de lo visto anteriormente.

PROPOSICIONES.

$$grd(f+g)\leq \max(grd(f),grd(g))$$

$$grd(fg)=grd(f)+grd(g)$$

$$grd(f^n)=n\ grd(f).\quad \forall\ n \in \mathbb{N}.$$

DEFINICION. Se llaman unidades de un anillo a todos aquellos elementos del anillo que tienen inverso multiplicativo.

COROLARIO. Las unidades de $K[x]$ son los elementos de $K^*=K-\{0\}$.

Demostración. Como el $grd(1)=0$ se tiene que si $f(x)$ es unidad entonces existe $g(x) \in K[x]$ tal que $f(x)g(x)=1$ entonces el $grd(f(x))+grd(g(x))=0$ por lo que el $grd(f(x))=0$ y por lo tanto $f(x)=cte\neq 0$ y si $f(x)=a\neq 0$ entonces existe $1/a$ tal que $a\cdot 1/a=1$ y $1/a \in K[x]$ por lo que a es unidad. ■

ALGORITMO DE LA DIVISION.

Sean $f(x)$, $g(x) \in K[x]$ con $g(x) \neq 0$ entonces existen únicos $q(x)$, $r(x) \in K[x]$ tales que $f(x)=g(x)q(x)+r(x)$ con $grd(r(x))<grd(g(x))$.

Demostración. Se probará la existencia por inducción sobre $grd(f(x))$.
Si $grd(f)=-\infty$ entonces $f(x)=0$ y $0=g(x)0 + 0$ y $-\infty<grd(g(x))$, supongámoslo cierto para $k<n=grd(f(x))$ con $n\geq 0$, como el $grd(f(x))=n\geq 0$ entonces $f(x)\neq 0$. Supongamos que

$$f(x)=a_0+a_1x+\ldots+a_nx^n$$

con $a_n\neq 0$. Si $n<grd(g(x))$ entonces $f(x)=g(x)0+f(x)$ y el $grd(f(x))<grd(g(x))$. Si $n\leq grd(g(x))=m$, sea $g(x)=b_0+b_1x+\ldots+b_mx^m$ con $b_m\neq 0$ entonces $f_1(x)=f(x)-g(x)[\frac{a_n}{b_m}x^{n-m}]$ es tal que $grd((f_1(x))<grd(f(x))$ y por hipótesis de inducción $f_1(x)=g(x)q_1(x)+r(x)$ con $grd(r(x))<grd(g(x))$ entonces $f(x)=g(x)[q_1(x)+\frac{a_n}{b_m}x^{n-m}]+r(x)$ y

$$grd(r(x))<grd(g(x))$$

Para probar la unicidad supóngase que
$f(x)=g(x)q_1(x)+r_1(x)=g(x)q(x)+r(x)$ con $grd(r(x))<grd(g(x))$ y $grd(r_1(x))<grd(g(x))$ entonces $g(x)[q(x)-q_1(x)]=r_1(x)-r(x)$ esto implica que $grd(g(x))+grd(q(x)-q_1(x))=grd[g(x)(q(x)-q_1(x))]=grd(r_1(x)-r(x))\leq max(grd(r_1(x),grd(r(x))<grd(g(x))$ esto implica que $grd(q(x)-q_1(x))=-\infty$ por lo que $q(x)=q_1(x)$ y $r(x)=r_1(x)$. ■
Y se tiene que $K[x]$ es un Anillo Euclidiano.

OBSERVACION. Dado $f(x) \in K[x]$ sus asociados son de la forma $af(x)$ con $a\neq 0$.

DEFINICION. Un polinomio $f(x)\neq 0$ es mónico si es de la forma -

$$f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}+x^n.$$

PROPOSICION. Dado un $f(x)\neq 0$, existe un único polinomio mónico asociado él.

Demostración. Si $f(x)=a_0+a_1x+\ldots+a_nx^n$ con $a_n\neq 0$ entonces $1/a_n f(x)$

es un mónico asociado a $f(x)$ y la unicidad se sigue de la -- observación anterior.

DEFINICION. Un polinomio $f(x) \in K[x]$ se llama polinomio primo si no puede ser factorizado en polinomios de grado menor que él en $K[x]$ salvo asociados.
A los polinomios primos les llamamos también irreducibles.
Por ser $K[x]$ anillo euclidiano es anillo de factorización única, entonces se tiene que si $f(x) \neq 0$ entonces $f(x)$ se puede expresar como una unidad por el producto de mónicos irreducibles y esta descomposición es única salvo por el orden.

PROPOSICION. Todo polinomio de grado 1 es irreducible.

Demostración. Sea $f(x)=ax+b$ con $a \neq 0$ entonces si $f(x)=g(x)q(x)$ se tiene que $1=grd(f(x))=grd(g(x))+grd(q(x))$ entonces si $grd(g(x))=1$ entonces el $grd(q(x))=0$ entonces $q(x)$ es unidad por lo que $g(x)$ - es asociado, o bien, si $grd(g(x))=0$ entonces $g(x)=cte$. ■
Como dos m.c.d. de $f(x)$ y $g(x)$ son asociados entonces denotamos - $(f(x),g(x))$ al m.c.d. mónico de $f(x)$ y $g(x)$ si alguno es distinto de cero, y $(0,0)=0$, y cuando hablemos del m.c.d. de $f(x)$ y $g(x)$ - nos referimos a éste.

LEMA. Sean $f(x),g(x) \in K[x]$ con $g(x) \neq 0$ y supóngase que $f(x)=g(x)q(x)+r(x)$ entonces $(f(x),g(x))=(g(x),r(x))$.
Demostración. Si $h|f$ y $h|g$ entonces $h|f-gq$ esto implica que $h|r$, y si $h|g$ y $h|r$ entonces $h|gq+r$ de donde $h|f$ y el lema se sigue. ■

ALGORITMO DE EUCLIDES. sean $f(x),g(x) \in K[x]$ con $g(x) \neq 0$ supóngase que

$$f(x)=g(x)q_1(x)+r_1(x) \quad \text{con} \quad -\infty < grd(r_1(x)) < grd(g(x))$$
$$g(x)=r_1(x)q_2(x)+r_2(x) \quad \text{con} \quad -\infty < grd(r_2(x)) < grd(r_1(x))$$
$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$
$$r_{n-2}(x)=r_{n-1}(x)q_n(x)+r_n(x) \quad \text{con} \quad -\infty < grd(r_n(x)) < grd(r_{n-1}(x))$$
$$r_{n-1}=r_n(x)q_{n-1}(x)$$

Entonces el mónico asociado a $r_n(x)$ es el m.c.d. de $f(x)$ y $g(x)$.

Demostración. Por el lema anterior se tiene que

$$(f,g)=(g,r_1)=(r_1,r_2)=\ldots=(r_{n-1},r_n)=(r_n,0).$$

Es claro que dados $f,g \in K[x]$ con $g(x)\neq 0$ entonces se puede repetir iteradamente el algoritmo de la división a los residuos y este proceso termina como se supuso en el agoritmo de Euclides puesto que $grd(g)>grd(r_1)>\ldots>grd(r_n)$. ■

Sean K,E campos, y sea K un subcampo de E. Para cada $\alpha \in E$ definiremos una función ϕ_α del anillo K[x] en el campo E, que será un homomorfismo de anillos y que llamaremos homomorfismo de evaluación en α.

DEFINICION. sean K un subcampo de E y $\alpha \in E$, sea $\phi_\alpha: K[x]\longrightarrow E$ tal que $\phi_\alpha(a_0+a_1x+\ldots+a_nx^n)=a_0+a_1\alpha+\ldots+a_n\alpha^n$.
Observemos por ejemplo que $\phi_\alpha(a_0)=a_0$ y que $\phi_\alpha(x)=\alpha$.
La función así definida es un homomorfismo puesto que si $f(x)=a_0+a_1x+\ldots+a_nx^n$, $g(x)=b_0+b_1x+\ldots+b_mx^m$, y $h(x)=f(x)+g(x)=c_0+c_1x+\ldots+c_rx^r$ entonces $\phi_\alpha(h(x))=c_0+c_1\alpha+\ldots+c_r\alpha^r$ mientras que $\phi_\alpha(f(x))+\phi_\alpha(g(x))=(a_0+a_1\alpha+\ldots+a_n\alpha^n)+(b_0+b_1\alpha+\ldots+b_m\alpha^m)$ como por definición de suma $c_i=a_i+b_i$ tenemos que $\phi_\alpha(f(x)+g(x))=\phi_\alpha(f(x))+\phi_\alpha(g(x))$.
Por otro lado si $f(x)g(x)=d_0+d_1x+\ldots+d_sx^s$ entonces $\phi_\alpha(f(x)g(x))=d_0+d_1\alpha+\ldots+d_s\alpha^s$ mientras que $\phi_\alpha(f(x))\phi_\alpha(g(x))=(a_0+a_1\alpha+\ldots+a_n\alpha^n)(b_0+b_1\alpha+\ldots+b_m\alpha^m)$, como por definición de multiplicación $d_k=\sum_{i+j=k} a_ib_j$ vemos que $\phi_\alpha(f(x)g(x))=\phi_\alpha(f(x))\phi_\alpha(g(x))$ y así ϕ_α es un homomorfismo de anillos, que se llama el homomorfismo de evaluación en α.

NOTACION. A $\phi_\alpha(f(x))$ la denotaremos como $f(\alpha)$, es decir :

$$\phi_\alpha(f(x))=f(\alpha)=a_0+a_1\alpha+\ldots+a_n\alpha^n.$$

DEFINICION. Si K es un subcampo de E y $\alpha \in E$ entonces decimos que α es una raíz o cero de $f(x)$ si $\phi_\alpha(f(x))=f(\alpha)=0$.

TEOREMA DEL FACTOR. Un elemento $\alpha \in K$ es una raíz de

$$f(x) \in K[x]$$

si y sólo si $x-\alpha$ es factor de $f(x)$.

Demostración. Supongamos que $\alpha \in K$ y que $f(\alpha)=0$. Por el algoritmo de la división existen polinomios únicos $q(x)$, $r(x) \in K[x]$ tales que $f(x)=(x-\alpha)q(x)+r(x)$ donde $grd(r(x)<1$ y por lo tanto $r(x)=r \in K$ de modo que $f(x)=(x-\alpha)q(x)+r$. Aplicando el homomorfismo de evaluación $\phi_\alpha : K[x] \rightarrow K$ vemos que $f(\alpha)=(\alpha-\alpha)q(\alpha)+r=r$ de modo que $r=0$ y entonces $f(x)=(x-\alpha)q(x)$ es decir $x-\alpha$ es factor de $f(x)$.
Recíprocamente si $x-\alpha$ es factor de $f(x) \in K[x]$ donde $\alpha \in K$ entonces, aplicando nuevamente el homomorfismo de evaluación a $f(x)=(x-\alpha)q(x)$ tenemos que $f(\alpha)=(\alpha-\alpha)q(\alpha)=0$ es decir α es una raíz de $f(x)$. ■

COROLARIO. Un polinomio distinto de cero $f(x) \in K[x]$ de grado n puede tener a lo más n raíces en el campo K.

Demostración. De acuerdo al teorema anterior, una raíz $\alpha_1 \in K$ de $f(x)$ resultará en la factorización $f(x)=(x-\alpha_1)q_1(x)$ donde $grd(q_1(x))=n-1$. Una raíz $\alpha_2 \in K$ de $q_1(x)$ resultará en la factorización $f(x)=(x-\alpha_1)(x-\alpha_2)q_2(x)$ donde claramente $grd(q_2(x))=n-2$. Continuando este proceso, por inducción, llegamos a que $f(x)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_r)q_r(x)$, donde $q_r(x)$ no tiene más raíces en K, obviamente $r \leq n$, además, si $\beta \neq \alpha_i$ para $i=1,2,\ldots,r$ y $\beta \in K$ entonces $f(\beta)=(\beta-\alpha_1)(\beta-\alpha_2)\ldots(\beta-\alpha_r)q_r(\beta) \neq 0$. Puesto que K no tiene divisores de cero y por construcción ninguno de los $\beta-\alpha_i$ o $q_r(\beta)$ son cero. De aquí que las α_i para $i=1,2,\ldots,r \leq n$ son todas las raíces de $f(x) \in K[x]$.

CAPITULO II

TEORIA DE CAMPOS

CARACTERISTICA DE CAMPOS.

DEFINICION. Sea K un campo, entonces, en particular es un anillo. Si 1 es el idéntico de K, decimos, para $n \in \mathbb{N}$

$$n \cdot 1 = \underbrace{1+1+\ldots+1}_{n\text{-veces}}$$

$$(-n)1 = -(n \cdot 1) \quad \text{y} \quad 0 \cdot 1 = 0.$$

La función $\phi: \mathbb{Z} \to K$ dada por $\phi(n) = n \cdot 1$ es un homomorfismo de anillos pues:

$$\phi(m+n) = (m+n) \cdot 1 = (m \cdot 1) + (n \cdot 1) = \phi(m) + \phi(n)$$

y

$$\phi(m \cdot n) = (m \cdot n) \cdot 1 = (m \cdot 1)(n \cdot 1) = \phi(m)\phi(n).$$

El núcleo de ϕ es un ideal de $\mathbb{Z}$ y todos los ideales de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$ para algún m en $\mathbb{Z}$, luego entonces consideremos los siguientes dos casos.

1.- Si $m=0$ entonces $\text{Ker}\phi = 0\mathbb{Z} = \langle 0 \rangle$ y por lo tanto ϕ es un monomorfismo, identificamos a $\mathbb{Z}$ con su imagen bajo ϕ que es $\phi(\mathbb{Z})$, es decir $K \supset \mathbb{Z}$. Como $K \supset \mathbb{Z}$, $K \supset \mathbb{Q}$ que es el campo de cocientes de $\mathbb{Z}$.
Cuando esto es así, decimos que la característica del campo K es - cero.

2.- Si $m \neq 0$ entonces $\text{Ker}\phi = m\mathbb{Z}$ y por el teorema fundamental de homo_ morfismos $\phi(\mathbb{Z}) \simeq \mathbb{Z}/\text{Ker}\phi = \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}m$ luego entonces $K \supset \mathbb{Z}m$, es decir $\mathbb{Z}m$ no tiene divisores de cero, o sea que, m es primo, y escribimos: $m=p$ y $K \supset \mathbb{Z}p$.
Cuando esto es así, decimos que la característica de K es p.

DEFINICION. Si $n \in \mathbb{N}$ y $a \in K$ entonces $n \cdot a = \underbrace{a+a+\ldots+a}_{n\text{-veces}}$.

TEOREMA. Para $n \in \mathbb{N}$, $n \cdot a = 0$ $\forall$ $a \in K$ si y sólo si $n \cdot 1 = 0$.

Demostración. Si $n \cdot a = 0$ $\forall$ $a \in K$, en particular $n \cdot 1 = 0$.
Recíprocamente. Supóngase que $n \in \mathbb{N}$ tal que $n \cdot 1 = 0$ entonces $\forall$ $a \in K$

$$n\cdot a=\underbrace{a+a+\ldots\ldots+a}_{n\text{-veces}}=a(\underbrace{1+1+\ldots\ldots+1}_{n\text{-veces}})=a(n\cdot 1)=a\cdot o=o.\ \blacksquare$$

En consecuencia si la característica de K es p entonces $p\cdot a=o$ -- $\forall\ a\in K$.

EXTENSION DE CAMPOS.

DEFINICION. Si K y E son campos y K es un subcampo de E entonces decimos que E es una extensión de K.

PROPOSICION. Si E es una extensión de K entonces E es un espacio vectorial sobre K con la operación $\cdot: K\times E\longrightarrow E$ tal que

$$(a,b)\longrightarrow ab.$$

DEFINICION. Sea E una extensión de K entonces el grado de la extensión de E sobre K es la dimensión de E como espacio vectorial sobre K y lo denotamos por $[E:K]$.
Para nosotros es de particular interés el caso en que $[E:K]$ es finito. Esta situación se describe diciendo que E es una extensión finita de K.

TEOREMA. Si E es una extensión finita de K y K es una extensión finita de F entonces E es una extensión finita de F y además $[E:F]=[E:K][K:F]$.

Demostración. Supongamos que $[E:K]=m$ y que $[K:F]=n$. sea $v_1,v_2,\ldots,v_m$ una base de E sobre K y $w_1,w_2,\ldots,w_n$ una base de K sobre F.
Sea t un elemento cualquiera de E, como todo elemento de E es una combinación lineal de $v_1,v_2,\ldots,v_m$ con coeficientes en K, el elemento t debe ser en particular de esa forma. Luego $t=k_1v_1+k_2v_2+\ldots+k_mv_m$, donde los elementos $k_1,\ldots,k_m$ estan todos en K. Pero todo elemento de K es una combinación lineal de $w_1,\ldots,w_n$ con coeficientes en F. Luego $k_1=f_{11}w_1+\ldots+f_{1n}w_n,\ldots,k_i=f_{i1}w_1+\ldots+f_{in}w_n,\ldots,k_m=f_{m1}w_1+\ldots+f_{mn}w_n$, donde todas las f_{ij} estan en F. Sustituyendo por estas expresiones a $k_1,\ldots,k_m$ en $t=k_1v_1+k_2v_2+\ldots+k_mv_m$ obtenemos $t=(f_{11}w_1+\ldots+f_{1n}w_n)v_1+\ldots+(f_{m1}w_1+\ldots+f_{mn}w_n)v_m$.
Efectuando las operaciones indicadas, llegamos finalmente a ---

$t=f_{11}v_1w_1+\ldots+f_{1n}v_1w_n+\ldots+f_{ij}v_iw_j+\ldots+f_{mn}v_mw_n$. Como los f_{ij} estan en F, hemos expresado t como combinación lineal sobre F de los elementos v_iw_j. Por tanto, los elementos v_iw_j generan ciertamente a E sobre F y por tanto, satisfacen la primera propiedad que se requiere para una base.

Debemos probar que los elementos v_iw_j son linealmente independientes sobre F.

Supongamos que $f_{11}v_1w_1+\ldots+f_{1n}v_1w_n+\ldots+f_{ij}v_iw_j+\ldots+f_{mn}v_mw_n=o$ donde los $f_{ij}\in F$. Reagrupando la expresión anterior se tiene que:

$(f_{11}w_1+\ldots+f_{1n}w_n)v_1+\ldots+(f_{i1}w_1+\ldots+f_{in}w_n)v_i+\ldots+(f_{m1}w_1+\ldots+f_{mn}w_n)v_m=o$ com las w_i estan en K y como K⊃F, todos los elementos $k_i=f_{i1}w_1+\ldots+f_{in}w_n$ estan en K. Y tenemos que $k_1v_1+\ldots+k_nv_m=o$ con $k_1,\ldots,k\in K$. Pero por hipotesis $v_1,\ldots,v_m$ forman una base de E sobre K, luego, en particular, deben ser linealmente independientes sobre K. Por lo tanto $k_1=k_2=\ldots=k_m=o$. Usando los valores explícitos de k_i tenemos que $f_{i1}w_1+\ldots+f_{in}w_n=o$ para $i=1,2,\ldots,m$.

Pero si recordamos el hecho de que las w_i son linealmente independientes sobre F, llegamos a la conclusión de que todas las f_{ij} -- han de ser nulas.

Hemos probado que las v_iw_j son linealmente independientes sobre f y de esta forma satisfacen la otra propiedad requerida por una base.

Hemos logrado probar que los mn elementos v_iw_j forman una base de E sobre F. Luego $[E:F]=mn$, como $m=[E:K]$ y $n=[K:F]$, hemos obtenido el resultado buscado que es $[E:F]=[E:K][K:F]$. ■

Supongamos que E,K,F son tres campos en la relación E⊃K⊃F y supongamos que [E:F] es finito. Es claro que cualesquiera elementos sobre E linealmente independientes sobre K son también linealmente - independientes sobre F. Luego, la hipotesis de que [E:F] es finito fuerza la conclución de que [E:K] es también finito. Además, como K es un subespacio de E, [K:F] es finito. Por el teorema $[E:F]=[E:K][K:F]$, de donde $[K:F]\mid[E:F]$. Hemos probado el siguiente

COROLARIO. Si E es una extensión finita de F y K es un subcampo de E que contiene a F entonces $[K:F]\mid[E:F]$. Así, por ejemplo, - si [E:F] es un múmero primo, no puede haber ningún campo

propiamente entre F y E.

DEFINICION. Sea una extensión de K, un elemento $\alpha \in E$ se dice que es algebráico sobre K si existe un polinomio $f(x) \in K[x]$ distinto del polinomio cero, tal que $f(\alpha)=0$.
En caso contrario se dice que α es trascendente sobre K, es decir, que si $f(\alpha)=0$ para algún $f(x) \in K[x]$ entonces $f(x)=0$.

DEFINICION. Una extención E sobre un campo K se llama algebráica si todos los elementos de E son algebráicos sobre K.
En caso contrario se dice que la extensión es trascendente.

TEOREMA DE KRONECKER. Sea K un campo y $f(x) \in K[x]$ con $f(x) \neq 0$ entonces existe un campo E extensión de K en el que $f(x)$ tiene una raíz α.

Demostración. El polinomio $f(x)$ se puede factorizar en $K[x]$ en polinomios que son irreducibles sobre K. Sea $p(x)$ un polinomio irreducible en dicha factorización, así, el ideal $\langle p(x)\rangle$ de $K[x]$ generado por $p(x)$ es maximal y por lo tanto $K[x]/\langle p(x)\rangle$ es un campo. El campo K puede ser identificado con un subcampo de $K[x]/\langle p(x)\rangle$ de manera natural mediante la transformación

$$\psi: K \longrightarrow k[x]/\langle p(x)\rangle$$

dada por $\psi(a)=a+\langle p(x)\rangle$ para $a \in K$. Esta transformación es inyectiva, pues si $a+\langle p(x)\rangle=b+\langle p(x)\rangle$ para algunos $a,b \in K$ entonces $a-b \in \langle p(x)\rangle$, y esto puede suceder sólo a cuenta de que $a-b=0$, es decir, que $a=b$. Además, si sumamos y multiplicamos escogiendo cualesquiera representantes, como por ejemplo, $a \in (a+\langle p(x)\rangle)$, vemos que ψ es un monomorfismo de K en $K[x]/\langle p(x)\rangle$. Hacemos la identificación de K con $\{a+\langle p(x)\rangle / a \in K\}$ mediante dicho monomorfismo, de este modo podemos considerar a $k[x]/\langle p(x)\rangle$ como una extensión de K.
Ahora hagamos a $\alpha=x+\langle p(x)\rangle$ de modo que $\alpha \in E$ con $E=K[x]/\langle p(x)\rangle$. Consideremos a la vez el homomorfismo de evaluación usual $\phi_\alpha: K[x] \longrightarrow E$. Si $p(x)=a_0+a_1x+\ldots+a_nx^n$ es un elemento de $k[x]$, entonces $\phi_\alpha(p(x))=p(\alpha)=a_0+a_1\alpha+\ldots+a_n\alpha^n=a_0+a_1[x+\langle p(x)\rangle]+\ldots+a_n[x+\langle p(x)\rangle]^n$

de donde $p(\alpha)=(a_o+a_1x+\ldots+a_nx^n)+\langle p(x)\rangle=p(x)+\langle p(x)\rangle=\langle p(x)\rangle=o$ en -- $K[x]/\langle p(x)\rangle$.

Hemos encontrado así, un elemento $\alpha \in E = K[x]/\langle p(x)\rangle$ de manera que $p(\alpha)=o$ y por lo tanto $f(\alpha)=o$. ■

COROLARIO. Sea K un campo y $f(x) \in K[x]$, entonces existe un campo E extensión de K en el que $f(x)$ tiene todas sus raíces.

Demostración. De acuerdo al teorema enterior, existe una extensión E_o de K en el que $f(x)$ tiene una raíz α, así, en $E_o[x]$, $f(x)$ se -- factoriza como $f(x)=(x-\alpha)q(x)$, donde $q(x)$ es de grado $n-1$, conti-- nuando este proceso, vemos, por inducción, que existe una extensión E de E_o en el que $q(x)$ tiene $n-1$ raíces. Como cualquier raíz de $f(x)$ es α o una raíz de $q(x)$, obtenemos así, en E, todas las raíces de $f(x)$. ■

PROPOSICION. Sean K y E campos con E extensión de K, sea $\alpha \in E$ y $\phi_\alpha: K[x] \rightarrow E$ el homomorfismo de evaluación usual. Consideremos los siguientes dos casos.

1.- α algebráico sobre K.

Entonces el núcleo de ϕ_α es ideal maximal $\langle f(x)\rangle$ de $K[x]$ don de α es la raíz del polinomio $f(x)$ irreducible sobre K. Esto implica que $K[x]/\langle f(x)\rangle$ es un campo isomorfo a la ima- gen de $\phi_\alpha(k(x))$ en E, este campo $\phi_\alpha(k(x))$ subcampo de E, es claramente elmenor subcampo de E que contiene a K y a α.

Denotamos este campo como $K(\alpha)$.

2.- α trascendente sobre K.

Entonces ϕ_α es un monomorfismo que transforma $K[x]$ en E, pero en este caso, $\phi_\alpha(K[x])$ no es un campo, sino un dominio entero que denotamos por $K[\alpha]$. por ser $K[\alpha]$ dominio entero E contiene al campo de cocientes de $K[\alpha]$, el cual es, el menor subcampo de E que contiene a K y a α. Como en el caso 1, denotamos a este campo por $K(\alpha)$.

DEFINICION. Un campo E extensión de un campo K se llama extensión simple de K si $E=K(\alpha)$ para algun $\alpha \in E$.

TEOREMA. Sea $E=K(\alpha)$ con α algebráico sobre K, y $f(x)=irr(K,\alpha)$ el polinomio mónico de grado n e irreducible sobre K del cual α es raíz, entonces todo elemento $\beta \in K(\alpha)$ puede expresarse de manera única en la forma $\beta=b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1}$ donde toda $b_i \in K$.

Demostración. Para el homomorfismo de evaluación ϕ_α todo elemento de $\phi_\alpha(K[x])=K(\alpha)$ es de la forma $\phi_\alpha(g(x))=g(\alpha)$ es decir, tiene la forma de un polinomio formal en α con coeficientes en K. Supongamos que $f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}+x^n=irr(K,\alpha)$ entonces por hipótesis $f(\alpha)=0$ de modo que $\alpha^n=-a_{n-1}\alpha^{n-1}-\ldots-a_0$. Esta evaluación que esta en $K(\alpha)$ se puede usar para expresar cualquier monomio α^m para $m\geq n$ en términos de potencias de α que son menores que n, por ejemplo $\alpha^{n+1}=\alpha\alpha^n=-a_{n-1}\alpha^n-a_{n-2}\alpha^{n-1}-\ldots-a_0\alpha=-a_{n-1}(-a_{n-1}\alpha^{n-1}-\ldots-a_0)-a_{n-2}\alpha^{n-1}-\ldots-a_0\alpha$. Así pues, si $\beta \in K(\alpha)$ entonces $\beta=g(\alpha)$ para algún $g(x) \in K[x]$, de donde $\beta=c_0+c_1\alpha+\ldots+c_m\alpha^m$. Y como todas las potencias de α mayores que $n-1$ se pueden expresar en términos de potencias de α menores que n, se tiene que $\beta=b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1}$. Ahora bien si $b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1}=b'_0+b'_1\alpha+\ldots+b'_{n-1}\alpha^{n-1}$ con $b_i, b'_i \in K$, entonces $(b_0-b_0')+(b_1-b_1')x+\ldots+(b_{n-1}-b'_{n-1})x^{n-1}=g(x)$ con $g(x) \in K[x]$, $g(\alpha)=0$ y $grd(g(x))<n$, debemos tener que $g(x)=0$ y por lo tanto $b_i-b'_i=0$ es decir $b_i=b'_i$. Lo que demuestra la unicidad. En esta forma no sólo demostramos que $\beta \in K(\alpha)$ puede expresarse de manera única en la forma $\beta=b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1}$ sino que ciertamente, probamos el resultado más preciso y que constituye realmente el corazón del teorema, que es: $[K(\alpha):K]=n$, y además una base de $K(\alpha)$ sobre K es:

$$\{1,\alpha,\ldots,\alpha^{n-1}\}\ .\ \blacksquare$$

TEOREMA. Si E es una extensión finita del campo K entonces E es algebráico sobre K.

Demostración. Supongamos que $\alpha \in E$ y que E es una extensión finita de K de grado m , $[E:K]=m$, entonces todos los elementos $1,\alpha,\ldots,\alpha^m$ estan en E, y son $m+1$. Estos elementos son linealmente dependientes sobre K, por tanto, hay elementos $a_0,a_1,\ldots,a_m \in K$, no todos cero, tales que $a_01+a_1\alpha+\ldots+a_m\alpha^m=0$. Luego entonces, α es

algebráico sobre K. ■

TEOREMA. Si a,b ∈ E y son algebráicos sobre el campo K, entonces, a±b,ab,a/b (si b≠o) son algebráicos sobre K.

Demostración. Supongamos que a,b son algebráicos sobre K de grado m y n respectivamente. Por el teorema anterior tenemos que K(a) es un subcampo de E de grado m y a fortiori b es algebráico de grado cunto más n sobre K(a)=F. Como [E:K]=[E:F][F:K] tenemos que [E:K]≤mn, E es por tanto una extensión finita de K. Como a,b ∈ E, tenemos que a±b,ab,a/b (si b≠o) estan en E, y como la extensión es finita, estos elementos son algebráicos sobre K. En otras palabras si E es extensión de K entonces {α ∈ E/α es algebráico sobre K} es un subcampo de E que contiene a K. ■

DEFINICION. Sea f(x) ∈ K[x]. Una extensión finita E del campo K se dice que es un campo de descomposición de f(x) sobre K si f(x) puede ser descompuesto en un producto de factores lineales sobre E pero no en ningún subcampo propio de E.

ISOMORFISMO DE CAMPOS.

DEFINICION. Un isomorfismo entre campos es un homomorfismo biyectivo entre dichos campos.
Si K y K' son dos campos y τ es un isomorfismo de K sobre K', denotamos τ(α)=α' si α ∈ K. Para un polinomio arbitrario $f(x)=a_o+a_1x+\ldots+a_nx^n \in K[x]$, definimos $\tau^*(f(x))=\alpha'_o+\alpha'_1t+\ldots+\alpha'_nt^n$ en K'[t].

LEMA. τ^* define un isomorfismo de K[x] sobre K'[t] con la propiedad de que $\tau^*(\alpha)=\alpha'$ ∀ α ∈ K.
Si f(x) ∈ K[x] escribimos $\tau^*(f(x))$ como f'(t). Las consecuencias inmediatas de este lema son que las factorizaciones de f(x) ∈ K[x] van a dar a factorizaciones análogas de f'(t) ∈ K'[t] y viceversa, en particular f(x) es irreducible en K[x] si y sólo si f'(t) es irreducible en K'[t].

LEMA. Hay un isomorfismo τ^{**} de $K[x]/\langle f(x)\rangle$ sobre $K'[t]/\langle f'(t)\rangle$ con la propiedad de que $\forall\ \alpha \in K$, $\tau^{**}(\alpha)=\alpha'$.

TEOREMA. Si $p(x)$ es irreducible en $K[x]$ y si v es una raíz de $p(x)$ entonces $K(v)$ es isomorfo a $K'(w)$, donde w es una raíz de $p'(t)$. Demás , este isomorfismo σ puede escogerse de modo que $\sigma(v)=w$ y $\sigma(\alpha)=\alpha'$ $\forall\ \alpha \in K$.

Demostración. Sea v una raíz del polinomio $p(x)$ con $v \in E$ y E una extensión de K. Sea $M=\{f(x) \in K[x]/f(v)=0\}$. M es un ideal de $K[x]$, $M\neq K[x]$, como $p(x) \in M$ y es irreducible, tenemos que $M=\langle p(x)\rangle$. Transformemos $K[x]$ en $K(v)\subset E$ con la aplicación ψ definida por $\psi(q(x))=q(v)$ para toda $q(x) \in K[x]$. El núcleo de ψ es precisamente M, luego debe ser $\langle p(x)\rangle$. Según el teorema fundamental de homomorfismos de anillos, hay un isomomorfismo ψ^* de $K[x]/\langle p(x)\rangle$ sobre $K(v)$ que deja todos los elementos de K fijos y con la propiedad de que $v=\psi^*[x+\langle p(x)\rangle]$. Como $p(x)$ es irreducible en $K[x]$, $p'(t)$ es irreducible en $K'[t]$ y por tanto hay un ismorfismo σ^* de $K'[t]/\langle p'(t)\rangle$ sobre $K(w)$, donde w es una raíz de $p'(t)$ tal que σ^* deja fijos todos los elementos de K' y tal que $\sigma^*[t+\langle p'(t)\rangle]=w$. De acuerdo con el lema anterior hay un isomorfismo τ^{**} de $K[x]/\langle p(x)\rangle$ sobre $K'[t]/\langle p'(t)\rangle$ que coincide con τ sobre K y que lleva $x+\langle p(x)\rangle$ sobre $t+\langle p'(t)\rangle$. Consideremos la aplicación

$$\sigma=\sigma^*[\tau^{**}(\psi^*)^{-1}]$$

definida por :

$$K(v)\xrightarrow{(\psi^*)^{-1}} K[x]/\langle p(x)\rangle \xrightarrow{\tau^{**}} K'[t]/\langle p'(t)\rangle \xrightarrow{\sigma^*} K'(w)$$

de $K(v)$ sobre $K'(w)$.
Es un isomorfismo de $K(v)$ sobre $K'(w)$ ya que todas las aplicaciones ψ^*, τ^{**} y σ^* son isomorfismos. Además como $w=\psi^*[x+\langle p(x)\rangle]$ entonces

$$\sigma(v)=\sigma^*\tau^{**}[(\psi^*)^{-1}(v)]=\sigma^*[\tau^{**}(x+\langle p(x)\rangle)]=\sigma^*[t+\langle p'(t)\rangle]=w.$$

Además para $\alpha \in K$

$$\sigma(\alpha)=\sigma^*\tau^{**}[(\psi^*)^{-1}(\alpha)]=\sigma^*[\tau^{**}(\alpha)]=\sigma^*(\alpha')=\alpha'.$$

que es lo que queriamos demostrar. ■

COROLARIO. si $p(x) \in K[x]$ es irreducible y a,b son dos raíces de $p(x)$ entonces $K(a)$, $k(b)$ son isomorfos, con un isomorfismo que lleva a en b y que deja fijos todos los elementos de K.

TEOREMA. Cualesquiera dos campos de descomposición Ey E' de los polinomios $f(x) \in K[x]$ y $f'(t) \in K'[t]$ respectivos, son isomorfos, con un isomorfismo ϕ con la propiedad de que $\phi(\alpha)=\alpha'$ $\forall$ $\alpha \in K$.

Demostración. Si $[E:K]=1$ entonces $E=K$, de donde $f(x)$ se descompone en un producto de factores lineales sobre el mismo K. $f'(t)$ también se descompone sobre K' en un producto de factores lineales, de donde $E'=K'$. Pero entonces $\phi=\tau$ nos proporciona el isomorfismo de E sobre E' que coincide con τ sobre K.

Supongamos ahora que el resultado es cierto para cualquier campo K_o y cualquier polinomio $f(x) \in K_o[x]$ con tal de que el grado de algún campo de descomposición E_o de $f(x)$ sea menor que n sobre K_o, es decir, $[E_o:K_o]<n$. Supongamos que $[E:K]=n>1$, donde E es un campo de descomposición de $f(x)$ sobre K. Como $n>1$, $f(x)$ tiene un factor irreducible $p(x)$ de grado $r>1$. Sea $p'(t)$ el correspondiente factor irreducible de $f'(t)$. Como E descompone a $f(x)$. Un juego completo de raíces de $f(x)$ y por tanto, de raíces de $p(x)$, estan en E. De esta manera, hay un $v \in E$ tal que $p(v)=0$ y entonces $[K(v):K]=r$.

Análogamente hay una $w \in E'$ tal que $p'(w)=0$ y entonces hay un isomorfismo σ de $K(v)$ sobre $K'(w)$ con la propiedad de que $\sigma(\alpha)=\alpha'$ $\forall$ $\alpha \in K$. Como $[K(v):K]=r>1$, $[E:K(v)]=[E:K]/[K(v):K]=n/r<n$.

Afirmamos que E es un campo de descomposición de $f(x)$ considerado como un polinomio de $K_o=K(v)$, pues ningún subcampo de E conteniendo a K_o y por tanto a K puede descomponer a $f(x)$ ya que E se supone es un campo de descomposición de $f(x)$ sobre K.

Análogamente E' es un campo de descomposición de $f'(t)$ sobre $K'_o=K'(w)$. Por nuestra hipótesis de inducción hay un isomorfismo ϕ de E sobre E' tal que $\phi(a)=\sigma(a)$ $\forall$ $a \in K_o$. Pero para cada $\alpha \in K$, $\sigma(\alpha)=\alpha'$, de donde $\alpha \in K \subset K_o$, $\phi(\alpha)=\sigma(\alpha)=\alpha'$, esto prueba el teorema. ■

Para ver la parte "en particular...", sea $K=K'$ y sea τ la aplicación idéntica $\tau(\alpha)=\alpha$ $\forall$ $\alpha \in K$. Supongamos que E_1 y E_2 son dos cam--

pos de descomposición de $f(x) \in K[x]$ considerando $E_1=E \supset K$ y $E_2=E' \supset K$ y aplicando el teorema que acabamos de probar tenemos que E_1 y E_2 son isomorfos con un isomorfismo que deja fijos todos los elementos de K. ■

Un campo puede tener un isomorfismo no trivial sobre si mismo, dichas transformaciones serán de la mayor importancia en lo que sige.

AUTOMORFISMO DE CAMPOS.

En la seccón precedente se examinó el concepto de isomorfismo de un campo en otro. El caso especial en el que el isomorfismo transforma un campo dado en si mismo se examina en esta parte.

DEFINICION. Un isomorfismo σ de un campo K sobre si mismo se llama automorfismo de campos.

DEFINICION.

- Si σ es un automorfismo de un campo K entonces un elemento $a \in K$ queda fijo bajo σ si $\sigma(a)=a$.
- Un automorfismo σ de K deja fijo un subcampo F de K si cada $a \in F$ queda fija bajo σ.
- Una colección $S=\{\sigma_i / i \in I\}$ de automorfismos de K deja fijo a un subcampo F de K si cada $a \in F$ queda fija bajo toda $\sigma_i \in S$.

TEOREMA. Si $S=\{\sigma_i / i \in I\}$ es una colección de automorfismos de un campo K entonces el conjunto F de todos los elementos $a \in K$ que quedan fijos bajo toda $\sigma_i \in S$ forman un subcampo de K.

Demostración. Si $\sigma_i(a)=a$ y $\sigma_i(b)=b$ $\forall\ i \in I$ entonces $\sigma_i(a \pm b)=\sigma_i(a) \pm \sigma_i(b)=a \pm b$, $\sigma_i(ab)=\sigma_i(a)\sigma_i(b)=ab$ y $\sigma_i(a/b)=\sigma_i(a)/\sigma_i(b)=a/b$ si $b \neq 0$. Como todas las σ_i son automorfismos, tenemos que $\sigma_i(0)=0$ y $\sigma_i(1)=1$ $\forall\ i \in I$. O sea que $0, 1 \in F$ y por lo tanto F es un subcampo de K. ■

DEFINICION. El campo F del teorema anterior se llama el campo

fijo de la colección de automorfismos σ_i de K.
con un solo automorfismo σ, diremos que F es el campo fijo del automorfismo σ de K.

TEOREMA. El conjunto $S=\{\sigma_i / i\in I\}$ de todos los automorfismos de un campo K es un grupo bajo la composición de funciones.

Demostración. Siendo la composición de funciones el producto de automorfismos, sabemos que dicho producto es asociativo. El automorfismo identiodad $I_k: K\longrightarrow K$ tal que $I_k(a)=a$ $\forall$ $a \in K$ es obviamente un automorfismo de K. Si σ es automorfismo entonces σ^{-1} también lo es. De esta forma demostramos lo afirmado en el teorema. ■

TEOREMA. Si K es un campo y F es un subcampo de K entonces el conjunto G(K/F) de aquellos automorfismos de K que dejan fijo a F es un subgrupo del grupo de todos los automorfismos de K.

Demostración. Para $\sigma_1, \sigma_2 \in G(K/F)$ y $\forall$ $a \in F$ tenemos que $(\sigma_2\circ\sigma_1)(a)=\sigma_2(\sigma_1(a))=\sigma_2(a)=a$, de manera que $\sigma_2\circ\sigma_1 \in G(K/F)$. Es claro que el automorfismo identidad $I_k \in G(K/F)$. Además, si $\sigma(a)=a$ $\forall$ $a \in F$ entonces $a=\sigma^{-1}(a)$, es decir, si $\sigma \in G(K/F)$ entonces $\sigma^{-1} \in G(K/F)$, así, vemos que G(K/F) es un subgrupo del grupo de todos los automorfismos de K. ■

DEFINICION. El grupo G(K/F) se llama el grupo de automorfismos de K que dejan fijo a F.

AUTOMORFISMO DE FROBENIUS. Si K es un campo finito de característica p entonces la transformación $\sigma_p: K\longrightarrow K$ tal que $\sigma_p(a)=a^p$ $\forall$ $a \in K$ es un automorfismo . Se le llama el automorfismo de Frobenius. Además el campo fijo de este automorfismo es isomorfo a $\mathbb{Z}_p$.

Demostración. Sean $a,b \in K$ entonces $a+b \in K$ y $\sigma_p(a+b)=(a+b)^p$ pero $(a+b)^p=a^p+b^p+\sum_{n=1}^{p-1}\binom{p}{n}a^n b^{p-n}$ si $1\leq n\leq p-1$, el coeficiente binomial $\binom{p}{n}$ es divisible por p y todos los términos de la sumatoria son cero, por lo tanto $(a+b)^p=a^p+b^p$ y en consecuencia $\sigma_p(a+b)=\sigma_p(a)+\sigma_p(b)$

así mismo $\sigma_p(ab)=\sigma_p(a)\sigma_p(b)$. Luego entonces σ_p es un homomorfismo, además si $\sigma_p(a)=0$ entonces $a^p=0$, y en consecuencia $a=0$ de tal forma, el $\text{Ker}\sigma_p=\{0\}$ y por lo tanto σ_p es un monomorfismo. Como K es finito, σ_p es suprayectiva, es decir σ_p es un epimorfismo, y es por tanto un isomorfismo y en consecuencia un automorfismo.

Por otro lado $\mathbb{Z}_p$ esta contenida en K puesto que K es de característica p. Por el teorema de Fermat, para $a \in \mathbb{Z}_p$, tenemos que $\sigma_p(a)=a^p=a$, por lo tanto $a \in K_{\{\sigma_p\}}$, de esta manera, el polinomio x^p-x tiene p raíces en K, a saber, los elementos de $\mathbb{Z}_p$. Como un polinomio de grado n sobre un campo K tiene a lo más n raíces en ese campo, y como los elementos fijos bajo σ_p son precisamente las raíces en K de x^p-x, vemos que $\mathbb{Z}_p=K_{\{\sigma_p\}}$. ■

CAPITULO III.

CAMPOS FINITOS

DEFINICION. El orden de un campo K es el número de elementos de K.

TEOREMA. Sea K un campo de orden p y E un campo finito extensión de K entonces E es extensión de K de grado n y el orden de E es p^n para algún $n \in \mathbb{N}$.

Demostración. E es un espacio vectorial sobre K, como E es finito, es ciertamente de dimensión finita como espacio vectorial sobre K. Supongamos que $[E:K]=n$ entonces E tiene una base de n elementos sobre K, sea $v_1, v_2, \ldots, v_n$ una base de E sobre K, entonces todo elemento de E tiene una representación única en la forma.

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$$

donde $\alpha_1, \alpha_2, \ldots, \alpha_n$ son todos elementos de K, así pues, el número de elementos de E es el número de combinaciones lineales que se forman cuando las $\alpha_1, \alpha_2, \ldots, \alpha_n$ van tomando valores sobre K. Como cada coeficiente puede tomar p valores, E debe tener p^n elementos. ■

De esta manera nos damos cuenta que no existen campos con, por ejemplo, 6, 10, 12, 14, 15, 18, 20, etc. elementos.

Nótese aquí el contraste con la teoría de grupos en donde existen grupos de cualquier orden, también existen grupos que son del mismo orden pero no son isomorfos. Esto último no puede suceder en los campos finitos como se verá a continuación.

TEOREMA. Sea K un campo de orden p^n entonces $\forall\, a \in K\ a^{p^n}=a$.

Demostración. Si $a=0$ la afirmación es clara. Si $a\neq 0$, los elementos distintos de cero de K forman un grupo bajo la multiplicación, el orden de este grupo es p^n-1 y por consiguiente $a^{p^n-1}=1\ \forall\, a \in K$ con $a\neq 0$. Multiplicando esta expresión por a obtenemos $a^{p^n}=a$. ■

DEFINICION. α es una raíz de multiplicidad m de $f(x)$ si

$(x-\alpha)^m | f(x)$ y $(x-\alpha)^{m+1} \nmid f(x)$.

DEFINICION. Si $f(x)=a_0+a_1x+\ldots+a_nx^n \in K[x]$ entonces $f'(x)=a_1+2a_2x+\ldots+na_nx^{n-1}$ es la derivada de $f(x)$.

Las siguientes igualdades son consecuencia inmediata de la definición anterior: $(f+g)'(x)=f'(x)+g'(x)$, $(fg)'(x)=f'(x)g(x)+f(x)g'(x)$, y $(f^n)'(x)=n(f^{n-1}(x))f'(x)$.

TEOREMA. Un polinomio $f(x) \in K[x]$ tiene una raíz multiple si y sólo si $f(x)$ y $f'(x)$ tienen un factor común de grado positivo.

Demostración. $\Rightarrow$) supongamos que las raíces de $f(x)$ se encuentran todas en K. Si $f(x)$ tiene una raíz multiple α entonces $f(x)=(x-\alpha)^m q(x)$ donde $m>1$, y así, $f'(x)=(x-\alpha)^m q'(x)+m(x-\alpha)^{m-1}q(x)=(x-\alpha)[(x-\alpha)^{m-1}q'(x)+m(x-\alpha)^{m-2}q(x)]=(x-\alpha)r(x)$, ya que $m>1$. Pero esto nos dice que $f(x)$ y $f'(x)$ tienen a $(x-\alpha)$ como factor común.
$\Leftarrow$) si $f(x)$ es mónico y no tiene ninguna raíz multiple, lo podemos expresar como $f(x)=(x-\alpha_1)\ldots(x-\alpha_n)$, donde las α_i son todas distintas. Pero entonces $f'(x)=\sum_{i=1}^{n}(x-\alpha_1)\ldots\overline{(x-\alpha_i)}\ldots(x-\alpha_n)$ donde: $\overline{}$, indica el término que se ha suprimido. Afirmamos que niguna raíz de $f(x)$ es raíz de $f'(x)$ ya que $f'(\alpha_i)=\prod_{j\neq i}(\alpha_i-\alpha_j)\neq 0$ ya que las raíces son todas distintas. Por otro lado si $f(x)$ y $f'(x)$ tubieran un factor común no trivial, tendrían una raíz común, a saber, cualquiera de las raíces de este factor común, cosa que no puede suceder y por lo tanto $f(x)$ y $f'(x)$ no tienen factores comunes no triviales. ■

TEOREMA. si $f(x)$ es irreducible sobre K entonces

1.- Si la característica de K es cero entonces $f(x)$ no tiene raíces multiples.
2.- Si la característica de K es p entonces $f(x)$ tiene una raíz multiple sólo si es de la forma $f(x)=g(x^p)$.

Demostración. Como $f(x)$ es irreducible, sus únicos factores en $K[x]$ son 1 y $f(x)$. Si $f(x)$ tiene una raíz multiple entonces $f(x)$ y

f'(x) tienen un factor común no trivial, de donde f(x)/f'(x), pero como el grado de f'(x) es menor que el de f(x), la única forma de que esto suceda es que f'(x)=0, en característica cero, esto implica que f(x) es constante, y por tanto que no tiene ninguna raíz. En característica p esto obliga a que $f(x)=g(x^p)$. ■

TEOREMA. Si K es un campo de característica p entonces el polinomio $x^{p^n}-x$ tiene p^n raíces distintas.

Demostración. La derivada de $x^{p^n}-x$ es $p^n x^{p^n-1}-1=-1$ ya que K es de característica p. Por lo tanto el polinomio $x^{p^n}-x$ y su derivada son primos relativos, esto implica que $x^{p^n}-x$ no tiene raíces multiples. ■

TEOREMA. Sea K un campo con p^n elementos entonces el polinomio $x^{p^n}-x \in K[x]$ se factoriza en K[x] como:

$$x^{p^n}-x = \prod_{\alpha \in K} (x-\alpha).$$

Demostración. $x^{p^n}-x$ tiene cuanto más p^n raíces, las p^n raíces de $x^{p^n}-x$ son todas elementos de K. Y por lo tanto $x^{p^n}-x= \prod_{\alpha \in K} (x-\alpha)$. ■

TEOREMA. Sea K un campo con p^n elementos entonces K es el campo de descomposición del polinomio $x^{p^n}-x$.

Demostración. $x^{p^n}-x$ se descompone en K, pero no puede descomponerse en un campo más pequeño porque ese campo tendría que tener todas las raíces de este polinomio y por tanto tendría que tener p^n elementos. De esta manera K es el campo de descomposición del polinomio $x^{p^n}-x$. ■

COROLARIO. Dos campos finitos de igual orden son isomorfos.

TEOREMA. Para todo número primo p y todo entero positivo n existe un único campo de orden p^n.

Demostración. Consideremos el polinomio $x^{p^n}-x \in \mathbb{Z}_p[x]$. Sea K el campo de descomposición de este polinomio y sea $F=\{a \in K / a^{p^n}=a\}$. Los elementos de F son las raíces de $x^{p^n}-x$, que son todas distintas, lo que implica que F tiene p^n elementos. F es un campo, pues si $a,b \in F$ entonces $a=a^{p^n}$, $b=b^{p^n}$ y $a^{p^n}b^{p^n}=ab \in F$. Además, como la característica del campo es p $(a\pm b)^{p^n}=a\pm b \in F$ y $(a/b)^{p^n}=a/b$ (si $b\neq 0$). Por tanto F es un subcampo de K y por lo tanto F=K. Este campo es único, (salvo isomorfismos). ■

DEFINICION. Sea G un grupo y $a \in G$. Al menor entero positivo n con la propiedad de que $a^n=1$ se le conoce como el orden de a. Si no existe dicho entero positivo n, decimos que a es de orden infinito.

DEFINICION. El exponente e(G) de un grupo finito G es el mínimo común múltiplo de los órdenes de los elementos de G.
Se puede observar que e(G) divide al orden de G. En general, G no necesita tener un lemento de orden e(G), por ejemplo, si $G=S_3$ entonces $e(G)=6$, pero S_3 no tiene ningún elementos de orden 6.
Los grupos abelianos se comportan mejor a este respecto como veremos a continuación.

TEOREMA. Todo grupo abeliano G contiene un elemento de orden e(G).

Demostración. Sea $e=e(G)=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$ donde las p_i son primos distintos y $\alpha_i \geq 1$. Por la definición de e(G), G debe poseer elementos g_i cuyos ordenes sean divisibles por $p_i^{\alpha_i}$, entonces una potencia apropiada a_i de g_i tiene orden $p_i^{\alpha_i}$. Definamos $g=a_1a_2\dots a_n$, y supongamos que $g^m=1$, donde $m\geq 1$, entonces $a_i^m=a_1^{-m}a_2^{-m}\dots a_{i-1}^{-m}a_{i+1}^{-m}\dots a_n^{-m}$, y así $q=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{i-1}^{\alpha_{i-1}}p_{i+1}^{\alpha_{i+1}}\dots p_n^{\alpha_n}$, y entonces $a_i^{mq}=1$, pero q es primo con respecto al orden de a_i, así que $p_i^{\alpha_i}$ divide a m, luego, $e=e(G)$ divide a m, pero claramente $g^e=1$, entonces g tiene orden $e=e(G)$, que es lo que deseabamos. ■

TEOREMA. Si G es un subgrupo finito del grupo multiplicativo

de un campo K entonces G es cíclico.

Demostración. Puesto que la multiplicación en K es conmutativa, G es un grupo abeliano.
Sea $e=e(G)$, entonces $\forall\ x \in G$ tenemos que $x^e=1$. De tal modo que x es una raíz del polinomio x^e-1 sobre el campo K. Hay a lo más e -- raíces de este polinomio, por lo que $o(G)\leq e$. Pero $e\leq o(G)$, por tanto $e=e(G)=o(G)$, y por el teorema anterior G es cíclico. ■

COROLARIO. El grupo multiplicativo de un campo finito es cíclico.

DEFINICION. Sea E una extensión de un campo K. Un elemento $\alpha \in E$ que es algebráico sobre K se dice que es separable sobre K si es una raíz simple de $irr(K,\alpha)$.
La extensión E se dice que es separable sobre K si es algebráica sobre K y si cada uno de sus elementos es separable sobre K. También decimos que E/K es separable.
Si E/K es algebráica pero no separable decimos que E es una extensión inseparable de K.

DEFINICION. Un campo K se llama perfecto si no tiene extensiones inseparables.

Sea $K^p=\{a^p/a \in K\}$. Notemos que si K es finito de característica p, $a \in K$ entonces a tiene a lo más una raíz p-ésima.
Tenemos que $a \in K^p$ si y sólo si a tiene una raíz p-ésima en K.

TEOREMA. Un campo dado K es perfecto si y sólo si la característica de K es cero o la característica de K es p y $K^p=K$.

Demostración. Supongamos que la característica de K es cero. Sea E una extensión algebráica de K, $a \in E$ y $p(x)=irr(K,a)$ entonces -- $p'(x)\neq 0$, $p'(x)$ es de grado menor que $p(x)$, de modo que $p(x)$ no puede dividir a $p'(x)$, por lo tanto $p'(a)\neq 0$. Lo que indica que a es separable sobre K y por lo tanto E/K es separable.

Ahora supongamos que la característica de K es p, y sean E,a,p(x) como se dijo arriba. Supóngase que $K^p=K$ y que a no es separable sobre K. Como p'(a)=0 y como el grd(p'(x))<grd(p(x)) se sigue que p'(x)=0. Y por el cuarto teorema de esta sección se tiene que

$$p(x)=\sum_{r=0}^{n} a_r x^{p^r}$$

como $K^p=K$, cada a_r tiene una única raíz p-ésima en K. Sea $b_r^p=a_r$ para $r=0,1,\ldots,n$. Entonces $p(x)=\sum_{r=0}^{n} b_r^p x^{p^r}=\left[\sum_{r=0}^{n} b_r x^r\right]^p$, lo que contradice el hecho de que p(x) es irreducible en K[x]. Entonces E/K debe ser separable y se sigue que K es perfecto.

Recíprocamente. Supoongamos que la característica de K es p y que K es perfecto. Sea $a \in K$ y consideremos el polinomio $x^p-a \in K^p$. Si este polinomio tiene una raíz b en K entonces $a=b^p \in K^p$. Supongamos que no tiene raíz en K, y sea p(x) uno de sus factores no constantes mónico e irreducible en K[x]. Consideremos la extensión K(b) donde p(b)=0. En K(b)[x] tenemos que $x^p-a=x^p-b^p=(x-b)^p$. Y como p(x) divide a este polinomio tenemos que $p(x)=(x-b)^m$ para algún m. Si m=1 entonces $(x-b) \in K[x]$ y así $b \in K$, lo cual no cierto, entonces m>1. Luego b no es una raíz simple de p(x), y como p(x)=irr(K,b), K(b) no es separable sobre K. Esto contradice el hecho de que K es perfecto, por lo tanto debemos tener que $a \in K^p$ $\forall \in K$, esto es: $K^p=K$. ■

COROLARIO. Todo campo finito es perfecto.

Demostración. Consideremos ahora un campo finito K de característica p, el automorfismo de Frobenius dado por $\sigma_p(a)=a^p$ implica que $K=K^p$.

BIBLIOGRAFIA

1) FRANK AYRES JR. ALGEBRA MODERNA. Mc GRAW-HILL, 1984.

2) I. N. HERSTEIN. ALGEBRA MODERNA. TRILLAS, 1983.

3) JOHN B. FRALEIGH. ALGEBRA ABSTRACTA. SITESA, 1988.

4) PAUL J. Mc CARTHY. ALGEBRAIC EXTENSIONS OF FIELDS. BLAISDELL PUBLISHING COMPANY, 1966.