U N I V E R S I D A D D E S O N O R A.

Escuela de Altos Estudios

"EL TEOREMA FUNDAMENTAL DEL ALGEBRA"

Tesis que para obtener el Título de Licenciado en Matemáticas presenta:

Jorge Ontiveros Almada

Hermosillo, Sonora. 1969.

A la memoria de mi Padre

A mi Madre.

INTRODUCCION

Todas las demostraciones del llamado Teorema Fundamental del Algebra, tienen carácter trascendente en el sentido de que emplean conceptos y métodos que caen fuera del álgebra y son del dominio del análisis matemático real o complejo.

El presente trabajo está basado en el artículo del Dr. Hans Zassenhauss: "On The Fundamental Theorem of Algebra" publicado en The American Mathematical Monthly de mayo de 1967 y tiene por objeto dar una demostración lo más algebraica posible del teorema fundamental y tratar además algunos tópicos relacionados con él.

En el Cap. I y con el objeto de redondear este trabajo se dan otras demostraciones del teorema fundamental, una basada en el teorema de Liouville y que es posiblemente la más sencilla de todas.

En el Cap. II se mencionan algunas propiedades del campo real y que motivan la definición de campo realmente cerrado. En la teoría de los campos formalmente reales de Artin y Schreier se definen los campos reales cerrados (aquí "cerrados" no se refiere a cerradura algebraica) y se demuestra que la definición de campo real cerrado implica la de campo realmente cerrado (cf [4] Cap. VI). Sería interesante determinar si estas definiciones son equivalentes o en caso contrario dar un contraejemplo.

En el Cap. III se da la definición de anillo ordenado.

En el Cap. IV se tratan los anillos con división ordenados y se incluye una condición necesaria y suficiente para la ordenabilidad de un subanillo de un anillo con división distinta de las generalmente tratadas. Además se incluye un Teorema de existencia para campos realmente cerrados.

En el Cap. V se tratan las extensiones anulares algebraicas simples y el equivalente del grupo de Galois asociado a un polinomio, para anillos.

En el Cap. VI se da una demostración del teorema fundamental, sugerida por el Prof. Enrique Valle Flores, en el seminario de exposición de ésta tesis.

No se incluye la demostración publicada en el artículo de Zassenhauss ya que en mi opinión, está un poco obscura.

Por último en el Cap. VII se amplía un algoritmo con el que se obtengan raices reales de polinomios con coeficientes reales, para que nos dé un algoritmo y obtener también las raices complejas de estos polinomios.

Una dificultad de este capítulo es calcular el polinomio $S_2(f)$ (x) a partir de los coeficientes de f(x).

Sería interesante calcular $S_2(f)$ para polinomios f(x) de grado mayor que 3, posiblemente con ayuda de una calculadora electrónica.

Agradezco al Prof. Enrique Valle Flores su estímulo y consejos sin los cuales este trabajo no habría sido posible. Mi agradecimiento también para el Ing. Alejandro Dueñas por su ayuda y apoyo durante toda mi carrera.

Mayo 1969.

CAPITULO I

Demostraciones del Teorema Fundamental del Algebra.

Daremos primero una demostración del teorema fundamental basada en el Teorema de Liouville (cf [1]. Cap. 6, Cap. 9)

Llamaremos funciones enteras a funciones de la forma $f(z)=\sum_{n=0}^{\infty} a_n z^n$ con a_i en C (campo complejo).

I.I. TEOREMA. Una función entera no constante toma valores arbitrariamente grandes.

DEMOSTRACION. Demostraremos una forma equivalente de este teorema: Una función entera acotada (es decir, tal que $|f(z)|\leqslant M$ para algún M positivo, para todo z en C) se reduce a una constante.

En efecto, si existe una constante M tal que $|f(z)|\leqslant M$ para toda z, entonces, de la desigualdad de Canchy $|a_n|\leqslant M/r^n$ ¼ deducimos que $a_n = 0$ para n = 1, 2,..., ya que r puede tomar valores arbitrariamente grandes. Entonces $f(z) = a_0$.

1.2. TEOREMA. Si f(z) es un polinomio de grado $m\geqslant 1$ y G es un real positivo arbitrario, entonces puede encontrarse R tal que $|f(z)|\geqslant G$ para toda z tal que $|z|\geqslant R$.

DEMOSTRACION. Sea $f(z) = a_0 + a_1 z + \dots + a_m z^m$

$$f(z) = z^m\left(a_m + \frac{a_{m-1}}{z} + \dots + \frac{a_0}{z^m}\right)$$

Si tomamos z tal que $|z| = r$.

$$1.3.\ |f(z)|\geqslant r^m\left(|a_m| - \frac{|a_{m-1}|}{r} - \dots - \frac{|a_0|}{r^m}\right)$$

y como $\left(\frac{|a_{m-1}|}{r} + \dots + \frac{|a_0|}{r^m}\right)$ se puede hacer menor que $\frac{1}{2}|a_m|$, la expresión 1.3 se puede hacer mayor que $\frac{1}{2}|a_m|r^m$ y por lo -

tanto mayor que G para r suficientemente grande.

1.4. Teorema fundamental del álgebra.

Si $f(z)$ es un polinomio de grado $m \geq 1$ con coeficientes complejos, entonces tiene al menos una raíz compleja.

DEMOSTRACION. Si $f(z) \neq 0$ para toda z, entonces $\frac{1}{f(z)} = g(z)$ es una función entera. Como $g(z)$ está acotada (ya que $f(z) \neq 0$ y si z se hace muy grande $g(z)$ tiende a cero) debe ser constante y lo mismo $f(z)$, lo cual es una contradicción. Entonces existe z_0 en C tal que $f(z_0) = 0$.

Daremos otra demostración del teorema 1.4 (cf [2] Cap. 5, Teorema 5).

Sea $g(z) = z^m + c_1 z^{m-1} + \dots + c_m$ y consideremos dos planos complejos, el plano Z y el plano W. q es entonces una función que asocia a cada punto z en el plano Z, el punto $w = q(z)$ en el plano W . Si z describe una curva contínua en el plano Z, entonces $q(z)$ describe también una curva continua en el plano W.

Para cada $r > 0$ fija, la función $w = q(r(\cos\theta + i \operatorname{sen}\theta))$ define una curva cerrada $C'r$ en el plano W, imagen de la circunferencia $Cr: |z| = r$ de radio r y centro O en el plano Z.

Para cada r fija considérese la integral

$$\varnothing(r,\theta) = \int_0^{(\theta)} d(\arg w) = \int_0^{\theta} \frac{u\,dv - v\,du}{u^2 + v^2}$$

con $w = q(r(\cos\theta + i \operatorname{sen}\theta)) = u + iv$ y definida para toda $C'r$ que no pasa por el origen $w = 0$. (Si $C'r$ pasa por $w = 0$, entonces $q(z)$ tiene una raíz).

Es fácil ver que $\emptyset(r, 2\pi) = 2\pi n(r)$ donde $n(r)$ es el número de veces que C'_r rodea al origen.

Como q es una función continua, $n(r)$ varía continuamente con r, excepto cuando C'_r pasa por el origen.

Además $q(0) = c_m \neq 0$ (a menos que $c_m = 0$ en cuyo caso $z = 0$ es una raiz) y entonces $n(0) = 0$.

Demostraremos que si r es suficientemente grande, $n(r)$ es igual al grado m de $q(z)$.

$$q(z) = z^m + c_1 z^{m-1} \ldots + c_{m-1} z + c_0 = z^m\left(1 + \sum_{k=1}^{m} c_k z^{-k}\right)$$

$$\arg q(z) = \arg z + \arg\left(1 + \sum_{k=1}^{m} c_k z^{-k}\right)$$

Si z describe la circunferencia $|z| = r$ en sentido positivo, el cambio de arg $q(z)$ es m veces el cambio de arg z((o sea $m \cdot 2\pi$) más el cambio en $\arg\left(1 + \sum_{k=1}^{m} c_k z^{-k}\right)$.

Pero si $|z| = r$ es suficientemente grande, $\left|\sum c_k z^{-k}\right| < \frac{1}{2}$ y $1 + \sum_{k=1}^{m} c_k z^{-k} = u$ está dentro del círculo $|u - 1| < \frac{1}{2}$ y no rodea al origen.

Tenemos que: Si r es bastante grande $n(r) = m$, es decir, el cambio total de arg $q(z)$ es $2\pi m$. Pero al variar r, C'_r se deforma continuamente ya que $q(z)$ es continua. Es evidente geométricamente que una curva, si rodea al origen $n \neq 0$ veces, no puede ser deformada en un punto sin pasar por el origen en alguna etapa de la deformación.

Entonces para alguna r, C'_r debe pasar por el origen, cuando esto sucede $q(z) = 0$ y queda demostrado el teorema 1.4

CAPITULO II

Algunas Propiedades del Campo Real.

El campo real R tiene las siguientes propiedades:

2.1. El simétrico de un elemento de R que no es cuadrado (de un elemento de R) es cuadrado.

2.2. La suma de cuadrados de elementos de R es cero si y sólo si cada sumando es cero.

2.3. Todo polinomio de grado impar con coeficientes en R tiene al menos una raíz en R.

La segunda propiedad es consecuencia de que existe un orden algebraico para el campo real. La primera se debe a que todo real positivo tiene raíz cuadrada real (Cf [3] Teorema 1.37). La última se deriva de la aplicación del teorema del valor intermedio para funciones continuas (Cf [3] Teorema 4.23) a la siguiente desigualdad:

Si $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$. n impar.

2.4. $f(1 + \sum_{i=1}^{n} |a_i|) > 0 > f(-(1 + \sum_{i=1}^{n} |a_i|))$.

Y por el teorema mencionado, existe c en el intervalo $(-1(1 + \sum_{i=1}^{n} |a_i|), 1 + \sum_{i=1}^{n} |a_i|)$ tal que $f(c) = 0$.

Demostraremos la desigualdad 2.4 por división sintética.

$$
\begin{array}{cccccc|l}
1 & a_1 & a_2 & & a_{n-1} & a_n & 1+\sum^{n}|a_i| \\
 & 1+|a_1|+\dots+|a_n| & 1+|a_2|+\dots+|a_n| \dots & & 1+|a_{n-1}|+|a_n| & 1+|a_n| & \\
 & & +A'_1 & \dots & +A'_{n-2} & +A'_{n-1} & \\
\hline
1 & 1+|a_2|+\dots+|a_n| & 1+|a_3|+\dots+|a_n| \dots & & 1+|a_n| & 1 \quad +A_n & \\
 & +A_1 & +A_2 & & +A_{n-1} & &
\end{array}
$$

Donde A es no negativo y los demas A son positivos.
Entonces $f(1+\sum_{i=1}^{n}|a_i|)>0$.

Para demostrar la otra desigualdad es conveniente tomar en cuenta el sigro de los coeficientes, de tal manera que considerareros las a_i reales no negativas.

Sea entonces $f(x) = x^n \pm a_1 x^{n-1} \pm \ldots \pm a_n$.

Para el polinomio $f(x)$ definimos el "peor" polinomio $f_1(x)$, relativo a $f(x)$ como el polinomio que tiene los mismos coeficientes de $f(x)$ excepto tal vez los signos, y tal que $f_1(c)$ es mayor que $f(x)$ para toda c negativa.

El peor polinomio es entonces:

$$f_1(x) = x^n + a_1 x^{n-1} - a_2 x^{n-2} + \ldots + (-1)^{i+1} a_i\, x^{n-i} + \ldots + a_n.$$

Si $f_2(x)$ es cualquier polinomio con los mismos coeficientes de $f(x)$ excepto signos tenemos por ejemplo, para i par, j irpar.

$$f_1(x) = x^n + a_1 x^{n-1} - a_2 x^{n-2} + \ldots - a_i x^{n-i} + \ldots + a_j x^{n-j} - \ldots + a_n$$

$$f_2(x) = x^n + a_1 x^{n-1} - a_2 x^{n-2} + \ldots + a_i x^{n-i} + \ldots - a_j x^{n-j} - \ldots + a_n$$

$$f_1(x) - f_2(x) = -2 \cdot a_i x^{n-i} + 2\, a_j x^{n-j}$$

$$f_1(c) - f_2(c) = -2\, a_i c^{n-i} + 2\, a_j\, c^{n-j} > 0.$$

$f_1(c) > f_2(c)$ y $f_1(c)$ es efectivamente el "peor" polinomio.

Calculemos $f_1(-(1+\sum_{i=1}^{n}|a_i|))$. $\qquad |a_i| = a_i$.

$$\begin{array}{llllll|l}
1 & a_1 & -a_2 & \ldots & -a_{n-1} & a_n & -1-\sum a_i \\
 & -1-a_1 \ldots -a_n & 1+a_2+\ldots+a_n & \ldots & 1+a_{n-1}+a_n & -1-a_n & \\
 & & +A_1 & & +A_{n-2} & -A_{n-1} & \\
\hline
1 & -1-a_2 \ldots -a_n & 1 \neq a_3+\ldots+a_n & 1 \ldots & 1+a_n & -1-A_{n-1} & \\
 & & +A_1 & & +A_{n-2} & &
\end{array}$$

Donde los A_i son positivos.

Entonces ya que f_1 es el "peor" polinomio:

$0 > f_1(-(1 + \sum_{i=1}^{n} |a_i|)) > f(-(1 + \sum_{i=1}^{n} |a_i|))$.

2.5. DEFINICION. A los campos que satisfacen 2.1, 2. 2.3, los llamaremos campos realmente cerrados.

Puede pensarse que las tres condiciones anteriores determinan el campo real o campos isomorfos a él. Demostraremos que no es así, ya que el campo de los números algebra cos reales (subcampo propio de R) es otro ejemplo de campo realmente cerrado como se hace ver enseguida.

Sea A el conjunto de los números algebraicos sobre los racionales, es decir, el conjunto de las raices de toda las ecuaciones de la forma $a_0 + a_1 x + \ldots + a_n x^n = 0$ con a_i en

2.6. El conjunto A de los números algebraicos forma un campo.

DEMOSTRACION. Sean u, $v \in A$. Entonces $u + v$, $u-v$, $u.v$ u/v (si $v \neq 0$) están en $Q(u,v)$.

Como u, v son raices de polinomios con coeficientes Q, $Q(u,v)$ es una extensión finitamente generada por elementos algebraicos sobre Q. Entonces $Q(u,v)$ es finita sobre Q, de donde todo elemento de $Q(u,v)$ es algebraico sobre Q y sumas, productos, diferencias, cocientes de elementos de A están en A y éste es campo.

2.7. El campo A de los números algebraicos es algebraicamente cerrado.

Sea un polinomio $f(x) = u_n x^n + u_{n-1} x^{n-1} + \ldots + u_0$ con coeficientes u_i en A.

$K = Q(u_n,\ldots,u_o)$ es una extensión finitamente generada por elementos algebraicos, entonces K es finita sobre Q.

Toda raiz r de f(x) es algebraica sobre K. Entonces K(r) es finita sobre K y $K(r) = Q(u_n,\ldots, u_0,r)$ es finita sobre Q. de donde r es algebraico sobre Q. Entonces r es elemento de A y éste es algebraicamente cerrado.

Sea $H = A\cap R$, el campo de los números algebraicos reales.

2.8. <u>AFIRMACION</u>. El campo H de los números algebraicos reales es realmente cerrado.

H satisface 2.1, ya que toda raiz de $x^2 - a = 0$ con $a\in H$, $a>0$ es algebraica y además es real.

H satisface 2.2 ya que es un subcampo de R.

H satisface 2.3 ya que todo polinomio de grado impar con coeficientes en H. tiene al menos una raiz r en R. Como r es raiz de una ecuación con coeficientes en A y este es algebraicamente cerrado, r está en A y entonces r está en H.

Ahora bien H no es isomorfo del campo real puesto que no contiene a los trascendentes reales. Otra demostración de que H no es isomorfo a R, que no envuelva la existencia de reales trascendentes consiste en observar que mientras R es no-numerable (infinito), H es numerable puesto que A lo es (ya que la colección de todos los polinomios sobre Q es numerable).

CAPITULO III

Anillos Ordenados.

3.1. <u>DEFINICION</u>. Un anillo ordenado es un anillo A con unitario 1 y un subconjunto no vacío P de A tales que

3. 3.2. $0 \notin P$

3.3. Si $a \in A$, entonces $a \in P$, $a = 0$ ó $-a \in P$.

3.4. P es cerrado bajo adición y multiplicación.

De esta forma tenemos que $A = P \cup \{0\} \cup (-P)$.*

Además, de 3.2, $P \cap \{0\} = \emptyset$, $(-P) \cap \{0\} = \emptyset$ y $P \cap (-P) = \emptyset$ ya que si $a \in P \cap (-P)$, entonces $a + (-a) = 0 \in P$, contrario a 3.2.

Tenemos entonces que un anillo ordenado puede definirse de manera equivalente:

3.1. Un anillo ordenado A es una pareja (A,P) formada por un anillo A con unitario 1 y un subconjunto P de A no vacío al cual llamaremos el conjunto de los elementos positivos y tales que:

3.2. El simétrico de cualquier elemento distinto de cero no positivo es positivo.

$A = P \cup \{0\} \cup (-P)$ (Unión Ajena)

3.3. La suma y el producto de dos elementos positivos son positivos.

$P + P \subset P$ $\quad$ $P P \subset P$

* Se utilizan las definiciones usuales para el cálculo de subconjuntos de un anillo:

$A + B = \{a + b \mid a \in A,\ b \in B\}$, $-A = \{-a \mid a \in A\}$,AB=..

Dado el anterior concepto de positividad definimos un orden algebraico en A diciendo que:

3.5 $\quad a>b \quad (b<a) \quad$ si $\quad a-b\in P$.

Esta definición satisface las reglas generalmente pedidas en una relación de orden algebraico.

3.6. Tricotomía. Para cualesquiera dos elementos a, b en A, vale una y sólo una de las relaciones

$a>b \quad , \quad a=b \quad , \quad b>a.$

Efectivamente, por 3.3, $(a-b)\in P$, $a-b=0$ ó $-(a-b)\in P$ y como P, (-P), $\{0\}$ son ajenos dos a dos, tenemos solo una de las relaciones anteriores.

3.7. Transitividad. Si $a>b$ y $b>c$, entonces $a>c$.

$(a-b)\in P$, $(b-c)\in P$ y ya que P es cerrado bajo la suma $(a-c)\in P$.

3.8. Si $a>b$ y $c>d$ entonces $a+c>b+d$ y $ac+bd>ad+bc$.

$(a-b)\in P$, $(c-d)\in P$ implican $(a-b)+(c-d)=(a+c)-(b+d)\in P$ y $(a-b).(c-d)=(ac+bd)-(ad+bc)\in P$.

Recíprocamente, un anillo en el cual esté definida una relación de orden total , define un concepto de positividad, con $P=\{a\in A \mid a>0\}$ el conjunto de los positivos y que satisface 3.2, 3.3, 3.4.

<u>OBSERVACIONES</u>:

3.9. $1\in P$. ya que si $(-1)\in P$, para $a\in P$

$(-1)a=-a\in P$. Contradicción.

3.10. La característica de cualquier anillo ordenado es 0, ya que como P es cerrado, no puede ser

$n \cdot 1 = 1 + 1 + \ldots + 1 = 0$ para alguna n.

3.11. Un anillo ordenado no tiene divisores de cero, ya que si a, b en A, distintos de cero y $a \cdot b = 0$

a ó $(-a) \in P$, b ó $(-b) \in P$ y

$a\,b = (-a)\,(-b) = (-a)\,b = a\,(-b) = 0$ y un producto es de elementos en P.

CAPITULO IV

Anillos con División Ordenados.

Los elementos positivos de un anillo con división ordenado D, forman un semianillo * H con las siguientes propiedades:

4.1. El semianillo H contiene el cuadrado de todo elemento distinto de cero del subanillo con división D_H generado por H.

4.2. El semianillo H es un sub-semianillo maximal de D que no contiene el cero de D.

En efecto, sea $D_H = [H]$ el anillo con división generado por H. $H^{-1} \subset H$, ya que si $h \in H$ y $h^{-1} \notin H$, $h(-h^{-1}) = -1 \in H$ contrario a 3.9. Entonces $D_H = H \cup \{0\} \cup (-H)$.

Sea $0 \neq u \in D_H$. Si $u \in H$, $u^2 \in H$.

Si $u \notin H$, $-u \in H$, $u^2 = (-u)(-u) \in H$.

Sea K un sub-semianillo de D que contenga propiamente a H. Existe x en K tal que x no está en H.

Si $x = 0$, $0 \in K$.

Si $x \neq 0$, $x \in (-H)$, $-x \in H \subset K$ y $x + (-x) = 0 \in K$.

4.3. Proposición: Recíprocamente, a cada semianillo H de D que satisfaga 4.1, 4.2 lo podemos asociar con un concepto de positividad de D_H poniendo $H = P$ y que cumple 3.2, 3.3

4.4. Proposición. $uH = Hu$ para toda $u \in D_H$, $u \neq 0$.

Sean $u, v \in D$ u, v distintas de cero.

$u\, v\, u^{-1} v^{-1} = (uv)^2 (v^{-1} u^{-1} v)^2 (v^{-1})^2 \in H$. Si $h \in H$,

$u\, h = h(h^{-1} u\, h\, u^{-1}) u \in Hu$. $uH \subseteq Hu$.

Similarmente $Hu \subseteq uH$ y entonces $uH = Hu$.

* Un semianillo (H, +, .) es un subconjunto no vacío de un anillo, cerrado bajo las operaciones de adición y multiplicación.

4.5. Proposición. Si $h \in H$, entonces $h^{-1} \in H$.

$H = 1 \cdot H = h^{-1}h\, H \subseteq h^{-1}H$. $h^{-1} = h^{-1}1^2 \in h^{-1}H$.

$h^{-1}H + h^{-1}H \subset h^{-1}H$ ya que $h^{-1}h_1 + h^{-1}h_2 = h^{-1}(h_1 + h_2) \in h^{-1}H$.

Por la proposición 4.4.

$(h^{-1}H)\,(h^{-1}H) = h^{-1}(H\, h^{-1})\, H = h^{-1}(h^{-1}H)\, H$.

$h^{-1}h^{-1}HH \subset H \subset h^{-1}H$.

$h^{-1}H$ es entonces un semianillo de D_H que contiene a H pero no contiene a cero. Como $D_H = D_{h^{-1}H}$ $h^{-1}H$ contiene el cuadrado de todos los elementos distintos de cero de $D_{h^{-1}H}$ y se sigue de la propiedad maximal de H que $h^{-1}H = H$ y entonces $h^{-1} \in H$.

4.6. Proposición. Si el elemento distinto de cero c de D_H no está en H, entonces $-c$ pertenece a H.

Sea $\overline{H} = H \cup cH \cup (H + cH)$

$\overline{H}$ contiene propiamente a H ya que $c = c.1^2 \in cH \subset \overline{H}$

$(H + cH) + (H + cH) \subset H + cH$.

$H\, cH = (cH)H \subset cH$.

$cH.cH = c(Hc)\, H = c(cH)\, H = c^2 H \cdot H \subset H$.

$(H + cH) \cdot (H + cH) \subset H\,H + H\,cH + cH\,H + cH \cdot cH \subset H + cH$.

Entonces la suma y el producto de elementos de $\overline{H}$, están en $\overline{H}$, de donde éste es un semianillo de D_H que contiene propiamente a H.

Debido a la propiedad maximal de H, $0 \in \overline{H}$. Como $0 \notin H$, $0 \notin c\,H$, entonces $0 \in (H + cH)$. Existen h_1, $h_2 \in H$ tales que $0 = h_1 + c\,h_2$ de donde $-c = h_1 h_2^{-1} \in HH \subset H$.

Podemos sintetizar los resultados anteriores en el siguiente

4.7. TEOREMA. Un subanillo con división D_H de un anillo con división D es ordenable si y sólo si D contiene un semianillo H con 4.1 y 4.2. El orden se da mediante H = P.

Necesitaremos el siguiente lema:

LEMA 4.8. Sea H_o semianillo de D que no contiene a cero, entonces H_o está contenido en un semianillo maximal H que no contiene a cero.

DEMOSTRACION. Sea $\bar{H} = \{H_i\}$ con $i \in I$ el conjunto de semianillos de D que no contienen a cero. Sea un orden parcial en $\bar{H}$ dado por

$H_k \leq H_l$ si $H_k \subseteq H_l$.

Sea $\{H_k\}$ $(k \in K)$ una cadena en H , entonces $\bigcup H_k$ $(k \in K)$ es una cota superior de $\{H_k\}$ $(k \in K)$. Efectivamente $\bigcup H_k$ $(k \quad K)$ es un semianillo, ya que si x, $y \in \bigcup H_k$, entonces $x \in H_r$, $y \in H_s$, y como H_r, H_s son elementos de la cadena, están relacionados entre si. Supongamos

$H_r \leq H_s$, entonces $x + y$, $x.y \in H_s \subset \bigcup H_k$ $(k \in K)$.

Además $\bigcup H_k$ no contiene a cero.

Por el lema de Zorn, existe un elemento maximal H en $\bar{H}$ respecto a la inclusión.

4.9. TEOREMA. Un anillo con división D puede ser ordenado algebraicamente si y sólo si la suma finita de productos finitos de cuadrados de elementos de D es cero sólo si todos los sumandos son cero.

<u>DEMOSTRACION</u>. La condición es necesaria, ya que como los cuadrados de elementos de D distintos de cero están en H, sumas finitas de productos finitos de cuadrados están en H y éste no contiene cero.

Supongamos que vale la condición. Sea H_0 el conjunto de todas las sumas finitas de productos finitos de cuadrados de elementos distintos de cero de D. Entonces H_0 es un semianillo y no contiene a cero. Por el Lema 4.7, H_0 está contenido en un semianillo maximal H que no contiene a cero.

$4 = 1^2 + 1^2 + 1^2 + 1^2 \in H_0 \subseteq H. \qquad 4 \neq 0.$

Como todo elemento u en D se puede poner como

$u = \frac{1}{4}\left[(u + 1)^2 - (u - 1)^2\right]$, entonces $u \in D_H$, tenemos que $D_H = D$ y D tiene el orden $a > b$ si y sólo si $a - b \in H$.

4.10. <u>TEOREMA</u>. Si el campo F es ordenado algebraicamente y F está contenido en una campo extensión algebraicamente cerrada Ω, entonces existe un subcampo Φ de Ω, realmente cerrado tal que

4.11. Cada elemento positivo de F es el cuadrado de un elemento de Φ.

4.12. Ω es algebraico sobre Φ.

<u>DEMOSTRACION</u>. Sea H_0 el conjunto de los elementos positivos de F. Por el lema 4.7 existe un semianillo maximal H de Ω que no contiene a cero y que contiene a H_0.

Sea Φ el campo generado por H. H contiene los elementos positivos de F y los cuadrados de todos los elementos de Φ distintos de cero, pero no contiene a cero.

Entonces podemos extender el orden de F a un orden algebraico de Φ, tal que H es el semianillo de los positivos de Φ.

4.12. Ω es algebraico sobre Φ.

DEMOSTRACION. Supongamos que $\xi \in \Omega$ no es algebraico sobre Φ.

Sea $H' = \left\{ \sum_i h_i \left(\frac{P_i(\xi)}{Q_i(\xi)} \right)^2 \middle| h \in H,\ P_i(x),\ Q_i(x) \in \Phi[x] \right\}$ formado por todas las sumas finitas de productos finitos de cuadrados de elementos distintos de cero de $\Phi(\xi)$ con coeficientes en HH' es un semianillo que contiene propiamente a H.

Debido a la propiedad maximal de H, cero está en H'.

$$0 = \sum_{i=1}^{n} h_i \left(\frac{P_i'(\xi)}{Q_i(\xi)} \right)^2 = \sum_{i=1}^{n} h_i \left(\frac{P_i(\xi)}{N(\xi)} \right)^2$$

$N(x)$, $P_1(x), \ldots, P_n(x)$ son polinomios distintos de cero de $\Phi[x]$

Sea m el grado máximo de los polinomios $P_1(x), \ldots, P_n(x)$ y sea a_i el coeficiente de X^m en $P_i(x)$.

Entonces ya que la extensión es trascendente

$$0 = \sum_{i=1}^{n} h_i P_i(\xi)^2 = \sum_{i=1}^{n} h_i P(x)^2$$

y el coeficiente de x^{2m} debe ser igual a cero ya que el único polinomio $\sigma(x) \in \Phi[x]$ que satisface $\sigma(\xi) = 0$ es el trivial De donde $0 = \sum_{i=1}^{n} h_i \cdot a_i^2 \in H$ lo que es falso.

Entonces Ω es algebraico sobre Φ.

Todo elemento de H es el cuadrado de un elemento de Ω

Si $u \in H$, entonces ya que Ω es algebraicamente cerrado existe $\xi \in \Omega$ tal que $\xi^2 = u$.

Si $\xi \notin H$ entonces $\overline{H} = \{a + b\xi \mid a \geq 0, b \geq 0,\ a + b > 0,\ a, b \in \Phi\}$ forma un subanillo que contiene propiamente a H.

$H \subset \bar{H} \subset \bar{H}\,\bar{H}^{-1}$ y $\bar{H}\,\bar{H}^{-1}$ es también un semianillo.

Además $\bar{H}\,\bar{H}^{-1}$ contiene el cuadrado de todo elemento de $\Phi(\xi)$ distinto de cero.

Efectivamente, sea $a + b\xi \neq 0$ con $a \geqslant 0$, $b \geqslant 0$, entonces $(a + b\xi)^2 = a^2 + 2\,a\,b\xi + b^2\xi^2 = a^2 + b^2 u + 2ab\xi \in H$.

Si $a + b\xi \neq 0$ con a ó $b < 0$.

$(a + b\xi)^2 = c + d\xi$ con $c = a^2 + b^2 u$, $d = 2ab < 0$.

$c^2 - d^2 u = (a^2 - b^2 u)^2 > 0$, ya que si $a - b^2 u = 0$ entonces $u = \frac{a^2}{b^2}$ y $\xi = \frac{a}{b}$. $- d \cdot u + c\xi \in H$, $(c + d\xi)\,(-d\,u + c\xi) = (c^2 - d^2 u)$, $\in H$ y $c + d\xi \in \bar{H}\,\bar{H}^{-1}$.

El cuadrado de todo elemento de $\Phi(\xi)$ está entonces en $\bar{H}\,\bar{H}^{-1}$ y ya que además es un semianillo que contiene propiamente a H, debido a la propiedad maximal de éste, $\bar{H}\,\bar{H}^{-1}$ debe contener a cero, lo que es una contradicción.

Cada elemento de H es el cuadrado de un elemento de Φ y ya que H contiene los elementos positivos de F tenemos 4.11.

Todo polinomio de grado impar con coeficientes en Φ tiene una raiz en Φ.

Supongamos que $f(x)$ es de grado impar y que la ecuación

$$4.13. \qquad -1 \equiv \sum_{i=1}^{s} f_i(x)^2 \qquad (f(x))$$

puede ser resuelta por polinomios $f_1(x)$, $f_2(x)$, .. $f_s(x)$ con coeficientes en Φ. Podemos encontrar un polinomio $f(x)$ de grado mínimo $2n + 1$ que satisfaga 4.13 y tomando los residuos de $f_1(x)$, $f_2(x)$, .. $f_s(x)$ al dividirlos por

$f(x)$ obtenemos una congruencia 4.13 con el grado máximo k de los polinomios $f_1(x),..f_s(x)$ no mayor que 2n.

$1+\sum_{i=1}^{s} f_i(x)^2 = f(x)\, g(x)$ es de grado 2 k o sea no mayor que 4 n, y como f (x) es de grado 2 n + 1, g(x) es de grado impar y menor que 2 n + 1.

Pero ya que

$$-1 \equiv \sum_{i=1}^{s} f_i(x)^2 \quad (g(x))$$

y el grado de f(x) es mínimo, llegamos a una contradicción. Entonces para un polinomio de grado impar con coeficientes en Φ nunca vale una relación de la forma 4.13.

Por otra parte, debe haber un polinomio de grado impar g(x) entre los factores de f(x) irreducibles en $\Phi[x]$. Ya que Ω es algebraicamente cerrado, hay una raíz ξ de g(x) en Ω.

Sea el campo extensión algebraica simple $\Phi(\xi)$, entonces: por lo demostrado anteriormente, ninguna suma finita de cuadrados de elementos de la extensión puede - ser igual a - 1.

Esto implica que las sumas finitas de cuadrados de elementos distintos de cero de $\Phi(\xi)$ forman un semianillo $\overline{H}$ que contiene a H pero sin contener a cero.

Supongamos que $\overline{H}$ contiene a cero.

$0 = \sum_{i=1}^{s} P_i(\xi)^2$ Supongamos que $P_1(x) \neq 0$

Ya que todo elemento de la campo extensión $\Phi(\xi)$ se puede poner como un polinomio, $P_1(\xi)^{-1} = Q(\xi)$

$-1 = \sum_{i=2}^{s} [P_i(\xi)\, Q(\xi)]^2$ lo cual es una contradicción.

Debido a la propiedad maximal de H tenemos que $\tilde{H} = H$ y sus campos generados son iguales, entonces $\Phi(\xi) = \Phi$ y todo polinomio de grado impar con coeficientes en Φ tiene una raiz en Φ .

Φ Es entonces realmente cerrado.

CAPITULO V

Extensiones Anulares Asociadas a una Ecuación.

Sean V un anillo conmutativo con unitario A y un polinomio $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ con coeficientes en V.

Construiremos formalmente una extensión anular conmutativa y con unitario de V en la cual f(x) tenga al menos una raíz.

Sea $V[u;f]$ el V-. módulo con base $1, u, \ldots, u^{n-1}$ sobre V.

5.1. La regla u_τ definida por:

$$u_\tau(1) = u$$
$$u_\tau(u^i) = u^{i+1} \qquad (0 < i < n-1)$$
$$u_\tau(u^{n-1}) = -a_1u^{n-1} - a_2u^{n-2} - a_3u^{n-3} - \ldots - a_n 1$$
$$u_\tau\left(\sum_{j=0}^{n-1} b_j u^j\right) = \sum_{j=0}^{n-1} b_j u_\tau(u^j) \quad (b\in V,\ 0 < j < n)$$

es un endomorfismo de $V[u;f]$.

$$u_\tau\left[\left(\sum_{i=0}^{n-1} a_i u^i\right) + \left(\sum_{i=0}^{n-1} b_i u^i\right)\right] = u_\tau\left[\sum_{i=0}^{n-1}(a_i + b_i)\, u^i\right] =$$
$$= \sum_{i=0}^{n-1}(a_i+b_i)\, u_\tau(u^i) = \sum_{i=0}^{n-1} a_i u_\tau(u^i) + \sum_{i=0}^{n-1} b_i u_\tau(u^i) = u_\tau\left[\sum a_i u^i\right] + u_\tau$$

$u_\tau\left[\sum b_i u^i\right]$ y u_τ es un homomorfismo de $V[u;f]$ en si mismo.

Definimos una multiplicación en $V[u;f]$ por:

5.2. $$\left(\sum_{h=0}^{n-1} k_h u^h\right)\cdot w = \sum_{h=0}^{n-1} k_h u_\tau^h(w) \qquad w\in V[u;f]$$

5.3. Proposición: $V[u;f]$ con la multiplicación anterior forma un anillo conmutativo con unitario, que contiene a V y tal que $f(u) = 0$.

<u>DEMOSTRACION</u>. Como u_τ es un homomorfismo, la multiplicación está determinada por el efecto de u_τ en los elementos de la base, y ya que $u_\tau^i(u^j) = u_\tau^j(u^i)$, $0 \leqslant i, j < n$, (si $i > j$) entonces $u_\tau^i(u^j) = u_\tau^j u_\tau^{j-i}(u^j) = u_\tau^j(u^i)$), es fácil demostrar

que la multiplicación es asociativa, conmutativa y distributiva con respecto a la suma.

Demostraremos como ejemplo, la conmutatividad de la multiplicación.

$$\left(\sum_{i=0}^{n-1} a_i u^i\right)\cdot\left(\sum_{j=0}^{n-1} b_j u^j\right) = \sum_{i=0}^{n-1} a_i u_z^i\left(\sum_{j=0}^{n-1} b_j u^j\right)$$

$$= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_i b_j u_z^i(u^j) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} b_j a_i u_z^j(u^i)$$

ya que $a_i b_j = b_j a_i$ y $u_z^i(u^j) = u_z^j(u^i)$.

$$\sum_{j=0}^{n-1} b_j u_z^j\left(\sum_{i=0}^{n-1} a_i u^i\right) = \left(\sum_{j=0}^{n-1} b_j u^j\right)\cdot\left(\sum_{i=0}^{n-1} a_i u^i\right)$$

Si $b \in V$, $b\cdot 1 + 0u + \ldots + 0\,u^{n-1} \in V[u;f]$.

V está contenido en $V[u;f]$.

El unitario de V es también el de $V[u;f]$, además

$$f(u) = u^n + a_1 u^{n-1} + \ldots + a_n = uu^{n-1} + a_1 u^{n-1} + \ldots + a_n$$

$$= u_z(u^{n-1}) + \ldots + a_n = (-a_1 u^{n-1} - \ldots - a_n) + a_1 u^{n-1} + \ldots + a_n$$

$$= 0.$$

5.4. u_z satisface la ecuación $f(u_z) = 0$.

Veamos el efecto de $f(u_z)$ en los elementos de la base.

$f(u_z)\,(1) = (u_z^n + a_1 u^{n-1} + \ldots + a_n.1)\,(1) = u^n + a_1 u^{n-1} + \ldots + a_n) = 0.$

$f\,(u_z)\,(u^i) = (u_z^n + a_1 u^{n-1} + \ldots + a_n.1)\,(u^i) = u_z^i(u^n + a_1 u^{n-1} + \ldots + a_n) = 0.$

De donde $f(u_z)\,(w) = 0$ para todo w en $V[u;f]$.

Sea $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ un polinomio con coeficientes $a_0 = 1, a_1, \ldots, a_n$ en el anillo conmutativo con unitario A, y supongamos que $f(x)$ tiene la raiz u en A, entonces:

$$f(x) = f(x) - f(u) = \sum_{h=0}^{n} a_{n-h}(x^h - u^h)$$

Estos $n!$ automorfismos forman un grupo γ_n tal que todo elemento de V está fijo para cada miembro de γ_n. Los elementos de V son los únicos elementos de $V[u_1, .. u_n ; f]$ que quedan fijos por γ_n.

DEMOSTRACION. Por inducción sobre el grado de $f(x)$ demostraremos la última afirmación ya que las anteriores - son inmediatas.

Para $n = 1$. $f(x) = x - u_1$, entonces u_1 está en V $V[u_1 ; f] = V$ y vale la afirmación.

Supongamos que vale la afirmación para $n-1$.

Como $V[u_1, .. u_n; f] = (V[u_1 ; f])[u_2, ... u_n; \frac{f}{x-u_1}]$ y $\frac{f}{x-u}$ es de grado $n-1$, tenemos que los elementos fijos por todas las permutaciones de $u_1, .. u_n$, deben ser, por la hipótesis de inducción, las del anillo base $V[u_1 ; f]$.

Si $\overline{V}$ es el conjunto de elemento fijos por γ_n, entonces $V \subset \overline{V} \subset V[u_1]$.

Supongamos que existe un elemento de $\overline{V}$ que no está en V.

Aplicándole a éste elemento un automorfismo resultado de una permutación que intercambie u_1 y u_2, obtenemos un elemento de $V[u_1][u_2]$ que no está contenido en $V[u_1]$. Tenemos entonces que $\overline{V} = V$.

Recíprocamente:

5.9 TEOREMA. Cualquier automorfismo de $V[u_1, .. u_n ; f]$ que deja fijo a V, es resultado de una permutación de $u_1, ... u_n$.

DEMOSTRACION. Sea T un automorfismo que deje fijo a V

$T(f(u_i)) = T(u_i^n + a_1 u_i^{n-1} + \dots + a_n) = T(u_i)^n + a_1 T(u_i)^{n-1} + \dots \neq a$

$= f(T(u_i)) = 0.$

El automorfismo T mapea raices de f(x) sobre raices y raices distintas en raices distintas, o sea únicamente permuta $u_1, \dots u_n$.

5.10. COROLARIO: Si $g(x_1, \dots, x_n)$ es un polinomio con coeficientes en V, fijo para todas las permutaciones de las variables (polinomio simétrico en $x_1, \dots x_n$) entonces el elemento $v = g(u_1, \dots, u_n)$ de $V[u_1, \dots, u_n]$ está en el anillo base V.

DEMOSTRACION. Si T es el automorfismo resultado de la permutación π, $T(v) = T(g(u_1, \dots, u_n)) = g(\pi u_1, \dots \pi u_n) = g(u_1, \dots, u_n) = v$ como esto vale para todo automorfismo que deja fija a V, por el teorema 5.8, v está en V.

5.11. COROLARIO: Teorema de las funciones simétricas.

Sea $R = V[x_1, \dots x_n]$ el anillo de polinomios en n indeterminadas sobre V. Sean

$$s_1 = x_1 + x_2 + \dots + x_n, \quad s_2 = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n, \dots,$$
$$s_n = x_1 x_2 \dots x_n$$

las n funciones simétricas básicas. Entonces cualquir polinomio simétrico en $x_1, \dots x_n$ sobre V, es igual a un polinomio en $s_1, s_2, \dots s_n$ sobre V.

DEMOSTRACION. Si $f(x) = (x - x_1)(x - x_2) \dots (x - x_n)$ entonces $f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} \dots + (-1)^n s_n$.

Sea $K = V[s_1, \dots, s_n]$ el anillo generado por $s_1, \dots, s_n$, sobre V. Entonces R se puede poner como $R = K[x_1, x_2, \dots, x_n; f]$ ya que los coeficientes de f están en K.

Sea $g(x_1, \dots, x_n)$ un polinomio simétrico en $x_1, \dots, x_n$ ya que g queda fijo para las permutaciones de $x_1, \dots x_n$, entonces g queda fijo para todos los automorfismos de N sobre K. Del corolario 5.10 se sigue que g está en el anillo base K, es decir $g(x_1, \dots x_n)$ se puede poner como polinomio en $S_1, S_2, \dots S_n$.

Del corolario anterior se sigue que si f(x) es un polinomio cpm cpeficientes en el anillo V, cualquier función simétrica g de las raices de f(x), puede ser expresada en términos de los coeficientes de f(x).

Supongamos $f(x) = (x - u_1)(x - u_2)\dots(x-u_n)$. Entonces el polinomio

$$S_2(f)(x) = (x-(u_1+u_2))(x-(u_1+u_3))\dots(x-(u_{n-1}+u_n))$$

cuyas raices son las sumas de dos raices de f(x) para todas las combinaciones de éstas tomadas de dos en dos, es simétrico en $u_1, \dots u_n$. Sus coeficientes se pueden poner en términos de los coeficientes de f(x) y están por lo tanto en V.

PROPOSICION 5.12. Sean V un campo y f(x) polinomio con coeficientes en V. Supongamos que $S_2(f)$ tiene la raíz u en V. Entonces d(x), el máximo común divisor de los polinomios f(x) y f(u-x) con coeficiente inicial 1, no es constante.

<u>DEMOSTRACION</u>. Sea $d(x) = m\,c\,d(f\,(x),\ f(u-x))$ con - coeficiente inicial 1. Entonces vale una ecuación:

$$d(x) = A(x)\,f(x) + B(x)\,f(u-x) \quad \text{con } A(x),\ B(x) \text{ en } V$$

En $V[u_1, \ldots u_n; f]$ tenemos:

$$d(x) = A(x)\,f(x) + B(x)\,f((u_1 + u_2 - x) + (u - u_1 - u_2))$$

$$= A(x)\,f(x) + B(x)\,f\,(u_1 + u_2 - x) + (u - u_1 - u_2)\,g(x, u_1$$

donde $g(x)$ es un polinomio en dos variables x, y sobre V.

Sustituyendo u_2 tenemos $d(u_2) = (u - u_1 - u_2)\,g\,(u_2, u_1 + 1$

Si $d(x)$ es constante distinta de cero, entonces $d(x) = 1 = d(u_2)$ y $u - u_1 - u_2$ es invertible en $V[u_1, \ldots u_n; f]$. Por el mismo razonamiento $u - u_i - u_j$ $(1 \leq i < j \leq n)$ es también invertible y lo mismo el producto. Pero el producto es $S_2(f)\,(u)$ el cual es cero y llegamos a una contradicción. Entonces $d(x)$ no es constante.

CAPITULO VI

Teorema Fundamental del Algebra.

Sea F un campo realmente cerrado. La campo extensión $E = F(i)$ donde i es una raiz de $x^2 + 1 = 0$ y que formalmente se construye como el campo complejo a partir del campo real, es algebraicamente cerrada.

Para cada elemento $Z = a + b\,i$ de E, definimos el conjugado de Z , $\bar{Z} = a - b\,i$. Además todo elemento de E tiene raiz cuadrada en E.

Necesitaremos el siguiente lema.

<u>LEMA</u> 6.2. Todo polinomio f(x) de grado $n \geq 1$ con coeficientes en F, tiene al menos una raiz en E.

<u>DEMOSTRACION</u>. Sea $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ con a_i en F, polinomio de grado n, donde $n = 2^m q$ y con q impar.

Demostraremos el lema por inducción sobre m.

Para $m = 0$, n es impar y ya que F es realmente cerrado, f(x) tiene una raiz en F y por lo tanto en E.

Supongamos que vale la hipótesis para todo entero menor que m, es decir, que para cualquier polinomio de grado $n' = 2^{m'} q'$ con coeficientes en F podemos encontrar una raiz si $m' < m$.

Sea $F[a_1, \ldots, a_n; f]$ un campo de descomposición de f.

Para cada natural k, sean los polinomios $T_1(f)$, $T_2(f)$ $T_k(f)$ definidos de la siguiente manera:

$$T_k(f(x)) = \prod_{1 \leq i < j \leq n} (x - (a_i + a_j + k a_i a_j))$$

$T_k(f(x))$ es simétrico en las a y por lo tanto tiene sus coeficientes en F. Además el grado de $T_k(f)$ es $\binom{n}{2} = \frac{n(n-1)}{2} = \frac{2^m q (n-1)}{2} = 2^{m-1} q'$ donde q' es impar.

Por la hipótesis de inducción cada $T_k(f(x))$ tiene al menos una raiz b en E.

Sean b_k y $b_{k'}$ las raices correspondientes a la combinación de a_i, a_j. (Es claro que para encontrar estas raices no se necesitan mas de $\binom{n}{2} + 1$ polinomios T_k).

Entonces

$$b_k = a_i + a_j + k a_i a_j \qquad b_{k'} = a_i + a_j + k' a_i a_j$$

y resolviendo este sistema

$$a_i + a_j = \frac{k' b_k - k b_{k'}}{k' - k} \qquad y \qquad a_i a_j = \frac{b_{k'} - b_k}{k' - k}$$

Resolviendo la ecuación de segundo grado con coeficientes en E:

$$x^2 - (a_i + a_j)\, x + a_i a_j = 0$$

Obtenemos las raíces a_i, a_j de $f(x)$ en E y queda demostrado el lema.

Demostración del Teorema Fundamental.

Demostraremos la existencia en E de una raíz del polinomio

6.3. $f(x) = x^m + a_1 x^{m-1} + \dots + a_m$

con coeficientes $1, a_1, a_2, \dots a_m$ en E.

$f_1(x) = f(x)\,\overline{f}(x)$ tiene coeficientes en F, por lo tanto tiene la raíz c en E.

$f_1(c) = f(c)\overline{f}(c) = 0$. Si $f(c) = 0$ está demostrado el teorema. Si $\overline{f}(c) = 0$, entonces $f(\overline{c}) = 0$ y todo pelinomio con coeficientes en E tiene una raíz en E.

CAPITULO VII

Ampliación de un Algoritmo

Suponiendo que existe un algoritmo para encontrar las raíces reales de un polinomio $f(x)$ con coeficientes reales, lo ampliaremos a un algoritmo que nos dé todas las raíces de $f(x)$.

7.1. Procedimiento para descomponer un polinomio en polinomios separables primos entre si.

Si mcd $(f(x), df/dx) = d(x)$ no constante, sea $(f/d)(x) = e_0(x)$, $\mathrm{mcd}(e_0(x), df/dx) = e_1(x)$ no constante, $(e_0/e_1)(x) = f_1(x)$, $\mathrm{mcd}(e_1(x), d^2f/dx^2) = e_2(x), \ldots,$ mcd $(e_{j-1}(x), d^j f/dx^j) = e_j(x)$ no constante, $(e_{j-1}/e_j)(x) = f_j(x)$, mcd $\left(e_j, \frac{d^{j+1} f}{d x^{j+1}}\right) = 1$ $(j > 0)$

Entonces $f(x) = f_1(x)\, f_2(x)^2 \ldots f_j(x)^j\, f_{j+1}(x)^{j+1}$ donde $f_1(x), f_2(x), \ldots, f_{j+1}(x)$ son polinomios primos entre si y separables.

<u>DEMOSTRACION</u>. Sean $a, b, \ldots l$, las raíces distintas de un polinomio $f(x)$ y sean $\alpha, \beta, \ldots, \lambda$, sus respectivas multiplicidades.

$$f(x) = (x-a)^{\alpha}(x-b)^{\beta} \ldots (x-l)^{\lambda}$$

Como una raíz de multiplicidad k de $f(x)$ es una raíz de multiplicidad $k-1$ de su derivada $f'(x)$ es claro que $f(x)$ y $f'(x)$ son divisibles por $(x-a)^{\alpha-1}(x-b)^{\beta-1} \ldots (x-l)^{\lambda-1}$

El máximo común divisor $d(x)$ de $f(x)$ y $f'(x)$ es entonces $d(x) = (x-a)^{\alpha-1} \ldots (x-l)^{\lambda-1}\, g(x)$.

Si $g(x)$ no es constante, tiene un factor $(x-m)$, donde m es una raíz de $f(x)$ digamos $\underline{a}$. Entonces $\underline{a}$ es una raíz de multiplicidad α de $f(x)$, lo cual es una contradicción, ya que $\underline{a}$ es raíz de multiplicidad $\alpha-1$ de $f'(x)$.

$g(x)$ es entonces constante y

7.2. $\operatorname{mcd}(f(x), f'(x)) = (x-a)^{\alpha-1}(x-b)^{\beta-1}\ldots(x-l)^{\lambda-1}$

Agrupando los factores de multiplicidad 1, 2, ... de $f(x)$ tenemos que $f(x) = f_1(x)\, f_2(x)^2\, f_3(x)^3 \ldots$ (si no hay factores de multiplicidad k, $f_k(x) = 1$). Donde los $f_i(x)$ son polinomios separables, mutuamente primos.

$$f'(x) = g_1(x)\, f_2(x)\, f_3(x)^2\, f_4(x)^3 \ldots$$

$$f''(x) = g_2(x)\, f_3(x)\, f_4(x)^2 \ldots$$

$$f'''(x) = g_3(x)\, f_4(x) \ldots$$

donde cada $g_i(x)$ no tiene factores en común con $f(x)$.

Por 7.2, $\operatorname{mcd}(f(x), f'(x)) = d(x) = f_2(x)\, f_3(x)^2\, f_4(x)^3 \ldots$

$$\frac{f(x)}{d(x)} = e_0(x) = f_1(x)\, f_2(x)\, f_3(x)\, f_4(x) \ldots$$

$$e_1(x) = (e_0(x), f'(x)) = f_2(x)\, f_3(x)\, f_4(x) \ldots, \quad \frac{e_0(x)}{e_1(x)} = f_1(x)$$

$$e_2(x) = (e_1(x), f''(x)) = f_3(x)\, f_4(x) \ldots \qquad \frac{e_1(x)}{e_2(x)} = f_2(x)$$

. . . .

$$e_{j+1}(x) = \left(e_j, \frac{d^{j+1} f}{dx^{j+1}}\right) = 1 \qquad \frac{e_j(x)}{e_{j+1}(x)} = f^{j+1}(x)$$

Si $f(x)$ es cualquier polinomio con coeficientes reales, por el procedimiento anterior lo podemos descomponer en polinomios separables.

Sea $g(x)$ un polinomio separable con coeficientes en R. Mediante el algoritmo que tenemos podemos encontrar las raíces reales de $g(x)$, a_1, a_2, ... a_r. Entonces $g(x) = (x-a_1)(x-a_2)..(x-a_r)\,h(x)$, donde $h(x)$ es un polinomio separable con raices complejas únicamente.

Nuestro problema es entonces encontrar las raíces de estos polinomios.

7.3. Método para encontrar las raices complejas de un polinomio con coeficientes reales.

Sea $f(x)$ polinomio separable con coeficientes reales y sin raíces reales.

1.- Fórmese $S_2(f(x))$ y encuéntrense todas sus raíces reales. Supongamos que éstas son simples, digamos b_1, b_2,.. Entonces $\mathrm{mcd}(f(x), f(b_j - x)) = (x-b_j/2)^2 + c_j^2$ donde c_j es positivo.

En este caso las raices de $f(x)$ son los $n=2r$ números complejos $b_j/2 \pm i\,c_j$ $(1 \leqslant j \leqslant r)$.

<u>DEMOSTRACION</u>. Sean $b_1/2 \pm ic_1$, $b_2/2 \pm ic_2$,... $b_r/2 \pm i$ las $2r$ raices de $f(x)$ con todas las c_i distintas. Entonces $S_2(f(x))$ no tiene raices reales repetidas y tiene únicamente r raices reales.

7.4. El máximo común divisor de $f(x)$ y $f(b_j - x)$ es $(x-b_j/2)^2 + c_j^2 = (x-(b_j/2 + i\,c_j))\,(x-(b_j/2 - ic_j))$.

Sean $z_j = b_j/2 + i\,c_j$ $\quad \overline{z}_j = b_j/2 - i\,c_j$

$(x - b_j/2)^2 + c_j^2 = (x-z_j)(x-\overline{z}_j)$. z_j, $\overline{z}_j$ son raices de $f(x)$ entonces $(x-z_j)(x-\overline{z}_j) \mid f(x)$.

Demostraremos que $(x-z_j)(x-\bar{z}_j) \mid f(b_j - x)$.

Como $b_j = z_j + \bar{z}_j$, $f(b_j - x) = f(z_j + \bar{z}_j - x)$.

Dividamos $f(z + z - x)$ por $(x - z)(x - z)$

$$f(z_j + \bar{z}_j - x) = q(x)\left[(x - z_j)\cdot(x-\bar{z}_j)\right] + r(x) \text{ con } gr(r) < 2$$

Sustituyendo z_j tenemos

$$f(z_j + \bar{z}_j - z_j) = q(z_j)\left[(z_j - z_j)(z_j - \bar{z}_j)\right] + r(z_j)$$

$$f(\bar{z}_j) = 0 = 0 + r(z_j).$$

$r(x)$ tiene como factor $(x-z_j)$. Similarmente $r(x)$ tiene como factor $(x-\bar{z}_j)$ de donde $gr(r)$ es al menos 2 lo cual es una contradicción. Entonces $(x- z_j)(x-\bar{z}_j) \mid f(b_j - x)$.

El máximo común divisor de $f(x)$, $f(b-x)$ es $(x - z_j)(x - \bar{z}_j)$.

Supongamos que $mcd(f(x), f(b_j - x)) = h(x)(x-z_j)(x-\bar{z}_j)$. Entonces $h(x)$ tiene como factor a $(x-z_i)$ donde z_i es alguna raíz de $f(x)$, $z_j, \bar{z}_j \neq z_i$

$$f(b_j - x) = f(z_j + \bar{z}_j - x) = \left[h(x)(x - z_j)(x - \bar{z}_j)\right] s(x).$$

Sustituyendo z_i tenemos

$$f(z_j + \bar{z}_j - z_i) = h(z_i)(z_i - \bar{z}_j)(z_i - z_j)\, s(z_i) = 0$$

Entonces $z_j + \bar{z}_j - z_i$ es alguna raíz de $f(x)$, digamos z_k

$z_j + \bar{z}_j - z_i = z_k$, $z_j + \bar{z}_j = z_i + z_k$, $b_j = z_i + z_k$

Contradicción, ya que entonces $S_2(f(x))$ tendría al menos la raíz b_j repetida.

II. Si las raices de $S_2(f(x))$ no son simples, se debe obtener un algoritmo un poco más elaborado.

7.5. Sea B_0 el conjunto de todas las raices b_i de $S_2(f(x))$ y sea $u_0(b_j)$ la multiplicidad de la raíz b_j de $S_2(f(x))$.

Denotemos por A_1 el conjunto de todos los elementos de B_o que no son medios aritméticos de elementos de B_o. Tenemos que mcd $(f(x), f(b-x) = g_b(x) = g_b(b-x)$ es no - constante para toda b de A_1. Entonces $g_b(x) = h_b((x-\frac{b}{2})^2)$

donde $g_b(x)$ tiene grado $2u_o(b)$ y h_b es un polinomio de grado la mitad de el grado de $g_b(x)$ tal que todas las raices de h_b son negativas, digamos son de la forma $-c_{b_k}^2 (1 \leq k \leq u_o(b))$ donde c_{b_k} es positivo. Entonces las raices de $g_b(x)$ son las $2u_o(b)$ números complejos $b/2 \pm ic_{b_k}$ $(1 \leq k \leq u_o(b))$.

DEMOSTRACION. Al formar el conjunto A_1, eliminamos las raices de $S_2(f(x))$ que provienen de raices de $f(x)$ con parte imaginaria igual.

Supongamos que $f(x)$ tiene las siguientes raices repetidas con parte real $\frac{b}{2}$ igual, con b en A_1:

$$z_1 = \frac{b}{2} + i\, c_1, \ \overline{z} = \frac{b}{2} - i\, c_1, \ldots \qquad z_k = \frac{b}{2} + i\, c_k, \ \overline{z}_k = \frac{b}{2} - i\, c_k$$

O sea que $u_o(b) = k$

$(x - z_1)(x - \overline{z}_1) \ldots (x - \overline{z}_k) \mid f(x)$.

Además como $f(x) = (x-z_1)(x-\overline{z}_1) \ldots (x-\overline{z}_k) \cdot g(x)$.

$$f(b - x) = (b - x - z_1)(b - x - \overline{z}_1) \ldots (b-x-\overline{z}_k) \cdot h(x)$$

$$= (\overline{z}_1 - x)(z_1 - x) \ldots (z_k - x) \cdot \emptyset(x) \text{ y entonces}$$

$(x - z_1)(x - \overline{z}_1) \ldots (x - \overline{z}_k) \mid f(b - x)$

Si mcd $(f(x), f(b-x)) = (x-z_1) \ldots (x-\overline{z}_k)\, p(x)$ entonces $p(x)$ tiene como factor a $x-z$ donde z es una raíz de $f(x)$ distinta de $z_1, \ldots \overline{z}_k$.

$$[(x - z_1) \ldots (x-\overline{z}_k)\, p(x)]\, s(x) = f(b - x)$$

$$[(z - z_1)\ldots (z - \overline{z}_k)\, p\,(z)]\, s\,(z) = f(b - z) = 0.$$

Contradicción, ya que $b - z$ sería raíz de $f(x)$ y las únicas raices con esta característica son $z_1, \ldots \overline{z}_k$.

Entonces $\operatorname{mcd}(f(x), f(b-x)) = (x-z_1) \ldots (x-\overline{z}_k) = g_b(x)$ $= g_b(b-x)$

$g_b(x) = h_b((x - b/2)^2).$

$g_b(x) = (x - z_1)\,(z - \overline{z}_1) \,..\, (x - z_k)\,(x - \overline{z}_k)$

$= (x -(b/2 + ic_1))\,(x -(b/2 - ic_1))\ldots(x - (b/2 - ic_k))$

$= [(x - b/2)^2 + c_1^2]\ldots [(x - b/2)^2 + c_k^2].$

$g_b(x) = h_b((x - b/2)^2)$ Si $(x - \frac{b}{2})^2 = y$

$g_b(x) = h_b(y) = (y + c_1^2) \ldots (y + c_k^2)$

De donde las k raices de $h_b((x - b/2)^b)$ son negativas y $f(x)$ tiene como raices los 2k números complejos $b/2 + ic_1, \ldots b/2 + ic_k$.

7.6. Efectuamos el procedimiento anterior para todos los elementos b_j de A . Si se obtienen n raices, nuestro problema está resuelto. Si no es así, procedemos de la siguiente manera.

Para cada elemento $\underline{d}$ de B_0 que no está en A_1, determinamos el número de veces, digamos $v_0(d)$ que $d = ½\,(b+b')$, para b, b' en A y $b<b'$.

Entonces tenemos que $u_1(d) = u_0(d) - 2\, v_0(d) \geqslant 0$ donde $u_1(d)$ así definida no siempre es cero. Formemos el conjunto B_1, de todas las $\underline{d}$ para las cuales $u_1(d)$ es positivo. De esta manera eliminamos las veces que una raíz de

$S_2(f)$ es media aritmética de la parte real de complejos con la parte imaginaria igual.

Procediendo de la manera anterior y sustituyendo B_1 por B_0, u_1 por u_0 y A_2 por A_1, donde A_2 es el subconjunto de todos los miembros de B_1 que no son medios aritméticos de miembros de B_1, encontramos algunas otras raices de $f(x)$.

Si no se obtienen todas las raices, se procede como antes hasta encontrar las n raices.

En la práctica la dificultad estriba en calcular $S_2(f)(x)$ a partir de los coeficientes de f.

Por ejemplo para $n = 3$. Si

$f(x) = x^3 + a_1 x^2 + a_2 x + a_3$, entonces

$S_2(f)(x) = x^3 + 2a_1 x^2 + (a_1^2 + a_2) x + (a_1 a_2 - a_3)$.

B I B L I O G R A F I A :

1.- KONRAD KNOPP.
Theory of Functions. Part I.- Dover Publications, New York, 1945.

2.- GARRETT BIRKHOFF and SAUNDERS MAC LANE.
A Survey of Modern Algebra. (Third Edition).- The Macmillan Company, New York, 1965.

3.- J. V. USPENSKY.
Theory of Equations.- Mc Graw Hill Book Company, New York, 1948.

4.- NATHAN JACOBSON.
Lectures in Abstract Algebra. Vol. III.- D. Van Nostrand Company Inc., New York, 1964.

5.- G. L. VAN DER WAERDEN.
Modern Algebra. Vol. I.- Frederick Ungar Publishing Co., New York, 1964.

6.- EMIL ARTIN.
Galois Theory (Second Edition).- University of Notre Dame Press, Nostre Dame Indiana, 1959.