UNIVERSIDAD DE EL SALVADOR

Facultad de Ingeniería y Arquitectura

Departamento de Matemática

APLICACIONES DE LA TEORIA DE GALOIS

TRABAJO DE GRADUACION PRESENTADO POR:

MARTIN ENRIQUE GUERRA CACERES

FRANCISCO ARMANDO MORENO FAJARDO

PARA OPTAR AL TITULO DE:

LICENCIADO EN MATEMATICA

ABRIL DE 1991

San Salvador, El Salvador, Centro América.

UNIVERSIDAD DE EL SALVADOR

RECTOR : DR. JOSE BENJAMIN LOPEZ GUILLEN

SECRETARIO GENERAL: DRA. GLORIA ESTELA GOMEZ DE PEREZ

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO : ING. JOAQUIN ALBERTO VANEGAS

SECRETARIO : ING. MARIO ARNOLDO MOLINA ARGUETA

DEPARTAMENTO DE MATEMATICA

JEFE EN FUNCIONES : ING. JOAQUIN ALBERTO VANEGAS

UNIVERSIDAD DE EL SALVADOR

TRABAJO DE GRADUACION

COORDINADOR: LIC. JOSE JAVIER RIVERA LAZO

ASESOR : LIC. JOSE JAVIER RIVERA LAZO

D E D I C A T O R I A

A NUESTROS PADRES

A MI COMPAÑERA DE VIDA (Martín Enrique Guerra)

A NUESTROS HERMANOS.

I N D I C E

Página Nº

INTRODUCCION

En el presente trabajo se desarrollan algunas aplicaciones de la teoría de Galois; una teoría bella e interesante del álgebra moderna, belleza que solamente puede apreciarse estudiando exhaustiva e ilustrativamente toda la teoría.

La teoría de Galois y sus aplicaciones permite relacionar el álgebra clásica y el álgebra moderna. Por otro lado, en ella se muestran, creativamente, conjugados todos los conceptos elementales del álgebra moderna: anillos, campos, espacios vectoriales, grupos solubles, grupos de permutaciones, ideales maximales, anillos cocientes, etc.; conceptos que se vuelven instrumentos imprescindibles para deducir las aplicaciones de la teoría de Galois.

El objetivo central es mostrar las aplicaciones más importantes del teorema fundamental de la teoría de Galois, con una exposición clara e ilustrativa de los conceptos principales.

El trabajo se desarrolla básicamente en tres etapas:

En el capítulo I se trata, en parte, de familiarizar al lector con el lenguaje, notación y conceptos utilizados que son propios de la teoría. Se establecen algunas definiciones de las extensiones de campo y de los grupos de Galois, así como ejemplos ilustrativos.

Siempre en el capítulo I, se establece el teorema funda-

mental de la teoría de Galois, que relaciona los campos intermedios de una extensión de campo normal separable finita y los subgrupos de su grupo de Galois. Finalizando el capítulo con ejemplos ilustrativos del teorema fundamental.

En los capítulos del II al VII, se muestra como el teorema fundamental de la teoría de Galois permite fundamentar las aplicaciones. Por ejemplo, se demuestra que un polinomio es soluble si, y sólo si, su grupo de Galois es soluble; se demuestra el teorema fundamental del álgebra y que el campo $\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_k})$ es de grado n^k sobre $\mathbb{Q}$. Por su puesto, los conceptos necesarios para asimilar las aplicaciones son claramente desarrollados al inicio de cada capítulo.

Al final del trabajo, capítulo VII, se presenta una idea que permite construir una teoría de Galois para ecuaciones diferenciales; idea que puede ser desarrollada en otros trabajos de este tipo.

Agradecemos de manera muy especial a nuestro asesor Lic. José Javier Rivera Lazo y a la Sra. Miriam de Yánez por su paciencia en la elaboración de este manuscrito.

CAPITULO I

TEOREMA FUNDAMENTAL DE LA TEORIA DE GALOIS

1.1 LA IDEA CENTRAL DE LA TEORIA DE GALOIS

Las ideas contenidas en los teoremas de esta sección son el fundamento del trabajo que desarrollaremos. Veremos como ellas se relacionan con el estudio de las estructuras de las extensiones de campo.

1.1.1 TEOREMA:

El conjunto de todos los automorfismos de un campo L forma un grupo bajo la composición de mapeos.

1.1.2 DEFINICION:

Sea K un subcampo de un campo L. Un automorfismo α de L es un K-automorfismo de L sí $\alpha(x) = x$, para toda $x \in K$.

1.1.3 TEOREMA:

Si L: K es una extensión de campo entonces el conjunto de todos los K-automorfismos de L forma un grupo bajo la composición de mapeos.

1.1.4 DEFINICION:

El grupo de Galois, $\Gamma(L:K)$, de la extensión L:K es el grupo de todos los K-automorfismos de L bajo la composición de mapeos.

1.1.5 EJEMPLOS:

1) Consideremos la extensión $\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}$. Supongamos que α es un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{2})$. Sea $j = \alpha(\sqrt{2})$, entonces:

$$\begin{aligned} j^2 &= (\alpha(\sqrt{2}))^2 \\ &= \alpha((\sqrt{2})^2) \\ &= \alpha(2) \\ &= 2 \end{aligned}$$

Por tanto: $j = \pm \sqrt{2}$.

Ahora, para cualquier $x,y \in \mathbb{Q}$ se tiene:

$$\begin{aligned} \alpha(x+y\sqrt{2}) &= \alpha(x) + \alpha(y).\alpha(\sqrt{2}) \\ &= x + yj \end{aligned}$$

Luego, hay dos elecciones para $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt{2})$:

$$\alpha_1(x+y\sqrt{2}) = x + y\sqrt{2} \quad y$$
$$\alpha_2(x+y\sqrt{2}) = x - y\sqrt{2}.$$

Claramente α_1(identidad) y α_2 son $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt{2})$.

También $\alpha_2^2 = \alpha_1$; así el grupo de Galois $\Gamma(\mathbb{Q}(\sqrt{2}): \mathbb{Q})$ es cíclico de orden 2.

2) Consideremos ahora la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$. Supongamos que α es un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Como $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}.\sqrt{3}\}$ es una base para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, se sigue que todo elemento de esta extensión es de la forma:

$$p + q\sqrt{2} + r\sqrt{3} + s\sqrt{2}.\sqrt{3}, \text{ donde } p, q, r, s \in \mathbb{Q}.$$

Así, un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ está determinado por sus valores sobre $\sqrt{2}$ y $\sqrt{3}$. Luego:

$$I = \text{identidad}$$

$$\sigma_1 : \sqrt{2} \longrightarrow -\sqrt{2}, \text{ dejando fijo } \sqrt{3},$$

$$\sigma_2 : \sqrt{3} \longrightarrow -\sqrt{3}, \text{ dejando fijo } \sqrt{2},$$

$$\sigma_3 : \sigma_1 \circ \sigma_2.$$

Son las únicas combinaciones posibles de los valores sobre $\sqrt{2}$, $\sqrt{3}$, y por lo tanto, todos los $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Obsérvese que:

0	I	σ_1	σ_2	σ_3
I	I	σ_1	σ_2	σ_3
σ_1	σ_1	I	σ_3	σ_2
σ_2	σ_2	σ_3	I	σ_1
σ_3	σ_3	σ_2	σ_1	I

y que el orden de grupo de Galois $\Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$ es 4.

3) Sea la extensión $\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}$. Si α es un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt[3]{3})$, entonces:

$$(\alpha(\sqrt[3]{3}))^3 = \alpha((\sqrt[3]{3})^3)$$

$$= \alpha(3)$$

$$= 3$$

Como $\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{R}$, debe tenerse que:

$$\alpha(\sqrt[3]{3}) = \sqrt[3]{3}.$$

Luego, el único $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt[3]{3})$ es la identidad y $\Gamma(\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q})$ tiene orden 1.

Ahora veremos como el grupo de Galois refleja aspectos de la estructura de una extensión L:K. Galois hizo el descubrimiento (por supuesto, expresado por él en términos de polinomios) que bajo *ciertas hipótesis* hay una correspondencia uno a uno entre:

1) Los subgrupos del grupo de Galois de L:K.
2) Los subcampos M de L, tales que: K $\subset$ M.

Exploremos como se establece esta correspondencia.

1.1.6 DEFINICION:

Si L:K es una extensión de campo, llamaremos a un campo M que cumple: K $\subset$ M $\subset$ L, un campo intermedio.

A cada campo intermedio M le asociamos el grupo

$$M^* = \Gamma(L:M),$$

de todos los M-automorfismos de L. Así:

$K^* = \Gamma(L:K)$, todo el grupo de Galois.

$L^* = \{I_L\}$, I_L la identidad sobre L.

Si M c N, entonces $M^* \supset N^*$. Pues cualquier mapeo que deja fijos los elementos de N, también deja fijos los elementos de M.

Recíprocamente, a cada subgrupo H de $\Gamma(L:K)$ le asociamos el conjunto H^+ de todos los elementos $x \in L$ tales que: $\alpha(x) = x$, para todo $\alpha \in H$. Es fácil probar que H^+ es un subcampo de L que contiene a K.

1.1.7 DEFINICION:

Si H es un subgrupo de $\Gamma(L:K)$, H^+ es el campo fijo de H.

Si H c G, entonces $H^+ \supset G^+$. Pues cualquier elemento de L que es dejado fijo por todo elemento $\alpha \in G$, también es dejado fijo por cualquier elemento de H.

Sea M un campo intermedio y H un subgrupo del grupo de Galois. Entonces:

$$M^+ = \Gamma(L:M) ,$$
$$H^+ = \{x \in L / \alpha(x) = x, \quad \forall \alpha \in H\}.$$

Luego:

(1) $\begin{cases} M \text{ c } M^{*+}, \text{ pues cada elemento de M es dejado fijo por cada elemento de } M^*. \\ H \text{ c } H^{+*}, \text{ pues cada automorfismo de H deja fijo los elementos de } H^+. \end{cases}$

El ejemplo 1.1.5-3 muestra que estas inclusiones no son siempre igualdades, porque:

$$\mathbb{Q}^* = \Gamma(\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}) = \{I\},\ I \text{ la identidad sobre } \mathbb{Q}(\sqrt[3]{3}),\ \text{y}$$

$$\mathbb{Q}^{*+} = \mathbb{Q}(\sqrt[3]{3}).$$

De donde: $\mathbb{Q} \subset \mathbb{Q}^{*+}$ y $\mathbb{Q}^{*+} \neq \mathbb{Q}$.

Si F denota el conjunto de los campos intermedios y G el conjunto de subgrupos del grupo de Galois, entonces tenemos dos mapeos:

$$*: F \longrightarrow G \text{ t.q } M \rightsquigarrow M^*\ , \text{ y}$$
$$+: G \longrightarrow F \text{ t.q } H \rightsquigarrow H^+.$$

Los cuales invierten las inclusiones y satisfacen (1). La idea de Galois puede ser interpretada como dar condiciones bajo las cuales * y + son mutuamente inversas, estableciendo así una biyección entre F y G. Las condiciones extras que necesitamos son llamadas separabilidad y normalidad.

1.1.8 EJEMPLOS:

1) Sabemos que $\Gamma(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \langle \alpha_2 : \alpha_2^2 = \alpha_1 \rangle$ es un grupo cíclico de orden 2. Es fácil ver que no hay otros subcampos intermedios entre $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}$ diferente de ellos. Así pues:

$$\mathbb{Q}^* = \{\alpha_2,\ \alpha_2^2\},$$

$$\mathbb{Q}^*(\sqrt{2}) = \{\alpha_2^2\}$$

$$\mathbb{Q}^{*+} = \mathbb{Q},$$

$$\mathbb{Q}^{*+}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

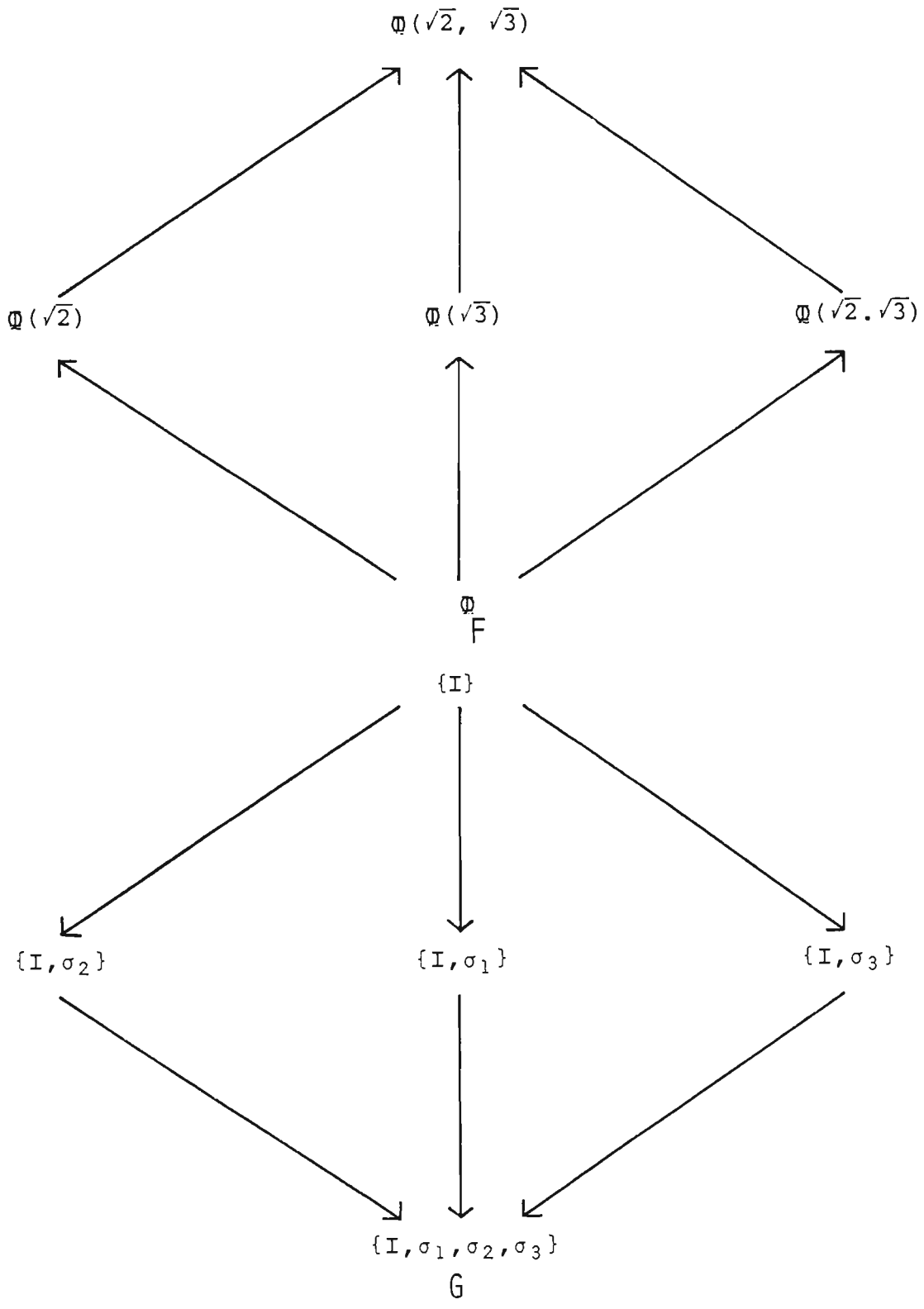
Por lo tanto, la correspondencia de Galois entre F y G es una biyección.

Formemos el siguiente diagrama:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \longleftrightarrow & \{\alpha_2^2\} \\ \uparrow & & \downarrow \\ \mathbb{Q} & \longleftrightarrow & \{\alpha_2,\ \alpha_2^2\} \end{array}$$

donde las flechas verticales representan inclusiones y las horizontales los elementos que se corresponden bajo la correspondencia de Galos.

2) Sea $\mathbb{Q}(\sqrt{2}, \sqrt{3})$: $\mathbb{Q}$ (ver 1.1.5-2). Entre los siguientes diagramas, la correspondencia de Galois es biyectiva.


$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(\sqrt{3})$
$\mathbb{Q}(\sqrt{2}.\sqrt{3})$
$\mathbb{Q}$
F
$\{I\}$
$\{I, \sigma_2\}$
$\{I, \sigma_1\}$
$\{I, \sigma_3\}$
$\{I, \sigma_1, \sigma_2, \sigma_3\}$
G

A manera de ilustración tenemos:

$$\mathbb{Q}^*(\sqrt{2}) = \{I, \sigma_2\} \qquad \mathbb{Q}^{*+}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}),$$

$$\mathbb{Q}^*(\sqrt{3}) = \{I, \sigma_1\} \qquad \mathbb{Q}^{*+}(\sqrt{3}) = \mathbb{Q}(\sqrt{3}),$$

$$\mathbb{Q}^*(\sqrt{2}.\sqrt{3}) = \{I, \sigma_3\} \qquad \mathbb{Q}^{*+}(\sqrt{2}\sqrt{3}) = \mathbb{Q}(\sqrt{2}.\sqrt{3})$$

1.2 NORMALIDAD Y SEPARABILIDAD.

CAMPO DE DESCOMPOSICION.

1.2.1 DEFINICION:

Si K es un campo y f es un polinomio sobre K, entonces f se descompone sobre K si f puede ser expresado como un producto de factores lineales, es decir:

$f(t) = k(t - \alpha_1)(t - \alpha_2) \ldots (t - \alpha_n)$ donde

$\alpha_1, \alpha_2, \ldots, \alpha_n \in K$.

1.2.2 EJEMPLO:

Sea $f(t) = t^2 + 1$ un polinomio sobre $\mathbf{Z}_2$, entonces $t^2 + 1 = (t + 1)(t + 1)$.

1.2.3 DEFINICION:

El campo Σ es un campo de descomposición para el polinomio f sobre el campo K si $K \subset \Sigma$ y:

1) f se descompone sobre Σ,

2) Si $K \subset \Sigma' \subset \Sigma$, y f se descompone sobre Σ' entonces $\Sigma = \Sigma'$.

La segunda condición es equivalente a:

2') $\Sigma = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ donde

$\alpha_1, \alpha_2, \ldots, \alpha_n$ son los ceros de f en Σ.

1.2.4 EJEMPLOS:

1) Sea $f(t) = t^3 - 1$ un polinomio sobre $\mathbb{Q}$. Entonces f se factoriza así:

$$f(t) = (t - 1)(t + \frac{1-\sqrt{3}\,i}{2})(t + \frac{1+\sqrt{3}\,i}{2}) \text{ donde}$$

$1, \frac{1 - \sqrt{3}\,i}{2}, \frac{1 + \sqrt{3}\,i}{2}$ son las raíces de f(t). Luego el campo de descomposición de f es $\mathbb{Q}(1, \frac{1 - \sqrt{3}\,i}{2} \quad \frac{1 + \sqrt{3}\,i}{2})$, el cual es igual a $\mathbb{Q}(\sqrt{3}\,i)$.

2) Sea $f(t) = t^2 + t + 1$ un polinomio sobre $\mathbf{Z}_2$. El campo $\mathbf{Z}_2$ consta de dos elementos 0 y 1. Evidentemente f es irreducible sobre $\mathbf{Z}_2$.

Sea ξ un elemento tal que ξ tenga a f como polinomio mínimo sobre $\mathbf{Z}_2$. Entonces

$$\xi^2 + \xi + 1 = 0$$

$$\xi^2 = -\xi - 1$$

$$\xi^2 = \xi + 1.$$

Como ξ es raíz de un polinomio mínimo de grado 2, los elementos de $\mathbf{Z}_2(\xi)$ son de la forma $a + b\xi$, donde $a,b \in \mathbf{Z}_2$. Luego, los elementos del campo $\mathbf{Z}_2(\xi)$ son:

$$1,\ 0,\ \xi,\ +\ 1\ +\ \xi.$$

Las siguientes tablas muestran el producto y la suma en $\mathbf{Z}_2(\xi)$:

+	0	1	ξ	$1+\xi$
0	0	1	ξ	$1+\xi$
1	1	0	$1+\xi$	ξ
ξ	ξ	$1+\xi$	0	1
$1+\xi$	$1+\xi$	ξ	1	0

.	0	1	ξ	$1+\xi$
0	0	0	0	0
1	0	1	ξ	$1+\xi$
ξ	0	ξ	$1+\xi$	1
$1+\xi$	0	$1+\xi$	1	ξ

Tenemos que $\mathbf{Z}_2(\xi)$ tiene cuatro elementos. Y f se descompone sobre $\mathbf{Z}_2(\xi)$ así:

$$t^2 + t + 1 = (t - \xi)(t - 1 - \xi),$$

pero no sobre un campo más pequeño. Luego, $\mathbf{Z}_2(\xi)$ es un campo de descomposición para f sobre $\mathbf{Z}_2$.

1.2.5 TEOREMA:

Si K es cualquier campo y f es un polinomio cualquiera sobre K, entonces existe un campo de descomposición para f sobre K.

1.2.6 TEOREMA:

Sea $i: K \longrightarrow K'$ un isomorfismo de campo. Sea T un campo de descomposición para f sobre K, T' un campo de descomposición para i(f) sobre K'. Entonces existe un isomorfismo $j: T \longrightarrow T'$ tal que $j/_K = i$. De otra manera, las extensiones T:K y T':K' son isomórficas.

Por lo tanto, tenemos que los campos de descomposición son únicos.

1.2.7 EJEMPLOS:

Sea $f(t) = t^3 - 3$, que no se descompone sobre $\mathbb{Q}(\sqrt[3]{3})$, donde $\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{R}$ y solamente un cero de f es real.

Así, f(t) se factoriza en $(\mathbb{Q}(\sqrt[3]{3}))[t]$ en un factor lineal, $t - \sqrt[3]{3}$, y un factor cuadrático irreducible. Sea Σ el campo de descomposición de $t^3 - 3$ sobre $\mathbb{Q}$, entonces

$$\begin{aligned}[\Sigma: \mathbb{Q}] &= [\Sigma: \mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{3}): \mathbb{Q}] \\ &= 2.3 \\ &= 6\end{aligned}$$

Hemos mostrado que el campo de descomposición Σ sobre $\mathbb{Q}$ de t^3-3 es de grado 6 sobre $\mathbb{Q}$. Los otros ceros de f(t) en $\mathbb{C}$ son:

$$\sqrt[3]{3}\left(\frac{-1 + \sqrt{3}\, i}{2}\right) \quad \text{y} \quad \sqrt[3]{3}\left(\frac{-1 - \sqrt{3}\, i}{2}\right)$$

Así el campo de descomposición Σ de $t^3 - 3$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}\, i)$.

Normalidad.

1.2.8 DEFINICION:

Una extensión L:K es normal si todo polinomio irreducible f sobre K que tiene al menos un cero en L, se descompone en L.

1.2.9 EJEMPLOS:

1) La extensión $\mathbb{C}$: $\mathbb{R}$ es normal, pues todo polinomio sobre $\mathbb{R}$ (irreducible o no) se descompone en $\mathbb{C}$.

2) Consideremos la extensión $\mathbb{Q}(\sqrt[3]{3})$: $\mathbb{Q}$. El polinomio irreducible $t^3 - 3$ sobre $\mathbb{Q}$ tiene un cero en $\mathbb{Q}(\sqrt[3]{3})$, sin embargo no se descompone en ese campo. (ver 1.2.7).

1.2.10 TEOREMA:

Una extensión L: K es normal y finita, si y sólo si, L es un campo de descomposición para algún polinomio sobre K.

1.2.11 EJEMPLO:

1.2.4-2 muestra que $\mathbf{Z}_2(\xi)$: $\mathbf{Z}_2$ es normal y finita, pues $\mathbf{Z}_2(\xi)$ es el campo de descomposición para el polinomio t^2+t+1 sobre $\mathbf{Z}_2$.

Separabilidad.

1.2.12 DEFINICION:

Un polinomio irreducible f sobre K es separable sobre K, si no tiene ceros múltiples en un campo de descomposición.

1.2.13 EJEMPLOS:

1) Sea $f(t) = t^2 + 1$ un polinomio sobre $\mathbb{Q}$. Los ceros de f son i, -i. Luego $\mathbb{Q}(i)$ es un campo de descomposición para f y además f es separable sobre $\mathbb{Q}$, pues no tiene ceros múltiples en dicho campo de descomposición.

2) Sea $f(t) = t^4 + t^3 + t^2 + t + 1$ un polinomio sobre $\mathbb{Q}$. f(t) es irreducible sobre $\mathbb{Q}$ y sus ceros son:

$$e^{\frac{2\pi}{5}i}, \quad e^{\frac{4\pi}{5}i}, \quad e^{\frac{6\pi}{5}i}, \quad e^{\frac{8\pi}{5}i},$$

los cuales son diferentes. Luego, el polinomio irreducible f(t) es separable sobre el $\mathbb{Q}$, ya que en el campo descomposición $\mathbb{Q}(e^{\frac{2\pi}{5}i})$ no hay ceros múltiplos.

1.2.14 DEFINICION:

Un polinomio irreducible sobre un campo K es no separable sobre K, si no es separable sobre K.

1.2.15 TEOREMA:

Si K es un campo de característica 0 (cero) entonces todo polinomio irreducible sobre K es separable sobre K.

Si K tiene característica $p > 0$ entonces un polinomio irreducible f sobre K es no separable, si y sólo si,

$$f(t) = k_0 + k_1 t^p + k_2 t^{2p} + \ldots + k_r t^{rp}$$

donde $k_0, k_1, k_2, \ldots, k_r \in K$.

1.2.16 EJEMPLOS:

1) Todo polinomio irreducible sobre $\mathbb{R}$ es separable sobre $\mathbb{R}$, pues $\mathbb{R}$ es de caracterísca cero.

2) Sea $f(t) = t^4 + t^2 + 1$ un polinomio sobre $\mathbf{Z}_2$. Este polinomio es irreducible sobre $\mathbf{Z}_2$. Adjuntemos un elemento α tal que

$$\alpha^4 + \alpha^2 + 1 = 0$$

$$\alpha^4 = \alpha^2 + 1.$$

Los elementos de $\mathbf{Z}_2(\alpha)$ son de la forma: $a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3$, con $a_i \in \mathbf{Z}_2$. Este es un campo de 16 elementos y el polinomio f(t)

se factoriza en $\mathbf{Z}_2(\alpha)$ de la forma siguiente:

$$f(t) = (t - \alpha)^2(t - (\alpha + 1))^2$$

Por lo tanto, $f(t) = t^4 + t^2 + 1$ es no separable sobre $\mathbf{Z}_2$.

1.2.17 DEFINICION:

a) Un polinomio sobre un campo K es separable sobre K, si todos sus factores irreducibles son separables sobre K.

b) Si L: K es una extensión, entonces un elemento algebraico $\alpha \in L$ es separable sobre K, si su polinomio mínimo sobre K es separable sobre K.

c) Una extensión algebraica L: K, es una extensión separable si todo $\alpha \in L$ es separable sobre K.

1.2.18 TEOREMA:

Sea L: K una extensión algebraica separable y sea M un campo intermedio. Entonces M: K y L: M son separables.

1.3 GRADOS DE CAMPOS Y ORDENES DE GRUPOS.

La cardinalidad de un conjunto S lo denotaremos por $|S|$. Luego, Si G es un grupo entonces $|G|$ es el orden de G.

1.3.1 TEOREMA:

Sea G un sugrupo finito del grupo de automorfismos de un campo K, y sea K_0 el campo fijo de G. Entonces:

$$[K: K_0] = |G|.$$

1.3.2 COROLARIO:

Si G es el grupo de Galois de la extensión finita L: K y H es un subgrupo finito de G, entonces:

$$[H^+: K] = \frac{[L: K]}{|H|}$$

1.3.3 EJEMPLO:

Sea $K = \mathbb{Q}(\omega)$, donde $\omega = e^{\frac{2\pi}{5}i} \in \mathbb{C}$. Ahora $\omega^5 = 1$ y $\mathbb{Q}(\omega)$ consiste de todos los elementos $p + q\omega + r\omega^2 + s\omega^3 + t\omega^4$, donde $p, q, r, s, t \in \mathbb{Q}$. El grupo de Galois de $\mathbb{Q}(\omega): \mathbb{Q}$ es fácil de encontrar.

Si α es un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\omega)$, entonces:

$$\begin{aligned}(\alpha(\omega))^5 &= \alpha(\omega^5)\\ &= \alpha(1)\\ &= 1\end{aligned}$$

Asi que: $\alpha(\omega) = \omega, \omega^2, \omega^3$ ó ω^4.

De esto resultan cuatro elecciones para $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\omega)$:

$$\alpha_1: p + q\omega + r\omega^2 + s\omega^3 + t\omega^4 \longrightarrow p + q\omega + r\omega^2 + s\omega^3 + t\omega^4$$

$$\alpha_2: \longrightarrow p + s\omega + q\omega^2 + t\omega^3 + r\omega^4$$

$$\alpha_3: \longrightarrow p + r\omega + t\omega^2 + q\omega^3 + s\omega^4$$

$$\alpha_4: \longrightarrow p + t\omega + s\omega^2 + r\omega^3 + q\omega^4.$$

Es sencillo verificar que estos son todos los $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\omega)$.

Luego:

$$[\mathbb{Q}(\omega): \mathbb{Q}] = |G|$$
$$= 4.$$

Hay que observar este ejemplo que $t^5 - 1$ no es el polinomio mínimo de ω, pues es reducible sobre $\mathbb{Q}$; es decir:

$$t^5 - 1 = (t-1)(t^4 + t^3 + t^2 + t + 1)$$

Así, tenemos que $t^4 + t^3 + t^2 + t + 1$ es irreducible sobre $\mathbb{Q}$, y lo satisface, entonces este es el polinomio mínimo de ω.

1.4 MONOMORFISMOS, AUTOMORFISMOS Y CERRADURAS NORMALES.

El objetivo de esta sección es usar K-monomorfismos para construir K-automorfismos, para luego poder calcular el orden del grupo de Galois de cualquier extensión normal separable finita.

1.4.1 DEFINICION:

Supongamos que K es un subcampo de cada uno de los campos M y L. Entonces un K-monomorfismo de M en L es un mapeo ϕ: M ——> L, el cual es un monomorfismo de campo, tal que:

$$\alpha(x) = x, \text{ para toda } x \in K.$$

En general, si K c M c L, entonces cualquier K-automorfismo de L se restringe a un K-monomorfismo M ——> L.

Ahora veamos el proceso inverso.

1.4.2 TEOREMA:

Supongamos que L: K es una extensión normal finita y K c M c L. Sea τ cualquier K-monomorfismo M ——> L. Entonces existe un K-automorfismo σ de L, tal que:

$$\sigma/M = \tau.$$

Este resultado puede ser usado para construir K-automorfismos como sigue:

1.4.3 TEOREMA:

Supongamos que L: K es una extensión normal finita y α, β son ceros en L del polinomio irreducible p sobre K. Entonces existe un K-automorfismo σ de L, tal que: $\sigma(\alpha) = \beta$.

CERRADURA NORMAL

1.4.4 DEFINICION:

Sea L una extensión algebraica de K. Una cerradura normal de L: K, es una extensión N de L tal que:

1) N: K es normal,
2) Si L c M c N y M: K es normal, entonces M = N.

El próximo teorema nos asegura la existencia de cerraduras normales para extensiones finitas.

1.4.5 TEOREMA:

Si L: K es una extensión finita, entonces existe una cerradura normal N, la cual es una extensión finita de K. Si M es otra cerradura normal, entonces las extensiones M: K y N: K son isomórficas.

1.4.6 EJEMPLO:

Sea $\mathbb{Q}(\sqrt[3]{3})$: $\mathbb{Q}$; esta extensión no es normal, pues el polinomio $t^3 - 3$ no se descompone en $\mathbb{Q}(\sqrt[3]{3})$. En 1.2.7 se ha probado que $\mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$ es el campo de descomposición de $t^3 - 3$ sobre $\mathbb{Q}$. Luego, $\mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$ es normal y finita sobre $\mathbb{Q}$. Ahora supongamos que M: $\mathbb{Q}$ es normal y $\mathbb{Q}(\sqrt[3]{3})$ c M c $\mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$; entonces el polinomio $t^3 - 3$ se descompone en M. Así, $\sqrt[3]{3}, i\sqrt{3} \in M$. Es decir:

$\mathbb{Q}(\sqrt[3]{3}, i\sqrt{3}) \subset M$, obteniendo así que $M = \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$.

Por lo tanto,

$$\mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$$

es la cerradura normal de la extensión $\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}$.

1.4.7 TEOREMA:

Supongamos que $K \subset L \subset N \subset M$ donde $L:K$ es finita y N es una cerradura normal de $L:K$. Si τ es cualquier k-monomorfismo $L \longrightarrow M$, entonces $\tau(L) \subset N$.

1.4.8 TEOREMA:

Para una extensión finita $L:K$ las siguientes proposiciones son equivalentes:

1) $L:K$ es noraml.
2) Existe una extensión normal N de K que contiene a L tal que todo K-monomorfismo $\tau: L \longrightarrow N$ es un K-automorfismo de L.
3) Para toda extensión normal M de K que contiene a L, todo K-monomorfismo $\tau: L \longrightarrow M$ es un K-automorfismo de L.

1.4.9 TEOREMA:

Supongamos que $L:K$ es una extensión separable finita de grado n. Entonces hay precisamente n distintos K-monomorfismo de L en una cerradura normal N (y por lo tanto cualquier extensión

normal M de K que contiene a L).

Ahora podemos calcular el orden del grupo de Galois de una extensión normal separable finita.

1.4.10 COROLARIO:

Si L:K es una extensión normal separable finita de grado n, entonces hay precisamente n distintos K-automorfismos de L; así que:

$$|\Gamma(L:K)| = n.$$

1.4.11 TEOREMA:

Sea L:K una extensión finita con grupo de Galois G. Si L:K es normal y separable entonces K es el campo fijo de G.

Hay un recíproco de este resultado, el cual muestra por qué debemos considerar extensiones normales separables a fin de hacer de la correspondencia de Galois una biyección.

1.4.12 TEOREMA:

Si L:K es una extensión finita con grupo de Galois G. Y sí K es el campo fijo de G, entonces L:K es normal y separable.

Si la correspondencia de Galois es una biyección ($K^{*+} = K$) entonces K debe ser el campo fijo de el grupo de Galois de L:K;

así por 1.4.12, L:K es separable y normal. Que esta hipótesis son también suficientes para hacer la correspondencia de Galois biyectiva, lo veremos en la siguiente sección.

1.5 TEOREMA FUNDAMENTAL DE GALOIS.

La correspondencia de Galois establece propiedades fundamentales entre una extensión de campo y su grupo de Galois.

Sea L:K una extensión de campo con grupo de Galois $\Gamma(L:K)$, el cual consiste de todos los K-automorfismos de L.

$$\Gamma(L:K) = \{\alpha : L \longrightarrow L/\alpha \text{ es un automorfismo y } \alpha(x) = x, \forall x \in K\}.$$

Sea F el conjunto de todos los campos intermedios y G el conjunto de todos los subgrupos H de $\Gamma(L:K)$. Entonces hemos definido dos mapeos:

$$*: F \longrightarrow G$$
$$+: G \longrightarrow F$$

Como sigue:

Si $M \in F$, entonces M^* es el grupo de todos los M-automorfismos de L.

Si $H \in G$, entonces H^+ es el campo fijo de H.

Obsérvese que: $M \subset M^{*+}$ y $H \subset H^{+*}$.

1.5.1 TEOREMA (El Teorema fundamental de la teoría de Galois):

Si L:K es una extensión normal separable finita de grado n con grupo de Galois $\Gamma(L:K)$, y sí $\mathcal{F}$, $\mathcal{G}$, $*$ y $+$ están definidos como anteriormente entonces:

1) El grupo de Galois tiene orden n.
2) Los mapeos $*$ y $+$ son mutuamente inversos y establecen una correspodencia uno a uno que invierten el orden entre $\mathcal{F}$ y $\mathcal{G}$; es decir: $M^{*+} = M$ y $H^{+*} = H$, si $M,N \in \mathcal{F}$ y si $M \subset N$ entonces $M^* \supset N^*$, y si $H,G \in \mathcal{G}$ y si $H \subset G$ entonces $H^+ \supset G^+$.
3) Si M es un campo intermedio, entonces

$$[L:M] = |M^*|$$

$$[M:K] = \frac{|\Gamma(L:K)|}{|M^*|}$$

4) Un campo intermedio M es una extensión normal de K si, y sólo sí M^* es un subgrupo normal de $\Gamma(L:K)$.
5) Si un campo intermedio M es una extensión normal de K, entonces el grupo de Galois de M:K es isomorfo al grupo cociente $\frac{\Gamma(L:K)}{M^*}$.

1.6 CALCULO DE GRUPOS DE GALOIS.

1.6.1 EJEMPLO:

1) i) Sea $f(t) = t^4 - 2$ un polinomio, el cual es irreducible so-

bre $\mathbb{Q}$, y sea K un campo de descomposición para f. Entonces $K \subset \mathbb{C}$ y en $\mathbb{C}$, podemos factorizar f como sigue:

$$f(t) = (t - \xi)(t + \xi)(t - i\xi)(t + i\xi)$$

donde $\xi = \sqrt[4]{2} \in \mathbb{R}^+$. Evidentemente $K = \mathbb{Q}(\xi, i)$, y en consecuencia es normal y finita. Como la característica de K es cero, entonces $K:\mathbb{Q}$ es separable.

Por lo tanto, $K:\mathbb{Q}$ es una extensión normal separable finita.

ii) Ahora encontremos el grado de $K:\mathbb{Q}$. Tenemos:

$[K:\mathbb{Q}] = [\mathbb{Q}(\xi,i):\mathbb{Q}(\xi)][\mathbb{Q}(\xi):\mathbb{Q}]$.

veamos el grado de $\mathbb{Q}(\xi,i):\mathbb{Q}(\xi)$. Como el polinomio mínimo de i sobre $\mathbb{Q}(\xi)$ es $t^2 + 1$, ya que: $i^2 + 1 = 0$ e $i \notin \mathbb{R} \supset \mathbb{Q}(\xi)$. Entonces

$$[\mathbb{Q}(\xi,i):\mathbb{Q}(\xi)] = 2.$$

Como ξ es un cero de f(t) y además f(t) es irreducible sobre $\mathbb{Q}$, entonces f(t) es el polinomio mínimo de ξ sobre $\mathbb{Q}$. Luego,

$$[\mathbb{Q}(\xi):\mathbb{Q}] = 4.$$

Por lo tanto

$$[K:\mathbb{Q}] = 2.4 = 8.$$

iii) Ahora encontremos los elementos del grupo de Galois de $K:\mathbb{Q}$.

Una base de $\mathbb{Q}(\xi,i)$ sobre $\mathbb{Q}(\xi)$ es:$\{1,i\}$; y una base de

$\mathbb{Q}(\xi)$ sobre $\mathbb{Q}$ es: $\{1, \xi, \xi^2, \xi^3\}$. Entonces una base de $\mathbb{Q}(\xi,i)$ sobre $\mathbb{Q}$ es:

$$\{1, \xi, \xi^2, \xi^3, i, i\xi, i\xi^2, i\xi^3\}.$$

Como K: $\mathbb{Q}$ es una extensión normal separable finita, por el teorema fundamental de Galois parte 1 (1.5.1):

$$|\Gamma(K:\mathbb{Q})| = [K:\mathbb{Q}] = 8.$$

Así, tenemos que encontrar 8 $\mathbb{Q}$-automorfismos de K.

Sabemos que cualquier $\mathbb{Q}$-automorfismos de K está completamente determinado por sus valores sobre los elementos de la base, y éstos a su vez, están determinados por los valores de ξ e i.

Sea σ un $\mathbb{Q}$-automorfismo de K y encontremos $\sigma(\xi)$ y $\sigma(i)$. Veamos:

$$\begin{aligned} j &= \sigma(\xi) \quad , \\ j^4 &= (\sigma(\xi))^4, \\ j^4 &= \sigma(\xi^4) \quad , \\ j^4 &= \sigma(2) \quad , \\ j^4 &= 2 \quad . \end{aligned}$$

luego: $j = \xi, -\xi, i\xi, -i\xi$.

$$\begin{aligned} \ell &= \sigma(i) \quad , \\ \ell^2 &= (\sigma(i))^2, \\ \ell^2 &= \sigma(i^2) \quad , \\ \ell^2 &= \sigma(-1) \quad , \\ \ell^2 &= -1 \quad . \end{aligned}$$

luego: $\ell = i, -i$.

Todas las posibles combinaciones son:

	I	σ	σ_1	σ_2	τ	τ_1	τ_2	τ_3
ξ	ξ	$i\xi$	$-\xi$	$-i\xi$	ξ	$i\xi$	$-\xi$	$-i\xi$
i	i	i	i	i	-i	-i	-i	-i

TABLA Nª 1.

A manera de ilustración tenemos:

$$\sigma_2(\xi) = -i\xi \quad y \quad \sigma_2(i) = i.$$

Ahora:

$$\begin{aligned}(\tau\sigma)(\xi) &= \tau(\sigma(\xi)) \\ &= \tau(i.\xi) \\ &= \tau(i).\tau(\xi) \\ &= -i.\xi.\end{aligned}$$

$$\begin{aligned}(\sigma\tau)(\xi) &= \sigma(\tau(\xi)) \\ &= \sigma(\xi) \\ &= i.\xi.\end{aligned}$$

Luego, $\tau\sigma \neq \sigma\tau$ y en consecuencia $\Gamma(K:\mathbb{Q})$ es no abeliano.

La tabla Nª 1 podemos volve a escribirla de la manera siguiente:

	I	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
ξ	ξ	$i\xi$	$-\xi$	$-i\xi$	ξ	$i\xi$	$-\xi$	$-i\xi$
i	i	i	i	i	-i	-i	-i	-i

TABLA Nª 2

donde: $\sigma^4 = I$, $\tau^2 = I$ y $\tau\sigma = \sigma^3\tau$.

La tabla siguiente nos muestra las operaciones entre los elementos del grupo de Galois de $K:\mathbb{Q}$.

0	I	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
I	I	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
σ	σ	σ^2	σ^3	I	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	τ
σ^2	σ^2	σ^3	I	σ	$\sigma^2\tau$	$\sigma^3\tau$	τ	$\sigma\tau$
σ^3	σ^3	I	σ	σ^2	$\sigma^3\tau$	τ	$\sigma\tau$	$\sigma^2\tau$
τ	τ	$\sigma^3\tau$	$\sigma^2\tau$	$\sigma\tau$	I	σ^3	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^3\tau$	$\sigma^2\tau$	σ	I	σ^3	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	$\sigma^3\tau$	σ^2	σ	I	σ^3
$\sigma^3\tau$	$\sigma^3\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^3	σ^2	σ	I

TABLA Nº 3.

iv) Entonces tenemos la relación siguiente:

$$\Gamma(K:\mathbb{Q}) = \langle \sigma, \tau : \sigma^4 = \tau^2 = I, \tau\sigma = \sigma^3\tau \rangle.$$

v) Los subgrupos de $\Gamma(K:Q)$ son obtenidos fácilmente de la tabla Nº 3:

orden 8: $\Gamma(K:\mathbb{Q})$.

orden 4: $S = \{I, \sigma, \sigma^2, \sigma^3\}$

$T = \{I, \sigma^2, \tau, \sigma^2\tau\}$

$U = \{I, \sigma^2, \sigma\tau, \sigma^3\tau\}$

Orden 2: $A = \{I, \sigma^2\}$

$B = \{I, \tau\}$

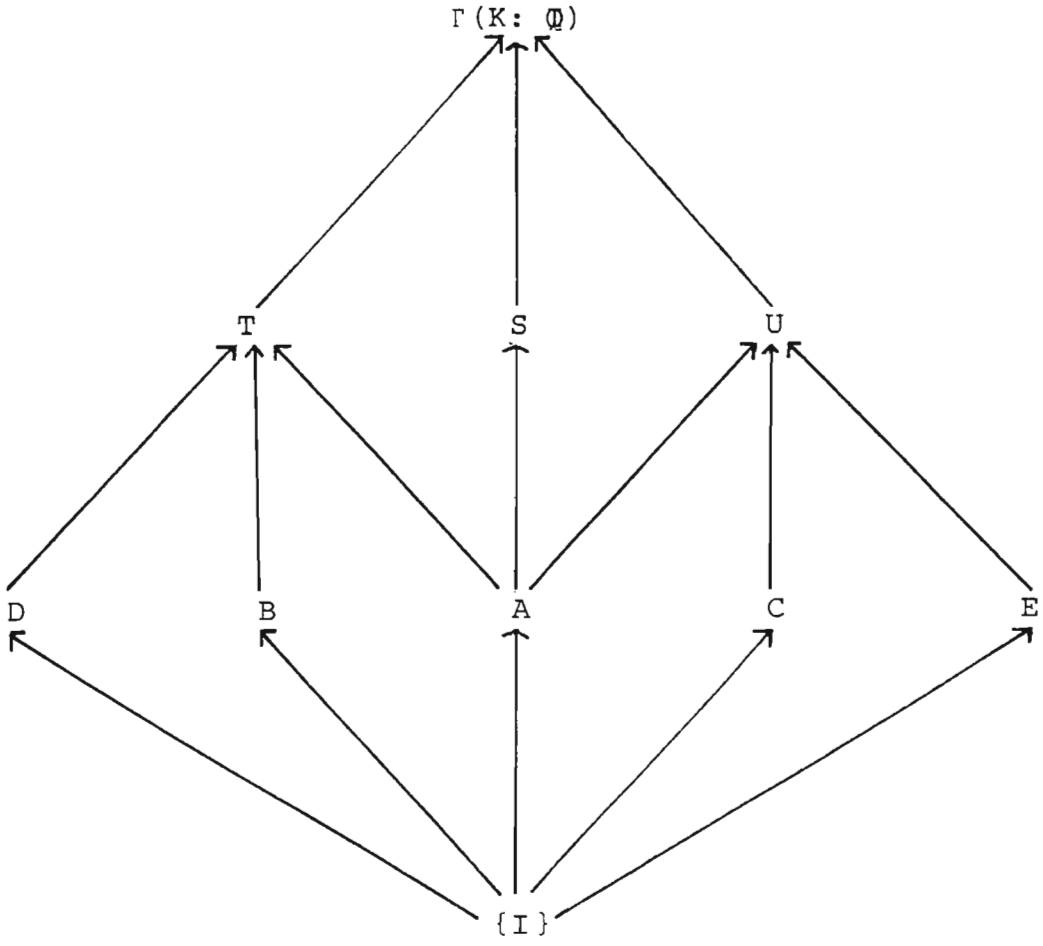
$C = \{I, \sigma\tau\}$

$D = \{I, \sigma^2\tau\}$

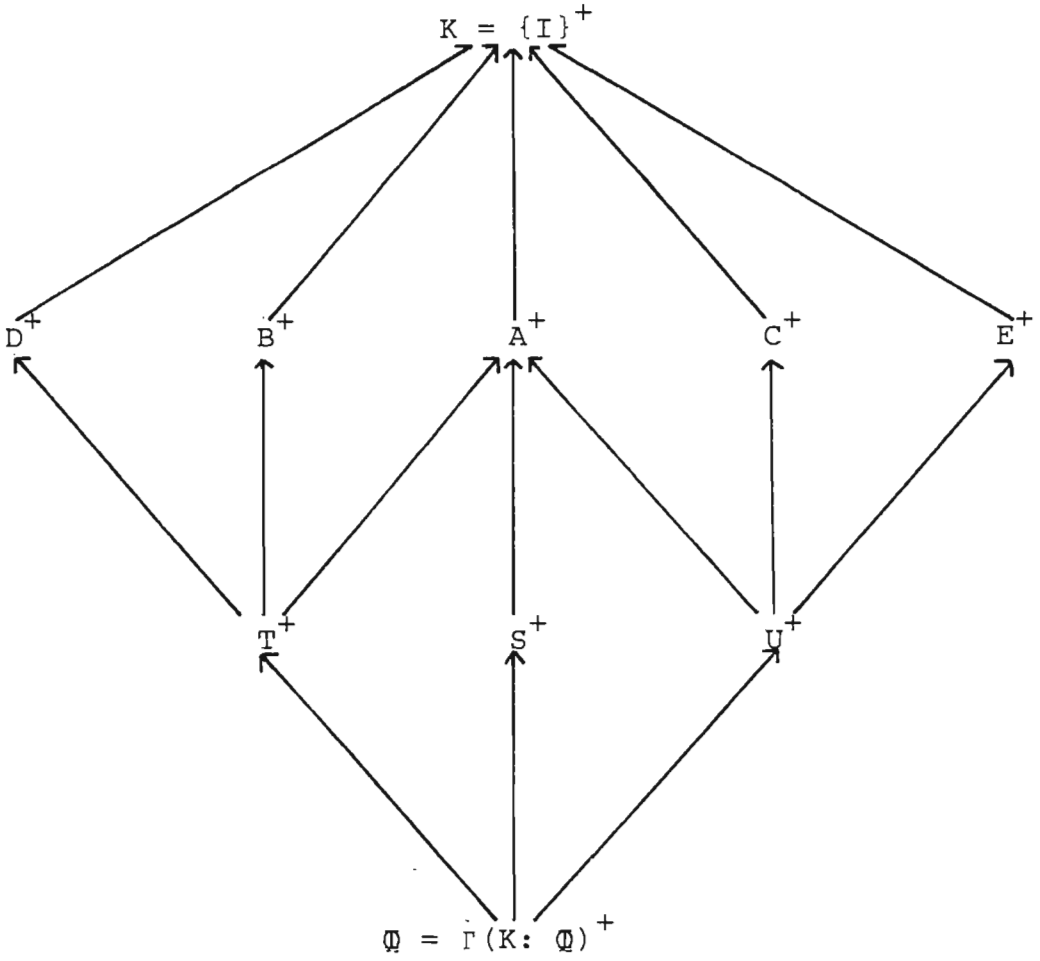
$E = \{I, \sigma^3\tau\}$.

Orden 1: $\{I\}$.

vi) Las relaciones de inclusión entre los subgrupos de $\Gamma(K: \mathbb{Q})$ están representados en el siguiente diagrama:



vii) Las relaciones de inclusión entre los campos intermedios de los subgrupos son:



viii) Ahora encontremos los campos fijos de los subgrupos del grupo de Galois.

De acuerdo a la parte 3) del teorema fundamental de Galois (1.5.1), hay únicamente tres subcampos de K de grado 2 sobre $\mathbb{Q}$.

Veamos que:

$$S^{+} = \mathbb{Q}(i),$$

$$T^+ = \mathbb{Q}(\sqrt{2}),$$

$$U^+ = \mathbb{Q}(i\sqrt{2}).$$

Ahora cualquier elemento de K puede ser expresado en la forma:

$x = a_0+a_1\xi+a_2\xi^2+a_3\xi^3+a_4 i+a_5 i\xi+a_6 i\xi^2+a_7 i\xi^3$, donde $a_0,a_1,\ldots,a_7 \in \mathbb{Q}$. Tomenos el elemento $\sigma\tau$ de C y apliquémoslo a x:

$$\alpha\tau(x) = a_0+a_1 i\xi-a_2\xi^2-a_3 i\xi^3-a_4 i+a_5(-i)i\xi-a_6 i(i\xi)^2-a_7 i(i\xi)^3.$$
$$= a_0+a_5\xi-a_2\xi^2-a_7\xi^3-a_4 i+a_1 i\xi+a_6 i.\xi^2-a_3 i\xi^3.$$

Luego, x es dejado fijo por $\sigma\tau$, si y sólo sí,

$a_0 = a_0$, $a_1 = a_5$, $a_2 = -a_2$, $a_3 = -a_7$, $a_4 = -a_4$, $a_5 = a_1$, $a_6 = a_6$, $a_7 = -a_3$. Por lo tanto, a_0 y a_6 son arbitrarios.
Reordenando x, tenemos:

$$x = a_0 + a_1(1+i)\xi + \frac{a_6}{2}\{(1+i)\xi\}^2 - \frac{a_3}{2}\{(1+i)\xi\}^3.$$

Además, el elemento $(i+i)\xi$ satisface al polinomio irreducible sobre $\mathbb{Q}$: $t^4 + 8$, lo cual significa que:

$$C^+ = \mathbb{Q}((1+i)\xi).$$

De igual forma obtenemos:

$$A^+ = \mathbb{Q}(i,\sqrt{2}),$$

$$B^+ = \mathbb{Q}(\xi),$$

$$D^+ = \mathbb{Q}(i\xi),$$

$$E^+ = \mathbb{Q}((1-i)\xi).$$

ix) Para obtener los subgrupos normales del grupo de Galois, utilizamos el siguiente resultado: "Si H es un subgrupo de G tal que H tiene sólo dos clases laterales derechas entonces H es normal en G. En el caso finito esto significa que el orden de H es la mitad del orden de G".

Aplicando este resultado vemos que S,T y U son subgrupos normales de $\Gamma(K:\mathbb{Q})$. También $A = S \cap T$ es normal, por ser intersección de dos subgrupos normales.

Es fácil verificar que para los subgrupos B,C,D y E no se cumple la condición de normalidad ($x^{-1}Nx \subset N$, $\forall x \in G$).

Luego, los subgrupos normales del grupo de Galois son:

$$\Gamma(K:\mathbb{Q}),\ S,T,U,A\ \ e\{I\}.$$

Por el teorema fundamental de Galois (1.5.1), se tiene que: $\mathbb{Q}$, S^+, T^+, U^+, A^+ y K serían las únicas extenciones normales de $\mathbb{Q}$ contenidas en K. En efecto estos son los campos de descomposición sobre $\mathbb{Q}$ para los polinomios: t, $t^2 + 1$, $t^2 - 2$, $t^2 + 2$, $t^4 - t^2 - 2$ y $t^4 - 2$ respectivamente. De otra manera $B^+:\mathbb{Q}$ no es normal, pues $t^4 - 4$ tiene un cero, ξ, en B^+ y no se descompone en B^+. De igual forma C^+, D^+ y E^+ no son extensiones normales de $\mathbb{Q}$.

x) De acuerdo a la parte 5) del teorema fundamental de Galois (1.5.1), el grupo de Galois de $A^+:\mathbb{Q}$ es isomorfo a

$$\frac{\Gamma(K:\mathbb{Q})}{A};$$

y por la parte 3) de 1.5.1, $|\Gamma(A^+:\mathbb{Q})| = 4$.

Calculando $\frac{\Gamma(K:\mathbb{Q})}{A}$, tenemos:

$$AI = \{1, \sigma^2\} = A\sigma^2$$

$$A\sigma = \{\sigma, \sigma^3\} = A\sigma^3$$

$$A\tau = \{\tau, \sigma^2\tau\} = A\sigma^2\tau$$

$$A\sigma^2\tau = \{\sigma\tau, \sigma^3\tau\} = A\sigma^3\tau \ ,$$

donde: $A\sigma$ y $A\tau$ son de orden 2. Luego:

$$\frac{\Gamma(K:\mathbb{Q})}{A} = \langle A\sigma, A\tau : A^2\sigma = A^2\tau = AI \rangle .$$

Ahora tenemos que $\frac{\Gamma(K:\mathbb{Q})}{A}$ es isomófico a $C_2 \times C_2$ (C_2 es el grupo cíclico de orden 2)

Calculemos el grupo de Galois de $A^+:\mathbb{Q}$, el cual tiene cuatro $\mathbb{Q}$-automorfismos:

	I	α	β	$\alpha\beta$
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
i	i	i	-i	-i

y como $\alpha^2 = \beta^2 = I$ y $\alpha\beta = \beta\alpha$, este grupo es isomorfo a $C_2 \times C_2$.

Luego

$$\Gamma(A^+:\mathbb{Q}) \approx \frac{\Gamma(K:\mathbb{Q})}{A} \ , \text{ como anteriormente.}$$

Para mostrar los isomorfismos entre $\frac{\Gamma(K:\mathbb{Q})}{A}$, $\Gamma(A^+:\mathbb{Q})$ y

($C_2 \times C_2$, se puede hacer uso del siguiente resultado: "si G es un grupo con dos subgrupos normales M y N tales que $M \cap N = \{e\}$ y $MN = G$, entonces $G \approx M \times N$".

2) Si $\xi = \frac{-1 + \sqrt{3}\, i}{2}$, 1.2.7 muestra que $K = \mathbb{Q}(\sqrt[3]{3}, \xi)$ es una extensión normal finita de grado 6. Además, la característica de K es cero, entonces K: $\mathbb{Q}$ es separable.

Por lo tanto K:$\mathbb{Q}$ es una extensión normal separable finita de grado 6, y por 1.5.1-1 $|\Gamma(K:\mathbb{Q})| = 6$.

Ahora encontremos $\Gamma(K:\mathbb{Q})$. Como ξ satisface al polinomio $t^2 + t + 1$, irreducible sobre $\mathbb{Q}(\sqrt[3]{3})$, una base de $\mathbb{Q}(\sqrt[3]{3}, \xi)$ sobre $\mathbb{Q}(\sqrt[3]{3})$ es $\{1, \xi\}$.

También una base de $\mathbb{Q}(\sqrt[3]{3})$ sobre $\mathbb{Q}$ es $\{1, \sqrt[3]{3}, (\sqrt[3]{3})^2\}$ (ver 1.2.7). Luego una base de K sobre $\mathbb{Q}$ es:

$$\{1,\ \sqrt[3]{3},\ (\sqrt[3]{3})^2,\ \xi,\ \sqrt[3]{3}\xi,\ (\sqrt[3]{3})^2\xi\}.$$

Como cualquier $\mathbb{Q}$-automorfismo está determinado por su efecto sobre la base, vemos que sólo es suficiente investigar los valores sobre $\sqrt[3]{3}$ y ξ.

Vemos que

$$\alpha(\sqrt[3]{3}) = \sqrt[3]{3},\ \sqrt[3]{3}\,\xi,\ \sqrt[3]{3}\,\xi^2 \quad \text{y}$$

$$\alpha(\xi) = \xi,\ \xi^2.$$

así,

$$\alpha_j^i(\sqrt[3]{3}) = \sqrt[3]{3}\,\xi^i$$

$$\alpha_j^i(\xi) = \xi^j \quad , \ i = 0,1,2 \ \text{ y } \ j = 1,2,$$

nos proporciona los seis $\mathbb{Q}$-automorfismos de K.

Además, $\alpha_1^1 \circ \alpha_2^2 \neq \alpha_2^2 \circ \alpha_1^1$.

Por lo tanto

$\Gamma(K:\mathbb{Q}) \approx S_3$, donde S_3 es el grupo simétrico y es el único grupo no abeliano de seis elementos.

3) Sea $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, 1.1.5-2 y 1.1.8-2, muestran que:

a) K:$\mathbb{Q}$ es una extensión normal separable finita.

b) Que la correspondencia de Galois es biyectiva.

c) $\Gamma(K:\mathbb{Q}) = \{I, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$.

d) Todos los subgrupos del grupo abeliano $\Gamma(K:\mathbb{Q})$ son normales.

e) Todos los campos intermedios son normales.

Si $M = \mathbb{Q}(\sqrt{3})$, M:$\mathbb{Q}$ es una extensión de grado 2. Luego por el teorema fundamental de Galois (1.5.1), hay dos $\mathbb{Q}$-autormorfismos de $\mathbb{Q}(\sqrt{3})$ y

$$\Gamma(M:\mathbb{Q}) \approx \frac{\Gamma(K:\mathbb{Q})}{|M^*|}, \text{ donde } M^* = \{I, \sigma_1\}$$

en efecto, calculando $\Gamma(M:\mathbb{Q})$ se obtiene que

$\Gamma(M:\mathbb{Q}) = \langle\alpha: \alpha^2 = I\rangle$, donde I es la identidad y $\alpha(\sqrt{3}) = -\sqrt{3}$.

Asi

$\Gamma(M:\mathbb{Q}) \approx C_2$, el grupo cíclico de orden 2.

Ahora calculemos $\frac{\Gamma(K:\mathbb{Q})}{|M^*|}$:

$$M^*I = \{I,\ \sigma_1\} = M^*\sigma_1$$

$$M^* = \{\sigma_2,\ \sigma_1\sigma_2\} = M^*\sigma_1\sigma_2$$

donde $(M^*\sigma_2)^2 = M^*\sigma_2^2 = M^*I$ y así:

$$\frac{\Gamma(K:\mathbb{Q})}{|M^*|} \approx C_2.$$

por lo tanto:

$$\frac{\Gamma(K:\mathbb{Q})}{|M^*|} \approx \Gamma(M:\mathbb{Q}).$$

C A P I T U L O I I

SOLUCION DE ECUACIONES POR RADICALES Y LA ECUACION POLINOMIAL GENERAL

2.1 ALGO DE TEORIA DE GRUPOS: GRUPOS SOLUBLES.

Para aplicar la correspondencia de Galois necesitamos tener a nuestra disposición ciertos conceptos y teoremas de teoría de grupos.

2.1.1 DEFINICION:

Un grupo G es soluble si tiene una serie finita de subgrupos

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

tal que:

i) $G_i \triangle G_{i+1}$ para $i = 0, \ldots, n-1$,

ii) $\frac{G_{i+1}}{G_i}$ es abeliano para $i = 0, \ldots, n-1$.

La notación $G_i \triangle G_{i+1}$ significa que G_i es un subgrupo normal de G_{i+1}. Observemos que la condición 1) no implica que $G_i \triangle G$, ya que $G_i \triangle G_{i+1} \triangle G_{i+2}$ no implica $G_i \triangle G_{i+2}$.

2.1.2 EJEMPLOS:

1) Sea G un grupo abeliano. La serie $\{e\} \subset G$ satisface la condición 1) de solubilidad, además $\frac{G}{\{e\}} \simeq G$ es abeliano. Luego todo grupo abeliano es soluble.

2) El grupo simétrico S_3 es soluble, pues la serie $\langle e\rangle \subset \langle (123)\rangle \subset S_3$ es tal que:

i) $\langle (123)\rangle \triangle S_3$, ya que $\langle (123)\rangle$ es un grupo de orden 3 (ver 1.6.1-ix).

ii) $\frac{\langle (123)\rangle}{\langle e\rangle} \simeq \mathbf{Z}_3$ es abeliano y,

$\frac{S_3}{\langle (123)\rangle} \simeq \mathbf{Z}_2$ es abeliano.

3) El diédrico D_8 de orden 8 es soluble.

Según el ejemplo 1.6.1.-v, S es un subgrupo normal de orden 4, pues S es de índice 2 en D_8; además S es cíclico. Por lo tanto $\frac{D_8}{S} \simeq \mathbf{Z}_2$ es abeliano.

Así, D_8 tiene la serie

$\{e\} \subset S \subset D_8$, que satisface las condiciones de solubilidad.

4) $G = \langle \sigma, \tau : \sigma^n = \tau^2 = e, \tau\sigma = \sigma^{-1}\tau\rangle$, el grupo diédrico de orden 2n, es soluble.

En efecto, la serie

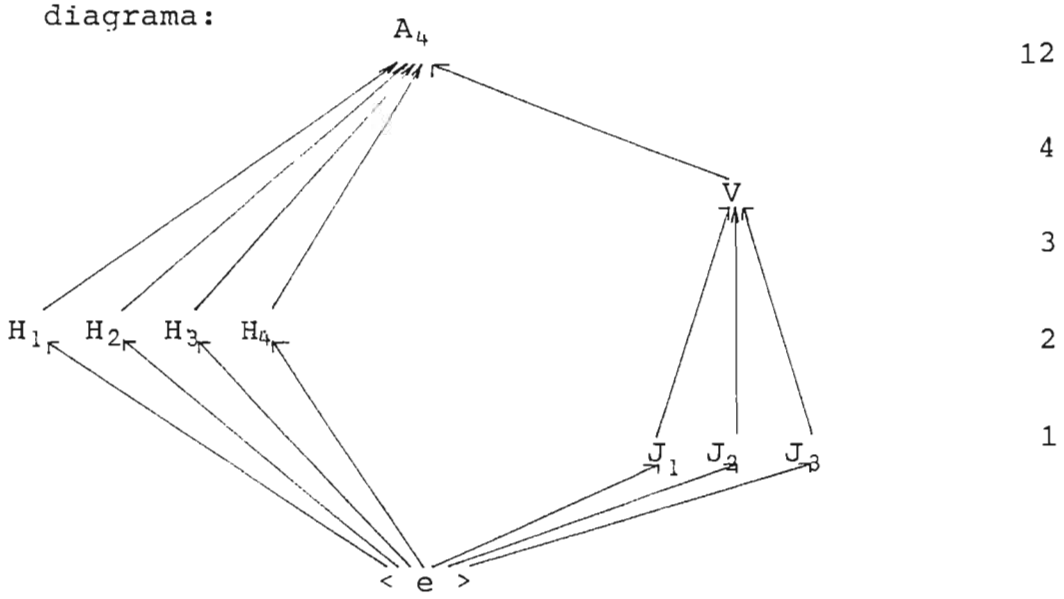
$\langle e\rangle \subset \langle \sigma\rangle \subset G$, satisface:

i) $\langle \sigma\rangle \triangle G$, pues $\langle \sigma\rangle \simeq \mathbf{Z}_n$ tiene índice dos en G.

ii) $\frac{G}{\langle\sigma\rangle} \simeq \mathbf{Z}_2$ es abeliano, y

$\frac{\langle\sigma\rangle}{\langle e\rangle} \simeq \frac{\mathbf{Z}_n}{\{0\}} \simeq \mathbf{Z}_n$ es abeliano también.

5) Sea A_4 el grupo alternante de orden 12. Veamos el siguiente diagrama:



Ya que V es el único subgrupo de orden 4, es normal en A_4.

$V = \{e, (12)(34), (13)(24), (14)(23)\} \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$ es abeliano.

Sea la serie $\langle e\rangle \subset V \subset A_4$. Como $\frac{A_4}{V} \simeq \mathbf{Z}_3$ es abeliano y,

$\frac{V}{\langle e\rangle} \simeq V$ también es abeliano, se sigue que A_4 es soluble.

6) El grupo simétrico, de orden 24, es soluble. En efecto, la serie $\langle e\rangle \subset V \subset A_4 \subset S_4$, satisface:

i) $V \triangle A_4$ y $A_4 \triangle S_4$

ii) $\frac{V}{\langle e\rangle} \simeq V$ es abeliano de orden 4,

$\frac{A_4}{V} \simeq \mathbf{Z}_3$ es abeliano de orden 3,

y

$$\frac{S_4}{A_4} \simeq \mathbf{Z}_2 \text{ es abeliano de orden 2.}$$

2.1.3 LEMA:

Sean G, H y A grupos.

1) Si $H \Delta G$ y $A \subset G$ entonces $H \cap A \Delta A$ y

$$\frac{A}{H \cap A} \simeq \frac{HA}{H}.$$

2) Si $H \Delta G$ y $H \subset A \Delta G$ entonces $H \Delta A$,

$$\frac{A}{H} \Delta \frac{G}{H}, \text{ y } \frac{\frac{G}{H}}{\frac{A}{H}} \simeq \frac{G}{A}$$

DEMOSTRACION:

1) Si $H \Delta G$, fácilmente se prueba que HA es un subgrupo de G.

Si $h \in H \cap A$ y $a \in A$, entonces $a^{-1}ha \in H$ ya que $H \Delta G$, y $a^{-1}ha \in A$ ya que $h \in A$. En consecuencia $a^{-1}ha \in H \cap A$, es decir, $a^{-1}(H \cap A)\, a \subset H \cap A$ para toda $a \in A$. Por lo tanto $H \cap A \Delta A$.

Sea $\phi: HA \longrightarrow \frac{A}{H \cap A}$ t.q $ha \rightsquigarrow (H \cap A)$. ϕ es un homomorfismo sobreyectivo y claramente $\ker \phi$ es H. Luego

$$\frac{HA}{H} \simeq \frac{A}{H \cap A}.$$ **Q.D.**

2) $H \Delta A$ sigue de 1) y que $\frac{A}{H} \Delta \frac{G}{H}$ se prueba fácilmente.

Sea $\phi: \frac{G}{H} \longrightarrow \frac{G}{A}$ t.q $Hg \rightsquigarrow Ag$.

Entonces ϕ es un homomorfismo sobreyectivo y claramente $\ker \phi = \frac{A}{H}$. Luego

$$\frac{\frac{G}{H}}{\frac{A}{H}} \approx \frac{G}{A} . \qquad \textbf{Q.D}$$

En la demostración anterior hemos hecho uso del siguiente resultado: "Si ϕ es un homomorfismo de un grupo G sobre un grupo $\bar{G}$, y $N = \ker \phi$, entonces $\frac{G}{N}$ es isomórfico a $\bar{G}$.

2.1.4 TEOREMA:

Sea G un grupo, H un subgrupo de G, y N un subgrupo normal de G.

1) Si G es soluble entonces H es soluble.
2) Si G es soluble entonces $\frac{G}{N}$ es soluble.
2) Si N y $\frac{G}{N}$ son solubles entonces G es soluble.

DEMOSTRACION:

1) Como G es soluble entonces existe una serie $\{e\} = G_0 \Delta G_1 \Delta \ldots \Delta G_r = G$, cuyos factores $\frac{G_{i+1}}{G_i}$ son abelianos.

Sea $H_i = G_i \cap H$, entonces H tiene la serie

$\{e\} = H_0 \subset H_1 \subset \ldots \subset H_r = H$. Ahora veamos que esta serie satisface las condiciones i), ii) de 2.1.1.

i) Tenemos que $G_{i+1} \cap H \subset G_{i+1}$ y $G_i \triangle G_{i+1}$, por 2.1.3-1 se tiene que:

$$G_i \cap (G_{i+1} \cap H) = G_i \cap H = H_i \triangle H_{i+1} = G_{i+1} \cap H.$$

ii) $$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \simeq \frac{G_i (G_{i+1} \cap H)}{G_i}$$

por 2.1.3-1. Ahora bien, $G_{i+1} \cap H \subset G_{i+1}$,

$G_i (G_{i+1} \cap H) \subset G_i G_{i+1}$ y

$$\frac{G_i (G_{i+1} \cap H)}{G_i} \subset \frac{G_i G_{i+1}}{G_i} = \frac{G_{i+1}}{G_i}.$$

Entonces $\frac{G_i (G_{i+1} \cap H)}{G_i}$ es subgrupo del grupo abeliano $\frac{G_{i+1}}{G_i}$. Luego $\frac{H_{i+1}}{H_i} \simeq \frac{G_i (G_{i+1} \cap H)}{G_i}$ es abeliano también.

Por lo tanto H es soluble. **Q.D.**

2) Definamos G_i como anteriormente tenemos que:

$N \triangle G_{i+1} N$ y $N \subset G_i N \triangle G_{i+1} N$, entonces por 2.1.3-2

$$\frac{G_i N}{N} \triangle \frac{G_{i+1} N}{N}$$

Luego $\frac{G}{N}$ tiene la serie:

$$\frac{N}{N} = \frac{G_0 N}{N} \triangle \frac{G_1 N}{N} \triangle \ldots \triangle \frac{G_r N}{N} = \frac{G}{N}$$

Además,

$$\frac{\frac{G_{i+1}N}{N}}{\frac{G_iN}{N}} \approx \frac{G_{i+1}N}{G_iN} = \frac{(G_{i+1}G_i)N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \approx \frac{G_{i+1}}{G_{i+1}\cap(G_iN)}, \text{ y}$$

$$\frac{G_{i+1}}{G_{i+1}\cap(G_iN)} \approx \frac{\frac{G_{i+1}}{G_i}}{\frac{G_{i+1}\cap(G_iN)}{G_i}}$$

Este último cociente es abeliano, pues

$\frac{G_{i+1}}{G_i}$ es abeliano.

Por lo tanto $\frac{G}{N}$ es soluble. **Q.D.**

3) Existen dos series

$$\{e\} = N_0 \triangle N_1 \triangle \ldots \triangle N_r = N,$$

$$\frac{N}{N} = \frac{G_0}{N} \triangle \frac{G_1}{N} \triangle \ldots \triangle \frac{G_s}{N} = \frac{G}{N},$$

con cocientes abelianos.

Consideremos la serie de G dada por

$$\{e\} = N_0 \triangle N_1 \triangle \ldots \triangle N_r = N = G_0 \triangle G_1 \triangle \ldots \triangle G_s = G$$

Los cocientes son $\frac{N_{i+1}}{N_i}$ (que son abelianos) ó $\frac{G_{i+1}}{G_i}$, los cuales son isomórficos a $\frac{\frac{G_{i+1}}{N}}{\frac{G_i}{N}}$ y que también son abelianos.

Luego G es soluble. **Q.D.**

Grupos Simples.

2.1.5 DEFINICION:

Un grupo G es simple si sus únicos subgrupos normales son {e} y G.

2.1.6 EJEMPLO:

Sea G un grupo cíclico de orden primo. Los únicos subgrupos de G son {e} y G, y por lo tanto no hay otros subgrupos normales diferentes de ellos. Estos grupos son también abelianos. Luego G es soluble y simple.

2.1.7 TEOREMA:

Un grupo soluble es simple si y sólo si es cíclico de orden primo.

DEMOSTRACION.

Supongamos que G es un grupo soluble simple que tiene una serie

$\{e\} = G_0 \Delta G_1 \Delta \ldots \Delta G_n = G$, en donde suponemos que $G_i \neq G_{i+1}$. Entonces G_{n-1} es un subgrupo normal porpio de G. Pero G es simple, así $G_{n-1} = \{e\}$ y $G \approx \frac{G_n}{G_{n-1}}$ el cual es abeliano.

Ya que todo subgrupo de un grupo abeliano es normal, y como todo elemento de G genera un subgrupo ciclico, G debe ser cíclico sin subgrupos propios no triviales. De aquí G debe tener orden primo.

Para el recíproco ver 2.1.6. **Q.D.**

2.1.8 TEOREMA:

Si $n \geq 5$ entonces el grupo alternante A_n de grado n es simple.

DEMOSTRACION:

Supongamos que $\{e\} \neq N \triangle A_n$. Nuestra estrategia será como sigue: primero, observese que si N contiene un 3-ciclo entonces contiene todos los 3-ciclos, y ya que los 3-ciclos generan A_n, debe tenerse que $N = A_n$. Segundo, probaremos que N contiene un 3-ciclo (es aquí donde necesitamos que $n \geq 5$).

Supongamos que N contiene un 3-ciclo; sin perder generalidad N contiene (123). Ahora para cualquier $k > 3$ el ciclo (32k) es una permutación par, así que está en A_n, y por lo tanto

$(32k)^{-1}(123)(32k) = (1k2)$ está en N.

De aquí N contiene $(12k) = (1k2)^2$ para toda $k \geq 3$. Ahora el grupo simétrico es generado por todos los 2-ciclos de la

forma (1i) para i = 2, ..., n. Ya que A_n es el conjunto de productos de un número par de estos, entonces es generado por todos los elementos de la forma (1i)(1j) = (1 ij). Pero para $i \neq 2$ tenemos, (1 ij) = (12j)(12i)$(12j)^{-1}$ así que A_n es generado por todos los ciclos (12k), lo cual nos muestra que $N = A_n$.

Ahora probaremos que N debe contener al menos un 3-ciclo. Haremos esto analizando los casos siguientes:

CASO 1.

Supongamos que N contiene un elemento

$$x = abc..$$

donde a,b,c,... son ciclos disjuntos y

$$a = (a_1 a_2 ... a_m)\ (m \geq 4).$$

Sea $t = (a_1 a_2 a_3)$. Entonces N contiene $t^{-1}xt$. Ya que t conmuta con b,c, ... (ciclos disjuntos) se sigue que

$$\begin{aligned} t^{-1}xt &= t^{-1}(abc...)t \\ &= (t^{-1}at)bc... \\ &= z \end{aligned}$$

así que N contiene $zx^{-1} = (a_1 a_2 a_m)$, el cual es un 3-ciclo.

CASO 2.

Ahora supongamos que N contiene un elemento que contenga al menos dos 3-ciclos. Sin perder generalidad N contiene

$$x = (123)(456)y,$$

donde y es una permutación que deja fijos 1, 2, 3, 4, 5, 6. Sea t = (234). Entonces N contiene

$$(t^{-1}xt)x^{-1} = (12436).$$

Entonces por caso 1, N contiene un 3-ciclo.

CASO 3.

Si N contiene elementos no considerados por los casos anteriores, entonces todo elemento de N involucra ya sea sólo un 3-ciclo o es un producto de 2-ciclos disjuntos. La primera posibilidad puede ser tratada considerando

$$x = (123)p$$

donde p conmuta con x y $p^2 = 1$. Entonces N contiene

$$x^2 = (132)p^2$$
$$= (132),$$

el cual es un 3-ciclo.

CASO 4.

Supongamos que todo elemento de N es un producto de 2-ciclos disjuntos. Pero como $n \geq 5$ podemos suponer que N contiene

$$x = (12)(34)p$$

donde p deja fijo 1,2,3,4. Si tomamos t = (234) entonces N contiene

$$(t^{-1}xt)x^{-1} = (14)(23)$$

y si u = (145) N contiene

$$u^{-1}(t^{-1}xtx^{-1})u = (45)(23)$$

Así N contiene

$$(45)(23)(14)(23) = (145)$$

contradiciendo la suposición de que todo elemento de N es un producto de 2-ciclos disjuntos.

Por lo tanto A_n es simple si $n \geq 5$. **Q.D.**

2.1.9 COROLARIO:

El grupo S_n de grado n no es soluble si $n \geq 5$.

DEMOSTRACION:

Si S fuera soluble entonces A sería soluble por 2.1.4-1 y simple por 2.1.8, luego A seria de orden primo por 2.1.7. Pero $|A_n| = \frac{n!}{2}$ no es primo si $n \geq 5$. **Q.D.**

p-grupos.

Empezaremos por recordar varias ideas de teoría de grupos.

2.1.10 DEFINICION:

Los elementos a y b de un grupo son conjugados en G si existe $g \in G$ tal que:

$$a = g^{-1}b\,g.$$

El conjugado es una relación de equivalencia; las clases de equivalencia son las clases de conjugados de G.

Si las clases de conjugados de G son C_1, C_2, ..., C_r entonces uno de ellos, digamos C_1, contiene sólo el elemento identidad de G. Por lo tanto $|C_1| = 1$. Ya que las clases de conjugados forman una partición de G tenemos

$$|G| = 1 + |C_2| + \ldots + |C_r| \quad \ldots\ldots\ldots\ldots \quad (1)$$

la cual es la ecuación de clase para G.

2.1.11 DEFINICION:

Si G es un grupo y $x \in G$ entonces el centralizador $C_G(x)$ de x en G es el conjunto de todos los $g \in G$ para el cual $xg = gx$.

El conjunto $C_G(x)$ siempre es un subgrupo de G. Hay una relación importante entre centralizadores y clases de conjugados.

2.1.12 LEMA:

Si G es un grupo y $x \in G$ entonces el número de elementos en la clase de conjugado de x es el índice de $C_G(x)$ en G.

DEMOSTRACION:

La ecuación

$$g^{-1}xg = h^{-1}xh$$

se cumple si y sólo si

$$hg^{-1}x = xhg^{-1},$$

lo cual significa que

$$hg^{-1} \varepsilon C_G(x),$$

lo cual se cumple si y sólo si

$$C_G(x)h = C_G(x)g$$

es decir, h y g están en la misma clase de $C_G(x)$ en G. Luego el número de elementos en la clase de conjugado de x es el índice de $C_G(x)$ en G. **Q.D.**

2.1.13 COROLARIO:

El número de elementos en cualquier clase de conjugado de un grupo finito G divide al orden de G.

Ahora introducimos la clase de p-grupos.

2.1.14 DEFINICION:

Sea p un primo. Un grupo finito G es un p-grupo si su orden es una potencia de p.

Por ejemplo, el grupo diédrico D_8 es un 2-grupo. Si $n \geq 3$ el grupo simétrico S_n nunca es un p-grupo para cualquier primo p.

A fin de establecer una importante propiedad de p-grupos necesitamos otra definición.

2.1.15 DEFINICION:

El centro Z(G) de un grupo G es el conjunto de elementos $x \in G$ tales que $xg = gx$ para toda $g \in G$.

Por ejemplo, $Z(S_3) = \{e\}$, y si G es un grupo abeliano se tiene que $Z(G) = G$.

2.1.16 TEOREMA:

Si $G \neq \{e\}$ es un p-grupo finito entonces G tiene centro no trivial.

DEMOSTRACION:

La ecuación de clase (1) de G es
$p^n = |G| = 1 + |C_2| + \ldots + |C_r|$ y por 2.1.13 tenemos

$$|C_i| = p^{n_i}$$

para algún $n_i \geq 0$. Ahora p divide a p^n, así, al menos p-1 valores de n_i deben ser iguales a cero. Pero si x está en una clase de conjugado con sólo un elemento ($x \neq e$), por 2.1.12 se tiene que $C_G(x) = G$, y luego $g^{-1}xg = x$ para toda $g \in G$, es decir, $xg = gx$. De donde $x \in Z(G)$. Por lo tanto $Z(G) \neq \{e\}$.

Q.D.

2.1.17 LEMA:

Si G es un p-grupo finito de orden p^n, entonces G tiene una serie de subgrupos normales

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

tal que

$$|G_i| = p^i, \text{ para } i = 0,1,\ldots,n.$$

DEMOSTRACION:

Usaremos inducción sobre n. Si n = 0 todo es claro. Si no, sea $Z = Z(G) \neq \{e\}$ por 2.1.16. Ya que Z es un grupo abeliano de orden p^m tiene un elemento de orden p. El subgrupo ciclico K generado por tal elemento tiene orden p y es normal en G ya que $K \subset Z$.

Ahora $\frac{G}{K}$ es un p-grupo de orden p^{n-1}, y por la hipótesis inductiva existe una serie de subgrupos normales:

$$\frac{K}{K} = \frac{G_1}{K} \subset \ldots \subset \frac{G_n}{K} \quad \text{donde}$$

$\left|\frac{G_i}{K}\right| = p^{i-1}$. Pero entonces

$|G_i| = p^i$ y por 2.1.3 $\dfrac{\frac{G}{K}}{\frac{G_i}{K}} \approx \frac{G}{G_i}$

con lo cual $G_i \triangle G$. Si agregamos a la serie $G_0 = \{e\}$ se obtiene el resultado requerido. **Q.D.**

2.1.18 COROLARIO:

Todo p-grupo finito es soluble.

DEMOSTRACION:

Por la serie proporcionada por 2.1.17 se tiene que $G_i \Delta G_{i+1}$ y $\frac{G_{i+1}}{G_i}$ son de orden p, y como p es primo entonces ciclicos y abelianos. **Q.D.**

Los siguientes resultados serán utilizados para la solución de ecuaciones por radicales y para la prueba del teorema fundamental del álgebra. Sólo probaremos la parte 1 del teorema siguiente.

2.1.19 TEOREMA (Sylow).

Sea G un grupo finito de orden $p^{\alpha}.r$ donde p es primo y no divide a r. Entonces:

1) G posee al menos un subgrupo de orden p^{α},
2) Cualquier par de subgrupos de orden p^{α} son conjugados en G,
3) Cualquier p-subgrupo de G está contenido en uno de orden p^{α},
4) El número de subgrupos de G de orden p^{α} deja resíduo 1 al dividirlo por p.

2.1.20 DEFINICION:

Si G es un grupo finito de orden $p^{\alpha}r$ donde p es primo y no divide a r, entonces un p-subgrupo de Sylow de G es un subgrupo de orden p^{α}.

2.1.21 EJEMPLO:

Sea $G = S_3$, el grupo simétrico, que tiene orden $6 = 2.3$. Sabemos que G tiene tres subgrupos de orden 2, entonces hay tres 2-subgrupos de Sylow. También G tiene un subgrupo de orden 3 y por lo tanto un 3-subgrupo de Sylow.

El 2.1.19 nos dice que para grupos finitos los p-subgrupos de Sylow existen para todos los primos p, todos son conjugados, son p-subgrupos maximales de G, y suceden en un número limitado.

Para probar la parte 1 del teorema 2.1.19 necesitamos el siguiente resultado.

2.1.22 LEMA:

Si A es un grupo abeliano finito cuyo orden es divisible por un número primo p entonces A tiene un elemento de orden p.

DEMOSTRACION:

Usaremos inducción sobre $|A|$. Si $|A|$ es primo entonces A es cíclico y el resultado sigue inmediatamente. Ahora tomemos un subgrupo propio M de A, de orden m, maximal. Si p divide a m entonces se sigue el resultado por la hipótesis inductiva. Supongamos que p no divide a m. Sea $t \in A$ y $t \notin M$, y sea T el subgrupo cíclico generado por t. Entonces MT es un subgrupo de A, que contiene propiamente a M, así por la maximalidad de M se tiene que $A = MT$. Por 2.1.3.

$$|MT| = \frac{|M||T|}{|M \cap T|}$$

Así que p divide al orden r de T. Ya que T es cíclico el elemento $t^{\frac{r}{p}}$ tiene orden p. Luego el lema queda probado. **Q.D.**

DEMOSTRACION DE 2.1.19-1

Usaremos inducción sobre $|G|$. El teorema es evidentemente cierto para $|G| = 1$ ó 2. Sean $c_1, c_2, \ldots, c_s$ las clases de conjugadas de G, y sea $|c_i| = \ell_i$. La ecuación de clase de G es

$$p^{\alpha}r = \ell_1 + \ell_2 + \ldots + \ell_s.$$

Sea Z_i el centralizador de algún elemento $x_i \in C_i$, y sea $|Z_i| = n_i$. Por 2.1.12 tenemos

$$n_i = \frac{p^{\alpha}r}{\ell_i} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (*)$$

Supongamos primero que algún ℓ_i es mayor que 1 y no divisible por p. Entonces por $(*)$ $n_i < p^{\alpha}r$ y es divisible por p^{α}.

De aquí por inducción Z_i contiene un subgrupo de orden p^α. Por lo tanto podemos suponer que para toda i = 1, 2, ..., s se tiene que $\ell_i = 1$ ó p divide a ℓ_i. Sea $z = |Z(G)|$. Como en 2.1.16, z es el número de valores de i tal que $\ell_i = 1$. Así

$$p^\alpha r = z + kp \quad \text{para algún entero } k.$$

De aquí p divide a z, y G tiene un centro Z no trivial tal que p divide a $|Z|$. Por 2.1.22 Z tiene un elemento de orden p, el cual genera un subgrupo P de G de orden p. Ya que P c Z se sigue que P Δ G. Por inducción $\frac{G}{P}$ contiene un subgrupo $\frac{S}{P}$ de orde $p^{\alpha-1}$, de donde S es un subgrupo de G de orden p^α y el teorema está demostrado **Q.D.**

2.1.23 TEOREMA (Cauchy).

Si un primo p divide el orden de un grupo finito G entonces G tiene un elemento de orden p.

DEMOSTRACION:

Sea S un p-subgrupo de Sylow de G, asi que $S \neq \{e\}$. Por 2.1.17 S tiene un subgrupo normal de orden p. Luego cualquier elemento distinto de la identidad en S tiene orden p. **Q.D.**

2.1.24 EJEMPLO:

Sea $G = S_4$, $|G| = 24$. De acuerdo a 2.1.19 (teorema de Sylow) G debe tener subgrupos de orden 3 y 8. Los subgrupos de

orden 3 son fáciles de encontrar: cualquier ciclo de longitud 3, tales como (123) ó (134) ó (124), generan tales grupos. En contraremos un subgrupo de orden 8. Sea V el grupo cuatro, el cual es normal en G (ver 2.1.2-6). Sea t cualquier ciclo de longitud 2, el cual genera un subgrupo T de orden 2. Entonces $V \cap T = \{e\}$, y VT es un subgrupo de orden 8.

2.2 SOLUCION DE ECUACIONES POR RADICALES.

El objetivo de esta sección es usar la correspondencia de Galois para dar una condición que debe ser satisfecha por una ecuación soluble por radicales, a saber: el grupo de Galois asociado debe ser un grupo soluble. También veremos que la solubilidad del grupo de Galois es una condición suficiente para que una ecuación sea soluble por radicales.

EXTENSIONES RADICALES

2.2.1 DEFINICION:

Una extensión L:K es radical si $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ en donde para cada $i = 1,2,\ldots,m$ existe un entero $n(i)$ tal que

$$\alpha_i^{n(i)} \in K(\alpha_1, \ldots, \alpha_{i-1}).$$

Los elementos α_i se dice que forman una sucesión radical para L:K.

2.2.2 DEFINICION:

Sea f un polinomio sobre un campo K de característica cero, y sea Σ un campo de descomposición para f sobre K. Decimos que f es soluble por radicales si existe un campo M que contiene a Σ tal que M:K es una extensión radical.

2.2.3 EJEMPLOS:

1) $\mathbb{Q}(\alpha, \beta, \gamma, \delta, \xi):\mathbb{Q}$ es una extensión radical, donde

$$\alpha^3 = 11,\ \beta^2 = 3,\ \gamma^5 = \frac{7+\beta}{2},\ \delta^3 = 4,\ \xi^4 = 1+\delta.$$

2) $\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}$ es una extensión radical.

3) Si $f(x) = x^3 + 3x - 2$ es un polinomio sobre $\mathbb{Q}$, entonces sus raices son:

$$\alpha_1 = \sqrt[3]{1+\sqrt{2}} + \sqrt[3]{1-\sqrt{2}}$$

$$\alpha_2 = w\sqrt[3]{1+\sqrt{2}} + w^2\sqrt[3]{1-\sqrt{2}}$$

$$\alpha_3 = w^2\sqrt[3]{1+\sqrt{2}} + w\sqrt[3]{1-\sqrt{2}},$$

donde

$$w \neq 1,\ w^3 = 1.$$

luego,

el campo de descomposición para f sobre $\mathbb{Q}$ es $\Sigma = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Entonces $M = \mathbb{Q}(\sqrt{2}, \sqrt[3]{1+\sqrt{2}}, \sqrt[3]{1-\sqrt{2}}, w)$ es una extensión radical de $\mathbb{Q}$ tal que $\Sigma \subset M$. Por lo tanto, $f(x) = x^3 + 3x - 2$ es soluble

por radicales.

También $M' = \mathbb{Q}(w\sqrt{2}, \sqrt[3]{1+\sqrt{2}})$ es una extensión radical de $\mathbb{Q}$. En efecto M' es de la forma $\mathbb{Q}(w\sqrt{2}, \beta)$ con $\beta^3 \in \mathbb{Q}(w\sqrt{2})$, ya que, $\sqrt{2} = \frac{1}{2}(w\sqrt{2})^3 \in \mathbb{Q}(w\sqrt{2})$.

Observemos también

$$w = \frac{1}{4}(w\sqrt{2})^4 \quad y \quad \sqrt[3]{1-\sqrt{2}} = -\frac{1}{\sqrt[3]{1+\sqrt{2}}}$$

estan en M'. Luego $\Sigma \subset M'$.

Como puede observarse, M no necesariamente, es único.

Claramente 2.2.2 es equivalente a:

2.2.3 DEFINICION:

Sea f un polinomio sobre un campo K de característica cero, y sea Σ un campo de descomposición para f sobre K. Decimos que f es soluble sobre K si hay una sucesión finita de campos:

$K = K_0 \subset K_1 \subset \ldots \subset K_r$ y una sucesión finita de enteros $n_0, \ldots, n_{r-1}$ tales que

$K_{i+1} = K_i(\alpha_i)$ con $\alpha_i^{n_i} \in K_i$, y todas las raices de f estan en K_r, esto es, $\Sigma \subset K_r$.

La sucesión $K_0 \subset K_1 \subset \ldots \subset K_r$ es llamada una extensión de K_0 por radicales o extensión radical de K_0.

2.2.4 EJEMPLO:

Si $f(x) = x^4 - 10x^2 + 1$ un polinomio sobre $\mathbb{Q}$, entonces sus raices son:

$$\alpha_1 = \sqrt{5+\sqrt{24}} = \sqrt{2} + \sqrt{3}$$

$$\alpha_2 = \sqrt{5-\sqrt{24}} = \sqrt{3} - \sqrt{2}$$

$$\alpha_3 = -\alpha_1 \quad y \quad \alpha_4 = -\alpha_2$$

Así, el campo de descomposición para f es

$$\Sigma = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Entonces podemos formar las siguientes extensiones radicales:

1) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \Sigma$,

2) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \Sigma$,

3) $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(\sqrt{i}, \sqrt{3})$ y $\Sigma \subset \mathbb{Q}(\sqrt{i}, \sqrt{3})$.

Por que $\mathbb{Q}(\sqrt{i}) = \mathbb{Q}(i, \sqrt{2})$. En efecto

$$\sqrt{i} = (\cos\tfrac{\pi}{2} + i \operatorname{sen}\tfrac{\pi}{2})^{1/2} = \cos\tfrac{\pi}{4} + i \operatorname{sen}\tfrac{\pi}{4} = \frac{\sqrt{2}}{2} + i\,\frac{\sqrt{2}}{2}.$$

También $i\sqrt{i} = -\frac{\sqrt{2}}{2} + i\,\frac{\sqrt{2}}{2}$. Entonces $\sqrt{i} - i\sqrt{i} = \sqrt{2}$.

Obviamente $i = (\sqrt{i})^2$.

Por lo tanto, $\mathbb{Q}(\sqrt{2}, i) \subset \mathbb{Q}(\sqrt{i})$ y ya que $\sqrt{i} = \frac{\sqrt{2}}{2} + i\,\frac{\sqrt{2}}{2}$, vemos que $\mathbb{Q}(\sqrt{i}) \subset \mathbb{Q}(\sqrt{2}, i)$.

4) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{2})$ y

$\Sigma \subset \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{2})$.

5) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{6}, \sqrt{2}) = \Sigma$,

6) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{6}, \sqrt{2}) = \Sigma$,

7) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{6}, \sqrt{5+2\sqrt{6}}) = \Sigma$, ya que

$\mathbb{Q}(\sqrt{6}, \sqrt{5+2\sqrt{6}}) = \mathbb{Q}(\sqrt{5+2\sqrt{6}}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ y

$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. En efecto,

$\sqrt{6} = \frac{1}{2}(\sqrt{5+2\sqrt{6}})^2 - \frac{5}{2}$, y $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$

está en $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, y en consecuencia, también $\sqrt{6}$ y

$\sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2}$, $\sqrt{2}$ y $\sqrt{3}$.

Así $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, por que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el campo más pequeño que contiene a $\sqrt{2}$ y $\sqrt{3}$.

2.2.5 LEMA:

Supongamos que L:K es finita y M es cerradura normal de L:K. Entonces M es generada por subcampos $L_1, L_2, \ldots, L_s$ que contiene a K, tal que cada extensión L_i:K es isomórfica a L:K.

DEMOSTRACION:

Como L:K es finita se tiene que $L = K(\alpha_1, \ldots, \alpha_r)$ para elementos algebraicos $\alpha_1, \alpha_2, \cdots, \alpha_r$ sobre K. Sea m_i el polinomio mínimo de α_i sobre K, y sea N un campo de descomposición para $f = m_1.m_2 \ldots m_r$ sobre K, que contiene a L. Entonces N:K es normal y finita por 1.2.10. Supongamos que $L \subset P \subset N$ donde P:K es normal. Cada polinomio m_i tiene un cero $\alpha_i \in P$, así por nor

malidad f se descompone en P. Ya que N es un campo de descomposición para f tenemos que P = N. Así, N es una cerradura normal de L:K. También por 1.4.5, las extensiones M:K y N:K son isomórficas, así podemos suponer que M = N.

Ahora si β_i es cualquier cero de m_i se sigue que las extensiones

$$K(\alpha_1,\ldots,\alpha_i,\ldots,\alpha_r):K$$

$$K(\alpha_1,\ldots,\beta_i,\ldots,\alpha_r):K$$

son isomórficas. Pero β_i e i varían y, las últimas extensiones generan a M. **Q.D.**

2.2.6 LEMA:

Si L:K es una extensión radical y M es una cerradura normal de L:K entonces M:K es radical.

DEMOSTRACION:

M es generado por $L_1, L_2, \ldots, L_s$, según 2.2.5, y las extensiones L_i:K son todas isomórficas a L:K, son extensiones radicales. Por inducción es suficiente probar que si R es generado por R_1 y R_2 donde R_1:K y R_2:K son radicales, entonces R:K es radical.

Sean $R_1 = K(\alpha_1,\ldots,\alpha_m)$ y $R_2 = K(\beta_1,\beta_2,\ldots,\beta_n)$ donde los α_i y β_i son sucesiones radicales. Entonces la sucesión combinada $\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n$ es una sucesión radical, así que

$$K(\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n):K \text{ es radical.}$$

Pero esto es R:K es radical. **Q.D.**

2.2.7 LEMA:

Sea K un campo de característica cero y sea L un campo de descomposición para $t-1$ sobre K, donde p es primo. Entonces el grupo de Galois de L:K es abeliano.

DEMOSTRACION:

La derivada de $t^p - 1$ es $p\,t^{p-1}$, así el polinomio no tiene ceros múltiples en L.

Claramente sus ceros forman un grupo bajo la multiplicación; éste tiene orden p ya que los ceros son distintos; así es cíclico. Sea ξ un generador de este grupo. Entonces $L=K(\xi)$ de modo que cualquier K-automorfismo de L es determinado por su efecto ξ. Además, los K-automorfismos de L es determinado por su efecto sobre ξ. Además, los K-automorfismos permutan los ceros de $t^p - 1$. De aquí cualquier K-automorfismo de L es de la forma:

$$\alpha_j : \xi \longrightarrow \xi^j.$$

Pero entonces ambos $\alpha_i\alpha_j$ y $\alpha_j\alpha_i$ mandan ξ a ξ^{ij}, así el grupo de Galois es abeliano. **Q.D.**

2.2.8 LEMA:

Sea K un campo de característica cero en el cual t^n-1 se

descompone. Sea a ε K, y sea L un campo de descomposición para t^{η}-a sobre K. Entonces el grupo de Galois de L:K es abeliano.

DEMOSTRACION:

Sea α cualquier cero de t^{η}-a. Ya que t^{η}-1 se descompone en K, los ceros de t^{η}-a son $\xi\alpha, \xi^2\alpha, \ldots, \xi^{\eta}\alpha$ donde ξ es un cero de t^{η}-1 diferente de uno. Como L=K(α), cualquier K-automorfismo de L es determinado por su efecto sobre α. Dados dos K-automorfismos

$$\phi: \alpha \longrightarrow \xi\alpha,$$

$$\psi: \alpha \longrightarrow \eta\alpha,$$

donde ξ y η ε K entonces $\phi\psi(\alpha) = \xi\eta\alpha = \eta\xi\alpha = \psi\phi(\alpha)$. Luego el grupo de Galois es abeliano **Q.D.**

2.2.9 TEOREMA:

Si K es un campo de característica cero y K c L c M donde M:K es una extensión radical, entonces el grupo de Galois de L:K es un grupo soluble.

DEMOSTRACION:

1. Sea K_0 el campo fijo del grupo de Galois Γ(L:K). Supongamos que podríamos probar 2.2.9 reemplazando K por K_0. Ya que el grupo de Galois $\Gamma(L:K_0)$ es el mismo que Γ(L:K), por defini-

ción, y como M es claramente radical sobre K_0 ⊃ K podemos deducir 2.2.9. Por lo tanto, podemos reemplazar K por K_0. Pero por 1.4.12, $L:K_0$ es normal, pues, K_0 es el campo fijo de $\Gamma(L:K) = \Gamma(L:K_0)$. La conclusión de todo esto es que podemos asumir que L:K es normal.

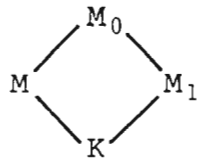
2. Si N es una clausura normal de M:K, entonces por 2.2.6 N:K es radical. Reemplazando M por N podemos asumir M:K es normal.

3. El grupo de Galois $\Gamma(L:K) \approx \frac{\Gamma(M:K)}{\Gamma(M:L)}$, por 1.5.1-5. Si probamos que $\Gamma(M:K)$ es soluble se sigue, por 2.1.4-2, $\Gamma(L:K)$ es soluble. Así podemos asumir que M = L.

4. Hemos reducido la prueba a considerar la situación siguiente: L:K es una extensión radical normal, la cual es separable por ser de característica cero. Deseamos mostrar que $\Gamma(L:K)$ es soluble.

   Supongamos que $M = K(\alpha_1,\ldots,\alpha_n)$ donde $\alpha_i^{n(i)} \in K(\alpha_1,\ldots,\alpha_{i-1})$. Adjuntando α_i adicionales, si es necesario, podemos asumir que n(i) es primo para todo i. En particular hay un primo p tal que $\alpha_i^p \in K$.

5. Ahora usemos inducción sobre n. Sea M_0 el campo de descomposición de t^p-1 sobre M, y sea M_1 el subcampo de M_0 generado por K y los ceros de t^p-1 en M_0.



ya que $\Gamma(M:K) \simeq \frac{\Gamma(M_0:K)}{\Gamma(M_0:M)}$, es suficiente probar que $\Gamma(M_0:K)$ es soluble. Además, M_1 es una extensión normal de K y $\Gamma(M_1:K)$ es abeliano por 2.2.7. Pero por 1.5.1-4,

$\Gamma(M_0:M_1) \Delta \Gamma(M_0:K)$, y por 1.5.1-5

$\Gamma(M_1:K) \simeq \frac{\Gamma(M_0:K)}{(M_0:M_1)}$.

Si podemos probar que $\Gamma(M_0:M_1)$ es soluble entonces, por 2.1.4-3, se sigue que $\Gamma(M_0:K)$ es soluble.

Sea $G = \Gamma(M_0:M_1)$. Entonces

$$M_0 = M_1(\alpha_1,\ldots,\alpha_n).$$

Sea $H = (M_1(\alpha_1))^*$, el subgrupo de G que corresponde a $M_1(\alpha_1)$ bajo la correspondencia de Galois.

Como t^p-1 se descompone en M_1, $M_1(\alpha_1)$ es un campo de descomposición para $t^p - \alpha_1^p$ sobre M_1. En consecuencia, $M_1(\alpha_1)$ es una extensión normal de M_1 y $\Gamma(M_1(\alpha_1):M_1)$ es abeliano (por 2.2.8). Además, por 1.5.1-4 $H \Delta G$. Y por 1.5.1-5,

$$\frac{G}{H} \simeq \Gamma(M_1(\alpha_1):M_1) \text{ que es soluble.}$$

Pero $M_0 = M_1(\alpha_1)(\alpha_2,\ldots,\alpha_n)$ y como

$M_0: M_1(\alpha_1)$ es normal, se sigue por inducción que

$\Gamma(M_0:M_1(\alpha_1))$ es soluble.

Es decir,

$\frac{G}{H}$ y H son solubles.

En consecuencia, por 2.1.4-3, G es soluble. **Q.D.**

La idea de esta prueba es simple: una extensión radical es una serie de extensiones por raices n-ésimas; tales extensiones tienen grupos de Galois abelianos; así el grupo de Galois de una extensión radical puede construirse "juntando" una sucesión de grupos abelianos. Desafortunadamente hay problemas tecnicos en realizar la prueba en ese sentido: necesitamos las raices de la unidad y tenemos que hacer varias extensiones normal antes de que la correspondencia de Galois pueda ser usada.

2.2.10 DEFINICION:

Sea f un polinomio sobre un campo K, con campo de descomposición Σ sobre K. El grupo de Galois de f sobre K es el grupo de Galois $\Gamma(\Sigma:K)$

Sea G el grupo de Galois de un polinomio f sobre el campo K. Si $\alpha \in \Sigma$ es un cero de f entonces $f(\alpha) = 0$; así para cualquier $g \in G$ tenemos $f(g(\alpha)) = g(f(\alpha)) = 0$. De aquí cada elemento $g \in G$ induce una permutación g' del conjunto de ceros de f en Σ. Elementos distintos de G inducen, permutaciones diferentes, ya que Σ es generado por los ceros de f. Se sigue fácilmente que el mapeo $g \longrightarrow g'$ es un monomorfismo de G en el grupo de todas las permutaciones de los ceros de f. En otras palabras, podemos ver en G un grupo de permutaciones sobre los ce-

ros de f.

Ahora podemos reescribir 2.2.9 de la siguiente manera:

2.2.11 TEOREMA:

Sea f un polinomio sobre un campo K de característica cero. Si f es soluble por radicales entonces el grupo de Galois de f sobre K es un grupo soluble.

DEMOSTRACION.

Ver 2.2.2 y 2.2.9 con L = Σ.

Un polinomio de quinto grado insoluble.

2.2.12 TEOREMA: Para cualquier n el grupo simétrico S_n es generado por los ciclos (12...n) y (12).

DEMOSTRACION:

Sea c = (12...n) t = (12), y sea G el grupo generado por c y t. Entonces G contiene $c^{-1}tc$ = (23); de esto $c^{-1}(23)c$=(34), ... y de aquí o también a todas las transformaciones (m,m+1). Entonces G contiene (12)(23)(12) = (13), (13)(34)(13) = (14), ..., y por lo tanto G contiene todas las transposiciones (1m). Pero entonces G contiene (1m)(1r)(1m) = (mr), y como todo elemento de S_n es un producto de transposiciones, se debe tener que G = S_n. **Q.D.**

2.2.14 LEMA:

Sea p un número primo, y f un polinomio irreducible de grado p sobre $\mathbb{Q}$. Supongamos que f tiene precisamente dos ceros no reales en $\mathbb{C}$. Entonces el grupo de Galois de f sobre $\mathbb{Q}$ es el grupo simétrico S_p.

DEMOSTRACION:

"Por el teorema fundamental del álgebra" $\mathbb{C}$ contiene un campo de descomposición Σ para f. Sea G el grupo de Galois de f sobre $\mathbb{Q}$, considerando como un grupo de permutaciones sobre los ceros f. Estos son distintos ya que la característica es cero, así G es un subgrupo de S_p. Cuando construimos un campo de descomposición para f, primero adjuntamos un elemento de grado p, así $[\Sigma: \mathbb{Q}]$ es divisible por p. Por 1.5.1-1, se tiene que p divide al orden de G. Por 2.1.23, G tiene un elemento de orden p. Pero los únicos elementos de S_p que tienen orden p son los p-cíclos.

La conjugación compleja es un $\mathbb{Q}$-automorfismo de $\mathbb{C}$, y por lo tanto induce un $\mathbb{Q}$-automorfismo de Σ. Estos dejan p-2 ceros reales de f fijos, mientras transponen los dos ceros no reales. Por lo tanto G contiene un 2-ciclo.

Por elección de notación, y si es preciso tomar una potencia del p-ciclo, podemos suponer que G contiene el 2-ciclo (12) y el p-ciclo (12...p) por 2.2.12, estos generan todo S_p.

Por lo tanto $G = S_p$.

2.2.14 TEOREMA:

El polinomio $t^5 - 6t + 3$ sobre $\mathbb{Q}$ no es soluble por radicales.

DEMOSTRACION:

Sea $f(t) = t^5 - 6t + 3$. Por el criterio de Eisensteis f es irreducible sobre $\mathbb{Q}$. Probaremos que f tiene precisamente 3 ceros reales, cada uno de multiplicidad 1, y de aquí tiene 2 ceros no reales. Ya que 5 es primo, por 2.2.13, el grupo de Galois de f sobre $\mathbb{Q}$ es S_5. Por 2.1.9 S_5 no es soluble. Luego, por 2.2.11, f no es soluble por radicales.

Falta demostrar que f tiene exactamente 3 ceros reales de multiplicidad uno. Como $f(-2) = -17$, $f(-1) = 8$, $f(0) = 3$, $f(1) = -2$ y $f(2) = 23$, parece ser que f tiene solamente 3 ceros reales. En efecto, por el teorema de Rolle los ceros de f estan determinados por los ceros de Df, y $Df = 5t^4 - 6$, el cual tiene 2 ceros $\pm \sqrt[4]{\frac{6}{5}}$. Ahora bien, f y Df son primos entre sí; así f no tiene ceros repetidos (esto también sigue de la irreducibilidad y característica cero) f tiene a lo sumo 3 ceros reales. Pero seguramente f tiene al menos 3 ceros reales, ya que una función continua definida sobre la recta real no puede cambiar de signo excepto que pase a través de un cero.

Por lo tanto f tiene precisamente 3 ceros reales, y el resulta do sigue. **Q.D.**

2.3 ECUACION POLINOMIAL DE GRADO N.

El objetivo de esta sección es estudiar un polinomio muy especial llamado polinomio general; cuyos coeficientes no satisfacen ninguna relación algebraica. Veremos que su grupo de Galois es fácil de calcular, y para el polinomio general de grado n, este es S_n. En particular mostramos que el polinomio general de grado 5 no es soluble por radicales. Inmediatamente, también mostramos la solubilidad de las ecuaciones cuárticas, cúbicas, cuadráticas, a través de la estructura S_4, S_3 y S_2 respectivamente.

GRADO TRASCENDENTE.

2.3.1 DEFINICION:

Una extensión L:K es finitamente generada si $L = K(\alpha_1,\ldots,\alpha_n)$ donde n es finito.

Observemos que los α_i pueden ser algebraicos o trascendentales sobre K.

2.3.2 DEFINICION:

Si $t_1, \ldots, t_n$ son elementos trascendentales sobre un cam

po K, todos permaneciendo en alguna extensión L de K, entonces ellos son independientes si no hay un polinomio diferente de 0 sobre K (en n indeterminadas) tales que $P(t_1,\ldots,t_n) = 0$ en L.

2.3.3 EJEMPLOS:

1) Si t es trascendental sobre K y u es trascendental sobre K(t) entonces K(t,u) es una extensión de K finitamente generada y t,u son independientes.

2) Si t es trascendental sobre K, también lo es t + 1, pero t y t + 1 no son independientes. En efecto, si $P(x_1,x_2) = x_1 - x_2 + 1$, resulta que $P(t,t+1) = 0$.

2.3.4 LEMA:

Si L:K es finitamente generada entonces existe un campo intermedio M tal que:

1) $M = K(\alpha_1,\ldots,\alpha_r)$ donde los α_i son elementos trascendentales independientes sobre K.

2) L:M es una extensión finita.

DEMOSTRACION:

Sabemos que $L = K(\beta_1,\ldots,\beta_n)$. Si todos los β_i son algebraicos sobre K entonces L:K es finita y podemos tomar M = K.

De otra manera, algún β_i es trascendental sobre K. Llamaremos α_1. Si $L:K(\alpha_1)$ no es finita existe algún β_k trascendental sobre K. Llamémoslo α_2. Podemos continuar este proceso hasta que $M = K(\alpha_1,\ldots,\alpha_r)$ sea tal que L:M es finita. Por construcción los α_i son elementos trascendentales independientes sobre K.

Q.D.

El siguiente resultado nos dice que el entero r que da el número de elementos trascendentales idependientes sobre K no depende de la elección de M.

2.3.5 LEMA:

Con la notación de 2.3.4, si hay otro campo intermedio $N = K(\beta_1,\ldots,\beta_s)$ tal que $\beta_1,\ldots,\beta_s$ son elementos trascendentales independientes sobre K y L:N es finita, entonces r = s.

DEMOSTRACION:

Ya que $[L:M]$ es finita β_1 es algebraico sobre M, luego hay un polinomio tal que

$$p(\beta_1,\alpha_1,\ldots,\alpha_r) = 0.$$

Algún α_i, sin pérdida de generalidad α_1, realmente aparece en esta ecuación (de lo contrario β_1 seria algebraico sobre K). Entonces α_1 es algebraico sobre $K(\beta_1,\alpha_2,\ldots,\alpha_r)$ y $L:K(\beta_1,\alpha_2,\ldots,\alpha_r)$ es finita, ya que $[L:M] = [L:M(\beta_1)][M(\beta_1):M]$ es finita y

$[L:K(\beta_1,\alpha_2,\ldots,\alpha_r)] = [L:M(\beta_1)][M(\beta_1):K(\beta_1,\alpha_2,\ldots,\alpha_r)]$. Inductivamente podemos reemplazar sucesivamente α_i por β_i, a si que $L:K(\beta_1,\ldots,\beta_r)$ es finita. Si $s > r$, entonces B_{r+1} debe ser algebraico sobre $K(\beta_1,\ldots,\beta_r)$, lo que es una contradicción al hecho de que los β_i son independientes. Por lo tanto $s \leq r$. Similarmente $r \leq s$. **Q.D.**

Esto significa que el entero r esta bién definido.

2.3.6 TEOREMA: El entero r definido en 2.3.4 es el grado trascendente de L:K.

2.3.7 EJEMPLO:

Consideremos $K(t,\alpha,u):K$, donde t es trascendental sobre K, $\alpha^2 = t$, y u es trascendental sobre $K(t,\alpha)$. Entonces $M = K(t,u)$ donde t y u son elementos trascendentales independientes sobre K, y $K(t,u,\alpha)$: $M = M(\alpha):M$ es finita, ya que α es algebraico sobre M. Luego el grado trascendente es 2.

EL POLINOMIO GENERAL.

Sea K cualquier campo, y sean $t_1,\ldots,t_n$ elementos trascendentales independientes sobre K. El grupo simétrico S_n puede considerarse como un grupo de K-automorfismos de $K(t_1,\ldots,t_n)$ definiendo

$$\sigma(t_i) = t\sigma(i)$$

para toda $\sigma \in S_n$. Claramente elementos distintos de S_n establecen distintos K-automorfismos.

El campo fijo F de S_n contiene todos los polinomios simétricos en los ti, y en particular los polinomios simétricos elementales $s_r = s_r(t_1,\ldots,t_n)$. Dando $s_r(t_1,\ldots,t_n)$ es la suma de todos los posibles distintos productos, tomando r a la vez de los $t_1, t_2,\ldots, t_n$. Mostraremos que los s_r generan a F.

2.3.8 LEMA:

Si F es el campo fijo de S_n, considerado como un grupo de K-automorfismos de $K(t_1,t_2,\ldots,t_n)$, entonces $F = K(s_1,\ldots,s_n)$, donde $s_1,\ldots,s_n$ son los polinomios simétricos elementales.

DEMOSTRACION:

Primero probaremos que

$$[K(t_1,\ldots,t_n): K(s_1,\ldots,s_n)] \leq n!$$

por inducción sobre n. Consideremos la doble extensión

$$K(t_1,\ldots,t_n) \supset K(s_1,\ldots,s_n,t_n) \supset K(s_1,\ldots,s_n).$$

Si $f(t) = t^n - s_1t^{n-1} + \ldots + (-1)^n s_n, f(t_n) = 0$

así que $[K(s_1,s_2,\ldots,s_n,t_n): K(s_1,\ldots,s_n)] \leq n.$

Si $s'_1,s'_2,\ldots,s'_{n-1}$ son los polinomios simétricos elementales en $t_1,\ldots,t_{n-1}$, tenemos $s_j = t_n s'_{j-1} + s'_j$ y por lo tanto

$$K(s_1,\ldots,s_n,t_n) = K(t_n,s'_1,\ldots,s'_{n-1}).$$

Ahora por inducción

$[K(t_1,\ldots,t_n):K(s_1,\ldots,s_n,t_n)] = [K(t_n)(t_1,\ldots,t_{n-1}):K(t_n)(s_1',\ldots,s_{n-1}')]$,

$[K(t_1,\ldots,t_n): K(s_1,\ldots s_n,t_n)] \leq (n-1)!$.

Luego $[K(t_1,\ldots,t_n): K(s_1,s_2,\ldots,s_n)] \leq n!$.

Como $K(s_1,\ldots,s_n)$ está claramente contenida en el campo fijo F de s_n, y por 1.3.1,

$[K(t_1,\ldots,t_n): F] = |S_n| = n!$, así por lo anterior debe tenerse que $F = K(s_1,\ldots,s_n)$. **Q.D.**

2.3.9 COROLARIO:

Cada polinomio simétrico en $t_1,\ldots,t_n$ sobre K puede ser escrito como una expresión racional en $s_1,\ldots,s_n$.

DEMOSTRACION:

Los polinomios simétricos en $t_1,\ldots,t_n$ permanecen en el campo fijo $F = K(s_1,\ldots,s_n)$. **Q.D.**

2.3.10 LEMA:

Con la notación anterior $s_1,\ldots,s_n$ son elementos trascendentales independientes sobre K.

DEMOSTRACION:

$K(t_1,...,t_n)$ es una extensión finita de $K(s_1,...,s_n)$. Si r es el grado trascendente de $K(s_1,...,s_n)$ sobre K, entonces el grado trascendente de $K(t_1,...,t_n)$ sobre K es r = n, por 2.3.5. Por lo tanto los si son independientes, pues de otra manera, el grado trascendente $K(s_1,...,s_n)$: K sería menor que n.

Q.D.

2.3.11 DEFINICION:

Sea K un campo y sean $s_1,...,s_n$ elementos trascendentales independientes sobre K. El polinomio general de grado n "sobre" K es el polinomio

$$t^n - s_1t^{n-1} + s_2t^{n-2} - ... + (-1)^n s_n$$

sobre el campo $K(s_1,...,s_n)$.

2.3.12 TEOREMA:

Para cualquier campo K sea g el polinomio general de grado n "sobre" K y sea Σ el campo de descomposición para g sobre $K(s_1,...,s_n)$. Entonces los ceros $t_1,...,t_n$ de g en Σ son elementos trascentatales independientes sobre K, y el grupo de Galois de $\Sigma:K(s_1,...,s_n)$ es todo el grupo simétrico s_n.

DEMOSTRACION:

La extensión Σ: $K(s_1,...,s_n)$, por 1.2.10, es finita; así el grado trascendente de Σ:K es igual al grado trascendente de $K(s_1,...,s_n)$: K, llamémoslo n. Ya que $\Sigma = K(t_1,...,t_n)$ se sigue que los t_i son elementos trascendentales independientes sobre K, pues de lo contrario una relación algebraica entre ellos disminuíria el grado trascendente. Sean los si los polinomios simétricos elementales. Como, S_n actua como un grupo de automorfismos de $\Sigma = K(t_1,...,t_n)$, y por 2.3.8, su campo fijo es $K(s_1,...,s_n)$. Por 1.4.12, Σ:$K(s_1,...,s_n)$ es normal y separable (la normalidad también sigue de la definición de Σ) y por 1.3.1, su grado es $|s_n| = n!$. Entonces por 1.5.1-1 el grupo de Galois tiene orden n! y además contiene a s_n. Por lo tanto el grupo de Galois de Σ:$K(s_1,...,s_n)$ es S_n. **Q.D.**

De 2.2.11 y 2.1.9 deducimos:

2.3.13 TEOREMA:

Si K es un campo de característica cero y $n \geq 5$, entonces el polinomio general de grado n "sobre" K no es soluble por radicales.

Solución de ecuaciones cuárticas.

Cuando el polinomio general de grado n "sobre" K puede ser resuelto por radicales, es fácil de decucir una solución por radicales de un polinomio de grado n sobre K, sustituyendo.

Lo que nos dice 2.3.13 es que lo mejor que podemos esperar es una solución para el polinomio general de grado menor o igual a 4; encontraremos la solución analizando la estructura de S_n y el recíproco de 2.2.9 que probaremos ahora.

2.3.14 DEFINICION:

Sea L:K una extensión normal finita con grupo de Galois G. La norma de un elemento $a \in L$ es

$$N(a) = \tau_1(a).\tau_2(a)...\tau_n(a)$$

donde $\tau_1,...,\tau_n$ son los elementos de G.

Claramente N(a) está en el campo fijo de G, así si la extensión L:K también es separable, entonces $N(a) \in K$.

2.3.15 TEOREMA:

Sea L:K un extensión normal finita con grupo de Galois G cíclico generado por un elemento τ. Entonces $a \in L$ tiene $N(a) = 1$ si, y sólo si, $a = \frac{b}{\tau(b)}$ para algún $b \in L$, $b \neq 0$.

DEMOSTRACION:

Si $a = \frac{b}{\tau(b)}$, $b \neq 0$, entonces si $|G| = n$

tenemos

$$N(a) = a\tau(a).\tau^2(a)...\tau^{n-1}(a)$$

$$= \frac{b}{\tau(b)} \cdot \frac{\tau(b)}{\tau^2(b)} \cdot \frac{\tau^2(b)}{\tau^3(b)} \cdots \frac{\tau^{n-1}(b)}{\tau^n(b)} = 1 \text{ ya que}$$

$\tau^n = 1$.

Recíprocamente, supongamos que $N(a) = 1$. Sea $c \in L$ y definamos

$$d_0 = ac$$

$$d_1 = (a.\tau(a))\tau(c)$$

$$\vdots$$

$$d_i = (a.\tau(a)\ldots\tau^i(a))\tau^i(c)$$

para $0 \leq i \leq n-1$. Entonces

$$d_{n-1} = N(a)\tau^{n-1}(c) = \tau^{n-1}(c)$$

y $$d_{i+1} = a.\tau(d_i) \quad \text{si } 0 \leq i \leq n-2.$$

Definamos $b = d_0 + d_1 + \ldots + d_{n-1}$.

Elijamos c tal que $b \neq 0$. Supongamos lo contrario que $b = 0$ para todas las elecciones de c. Entonces para cualquier $c \in L$ tenemos

$$\lambda_0\tau^0(c) + \lambda_1\tau(c) + \ldots + \lambda_{n-1}\tau^{n-1}(c) = 0$$

donde $\lambda_i = a.\tau(a)\ldots\tau^i(a)$ pertenecen a L. Resultando que los distintos automorfismos τ^i son linealmente dependientes sobre L, lo que es contrario al hecho que cualquier conjunto de distintos monomorfismos $K \to L$ es linealmente independiente sobre L.

Por lo tanto podemos elegir c tal que $b \neq 0$.

Pero entonces

$$\tau(b) = \tau(d_0) + \ldots + \tau(d_{n-1})$$

$$= \frac{1}{a}(d_1 + \ldots + d_{n-1}) + t^n(c)$$

$$= \frac{1}{a}(d_0 + d_1 + \ldots + d_{n-1})$$

$$= \frac{b}{a} .$$

por lo tanto $a = \frac{b}{\tau(b)}$. **Q.D.**

2.3.17 TEOREMA:

Supongamos que L:K es una extensión normal separable finita con grupo de Galois G cíclico de orden primo p, generado por τ. Asumamos que la característica de K es cero o p, y que t^p-1 se descompone en K. Entonces $L = K(\alpha)$ donde α es un cero de un polinomio irreducible $t^p - a$ sobre K, para algún $a \varepsilon K$.

DEMOSTRACION:

Los p ceros de $t^p - 1$ forman un grupo de orden p, el cual debe ser cíclico, así los ceros de $t^p - 1$ son potencias de algún $\xi \varepsilon K$ donde $\xi^p = 1$. Pero entonces

$$N(\xi) = \xi.\xi \ldots\xi = 1$$

ya que $\xi \varepsilon K$ y así $\tau^i(\xi) = \xi$ para toda i. Por 2.3.15, tenemos

$$\xi = \frac{\alpha}{\tau(\alpha)} \quad \text{para algún } \alpha \varepsilon L.$$

De aquí se sigue que $\tau(\alpha) = \xi^{-1}\alpha$, $\tau^2(\alpha) = \xi^{-2}\alpha, \ldots$, y $a = \alpha^p$ es dejado fijo por G, y así está en K. Luego $K(\alpha)$ es el campo de descomposición para $t^p - a$ sobre K, y los K-automorfismos $1, \tau, \tau^2, \ldots, \tau^{n-1}$ mapean a α en elementos distintos, asi

ellos nos proporcionan p distintos K-automorfismos de $K(\alpha)$. Por 1.5.1-1 $[K(\alpha):K] \geq p$. Pero $[L:K] = |G| = p$, así $L = K(\alpha)$. Por lo tanto $t^p - a$ es el polinomio mínimo de α sobre K, y en consecuencia $t^p - a$ es irreducible sobre K. **Q.D.**

2.3.18 TEOREMA (recíproco de 2.2.9):

Sea K un campo de característica cero y sea L:K una extensión normal finita con grupo de Galosi soluble G. Entonces existe una extensión R de L tal que R:K es radical.

DEMOSTRACION:

Como la característica de K es cero todas las extensiones son separables. Usaremos inducción sobre G. El resultado es claro cuando $|G| = 1$. Si $|G| \neq 1$ tomemos un subgrupo normal propio H de G (el cual existe ya que G es un grupo finito). Entonces $\frac{G}{H}$ es simple (ya que H es maximal) y soluble por 2.1.4-2. Por 2.1.7 $\frac{G}{H}$ es cíclico de orden primo p.

Sea N el campo de descomposición de $t^p - 1$ sobre L. Entonces N:K es normal; pues, por 1.2.10 L es un campo de descomposición sobre K para algún polinomio f, así N es un campo de descomposición sobre K de $(t^p - 1).f$, y así N:K es normal por 1.2.10 otra vez. El grupo de Galois de N:L es abeliano por 2.2.7 y por 1.1.5-5 $\Gamma(L:K) \simeq \frac{\Gamma(N:K)}{\Gamma(N:L)}$.

Por 2.1.4-3 $\Gamma(N:K)$ es soluble. Sea M el subcampo de N generado por K y los ceros de $t^p - 1$. Entonces N:M es normal. Como M:K es claramente radical, y como L c N, el resultado seguirá si podemos encontrar una extensión R de N tal que R:M sea radical.

Afirmamos que el grupo de Galois de N:M es isomórfica a un subgrupo de G.

Si τ es un M-automorfismo de N, consderemos su restricción a L:τ/L. Ya que L:K es normal τ/L es un K-automorfismo de L, y en consecuencia tenemos un homomorfismo de grupos:

$$\phi: \Gamma(N:M) \longrightarrow \Gamma(L:K).$$

Si $\tau \in \ker(\phi)$, entonces τ fija todos los elementos de M y L, los cuales generan N. Por lo tanto $\tau = 1$, es decir, ϕ es un monomorfismo, y en consecuencia

$\Gamma(N:M)$ es isomórfico a un subgrupo J de $\Gamma(L:K)$.

Si $J = \phi(\Gamma(N:M))$ es un subgrupo propio de G, entonces por inducción hay una extensión R de N tal que R:M es radical.

La posibilidad que flata es si J = G. Entonces podemos encontrar un subgrupo $I \triangle \Gamma(N:M)$ de índice p, $I = \phi^{-1}(H)$. Sea p el campo fijo I^+. Entonces $[P:M] = p$ por 1.5.1-3, P:M es normal por 1.5.1-4, y $t^p - 1$ se descompone en M. Por 2.3.17, $P = M(\alpha)$ donde $\alpha^p = a \in M$. Pero N:P es una extensión normal con grupo de Galois soluble de orden menor que $|G|$, así por inducción existe una extensión R de N tal que R:P es radical.

Luego R:M es radical y en consecuencia R:K es radical.

Q.D.

2.3.19 TEOREMA:

Sobre un campo de característica cero un polinomio es soluble por radicales si, y sólo sí, su grupo de Galois es soluble.

DEMOSTRACION, ver 2.2.11 y 2.3.18.

2.3.20.

El polinomio general de grado n tiene a S_n como su grupo de Galois y sabemos que para $n \leq 4$, S_n es soluble (ver 2.1.2). Por lo tanto para un campo de característica cero el polinomio general de grado menor o igual a 4 puede ser resuelto por radicales.

Podemos usar la estructura del grupo simétrico para encontrar la solución por radicales.

1. Lineal

$$t - s_1.$$

fácilmente $t_1 = s_1$ es un cero.

2. Cuádratica

$$t^2 - s_1 t + s_2.$$

Sean t_1 y t_2 los ceros de la ecuación cuadrática. El gru-

po de Galois s_2 consiste del mapeo identidad y de un mapeo que intercambia t_1 y t_2. Luego

$$(t_1 - t_2)^2$$

está en el campo fijo de s_2, es decir, $(t_1 - t_2)^2 \varepsilon K(s_1,s_2)$. Calculando vemos que $(t_1 - t_2)^2 = s_1^2 - 4s_2$.

Entonces

$$t_1 - t_2 = \pm \sqrt{s_1^2 - 4s_2}$$

$$t_1 + t_2 = s_1,$$

y en consecuencia, tenemos la fórmula familiar

$$t_1,\ t_2 = \frac{s_1 \pm \sqrt{(s_1^2 - 4s_2)}}{2} .$$

3. Cúbica

$$t^3 - s_1t^2 + s_2t - s_3.$$

Sean t_1, t_2, t_3 sus ceros. El grupo de Galois s_3 tiene la serie normal.

$$\langle e \rangle \text{ c } A_3 = \langle (123) \rangle \text{ c } s_3$$ con cocientes abelianos (ver 2.1.2-2). Es decir el grupo de Galois s_3 es soluble.

Adjuntemos un elemento $\omega \neq 1$ tal que $\omega^3 = 1$, y consideremos

$$y = t_1 + \omega t_2 + \omega^2 t_3.$$

Los elementos de A_3 permutan t_1, t_2 y t_3 cíclicamente, y por lo tanto multiplican a y por una potencia de ω si $\sigma_1 = (123)$, $\sigma_1(y) = \omega(y)$. Enconsecuencia y^3 es dejado fijo por los elementos de A_3.

Similarmente si

$$z = t_1 + \omega^2 t_2 + \omega t_3,$$

entonces z^3 es dejado fijo por todos los elementos de A_3.

También cada permutación impar es s_3 intercambia y^3 y z^3 (si $\sigma_2 = (13)$, $\sigma_2(y) = t_3 + \omega t_2 + \omega^2 t_1 = \omega^2 z$). Así, que $y^3 + z^3 \wedge y^3 z^3$ son fijados por todo s_3, es decir, pertenecen a $K(s_1,s_2,s_3)$. Por lo tanto y^3 y z^3 son ceros de una ecuación cuadrática sobre $K(s_1,s_2,s_3)$ la cual puede ser resuelta como en la parte 2. Luego tomando raices cúbicas, conocemos $y \wedge z$.

Pero

$$s_1 = t_1 + t_2 + t_3 \quad ,$$
$$y = t_1 + \omega t_2 + \omega^2 t_3 \ ,$$
$$z = t_1 + \omega^2 t_2 + \omega t_3 \ ,$$

se sigue que $t_1 = \frac{1}{3}(s_1 + y + z)$

$$t_2 = \frac{1}{3}(s_1 + \omega^2 y + \omega z)$$

$$t_3 = \frac{1}{3}(s_1 + \omega y + \omega^2 z).$$

4. Cuárticas

$$t^4 - s_1 t^3 + s_2 t^2 - s_3 t + s_4.$$

sean t_1, t_2, t_3, t_4 sus ceros.

El grupo de Galois s_4 tiene una serie normal

$$\langle e \rangle \subset V \subset A_4 \subset S_4, \text{ donde}$$

$V = \{1, (12)(34), (13)(24), (14)(23)\}$

con cocientes abelianos (ver 2.1.2-6), es decir, s_n es soluble.

Consideremos las tres expresiones

$$y_1 = (t_1 + t_2)(t_3 + t_4)$$

$$y_2 = (t_1 + t_3)(t_2 + t_4)$$

$$y_3 = (t_1 + t_4)(t_2 + t_3).$$

Los elementos y_1, y_2, y_3 son permutados entre ellos por cualquier permutación de s_4; así que, todos los polinomios simétricos elementales en y_1, y_2, y_3 están en $K(s_1,s_2,s_3,s_4)$. Entonces y_1, y_2, y_3 son los ceros de cierta cúbica sobre $K(s_1, s_2, s_3, s_4)$ llamada la resolvente cúbica.

Como

$$t_1 + t_2 + t_3 + t_4 = s_1$$

podemos encontrar tres polinomios cuadráticos cuyos ceros son $t_1 + t_2$ y $t_3 + t_4$, $t_1 + t_3$ y $t_2 + t_4$, $t_1 + t_4$ y $t_2 + t_3$. Y de aquí es fácil encontrar t_1, t_2, t_3, t_4.

Establezcamos ahora fórmulas explícitas para las soluciones, cuya existencia se asegura en las partes 2 y 3.

3') Cúbica. Haciendo $u = t - \frac{1}{3}s_1$, el polinomio general de grado 3 toma la forma

$$u^3 + pu + q, \quad \text{donde}$$

$$p = s_2 - \frac{s_1^2}{3}, \quad q = \frac{s_1 s_2}{3} - s_1 - \frac{2}{27}s_1^3.$$

Si podemos encontrar los ceros de esta última ecuación entonces es fácil encontrar la solución, de la cúbica general. Siguiendo el procedimiento anterior para este polinomio tenemos explícitamente

$$y^3 + z^3 = -27q$$

$$y^3z^3 = -27p^3.$$

de las cuales se sigue y^3 y z^3 son los ceros del polinomio cuadrático

$$t^2 + 27qt - 27p^3.$$

calculando

$$y = 3\sqrt{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

$$z = 3\sqrt{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

por lo tanto:

$$u_1 = \frac{1}{3}(y+z)$$

$$u_2 = \frac{1}{3}(w^2y + wz),$$

$$u_3 = \frac{1}{3}(wy + w^2z).$$

4') Cuártica. Haciendo la transformación $u = t - \frac{1}{4}s_1$ la ecuación cuártica se reduce a la forma

$$t^4 + pt^2 + qt + r.$$

Siguiendo el procedimiento

$$y_1 + y_2 + y_3 = 2p$$

$$y_1y_2 + y_1y_3 + y_2y_3 = p^2 - 4r$$

$$y_1y_2y_3 = -q^2 .$$

Entonces la resolvente cúbica toma la forma

$t^3 - 2pt^2 + (p^2-4r)t + q^2$, cuyas raices son y_1, y_2, y_3.

Como en este caso: $t_1 + t_2 + t_3 + t_4 = 0$, $x^2 + y_1 = 0$, es

decir $x = \pm \sqrt{-y_1}$. Similarmente $y = \pm \sqrt{-y_2}$ y $z = \pm \sqrt{-y_3}$.

Luego

$$t_1 + t_2 = \sqrt{-y_1} \quad ,$$
$$t_3 + t_4 = -\sqrt{-y_1} \quad ,$$

$$t_1 + t_3 = \sqrt{-y_2} \quad ,$$
$$t_2 + t_4 = -\sqrt{-y_2} \quad ,$$

$$t_1 + t_4 = \sqrt{-y_3} \quad ,$$
$$t_2 + t_3 = -\sqrt{-y_3} \quad ,$$

donde se deduce que:

$$2t_1 = \sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3} \quad ,$$
$$2t_2 = \sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3} \quad ,$$
$$2t_3 = -\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3} \quad ,$$
$$2t_4 = -\sqrt{-y_1} - \sqrt{-y_2} + \sqrt{-y_3} \quad ,$$

donde las raíces cuadradas estan sujetas a $\sqrt{-y_1}.\sqrt{-y_2}.\sqrt{-y_3} = -q$.

C A P I T U L O I I I

CONSTRUCCIONES CON REGLA Y COMPAS

De acuerdo a Platón las únicas figuras geométricas "perfectas" son la línea recta y el círculo.

En la antigua Grecia esta creencia tuvo el efecto de restringir los instrumentos disponibles para llevar a cabo construcciones geométricas a dos: la regla y el compás.

Con sólo estos instrumentos es posible llevar a cabo un amplio rango de construcciones. Líneas pueden ser divididas en muchos segmentos iguales, los ángulos pueden ser bisectados, líneas paralelas trazadas. Dado cualquier polígono es posible construir un cuadrado de área igual, o dos veces el área, etc. Sin embargo, hay muchos conceptos geométricos que intuitivamente deberían ser constructibles, es para los cuales los instrumentos de regla y compas son inadecuados. Hay tres famosas construcciones que los griegos no pudieron llevar a cabo: la duplicación del cubo, la trisección del ángulo, y la cuadratura del círculo.

No es sorprendente que los griegos encontraran estas construcciones tan difíciles. Ello era imposible. Pero los griegos ni tuvieron los métodos para probar la imposibilidad ni las

sospechas que las soluciones no existian.

Con la maquinaria a nuestra disposición es relativamente simple dar una respuesta completa a los tres problemas. Usaremos geometría con coordenadas para expresarlos en términos algebraicos, y aplicar la teoría de extensiones de campo a los problemas algebraicos que aparezcan.

3.1.1 FORMULACION ALGEBRAICA.

Nuestro primer paso es formular la idea intuitiva de una construcción con regla y compás. Supongamos que nos damos un conjunto de puntos P_0 en el plano Eucliniano $\mathbb{R}^2$, y consideramos operaciones de las siguientes dos clases:

Operación 1 (Regla): A través de cualesquiera dos puntos de P_0 se traza una línea recta.

Operacion 2 (compás): Trazar un círculo, cuyo centro es un punto de P_0, y cuyo radio es igual a la distancia entre algún par de puntos en P_0.

3.1.2 DEFINICION.

Los puntos de intersección de cualesquiera dos círculos o líneas distintas, trazadas usando operaciones 1 ó 2, se dice que son constructibles en una etapa de P_0.

Un punto $r \in \mathbb{R}^2$ es constructible de P_0 si hay una suce-

sión finita

$$r_1, r_2, \ldots, r_n = r$$

de puntos de $\mathbb{R}^2$ tal que para cada $i = 1,2,\ldots,n$ el punto r_i es constructible en una etapa del conjunto

$$p_0 \cup \{r_1, r_2, \ldots, r_{i-1}\}$$

3.1.3 EJEMPLO:

Mostraremos como la construcción del punto medio de una línea puede ser realizada dentro de nuestra estructura formal. Supongamos que nos damos dos puntos $p_1, p_2 \in \mathbb{R}^2$ (fig. 1.).

Sea $p_0 = \{p_1, p_2\}$

1) Trazar la línea p_1p_2 (operación 1)
2) Trazar el círculo de centro p_1 y radio p_1p_2 (operación 2)
3) Trazar el círculo de centro p_2 y radio p_1p_2 (operación 2)
4) Sean r_1 y r_2 los puntos de intersección de estos círculos
5) Trazar la línea r_1r_2 (operación 1)
6) Sea r_3 la intersección de las líneas p_1p_2 y r_1r_2.

Entonces la sucesión r_1, r_2, r_3 define una construcción del punto medio de la línea p_1p_2.

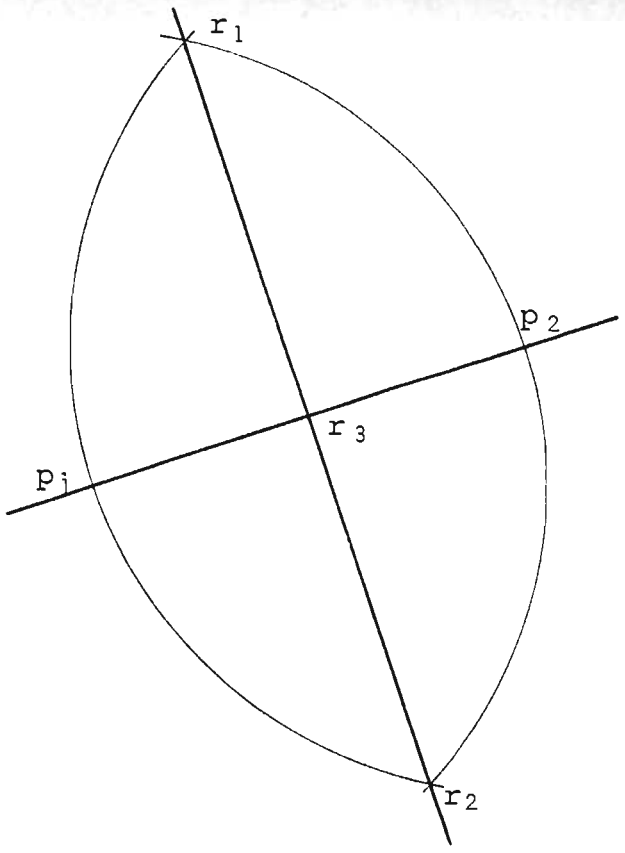


Fig. 1

Entraremos a la teoría de campo en una forma natural. En cada una de las etapas en la construcción asociaremos el subcampo de $\mathbb{R}$ generado por las coordenadas de los puntos construidos. Así sea K_0 es subcampo de $\mathbb{R}$ generado por las coordenadas x,y de los puntos en P_0. Si r_i tiene coordenadas (x_i,y_i) entonces inductivamente definimos K_i como el campo obtenido de K_{i-1} adjuntándole x_i, y_i, es decir,

$$K_i = K_{i-1}(x_i,y_i).$$

Claramente

$$K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{R}$$

3.1.4 LEMA:

Con la notación anterior x_i ^ y_i son ceros en K_i de polinomios cuadráticos sobre K_{i-1}.

DEMOSTRACION

Hay tres casos a considerar; intersecciones de:

i) recta y recta,

ii) recta y círculo,

iii) círculo y círculo.

Cada caso es tratado con geometría con coordenadas; como un ejemplo haremos el caso "recta intersectada con círculo".

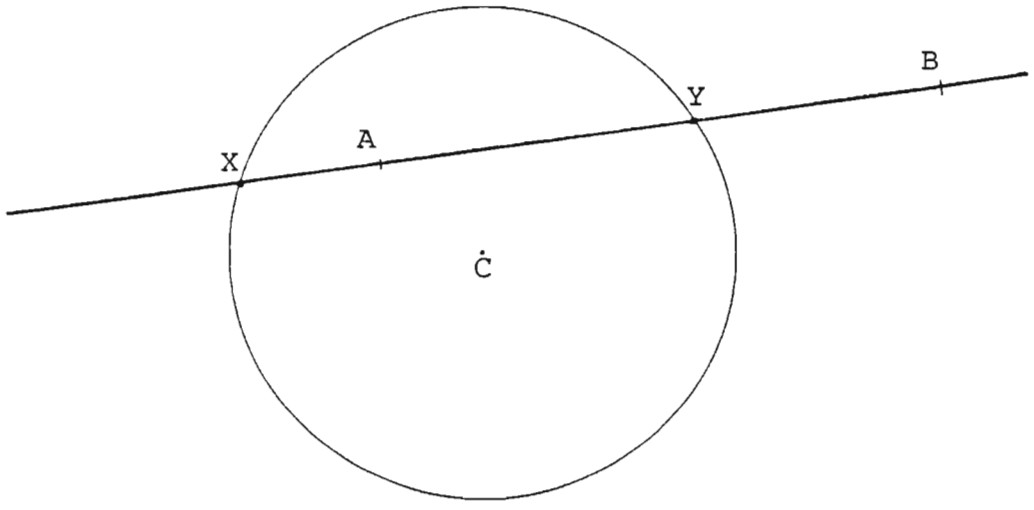


Fig. 2

Sean A, B, C puntos cuyas coordenadas (p,q), (r,s), (t,u) estan en K_{i-1}. Trazar la recta AB y el círculo de centro C, radio w, donde $w^2 \varepsilon K_{i-1}$, como en la figura 2, (observe que $w^2 \varepsilon K_{i-1}$, ya que w es la distancia entre dos puntos cuyas coordenadas están en K_{i-1}). La ecuación de la recta AB es

$$\frac{x - p}{r - p} = \frac{y - q}{s - q} \ldots \qquad (1)$$

y la ecuación del círculo es

$$(x-t)^2 + (y-u)^2 = w^2 \ldots \qquad (2)$$

así la coordenada x de los puntos de intersección X y Y son Resolviendo (1) y (2) obtenemos

$$(x-t)^2 + \left[\frac{(s-q)}{(r-p)} (x-p) + q-u\right]^2 = w^2$$

así la coordenada x de los x de los puntos de intersección X y Y son ceros de polinomios cuadráticos sobre K_{i-1}. Lo mismo se cumple para la coordena Y. **Q.D.**

3.1.5 TEOREMA:

Si r = (x,y) es constructible de un subconjunto P_0 de $\mathbb{R}^2$, y si K_0 es el subcampo de $\mathbb{R}$ generado por las coordenadas de los puntos de P_0, entonces los grados

$$[K_0(x): K_0] \quad y \quad [K_0(y): K_0]$$

son potencias de 2.

DEMOSTRACION:

Por 3.1.4 tenemos que

$$[K_{i-1}(x): K_{i-1}] = 1 \text{ o } 2, \text{ y}$$

$$[K_{i-1}(y): K_{i-1}] = 1 \text{ o } 2, \text{ (El valor de 2 ocurre}$$

si el polinomio cuadrático sobre K_{i-1} del cual x_i es un cero, es irreducible; de otro modo ocurre 1).

Por tanto

$$[K_{i-1}(x_i,y_i):K_{i-1}] = [K_{i-1}(x_i,y_i):K_{i-1}(x_i)][K_{i-1}(x_i):K_{i-1}]$$

$$= 1, 2, \text{ ó } 4.$$

De donde $[K_i: K_{i-1}]$ es una potencia de 2.

Por inducción vemos que $[K_n: K_0]$ es una potencia de 2. Pero

$$[K_n: K_0(x)][K_0(x): K_0] = [K_n: K_0].$$

Se sigue que $[K_0(x): K_0']$ es una potencia de 2. Similarmente $[K_0(y): K_0]$ es una potencia de 2. **Q.D.**

Pruebas de imposibilidad.

Ahora aplicamos la teoría anterior para pro-ar que no existen construcciones con regla y compás para los tres proble_ mas clásicos mencionados en la introducción de este capítulo.

.1.6 TEOREMA:

El cubo no puede ser duplicado mediante construcciones con regla y compás.

DEMOSTRACION:

Consideremos un cubo, y sea uno de sus lados el intervalo unidad sobre eje x. Por lo tanto, podemos suponer que $P_0 = \{(0,0),(1,0)\}$ es decir $K_0 = \mathbb{Q}$. Si pudieramos duplicar el cubo entonces podríamos construir el punto $(\alpha,0)$ donde $\alpha^3 = 2$. por 3.1.5 $[\mathbb{Q}(\alpha): \mathbb{Q}]$ sería una potencia de 2. Pero α es un cero del polinomio t^3-2 irreducible sobre $\mathbb{Q}$ (criterio de Eisensteín). Luego t^3-2 es el polinomio mínimo de α sobre $\mathbb{Q}$, y en consecuencia $[\mathbb{Q}(\alpha): \mathbb{Q}] = 3$. Esto es una contradicción. **Q.D.**

4.1.7 TEOREMA:

El ángulo $\frac{\pi}{3}$ no puede ser trisecado mediante construcciones con regla y compás.

DEMOSTRACION:

Para construir un ángulo trisecando $\frac{\pi}{3}$ es equivalente a construir el punto $(\alpha,0)$ dado $(0,0)$ y $(1,0)$, donde $\alpha = \cos(\frac{\pi}{9})$. (ver figura 3).

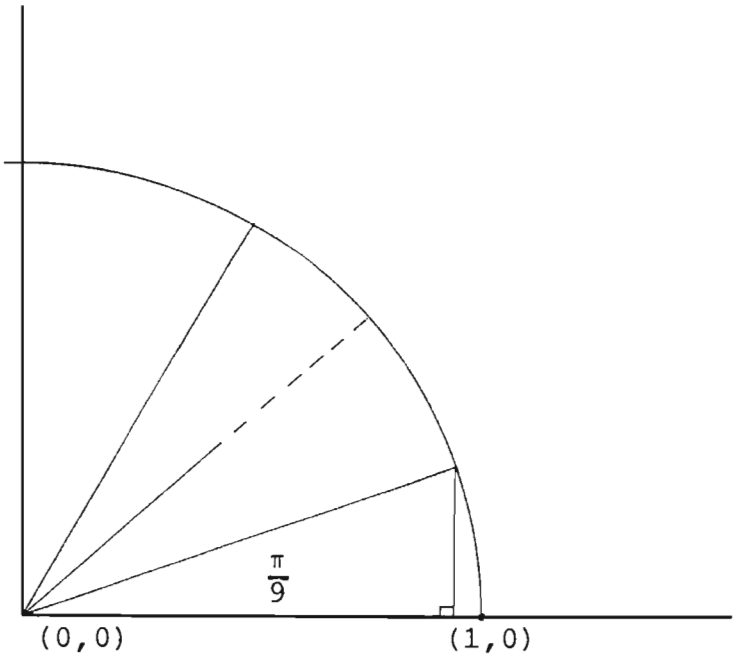


Fig. 3

De esto podríamos construir $(\beta,0)$, donde $\beta = 2\cos(\frac{\pi}{q})$.

Por trigonometría elemental,

$$\cos(3\theta) = 4(\cos^3(\theta) - 3\cos(\theta).$$

Si $\theta = \frac{\pi}{q}$, $\cos(3\theta) = \frac{1}{2}$, y encontramos que

$$\beta^3 - 3\beta - 1 = 0.$$

Ahora $f(t) = t^3-3t-1$ es irreducible sobre $\mathbb{Q}$, ya que $f(t+1) = t^3 + 3t^2 - 3$ es irreducible sobre $\mathbb{Q}$ (criterio de Eisensteín). Como en el teorema previo tenemos que $[\mathbb{Q}(\beta): \mathbb{Q}] = 3$, lo cual es una contradicción. **Q.D.**

4.1.8 TEOREMA:

El círculo no puede ser cuadrado mediante construcciones con regla y compás.

DEMOSTRACION:

Tal construcción es equivalente a una del punto $(0,\sqrt{\pi})$ de $\{(0,0), (1,0)\}$. De esto podemos fácilmente construir $(0,\pi)$. Así $[\mathbb{Q}(\pi): \mathbb{Q}]$ es una potencia de 2, y en particular π es algebraico sobre $\mathbb{Q}$. Por otro lado está el famoso teorema de Lindemann el cual asegura que π no es algebraico sobre $\mathbb{Q}$.

Q.D.

CAPITULO IV

CAMPOS FINITOS

En este capítulo daremos una clasificación completa de todos los campos finitos. Estableceremos que un campo finito está únicamente determinado por el número de elementos que contiene, salvo isomorfismo; que este número debe ser una potencia de un primo; y que para todo primo p y entero $n > 0$ existen un campo con p^n elementos.

Empezaremos por probar la segunda de estas tres afirmaciones.

4.1.1 TEOREMA:

Si F es un campo finito entonces F tiene característica p, donde p es primo, y el número de elementos en F es p^n donde n es el grado de F sobre su subcampo primo.

DEMOSTRACION:

Sea P el subcampo primo de F. P no es isomórfico a $\mathbb{Q}$, pues $\mathbb{Q}$ es infinito, así que P es isomórfico a $\mathbb{Z}_p$ para algún primo p, y por tanto F tiene característica P. F es un espacio

vectorial sobre P. Este espacio vectorial tiene un número finito de elementos, así que debe ser dimensión finita. De esto $[F: P] = n$ es finito. Sea $x_1,\ldots,x_n$ una base para F sobre P. Todo elemento de F es expresable en la forma única $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n$, donde $\lambda_1, \ldots, \lambda_n \in P$. Cada λ_i puede escogerse en p formas ya que $|P| = p$, por tanto, hay p^n de tales expresiones. Luego

$$|F| = p^n. \qquad \textbf{Q.D.}$$

Este resultado nos garantiza que no existen campos con 6, 10, 12, 14, 18, 20, ... elementos.

4.1.2 LEMA:

Sea K un campo de característica p, donde p es primo. Entonces el mapeo $\phi : K \longrightarrow K$ definido por $\phi(x) = x^p (x \in K)$ es un monomorfismo de campo. Si K es finito ϕ es un automorfismo.

DEMOSTRACION:

Sea $x,y \in K$. Entonces

$$\begin{aligned} \phi(xy) &= (xy)^p \\ &= x^p y^p \\ &= \phi(x).\phi(y). \end{aligned}$$

También

$$\begin{aligned} \phi(x+y) &= (x+y)^p \\ &= x^p + px^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \ldots + pxy^{p-1} + y^p. \end{aligned}$$

El coeficiente $\binom{p}{r}$ es divisible por p si $1 \leq r \leq p - 1$. Por tanto esta suma se reduce a $x^p + y^p$, es decir,

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

Luego ϕ es un homomorfismo. Pero $\phi(1) = 1 \neq 0$ así, que ϕ es un monomorfismo.

Si K es finito cualquier monomorfismo $K \to K$ es automáticamente sobreyectiva, es decir, ϕ es un automorfismo.

Q.D.

4.1.3 DEFINICION:

Si K es un campo de característica p, donde p es primo, entonces el mapeo $\phi: K \to K$ definido por $\phi(x) = x^p (x \in K)$ es el monomorfismo de Frobenius de K. Si K es finito es referido como el automorfismo de Frobenius.

4.1.4 TEOREMA:

Sea p cualquier número primo y n cualquier entero positivo. Un campo F tiene $q = p^n$ elementos si y sólo si es un campo de descomposición para $f(t) = t^q - t$ sobre el subcampo primo $P \approx \mathbf{Z}_p$ de F.

DEMOSTRACION:

Supongamos que $|F| = q$. Ahora el conjunto $F - \{0\}$ forma

un grupo bajo la multiplicación de orden q-1; así que si $0 \neq x \in F$ entonces $x^{q-1} = 1$.

Por tanto $x^q - x = 0$. Ya que $0^q - 0 = 0$. Todo elemento de F es un cero de $t^q - t$, y f(t) se descompone en F. Ya que los ceros de f agotan F ellos lo generaran, así F es un campo de descomposición para f sobre P.

Inversamente sea K un campo de descomposición para f sobre $\mathbb{Z}_p$. Ya que $D_f = -1$ es primo a f, todos los ceros de f en K son distintos, y en consecuencia f tiene exactamente q ceros. Supongamos que x ^ y son ceros de f. Entonces $\phi^n(x) = x^q$ donde ϕ es el monomorfismo de Frobenius. Por tanto ϕ^n es también un monomorfismo.

Entonces

$$\begin{aligned}(xy)^q - xy &= x^q y^q - xy \\ &= xy - xy \\ &= 0.\end{aligned}$$

$$\begin{aligned}(x+y)^q - (x+y) &= x^q + y^q - (x+y) \\ &= (x+y) - (x+y) \\ &= 0.\end{aligned}$$

$$\begin{aligned}(x^{-1})^q - x^{-1} &= x^{-q} - x^{-1} \\ &= x^{-1} - x^{-1} \\ &= 0.\end{aligned}$$

Es decir, el conjunto de ceros de f en K es un campo, el cual debe ser todo el campo de descompsición K. Luego

$$|K| = q.$$

Q.D.

4.1.5 TEOREMA:

Un campo finito debe tenr $q = p^n$ elementos donde p es un número primo y n es un entero positivo. Para cada una de tales q existe salvo isomorfismo precisamente un campo de descomposición para $t^q - t$ sobre $\mathbb{Z}_p$.

DEMOSTRACION. ver 4.1.4.

Notación: El campo con q elementos es escrito GF(q).

El grupo multiplicativo.

4.1.6 DEFINICION.

El exponente e(G) de un grupo finito es el mínimo común múltiplo de las órdenes de los elementos de G.

Evidentemente e(g) divide al orden de G. En general G no necesita poseer un elemento de orden e(G); por ejemplo si $G = S_3$ entonces e(G) = 6, pero G no tiene un elemento de orden 6. Sin embargo, los grupos abelianos tienen un mejor comportamiento al respecto:

4.1.7 LEMA:

Cualquier grupo abeliano finito G contiene un elemento de orden e(G).

DEMOSTRACION:

Sea $e = e(G) = p_1^{\alpha_1},\ldots,p_n^{\alpha_n}$ donde los números primos p_i son distintos y $\alpha_i \geq 1$. Entonces G debe poseer elementos g_i cuyos órdenes son divisibles por $p_i^{\alpha_i}$ de la definición de e(G). Entonces una potencia adecuada a_i de g_i tiene orden $p_i^{\alpha_i}$. Definamos

$$g = a_1.a_2\ldots a_n$$

supongamos $g^m = 1$ donde $m \geq 1$. Entonces

$$a_i^m = a_1^{-m}\ldots a_{i-1}^{-m} : a_{i+1}^{-m}\ldots a_n^{-m}.$$

Así, si $q = p_1^{\alpha_1}\ldots p_{i-1}^{\alpha_{i-1}}.p_{i+1}^{\alpha_{i+1}}\ldots p_n^{\alpha_n}$ entonces $a_i^{mq} = 1$. Pero q es primo con el orden de a_i, así $p_i^{\alpha_i}$ divide a m. Por tanto e divide a m. Pero claramente $g^e = 1$. Luego g tiene orden e.

Q.D.

4.1.8 COROLARIO:

Si G es un grupo abeliano finito tal que $e(G) = |G|$ entonces G es cíclico.

DEMOSTRACION:

El elemento g construido en el lema anterior genera G.

Q.D.

Podemos aplicar este corolario inmediatamente.

4.1.9 TEOREMA:

Si G es un subgrupo finito del grupo multiplicativo $K - \{0\}$ de un campo K, entonces G es cíclico.

DEMOSTRACION:

Ya que la multiplicación en K es conmutativa, G es un grupo abeliano. Sea $e = e(G)$. Entonces para cualquier $x \in G$, $x^e = 1$, así x es un cero del polinomio $t^e - 1$ sobre K. Este polinomio tiene al menos e ceros, así que $|G| \leq e$. Pero $e \leq |G|$, por tanto, $|G| = e$ y por 4.1.8 G es cíclico.

Q.D.

4.1.10 COROLARIO:

El grupo multiplicativo de un campo finito es cíclico.

Por lo tanto para cualquier campo finito F hay al menos un elemento x tal que todo elemento distinto de cero de F es una potencia de x. Daremos dos ejemplos.

4.1.11 EJEMPLOS:

1. El campo GF(11). Las potencias de 2, en orden, son

1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1

así que 2 genera el grupo multiplicativo. Las potencias de

4 son

1, 4, 5, 9, 3, 1

así que 4 no genera el grupo multiplicativo.

2. El campo GF(25). Este puede ser construido como un campo de descomposición para $t^2 - 2$ sobre $\mathbf{Z}_5$, ya que $t^2 - 2$ es irreducible y de grado 2.

Podemos por lo tanto representar los elementos de GF(25) en la forma $a + b\alpha$ donde $\alpha^2 = 2$. No hay error en escribir $\alpha = \sqrt{2}$. Considerando $2 + \sqrt{2}$, sus potencias sucesivas son:

$1,\ 2 + \sqrt{2},\ 1 + 4\sqrt{2},\ 4\sqrt{2},\ 3 + 3\sqrt{2},\ 2 + 4\sqrt{2}$

$2,\ 4 + 2\sqrt{2},\ 2 + 3\sqrt{2},\ 3\sqrt{2},\ 1 + \sqrt{2},\ 4 + 3\sqrt{2}$

$4,\ 3 + 4\sqrt{2},\ 4 + \sqrt{2},\ \sqrt{2},\ 2 + 2\sqrt{2},\ 3 + \sqrt{2},\ 3$

$1 + 3\sqrt{2},\ 3 + 2\sqrt{2},\ 2\sqrt{2},\ 4 + 4\sqrt{2},\ 1 + 2\sqrt{2},\ 1.$

Por tanto $2 + \sqrt{2}$ genera el grupo multiplicativo.

4.1.12. TEOREMA:

Si $|F| = p^n$, entonces F es una extensión normal de GF(p).

DEMOSTRACION:

Por 4.1.1, F tiene característica p, así GF(p) c F. Por 1.4.1, F es el campo de descomposición de un polinomio separable sobre GF(p) y así F debe ser una extensión normal.

Q.D.

4.1.13 TEOREMA:

Si F es finito de característica p, entonces $\Gamma(F: GF(p))$ es cíclico.

DEMOSTRACION:

Por 4.1.2, $\phi: F \to F$ t.q $\phi(x) = x^p$ es un automorfismo.

Sea $|F| = p^n$, así $[F: GF(p)] = n$, y sea g el generador del grupo cíclico $F^* = F - \{0\}$ bajo la multiplicación. Entonces los n elementos

$$g^p, g^{2p}, \ldots, g^{(n-1)p}, g^{np} = g \text{ son}$$

todos diferentes entre sí, y así los n automorfismos

$$\phi: g \to g^p$$
$$\phi^2: g \to g^{2p}$$
$$\vdots$$
$$\phi^n: g \to g^{np}$$

son todos diferentes. Por 1.5.1-1 sabemos que

$$n = [F: GF(p)] = \Gamma(F: GF(p)), \text{ así}$$

estos n automorfismos son los únicos posibles (observemos que por 4.1.12 es posible usar el teorema fundamental). Luego $\Gamma(F: GF(p))$ debe ser cíclico generado por ϕ, el automorfismo de Frobenius. **Q.D.**

4.1.4. TEOREMA:

El grupo $\Gamma(GF(p^{nk}): GF(p^n))$ es isomórfico al grupo cícli-

colo $C_k \approx \mathbf{Z}_k$.

DEMOSTRACION:

$GF(p^{nk})$ es una extensión normal de $GF(p)$, con característica p.

Sea $GF(p) \subset GF(p^n) \subset GF(p^{nk})$, y como $GF(p^n)$ es una extensión normal de $GF(p)$ (por 4.1.12) con

$\Gamma(GF(p^n): GF(p))$ cíclico de orden n, entonces, por 1.5.1, se tiene que:

$$\Gamma(GF(p^n): GF(p)) \approx \frac{\Gamma(GF(p^{nk}): GF(p))}{\Gamma(GF(o^{nk}): GF(p^n))} .$$

Además, $\Gamma(GF(p^{nk}): GF(p))$ es cíclico de orden nk.

Entonces, necesariamente

$$|\Gamma(GF(p^{nk}): GF(p^n))| = k$$

y en consecuencia

$$\Gamma(GF(p^{nk}): GF(p^n)) \approx C_k \qquad \text{Q.D.}$$

CAPITULO V

TEOREMA FUNDAMENTAL DEL ALGEBRA

Un campo es algebraicamente cerrado si todo polinomio se descompone sobre él. El resultado referido en el título de este capítulo establece que el campo de los números complejos es algebraicamente cerrado.

5.1.1 DEFINICION:

Un campo ordenado es un campo K con una relación $\leq$ tal que:

1) $x \leq x$ para toda $x \in K$

2) $x \leq y \wedge y \leq z$ implica que $x \leq z$ para toda $x,y,z \in K$.

3) $x \leq y \wedge y \leq x$ implica que $x = y$ para toda $x,y \in K$

4) Si $x,y \in K$ entonces $x \leq y$ ó $y \leq x$.

5) Si $x,y,z \in K$ y $x \leq y$ entonces $x + z \leq y + z$.

6) Si $x,y,z \in K$ y $x \leq y$, $0 \leq z$ entonces $xz \leq yz$.

La relación $\leq$ es un orden sobre K. Las relaciones $<$, $\geq$, $>$ son definidas en la forma obvia, así como los conceptos positivo y negativo.

Ejemplos de campo ordenados son $\mathbb{Q}$ y $\mathbb{R}$. Necesitaremos

dos consecuencias simples de la definición de un campo ordenado.

5.1.2 LEMA:

Sea K un campo ordenado. Para cualquier $x \in K$ tenemos $x^2 \geq 0$. La característica de K debe ser cero.

DEMOSTRACION:

Si $x \geq 0$ entonces $x^2 \geq$ por 6). Supongamos que $x < 0$. Si tuvieramos $-x < 0$, entonces

$0 = x + (-x) < x + 0 = x$, una contradicción. Así, $x \geq 0$, de donde $x^2 = (-x)^2 \geq 0$.

Por lo tanto $1 = 1^2 > 0$, y de esto para cualquier n finito:

$$n.1 = 1 + 1 + 1 + \ldots + 1 > 0,$$

de modo que $n.1 \neq 0$ y K debe tener característica cero.

Q.D.

5.1.3 LEMA:

$\mathbb{C}$ y A (el campo de los números algebraicos) no son campos ordenados.

DEMOSTRACION

En ambos casos tenemos un elemento $i = \sqrt{-1}$. Si los campos

fueran ordenados, $x^2 \geq 0$ por 5.1.2. Sin embargo, $i^2 = -1 \geq 0$, lo que es una contradicción con el hecho de que $1 > 0$. **Q.D.**

Citaremos las siguientes propiedades de $\mathbb{R}$.

5.1.4 LEMA:

$\mathbb{R}$, con el orden usual, es un campo ordenado. Todo elemento positivo de $\mathbb{R}$ tiene una raíz cuadrada en $\mathbb{R}$. Todo polinomio de grado impar sobre $\mathbb{R}$ tiene cero en $\mathbb{R}$.

5.1.5 LEMA:

Sea K un campo de característica cero, tal que para algún primo p toda extensión finita M:K con $M \neq K$ tiene $[M:K]$ divisible por p. Entonces toda extensión finita de K tiene grado una potencia de p.

DEMOSTRACION:

Sea N una extensión de K. La característica es cero. Entonces N:K es separable. Pasando a una cerradura normal, podemos suponer que N:K es también normal, así la correspondencia de Galois es biyectiva. Sea G el grupo de Galois de N:K, y sea P un p-subgrupo de Sylow de G. El campo fijo P^+ tiene grado $[P^+:K]$ igual a1 índice de P en G. (1.5.1-1), pero este es primo con p. Por hipótesis se tiene que $P^+ = K$ así que $P = G$. Entonces $[N:K] = |G| = p^n$ para algún n. **Q.D.**

5.1.6 TEOREMA:

Sea K un campo ordenado en el cual todo elemento positivo tiene una raíz cuadrada y todo polinomio de grado impar tiene un cero. Entonces K(i) es algebraicamente cerrado, donde $i^2 = -1$.

DEMOSTRACION:

K no puede tener extensiones finitas de grado impar mayor que 1.

Pero supongamos que $[M:K] = r > 1$ donde r es impar. Sea $\alpha \in M - K$ que tiene polinomio mínimo a m. Entonces el grado de m divide a r, así es impar. Por hipótesis m tiene un cero en K, asi es reducible, lo cual es una contradicción. Por tanto toda extensión finita de K tiene grado par sobre K. La característica de K es cero por 5.1.2, y por 5.1.5 toda extensión finita de K tiene grado una potencia de 2.

Sea $M \neq K(i)$ una extensión finita de K(i) donde $i^2 = -1$. Tomando una cerradura normal podemos suponer que M:K es normal, así el grupo de Galois de M:K es un 2-grupo. Usando 2.1.17 y 1.5.1 podemos encontrar una extensión N de K(i) de grado $[N:K(i)] = 2$. Por la fórmula para resolver ecuaciones cuadráticas, tenemos

$$N = K(i)(\alpha)$$

donde $\alpha^2 \in K(i)$. Pero si $a,b \in K$ tenemos

$$\sqrt{a + bi} = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$$

donde la raíz cuadrada de $a^2 + b^2$ es positiva, y los signos de las otras raíces cuadradas son escogidas de tal forma que su producto sea igual a b. Las raíces cuadradas existen en K ya que los elementos dentro de ellas son positivos.

Por lo tanto $\alpha \in K$, asi $N = K(i)$, lo cual contradice nuestra suposición sobre N. Luego $M = K(i)$ no tiene extensiones finitas de grado mayor que 1.

Por tanto, cualquier polinomio irreducible sobre K(i) tiene grado 1, pues de otra manera un campo de descomposición tendría grado finito mayor que 1 sobre K(i). Luego K(i) es algebraicamente cerrado. **Q.D.**

5.1.7 COROLARIO: (Teorema fundamental del Algebra).

El Campo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.

DEMOSTRACION:

Hagamos $K = \mathbb{R}$ y apliquemos 5.1.6 y 5.1.4. **Q.D.**

C A P I T U L O V I

EL TEOREMA DE RICHARD

6.1.1 TEOREMA: (Teorema de Richard)

Sea n un entero, sean $p_1,\ldots,p_k$ números primos distintos y $\sqrt[n]{a}$, a > 0, la raíz n-ésima real positiva. Entonces el campo $\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_k})$ es de grado n^k sobre $\mathbb{Q}$.

DEMOSTRACION:

Sea ξ = una raíz n-ésima primitiva de la unidad,

$R = \mathbb{Q}(\xi)$,

$\{\alpha_i\}$ el conjunto de los n^k elementos de la forma

$$p_1^{\frac{r_1}{n}},\ldots,\ p_k^{\frac{r_k}{n}} \quad (0 \leq r_i < n),$$

$\{\beta_i\}$, en el caso que n sea par, el conjunto de los $(\frac{n}{2})^k$ elementos de la forma

$$p_1^{\frac{r_1}{n}},\ldots,\ p_k^{\frac{r_k}{n}} \quad (0 \leq r_i < \tfrac{n}{2}),$$

$$S = \mathbb{Q}(p_1^{\frac{1}{2}},\ldots,\ p_k^{\frac{1}{2}}),$$

$$T = R(p_1^{\frac{1}{2}},\ldots,\ p_k^{\frac{1}{2}}).$$

El conjunto $\{\alpha_i\}$ claramente genera $\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_k})$ sobre

$\mathbb{Q}$, y el teorema es equivalente a la proposición de que los α_i son linealmente independientes sobre $\mathbb{Q}$. Ya que el teorema para cualquier múltiplo nn_i claramente implica el teorema para n, sin perder generalidad, podemos asumir que n es par. Probaremos que:

i) $[S: \mathbb{Q}] = 2^k$,

ii) $[R(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_k}):T] = (\frac{n}{2})^k$.

Ya que el conjunto $\{\beta_i\}$ genera $\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_k})$ sobre S, ii implica que

iii) $[\mathbb{Q}(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_k}): S] = (\frac{n}{2})^k$.

i, iii, implican nuestro teorema:

$[\mathbb{Q}(\sqrt[n]{p_1},..,\sqrt[n]{p_k}): \mathbb{Q}] = n^k$.

Pero antes unos lemas:

6.1.2 LEMA:

Sea F un campo de característica cero. Supóngase a ε F y que el polinomio $x^n - a$ se factoriza sobre F. Entonces hay un m/n, m > 1, una raíz n-ésima ξ de la unidad y un valor de $\sqrt[m]{a}$ tal que $\xi\sqrt[m]{a}$ ε F.

DEMOSTRACION:

Como $x^n - a = (x - \sqrt[n]{a})(x-\xi\sqrt[n]{a})\ldots(x-\xi^{n-1}\sqrt[n]{a})$. El término constante en cualquier factor de $x^n - a$ tiene la forma

$\pm \xi^c a^{\frac{r}{n}} \in F$ $(0 < r < n)$. Sea s = máximo común divisor de r,n y $m = \frac{n}{s}$. Tomenos enteros M, N tales que Mn + N.r = S. Entonces

$$b = a^M (\xi^c a^{\frac{r}{n}})^N \in F, \text{ y en consecuencia}$$

$$b = \xi^{cN} a^{\frac{1}{m}}. \qquad \textbf{Q.D.}$$

6.1.3. LEMA:

Para cualquier n, los grupos de Galois de R sobre $\mathbb{Q}$ y de T sobre $\mathbb{Q}$ son abelianos.

DEMOSTRACION:

Tenemos que $R = \mathbb{Q}(\xi)$, $\xi^n = 1$, y todas las raíces de $t^n - 1$ son potencias de ξ. Entonces, si σ y τ son dos elementos distintos de $\Gamma(R:\mathbb{Q})$, $\sigma(\xi) \neq \tau(\xi)$. Pero $\sigma(\xi)$ es una raíz de $t^n - 1$, y por tanto, una potencia de ξ. Así $\sigma(\xi) = \xi^{n\sigma}$ donde n_σ es un entero $1 \leq n_\sigma < n$. Además,

$$\tau\sigma(\xi) = \tau(\sigma(\xi)) = \tau(\xi^{n\sigma}) = (\tau(\xi))^{n\sigma} = \xi^{n\tau . n\sigma}$$
$$= \sigma\tau(\xi).$$

Así, $n_{\sigma\tau} = n_\sigma . n_\tau \bmod n$. Luego, el mapeo de σ con n_σ es un homomorfismo de $\Gamma(R:\mathbb{Q})$ en un subgrupo multiplicativo de los enteros módulo n. Ya que $\tau \neq \sigma$ implica que $\tau(\xi) \neq \sigma(\xi)$, se sigue que, $\tau \neq \sigma$ implica que $n_\sigma \neq n_\tau$, es decir, el mapeo es inyectivo. Por tanto, el homomorfismo es un isomorfismo, o sea,

$\Gamma(R:\mathbb{Q}) \simeq$ (al grupo multiplicativo de los enteros modelo n).

Examinando directamente los posibles automorfismos, vemos que $\Gamma(T:\mathbb{Q}) \simeq \Gamma(R:\mathbb{Q}) \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \ldots \oplus \mathbf{Z}_2$, donde el grupo $\mathbf{Z}_2$ ocurre un número $j \leq k$ veces.

6.1.4 LEMA:

Si m es primo y $R^1 = \mathbb{Q}(\xi_m)$, entonces $[R^1:\mathbb{Q}] = m - 1$.

DEMOSTRACION:

Sabemos que f(t) es irreducible si y sólo si g(t) = f(t+1) es irreducible.

Si $\phi(t) = \frac{t^m - 1}{t - 1}$, entonces

$$\phi(t+1) = \frac{(t+1)^m - 1}{t}$$

$$= \frac{1}{t} \sum_{k=0}^{m-1} \binom{m}{k} t^{m-k}$$

$$= t^{m-1} + \binom{m}{1} t^{m-2} + \binom{m}{2} t^{m-3} + \ldots + \binom{m}{m-1}.$$

Tomando p = m, en el criterio de Eisenstein, resulta que $\phi(t+1)$ es irreducible sobre $\mathbb{Q}$. Luego

$$\frac{t^m - 1}{t - 1} \text{ es irreducible sobre } \mathbb{Q},$$

y en consecuencia $[R': \mathbb{Q}(\xi_m)] = m - 1$. **Q.D.**

6.1.5 LEMA:

1. Si m es primo y a ε $\mathbb{Q}$ no tiene raíz m-ésima racional, entonces $x^m - a$ es irreducible sobre $R^1 = \mathbb{Q}(\xi_m)$.

2. Para m = 4: si a > 0 y a ε $\mathbb{Q}$ no tiene raíz cuadrada racional, entonces $x^4 - a$ es irreducible sobre $R^1 = \mathbb{Q}(i)$.

DEMOSTRACION:

1. Asumamos que $x^m - a$ se factoriza sobre $R^1 = \mathbb{Q}(\xi_m)$ entonces por 6.1.2 resulta que $\xi\sqrt[m]{a} \varepsilon R^1$, $\xi^m = 1$, de aquí se deduce que $\sqrt[m]{a} \varepsilon R^1$. Luego podemos formar las siguientes extensiones:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[m]{a}) \subset R^1, \text{ de donde}$$
$$[\mathbb{Q}(\sqrt[m]{a}) : \mathbb{Q}] \mid [R^1 : \mathbb{Q}].$$

Como $x^m - a$ es irreducible sobre $\mathbb{Q}$, resulta que

$$[\mathbb{Q}(\sqrt[m]{a}) : \mathbb{Q}] = m, \text{ y por 6.1.4}$$
$$[R^1 : \mathbb{Q}] = m - 1, \text{ lo que es una contradicción.}$$

Q.D.

2. Asumamos que $x^4 - a$ se factoriza sobre $R^1 = \mathbb{Q}(i)$, entonces por 6.1.2 existe un entero m/4, m > 1, y una taíz cuarta de la unidad, tal que, $\xi\sqrt[m]{a} \varepsilon R^1$. Tenemos dos casos: ó m = 2, ó m = 4, y en ambos casos se establece que $\sqrt{a} \varepsilon \mathbb{Q}$, lo que es contrario a nuesta hipótesis.

6.1.6 LEMA:

1. Si $m > 2$ es primo y $a \in \mathbb{Q}$ es como en 6.1.5-1, entonces el grupo de Galois de $R^1(\sqrt[m]{a})$ sobre $\mathbb{Q}$ no es abeliano.

2. Para $m = 4$, $a \in \mathbb{Q}$ como en 6.1.5-2 el grupo de Galois $R^1(\sqrt[m]{a})$ sobre $\mathbb{Q}$ no es abeliano.

DEMOSTRACION:

1. De los lemas 6.1.4 y 6.1.5-1, sabemos que
   $[R^1:\mathbb{Q}] = m - 1$ y $[R^1(\sqrt[m]{a}):R^1] = m$, luego
   $[R^1(\sqrt[m]{a}):\mathbb{Q}] = m.(m-1)$.

   Observemos que $\{\xi,\ldots,\xi^{m-1}\}$ es una base de R^1 sobre $\mathbb{Q}$.
   $\{a, \sqrt[m]{a}, (\sqrt[m]{a})^2,\ldots,(\sqrt[m]{a})^{m-1}\}$ es una base de $R^1(\sqrt[m]{a})$ sobre R^1.

   De donde, se deduce que
   $\{\xi a,\ldots,\xi^{m-1}.a,\xi\sqrt[m]{a},\ldots,\xi^{m-1}\sqrt[m]{a},\ldots,\xi(\sqrt[m]{a})^{m-1},\ldots,\xi^{m-1}(\sqrt[m]{a})^{m-1}\}$
   es una base de $R^1(\sqrt[m]{a})$ sobre $\mathbb{Q}$.

   Sabemos que cualquier automorfismo de $R^1(\sqrt[m]{a})$ sobre $\mathbb{Q}$ queda completamente determinado por su efecto sobre la base, y vemos que esto está determinado, en último momento, por el efecto de los automorfismos sobre ξ y $\sqrt[m]{a}$. En consecuencia todo los automorfismos de $\Gamma(R^1(\sqrt[m]{a}):\mathbb{Q})$ son de la forma:

$$\phi_k^s(\xi) = \xi^s,\ 0 < s < m$$

$$\phi_k^s(\sqrt[m]{a}) = \xi^k \sqrt[m]{a},\ k = 0,1,\ldots,m-1.$$

Considerando

$$\phi_0^2(\xi) = \xi^2$$

$$\phi_0^2(\sqrt[m]{a}) = \sqrt[m]{a}\ , \qquad y$$

$$\phi_1^2(\xi) = \xi^2$$

$$\phi_1^2(\sqrt[m]{a}) = \xi\sqrt[m]{a}, \quad \text{vemos que}$$

$$(\phi_0^2 \circ \phi_1^2)(\xi) = \phi_0^2(\xi^2) = \left[\phi_0^2(\xi)\right]^2 = \xi^4,$$

$$(\phi_0^2 \circ \phi_1^2)(\sqrt[m]{a}) = \phi_0^2(\xi\sqrt[m]{a}) = \phi_0^2(\xi).\phi_0^2(\sqrt[m]{a}) = \xi^2\sqrt[m]{a}\ ,$$

o sea que $\phi_0^2 \circ \phi_1^2 = \phi_2^4$.

De manera similar,

$$(\phi_1^2 \circ \phi_0^2)(\xi) = \phi_1^2(\xi^2) = \left[\phi_1^2(\xi)\right]^2 = \xi^4$$

$$(\phi_1^2 \circ \phi_0^2)(\sqrt[m]{a}) = \phi_1^2(\sqrt[m]{a}) = \xi\sqrt[m]{a}, \text{ es decir}$$

$$\phi_1^2 \circ \phi_0^2 = \phi_1^4.$$

Por tanto $\phi_0^2 \circ \phi_1^2 \neq \phi_1^2 \circ \phi_0^2$.

2. Demanera similar por los lemas 6.1.4 y 6.1.5-2, deducimos que

$$\left[R^1(\sqrt[m]{a}) : \mathbb{Q}\right] = 4.2\ .$$

En consecuencia, todos los automorfismos de

$$\Gamma(R^1(\sqrt[m]{a}) : \mathbb{Q}) \text{ son:}$$

$$\phi_k^s(\sqrt[4]{a}) = (i)^k\ \sqrt[4]{a},\ k = 0,1,2,3,$$

$$\phi_k^s(i) = (i)^s\ ,\ s = 1 \text{ ó } 3.$$

Considerando

$$\phi_0^3(\sqrt[4]{a}) = \sqrt[4]{a}$$

$$\phi_0^3(i) = -i, \quad y$$

$$\phi_1^1(\sqrt[4]{a}) = i\sqrt[4]{a},$$

$$\phi_1^1(i) = i, \text{ vemos que:}$$

$$(\phi_0^3 \circ \phi_1^1)(\sqrt[4]{a}) = \phi_0^3(i\sqrt[4]{a}) = \phi_0^3(i).\phi_0^3\sqrt[4]{a}) = -i\sqrt[4]{a},$$

$$(\phi_0^3 \circ \phi_1^1)(i) = \phi_0^3(i) = -i, \text{ es decir:}$$

$$\phi_0^3 \circ \phi_1^1 = \phi_3^3.$$

Por otro lado,

$$(\phi_1^1 \circ \phi_0^3)(\sqrt[4]{a}) = i\sqrt[4]{a}$$

$$(\phi_1^1 \circ \phi_0^3)(i) = -i, \text{ o sea:}$$

$$\phi_1^1 \circ \phi_0^3 = \phi_1^3.$$

Por tanto, $\phi_0^3 \circ \phi_1^1 \neq \phi_1^1 \circ \phi_0^3$. **Q.D.**

6.1.7 LEMA:

Aquí n es arbitrario, R y T son como anteriormente. Supóngase que m > 2, a > 0 a ε $\mathbb{Q}$, y a no tiene raíz q-ésima en $\mathbb{Q}$ para cualquier q/m, q > 1. Entonces

$$\sqrt[m]{a} \notin T = R(p_1^{\frac{1}{2}}, \ldots, p_k^{\frac{1}{2}})$$

DEMOSTRACION:

Basta considerar solamente dos casos, m = primo > 2, y m = 4. Como T es una extensión finita normal de $\mathbb{Q}$, y si $\sqrt[m]{a} \varepsilon T$,

entonces por el teorema fundamental,

$$\Gamma(R(\sqrt[m]{a}):\mathbb{Q}) \simeq \frac{\Gamma(T:\mathbb{Q})}{\Gamma(T:R(\sqrt[m]{a}))} .$$

Pero por los lemas 6.1.3 y 6.1.6, sabemos que $\Gamma(T:\mathbb{Q})$ es abeliano, $\Gamma(R(\sqrt[m]{a}):\mathbb{Q})$ es no abeliano, lo que es una contradicción. **Q.D.**

Ahora volvamos a la prueba del teorema t.1.1.

Hemos visto que ii implica iii. Para probar ii tomemos un $M \geq k$ fijo y sea

$$T^* = R(p_1^{\frac{1}{2}}, \ldots, p^{\frac{1}{2}}).$$

T^* permanecerá fijo, y sea $F_k = T^*(p_1^{\frac{1}{n}}, \ldots, p_k^{\frac{1}{n}})$ donde $k \leq M$.

Probaremos por inducción que $[F_k:T^*] = (\frac{n}{2})^k$. Para $k = 1$, consideremos $x^{\frac{n}{2}} - p_1^{\frac{1}{2}}$ sobre T^* y veamos que este polinomio es irreducible. Supongamos que no. Entonces por 6.1.2, existe un entero $m/\frac{n}{2}$, $m > 1$ y una raíz $\frac{n}{2}$-ésima de la unidad tal que:

$$\xi\sqrt[m]{p_1^{\frac{1}{2}}} \in T^*; \text{ donde } \xi^{\frac{n}{2}} = 1$$

implica $(\xi^{\frac{1}{2}})^n = 1$, $\xi^{\frac{1}{2}} \in T^*$ y $\xi \in T^*$.

Luego

$$\sqrt[m]{p_1^{\frac{1}{2}}} \in T^*,$$ lo que es contrario a 6.1.7. Por tanto $x^{\frac{n}{2}} - p^{\frac{1}{2}}$ es irreducible sobre T^* y $p^{\frac{1}{n}}$ lo satisface, o sea que,

$$[F:T^*] = \frac{n}{2}.$$

Asumamos ahora que $[F_k : T^*] = (\frac{n}{2})^k$.

Deseamos mostrar que $x^{\frac{n}{2}} - P_{k+1}^{\frac{1}{2}}$ es irreducible sobre F_k. Supongamos que no. Entonces por 6.1.2 hay un entero $m/\frac{n}{2}$, $m > 1$, tal que

$$P_{k+1}^{\frac{1}{2m}} \in F_k.$$

Por nuestra hipótesis inductiva, el conjunto $\{\beta_i\}$, que genera a F_k sobre T^*, forma una base. Así

(α) ... $P_{k+1}^{\frac{1}{2m}} = c_1\beta_1 + \ldots + c_N\beta_N$, donde $c_i \in T^*$ y $N = (\frac{n}{2})$.

Hay ahora dos casos:

Caso 1. Exactamente uno de los $c_i \neq 0$, es decir, para algún i,

$$P_{k+1}^{\frac{1}{2m}} = c_i.\beta_i, \quad c_i \in T^*.$$

$$\frac{P_{k+1}^{\frac{1}{2m}}}{\beta_i} \in T^*, \text{ lo que puede llevarse a la forma}$$

$$\sqrt[m]{\frac{\sqrt{P_{k+1}}}{\sqrt{p_1^{k_1}}\sqrt{p_2^{k_2}}\ldots\sqrt{p_k^{k_k}}}} \in T^*$$

lo que es contrario a 6.1.7.

Caso 2. Tenemos que c_i y c_i son distintos de cero, $i \neq j$. Ya que

$$\frac{\beta_i}{\beta_i} \notin T^* \text{ , existe un automorfismo } \phi \text{ de } F_k \text{ so-}$$

bre T* talque $\phi(\frac{\beta_i}{\beta_j}) \neq \frac{\beta_i}{\beta_j}$. Pero todos los β's y también $P_{k+1}^{\frac{1}{2m}}$ son raíces n-ésimas de enteros,

$$\phi(\beta_i) = \xi^r \beta_i ,$$

$$\phi(\beta_j) = \xi^s \beta_j , \quad \text{donde } \xi^s \neq \xi^r,$$

$$\phi(\beta_h) = \xi^{c(h)} \beta_h, \text{ para } h \neq i,j,$$

$$\phi(P_{k+1}^{\frac{1}{2m}}) = \xi^t P_{k+1}^{\frac{1}{2m}}$$

para algunos r, s, c(h), t. Entonces ya que $\xi \in T^*$, aplicando ϕ a (α):

$$\xi^t P_{k+1}^{\frac{1}{2m}} = c_i \xi^{c(1)} \beta_1 + \ldots + c_i \xi^r \beta_i + c_k \xi^{c(k)} \beta_k + \ldots + c_j \xi^s \beta_j + \ldots + c_N \xi^{c(N)} \beta_N$$

esta última expresión:

$$c_1(\xi^{c(1)} - \xi^t)\beta_1 + \ldots + c_i(\xi^r - \xi^t)\beta_i + c_k(\xi^{c(k)} - \xi^t)\beta_k + \ldots + c_n(\xi^{c(N)} - \xi^t)\beta_N = 0$$

pero esta es una continuación lineal nula de los $\{\beta_i\}$ donde no todos los escalares son cero, puesto que $\xi^r \neq \xi^r$, contradiciendo de esta forma la independencia lineal de $\{\beta_i\}$ sobre T^*.

Por tanto, $x^{\frac{n}{2}} - P_{k+1}^{\frac{1}{2}}$ es irreducible sobre F_k, y $P_{k+1}^{\frac{1}{n}}$ satisface este polinomio, es decir,

$[F_{k+1}:F_k] = \frac{n}{2}$. Luego $[F_{k+1}:T^*] = (\frac{n}{2})^{k+1}$, y esto nos prueba ii.

Reemplazando T^* por $\mathbb{Q}$ en la demostración anterior, obtene

mos una prueba de i. **Q.D.**

Este resultado muestra que $\sqrt[n]{p_1}$ no es expresable racionalmente en términos de otras raices n-ésimas, así por ejmplo, $\sqrt[3]{2}$ no es una combinación racional de raices cúbicas de otros números primos.

6.1.8 TEOREMA:

$\sqrt[3]{2}$ no es una combinación racional de raices cuadradas de números racionales.

DEMOSTRACION:

Si en el teorema 6.1.1, n = 2 y 3, entonces

$$[\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_k}):\mathbb{Q}] = 2^k,$$

$$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3.$$

Supongamos que $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_k})$,
entonces $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] \mid 2^k$, o sea, $3 \mid 2^k$ cosa que no puede suceder.
Q.D.

Similarmente, $\sqrt[3]{2}$ no es expresable como una combinación de raices quintas, y así, sucesivamente.

6.1.9 DEFINICION:

Definimos los polinomios ciclotómicos $\phi_n(t)$ inductivamen-

te como:

1. $\phi_1(t) = t - 1$

2. Si $n > 1$, entonces $\phi_n(t) = \frac{t^n - 1}{\Pi \phi_d(t)}$

donde $d|n$, $d \neq n$.

6.1.10 DEFINICION:

Llamamos $\mathbb{Q}_\xi$ al campo ciclotómico obtenido de los racionales adjuntandole todas las raices n-ésimas de la unidad ξ_n para cada n.

Ya sabemos que $\Gamma(\mathbb{Q}(\xi_n): \mathbb{Q})$ es abeliano, así el próximo teorema podría ser usado en la prueba del teorema de Richard para mostrar que

$$\Gamma(\mathbb{Q}(p_1^{\frac{1}{2}}, \ldots, p_n^{\frac{1}{2}}): \mathbb{Q}) \text{ es abeliano}$$

6.1.11. TEOREMA:

$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots, \sqrt{n}, \ldots)$ es un subcampo de $\mathbb{Q}_\xi$.

DEMOSTRACION:

Es suficiente mostrar que $\sqrt{p} \in \mathbb{Q}$, para cada primo p.

(1) Sea p un primo, $p > 2$, y sea

$\phi_p(t) = t^{p-1}+\ldots+ t + 1$ el p-ésimo polinomio ciclotómico. El discriminante Δ de $\phi_p(t)$ es $\Delta = \prod_{i<j} (\xi^i-\xi^j)^2$, donde $i,j = 1,\ldots,p-1$ y ξ una raíz p-ésima de la unidad.

(2) Ya que $\xi,\xi^2,\ldots$ son raices de $\phi_p(t)$, tenemos

$\phi_p(t) = (t-\xi)(t-\xi^2)\ldots(t-\xi^{p-1})$, y diferenciando con respecto a t, conseguimos

$$\phi_p^1(t) = \sum_{i=1}^{p-1} (x-\xi)\ldots(x-\xi^{i-1})(x-\xi^{i+1})\ldots(x-\xi^{p-1})$$

$$\phi_p^1(\xi^i) = (\xi^i-\xi)\ldots(\xi^i-\xi^{i-1})(\xi -\xi^{i+1})\ldots(\xi^i-\xi^{p-1}),$$

(3) Multiplicando todos los $\phi^1(\xi^i)$, obtenemos

$$\prod_i \phi^1(\xi^i) = \left[(\xi-\xi^2)(\xi-\xi^3)\ldots(\xi-\xi^{p-1})\right]$$
$$- \left[(\xi^2-\xi)(\xi^2-\xi^3)\ldots(\xi^2-\xi^{p-1})\right]$$
$$\ldots$$
$$\left[(\xi^{p-1}-\xi)(\xi^{p-1}-\xi^2)\ldots(\xi^{p-1}-\xi^{p-2})\right]$$
$$= (-1)^{\frac{p(p-1)}{2}} \Delta.$$

(4) Pero también $t^p-1 = (t-1)\phi_p(t)$ y diferenciando,

$$pt^{p-1} = \phi_p(t) + (t-1)\phi_p^1(t).$$

(5) Esto da

$$p\xi^{i(p-1)} = (\xi^i-1)\phi_p^1(\xi^i), \text{ ya que } \phi_p(\xi^i) = 0.$$

(6) Multiplicando todas estas expresiones, para $i = 1,\ldots,p-1$.

$$p^{p-1} \cdot \xi^{p-1} \cdot \xi^{2(p-1)} \cdot \xi^{3(p-1)} \cdots \xi^{(p-1)\cdot(p-1)}$$

$$= \prod_i (\xi^i - 1) \prod_i \phi^1(\xi^i)$$

y usando el hecho de que

$$\xi^{p-1} \cdot \xi^{2(p-1)} \cdot \ldots \xi^{(p-1)(p-1)} = (\xi \cdot \xi^2 \ldots \xi^{p-1}) = 1^{p-1} = 1,$$

mientras

$$\prod_i (\xi^i - 1) = (-1)^{p-1} \phi_p(1), \text{ conseguimos}$$

$$p^{p-1} = (-1)^{p-1} \cdot p \prod_i \phi_p^1(\xi^i), \text{ pues}$$

$$\prod_i (\xi^i - 1) = \prod_i (1 - \xi^i) = p, \text{ porque } p-1 \text{ es par.}$$

(7) Combinando esto con (3)

$$p^{p-2} = (-1)^{\frac{p(p-1)}{2}} \Delta = (-1)^{\frac{p-1}{2}} \Delta, \text{ ya que}$$

$$(-1)^{\frac{p(p-1)}{2}} = ((-1)^p)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

(8) Por lo tanto

$$\Delta = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$$

$$= \begin{cases} p^{p-2}, & \text{si } \frac{p-1}{2} \text{ es par,} \\ -p^{p-2}, & \text{si } \frac{p-1}{x} \text{ es impar.} \end{cases}$$

(9) Sin embargo,

$\frac{p-1}{2}$ es par $\iff p \equiv 1$, mod. 4.

$\frac{p-1}{2}$ es impar $\iff p \equiv 3$ mod. 4.

(10) Cambiando esto con (8) tenemos

$$\Delta = \begin{cases} p.p & , \text{ si } p \equiv 1 \bmod 4, \\ -p.p & , \text{ si } p \equiv 3 \bmod 4, \end{cases}$$

$$\sqrt{\Delta} = \begin{cases} p^{\frac{p-3}{2}}.\sqrt{p}, & \text{si } p \equiv 1 \bmod 4, \\ ip^{\frac{p-3}{2}}.\sqrt{p}, & \text{si } p \equiv 3 \bmod 4. \end{cases}$$

(11) Por definición de Δ, este es el cuadrado de un elemento del campo $\mathbb{Q}(\xi_p)$, así $\sqrt{\Delta} \in \mathbb{Q}(\xi_p)$.

Nótese que $p-3$ es par, haciendo $p^{\frac{p-3}{2}}$ un entero.

Como resultado tenemos

$$\sqrt{p} = \begin{cases} \dfrac{\sqrt{\Delta}}{p^{\frac{p-3}{2}}} \in \mathbb{Q}(\xi), & \text{si } p \equiv 1 \bmod 4, \\ -i.\dfrac{\sqrt{\Delta}}{p^{\frac{p-3}{2}}} \in \mathbb{Q}(i,\xi), & \text{si } p \equiv 3 \bmod 4, \end{cases}$$

y $\mathbb{Q}(i,\xi_p) \simeq \mathbb{Q}(\xi_{2p})$.

Por tanto, $\sqrt{p} \in \mathbb{Q}\xi$, para todo primo $p > 2$.

(12) Mostremos ahora que $\sqrt{2} \in \mathbb{Q}\xi$.

Evidentemente

$$\xi_8 = e^{\frac{2\pi i}{8}} = \cos\left(\frac{\pi}{4}\right) + i \operatorname{sen}\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}(1+i),$$

así $\sqrt{2} = \dfrac{2\xi_8}{1+i} = \dfrac{2\xi_8(1-i)}{(1+i)(1-i)} = \xi_8(1-i) \in \mathbb{Q}\xi$

(13) En síntesis, tenemos

$\sqrt{2} \in \mathbb{Q}(\xi_8)$,

$\sqrt{p} \in \mathbb{Q}(\xi_p)$, si $p \equiv 1 \bmod 4$,

$\sqrt{p} \in \mathbb{Q}(\xi_2 p)$, si $p \equiv 3 \bmod 4$.

(14) En cualquier caso, hemos demostrado que

$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$ es un subcampo de $\mathbb{Q}\xi$. **Q.D.**

6.1.12 COROLARIO:

Si $p > 2$ y $a \in \mathbb{Q}$ no tiene raíz p-ésima racional, entonces $a^{\frac{1}{p}} \notin \mathbb{Q}\xi$, pero $a^{\frac{1}{2}} \in \mathbb{Q}\xi$.

DEMOSTRACION:

Si $a^{\frac{1}{p}} \in \mathbb{Q}\xi$, $\mathbb{Q} \subset \mathbb{Q}(\xi_p, a^{\frac{1}{p}}) \subset \mathbb{Q}\xi$, en consecuencia

$$\Gamma(\mathbb{Q}(\xi_p, a^{\frac{1}{p}}) : \mathbb{Q}) = \frac{\Gamma(\mathbb{Q}\xi : \mathbb{Q})}{\Gamma(\mathbb{Q}\xi : \mathbb{Q}(\xi_p, a^{\frac{1}{a}}))}$$

seria abeliano, lo que es contrario al 6.1.6.

Q.D.

CAPITULO VII

TEORIA DE GALOIS DE ECUACIONES DIFERENCIALES

Para las ecuaciones diferenciales hay una teoría semajante a la teoría de Galois para polinomios.

7.1.1 DEFINICION:

Un campo diferencial es un campo K junto con una derivación

$D: K \longrightarrow K$ con las propiedades

$D(x+y) = D(x) + D(y)$,

$D(x.y) = xD(y) + D(x).y$, para toda $x,y \in K$.

7.1.2 EJEMPLO:

El ejemplo canónico y uno de los más importantes para las aplicaciones, es cuando K es el campo $\mathbb{C}(x)$ de las funciones racionales complejas, y D es la derivada usual.

Podemos definir subcampos diferenciales, extensiones diferenciales en la forma obvia. La derivación debe conmutar con el mapeo inclusión. El campo de constantes de K es el conjunto de todas las $x \in K$ tal que $D(x) = 0$; este es un subcampo que

contiene al subcampo primo.

7.1.3 DEFINICION:

Un automorfismo diferencial α de K es un automorfismo que hace que el diagrama

$$\begin{array}{ccc} K & \xrightarrow{\alpha} & K \\ {\scriptstyle D}\downarrow & & \downarrow{\scriptstyle D} \\ K & \xrightarrow{\alpha} & K \end{array}$$

conmute, es decir, $\alpha \circ D = D \circ \alpha$.

7.1.4 DEFINICION:

Si M es una extensión diferencial de K entonces el grupo de Galois de M:K es el grupo de todos los automorfismos diferenciales de M los cuales dejan fijo todo elemento de K. Es usualmente un grupo infinito.

Hasta ahora lo que hemos hecho es poner la palabra "diferencial" en frente de cada concepto referido a polinomios ya podemos establecer la correspondencia de Galois:

Si L es un subcampo diferencial de M definimos L* como un subgrupo del grupo de Galois G de M:K; y si H es un subgrupo de G definimos H^+ en la manera usual. Pero la correspondencia de Galois no funciona todavía. Un subgrupo H se llama cerrado si $H = H^{+*}$, y un subcampo L es cerrado si $L = L^{*+}$. Entonces *

y + definen una biyección entre subgrupos cerrados y subcampos cerrados.

Abordemos ahora las ecuaciones diferenciales. Para $y \in K$ definimos $y' = D(y)$, $y'' = D^2(y), \ldots, y^{(n)} = D^n(y)$.

Consideremos la ecuación diferencial lineal homogenea

(1) $$y^{(n)} + a_1 y^{(n-1)} + \ldots + a_{n-1}y' + a_n y = 0$$

donde $a_1, a_2, \ldots, a_n \in K$. Supongamos que en algún campo diferencial más grande $u_1, \ldots, u_{n+1}$ son soluciones de (1). Entonces podemos mostrar que existen constantes $c_1, \ldots, c_{n+1} \in K$ tales que

$c_1u_1 + \ldots + c_{n+1}u_{n+1} = 0$ donde no todos los c_i son cero. Así hay a lo sumo n soluciones de (1) linealmente independiente sobre las constantes.

Una extensión diferencial M de K es una extensión Picard - Vessiot (para la ecuación (1)) si:

1. M es el campo diferencial generado por K junto con $u_1, u_2, \ldots, u_n$ donde u_i satisfacen (1) y son linealmente independiente sobre las constantes.

2. M tiene el mismo campo de constantes que K.

En la misma forma que preguntamos si la ecuación quíntica puede ser resuelta por radicales, podemos preguntar si una ecuación diferencial particular puede ser resuelta por métodos

específicos. Dos métodos importantes son los siguientes

1. Adjuncín de una integral. Adjuntar u tal que $u'-a = 0$, para $a \in K$.

2. Adjunción de una exponencial de una integral. Adjuntar u tal que $u' - au = 0$, para $a \in K$.

La terminología es clara considerando ecuaciones diferenciales para funciones u de valor real.

M es una extensión de liouville de K si existen una cadena de subcampos

$$K = K_0 \subset K_1 \subset \ldots \subset K_n = M$$

tal que cada extensión $K_{i+1}: K_i$ es la adjunción de una integral o la exponencial de una integral. Se puede entonces probar:

7.1.5 TEOREMA:

Si M es una extensión de Liouville de K entonces el grupo diferencial de Galois es soluble.

Para ir más lejos debemos introducir más estructuras sobre el grupo diferencial de Galois. Este puede ser considerado como un grupo algebraico sobre el campo de constantes, es decir, un grupo de matrices (g_{ij}) definidas por un sistema de ecuaciones polinomiales. Así la ecuación $\det(g_{ij}) = 1$ define el grupo algebraico de todas las matrices unimodulares. Las ma

trices surgen porque los automorfismos inducen transformaciones lineales sobre el espacio vectorial de las soluciones de la ecuación diferencial generada por u_1, u_2, ..., u_n.

Para una extensión Picard - Vessiot se tiene que todo campo intermedio es cerrado; mientras que los subgrupos cerrados del grupo diferencial de Galois son subgrupos algebraicos.

En nuestro próximo resultado necesitaremos una definición más. En cualquier grupo algebraico puede definirse una topología, llamada la topología de Zariski. No necesitamos estar relacionados con esta topología, pero de seguro se divide en componentes conexas. La componente que contiene el elemento identidad del grupo es un subgrupo normal llamada componente de la identidad.

7.1.6 TEOREMA:

Supongamos que M:K es una extensión Picard - Vessiot, tal que K tiene característica cero y el campo de constantes $\mathbb{C}$ es algebraicamente cerrado. Supongamos que M puede ser incluido en un campo diferencial obtenido de K por una serie finita de extensiones algebraicas simples, adjunciones de integrales, o adjunciones de exponenciales de integrales. Entonces la componente de la identidad del grupo diferencial de Galois es soluble.

Recíprocamente, si el grupo diferencial de Galois de M:K tiene la componente de la identidad soluble, entonces M puede ser obtenido de K junto con una extensión normal finita seguida por una extensión de Liouville.

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

1- CLASSICAL GALOIS THEORY

Gaal, L. Chelsea,

Publishine Company, 2a. Edición

2- GALOIS THEORY

Stewart, D. Napco

2a. Edición

3- GALOIS THEORY

Artin, E. Napco

6a. Edición

4- INTRODUCCION TO ABSTRACT ALGEBRA

Shapiro, L. MacGraw Hill

2a. Edición

5- ALGEBRA MODERNA

Herstein, I.N. Trillas

4a. Edición.