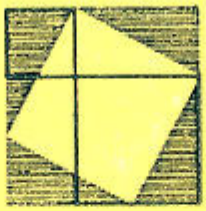
# INFORME TECNICO INTERNO

## Nº. 20

INSTITUTO DE MATEMATICA DE BAHIA BLANCA

INMABB (UNS - CONICET)



UNIVERSIDAD NACIONAL DEL SUR

Avda. ALEM 1253 - 8000 BAHIA BLANCA

República Argentina

I. T. I. Nº 20

# EXTENSIONES ALGEBRAICAS

# TEORIA DE GALOIS

María Luisa Gastaminza

INMABB

UNS - CONICET



1989

# INDICE

# INTRODUCCION

En estas notas se desarrolla la Teoría de Galois para cuerpos arbitrarios. El propósito central es demostrar el criterio de resolubilidad por radicales de una ecuación algebraica y estudiar la ecuación general de grado n.

La armonía y profundidad de esta teoría, su fuerte motivación histórica y las aplicaciones de sus resultados la hacen especialmente recomendable para un curso optativo de álgebra.

El cálculo de las raíces de los polinomios fue el problema central del álgebra durante siglos. Los babilonios ya conocían la fórmula que da las raíces de la ecuación cuadrática $aX^2 + bX + c = 0$ en función de sus coeficientes mediante operaciones racionales y radicales de segundo grado. Se trataba de encontrar fórmulas que permitieran resolver en forma análoga ecuaciones de grado superior al segundo.

En el renacimiento italiano se hallaron las que dan las raíces de los polinomios de tercer y cuarto grados. La de la ecuación cúbica fue encontrada por Scipione del Ferro (1465-1526), sin que se conozca la fecha exacta. Se sabe que en 1541 Niccolo Tartaglia (1490-1557), tal vez conociendo el trabajo de del Ferro, la redescubrió. La fórmula de Tartaglia fue publicada por Gerolamo Cardano (1501-1576) en su Ars Magna (1545) y se conoce como "las fórmulas de Cardano". Un método general para resolver las ecuaciones de cuarto grado, también publicado por Cardano, se atribuye a un ayudante del mismo, Ludovico Ferrari (1522-1565).

Desde mediados del siglo XVI hasta comienzos del XIX numerosos esfuerzos fueron hechos por los más notables matemáticos de la época para generalizar estos resultados a la ecuación de quinto grado. Joseph-Louis Lagrange (1736-1813) hizo un profundo análisis de la resolubilidad de las ecuaciones cúbicas y cuárticas y mostró que la razón de que ello fuera posible era que la resolución de estas ecuaciones podía reducirse a la de "ecuaciones resolventes" de menor grado. Por otro lado encontró que aplicando los mismos métodos a la ecuación de quinto grado se obtenía una resolvente de grado seis. Este resultado sugería la imposibilidad de resolver por radicales las ecuaciones de quinto grado, lo que fue demostrado independientemente por Paolo Ruffini (1765-1822) (publicado en 1813) y

por Niels Abel (1802-1829) (publicado en 1827). El trabajo de Évariste Galois (1811-1832) sobre este problema fue más profundo y completo porque dio una condición necesaria y suficiente para que cada ecuación algebraica particular sea resoluble por radicales. Esta condición se refiere a las propiedades de un cierto grupo de permutaciones que se asocia a la ecuación. Galois murió en un duelo antes de cumplir veintiun años, y sus escritos recién fueron publicados en 1846. Sus ideas, elaboradas y desarrolladas, constituyen lo que actualmente se llama Teoría de Galois.

Otro problema clásico que estudiamos en estas notas y que se resuelve en términos de extensiones de cuerpos es el de las construcciones con regla y compás. Tiene su origen en los matemáticos griegos, quienes no supieron decidir si ciertas construcciones geométricas son posibles usando la regla y compás solamente (regla = regla no subdividida). Las más famosas eran: 1) Trisección de cualquier ángulo, 2) Duplicación del cubo, es decir, construir el lado de un cubo de volumen igual al doble de uno dado, 3) Cuadratura del círculo, es decir, construir un cuadrado de área igual a la de un círculo dado. Todo problema de construcción con regla y compás puede formularse como un problema algebraico sobre cuerpos. No es difícil ver que hay ángulos no trisecables y que las dos últimas construcciones son imposibles, usando para la cuadratura del círculo que $\pi$ no es algebraico sobre Q, lo que fue demostrado por F.Lindemann (1852-1939) en 1882.

Es de señalar que lo que se demuestra es la imposibilidad de construcciones exactas.(Las hay que dan muy buena aproximación).

Para los datos históricos y biográficos que complementan necesariamente los resultados matemáticos expuestos en estas notas puede consultarse la bibliografía que se indica, particularmente [17], [19], [20], [21].

# CAPITULO I

## POLINOMIOS Y RAICES

Recordemos algunos resultados conocidos sobre el anillo de polinomios K[X] con coeficientes en un cuerpo K:

1) K[X] tiene división entera: cualesquiera sean $f(X), g(X) \in K[X]$, $g \neq 0$, existen polinomios únicos $q(X), r(X) \in K[X]$ tales que $f = q.g + r$ y $r = 0$ o $gr\ r < gr\ g$. K[X] es dominio euclideano.

2) K[X] es un dominio principal y por lo tanto D.F.U. (dominio de factorización única). Si $f(X) \in K[X]$, $gr\ f \geq 1$, las siguientes propiedades son equivalentes:

   i) $f(X)/g(X).n(X)$ implica $f/g$ o $f/n$.
   ii) $f(X)$ es irreducible.
   iii) $(f(X))$ es un ideal maximal.
   iv) $(f(X))$ es un ideal primo.

3) A D.F.U. implica A[X] D.F.U., y de aquí
   A D.F.U. implica $A[X_1, X_2, \ldots, X_n]$ D.F.U.

   TEOREMA 1.1. Si A es un D.F.U. entonces A[X] es D.F.U. Los irreducibles de A[X] son los primos de A y los polinomios primitivos de A[X] que son irreducibles en K[X], siendo K el cuerpo de cocientes de A. ( Un polinomio $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ se dice primitivo si el m.c.d. de sus coeficientes es 1).

Decidir si un polinomio $f(X) \in K[X]$ es irreducible es un problema difícil.

4) Criterio de irreducibilidad de Eisenstein: Si A es un D.F.U., K su cuerpo de cocientes, $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$, $n \geq 1$ y existe un primo $p \in A$ tal que $p \nmid a_n$, $p \mid a_i$, $i = 0,1,\ldots,n-1$ y $p^2 \nmid a_0$ entonces f(X) es irreducible en K[X].

EJEMPLOS. Si a es un entero $\neq \pm 1$ y no divisible por cuadrados $\neq 1$ el polinomio $X^n - a$ es irreducible en $Q[X]$. También lo son $3X^3 - 2X + 6$ , $10X^4 - 6X^2 + 3$.

A veces un polinomio no satisface las condiciones del critero de Eisenstein, pero una transformación del mismo sí.

Por ejemplo, se verifica que $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ es irreducible sobre Q, para todo primo p. Para verlo es suficiente mostrar que $f(X+1)$ es irreducible sobre Q:

Como $f(X) = \dfrac{X^p - 1}{X - 1}$ , es $f(X + 1) = \dfrac{(X + 1)^p - 1}{X + 1 - 1}$ y se tiene

$$f(X+1) = \frac{X^p + \binom{p}{1}X^{p-1} + \ldots + \binom{p}{p-1}X}{X} = X^{p-1} + \binom{p}{1}X^{p-2} + \ldots + p$$

que verifica las condiciones del criterio.

Notar que de 3) resulta que para estudiar la factorización en $Q[X]$ de un polinomio $f(X)$ con coeficientes racionales podemos suponer que todos sus coeficientes son enteros y hallar su factorización en $Z[X]$.

(En general, si A es un D.F.U. y K su cuerpo de cocientes, si $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ entonces $f(X) = c.f_1(X)$ siendo $c \in K$ y $f_1(X) \in A[X]$ primitivo. Entonces es suficiente hallar la factorización de $f_1(X)$).

Existe un algoritmo para hallar en un número finito de pasos la descomposición en factores irreducibles en $Q[X]$ de cualquier polinomio $f(X) \in Q[X]$, debido a Leopold Kronecker (1823-1891). (Ver Van der Waerden, Modern algebra I, pág. 77).

5) Otro criterio de irreducibilidad.

En general, si $\varphi: A \to B$ es un homomorfismo de un anillo A en otro B, $\varphi$ puede extenderse a uno $\tilde{\varphi}: A[X] \to B[X]$ definiendo $\tilde{\varphi}(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \varphi(a_i)X^i$. Es claro que $\tilde{\varphi}/A = \varphi$.

TEOREMA 1.2: Sean A,B dominios de integridad, K, L sus cuerpos de cocientes y $\varphi$: A → B un homomorfismo de anillos. Sea $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ tal que gr $\tilde{\varphi}(f(X))$ = gr f. Entonces si $\tilde{\varphi}(f(X))$ es irreducible en L[X], f(X) no se puede factorizar f(X) = g(X).h(X), con g,h ∈ A[X] y gr g, gr h ≥ 1.

Demostración. En las condiciones del enunciado, si f(X) se pudiera factorizar en A[X] f = g.h con g,h no constantes entonces $\tilde{\varphi}(f) = \tilde{\varphi}(g).\tilde{\varphi}(h)$. Como gr $\tilde{\varphi}(f)$ = gr $\tilde{\varphi}(g)$ + gr $\tilde{\varphi}(h)$ y gr $\tilde{\varphi}(g) \leq$ gr g (1) y gr $\tilde{\varphi}(h) \leq$ gr h (2), de la hipótesis gr $\tilde{\varphi}(f)$ = gr f sigue que (1) y (2) son igualdades, lo que contradice la irreducibilidad de $\tilde{\varphi}(f)$ en L[X].

Este criterio se puede aplicar al caso particular en que A es un D.F.U. y se tiene entonces: "Si $\varphi$: A → B es un homomorfismo de un D.F.U. A en un dominio B, K, L son sus respectivos cuerpos de cocientes, $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ es tal que gr($\tilde{\varphi}(f)$) = gr f, entonces si $\tilde{\varphi}(f)$ es irreducible en L[X], f es irreducible en K[X]".

Demostración. f se puede escribir en A[X] como f = c.$f_1$, c = m.c.d. de los coeficientes de f, $f_1$ polinomio primitivo. Por el teorema anterior y el 1.1 se tiene $\tilde{\varphi}(f)$ irreducible en L[X] ⇒ $f_1$ irreducible en A[X] ⇒ $f_1$ irreducible en K[X] ⇒ f irreducible en K[X].

Este criterio puede aplicarse para decidir si un polinomio f(X) ∈ Z[X] es irreducible: tomando $\varphi$: Z → $Z_p$ el homomorfismo canónico, si gr($\tilde{\varphi}(f)$) = gr f y $\tilde{\varphi}(f)$ es irreducible en $Z_p$[X] entonces f es irreducible en Q[X].

Ejemplo. El polinomio $f(X) = X^3 + 5X^2 - 9X + 16$ es irreducible sobre Q pues si consideramos el homomorfismo canónico $\varphi$: Z → $Z_3$, es $\tilde{\varphi}(f) = X^3 + 2X^2 + 1$ que es irreducible en $Z_3$[X].

Nota. No vale el criterio recíproco: $X^2 + 1$ es irreducible en Q[X] y no lo es en $Z_2$[X]. Más aún, existen polinomios con coeficientes enteros irreducibles sobre Q pero reducibles sobre $Z_p$, para todo primo p.
Por ejemplo, el polinomio $f(X) = X^4 - 10X^2 + 1$ está en esas condiciones. En efec

to, sus raíces son $\pm \sqrt{\frac{10 \pm \sqrt{100-4}}{2}} = \pm(\sqrt{2} \pm \sqrt{3})$.

Luego $f(X) = (X - (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3}))(X + (\sqrt{2} + \sqrt{3}))(X + (\sqrt{2} - \sqrt{3}))$ (1)
y como los factores y sus productos tomados de a dos no son polinomios de $Q[X]$, $f(X)$ es irreducible en $Q[X]$. Veamos que $f(X)$ es reducible sobre cualquier $Z_p$.

Lema. Si a y b elementos de un grupo cíclico G no son cuadrados, su producto es un cuadrado.

De aquí se deduce que en cualquier $Z_p$ uno de los elementos 2, 3 ó 6 es un cuadrado, es decir 2, 3 ó 6 es congruente con un cuadrado módulo p.
En efecto, si $p = 2$ ó 3, $2 \equiv 0 \pmod 2$ ó $3 \equiv 0 \pmod 3$. Si $p = 5$, $6 \equiv 1 \pmod 5$ y si $p > 5$, por el lema 2, 3 ó 6 es un cuadrado.
Si $2 = a^2$ entonces multiplicando en (1) se tiene que $f(X) = (X^2+2aX-1)(X^2-2aX-1)$.
Si $3 = a^2$, $f(X) = (X^2+2aX+1)(X^2-2aX+1)$. Finalmente si $6 = a^2$, $f(X) = (X^2-5+2a)$. $(X^2-5-2a)$.

## RAICES DE POLINOMIOS.

Si K es un cuerpo, todo cuerpo E que contiene a K como subcuerpo se llama una extensión de K. Escribiremos $K \subset E$ para significar que E es una extensión de K.
Es claro que si $K \subset E$, $K[X] \subset E[X]$. Dado un polinomio $f(X) = \sum_{i=0}^{n} c_i X^i \in K[X]$ un elemento $a \in E$ se dice una raíz de $f(X)$ si $f(a) = \sum_{i=0}^{n} c_i a^i = 0$.

TEOREMA 1.3. (del resto). Si $f(X) \in K[X]$ y $a \in K$, el resto de dividir $f(X)$ por $X - a$ es $f(a)$.

Como consecuencia, cualquiera sea $f(X) \in K[X]$, $a \in K$ es raíz de $f(X)$ si y sólo si $X - a \mid f(X)$.

Raíces múltiples. Si $f(X) \in K[X]$ y $a \in K$ es una raíz de f entonces se puede escribir $f(X) = (X - a)^m . g(X)$ donde $g(X) \in K[X]$ y $X - a \nmid g(X)$ (o lo que es equivalente, $g(a) \neq 0$). Es claro que $m \geq 1$.

El número natural m se llama el orden de multiplicidad de la raíz a. Si $m = 1$ a se dice simple y si $m > 1$ a se dice una raíz múltiple.

TEOREMA 1.4. Un polinomio $f(X) \in K[X]$ de grado $n \geq 1$ tiene a lo sumo n raíces en K, contando cada raíz tantas veces como su orden de multiplicidad.

Demostración. Si $a_1,\ldots,a_s$ son raíces distintas de f(X) en K de órdenes de multiplicidad $m_1,\ldots,m_s$ respectivamente, razonando por inducción se ve que f(X) es divisible por $(X-a_1)^{m_1} \ldots (X-a_s)^{m_s}$ de donde sigue que $m_1 + \ldots + m_s \leq n$.

Usando este teorema se puede demostrar que:

TEOREMA 1.5. Si K es un cuerpo, todo subgrupo finito U del grupo multiplicativo K* es cíclico. En particular, si K es un cuerpo finito, K* es un grupo cíclico.

Demostración. Sea $U \subset K^*$ un subgrupo finito de orden n, $U = U_{p_1} \times \ldots \times U_{p_r}$ su descomposición en las componentes primarias. Basta ver que $U_{p_i}$ es cíclico para todo i. Sea entonces U un p-grupo abeliano de orden $p^t$ y a un elemento de orden máximo entre los de U, orden de $a = p^e$. Entonces como orden de x / orden de a cualquiera sea $x \in U$, es $x^{p^e} = 1$, para todo $x \in U$.
Por otro lado, el número de raíces del polinomio $X^{p^e} - 1 \in K[X]$ es $\leq p^e \Rightarrow$
$\Rightarrow p^t \leq p^e \Rightarrow p^t = p^e \Rightarrow U = (a)$.

En particular, si p es primo, $Z_p^*$ es un grupo cíclico.

Polinomio derivado. Dado $f(X) = \sum_{i=0}^{n} a_i X^i$ se llama polinomio derivado de f(X) al polinomio $f'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$. Valen las siguientes propiedades:

1) $(f + g)' = f' + g'$

2) $(f.g)' = f'.g + f.g'$.

Observación. Para la comprensión del significado del teorema que sigue conviene tener presente que: a) Si $f,g \in K[X]$, el m.c.d.$(f,g) = D(X)$ se puede calcular

por el algoritmo de Euclides, es decir por divisiones sucesivas. Dada la unicidad del cociente y el resto, éstos son los mismos aunque se considere una extensión $K \subset E$, se piense a f y g como polinomiosde $E[X]$ y se haga la división entera en $E[X]$.Luego el m.c.d. $D(X)$ no depende del cuerpo al que se consideren pertenecientes los coeficientes de f y g.

b) Más adelante se demostrará que para cualquier polinomio no constante de $K[X]$ existe una extensión $E \supset K$ en la que el polinomio tiene por lo menos una raíz.

Escribiremos $(f,g) = \text{m.c.d.}(f,g)$.

TEOREMA 1.6. Sea $f(X) \in K[X]$, gr $f \geq 1$. Entonces

1) $a \in K$ es raíz múltiple de $f(X) \iff a$ es raíz de $f(X)$ y de $f'(X) \iff X-a/(f,f') \iff a$ es raíz de $(f,f')$.

2) Todas las raíces de $f(X)$ son simples si y sólo si $(f,f') = 1$.

3) Si $f(X)$ es irreducible, todas las raíces de $f(X)$ son simples si y sólo si $f'(X) \neq 0$.

4) Si car $K = 0$ entonces $f'(X) \neq 0$. Si car $K = p \neq 0$, entonces $f'(X) = 0$ si y sólo si $f(X) = h(X^p)$ con h un polinomio de $K[X]$. Si $f(X)$ es irreducible, h es irreducible y $f(X)$ se puede escribir $f(X) = t(X^{p^e})$, $e > 0$, donde t es un polinomio irreducible con raíces simples, y todas las raíces de f tienen multiplicidad $p^e$. (Si $\alpha_1,\ldots,\alpha_s$ son las raíces distintas de f, $\alpha_1^{p^e},\ldots,\alpha_s^{p^e}$ son las raíces de t).

Demostración. 1) Si $f(X) = (X-a)^m.g(X)$ con $X - a \nmid g(X)$, $f'(X) =$

$= m(X-a)^{m-1}g(X) + (X-a)^m g'(X) = (X-a)^{m-1}\underbrace{(mg(X) + (X-a)g'(X))}_{h(x)}$ con $X-a \nmid h$, de

donde sigue que $X-a \mid f$ y $X-a \mid f'$ si y sólo si $m > 1$.

2) $\Leftarrow$ es inmediato por 1). $\Rightarrow$ : Si $D(X) = (f,f') \neq 1$ en alguna extensión E de K $D(X)$ tiene una raíz. Si $a \in E$ es raíz de $D(X)$, $X-a \mid D = X-a \mid f$ y $X-a \mid f'$ $\Rightarrow$ a es raíz múltiple de f, contradicción.

3) Sea f irreducible; todas las raíces de f simples $\iff (f,f') = 1 \iff$ $\iff f'(X) \neq 0$.

4) Si car K = 0, como gr f $\geq$ 1 es claro que f'(X) $\neq$ 0. Si car K = p $\neq$ 0, $f'(X) = 0 \Rightarrow \sum_{i=1}^{n} i a_i X^{i-1} = 0 \Rightarrow i a_i = 0,\ 1 \leq i \leq n \Rightarrow i.1_K = 0$ o $a_i = 0 \Rightarrow$ $\Rightarrow p / i$ o $a_i = 0 \Rightarrow f(X) = \sum_{i=0}^{n} a_i X^{pk_i}$ y $f(X) = h(X^p)$ con $h(X) = \sum_{a_i \neq 0} a_i X^{k_i}$. La recíproca es trivial.

Si f(X) es irreducible y f'(X) = 0, es $f(X) = h(X^p)$ con h de grado menor que el de f e irreducible pues $h = h_1.h_2 \Rightarrow h(X^p) = h_1(X^p).h_2(X^p)$. Las raíces de h pueden ser todas simples o haber múltiples. En este último caso $h'(X) = 0 \Rightarrow$ $\Rightarrow h(X) = g(X^p)$ con g irreducible $\Rightarrow f(X) = g(X^{p^2})$. Iterando el razonamiento resulta $f(X) = t(X^{p^e})$ con t irreducible con todas las raíces simples $\Rightarrow$ todas las raíces de f son múltiples de orden $p^e$: a raíz de f $\Rightarrow 0 = f(a) = t(a^{p^e}) \Rightarrow$ $\Rightarrow a^{p^e}$ es raíz de t $\Rightarrow t(X) = (X-a^{p^e}).t_1(X)$ con $X-a^{p^e} \not| t_1 \Rightarrow f(X) = t(X^{p^e}) =$ $= (X^{p^e}-a^{p^e}).t_1(X^{p^e}) = (X-a)^{p^e}.t_1(X^{p^e}) \Rightarrow$ a es raíz $p^e$-múltiple, pues si fuera raíz de $t_1(X^{p^e})$ sería $t_1(a^{p^e}) = 0$ y se tendría $X-a^{p^e} / t_1$, contradicción.

EJERCICIOS

1) Probar que los polinomios $X^4 + 1$ y $X^6 + X^3 + 1$ son irreducibles sobre los racionales.

2) Escribir todos los polinomios irreducibles en $Z_2[X]$ de 2º, 3º y 4º grados.

3) Decir si $X^5+X+1$ y $X^6+X^3+1$ son irreducibles en $Z_2[X]$.

4) Decir si $4X^4+10X^3+X^2+23$ y $\frac{1}{3}X^3+6X+\frac{7}{2}$ son irreducibles sobre Q.

5) a) Sea A un dominio de integridad, a,b elementos de A, a inversible. Demostrar que la aplicación $X \to aX+b$ se extiende a un único automorfismo de A[X] que induce la identidad sobre A. ¿Cuál es el automorfismo inverso?.

   b) Demostrar que todo automorfismo de A[X] que restringido a A da la identidad es de la forma indicada en a).

6) Sea A un dominio de integridad, K su cuerpo de cocientes. Demostrar que en el cuerpo de cocientes K(X) de A[X] todo automorfismo de K(X) que induce la iden

tidad en K es del tipo $X \to \frac{aX+b}{cX+d}$ , $a,b,c,d \in K$, tal que $\frac{aX+b}{cX+d} \notin K$, o lo que es equivalente $ad - bc \neq 0$.

7) (Resultante). Sea K un cuerpo, $f(X) = \sum_0^m a_i X^i$ , $g(X) = \sum_0^n b_j X^j$ donde $a_m \neq 0$ o $b_n \neq 0$. Probar que f(X) y g(X) tienen un factor común de grado $\geq 1$ si y sólo si existen u(X), v(X) $\in K[X]$ no nulos simultáneamente, tales que $u(X).f(X) = v(X).g(X)$ con gr $u < n$ y gr $v < m$. Poniendo $u(X) = \sum_0^{n-1} u_j X^j$, $v(X) = \sum_0^{m-1} v_i X^i$, describir las m+n ecuaciones lineales en $u_j$, $v_i$ que se satisfacen si y sólo si $u(X)f(X) = v(X)g(X)$. Concluir que f(X) y g(X) tienen un factor común de grado $\geq 1$ si y sólo si el siguiente determinante de orden m+n, llamado la resultante de f y g, se anula:

$$\begin{vmatrix}
a_m & a_{m-1} & \cdots & & a_0 & & \\
 & a_m & a_{m-1} & \cdots & & a_0 & \\
 & & \ddots & \ddots & & & \ddots \\
 & & & a_m & a_{m-1} & \cdots & a_0 \\
b_n & b_{n-1} & \cdots & b_1 & b_0 & & \\
 & b_n & b_{n-1} & \cdots & b_1 & b_0 & \\
 & & \ddots & \ddots & & & \ddots \\
 & & & b_n & b_{n-1} & \cdots & b_1 \quad b_0
\end{vmatrix}$$

8) Interpretar la anulación del siguiente determinante de acuerdo con el ejercicio anterior:

$$\begin{vmatrix}
1 & 0 & -4 & 0 & 0 \\
0 & 1 & 0 & -4 & 0 \\
0 & 0 & 1 & 0 & -4 \\
1 & -2 & 1 & -2 & 0 \\
0 & 1 & -2 & 1 & -2
\end{vmatrix}$$

# CAPITULO II

## EXTENSIONES

Si K es un cuerpo, un cuerpo E se dice una extensión de K si E contiene a K como un subcuerpo. Se escribe $K \subset E$.
Si $K \subset E$, E se puede considerar como un K-espacio vectorial. La dimensión de este espacio se llama el grado de la extensión E sobre K y se nota $[E:K]$. E se dice una extensión finita o infinita de K según que $[E:K]$ sea finito o no. Si $[E:K] = n$, E se dice una extensión de grado n de K.

Es clara la transitividad de extensiones: Si $K \subset E$ y $E \subset F$ entonces $K \subset F$. Se escribe $K \subset E \subset F$.

Ejemplos. 1) $Q \subset R$, $R \subset C$, $Q \subset C$. $[C:R] = 2$; $[R:Q]$ y $[C:Q]$ son infinitos.

2) $Q \subset Q(X) \subset R(X) \subset C(X)$, donde $Q(X)$, $R(X)$, $C(X)$ son los cuerpos de cocientes de los anillos de polinomios $Q[X]$, $R[X]$, $C[X]$. Son todas extensiones infinitas, excepto $C(X)$ que es una extensión de grado 2 de $R(X)$.

Dada una extensión $K \subset E$, veamos cómo construir extensiones intermedias F: $K \subset F \subset E$.
Si $A \neq \emptyset$ es un subconjunto de E, el subanillo de E generado por K y A, es decir el menor subanillo de E que contiene a K y a A, se representa $K[A]$. El subcuerpo de E generado por K y A se escribe $K(A)$ y es el cuerpo de cocientes de $K[A]$. Así se construye una extensión intermedia: $K \subset K(A) \subset E$.
Si A es un conjunto finito, $A = \{a_1,\ldots,a_m\}$, $K[A]$ ( $K(A)$) se escribe $K[a_1,\ldots,a_m]$ ( $K(a_1,\ldots,a_m)$ ).

TEOREMA 2.1. Si $K \subset E$ y $A \neq \emptyset$ es un subconjunto de E entonces:

a) $K[A] = \{f(a_1,\ldots,a_n): n \in N,\ f \in K[X_1,\ldots,X_n],\ a_1,\ldots,a_n \in A\}$.

En particular, si A es un subanillo de E (conteniendo a la unidad de E), entonces $K[A]$ está formado por todas las sumas finitas $\Sigma\, k_i a_i$, $k_i \in K$, $a_i \in A$.

b) $K(A) = \{\frac{u}{v} : u,v \in K[A],\ v \neq 0\} = \{\frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)} : n \in N,\ f,g \in K[X_1,\ldots,X_n],$ $a_1,\ldots,a_n \in A,\ g(a_1,\ldots,a_n) \neq 0\}$.

En particular:

c) Si A es un conjunto finito, $A = \{a_1,\ldots,a_m\}$ entonces

$K[a_1,\ldots,a_m] = \{f(a_1,\ldots,a_m) : f \in K[X_1,\ldots,X_m]\}$.

$K(a_1,\ldots,a_m) = \{\frac{f(a_1,\ldots,a_m)}{g(a_1,\ldots,a_m)} : f,g \in K[X_1,\ldots,X_m],\ g(a_1,\ldots,a_m) \neq 0\}$.

d) Si $A = \{a\}$ entonces

$K[a] = \{f(a) : f \in K[X]\}$

$K(a) = \{\frac{f(a)}{g(a)} : f,g \in K[X],\ g(a) \neq 0\}$.

Demostración. Ejercicio.

Ejemplos. $Q \subset Q(\sqrt{2}) \subset R$ ; $Q \subset Q(\sqrt{2},\sqrt{3}) \subset C$ ; $R(i) = C$.

Se dice que la extensión $K(a_1,\ldots,a_m)$ se obtiene por adjunción a K de los elementos $a_1,\ldots,a_m$. Una extensión K(a) de K que se obtiene adjuntando un solo elemento se dice una extensión simple de K.

Ejercicio. 1) $Q(\sqrt{2},\sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$.

2) a) Sea $K \subset E$, $u,v \in E$. Demostrar que $K(u,v) = K(u)(v) = K(v)(u)$.

b) En general, si $K \subset E$ y A y B son subconjuntos de E se tiene que $K(A \cup B) = K(A)(B) = K(B)(A)$.

TEOREMA 2.2. Si K es un cuerpo y $K \subset L \subset F$ entonces

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

Si $\{a_i\}_{i\in I}$ es una base de E sobre K y $\{b_j\}_{j\in J}$ es una base de F sobre E entonces $\{a_i b_j\}_{(i,j)\in I\times J}$ es una base de F sobre K.

Demostración. Ejercicio.

COROLARIO. Si $K \subset E \subset F$, F es finita sobre K si y sólo si F es finita sobre E y E es finita sobre K.

Si K es un cuerpo y $K \subset E$, interesan los elementos de E que son raíces de polinomios con coeficientes en K.

DEFINICION. Si $K \subset E$, un elemento $\alpha \in E$ se dice algebraico sobre K si existen elementos $a_0, a_1, \ldots, a_n \in K$, no todos nulos, tales que

$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ , es decir

$\alpha$ algebraico sobre K $\iff$ existe $f(X) \in K[X]$ no nulo tal que $f(\alpha) = 0$.

Si $\alpha$ no es algebraico sobre K, se dice trascendente sobre K.

Ejemplos.

1) $i \in C$ es algebraico sobre Q y R.
2) $\sqrt[6]{3} \in R$ es algebraico sobre Q. Los números complejos que son algebraicos sobre Q se llaman números algebraicos.
3) Todo $\alpha \in K$ es algebraico sobre K.
4) Si $\varepsilon$ es una raíz n-ésima de la unidad entonces $\varepsilon$ es algebraico sobre cualquier cuerpo de números K ya que $X^n - 1 \in K[X]$.
5) e es trascendente sobre Q (Hermite) y $\pi$ es trascendente sobre Q (Lindemann). También lo son los números de la forma $\alpha^\beta$, con $\alpha$ algebraico y $\beta$ algebraico irracional.

Sea $K \subset E$, $\alpha \in E$. Consideremos $\varphi: K[X] \to E$ la aplicación definida como sigue: $\varphi(f) = f(\alpha)$, cualquiera sea $f \in K[X]$.
$\varphi$ es un homomorfismo de anillos, su imagen es $K[\alpha]$ y su núcleo, que es un ideal de K[X], es el conjunto de todos los polinomios de K[X] que se anulan en $\alpha$, es decir, que tienen a $\alpha$ como raíz.

$$K[X]/\mathrm{Nuc}\,\varphi \cong K[\alpha] .$$

Como $K[X]$ es un dominio principal, $\text{Nuc}\,\varphi$ es un ideal principal.
Si $\text{Nuc}\,\varphi = (0)$ entonces $\alpha$ es trascendente sobre $K$ y $K[X] \cong K[\alpha]$.
Si $\text{Nuc}\,\varphi \neq 0$, $\alpha$ es algebraico sobre $K$ y $\text{Nuc}\,\varphi = (f_0)$ con $f_0 \neq 0$. Podemos suponer $f_0$ mónico.

$K[X]/(f_0) \cong K[\alpha]$ dominio de integridad $\Rightarrow$ $(f_0)$ ideal primo $\Rightarrow$ $f_0$ irreducible en $K[X]$ $\Rightarrow$ $K[X]/(f_0) \cong K[\alpha]$ cuerpo $\Rightarrow$ $K[\alpha] = K(\alpha)$.

Es claro que $\text{Nuc}\,\varphi \neq (0) \iff \alpha$ algebraico.

El polinomio irreducible mónico $f_0$ está unívocamente determinado por $\alpha$ y se llama el polinomio minimal de $\alpha$ sobre $K$. Si $\text{gr}\, f_0 = n$, $\alpha$ se dice algebraico sobre $K$ de grado $n$.

TEOREMA 2.3. Si $K \subset E$ y $\alpha \in E$ es algebraico sobre $K$ entonces:

a) Existe un polinomio irreducible mónico único $f \in K[X]$ tal que $f(\alpha) = 0$.

b) Cualquiera sea $g \in K[X]$, $g(\alpha) = 0$ si y sólo si $f/g$.

c) $K[\alpha] = K(\alpha)$.

d) Si $\text{gr}\, f = n$, $[K(\alpha): K] = n$ y $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)$ sobre $K$.

Demostración. a),b) y c) siguen del razonamiento anterior. Queda propuesta la demostración de d) como ejercicio.

Ejemplos.

1) $\sqrt{2}$ es algebraico sobre $Q$, su polinomio minimal es $X^2-2$, $[Q(\sqrt{2}):Q] = 2$ y una base de $Q(\sqrt{2})$ sobre $Q$ es $1, \sqrt{2}$; luego los elementos de $Q(\sqrt{2})$ son los números de la forma $q_1 + q_2\sqrt{2}$, $q_1, q_2 \in Q$.

2) $\alpha$ algebraico sobre $K$ de grado $1$ $\iff$ $\alpha \in K$.

3) $X^4-X^2+1$ es irreducible sobre $Q$. Si $\alpha \in C$ es una raíz, $[Q(\alpha):Q] = 4$ y $Q(\alpha) = \{q_0 + q_1\alpha + q_2\alpha^2 + q_3\alpha^3 : q_i \in Q\}$.

4) Si $\varepsilon \in C$ es una raíz cúbica primitiva de $1$, $X^2+X+1$ es su polinomio minimal sobre $Q$, $[Q(\varepsilon):Q] = 2$ y $Q(\varepsilon) = \{q_1 + q_2\varepsilon : q_1, q_2 \in Q\}$.

$X^2+X+1$ se llama el polinomio ciclotómico de orden 3. En general, si $n \in N$, $f_n(X) = \Pi(X-\varepsilon_i)$ donde $\varepsilon_i$ son las raíces n-ésimas primitivas de la unidad se llama el polinomio ciclotómico de orden n.

Más adelante probaremos que $f_n(X)$ es un polinomio con coeficientes enteros irreducible sobre Q, de donde resulta que $f_n(X)$ es el polinomio minimal de cualquier raíz n-ésima primitiva $\varepsilon$ de la unidad y que $[Q(\varepsilon):Q] = \phi(n)$.($\phi(n)$ = = número de números naturales $\leq$ que n y primos con n). $Q(\varepsilon)$ se llama el cuerpo ciclotómico de orden n.

En particular, si n = p primo, $f_p(X) = X^{p-1} + \ldots + X + 1$ , $[Q(\varepsilon_p):Q] = p-1$.

Si $K \subset E \subset F$ y $\alpha \in F$ es algebraico sobre K, entonces es algebraico sobre E y el polinomio minimal de $\alpha$ sobre E divide al polinomio minimal sobre K.

Ejemplo. $Q \subset Q(\sqrt{2}) \subset Q(\sqrt[4]{2})$.

$\sqrt[4]{2}$ es algebraico sobre Q y sobre $Q(\sqrt{2})$. Sobre Q el polinomio minimal es $X^4-2$. Pero este polinomio no es irreducible en $Q(\sqrt{2})[X]$ pues $X^4-2 = (X^2-\sqrt{2})(X^2+\sqrt{2})$. El polinomio minimal sobre $Q(\sqrt{2})$ es $X^2-\sqrt{2}$.

DEFINICION. Una extensión $K \subset E$ se dice algebraica si todo elemento $\alpha \in E$ es algebraico sobre K. En caso contrario E se dice una extensión trascendente de K, o sea, si existe algún elemento de E que es trascendente sobre K.

Ejemplos.

1) C es una extensión algebraica de R; cualquiera sea $a+bi \in C$ es raíz del polinomio $X^2-2aX+a^2+b^2 \in R[X]$.

2) $Q(\sqrt{2})$ es una extensión algebraica de Q pues cualquiera sea $q_1+q_2\sqrt{2}$ es raíz de $X^2-2q_1X+q_1^2-2q_2^2 \in Q[X]$.

3) $Q \subset R$ es trascendente.

TEOREMA 2.4. Toda extensión finita E de K es algebraica. Si $[E:K] = n$ todo elemento de E es raíz de un polinomio de grado $\leq n$ con coeficientes en K.

Demostración. Sea $\alpha \in E$. Como $[E:K] = n$, $1,\alpha,\ldots,\alpha^n$ son linealmente dependientes sobre K, luego $\alpha$ es raíz de un polinomio $\in K[X]$ de grado $\leqslant n$. Entonces $\alpha$ es algebraico sobre K.

(Observar que como $K \subset K(\alpha) \subset E$, el grado de $\alpha$ sobre K divide a n).

COROLARIO. $\alpha$ es algebraico sobre K $\iff$ $K(\alpha)$ es una extensión finita de K.

La recíproca del teorema no es verdadera: No toda extensión algebraica es finita. Por ejemplo, más adelante veremos que el subconjunto $\overline{Q} \subset C$ formado por las raíces de todos los polinomios con coeficientes racionales es un subcuerpo de C, y $\overline{Q}$ es claramente una extensión algebraica de Q: $Q \subset \overline{Q}$. Si fuera $[\overline{Q}:Q] = n$ finito entonces todo polinomio irreducible de Q[X] tendría grado $\leqslant n$, absurdo puesto que hay polinomios irreducibles sobre Q de grados arbitrariamente grandes.

Ejemplo. Consideremos el polinomio $f(X) = X^3+X+1$, irreducible sobre Q. Si $\alpha$ es una raíz de f(X), $[Q(\alpha):Q] = 3$. Todos los elementos de $Q(\alpha)$ son algebraicos sobre Q. Si $\beta \in Q(\alpha)$ , $\beta \neq \alpha$, ¿cuál es el polinomio minimal de $\beta$?. Si $\beta \in Q$, es $X-\beta$. Si $\beta \notin Q$, de $Q \subset Q(\beta) \subset Q(\alpha)$ sigue que $[Q(\beta):Q] = 3$, luego el polinomio minimal de $\beta$ es de grado 3: $X^3 + q_2X^2 + q_1X + q_0$. Una base de $Q(\alpha)$ es $1,\alpha,\alpha^2$ y $\beta$ se escribe como combinación lineal de estos elementos.
Por ejemplo, supongamos $\beta = 1+2\alpha^2$. Entonces como $\alpha^3 = -\alpha-1$ , $\alpha^4 = -\alpha^2-\alpha$ , es $\beta^2 = 1+4\alpha^2+4\alpha^4 = 1+4\alpha^2-4\alpha^2-4\alpha = 1-4\alpha$ ; $\beta^3 = \beta^2.\beta = 2\alpha^2+4\alpha+9$. Reemplazando en el polinomio minimal, $2\alpha^2+4\alpha+9+q_2(1-4\alpha)+q_1(1+2\alpha^2)+q_0 = 0$.

$(2+2q_1)\alpha^2+(4-4q_2)\alpha+9+q_2+q_1+q_0 = 0 \Rightarrow q_1 = -1$ , $q_2 = 1$ , $q_0 = -9$.

Luego $X^3+X^2-X-9$ es el polinomio minimal de $\beta$ sobre Q.

DEFINICION. Sea $K \subset E$. Se dice que E es una extensión finitamente generada de K si existe un número finito de elementos $\alpha_1,\alpha_2,\ldots,\alpha_n \in E$ tales que $E = K(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Es claro que toda extensión finita E de K es finitamente generada pues si $\{\beta_1,\ldots,\beta_t\}$ es una K-base de E, entonces $E = K(\beta_1,\ldots,\beta_t)$.

La recíproca no vale. Por ejemplo, $K \subset K(X)$ no es una extensión finita.

TEOREMA 2.5. Si $K \subset E$, E es una extensión finita de K si y sólo si E es finitamente generada sobre K por elementos algebraicos, es decir, si y sólo si $E = K(\alpha_1,\ldots,\alpha_n)$ con $\alpha_1,\ldots,\alpha_n$ algebraicos sobre K.

Demostración. $K \subset E$ finita $\Rightarrow$ E algebraica y f.g. $\Rightarrow$ existen $\alpha_1,\ldots,\alpha_n \in E$ algebraicos tales que $E = K(\alpha_1,\ldots,\alpha_n)$.

Recíprocamente, sea $K \subset E$, $E = K(\alpha_1,\ldots,\alpha_n)$, $\alpha_i$ algebraico sobre K, $1 \leqslant i \leqslant n$. Por inducción sobre n. Si $n = 1$, $\alpha$ algebraico sobre K implica $[K(\alpha):K] < \infty$. Sea $n > 1$, y supongamos $[K(\alpha_1,\ldots,\alpha_{n-1}):K] < \infty$. Como $\alpha_n$ es algebraico sobre K, es algebraico sobre $K(\alpha_1,\ldots,\alpha_{n-1})$ $\Rightarrow$ $K(\alpha_1,\ldots,\alpha_{n-1})(\alpha_n)$ es una extensión finita de $K(\alpha_1,\ldots,\alpha_{n-1})$. De $K \subset K(\alpha_1,\ldots,\alpha_{n-1}) \subset K(\alpha_1,\ldots,\alpha_{n-1})(\alpha_n) = E$ se tiene

$$[E:K] = [E:K(\alpha_1,\ldots,\alpha_{n-1})] \cdot [K(\alpha_1,\ldots,\alpha_{n-1}):K] ,$$

de donde sigue que [E:K] es finito.

Entonces, algebraica $\not\Leftarrow$ finita $\Leftrightarrow$ f.g. por elementos algebraicos.

TEOREMA 2.6. (Transitividad de extensiones algebraicas)
Si $K \subset E \subset F$, F es algebraica sobre K si y sólo si F es algebraica sobre E y E es algebraica sobre K.

Demostración. ( $\Rightarrow$ ) Trivial.
( $\Leftarrow$ ) Si $\alpha \in F$, sea $f(X) = c_0 + c_1X + \ldots + X^n \in E[X]$ su polinomio minimal sobre E. Entonces $\alpha$ es algebraico sobre $K(c_0,\ldots,c_{n-1})$ $\Rightarrow$
$[K(c_0,\ldots,c_{n-1})(\alpha) : K(c_0,\ldots,c_{n-1})] < \infty$. Como $K(c_0,\ldots,c_{n-1})$ es f.g. sobre K por elementos algebraicos, es una extensión finita de K. Luego
$[K(c_0,\ldots,c_{n-1})(\alpha) : K(c_0,\ldots,c_{n-1})] \cdot [K(c_0,\ldots,c_{n-1}):K] < \infty$ $\Rightarrow$
$[K(c_0,\ldots,c_{n-1})(\alpha) : K] < \infty$ $\Rightarrow$ $\alpha$ algebraico sobre K.

TEOREMA 2.7. Sea $K \subset E$.

a) Si $\alpha,\beta \in E$ son algebraicos sobre K entonces $\alpha \pm \beta$ , $\alpha.\beta$ y $\alpha.\beta^{-1}$ $(\beta \neq 0)$ son algebraicos sobre K.

b) El conjunto L de todos los elementos de E que son algebraicos sobre K es un subcuerpo de E: $K \subset L \subset E$.

Demostración. a) $\alpha,\beta \in E$ algebraicos sobre K $\Rightarrow$ $K(\alpha,\beta)$ algebraica sobre K. Como $\alpha \pm \beta$ , $\alpha.\beta$ , $\alpha.\beta^{-1} \in K(\alpha,\beta)$, son algebraicos sobre K.

b) Sigue de a).

DEFINICION. L se llama la clausura algebraica de K en E.

Es claro que L es una extensión algebraica de K y es la mayor de las extensiones algebraicas de K contenidas en E.

EJERCICIOS.

1) Si [E:K] es un número primo, decir cuántos subcuerpos intermedios hay entre K y E.

2) Demostrar que $Q(\sqrt{2},\sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$ y hallar $[Q(\sqrt{2},\sqrt{3}):Q]$.

3) Hallar el polinomio minimal sobre Q de cada uno de los siguientes números:

$$\sqrt[3]{6} \quad , \quad 3i \quad , \quad 1+\sqrt{3} \quad , \quad \sqrt[5]{3}\,i \quad , \quad \sqrt{2}+\sqrt{3} \quad , \quad \sqrt[3]{2}+\sqrt[3]{4}$$

$\varepsilon$ = raíz primitiva de la unidad de orden primo p.
Indicar una base de cada una de las extensiones simples de Q que se obtienen por adjunción de cada uno de esos números, e indicar la forma de sus elementos.

4) Sea $E = Q(u)$ donde $u^3-u^2+u+2 = 0$. Expresar $(u^2+u+1)(u^2-u)$ y $(u-1)^{-1}$ en la forma $au^2+bu+c$ , $a,b,c \in Q$.

5) Hallar el grado de las siguientes extensiones e indicar una base de las finitas:

$Q \subset C$ ; $R \subset R(\sqrt{5})$ : $Z_5 \subset Z_5(X)$ ; $Q \subset Q(\sqrt{2},\sqrt[3]{10})$ ; $Q \subset Q(\sqrt{2},\sqrt{5},\sqrt{11})$ ; $Q(\sqrt{3}) \subset Q(\sqrt[6]{3})$ ; $Q(\varepsilon) \subset Q(i,\sqrt{3})$ siendo $\varepsilon^3 = 1$ , $\varepsilon \neq 1$.

6) Sea $\omega = e^{\pi i/6}$. Probar que $[Q(\omega):Q] = 4$ y hallar el polinomio minimal de $\omega$ sobre Q.

7) Sea $K \subset E$ una extensión finita y $f \in K[X]$ un polinomio irreducible. Si gr $f > 1$ y es relativamente primo con $[E:K]$ entonces f no tiene ninguna raíz en E.

8) Si $K \subset E$ es una extensión de grado primo entonces es simple.

9) Si $K \subset E$ y $\alpha \in E$ es algebraico de grado impar sobre K entonces $K(\alpha) = K(\alpha^2)$.

10) Sea $E = K(u)$, u trascendente, y $K \subsetneq F \subset E$. Mostrar que u es algebraico sobre F.

11) Sea $\alpha$ una raíz del polinomio irreducible sobre K $X^n - a$ y supongamos que m/n. Probar que el grado de $\alpha^m$ sobre K es $\frac{n}{m}$. ¿Cuál es el polinomio minimal de $\alpha^m$ sobre K?.

12) Sea $K \subset E$ una extensión algebraica y A un subanillo tal que $K \subset A \subset E$. Probar que A es un cuerpo. Concluir que todo subanillo de una extensión finita de K es un subcuerpo.

13) Sean E y F dos extensiones de K contenidas ambas en un cuerpo L, E.F el menor subcuerpo de L que contiene a E y a F. Sea A el conjunto de todas las sumas (finitas) $\Sigma e_i f_i$ , $e_i \in E$, $f_i \in F$.

a) Probar que A es un subanillo.
b) Probar que E.F es el cuerpo de cocientes de A.
c) Si E y F son algebraicas sobre K entonces A = E.F y E.F es una extensión algebraica de K.

14) Sean $K \subset E$ y $K \subset F$ dos extensiones de K, ambas contenidas en una extensión L de K, de grados m y n sobre K relativamente primos. Probar que:

$$E \cap F = K \qquad y \qquad [L.F:K] = m.n$$

15) Sea $f(X) \in K[X]$ de grado n irreducible sobre K y E una extensión de K de grado m, $(m,n) = 1$. Demostrar que f es irreducible sobre E.

16) Para cuáles de los siguientes polinomios f(X) existen extensiones $K(\alpha)$ de K tales que f es el polinomio minimal de $\alpha$?:

a) $X^3 - 7$ , $K = R$ b) $X^2 + 1$ , $K = Z_3$

c) $X^7-3X^6+4X^3-X-1$ , $K = R$ d) $X^3-X+1$ , $K = Q$.

17) Sea K un cuerpo de característica $\neq 2$ y f(X) un polinomio cuadrático sobre K. Probar que f(X) tiene ambas raíces en una extensión $K(\alpha)$, con $\alpha^2 \in K$. De modo que si K contiene a las "raíces cuadradas" de todos sus elementos, todos los polinomios de 2º grado sobre K tienen dos raíces en K.

18) Mostrar que para cuerpos de característica 2 existen ecuaciones cuadráticas que no pueden resolverse adjuntando raíces cuadradas de elementos del cuerpo.

19) Sea $K = Z_3$. Encontrar todos los polinomios cuadráticos irreducibles sobre K y para cada uno de ellos todas las extensiones $K(\alpha)$, siendo $\alpha$ una raíz.

20) Indicar un cuerpo con 8 elementos, dando su estructura multiplicativa.

21) Sea K un cuerpo y C una clase de extensiones de K. Se dice que C es una clase distinguida si satisface las tres propiedades siguientes:

(1) Si $K \subset F \subset E$, la extensión $K \subset E$ está en C si y sólo si las extensiones $K \subset F$ y $F \subset E$ están en C.

(2) Si $K \subset E$ está en C, F es una extensión de K y E, F están contenidos en un mismo cuerpo entonces $F \subset E.F$ está en C.

(3) Si $K \subset F$ y $K \subset E$ están en C y E y F están contenidos en un mismo cuerpo entonces $K \subset E.F$ está en C.

Demostrar que la clase de las extensiones algebraicas de un cuerpo K es distinguida; también lo es la de las extensiones finitas.

22) Decir si es verdadero que:

a) Toda extensión algebraica es finita.
b) Toda extensión trascendente es no finita.
c) Todo elemento de C es algebraico sobre R.
d) Toda extensión de R es finita.
e) Toda extensión algebraica de Q es finita.
f) Toda extensión de un cuerpo finito es finita.
g) $Q(\pi)$ y $Q(e)$ son cuerpos no isomorfos.
h) $Q(\pi)$ es isomorfo a $Q(\pi^2)$.
i) Si E es una extensión trascendente simple de K entonces para cualquier

subcuerpo F tal que $K \subsetneq F \subset E$ es $[E:F] < \infty$.

j) Sea $K \subset K(X)$, donde $K(X)$ es el cuerpo de cocientes del anillo de polinomios $K[X]$. Ningún subcuerpo intermedio $\neq K$ es de dimensión finita sobre $K$.

# CAPITULO III

## CONSTRUCCIONES CON REGLA Y COMPAS

Vamos hacer un paréntesis en el estudio de las extensiones de cuerpos para mostrar una aplicación que pone en evidencia la fuerza de estas ideas.
Nos ocuparemos de un problema muy antiguo: la posibilidad de realizar ciertas construcciones geométricas utilizando solamente la regla (no subdividida) y el compás.
Para los griegos la regla era una tablita sin subdivisiones, concebida para dibujar segmentos de recta, pero no relacionada con la operación de medida.
Con estos dos instrumentos, regla y compás, se pueden hacer muchas construcciones: dibujar perpendiculares, paralelas, dividir un segmento en n partes iguales, bisectar un ángulo, dibujar un cuadrado de área igual o doble a la de un polígono dado, etc. Sin embargo hay construcciones que intuitivamente parecieran posibles y que no lo son.
Los siguientes son tres problemas clásicos famosos no resolubles con regla y compás: 1) duplicación de un cubo; 2) trisección de un ángulo; 3) cuadratura de un círculo.
Los griegos trataron empeñosamente de encontrar estas construcciones sin ser capaces de decidir si eran o no posibles, y la solución de estos problemas ocupó a muchos matemáticos hasta el siglo pasado.
Es relativamente simple ver que no son resolubles usando la noción de extensión algebraica y la multiplicatividad de los grados.

Comenzaremos formulando con precisión qué significa que un problema geométrico sea resoluble con regla y compás.

Sea M un conjunto de puntos del plano euclideo $R^2$, con más de un punto. A partir de M se pueden efectuar los dos siguientes tipos de construcción:

(I) Trazar rectas determinadas por pares de puntos distintos de M. (Regla)

(II) Trazar circunferencias que tienen centro en puntos de M y radios iguales a segmentos de extremos en M. (Compás)

DEFINICION. Sea $M_0$ un conjunto de puntos del plano euclideo $R^2$, con más de un punto. Un punto $P \in R^2$ se dice construible en un paso a partir de $M_0$ si es punto de intersección de dos rectas, de una recta y una circunferencia o de dos circunferencias obtenidas de $M_0$ por (I) o (II).
Un punto $P \in R^2$ se dice construible a partir de $M_0$ si existe una sucesión finita de puntos $P_1, P_2, \ldots, P_n = P$ de $R^2$ tal que $P_1$ es construible en un paso a partir de $M_0$ y para cada $i = 2, \ldots, n$ el punto $P_i$ es construible en un paso a partir del conjunto $M_{i-1} = M_0 \cup \{P_1, \ldots, P_{i-1}\}$.

Se ve claramente que esta definición comprende todas las construcciones geométricas que se pueden hacer con regla y compás en el plano euclideo.

Ejemplo. Construir el punto medio de un segmento dado $\overline{A_1A_2}$. En este caso $M_0 = \{A_1, A_2\}$. El procedimiento es el siguiente:

(1) Trazar la recta determinada por $A_1$ y $A_2$. (I)

(2) Trazar la circunferencia de centro $A_1$ y radio $\overline{A_1A_2}$. (II)

(3) Trazar la circunferencia de centro $A_2$ y radio $\overline{A_1A_2}$. (II)

(4) Sean $P_1$ y $P_2$ los puntos de intersección de las dos circunferencias.

(5) Trazar la recta determinada por $P_1$ y $P_2$. (I)

(6) El punto de intersección P de las rectas $A_1A_2$ y $P_1P_2$ es el punto medio buscado.

La sucesión de puntos $P_1$, $P_2$, P define la construcción pedida a partir de $M_0$.

La teoría de extensiones de cuerpos interviene en forma natural en el problema de las construcciones con regla y compás. Elijamos en $R^2$ un sistema de coordenadas cartesianas tal que $A_1 = (0,0)$ y $A_2 = (1,0)$ con $A_1, A_2 \in M_0$. Con regla y compás se pueden construir con operaciones (I) y (II) perpendiculares y paralelas a una recta por puntos dados. Un punto (x,y) es construible si y sólo si

los puntos $(x,0)$ y $(0,y)$ son construibles. Es fácil ver que si $(x,0)$ , $(y,0)$ son construibles a partir de $M_0$ también lo son los puntos $(0,x)$ , $(x\pm y,0)$ , $(xy,0)$ , $(1/x,0)$ $(x \neq 0)$, y además $(\sqrt{x},0)$ si $x > 0$.
En particular, a partir de los puntos $(0,0)$ y $(1,0)$ pueden construirse todos los puntos de $R^2$ de coordenadas racionales, y a partir de $(0,0)$ y un punto $(x,y)$ distinto del origen pueden construirse todos los puntos con coordenadas en el cuerpo $Q(x,y)$. Más general, si $K_0$ es el subcuerpo de R generado por las coordenadas de los puntos de $M_0$, todos los puntos con coordenadas en $K_0$ son construibles a partir de $M_0$.

Teniendo en cuenta estas observaciones, si $P \in R^2$ es construible a partir de $M_0$ y $P_1,P_2,\ldots,P_n = P$ es una sucesión tal que $P_i$ es construible en un paso a partir del conjunto $M_0 \cup \{P_1,\ldots,P_{i-1}\}$ , para $i = 1,\ldots,n$ , en cada paso de la construcción se considera el subcuerpo de R generado por las coordenadas del punto construido y de los puntos anteriores. Así, dado el conjunto inicial $M_0$, se considera el subcuerpo $K_0 \subset R$ generado por las coordenadas de los puntos de $M_0$; e inductivamente, si $P_i$ tiene coordenadas $(x_i,y_i)$ entonces $K_i = K_{i-1}(x_i,y_i)$, $i = 1,\ldots,n$. Se tiene la siguiente torre de extensiones

$$K_0 \subset K_1 \subset \ldots \subset K_n \subset R$$

Cada punto $P_i$ es intersección de dos rectas (caso A), de una recta y una circunferencia (caso B) o de dos circunferencias (caso C) obtenidas por operaciones (I) o (II) a partir de puntos con coordenadas en $K_{i-1}$. Y es fácil ver que toda recta de este tipo tiene una ecuación de la forma $ax+by+c = 0$ con $a,b,c \in K_{i-1}$, y toda circunferencia de esa clase tiene una ecuación $x^2+y^2+ax+by+c = 0$ con $a,b,c \in K_{i-1}$.

En el caso A el punto de intersección $P_i$ tiene sus coordenadas en el cuerpo $K_{i-1}$, pues ellas son solución de un sistema de dos ecuaciones lineales con coeficientes en $K_{i-1}$, y entonces $K_i = K_{i-1}$; en cambio en los casos B y C aparecen en general radicales cuadráticos pues la resolución del correspondiente sistema de ecuaciones se reduce a la de una ecuación de 2º grado. (Los puntos de intersección de dos circunferencias $x^2+y^2+ax+by+c = 0$ y $x^2+y^2+a'x+b'y+c' = 0$ coinciden con los puntos de intersección de cualquiera de ellas con la recta $(a-a')x + (b-b')y + (c-c') = 0$). Luego $P_i$ tiene sus coordenadas en un cuerpo

$K_{i-1}(\sqrt{u})$ con $u \in K_{i-1}$, y $K_i = K_{i-1}(\sqrt{u})$.

En conclusión, si un punto P(x,y) es construible con regla y compás a partir de $M_0$, sus coordenadas x, y pertenecen a $K_0$ o a un cuerpo F que se obtiene a partir de $K_0$ mediante extensiones cuadráticas sucesivas:

$$K_0 = F_0 \subset F_1 \subset \ldots \subset F_t = F$$

donde $F_i = F_{i-1}(\alpha_i)$ con $\alpha_i^2 \in F_{i-1}$ , $\alpha_i \notin F_{i-1}$ , $i = 1,\ldots,t$.
Luego $[F:K_0] = 2^t$.

Recíprocamente, si P(x,y) es un punto cuyas coordenadas pertenecen a una extensión de $K_0$ del tipo indicado, entonces P es construible a partir de $M_0$ pues todas las operaciones racionales y radicales cuadráticos de las coordenadas dan lugar a puntos que pueden obtenerse mediante construcciones geométricas con regla y compás.

Queda probado así

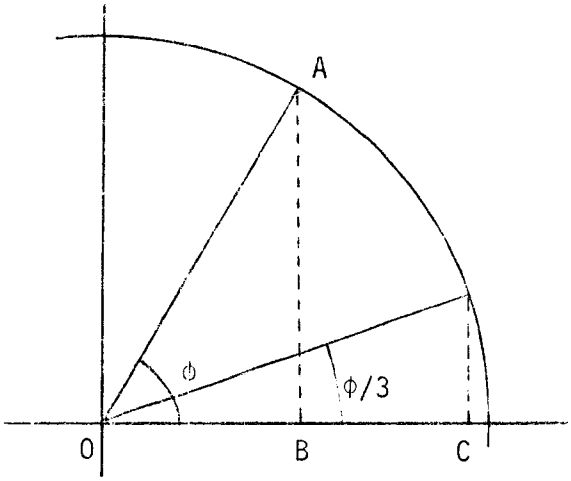
TEOREMA. Un punto P del plano euclideo es construible con regla y compás a partir de un conjunto de puntos $M_0$ si y sólo si las coordenadas de P pertenecen a $K_0$ o a una extensión F de $K_0$ de la forma $F = K_0(\alpha_1,\ldots,\alpha_t)$ con $\alpha_i^2 \in K_0(\alpha_1,\ldots,\alpha_{i-1})$ , $i = 1,\ldots,t$ , siendo $K_0$ el subcuerpo de R generado por las coordenadas de los puntos de $M_0$.

Veremos ahora que no hay solución con regla y compás para los tres problemas clásicos antes mencionados.

Duplicación del cubo. Determinar un cubo cuyo volumen sea el doble del de uno dado.
Podemos tomar la arista del cubo dado como unidad de medida. Consideremos en el plano los puntos (0,0) y (1,0), el cuerpo de base $K_0 = Q$. Resolver el problema con regla y compás consiste en construir un punto P(a,0) tal que $a^3 = 2$, o sea a es raíz del polinomio $X^3-2$. Como este polinomio es irreducible sobre Q es $[Q(a):Q] = 3$. Si P fuera construible existiría una extensión $Q \subset F$ tal que

$a \in F$ y $[F:Q] = 2^t$, y entonces de $Q \subset Q(a) \subset F$ resultaría que 3 divide a $2^t$.

Trisección de un ángulo. Se trata de dividir un ángulo dado $\phi$ en tres ángulos iguales. No cualquier ángulo es trisecable utilizando regla y compás.




Dar el punto A equivale a dar el punto $B(\cos\phi, 0)$. Se desea construir el ángulo $\phi/3$, o lo que es equivalente, el punto $C(\cos\phi/3, 0)$.

Por una fórmula trigonométrica

$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$.

$\cos\phi/3$ es entonces raíz de la ecuación

$$4X^3 - 3X - \cos\phi = 0 \qquad (1)$$

donde el polinomio del primer miembro tiene sus coeficientes en el cuerpo $K_0 = Q(\cos\phi)$.

Por ejemplo, si $\phi = 60°$ es $\cos\phi = \frac{1}{2}$, $K_0 = Q$, y $\cos 20°$ es raíz de la ecuación

$$4X^3 - 3X - \frac{1}{2} = 0$$

o equivalentemente de

$$8X^3 - 6X - 1 = 0$$

Pero el polinomio $f(X) = 8X^3 - 6X - 1$ es irreducible sobre Q (puede verse pensándolo en $Z_5[X]$). Luego si u es una raíz de f, Q(u) tiene grado 3 sobre Q y en consecuencia el punto C(u,0) no es construible con regla y compás.

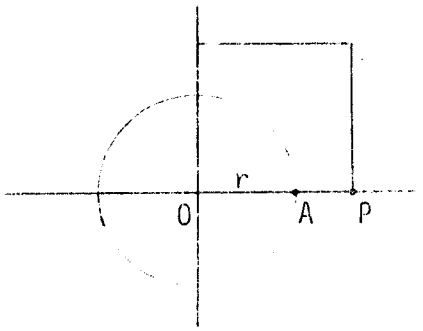
Este razonamiento es aplicable a (1) y resulta que el ángulo $\phi$ no es trisecable con regla y compás si y sólo si el polinomio $4X^3 - 3X - \cos\phi$ es irreducible sobre el cuerpo de base $K_0 = Q(\cos\phi)$.

Es lo que sucede, por ejemplo, si $\cos\phi$ es un número trascendente sobre Q. Entonces $Q(\cos\phi) \simeq Q(Y)$ siendo Y una indeterminada y podemos considerar la ecuación (1) reemplazando $\cos\phi$ por Y. Veamos que el polinomio $f(X) = 4X^3 - 3X - Y$ es irre

ducible sobre $Q(Y)$. Si fuera $f(X) = g(X).h(X)$, $g,h \in Q(Y)[X]$, como $gr_Y f = 1$, debe ser, por ejemplo, $gr_Y g = 0$ y $gr_Y n = 1$, y como en f no hay ningún término en $X^iY$ con $i > 0$ debe ser $g(X)$ = constante $\in Q$, lo que prueba que f es irreducible sobre $Q(Y)$.

En cambio si b es un número racional positivo tal que $0 < 4-3b^2 < b^3$ (2) entonces $\phi = \text{arc cos } \frac{4-3b^2}{b^3}$ es trisecable con regla y compás ya que $\cos \phi/3 = \frac{1}{b}$.
Y todo número racional b tal que $1 < b \leqslant 1{,}15$ verifica (2).

Cuadratura del círculo. Dibujar un cuadrado de área igual a la de un círculo dado.

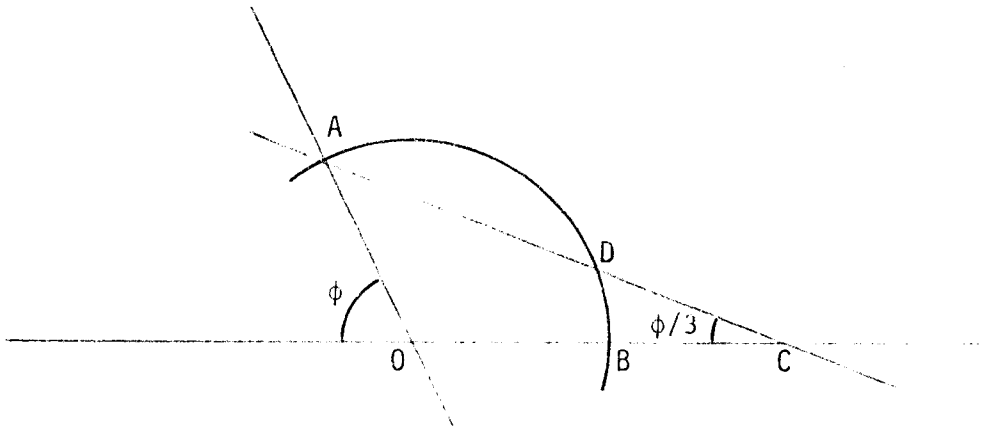



Se da $A(r,0)$ y se desea contruir $P(a,0)$ tal que $a^2 = \Pi r^2$. Tomando $r=1$, $K_0 = Q$, y hay que considerar las raíces de la ecuación $X^2-\Pi = 0$. Si fueran construibles, existiría una extensión F de Q tal que $\sqrt{\Pi} \in F$ y $[F:Q] = 2^t$, lo que implicaría $\sqrt{\Pi}$ algebraico sobre Q, y por lo tanto $\Pi$ algebraico sobre Q. Que esto último es falso fue demostrado por F.Lindemann (1852-1939) en 1882.

OBSERVACION. Lo que se prueba en los tres problemas planteados es la imposibilidad de hacer construcciones exactas. Pero se conocen construcciones aproximadas, algunas de notable precisión.

Es de señalar que con una regla subdividida es posible trisecar cualquier ángulo, más precisamente, dividirlo en n partes iguales. (Cundy H.M. and Rollet A.P., Mathematical models, 1961, Oxford).

La siguiente construcción permite trisecar un ángulo usando una regla con dos puntos marcados separados por una distancia d.




Dado el ángulo $\phi$ se dibuja una circunferencia con centro O y radio d que determina los puntos de intersección A y B. Se apoya la regla sobre el punto A y se la desliza hasta hacer que los puntos marcados estén, uno sobre la recta OB, y el otro sobre la circunferencia. Se determina así los puntos C y D. Es fácil ver que el ángulo en C es $\phi/3$.

# CAPITULO IV

## CLAUSURA ALGEBRAICA. EXTENSIONES SEPARABLES, NORMALES.

### CUERPO DE RAICES

Dado un cuerpo K y un polinomio $f(X) \in K[X]$ no constante puede suceder que $f(X)$ no tenga ninguna raíz en K o que tenga un número de raíces menor que su grado. Por ejemplo, el polinomio $X^3+X^2+X+1 = (X+1)(X^2+1) \in Q[X]$ tiene sólo una raíz en Q. Se plantea el siguiente problema:

En general, dado un cuerpo K y un polinomio $f \in K[X]$ no constante, ¿existe alguna extensión E de K en la que f tiene tantas raíces como su grado, es decir, tal que f se puede escribir como el producto de polinomios de primer grado en E[X]: $f(X) = c(X-\alpha_1) \dots (X-\alpha_n)$ , $c \in K$ , $\alpha_i \in E$?.

La respuesta es afirmativa. Para verlo comenzaremos por demostrar que existe una extensión de K donde f tiene una raíz, y luego por recurrencia llegaremos a ese resultado.

Pero antes vamos a ver algo sobre homomorfismos de extensiones:

1) Si K y E son cuerpos, todo homomorfismo de anillos $\varphi: K \to E$ es inyectivo o nulo. De modo que si $\varphi$ es un homomorfismo no nulo, es un monomorfismo y entonces $K \simeq \varphi(K) \subset E$, $\varphi(K)$ es un subcuerpo de E y E es una extensión de $\varphi(K)$. Se puede construir una extensión F de K isomorfa a E, más precisamente, una extensión F de K y un isomorfismo $\bar{\varphi}: F \to E$ que extiende a $\varphi$, es decir, tal que $\bar{\varphi}/K = \varphi$.

$$\begin{array}{ccc} K & \subset & F \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\bar{\varphi}} \\ \varphi(K) & \subset & E \end{array}$$

En efecto, sea S un conjunto coordinable con $E-\varphi(K)$ y disjunto con K y sea $F = K \cup S$. Es claro que $\varphi: K \to E$ se puede extender a una biyección $\bar{\varphi}: F \to E$. En F se definen una suma y una multiplicación como sigue:

$$x + y = \bar{\varphi}^{-1}(\bar{\varphi}(x) + \bar{\varphi}(y))$$

$$x \cdot y = \bar{\varphi}^{-1}(\bar{\varphi}(x) \cdot \bar{\varphi}(y))$$

F con estas operaciones es un cuerpo, y las mismas restringidas a K coinciden con la suma y la multiplicación de K, de modo que K es un subcuerpo de F, y $\bar{\varphi}$ es un isomorfismo. (Observar que de la construcción de la extensión F resulta que hay infinitas de este tipo si $\varphi(K) \neq E$).
Entonces se puede identificar F con E por el isomorfismo $\bar{\varphi}$, lo que identifica a K con $\varphi(K)$.
Esta situación se expresa diciendo que identificando a K con $\varphi(K)$ por $\varphi$, E se considera una extensión de K.

2) DEFINICION. Si E y E' son dos extensiones de un cuerpo K, un homomorfismo $\varphi: E \to E'$ se dice un K-homomorfismo si $\varphi/K = id_K$, o sea, si $\varphi(a) = a$ para todo $a \in K$. Se dice que $\varphi$ deja fijos los elementos de K. Observemos que:

- Si $\varphi: E \to E'$ es un K-homomorfismo, es un homomorfismo de K-espacios vectoriales. (De ahí el nombre de K-homomorfismo).
- Si $\varphi: E \to E'$ es un K-homomorfismo y $\alpha \in E$ es raíz de un polinomio $f(X) \in K[X]$, entonces $\varphi(\alpha) \in E'$ también es raíz de $f(X)$. En efecto, si $f(X) = a_0 + a_1X + \ldots + a_nX^n$ , $a_i \in K$ y $f(\alpha) = 0$ entonces
$f(\varphi(\alpha)) = a_0 + a_1\varphi(\alpha) + \ldots + a_n(\varphi(\alpha))^n = \varphi(a_0 + a_1\alpha + \ldots + a_n\alpha^n) =$
$= \varphi(0) = 0.$
Es decir, un K-homomorfismo aplica raíces de f en raíces de f.

Como aplicación inmediata de esto resulta:

TEOREMA 4.1. Si $K \subset E$ es una extensión algebraica, todo K-endomorfismo $\varphi: E \to E$ es un automorfismo.

Demostración. Hay que probar que $\varphi$ es epiyectiva, pues siendo K-homomorfismo

no es nulo y por lo tanto es monomorfismo. Si $\alpha \in E$, $\alpha$ es algebraico sobre K; sea $f(X) \in K[X]$ un polinomio cualquiera que tiene a $\alpha$ como raíz (por ejemplo el minimal) y sea $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ , $\alpha_1 = \alpha$, el conjunto de raíces de f en E. Como $\varphi$ aplica raíces de f en raíces de f y $\varphi$ es endomorfismo, $\varphi$ aplica S en S, y como $\varphi$ es inyectiva y S es finito, $\varphi(S) = S$. Luego $\varphi(\alpha_i) = \alpha$ para algún i.

Observación: Un endomorfismo no nulo $\varphi: E \to E$ no es en general un automorfismo de E pues puede no ser epiyectivo. Por ejemplo, la aplicación $\varphi: Z_p(X) \to Z_p(X)$ tal que $\varphi(f(X)) = (f(X))^p$ es un monomorfismo no epiyectivo.
En general, si $\varphi: E \to E$ es un endomorfismo los elementos que quedan fijos por $\varphi$ forman un subcuerpo $K \subset E$. Acabamos de ver que si E es algebraico sobre K entonces $\varphi$ es un automorfismo de E.

3) Si K y K' son dos cuerpos y $\varphi: K \to K'$ es un isomorfismo, $\varphi$ se puede extender a un isomorfismo $\tilde{\varphi}: K[X] \to K'[X]$ poniendo $\tilde{\varphi}(\sum a_i X^i) = \sum \varphi(a_i) X^i$.

Es claro que

$f(X) \in K[X]$ irreducible sobre K $\iff$ $\tilde{\varphi}(f(X)) \in K'[X]$ irreducible sobre K'.

TEOREMA 4.2. Sean K y K' dos cuerpos, $\varphi: K \to K'$ un isomorfismo, $f(X) = \sum a_i X^i \in K[X]$ irreducible sobre K, $\tilde{f}(X) = \sum \varphi(a_i) X^i \in K'[X]$. Si $\alpha$ es una raíz de f en alguna extensión de K y $\beta$ es una raíz de $\tilde{f}$ en alguna extensión de K' entonces existe un único isomorfismo $\bar{\varphi}: K(\alpha) \to K'(\beta)$ tal que $\bar{\varphi}(\alpha) = \beta$ y $\bar{\varphi}/K = \varphi$.
Más precisamente, si $\alpha$ es una raíz de f(X) en una extensión de K y E' es una extensión de K', $\varphi$ se puede extender a un nomomorfismo $\bar{\varphi}: K(\alpha) \to E'$ si y sólo si $\tilde{f}(X)$ tiene una raíz en E', y hay tantas extensiones de $\varphi$ como raíces distintas tiene $\tilde{f}(X)$ en E'.

Demostración. En las condiciones del enunciado, si $n = gr\ f = gr\ f'$, $1, \alpha, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)$ sobre K, y $1, \beta, \ldots, \beta^{n-1}$ es una base de $K'(\beta)$

sobre K'. Sea $\bar{\varphi}$: $K(\alpha) \to K'(\beta)$ definida como sigue:

$\forall\ x \in K(\alpha)$ , $x = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ , $a_i \in K$ , es

$\bar{\varphi}(x) = \varphi(a_0) + \varphi(a_1)\beta + \ldots + \varphi(a_{n-1})\beta^{n-1}$.

Es fácil ver que $\bar{\varphi}$ es un isomorfismo, $\bar{\varphi}/K = \varphi$ y $\bar{\varphi}(\alpha) = \beta$. La unicidad de $\bar{\varphi}$ resulta de que $\bar{\varphi}(\alpha) = \beta \Rightarrow \bar{\varphi}(\alpha^i) = \beta^i$ y de que $1,\alpha,\ldots,\alpha^{n-1}$ es una K-base de $K(\alpha)$.

Recíprocamente, si $\alpha$ es una raíz de f en una extensión de K y E' es una extensión de K' tal que existe un homomorfismo $\bar{\varphi}$: $K(\alpha) \to E'$ que extiende a $\varphi$ entonces se ve sin dificultad que $\bar{\varphi}(\alpha)$ es una raíz de $\tilde{f}$.

COROLARIO: Sean E y F dos extensiones de K, y $\alpha \in E$ , $\beta \in F$ elementos algebraicos sobre K. Entonces $\alpha$ y $\beta$ tienen el mismo polinomio minimal sobre K si y sólo si existe un K-isomorfismo de $K(\alpha)$ sobre $K(\beta)$ que aplica $\alpha$ en $\beta$ .

Demostración. ($\Rightarrow$) Es el teorema haciendo $K = K'$ , $\varphi = id_K$.

($\Leftarrow$) Sea $\sigma$: $K(\alpha) \to K(\beta)$ un K-isomorfismo tal que $\sigma(\alpha) = \beta$. Sea $f = \sum a_i X^i$ el polinomio minimal de $\alpha$ sobre K y $f' = \sum b_j X^j$ el polinomio minimal de $\beta$ sobre K.

$f(\beta) = f(\sigma(\alpha)) = \sum a_i(\sigma(\alpha))^i = \sigma(\sum a_i\alpha^i) = \sigma(0) = 0 \Rightarrow f'/f$, y como son polinomios irreducibles mónicos es $f = f'$.

De aquí resulta que si $K \subset E$, $f(X) \in K[X]$ es irreducible y $\alpha,\beta \in E$ son raíces de f entonces $K(\alpha) \simeq K(\beta)$.

Ejemplo. $Q \subset C, X^4-2$ es irreducible sobre Q. Sus raíces son $\sqrt[4]{2}$ , $-\sqrt[4]{2}$ , $\sqrt[4]{2}i$ , $-\sqrt[4]{2}i$. $Q(\sqrt[4]{2}) \simeq Q(\sqrt[4]{2}i)$ , pero $Q(\sqrt[4]{2}) \neq Q(\sqrt[4]{2}i)$. Ninguno de estos dos cuerpos contiene todas las raíces de f.

Observación.

a) En el corolario, que el K-isomorfismo de $K(\alpha)$ sobre $K(\beta)$ aplique $\alpha$ en $\beta$ es esencial para concluir que $\alpha$ y $\beta$ tienen el mismo polinomio minimal.
Por ejemplo, considerar los polinomios irreducibles $X^2-2$ y $X^2-4X+2$ en

$Q[X]$. Si $\alpha$ es una raíz del primero y $\beta$ una del segundo, las extensiones $Q(\alpha)$ y $Q(\beta)$ son Q-isomorfas.

b) El teorema anterior no es verdadero si se suprime la hipótesis de que f es irreducible.
Por ejemplo, el polinomio $f(X) = (X^2-2)(X^2-3)$ tiene raíces $\sqrt{2}$ y $\sqrt{3}$ pero $Q(\sqrt{2})$ no es isomorfo a $Q(\sqrt{3})$: En el primer cuerpo hay un elemento que al cuadrado da 2. En el segundo, teniendo en cuenta que sus elementos son de la forma $q_1 + q_2\sqrt{3}$ , se tiene:

$$(q_1 + q_2\sqrt{3})^2 = q_1^2 + 3q_2^2 + 2\sqrt{3}q_1q_2 \neq 2 \qquad \forall \quad q_1, q_2 \in Q.$$

TEOREMA 4.3. Si K es un cuerpo y $f(X) \in K[X]$ es un polinomio de grado $\geqslant 1$, existe una extensión E de K donde f tiene una raíz.

Demostración. Podemos suponer que f es irreducible. Sea $\varphi$: $K[X] \to K[X]/(f)$ el homomorfismo canónico. f irreducible implica $K[X]/(f)$ cuerpo.
Como dos constantes distintas no son congruentes módulo (f), el homomorfismo $\varphi$ restringido a K es un isomorfismo de K sobre el conjunto K' de las clases de equivalencia que contienen a las constantes. Entonces el cuerpo $K[X]/(f) = E$ es una extensión del cuerpo K' y como $K \simeq K'$ podemos considerar que E contiene a K identificando los elementos de K con los de K': $a = \varphi(a)$ cualquiera sea $a \in K$ .
E es una extensión como la buscada ya que $\xi = \varphi(X)$ es una raíz de f. En efecto, si $f(X) = a_0 + a_1X + \ldots + a_nX^n$ se tiene:

$$f(\xi) = f(\varphi(X)) = a_0 + a_1\varphi(X) + \ldots + a_n(\varphi(X))^n =$$

$$= \varphi(a_0 + a_1X + \ldots + a_nX^n) = \varphi(f) = 0.$$

Observar que f es a menos de una constante el polinomio minimal de $\xi$ y que $E = K(\xi)$.

COROLARIO. Si K es un cuerpo y $f(X) \in K[X]$ es un polinomio de grado $n \geqslant 1$, existe una extensión E de K tal que

$$f(X) = c(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n) \quad , \quad c \in K \quad , \quad \alpha_i \in E.$$

(Los $\alpha_i$ no necesariamente distintos).

Demostración. Por inducción sobre el grado de f.
Si gr f = 1 se verifica.
Sea gr f $>$ 1 y supongamos la propiedad verdadera para todo polinomio de grado n-1. Por el teorema existe una extensión $E_1$ de K en la que f tiene una raíz $\alpha_1$.
Luego $f(X) = (X-\alpha_1).f_1(X)$ , $f_1(X) \in E_1[X]$.
Como gr $f_1$ = n-1, por la hipótesis de inducción existe una extensión $E_1 \subset E$ tal que $f_1$ se puede escribir $f_1(X) = c(X-\alpha_2) \ldots (X-\alpha_n)$ , $\alpha_2,\ldots,\alpha_n \in E$ , $c \in K$.
Luego $f(X) = c(X-\alpha_1) \ldots (X-\alpha_n)$ , $\alpha_i \in E$ , $c \in K$.

Si $K \subset E$ y $f(X) \in K[X]$ se descompone en E[X]:

$$f(X) = c(X-\alpha_1) \ldots (X-\alpha_n) \quad , \quad \alpha_i \in E \quad , \quad c \in K$$

entonces el subcuerpo generado por K y $\alpha_1,\ldots,\alpha_n$ , $K(\alpha_1,\ldots,\alpha_n)$, es el menor subcuerpo de E sobre el que f se factoriza en polinomios de primer grado. A este cuerpo se lo llama un cuerpo de raíces de f.

DEFINICION. Sea K un cuerpo y $f \in K[X]$ de grado $\geq 1$. Una extensión L de K se dice un cuerpo de raíces de f sobre K si:

1) f se factoriza en producto de polinomios de primer grado en L[X]

$$f(X) = c(X-\alpha_1)\ldots.(X-\alpha_n) \quad , \quad \alpha_i \in L.$$

2) $L = K(\alpha_1,\ldots,\alpha_n)$.

La segunda condición es claramente equivalente a

2') Si $K \subset L' \subset L$ y f se descompone en producto de polinomios de primer grado en L'[X] entonces L = L'.

La existencia de un cuerpo de raíces para cada polinomio no constante $f \in K[X]$ está asegurada por el corolario del teorema anterior. Pero no es único. Por ejemplo, sea $f(X) = X^2-2 \in Q[X]$. Sabemos que el cuerpo $E = Q[X]/(X^2-2)$, con-

siderado como extensión de Q, es un cuerpo de raíces de f sobre Q. Otro es $E' = Q(\sqrt{2}) = \{q_0+q_1\sqrt{2} : q_0,q_1 \in Q\}$. Como el número $\pi$ es trascendente sobre Q, $Q[\pi] \simeq Q[X]$ y el cuerpo $E'' = Q[\pi]/(\pi^2-2)$ , considerado como una extensión de Q, también es un cuerpo de raíces de f sobre Q; etcétera.

TEOREMA 4.4. (Unicidad del cuerpo de raíces).
Sean K y K' dos cuerpos, $\varphi$: K → K' un isomorfismo, $f(X) = \sum a_i X^i$ un polinomio no constante de K[X] y $\tilde{f}(X) = \sum \varphi(a_i)X^i$ el polinomio correspondiente de K'[X]. Sea L un cuerpo de raíces de f sobre K y L' uno de $\tilde{f}$ sobre K'. Entonces el isomorfismo $\varphi$ se puede extender a un isomorfismo de L sobre L'.
(en general en más de una manera, y cada raíz de f en L se aplica en una raíz de $\tilde{f}$ en L').

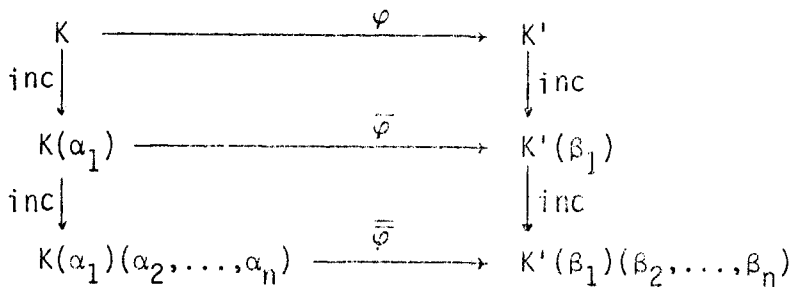
Demostración. Por inducción sobre grado de f.
Si gr f = 1, es L = K y L' = K' y el teorema se verifica.
Sea gr f = n > 1 y supongamos que la propiedad es verdadera para todos los polinomios de grado n-1. Sean $\alpha_1,\ldots,\alpha_n$ las raíces de f en L, $L = K(\alpha_1,\ldots,\alpha_n)$ , y $\beta_1,\ldots,\beta_n$ las de $\tilde{f}$ en L' , $L' = K'(\beta_1,\ldots,\beta_n)$.
Sea $f_1$ un factor irreducible de f, $\tilde{f}_1$ el correspondiente de $\tilde{f}$. Sea $\alpha$ una raíz de $f_1$ en L y $\beta$ una de $\tilde{f}_1$ en L'. Podemos suponer $\alpha = \alpha_1$, $\beta = \beta_1$. Entonces por el teorema 4.2 el isomorfismo $\varphi$ puede extenderse a uno $\bar{\varphi}$: $K(\alpha_1) \to K'(\beta_1)$ tal que $\bar{\varphi}(\alpha_1) = \beta_1$.

Por otro lado $f = (X-\alpha_1).g_1$ , $g_1 \in K(\alpha_1)[X]$ , gr $g_1$ = n-1

$\tilde{f} = (X-\beta_1).\tilde{g}_1$ , $\tilde{g}_1 \in K'(\beta_1)[X]$ , gr $\tilde{g}_1$ = n-1

$\tilde{g}_1$ es el polinomio correspondiente a $g_1$ por el isomorfismo
$\tilde{\bar{\varphi}}$: $K(\alpha_1)[X] \to K'(\beta_1)[X]$; $\alpha_2,\ldots,\alpha_n$ son las raíces de $g_1$ de modo que $K(\alpha_1)(\alpha_2,\ldots,\alpha_n) = L$ es un cuerpo de raíces de $g_1$ sobre $K(\alpha_1)$. Análogamente $K'(\beta_1)(\beta_2,\ldots,\beta_n) = L'$ es un cuerpo de raíces de $\tilde{g}_1$ sobre $K'(\beta_1)$. Entonces por la hipótesis de inducción $\tilde{\bar{\varphi}}$ puede extenderse a un isomorfismo $\bar{\bar{\varphi}}$: $K(\alpha_1)(\alpha_2,\ldots,\alpha_n) \to K'(\beta_1)(\beta_2,\ldots,\beta_n)$ (que aplica cada raíz $\alpha_i$, $2 \leq i \leq n$ ,

en una raíz $\beta_j$, $2 \leq j \leq n$).




Se ve entonces que $\bar{\bar{\varphi}}: L \to L'$ es el isomorfismo buscado.

En particular, si $K = K'$ sigue la unicidad del cuerpo de raíces de un polinomio $f \in K[X]$ a menos de K-isomorfismos.

Por eso se habla del cuerpo de raíces de un polinomio $f(X)$ sin especificar en qué extensión de K está contenido ese cuerpo.

¿Por qué en el teorema anterior $\varphi$ puede extenderse en más de una manera?. ¿Cuántas son las extensiones que hay?. ¿En qué casos la extensión de $\varphi$ es única?.

Ejemplos.

1) Sea $f(X) = (X^2-3)(X^3+1) \in Q[X]$. Sus raíces en C son $\pm\sqrt{3}$ , $-1$ , $\frac{1\pm\sqrt{3}\,i}{2}$ .
   El cuerpo de raíces es entonces $Q(\sqrt{3}, \frac{1+\sqrt{3}\,i}{2})$ que claramente es el mismo que $Q(\sqrt{3}, i)$ . Su grado sobre Q es 4.
   $f(X) = (X-\sqrt{3})(X+\sqrt{3})(X+1)(X - \frac{1+\sqrt{3}\,i}{2})(X - \frac{1-\sqrt{3}\,i}{2})$ en $Q(\sqrt{3}, i)[X]$.

2) $f(X) = (X^2-2X+2)(X^2+3)$ sobre Q. Las raíces en C son $1\pm i$ , $\pm\sqrt{3}\,i$ y el cuerpo de raíces es entonces $Q(1+i, \sqrt{3}\,i)$ que coincide con $Q(\sqrt{3}, i)$.
   Es el mismo cuerpo que en el ejemplo anterior aunque los polinomios son distintos. Esto puede suceder aún cuando se trate de polinomios irreducibles, como se ve en el siguiente ejemplo:

3) $f(X) = X^2-2X+2$ y $g(X) = X^2+1$ son irreducibles sobre Q y ambos tienen $Q(i)$ como cuerpo de raíces sobre Q.

4) Consideremos $f(X) = X^2+X+1$ sobre $Z_2$. Aquí no se puede trabajar en C y usaremos la construcción básica del cuerpo de raíces. f es irreducible, entonces se puede construir una extensión $Z_2(\xi)$ de $Z_2$ siguiendo el método del teorema 4.3, donde $\xi$ es una raíz de f. $\varphi: Z_2[X] \to Z_2[X]/(f) = E$, $E = Z_2(\xi)$ siendo $\xi = \varphi(X)$. $\xi$ tiene a f como polinomio minimal sobre $Z_2$, luego $[Z_2(\xi):Z_2] = 2$ y $\xi^2+\xi+1 = 0$, así que $\xi^2 = \xi + 1$. $\{1,\xi\}$ es una base de $Z_2(\xi)$ sobre $Z_2$ de modo que los elementos de $Z_2(\xi)$ son: 0, 1, $\xi$, $1+\xi$.
Las tablas de la suma y la multiplicación en $Z_2(\xi)$ son:

| + | 0 | 1 | $\xi$ | $1+\xi$ |
|---|---|---|---|---|
| 0 | 0 | 1 | $\xi$ | $1+\xi$ |
| 1 | 1 | 0 | $1+\xi$ | $\xi$ |
| $\xi$ | $\xi$ | $1+\xi$ | 0 | 1 |
| $1+\xi$ | $1+\xi$ | $\xi$ | 1 | 0 |

| . | 0 | 1 | $\xi$ | $1+\xi$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $\xi$ | $1+\xi$ |
| $\xi$ | 0 | $\xi$ | $1+\xi$ | 1 |
| $1+\xi$ | 0 | $1+\xi$ | 1 | $\xi$ |

En $Z_2(\xi)[X]$ f se descompone: $f(X) = (X-\xi)(X-1-\xi)$.

EJERCICIOS

1) a) Si E y F son dos extensiones del cuerpo Q de los racionales, demostrar que todo homomorfismo de anillos no nulo $\varphi: E \to F$ es un Q-homomorfismo.

b) Encontrar todos los Q-automorfismos de:

i) $Q(\sqrt{2})$ ii) $Q(\alpha)$ siendo $\alpha$ la raíz real $\sqrt[5]{7}$

iii) $Q(\alpha)$ siendo $\alpha^5=1$, $\alpha \neq 1$ iv) $Q(\sqrt{2},\sqrt{3})$.

2) Hallar los subcuerpos de C que son cuerpos de raíces sobre Q de los polinomios: $X^3-1$, $X^4+5X^2+6$, $X^6-8$. Indicar sus grados.

3) a) Construir un cuerpo de raíces de $f(X) = X^3+2X+1$ sobre $Z_3$.

b) Construir un cuerpo de raíces de $g(X) = X^3+X^2+X+2$ sobre $Z_3$.

¿Es isomorfo al obtenido en a)?.

4) Si E es un cuerpo de raíces de f(X) sobre K y $K \subset L \subset E$, probar que E es un cuerpo de raíces de f sobre L.

5) Si $f(X) \in K[X]$ es un polinomio de grado n y E un cuerpo de raíces de f sobre K entonces $[E:K] / n!$.

6) Decir si es verdadero que:

   a) Extensiones del mismo grado son isomorfas.
   b) Extensiones isomorfas tienen el mismo grado.
   c) Si f(X) es un polinomio irreducible sobre K y $\alpha$ es una raíz de f en alguna extensión de K, entonces $K(\alpha)$ es un cuerpo de raíces de f.
   d) Polinomios irreducibles distintos sobre un cuerpo K tienen cuerpos de raíces distintos.

## CUERPOS ALGEBRAICAMENTE CERRADOS. CLAUSURA ALGEBRAICA.

DEFINICION. Un cuerpo L se dice algebraicamente cerrado si todo polinomio no constante de L[X] tiene una raíz en L.

Se ve que las siguientes propiedades son equivalentes:

i) L es algebraicamente cerrado.

ii) Todo polinomio no constante de L[X] se descompone en producto de polinomios de primer grado.

iii) Los polinomios irreducibles de L[X] son los de primer grado.

iv) Toda extensión algebraica de L coincide con L.

DEFINICION. Dado un cuerpo K, una extensión $K \subset E$ se dice una clausura algebraica de K si E es una extensión algebraica de K y E es algebraicamente cerrado.

Es claro que si $K \subset F \subset E$ y E es una clausura algebraica de K entonces E es una clausura algebraica de F.

La recíproca no es verdadera. Por ejemplo, $Q \subset R \subset C$; C es algebraicamente cerrado (Teorema fundamental del álgebra) y es algebraico sobre R, luego C es una clausura algebraica de R. Pero no lo es de Q pues C no es algebraico sobre Q.

Vamos a ver que un cuerpo algebraicamente cerrado es una suerte de "receptor universal" de homomorfismos. En primer lugar veamos que para cualquier cuerpo K existe una clausura algebraica de K y que ésta es única salvo K-isomorfismos.

TEOREMA 4.5. Si K es un cuerpo, existe un cuerpo algebraicamente cerrado que contiene a K como subcuerpo.

Demostración. En primer lugar se construye una extensión $E_1$ de K en la que todo polinomio no constante de K[X] tiene una raíz.
A cada polinomio no constante f de K[X] se le asocia una indeterminada $Y_f$. Sea S el conjunto de las mismas y consideremos el anillo de polinomios K[S]. (El anillo de polinomios sobre K en infinitas indeterminadas $\{Y_f: Y_f \in S\}$ se define como la unión de los anillos de polinomios con coeficientes en K en un número finito de $Y_f$ con las operaciones naturales). Sea I el ideal de K[S] generado por los polinomios $f(Y_f)$. I es propio, pues si no $1 \in I$ lo que implica que hay una combinación finita de elementos de I que da 1:

$$(1) \qquad g_1 f_1(Y_{f_1}) + \ldots + g_n f_n(Y_{f_n}) = 1 \quad , \quad \text{con} \quad g_i \in K[S] .$$

Por simplicidad escribiremos $Y_{f_i} = Y_i$. En los $g_i$ figura en total un número finito de indeterminadas, $Y_1, Y_2, \ldots, Y_N$ $(N \geqslant n)$. Entonces (1) se puede escribir

$$(2) \qquad \sum_{i=1}^{n} g_i(Y_1, \ldots, Y_N) f_i(Y_i) = 1$$

Sea F una extensión de K en la que cada polinomio $f_1, \ldots, f_n$ tiene una raíz $\alpha_1, \ldots, \alpha_n$. Pongamos $\alpha_i = 0$ para $n < i \leqslant N$. Reemplazando $Y_i$ por $\alpha_i$ en (2) resulta $0 = 1$, contradicción. Luego I es propio.
Sea M un ideal maximal de K[S] que contiene a I. Entonces K[S]/M es un cuerpo. El homomorfismo canónico $\varphi$: K[S] $\to$ K[S]/M restringido a K es un isomorfismo, $K \simeq \varphi(K)$, e identificando a K con su imagen se puede considerar que $K[S]/M = E_1$ es una extensión de K. Cada polinomio no constante $f \in K[X]$ tiene una raíz en

$E_1$: $f(\varphi(Y_f)) = \varphi(f(Y_f)) = 0$, luego $\varphi(Y_f) \in E_1$ es raíz de f.

Procediendo por recurrencia se puede formar una cadena de cuerpos

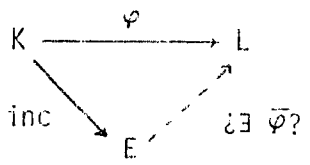
$$K \subset E_1 \subset E_2 \subset \ldots \subset E_n \subset \ldots$$

tal que todo polinomio no constante de $E_i[X]$ tiene una raíz en $E_{i+1}$. Sea $E = \cup E_i$. E es naturalmente un cuerpo pues si $x,y \in E$, existe un índice n tal que $x,y \in E_n$. Entonces $x+y$, $x.y \in E_n$, y esta suma y producto no dependen del índice n considerado. Se tiene así una estructura de cuerpo sobre E. Además cualquier polinomio de E[X] tiene todos sus coeficientes en algún $E_j$, y por lo tanto una raíz en $E_{j+1}$, o sea una raíz en E, lo que prueba que E es algebraicamente cerrado.

COROLARIO. Si K es un cuerpo, existe una clausura algebraica de K.

Demostración. Sea E una extensión de K algebraicamente cerrada y $\overline{K}$ la clausura algebraica de K en E, es decir el conjunto de todos los elementos de E que son algebraicos sobre K: $K \subset \overline{K} \subset E$. Entonces $\overline{K}$ es una clausura algebraica de K, pues es algebraico sobre K y algebraicamente cerrado, ya que todo polinomio no constante f con coeficientes en $\overline{K}$ tiene una raíz $x \in E$; x es algebraico sobre $\overline{K}$, luego $\overline{K}(x)$ es algebraico sobre $\overline{K}$ y como $\overline{K}$ es algebraico sobre K, se tiene x algebraico sobre K, o sea $x \in \overline{K}$.

Queremos demostrar que dos clausuras algebraicas de un cuerpo K son K-isomorfas. Para eso vamos a estudiar cuáles son las extensiones posibles de una inmersión (monomorfismo) $\varphi$: $K \to L$, de un cuerpo K en uno L algebraicamente cerrado, a un homomorfismo $\overline{\varphi}$: $E \to L$ donde E es una extensión algebraica cualquiera de K.




Para el caso en que E es una extensión algebraica simple de K, $E = K(\alpha)$, por el teorema 4.2 sabemos que hay tantas extensiones $\overline{\varphi}$: $K(\alpha) \to L$ como raíces distintas tiene en L el polinomio $\tilde{f} \in \varphi(K)[X]$, siendo $f \in K[X]$ el polinomio minimal

de $\alpha$. Si L es algebraicamente cerrado, contiene a todas las raíces de $\tilde{f}$, es decir, a su cuerpo de raíces, que es isomorfo al de f. Entonces resulta

TEOREMA 4.6. Si $\varphi$: K → L es una inmersión de un cuerpo K en uno L algebraicamente cerrado y K($\alpha$) es una extensión algebraica de K entonces $\varphi$ se puede extender a una inmersión $\bar{\varphi}$: K($\alpha$) → L y el número de éstas es igual al número de raíces distintas del polinomio minimal de $\alpha$. (en un cuerpo de raíces cualquiera).

Para una extensión algebraica cualquiera K ⊂ E se tiene, usando el lema de Zorn:

TEOREMA 4.7. Sea K ⊂ E una extensión algebraica, $\varphi$: K → L una inmersión de K en un cuerpo L algebraicamente cerrado. Entonces $\varphi$ puede extenderse a una inmersión $\bar{\varphi}$: E → L. Si E es algebraicamente cerrado y L es algebraico sobre $\varphi$(K) entonces $\bar{\varphi}$ es un isomorfismo de E sobre L.

Demostración. Consideremos los pares $(F,\sigma)$ donde K ⊂ F ⊂ E y $\sigma$: F → L es un homomorfismo que extiende a $\varphi$, es decir, $\sigma/K=\varphi$. El conjunto S de todos estos pares no es vacío pues $(K,\varphi) \in S$. En S se define la siguiente relación: $(F_1,\sigma_1) \leq (F_2,\sigma_2)$ si y sólo si $F_1 \subset F_2$ y $\sigma_2/F_1 = \sigma_1$. Es una relación de orden y S es inductivo superiormente con respecto a ella. En efecto, si $\{(F_i,\sigma_i)\}_{i\in I}$ es una cadena en S, sea $F = \bigcup_{i\in I} F_i$ y $\sigma$: F → L la aplicación tal que $\sigma(x) = \sigma_i(x)$ si $x \in F_i$. Se ve que F es un subcuerpo de E, K ⊂ F ⊂ E, y que $\sigma$ está bien definida y es un homomorfismo que extiende a $\varphi$. Luego $(F,\sigma) \in S$, lo que prueba que S es inductivo superiormente.

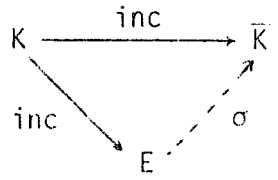
Entonces por el lema de Zorn existe un elemento maximal en S, $(H,\bar{\varphi})$. Se trata de probar que H = E. Si no fuera así existiría $\alpha \in E$, $\alpha \notin H$. Por la hipótesis sobre E, $\alpha$ es algebraico sobre K, luego lo es sobre H. Entonces por el teorema 4.6, $\bar{\varphi}$: H → L puede extenderse a un homomorfismo $\bar{\bar{\varphi}}$: H($\alpha$) → L. En consecuencia $(H(\alpha),\bar{\bar{\varphi}}) \in S$ lo que contradice la maximalidad de $(H,\bar{\varphi})$. Luego H = E y $\bar{\varphi}$: E → L es la extensión buscada.

Si E es algebraicamente cerrado, como $E \simeq \bar{\varphi}(E)$, $\bar{\varphi}(E)$ es algebraicamente cerrado. Si L es algebraico sobre $\varphi$(K), de $\varphi(K) \subset \bar{\varphi}(E) \subset L$ sigue que L es algebraico sobre $\bar{\varphi}(E)$, lo que implica $L = \bar{\varphi}(E)$.

COROLARIO 1. Si K es un cuerpo, dos clausuras algebraicas de K son K-isomorfas.

De lo visto resulta que dado un cuerpo K, toda extensión algebraica $K \subset E$ está contenida en una clausura algebraica de K.
En efecto, si $K \subset E$ es algebraica, sea $\overline{E}$ una clausura algebraica de E, $K \subset E \subset \overline{E}$. Como $\overline{E}$ es algebraico sobre E y E sobre K, $\overline{E}$ es extensión algebraica de K y como $\overline{E}$ es algebraicamente cerrado resulta que $\overline{E} = \overline{K}$.
Recíprocamente, si $K \subset \overline{K}$ es una clausura algebraica de K, todo subcuerpo intermedio $K \subset E \subset \overline{K}$ es una extensión algebraica de K y $\overline{E} = \overline{K}$.

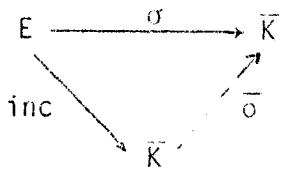
Ahora bien, elegida una clausura algebraica $\overline{K}$ de K, cualquier extensión algebraica $K \subset E$ admite una inmersión en $\overline{K}$ por un K-monomorfismo: por el teorema 4.7 la inclusión $inc: K \to \overline{K}$ se puede extender a un K-homomorfismo $\sigma$




Luego $E \simeq \sigma(E)$ y $K \subset \sigma(E) \subset \overline{K}$.
Identificando a E con su imagen $\sigma(E)$ se puede considerar a E contenido en $\overline{K}$. Supondremos entonces que todas nuestras extensiones algebraicas de K están contenidas en $\overline{K}$.
Si $K \subset E \subset \overline{K}$ estudiaremos los K-homomorfismos de E en $\overline{K}$, entre los cuales está la inclusión de E en $\overline{K}$.

COROLARIO 2. Sea $K \subset E \subset \overline{K}$ y $\sigma: E \to \overline{K}$ un K-homomorfismo. Entonces existe un K-automorfismo $\overline{\sigma}: \overline{K} \to \overline{K}$ que extiende a $\sigma$.

Demostración. Resulta inmediatamente aplicando el teorema anterior:



## EXTENSIONES SEPARABLES

DEFINICION. Si $K \subset E \subset \overline{K}$, la cardinalidad del conjunto de todos los K-homomorfismos de E en $\overline{K}$ se llama el grado de separabilidad de E sobre K y se nota $[E:K]_s$.

En particular, del teorema 4.6 resulta que si $\alpha$ es un elemento algebraico sobre K, $K \subset K(\alpha) \subset \overline{K}$, el número de K-homomorfismos de $K(\alpha)$ en $\overline{K}$ es igual al número de raíces distintas del polinomio minimal f de $\alpha$ sobre K:

$$[K(\alpha):K]_s = \text{número de raíces distintas de } f.$$

TEOREMA 4.8. a) Si $K \subset E \subset F \subset \overline{K}$ entonces

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

Si $\{\sigma_i\}_{i\in I}$ es el conjunto de los K-homomorfismos de E en $\overline{K}$ y $\{\tau_j\}_{j\in J}$ el de los E-homomorfismos de F en $\overline{K}$, para cada índice i sea $\overline{\sigma}_i$ un K-automorfismo de $\overline{K}$ que extiende a $\sigma_i$ (Pueden existir varias extensiones de $\sigma_i$, se elige una).

Definiendo $\omega_{ij}: F \to \overline{K}$ como la composición $\omega_{ij} = \overline{\sigma}_i \circ \tau_j$ se tiene que $\{\omega_{ij}\}_{(i,j)\in I\times J}$ es el conjunto de todos los K-homomorfismos de F en $\overline{K}$.

b) Si E es una extensión finita de K, $[E:K]_s \leq [E:K]$.

Demostración. a) Es claro que $\omega_{ij}$ es un K-homomorfismo de F en $\overline{K}$. Son todos distintos pues si $\omega_{ij} = \omega_{i'j'}$ es $\overline{\sigma}_i\tau_j = \overline{\sigma}_{i'}\tau_{j'}$; entonces para cualquier $b \in E$, $\sigma_i(b) = \overline{\sigma}_i(b) = \overline{\sigma}_i(\tau_j(b)) = \overline{\sigma}_i\tau_j(b) = \overline{\sigma}_{i'}\tau_{j'}(b) = \overline{\sigma}_{i'}(b) = \sigma_{i'}(b) \Rightarrow \sigma_i = \sigma_{i'}$ $\Rightarrow \tau_j = \tau_{j'}$. Luego $i = i'$ y $j = j'$.

Veamos que si $\omega: F \to \overline{K}$ es un K-homomorfismo, entonces $\omega = \omega_{ij}$ para algún par de índices i,j. $\omega/E$ es un K-homomorfismo de E en $\overline{K}$, luego $\omega/E = \sigma_i$ para algún i. Consideremos $\overline{\sigma}_i^{-1}\omega: F \to \overline{K}$. Es un E-homomorfismo, entonces $\overline{\sigma}_i^{-1}\omega = \tau_j$ y $\omega = \overline{\sigma}_i\tau_j = \omega_{ij}$.

De aquí resulta inmediatamente la multiplicatividad de los grados de separabili-

dad para extensiones sucesivas.

b) Sea E una extensión finita de K, entonces E es finitamente generada sobre K por elementos algebraicos, $E = K(\alpha_1,\ldots,\alpha_n)$, y E se puede obtener a partir de K por sucesivas extensiones simples:

$$K \subset K(\alpha_1) \subset K(\alpha_1,\alpha_2) \subset \ldots \subset K(\alpha_1,\ldots,\alpha_n) = E \qquad (1)$$

Llamemos $F_0 = K$, $F_i = K(\alpha_1,\ldots,\alpha_i)$, $1 \leqslant i \leqslant n$. Luego $F_{i+1} = F_i(\alpha_{i+1})$.

Por el teorema 4.6 sabemos que el número de extensiones posibles de un monomorfismo $F_i \to \overline{K}$ a uno de $F_i(\alpha_{i+1})$ en $\overline{K}$ es menor o igual que el grado del polinomio minimal de $\alpha_{i+1}$ sobre $F_i$, que es $[F_{i+1}:F_i]$. Luego $[F_i(\alpha_{i+1}):F_i]_s \leqslant$

$\leqslant [F_i(\alpha_{i+1}):F_i]$.

Esta relación se verifica en cada escalón de la cadena (1). Entonces en virtud de la multiplicatividad del grado y del grado de separabilidad sigue que $[E:K]_s \leqslant [E:K]$.

DEFINICION. Dado un cuerpo K, un elemento $\alpha$ algebraico sobre K se dice separable sobre K si $[K(\alpha):K]_s = [K(\alpha):K]$.

Esto es equivalente a decir que el polinomio minimal de $\alpha$ sobre K no tiene raíces múltiples.

Dada una extensión $K \subset E \subset \overline{K}$, se dice que E es separable sobre K si todos los elementos de E son separables sobre K. Una extensión que no es separable se dice inseparable.

Como $K \subset K(\alpha)$ es separable si y sólo si el polinomio minimal de $\alpha$ sobre K no tiene raíces múltiples, es natural introducir la siguiente definición:

DEFINICION. Dado un cuerpo K, un polinomio irreducible $f(X) \in K[X]$ se dice separable si no tiene raíces múltiples. Un polinomio no constante $f(X) \in K[X]$ se dice separable si todos sus factores irreducibles lo son.

Entonces, un elemento algebraico sobre K es separable sobre K si y sólo si su

polinomio minimal es separable.

DEFINICION. Un cuerpo K se dice perfecto si todos los polinomios no constantes de K[X] son separables.

Por ejemplo, todo cuerpo algebraicamente cerrado es perfecto. En general, si car K = 0, cualquiera sea $f \in K[X]$ no constante, es $f' \neq 0$, así que por el teorema 1.6, 3) todo polinomio irreducible es separable. Luego los cuerpos de característica cero son perfectos.
Pero si car K = $p \neq 0$, entonces $f \in K[X]$ puede ser irreducible y no separable, es decir, puede ser $f' = 0$. Para encontrar un ejemplo hay que pensar en un cuerpo K de característica $\neq 0$ infinito, pues veremos más adelante que los cuerpos finitos son perfectos.

Sea $K = Z_2(X)$ , $f(Y) \in K[Y]$ , $f(Y) = Y^2 - X$ ; f es irreducible sobre K pues $\sqrt{X} \notin K$ y $f' = 0$. f tiene raíces múltiples: $\sqrt{X}$ es raíz doble de f.

De los teoremas 1.6 y 4.6 resulta

TEOREMA 4.9. Sea $f(X) \in K[X]$ un polinomio irreducible de grado n. Si car K = 0 entonces f tiene n raíces distintas $\alpha_1,\ldots,\alpha_n$ y $[K(\alpha_i):K]_s = [K(\alpha_i):K] = n$ , $i = 1,\ldots,n$. Si car K = $p \neq 0$ entonces existe un entero $e \geq 0$ tal que f tiene m raíces distintas $\alpha_1,\ldots,\alpha_m$ todas de multiplicidad $p^e$ ; $n = p^e.m$ , $[K(\alpha_i):K]_s = m$ y por lo tanto $[K(\alpha_i):K] = p^e.[K(\alpha_i):K]_s$. Además $\alpha_i^{p^e}$ es un elemento separable sobre K, $i = 1,\ldots,m$.

COROLARIO. Si $K \subset E$ es una extensión finita, el grado de separabilidad $[E:K]_s$ divide a $[E:K]$.

Demostración. $K \subset E$ finita implica $E = K(\alpha_1,\ldots,\alpha_t)$, $\alpha_i$ algebraico sobre K. Consideremos las extensiones

$$K \subset K(\alpha_1) \subset K(\alpha_1,\alpha_2) \subset \ldots \subset K(\alpha_1,\ldots,\alpha_t) = E \qquad (1)$$

Por el teorema anterior, si $\alpha$ es algebraico sobre un cuerpo F entonces

$[F(\alpha):F]_s$ divide a $[F(\alpha):F]$, más precisamente $[F(\alpha):F] = p^e.[F(\alpha):F]_s$, $e \geq 0$. Esto vale en cada escalón de (1). Luego por la multiplicatividad del grado y del grado de separabilidad sigue el corolario.

DEFINICION. Si $K \subset E$ es finita el número $[E:K]/[E:K]_s$ se llama el grado de inseparabilidad de E sobre K. Se nota $[E:K]_i$.
Hemos visto que es una potencia $p^e$ , p = car K , $e \geq 0$ y
$[E:K] = [E:K]_s.[E:K]_i$.

Ejemplos.

1) $f = X^4+X^3+1$ sobre $Z_2$. ¿Es separable?.

   $f' = X^2$ , m.c.d.(f,f') = 1 luego f es separable. (lo podemos afirmar aunque no sepamos si es irreducible sobre $Z_2$).

2) $f(X) = X^9+X^3+1$ sobre $Z_3$.

   $f'(X) = 0$, m.c.d.(f,f') $\neq$ 1. No podemos decir nada en principio sobre la separabilidad de f porque no sabemos si f es irreducible.

   $f = (X^3+X+1)^3$ ; $g = X^3+X+1$ no es irreducible sobre $Z_3$ , $g = (X-1)(X^2+X+2)$ con ambos factores irreducibles. Luego $f = (X-1)^3(X^2+X+2)^3$ ;

   $(X^2+X+2)' = 2X+1 \neq 0$ y por lo tanto f es separable pues sus factores irreducibles lo son.

3) Sea $K = Z_2(X)$. En K[Y] consideremos el polinomio $f(Y) = (Y^2-X)Y$. Esta es la descomposición de f en factores irreducibles sobre K. Como $(Y^2-X)' = 0$ , $Y^2-X$ no es separable, luego f no lo es.

TEOREMA 4.10.

a) Si $K \subset E \subset F$ y $\alpha \in F$ es separable sobre K entonces $\alpha$ es separable sobre E.

b) Si $K \subset E$ es una extensión finita entonces E es separable sobre K si y sólo si $[E:K]_s = [E:K]$.

c) Si $\{\alpha_i\}_{i \in I}$ es una familia de elementos de $\bar{K}$, entonces los $\alpha_i$ son separables

sobre K si y sólo si $K(\{\alpha_i\}_{i\in I})$ es una extensión separable de K.

d) Si $K \subset E$, el conjunto L de todos los elementos de E que son separables sobre K es una extensión separable de K.

Demostración.

a) Si $\alpha \in F$ es separable sobre K su polinomio minimal f sobre K no tiene raíces múltiples y como el polinomio minimal de $\alpha$ sobre E divide a f, tampoco las tiene.

b) Sea $K \subset E$ finita y separable. Luego $E = K(\alpha_1,\ldots,\alpha_m)$, $\alpha_i$ separable. Consideremos

$$K \subset K(\alpha_1) \subset \ldots \subset K(\alpha_1,\ldots,\alpha_m) = E$$

$\alpha_i$ es separable sobre $K(\alpha_1,\ldots,\alpha_{i-1})$ por a). Entonces por la multiplicatividad del grado y del grado de separabilidad resulta $[E:K]_s = [E:K]$.

Recíprocamente, sea $K \subset E$ finita y $[E:K]_s = [E:K]$. Cualquiera sea $\alpha \in E$, $K \subset K(\alpha) \subset E$. En cada escalón se tiene una extensión finita, luego $[E:K(\alpha)]_s \leqslant [E:K(\alpha)]$ y $[K(\alpha):K]_s \leqslant [K(\alpha):K]$. Multiplicando, se ve por la hipótesis hecha que deben valer los dos signos de igualdad. En particular debe ser $[K(\alpha):K]_s = [K(\alpha):K]$, lo que implica $\alpha$ separable sobre K.

c) Supongamos que $\alpha_i \in \overline{K}$ es separable sobre K para todo $i \in I$ y probemos que $K(\{\alpha_i\}_{i\in I})$ es separable sobre K. Si $\alpha \in K(\{\alpha_i\}_{i\in I})$ entonces $\alpha$ pertenece a una subextensión finitamente generada $K(\alpha_{i_1},\ldots,\alpha_{i_t})$. Luego basta probar que $K(\alpha_{i_1},\ldots,\alpha_{i_t})$ es separable sobre K. Consideremos las extensiones sucesivas

$$K \subset K(\alpha_{i_1}) \subset \ldots \subset K(\alpha_{i_1},\ldots,\alpha_{i_t}) \qquad (1)$$

Por a) cada $\alpha_{i_j}$ es separable sobre $K(\alpha_{i_1},\ldots,\alpha_{i_{j-1}})$, luego en cada escalón de (1) el grado y el grado de separabilidad coinciden. Multiplicando se tiene $[K(\alpha_{i_1},\ldots,\alpha_{i_t}):K]_s = [K(\alpha_{i_1},\ldots,\alpha_{i_t}):K]$ y por b) sigue lo que se quería demostrar.

La otra implicación es trivial.

d) Sea $K \subset E$, $L = \{x \in E: x \text{ separable sobre } K\}$. Por c) $K(L)$ es una extensión separable de $K$ y $K \subset K(L) \subset E$, luego $K(L) \subset L$. Entonces $K(L) = L$.

TEOREMA 4.11. (Transitividad)

Si $K \subset E \subset F$, $F$ es separable sobre $K$ si y sólo si $F$ es separable sobre $E$ y $E$ es separable sobre $K$.

Demostración. Si $F$ es separable sobre $K$, entonces $E$ es separable sobre $K$ y por a) del teorema anterior $F$ es separable sobre $E$.
Sea ahora $F$ separable sobre $E$ y $E$ separable sobre $K$. Cualquiera sea $\alpha \in F$, $\alpha$ es separable sobre $E$. Si $f = X^n + c_{n-1}X^{n-1} + \ldots + c_0$, $c_i \in E$, es el polinomio minimal de $\alpha$ sobre $E$, $f$ es separable y entonces $\alpha$ es separable sobre $K(c_0,\ldots,c_{n-1})$. Por otro lado $c_i \in E$, luego $c_i$ es separable sobre $K$, $i = 0,\ldots,n-1$. Entonces se tiene

$$K \subset K(c_0,\ldots,c_{n-1}) \subset K(c_0,\ldots,c_{n-1},\alpha)$$

con cada extensión finita y separable sobre la anterior, luego en cada escalón el grado de separabilidad coincide con el grado. Por lo tanto $[K(c_0,\ldots,c_{n-1},\alpha):K]_s = [K(c_0,\ldots,c_{n-1},\alpha):K]$, de donde resulta $K(c_0,\ldots,c_{n-1},\alpha)$ separable sobre $K$ y $\alpha$ separable sobre $K$.

¿Cuáles son los cuerpos perfectos?.
Si car $K = 0$ sabemos que $K$ es perfecto.
Si car $K = p \neq 0$, la aplicación $\varphi: K \to K$ tal que $x \mapsto x^p$ es un homomorfismo de anillos no nulo, es decir un monomorfismo, que se llama el monomorfismo de Frobenius. Su imagen es un subcuerpo de $K$, $K^p = \{x^p: x \in K\}$.
Si $K^p = K$, $\varphi$ es un automorfismo de $K$ y todo elemento de $K$ tiene una raíz p-ésima en $K$.

TEOREMA 4.12. Las siguientes propiedades son equivalentes:

a) K es un cuerpo perfecto.

b) car K = 0 o car K = p ≠ 0 y $K^p = K$.

c) Toda extensión algebraica de K es separable.

Demostración.

a ⇒ b. Si car K = 0 no hay nada que probar.
Si car K = p ≠ 0, hay que probar que $K^p = K$. Sea $\alpha \in K$, $\beta \in \overline{K}$ una raíz del polinomio $X^p-\alpha$ , es decir, $\beta^p = \alpha$. El polinomio minimal de β sobre K divide a $X^p-\alpha = (X-\beta)^p$, luego es de la forma $(X-\beta)^q$.

Como K es perfecto, debe ser q = 1 pues de lo contrario tendría una raíz múltiple. Entonces el polinomio minimal de β sobre K es X-β, luego $\beta \in K$.

b ⇒ a. Si car K = 0 sabemos que K es perfecto.
Sea car K = p ≠ 0, $K = K^p$. Para probar que K es perfecto, supongamos que existe $f(X) \in K[X]$ irreducible y no separable; entonces f'(X) = 0 y f es de la forma $f = n(X^p)$, es decir, $f = a_0 + a_1X^p + a_2X^{2p} + \ldots + a_nX^{np}$ , $n \geq 1$, $a_n \neq 0$. Como $K = K^p$ es $a_i = b_i^p$ , i = 0,...,n; luego $f = (b_0 + b_1X + b_2X^2 + \ldots + b_nX^n)^p$ , lo que implica f no irreducible. Esta contradicción prueba que K es perfecto.

La demostración de c ⇔ a queda propuesta como ejercicio.

COROLARIO. Todo cuerpo finito es perfecto.

Ejercicio. Demostrar que las extensiones separables de un cuerpo K forman una clase distinguida. (ver ejercicio 21, pág.18).

## EXTENSIONES NORMALES

La noción de extensión separable E de un cuerpo K tiene su origen en el problema de saber, dada una extensión algebraica $K \subset E$, cuántos K-homomorfismos distintos $E \to \overline{K}$ admite E. Vimos que si E es una extensión finita este número es a

lo sumo [E:K] y caracterizamos las extensiones para las cuales vale la igualdad.

Sabemos también que si $E = K(\alpha)$, un K-homomorfismo $\sigma: K(\alpha) \to \overline{K}$ está completamente determinado por la imagen de $\alpha$ y que $\sigma(K(\alpha)) = K(\sigma(\alpha))$ pues

$$c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} \in K(\alpha) \xrightarrow{\sigma} c_0 + c_1\sigma(\alpha) + \ldots + c_{n-1}(\sigma(\alpha))^{n-1} \in K(\sigma(\alpha)).$$

En particular sigue que $\alpha$ y $\sigma(\alpha)$ son raíces del mismo polinomio irreducible mónico de K[X].

Más general, si $E = K(\alpha_1,\ldots,\alpha_n)$, todo homomorfismo $\sigma: E \to \overline{K}$ está unívocamente determinado por las imágenes de los $\alpha_i$; y $\alpha_i$ y $\sigma(\alpha_i)$ son raíces del mismo polinomio irreducible mónico de K[X], $i = 1,\ldots,n$.

Supongamos que los $\alpha_i$ son tales que $E = K(\alpha_1,\ldots,\alpha_n)$ contiene a todas las raíces de los respectivos polinomios minimales $f_i \in K[X]$, $i = 1,\ldots,n$. Entonces cualquiera sea el K-homomorfismo $\sigma: E \to \overline{K}$, $\sigma(\alpha_1),\ldots,\sigma(\alpha_n)$ son elementos de E y por lo tanto $\sigma$ es un K-endomorfismo de E, es decir un automorfismo de E.

Vamos a ocuparnos ahora de las extensiones $K \subset E \subset \overline{K}$ que tienen esa propiedad: todo K-homomorfismo de E en $\overline{K}$ es un automorfismo de E.

DEFINICION. Si $K \subset E \subset \overline{K}$, E se dice una extensión normal de K si todo K-homomorfismo $\sigma: E \to \overline{K}$ es un automorfismo de E.

Ejemplo. Consideremos $Q \subset Q(\sqrt[4]{2})$.

$[Q(\sqrt[4]{2}):Q]_s = [Q(\sqrt[4]{2}):Q] = 4$.

Los Q-homomorfismos $Q(\sqrt[4]{2}) \to \overline{Q}$ son 4 y están determinados por las imágenes de $\sqrt[4]{2}$, cuyo polinomio minimal sobre Q es $X^4-2$.

Luego $\sqrt[4]{2} \to \sqrt[4]{2}$ define un Q-homomorfismo $\sigma_1 = id : Q(\sqrt[4]{2}) \to \overline{Q}$.

$\sqrt[4]{2} \to -\sqrt[4]{2}$ " " $\sigma_2$ : " .

$\sqrt[4]{2} \to \sqrt[4]{2}\,i$ " " $\sigma_3$ : " ,

$\sqrt[4]{2} \to -\sqrt[4]{2}\,i$ " " $\sigma_4$ : " .

De ellos sólo $\sigma_1$ y $\sigma_2$ son endomorfismos de $Q(\sqrt[4]{2})$, luego $Q(\sqrt[4]{2})$ no es una extensión normal de Q.

En cambio $Q(\sqrt[4]{2},i)$ sí lo es: $Q \subset Q(\sqrt[4]{2}) \subset Q(\sqrt[4]{2})(i) = E$.

Los Q-homomorfismos $Q(\sqrt[4]{2}) \to \overline{Q}$ son $\sigma_1, \sigma_2, \sigma_3, \sigma_4$.

Los $Q(\sqrt[4]{2})$-homomorfismos $Q(\sqrt[4]{2})(i) \to \overline{Q}$ son dos: $\tau_1: i \to i$

$\tau_2: i \to -i$.

Entonces los Q-homomorfismos $Q(\sqrt[4]{2},i) \to \overline{Q}$ son 8 y están definidos por (teorema 4.8):

$$\varphi_1 \begin{cases} \sqrt[4]{2} \to \sqrt[4]{2} \\ i \to i \end{cases} \qquad \varphi_3 \begin{cases} \sqrt[4]{2} \to -\sqrt[4]{2} \\ i \to i \end{cases} \qquad \varphi_5 \begin{cases} \sqrt[4]{2} \to \sqrt[4]{2}\,i \\ i \to i \end{cases}$$

$$\varphi_2 \begin{cases} \sqrt[4]{2} \to \sqrt[4]{2} \\ i \to -i \end{cases} \qquad \varphi_4 \begin{cases} \sqrt[4]{2} \to -\sqrt[4]{2} \\ i \to -i \end{cases} \qquad \varphi_6 \begin{cases} \sqrt[4]{2} \to \sqrt[4]{2}\,i \\ i \to -i \end{cases}$$

$$\varphi_7 \begin{cases} \sqrt[4]{2} \to -\sqrt[4]{2}\,i \\ i \to i \end{cases} \qquad \varphi_8 \begin{cases} \sqrt[4]{2} \to -\sqrt[4]{2}\,i \\ i \to -i \end{cases}$$

DEFINICION. Si E es una extensión algebraica de K, dos elementos $\alpha$ y $\beta$ se dicen conjugados si son raíces de un mismo polinomio irreducible, o sea, si tienen el mismo polinomio minimal sobre K.

TEOREMA 4.13.

a) Sea $K \subset E \subset \overline{K}$. Entonces E es una extensión normal de K si y sólo si todo polinomio irreducible de K[X] que tiene una raíz en E tiene todas sus raíces en E.

b) E es una extensión normal y finita de K si y sólo si E es el cuerpo de raíces de un polinomio de K[X].

Demostración. a) Sea $K \subset E \subset \overline{K}$, E una extensión normal de K. Sea f(X) con coeficientes en K, irreducible, con una raíz $\alpha \in E$. Podemos suponer f(X) mónico. Si $\beta$ es otra raíz de f, $\beta \in \overline{K}$, sabemos que existe un K-homomorfismo $\sigma: K(\alpha) \to \overline{K}$ tal que $\sigma(\alpha) = \beta$. Sea $\overline{\sigma}: E \to \overline{K}$ una extensión de $\sigma$. Como E es nor-

mal, $\overline{\sigma}$ es un automorfismo de E, luego $\overline{\sigma}(\alpha) = \sigma(\alpha) = \beta \in E$.

Recíprocamente, supongamos $K \subset E \subset \overline{K}$ y que todo polinomio irreducible de K[X] que tiene una raíz en E tiene todas sus raíces en E.
Sea $\sigma$: $E \to \overline{K}$ un K-homomorfismo. Se trata de probar que $\sigma(E) \subset E$. Si $\alpha \in E$, sea $f(X) \in K[X]$ su polinomio minimal. Sabemos que $\sigma(\alpha)$ es un conjugado de $\alpha$, es decir es raíz de f; entonces, por hipótesis, $\sigma(\alpha) \in E$.

b) Sea E una extensión finita y normal de K. Por ser finita $E = K(\alpha_1,\ldots,\alpha_n)$, $\alpha_i$ algebraico sobre K, $i = 1,\ldots,n$. Sea $f_i \in K[X]$ el polinomio minimal de $\alpha_i$. Como E es normal, por a) E contiene a todas las raíces de cada $f_i$, luego E contiene a todas las raíces del polinomio $f = \prod_{i=1}^{n} f_i$ y por lo tanto es el cuerpo de raíces de f.

Supongamos ahora que E es el cuerpo de raíces de un polinomio $f(X) \in K[X]$. Sean $\alpha_1,\ldots,\alpha_n$ las raíces de f; $E = K(\alpha_1,\ldots,\alpha_n)$ con los $\alpha_i$ algebraicos sobre K, luego E es una extensión finita de K. Veamos que es normal: cualquiera sea el K-homomorfismo $\sigma$: $K(\alpha_1,\ldots,\alpha_n) \to \overline{K}$, $\sigma$ está determinado por los elementos $\sigma(\alpha_1),\ldots,\sigma(\alpha_n)$ que pertenecen a $K(\alpha_1,\ldots,\alpha_n)$, pues o aplica cada raíz de f en una raíz de f. Luego $\sigma$ es un endomorfismo de E y E es normal sobre K.

No vale la transitividad para extensiones normales. Sólo se verifica la siguiente propiedad:

TEOREMA 4.14. Si $K \subset E \subset F$ y F es una extensión normal de K entonces F es una extensión normal de E.

Demostración. Todo E-homomorfismo $F \to \overline{K}$ es en particular un K-homomorfismo.

Ejemplos.

1) $Q \subset Q(\sqrt[4]{2}) \subset Q(\sqrt[4]{2},i)$. $Q(\sqrt[4]{2},i)$ es normal sobre Q, luego sobre $Q(\sqrt[4]{2})$, pero ésta no es una extensión normal de Q.
2) $Q \subset Q(\sqrt{2}) \subset Q(\sqrt[4]{2})$. Cada una de estas extensiones es normal sobre la anterior pero $Q(\sqrt[4]{2})$ no lo es sobre Q.

Ejercicio. Sabemos que dado un cuerpo K, las extensiones algebraicas y las separables forman clases distinguidas.
Demostrar que las extensiones normales de K verifican las propiedades de clase distinguida, excepto la transitividad, como acabamos de ver.

TEOREMA 4.15. Sea $K \subset E \subset \overline{K}$. La intersección N de todas las extensiones normales de K que contienen a E y contenidas en $\overline{K}$ es una extensión normal de K. Si E es una extensión finita de K entonces N es una extensión finita. Si E es una extensión separable de K, N es una extensión normal y separable de K.

Demostración. El conjunto de las extensiones normales L de K tales que $K \subset E \subset L \subset \overline{K}$ no es vacío pues $\overline{K}$ es una de ellas. Para ver que N es normal debemos probar que si $\sigma: N \to \overline{K}$ es K-homomorfismo entonces $\sigma(N) \subset N$. Sea $\overline{\sigma}: \overline{K} \to \overline{K}$ la extensión de $\sigma$ a un automorfismo de $\overline{K}$. Cualquiera sea la extensión normal L de K tal que $K \subset E \subset L \subset \overline{K}$, $\overline{\sigma}/L: L \to \overline{K}$ es un K-homomorfismo y como L es normal sobre K, $\overline{\sigma}/L$ es un automorfismo de L. Luego $\overline{\sigma}(L) = L$. Como $N \subset L$ y $\overline{\sigma}/N = \sigma$ resulta que $\sigma(N) \subset \overline{\sigma}(L) = L$, cualquiera sea L, entonces $\sigma(N) \subset N$ c.q.d.

Veamos ahora cómo es la extensión N.
Se puede considerar $E = K(\{\alpha_i\}_{i \in I})$ donde $\{\alpha_i\}_{i \in I}$ puede ser finita o no. (por ejemplo tomando $\{\alpha_i\}$ una K-base de E). Sea $\{\sigma_j\}_{j \in J}$ el conjunto (finito o no) de todos los K-homomorfismos $E \to \overline{K}$. El conjunto de los elementos $\{\sigma_j(\alpha_i)\}_{i,j}$ está en $\overline{K}$ y consideremos la extensión por ellos generada $L = K(\{\sigma_j(\alpha_i)\})$. Como la inclusión $E \to \overline{K}$ es un K-homomorfismo, está entre los $\sigma_j$ y entonces $K \subset E \subset L \subset \overline{K}$. Queremos probar que $L = N$, para lo cual bastará ver que $L \subset N$ y que L es una extensión normal de K. Es claro que $L \subset N$ pues los $\sigma_j(\alpha_i)$ están en todas las extensiones normales de K que contienen a E.
Sea $\tau: L \to \overline{K}$ un K-homomorfismo. Tenemos que ver que $\tau(L) \subset L$. Si $f_i$ es el polinomio minimal de $\alpha_i$ sobre K, $\sigma_j(\alpha_i)$ es raíz de $f_i$, y como $\tau$ es un K-homomorfismo, $\tau(\sigma_j(\alpha_i))$ también es raíz de $f_i$. Luego existe un K-homomorfismo $K(\alpha_i) \to \overline{K}$ que aplica $\alpha_i$ en $\tau(\sigma_j(\alpha_i))$, y que puede extenderse a uno de $E \to \overline{K}$. Este último debe ser un $\sigma_h$, para algún índice h. Entonces $\tau(\sigma_j(\alpha_i)) = \sigma_h(\alpha_i) \in L$, lo que

prueba que Im $\tau \subset L$. Luego L es una extensión normal de K, y $L \subset N$ implica $L = N$.

Si $[E:K] < \infty$ , $E = K(\alpha_1,\ldots,\alpha_n)$. Como $[E:K]_s < \infty$ , hay un número finito de K-homomorfismos $E \to \overline{K}$, $\sigma_1,\ldots,\sigma_t$ y por lo tanto $N = K(\sigma_j(\alpha_i))$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant t$, es una extensión finita de K.

Finalmente, si E es separable sobre K, $E = K(\{\alpha_i\})$, con los $\alpha_i$ separables sobre K; luego $\sigma_j(\alpha_i)$ es separable sobre K cualquiera sea el K-homomorfismo $\sigma_j: E \to \overline{K}$ (pues $\alpha_i$ y $\sigma_j(\alpha_i)$ tienen el mismo polinomio minimal sobre K) y por lo tanto $N = K(\{\sigma_j(\alpha_i)\})$ es separable sobre K.

El cuerpo N está unívocamente determinado por E salvo E-isomorfismos. Más precisamente, si $\overline{\overline{K}}$ es otra clausura algebraica de K tal que $K \subset E \subset \overline{\overline{K}}$ entonces la intersección N' de todas las extensiones normales de K que contienen a E y contenidas en $\overline{\overline{K}}$ es un cuerpo E-isomorfo a N, lo que queda propuesto como ejercicio.

DEFINICION. El cuerpo N se llama la clausura normal de E sobre K.

Del teorema anterior resulta que toda extensión separable de un cuerpo K está contenida en una extensión normal y separable de K.
Las extensiones normales y separables se llaman extensiones de Galois. Luego toda extensión separable de un cuerpo K está contenida en una extensión Galois de K.

## ELEMENTOS PRIMITIVOS

TEOREMA 4.16. (del elemento primitivo).
Sea E una extensión finita de un cuerpo K. E es una extensión simple de K si y sólo si existe sólo un número finito de subcuerpos intermedios entre K y E. Si E es una extensión finita y separable de K, entonces E es simple.

Demostración. Si K es un cuerpo finito, E es finito y el grupo multiplicativo

$E^*$ es cíclico. (teorema 1.5). Si $\alpha$ es un generador de $E^*$, es claro que $E = K(\alpha)$ y el teorema es trivial.

Sea entonces K infinito. Supongamos que sólo hay un número finito de cuerpos intermedios. Sean $\alpha, \beta \in E$ y para cada $c \in K$ consideremos el cuerpo $K(\alpha + c\beta)$: $K \subset K(\alpha + c\beta) \subset E$. Por las nipótesis hechas, deben existir $c_1, c_2 \in K$, $c_1 \neq c_2$ tales que $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Es claro que $K(\alpha + c_i\beta) \subset K(\alpha,\beta)$. Veamos que son iguales: $\alpha + c_1\beta$ y $\alpha + c_2\beta \in K(\alpha + c_1\beta) \Rightarrow (c_1-c_2)\beta$ pertenece a ese cuerpo y como $c_1-c_2 \neq 0$, $\beta$ pertenece a él $\Rightarrow$ $\alpha$ también $\Rightarrow K(\alpha,\beta) \subset K(\alpha + c_1\beta)$. Luego $K(\alpha,\beta) = K(\alpha + c_1\beta)$.

Razonando por inducción, como $E = K(\alpha_1,\ldots,\alpha_n)$ existen $c_2,\ldots,c_n \in K$ tales que $E = K(\alpha_1,\ldots,\alpha_n) = K(\alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n)$, luego E es simple.

Recíprocamente, sea $E = K(\alpha)$ extensión finita de K y probemos que sólo hay un número finito de cuerpos intermedios entre K y E.

Si $K \subset F \subset E$, como $\alpha$ es algebraico sobre K, lo es sobre F. Sean $f(X) \in K[X]$ y $g(X) \in F[X]$ los polinomios minimales de $\alpha$ sobre K y sobre F. Entonces g/f en $F[X]$. Si $g(X) = b_0 + b_1X + \ldots + b_{t-1}X^{t-1} + X^t$, $K \subset K(b_0,\ldots,b_{t-1}) \subset F$ y el grado de E sobre ambas extensiones es t. Por lo tanto $F = K(b_0,\ldots,b_{t-1})$. Esto muestra que cada cuerpo intermedio F está unívocamente determinado por un factor irreducible de f en $F[X]$. La descomposición de f en irreducibles en $E[X]$ tiene un número finito de factores, y los factores irreducibles de f sobre un cuerpo intermedio son producto de algunos de sus factores irreducibles en $E[X]$. Luego sólo existe un número finito de cuerpos intermedios.

Supongamos ahora que E es finita y separable sobre K, $E = K(\alpha_1,\ldots,\alpha_m)$ con los $\alpha_i$ separables sobre K. Se demuestra que E es simple por inducción sobre m, y entonces es suficiente probarlo para $E = K(\alpha,\beta)$. Suponemos $E \neq K(\alpha)$, $E \neq K(\beta)$ pues de lo contrario no hay nada que probar. Sea $[E:K] = n = [E:K]_s$, $\sigma_1,\ldots,\sigma_n$ los K-nomomorfismos distintos de E en $\bar{K}$. Luego $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ o $\sigma_i(\beta) \neq \sigma_j(\beta)$ si $i \neq j$. Consideremos el polinomio

$$P(X) = \prod_{i \neq j} (\sigma_i(\alpha) + X\sigma_i(\beta) - \sigma_j(\alpha) - X\sigma_j(\beta))$$

Como $P(X)$ no es nulo y $K$ es infinito existe un $c \in K$ tal que $P(c) \neq 0$. Entonces $\sigma_i(\alpha) + c\alpha_i(\beta) \neq \sigma_j(\alpha) + c\sigma_j(\beta)$ para $i \neq j$, es decir los elementos $\sigma_i(\alpha + c\beta)$, $i = 1,\ldots,n$ , son todos distintos. Luego $[K(\alpha + c\beta):K] \geq n$. Pero $K \subset K(\alpha + c\beta) \subset K(\alpha,\beta)$ y $[K(\alpha,\beta):K] = n$, de donde resulta $K(\alpha,\beta) = K(\alpha + c\beta)$, lo que termina la demostración.

DEFINICION. Si $E$ es una extensión finita de $K$ y existe $\alpha \in E$ tal que $E = K(\alpha)$, $\alpha$ se llama un elemento primitivo de $E$.

De la demostración del teorema resulta un método para determinar un elemento primitivo de una extensión finita y separable $K \subset E$ de un cuerpo infinito: si $E = K(\alpha_1,\ldots,\alpha_m)$ y $\sigma_1,\ldots,\sigma_n$ son los $K$-homomorfismos de $E$ en una clausura algebraica $\overline{K}$ entonces es cuestión de hallar elementos $c_2,\ldots,c_m \in K$ tales que los elementos $\sigma_i(\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m)$ , $i = 1,\ldots,n$ sean todos distintos. En ese caso $E = K(\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m)$.

Ejemplos.

1) Sea $Q \subset Q(i,\sqrt[4]{2})$. Como es separable y finita es simple. Hallemos un elemento primitivo: $z = \sqrt[4]{2} + ci$ , $c \in Q$ tal que $\sigma_i(z) \neq \sigma_j(z)$ para todo $i \neq j$, siendo $\{\sigma_i\}$ los $Q$-automorfismos de $Q(\sqrt[4]{2},i)$.

Como $[Q(\sqrt[4]{2},i):Q] = 8$ hay ocho. Ya los calculamos en otro ejemplo.

$\sigma_1(z) = \sqrt[4]{2} + ci$ ; $\sigma_2(z) = \sqrt[4]{2} - ci$ ; $\sigma_3(z) = -\sqrt[4]{2} + ci$ ; $\sigma_4(z) = -\sqrt[4]{2} - ci$ ;

$\sigma_5(z) = \sqrt[4]{2}\,i + ci$ ; $\sigma_6(z) = \sqrt[4]{2}\,i - ci$ ; $\sigma_7(z) = -\sqrt[4]{2}\,i + ci$ ; $\sigma_8(z) = -\sqrt[4]{2}\,i - ci$.

Tomando $c = 1$, no hay dos iguales; luego $z = \sqrt[4]{2} + i$ y $Q(\sqrt[4]{2},i) = Q(\sqrt[4]{2} + i)$.

2) Ejemplo de una extensión finita que no es simple.

(Debe ser no separable, luego el cuerpo base debe ser infinito de car $\neq 0$).

Sea $K = Z_2(X,Y)$. Sea $F = K[U]/_{(U^2-X)} \simeq K(\alpha)$ donde $\alpha = \sqrt{X}$ y sea $E = F[V]/_{(V^2-Y)} \simeq$

$\simeq F(\beta)$ siendo $\beta = \sqrt{Y}$. $K \subset F \subset E$ ; $K \subset K(\sqrt{X}) \subset K(\sqrt{X},\sqrt{Y})$ , $[F:K] = [E:F] = 2$ , luego $[E:K] = 4$.

Si E fuera simple, habría sólo un número finito de cuerpos entre K y E, entonces existirían $c_1, c_2 \in K$, $c_1 \neq c_2$ tales que $K(\sqrt{X} + c_1\sqrt{Y}) = K(\sqrt{X} + c_2\sqrt{Y})$ y de aquí, como en la demostración del teorema, seguiría $E = K(\sqrt{X} + c_1\sqrt{Y})$.

Basta ver entonces que $K(\sqrt{X} + c_1\sqrt{Y}) \neq E$. Pero $(\sqrt{X} + c_1\sqrt{Y})^2 = X + c_1^2 Y \in K$, luego $[K(\sqrt{X} + c_1\sqrt{Y}):K] \leqslant 2$.

EJERCICIOS

1- a) Si E es un cuerpo de característica 0, el cuerpo primo de E es isomorfo a Q. Si car $E = p \neq 0$, el cuerpo primo de E es isomorfo a $Z_p$.

b) Si E y F son cuerpos, todo homomorfismo no nulo $f: E \to F$ aplica el cuerpo primo de E sobre el de F, es decir, f restringido al cuerpo primo de E es un isomorfismo sobre el de F. Luego E y F tienen la misma característica.

c) Si P es el cuerpo primo de E, todo endomorfismo no nulo $f: E \to E$ es un P-homomorfismo.

2- a) Si $Q \subset E \subset C$, probar que todo homomorfismo no nulo $E \to C$ es un Q-homomorfismo.

b) Decir de cuántas maneras puede sumergirse $Q(\sqrt[3]{2})$ en C. ¿y en R?.

c) ¿Cuántos subcuerpos isomorfos a $Q(\sqrt[4]{3})$ hay en C? ¿Cuáles son? ¿Es $Q(\sqrt[4]{5})$ uno de ellos?.

d) ¿Cuántos automorfismos distintos admite $Q(\sqrt[4]{3})$?.

e) Hallar el grado de separabilidad:

i) $[Q(\sqrt{2}+\sqrt{3}):Q]_s$

ii) $[Q(\alpha):Q]_s$ siendo $\alpha \notin Q$ una raíz del polinomio $X^7+X^6+2X+2$.

iii) $[Z_3(\alpha):Z_3]_s$ siendo $\alpha \notin Z_3$ una raíz del polinomio $X^7+X^6+X+1$.

3- Hallar todos los K-automorfismos de E para las siguientes extensiones $K \subset E$:

a) $Q \subset Q(\sqrt{2})$ ; b) $Q \subset Q(\sqrt[3]{7})$ ; c) $Q \subset Q(\sqrt{2} + i)$

4- Decir si las siguientes proposiciones son verdaderas:

a) Si $K \subset E$ todo K-automorfismo de E es un automorfismo de E.

b) Todo monomorfismo $E \to \overline{K}$ es un K-homomorfismo ($K \subset E \subset \overline{K}$).

c) Si $K \subset E$, todo automorfismo de E es un K-automorfismo.

d) Hay un solo homomorfismo no nulo $Q \to Q$.

e) Hay un solo homomorfismo no nulo $C \to C$.

f) $Q(\sqrt{17})$ es separable sobre Q.

g) Si E y F son cuerpos existe un homomorfismo no nulo de E en F.

h) Si E y F tienen la misma característica entonces existe un homomorfismo no nulo de E en F.

i) Si car $K = p \neq 0$ existe un único homomorfismo no nulo $Z_p \to K$.

5- Si $K \subset E$ es una extensión finita sabemos que $[E:K]_s$ divide a $[E:K]$. Se llama grado de inseparabilidad de E sobre K al número $[E:K]/[E:K]_s$. Se lo representa $[E:K]_i$. Luego $[E:K] = [E:K]_s . [E:K]_i$.
Un elemento $\alpha \in E$ se dice puramente inseparable sobre K si $[K(\alpha):K]_s = 1$.
E se dice una extensión puramente inseparable de K si $[E:K]_s = 1$.

Demostrar que:

a) Una extensión finita $K \subset E$ es separable si y sólo si $[E:K]_i = 1$.

b) Si $K \subset E \subset F$ son extensiones finitas $[F:K]_i = [F:E]_i . [E:K]_i$.

c) Una extensión finita $K \subset E$ es a la vez separable y puramente inseparable si y sólo si $E = K$.

6- Sea K un cuerpo de característica $p \neq 0$, $K \subset E$ finita.
Probar que las siguientes propiedades son equivalentes:

a) E es una extensión puramente inseparable de K.

b) $\forall \alpha \in E$, el polinomio minimal de $\alpha$ sobre K es de la forma $X^{p^e} - a$, e entero $\geq 0$.

c) $\forall\ \alpha \in E$, $\alpha^{p^e} \in K$ para algún entero $e \geq 0$.

d) Todos los elementos de E son puramente inseparables sobre K.

e) $E = K(\alpha_1,\ldots,\alpha_t)$ con $\alpha_1,\ldots,\alpha_t$ puramente inseparables sobre K.

7- Si $K \subset E$ es una extensión finita de grado $> 1$ y puramente inseparable sobre K entonces $[E:K]$ es una potencia de p, p primo.

8- Si $K \subset E$ es una extensión finita, sabemos que el conjunto L de todos los elementos de E que son separables sobre K es una extensión separable de K: $K \subset L \subset E$. Demostrar que E es puramente inseparable sobre L. Deducir que toda extensión finita de K se obtiene como una extensión puramente inseparable de una extensión separable de K.

9- Sea $K = Z_3$, $K \subset K(\alpha) \subset \overline{K}$ donde $\alpha$ es una raíz del polinomio $f(X) = X^6+2X^3+2 \in K[X]$.

a) Decir cuántos K-homomorfismos $K(\alpha) \to \overline{K}$ hay. ¿$[K(\alpha):K]_s$ y $[K(\alpha):K]_i$?.

b) Encontrar esos K-homomorfismos. ¿Es $K(\alpha)$ normal sobre K?.

10- Igual que en el ejercicio anterior siendo $K = Z_3(X)$, $K \subset K(\alpha) \subset \overline{K}$ y $\alpha$ una raíz de $f(Y) = Y^3+2X \in K[Y]$.

11- Sea car $K = p \neq 0$. Demostrar que si $\alpha$ es algebraico sobre K, $\alpha$ es separable sobre K si y sólo si $K(\alpha) = K(\alpha^p)$.
Sea $K \subset E$ una extensión finita. Deducir que si E es separable entonces $K.E^{p^n} = E$, $\forall\ n \geq 1$. Recíprocamente, si $K.E^p = E$ entonces E es separable sobre K.
($E^{p^i} = \{x^{p^i} : x \in E\}$, $i \in Z$, es un subcuerpo de E y $K.E^{p^i}$ es el subcuerpo de E generado por K y $E^{p^i}$).

12- Sea K un cuerpo de característica $p \neq 0$, $a,b \in K$ no nulos.

a) Probar que $X^p-X-a$ es irreducible o se factoriza en polinomios de 1er. grado sobre K. (Sugerencia: si $\alpha$ es una raíz entonces $\alpha,\alpha+1,\alpha+2,\ldots,\alpha+(p-1)$ son todas las raíces).

b) Probar que $X^p - b^{p-1}X - a$ es irreducible o se factoriza completamente sobre K. (Hacer $X = bY$).

c) Demostrar que $X^p + b^{p-1}a^{-1}X^{p-1} - a^{-1}$ es irreducible o se factoriza completamente sobre K. (Hacer $X = \frac{1}{Y}$).

13- Decir cuáles de las siguientes extensiones son normales:

a) $Q \subset Q(\sqrt{-5})$.

b) $Q \subset Q(\alpha)$, donde $\alpha$ es la raíz real $\sqrt[5]{9}$.

c) $Q \subset Q(X)$.

d) $Q \subset Q(\sqrt{5}, \sqrt[3]{5})$

e) $R \subset R(\alpha)$ donde $\alpha$ es una de las raíces quintas complejas de 9.

f) $Q \subset Q(\alpha)$ donde $\alpha$ es una raíz de $X^3 + 3X^2 + 3X + 3$.

14- Hallar las clausuras normales de las extensiones del ejercicio anterior que no son normales e indicar su grado.

15- a) Sea $K \subset E \subset \overline{K}$ y N la clausura normal de E en $\overline{K}$. Entonces para todo K-homomorfismo $\sigma: E \to \overline{K}$, $\sigma(E) \subset N$.

b) Si E es finita de grado n sobre K entonces E es separable sobre K si y sólo si hay n K-homomorfismos distintos $E \to N$.

16- Sea $K \subset E \subset M$ con E normal sobre K (finita o no) y M el cuerpo de raíces sobre E de un polinomio $f \in K[X]$. Demostrar que M es normal sobre K.
Si M es el cuerpo de raíces sobre E de un polinomio $f \in E[X]$, vale la conclusión?.

17- Sea $K \subset E \subset M$, M cuerpo de raíces sobre K. Demostrar que E es cuerpo de raíces sobre K si y sólo si todo K-automorfismo de M restringido a E es un endomorfismo de E.

18- Dar un ejemplo $K \subset E \subset F$ tal que F es normal sobre K (y por lo tanto sobre E) y E es normal sobre K.

19- Decir si las siguientes proposiciones son verdaderas:

a) Una extensión normal de un cuerpo K es finita.

b) Una extensión finita de un cuerpo K es normal.

c) Toda extensión separable es normal.

d) Una extensión normal es separable.

e) K es un cuerpo perfecto si y sólo si toda extensión algebraica de K es separable.

f) Toda extensión normal finita es un cuerpo de raíces de algún polinomio.

g) Si K es un cuerpo perfecto, toda extensión algebraica de K es un cuerpo perfecto.

h) Toda extensión finita tiene una clausura normal.

i) Si $K \subset E \subset F$ y $\sigma$ es un K-automorfismo de F entonces $\sigma/E$ es un K-automorfismo de E.

j) Si $K \subset E \subset F$ y F es normal y separable sobre E entonces E es normal y separable sobre K.

l) Toda extensión normal y separable es finita.

m) El único automorfismo que tiene $\mathbb{Q}$ es la identidad.

n) El único automorfismo que tiene $\bar{\mathbb{Q}}$ es la identidad.

o) Toda clausura algebraica de un cuerpo K es una extensión normal y separable de K.

p) Si car K = 0, toda clausura algebraica de K es normal y separable sobre K.

q) Si K es un cuerpo finito toda extensión normal de K es separable.

# CAPITULO V

## CUERPOS FINITOS

En general, si F es un cuerpo, los automorfismos de F forman un grupo Aut(F) con respecto a la composición de aplicaciones. Si $K \subset F$, los K-automorfismos de F forman un subgrupo de Aut(F) que representaremos G(F/K). Si F es una extensión normal de K entonces $|G(F/K)| = [F:K]_s$, y si F es una extensión finita, normal y separable de K entonces $|G(F/K)| = [F:K]$, y G(F/K) se llama el grupo de Galois de F sobre K.
Observar que si P es el cuerpo primo de F, todo automorfismo de F es un P-automorfismo y Aut(F) = G(F/P).

Vamos a estudiar como ejemplo los cuerpos finitos (que también suelen llamarse cuerpos de Galois) y sus automorfismos.

En primer lugar $Z_p$, p primo, es un cuerpo sin subcuerpos propios y el único automorfismo que admite es la identidad.
Si F es un cuerpo finito con q elementos, su característica es un primo p, y el cuerpo primo de F es isomorfo a $Z_p$. En efecto, la aplicación $\sigma: Z \to F$ tal que $n \to n.1_F$ es un homomorfismo de anillos cuyo núcleo es un ideal primo de Z. Como F es finito es Nuc $\sigma = (p)$, con p primo, y $\sigma(Z) \simeq Z/(p)$. Entonces p es la característica de F, $\sigma(Z) \simeq Z_p$ y $\sigma(Z)$ es el cuerpo primo de F. (Notar que hay un único isomorfismo posible entre el cuerpo primo de F y $Z_p$, que es el definido por $1_F \to 1_{Z_p}$). Identificando el cuerpo primo de F con $Z_p$, F puede considerarse una extensión de $Z_p$. Si $[F:Z_p] = n$ entonces F tiene $p^n$ elementos y por lo tanto $q = p^n$. Luego

Todo cuerpo finito tiene $p^n$ elementos, p primo, n entero $\geq 1$.

Si F tiene $p^n$ elementos, el grupo multiplicativo F* es de orden $p^n-1$, luego todo $\alpha \in F^*$ satisface la ecuación $X^{p^n-1} = 1$. Entonces todos los elementos de F,

incluido el cero, son raíces del polinomio $f(X)=X^{p^n}-X$, que tiene sus coeficientes en el cuerpo primo de F. Así f(X) tiene $p^n$ raíces distintas en F, y como éstas forman el cuerpo F, F es un cuerpo de raíces del polinomio $X^{p^n}-X$ sobre su cuerpo primo.

De este resultado y del teorema 4.4 sigue que

Dos cuerpos finitos con el mismo número de elementos son isomorfos.

Por último, existe un cuerpo con $p^n$ elementos, para todo primo p y n entero $\geqslant 1$.

Para probarlo consideremos el polinomio $f(X) = X^{p^n}-X \in Z_p[X]$, que no tiene raíces múltiples pues $f'(X) = -1$, luego $(f,f') = 1$. Entonces f(X) tiene $p^n$ raíces distintas en una clausura algebraica $\overline{Z}_p$. Estas $p^n$ raíces forman un subcuerpo de $\overline{Z}_p$: si $\alpha,\beta \in \overline{Z}_p$ son raíces de f(X) entonces $\alpha \pm \beta$, $\alpha.\beta$, $\beta^{-1}$ $(\beta \neq 0)$ también lo son. En efecto, $\alpha^{p^n}-\alpha = 0$ y $\beta^{p^n}-\beta = 0$ implica $(\alpha \pm \beta)^{p^n} - (\alpha \pm \beta) =$
$= \alpha^{p^n} \pm \beta^{p^n} - \alpha \mp \beta = 0$, y análogamente para las otras.
Se tiene así un cuerpo con $p^n$ elementos, que notaremos $F_{p^n}$. En particular $F_p = Z_p$.

De todo lo dicho resulta el siguiente

TEOREMA 5.1. Dado un primo p, y fijada una clausura algebraica $\overline{Z}_p$, para cada entero $n \geqslant 1$ existe uno y sólo un subcuerpo de $\overline{Z}_p$ con $p^n$ elementos. Es el cuerpo de raíces $F_{p^n}$ del polinomio $X^{p^n}-X$ sobre $Z_p$, que está formado por las raíces de este polinomio. Todo cuerpo finito de característica p es isomorfo a un $F_{p^n}$.

OBSERVACION. (Tal vez el lector la encuentra superflua).

Si F es un cuerpo finito de característica p, su cuerpo primo P es isomorfo a $Z_p$. Sea $\tau: P \to Z_p$ el isomorfismo en cuestión y $\overline{F}$, $\overline{Z}_p$ clausuras algebraicas. Es claro que $\overline{F}$ es una clausura algebraica de P, $\overline{F} = \overline{P}$. Sea $\overline{\tau}: \overline{P} \to \overline{Z}_p$ un isomor-

fismo que extiende a $\tau$. Entonces, usando este isomorfismo, se pueden estudiar las propiedades algebraicas de F y las extensiones y subextensiones de F en $\overline{P}$ estudiando las de $\overline{\tau}(F)$ en $\overline{Z}_p$. De aquí que el estudio algebraico de los cuerpos finitos de característica p pueda reducirse al de los subcuerpos finitos de una clausura $\overline{Z}_p$.

Del teorema sigue que toda extensión finita de un cuerpo finito es una extensión normal. Además es separable pues los cuerpos finitos son perfectos. Luego

COROLARIO 1. Toda extensión finita de un cuerpo finito es normal y separable. (En general a las extensiones normales y separables de un cuerpo se las llama extensiones de Galois).

COROLARIO 2. Sea $F_q$ un cuerpo finito, $q = p^n$ , y $\overline{F}_q$ una clausura algebraica dada. Para cada entero $m \geq 1$ existe en $\overline{F}_q$ una y solo una extensión de $F_q$ de grado m, que es el cuerpo $F_{q^m}$.

Demostración. Es suficiente probarlo para el caso $F_q$ subcuerpo de una clausura algebraica $\overline{Z}_p$. Si $q = p^n$ , $q^m = p^{nm}$. El cuerpo de raíces de $X^{p^{nm}}-X$ sobre $Z_p$ en $\overline{Z}_p$ es $F_{p^{nm}}$ y $F_{p^n} \subset F_{p^{nm}}$ pues cualquiera sea $\alpha \in F_{p^n}$ , $\alpha^{p^n} = \alpha$ implica $\alpha^{p^{nt}} = \alpha$ para todo entero $t \geq 1$. (por inducción sobre t). Luego, en particular, $\alpha^{p^{nm}} = \alpha$ para todo $\alpha \in F_{p^n}$. Además de $Z_p \subset F_{p^n} \subset F_{p^{nm}}$ sigue que $[F_{p^{nm}}:F_{p^n}] = m$ pues el grado de $F_{p^{nm}}$ sobre $Z_p$ es nm y el de $F_{p^n}$ es n.

Como otra propiedad de los cuerpos sabemos que: Si F es un cuerpo, todo subgrupo finito del grupo multiplicativo F* es cíclico. En particular

TEOREMA 5.2. El grupo multiplicativo de un cuerpo finito es cíclico.

Estudiemos ahora el grupo que forman los automorfismos de un cuerpo finito. Si $q = p^n$, sea $F_q$ un cuerpo con q elementos. Como es finito el monomorfismo de

Frobenius $\varphi$: $F_q \to F_q$ tal que $x \mapsto x^p$ es un automorfismo de $F_q$.

TEOREMA 5.3. El grupo de automorfismos de $F_q$ es cíclico de orden n (siendo $q = p^n$) y $\varphi$ es un generador.

Demostración. $\varphi^n = id$ pues $\varphi^n(x) = x^{p^n} = x$ cualquiera sea $x \in F_q$.
Sea d el orden de $\varphi$ en el grupo de automorfismos de $F_q$, es decir el menor entero $\geq 1$ tal que $\varphi^d = id$. Entonces $d \leq n$ y $\varphi^d(x) = x^{p^d} = x$ para todo $x \in F_q$.
Por otro lado, como el polinomio $X^{p^d}-X$ tiene a lo sumo $p^d$ raíces, sigue $p^d \geq p^n$. Luego $d = n$.
Falta probar que $\varphi$ genera $Aut(F_q)$. Cualquier automorfismo de $F_q$ deja fijo al cuerpo primo $F_p$, luego es un $F_p$-automorfismo. Como $[F_q:F_p] = n$, el número de $F_p$-automorfismos de $F_q$ es $\leq n$. Entonces $Aut(F_q) = (\varphi)$.

TEOREMA 5.4. Sean m,n enteros $\geq 1$, $\overline{Z}_p$ una clausura dada, $F_{p^n}$, $F_{p^m}$ subcuerpos de $\overline{Z}_p$. Entonces $F_{p^n} \subset F_{p^m}$ si y sólo si n divide a m. Si $F_{p^n} \subset F_{p^m}$, $F_{p^m}$ es normal y separable sobre $F_{p^n}$ de grado m/n y el grupo de $F_{p^n}$-automorfismos de $F_{p^m}$ es cíclico, generado por $\varphi^n$, siendo $\varphi$ el automorfismo de Frobenius de $F_{p^m}$.

Demostración. Si $F_{p^n} \subset F_{p^m}$, $[F_{p^n}:F_p]$ = n divide a $[F_{p^m}:F_p]$ = m.
Recíprocamente, supongamos que n divide a m. Por el corolario 2 del teorema 5.1 $F_{p^n}$ tiene en $\overline{Z}_p$ una única extensión de grado m/n, y es $F_{p^m}$. Luego $F_{p^n} \subset F_{p^m}$.
Queda a cargo del lector terminar la demostración.

COROLARIO. Toda extensión finita E de un cuerpo finito F es una extensión de Galois y su grupo de Galois G(E/F) es cíclico.

Ejercicios.

1- Para cuáles de los siguientes n existe un cuerpo con n elementos?
1 , 2 , 3 , 4 , 5 , 6 , 17 , 24 , 312 , 16.807.

2- a) Construir cuerpos con 4, 8, 9, 16 y 27 elementos.

b) Indicar cómo construir un cuerpo con $p^p$ elementos, p primo.

c) Indicar generadores de los grupos multiplicativos de los cuerpos de a).

3- Sea K un cuerpo finito. Probar que para todo entero $n > 0$ existe un polinomio irreducible sobre K de grado n. Concluir que una clausura algebraica $\overline{K}$ es una extensión infinita de K (y numerable).

4- Dibujar el reticulado que forman los cuerpos $F_3$, $F_9$, $F_{27}$, $F_{81}$, $F_{243}$ y $F_{729}$ con respecto a la relación de inclusión, suponiéndolos contenidos en una clausura $\overline{F}_3$.

5- Demostrar que el grupo aditivo de $F_{p^n}$ es la suma directa de n subgrupos cíclicos de orden p.

6- Sea $F_{p^n}$ y $f(X) \in F_{p^n}[X]$ irreducible. Demostrar que:

$f(X) \mid X^{p^{n.m}} - X$ si y sólo si $gr\, f \mid m$.

Luego $X^{p^{n.m}} - X = \prod_{d/m} \left( \prod_{\substack{f_d \text{ irreducible} \\ gr\, f_d = d}} f_d(X) \right)$.

Deducir que $p^{n.m} = \sum_{d/m} d\, \psi(d)$ , siendo $\psi(d) =$ n° de polinomios irreducibles de grado d en $F_{p^n}[X]$.

7- Sea E una extensión simple de un cuerpo K, $[E:K] = n$.
Probar que el número de cuerpos intermedios (incluyendo K y E) es a lo sumo $2^{n-1}$.

8- Si $Q \subset Q(\sqrt[3]{5}, \varepsilon)$ , $\varepsilon^3 = 1$, $\varepsilon \neq 1$, hallar los cuerpos intermedios.

Idem para $Q \subset Q(\sqrt[4]{2})$.

9- Decir si las siguientes proposiciones son verdaderas o falsas:

a) Existe un cuerpo con 124 elementos.

b) Existe un cuerpo cuyo grupo multiplicativo tiene 124 elementos.

c) El grupo multiplicativo de $F_{19}$ tiene un único elemento de orden 3.

d) Todos los cuerpos con 121 elementos son isomorfos.

e) $F_{p^n}$ contiene un único subcuerpo con $p^m$ elementos, $\forall\ 1 \leq m \leq n$.

f) $F_{16}$ contiene un subcuerpo isomorfo a $F_8$.

g) Todo endomorfismo no nulo de un cuerpo finito es un automorfismo.

h) El grupo aditivo de un cuerpo finito es cíclico.

i) Ningún cuerpo finito es algebraicamente cerrado.

j) Si F es un cuerpo finito sólo hay un número finito de polinomios de grado n irreducibles sobre F.

l) Toda extensión algebraica de un cuerpo finito es finita.

m) Toda extensión finita de un cuerpo finito es una extensión simple.

n) $F_{75}$ tiene 5 subcuerpos.

o) Todo cuerpo finito que no tiene un número primo de elementos tiene un único subcuerpo maximal.

p) Todo cuerpo finito es una extensión abeliana de su cuerpo primo.

q) Todo cuerpo finito es una extensión cíclica de cualquiera de sus subcuerpos.

# CAPITULO VI

## EXTENSIONES DE GALOIS

Sabemos que si E es un cuerpo todos los automorfismos de E forman un grupo Aut(E) con respecto a la composición de aplicaciones. Si $F \subset E$ es un subcuerpo de E, el conjunto de los F-automorfismos de E es un subgrupo de Aut(E) que representaremos G(E/F).

Se tiene así una aplicación $F \to G(E/F)$ que a cada subcuerpo de E asocia un subgrupo de Aut(E).

Por otra parte, si H es un grupo de automorfismos de E (no necesariamente el de todos los automorfismos, es decir, $H \subset Aut(E)$), el conjunto de todos los elementos $x \in E$ tales que $\sigma(x) = x$ cualquiera sea $\sigma \in H$, es un subcuerpo de E.
Se llama el cuerpo fijo de H y lo representaremos $E^H$.

$$E^H = \{x \in E: \sigma(x) = x \text{ , cualquiera sea } \sigma \in H\}.$$

Se tiene así otra aplicación $H \to E^H$ del conjunto de todos los subgrupos de Aut(E) en el conjunto de los subcuerpos de E.

Es fácil ver que:

1) $H_1 \subset H_2 \subset Aut(E) \Rightarrow E^{H_2} \subset E^{H_1}$.

2) $F_1 \subset F_2 \subset E \Rightarrow G(E/F_2) \subset G(E/F_1)$.

3) $F \subset E^{G(E/F)}$.

4) $H \subset G(E/E^H)$.

DEFINICION. Dado un cuerpo K, una extensión algebraica $K \subset E$ se dice una extensión de Galois de K si E es normal y separable sobre K. También se dice que E es Galois sobre K o que E es una extensión galoisiana de K.

Si E es Galois sobre K, el grupo G(E/K) se llama el grupo de Galois de E sobre K y coincide con el conjunto de todos los K-nomomorfismos $E \to \overline{K}$.

Si $K \subset E$ es una extensión finita y Galois de K, entonces para cualquier cuerpo intermedio $K \subset F \subset E$, E es una extensión finita y Galois de F y

$$|G(E/F)| = [E:F].$$

En particular, $$|G(E/K)| = [E:K].$$

DEFINICION. Una extensión E de un cuerpo K se dice una extensión abeliana (resp. cíclica) si E es Galois sobre K y su grupo de Galois es abeliano (resp. cíclico).

Ejemplos.

1) Si $K = E$, $G(E/F) = \{id\}$.

2) $Q \subset Q(\sqrt{2})$ es normal y separable, luego es Galois sobre Q. Los Q-automorfismos de $Q(\sqrt{2})$ son dos: id y $\sigma$, donde $\sigma(\sqrt{2}) = -\sqrt{2}$. $G(Q(\sqrt{2})/Q) \simeq Z_2$ y $G(Q(\sqrt{2})/Q) = Aut(Q(\sqrt{2}))$.

3) $R \subset C$. Como $C = R(i)$, es Galois sobre R y $G(C/R) \simeq Z_2$.

4) $Q \subset Q(\sqrt[3]{5})$. No es Galois sobre Q, $G(Q(\sqrt[3]{5})/Q) = \{id\} = Aut(Q(\sqrt[3]{5}))$.

5) Sea E el cuerpo de raíces del polinomio $X^3-5$ sobre Q. $E = Q(\sqrt[3]{5},\varepsilon)$ siendo $\varepsilon$ una raíz primitiva de la unidad de tercer orden, $[E:Q] = 6$. E es una extensión Galois de Q y $G(E/Q) = Aut(E) \simeq S_3$. En este ejemplo cada permutación de las tres raíces de $X^3-5$ determina un automorfismo de E, lo que no es cierto en general.

6) Ya vimos que toda extensión finita de un cuerpo finito es normal y separable, de ahí el nombre de cuerpos de Galois que se les da a los cuerpos finitos. Si $K \subset E$ son cuerpos finitos, sabemos que $G(E/K) \simeq Z_n$ siendo $n = [E:K]$. Luego toda extensión finita de un cuerpo finito es una extensión cíclica.

7) $Q \subset R$ es de grado infinito (no algebraica). Se tiene que $G(R/Q) = \{id\} = Aut(R)$. Para verlo vamos a demostrar que cualquiera sea el automorfismo $\sigma$

de R, $\sigma$ es monótono, es decir, $a < b$ implica $\sigma(a) < \sigma(b)$. Es suficiente ver que $0 < a$ implica $0 < \sigma(a)$. Si $a > 0$ entonces existe $x \in R$ tal que $x^2 = a$, de donde $\sigma(a) = \sigma(x^2) = (\sigma(x))^2 > 0$.

Supongamos ahora que $\sigma \neq id_R$, lo que implica que existe $a \in R$ tal que $\sigma(a) \neq a$, de donde $\sigma(a) < a$ o $a < \sigma(a)$. Sea, por ejemplo, la primera desigualdad, entonces existe $q \in Q$ tal que $\sigma(a) < q < a$, de donde sigue $\sigma(q) = q < \sigma(a)$, contradicción.

EJERCICIO. Sea $Q \subset Q(\sqrt[4]{2})$. Hallar el cuerpo fijo de $G(Q(\sqrt[4]{2})/Q)$.

Sólo vamos a estudiar las extensiones de Galois finitas.
Para demostrar el resultado fundamental de la teoría de Galois probaremos primero:

TEOREMA 6.1. Si $K \subset E$ es una extensión finita, entonces E es Galois sobre K si y sólo si K es el cuerpo fijo de $G(E/K)$.

Demostración. Es fácil ver que si $K \subset E$ es una extensión Galois entonces K es el cuerpo fijo de $G(E/K)$. En efecto, es claro que $K \subset E^{G(E/K)}$. Por otro lado, si $a \in E^{G(E/K)}$, como a es separable su polinomio minimal sobre K debe ser de primer grado pues si no a tendría un conjugado $b \neq a$ y existiría $\sigma \in G(E/K)$ tal que $\sigma(a) = b$. Luego el polinomio minimal de a es $X-a$ y $a \in K$.

La otra implicación, si $K \subset E$ es una extensión finita y K es el cuerpo fijo del grupo $G(E/K)$ entonces E es una extensión Galois de K, resulta de los dos teoremas siguientes:

TEOREMA 6.2. Sea $K \subset E$ una extensión separable. Si existe un entero $n \geq 1$ tal que todo elemento $\alpha \in E$ es de grado $\leq n$ sobre K, entonces E es una extensión finita de K y $[E:K] \leq n$.

Demostración. Sea $\alpha \in E$ un elemento tal que $[K(\alpha):K]$ es maximal, $[K(\alpha):K] = m \leq n$. Vamos a probar que $E = K(\alpha)$. Si no fuera así, existiría $\beta \in E-K(\alpha)$ y como $K(\alpha,\beta)$ es una extensión finita y separable de K, por el teorema del elemen-

to primitivo existe $\gamma \in E$ tal que $K(\alpha,\beta) = K(\gamma)$. Pero de $K \subset K(\alpha) \subset K(\alpha,\beta)$ se ve que $[K(\alpha,\beta):K] > m$ lo que implica grado de $\gamma > m$, contradicción.

TEOREMA 6.3. (Artin). Sea E un cuerpo y G un grupo finito de automorfismos de E de orden n. Sea $K = E^G$ el cuerpo fijo. Entonces E es una extensión Galois finita de K, su grupo de Galois es G y $[E:K] = n$.

Demostración. Sea $\alpha \in E$ y $\sigma_1,\ldots,\sigma_r$ un conjunto maximal de elementos de G tal que $\sigma_1(\alpha),\ldots,\sigma_r(\alpha)$ son distintos. Si $\tau \in G$ entonces $(\tau\sigma_1(\alpha),\ldots,\tau\sigma_r(\alpha))$ difiere de $(\sigma_1(\alpha),\ldots,\sigma_r(\alpha))$ sólo en una permutación pues $\tau$ es inyectivo y cada $\tau\sigma_i(\alpha)$ es uno de los $\sigma_j(\alpha)$, pues si no $\sigma_1,..,\sigma_r$ no sería maximal. Entonces $\alpha$ es raíz del polinomio $f(X) = \prod_{i=1}^{r} (X-\sigma_i(\alpha))$ y cualquiera sea $\tau \in G$, se tiene que $\tilde{\tau}(f(X)) = f(X)$, es decir los coeficientes de f son invariantes para todo $\tau \in G$, luego $f(X) \in K[X]$. Como f es separable, resulta que todo elemento $\alpha \in E$ es raíz de un polinomio separable de K[X] de grado $\leq n$. Además este polinomio se factoriza en polinomios de primer grado en E[X], lo que prueba que E es una extensión normal y separable de K, y por el teorema anterior $[E:K] \leq n$. Como $G \subset G(E/K)$ y orden $G(E/K) = [E:K]$, debe ser $[E:K] = n$ y $G = G(E/K)$.

COROLARIO. Si $K \subset E$ es una extensión finita y el cuerpo fijo de G(E/K) es K entonces E es una extensión Galois de K.

Vamos a demostrar ahora el resultado fundamental de la teoría de Galois.

TEOREMA 6.4. Sea $K \subset E$ una extensión finita Galois sobre K, $G = G(E/K)$ su grupo de Galois. A cada subcuerpo intermedio F, $K \subset F \subset E$, se le asocia el subgrupo $H \subset G$ tal que $H = G(E/F)$, y a cada subgrupo H de G se le asocia su cuerpo fijo $F = E^H$. Entonces

a) Estas aplicaciones son biyecciones entre el conjunto F de los subcuerpos intermedios y el conjunto S de los subgrupos de G, una inversa de la otra. Además $F_1 \subset F_2$ si y sólo si $H_2 \subset H_1$.

b) Un cuerpo intermedio F es Galois sobre K si y sólo si el grupo correspondien-

te $H = G(E/F)$ es un subgrupo normal de $G$, y en tal caso la aplicación $G \to G(F/K)$ definida por $\sigma \mapsto \sigma/F$ induce un isomorfismo.

$$G/H \simeq G(F/K).$$

c) Si $F_1$ y $F_2$ son dos cuerpos intermedios, existe un K-homomorfismo $F_1 \to F_2$ si sólo si existe un $\sigma \in G$ tal que $\sigma^{-1}H_2\sigma \subset H_1$, siendo $H_i = G(E/F_i)$, $i = 1,2$. En particular $F_1$ y $F_2$ son K-isomorfos si y sólo si existe $\sigma \in G$ tal que $\sigma^{-1}H_2\sigma = H_1$. Más precisamente, $\sigma \in G$ es tq $\sigma(F_1) = F_2$ si y sólo si $\sigma^{-1}H_2\sigma = H_1$.

Demostración. a) Sean $\theta: F \to S$ y $\theta': S \to F$ las aplicaciones definidas en el enunciado: $\theta(F) = G(E/F)$ $\forall$ $F \in F$ ; $\theta'(H) = E^H$ $\forall$ $H \in S$.

Vamos a demostrar que $\theta \circ \theta' = id_S$ y $\theta' \circ \theta = id_F$.

Si $H \in S$, $\theta'(H) = E^H$. Por el teorema 6.3, el grupo de Galois $G(E/E^H) = H$, luego $\theta(\theta'(H)) = H$ , $\forall$ $H \in S$.

Si $F \in F$, como E es una extensión Galois de F, F es el cuerpo fijo de $G(E/F)$, es decir $F = \theta'(\theta(F))$.

Ya vimos que $F_1 \subset F_2 \iff H_2 \subset H_1$.

b) Sea $K \subset F \subset E$ , $H = G(E/F)$.
Supongamos que F es una extensión Galois de K. Entonces es normal y la restricción $\sigma \mapsto \sigma/F$ define una aplicación $\varphi: G \to G(F/K)$, que es un nomomorfismo de grupos cuyo núcleo es H. Luego H es un subgrupo normal de G. Además $\varphi$ es un epimorfismo pues todo K-automorfismo $\sigma: F \to F$ puede extenderse a un K-automorfismo $\overline{\sigma}: E \to E$. Luego $G/H \simeq G(F/K)$.

Supongamos anora que $H \lhd G$ y probemos que F es Galois sobre K. Como F es separable sobre K, hay que probar que es normal, o sea que todo K-nomomorfismo $\sigma: F \to \overline{K}$ es un automorfismo de F, para lo cual es suficiente ver que es un endomorfismo, es decir, que $\sigma(a) \in F$ para todo $a \in F$. Y para probar esto basta ver que si $a \in F$, $\sigma(a)$ es fijo para todos los $\tau \in G(E/F) = H$.

Sea $\overline{\sigma}: E \to E$ una extension de $\sigma$ a E. Como $H \lhd G$, $\overline{\sigma}^{-1}\tau\overline{\sigma} \in H$ para todo $\tau \in H$ $\Rightarrow$

$\Rightarrow \bar{\sigma}^{-1}\tau\bar{\sigma} = \tau' \Rightarrow (\bar{\sigma}^{-1}\tau\bar{\sigma})(a) = \tau'(a) = a$ para todo $a \in F \Rightarrow \tau\bar{\sigma}(a) = \bar{\sigma}(a)$. Pero $\bar{\sigma}/F = \sigma$, luego $\tau\sigma(a) = \sigma(a)$, $\forall\, a \in F$, $\tau \in H$.

c) Sean $F_1$ y $F_2$ dos cuerpos intermedios, $\tau\colon F_1 \to F_2$ un K-homomorfismo. Queremos probar que existe un $\sigma \in G$ tal que $\sigma^{-1}H_2\sigma \subset H_1$. Sea $\bar{\tau}\colon E \to E$ una extensión de $\tau$ a un automorfismo de E, $\bar{\tau}/F_1 = \tau$. Veamos que $\sigma = \bar{\tau}$ cumple lo pedido: $\bar{\tau}^{-1}H_2\bar{\tau} \subset H_1$. Cualesquiera sean $\phi \in H_2$, $x \in F_1$, se tiene $(\bar{\tau}^{-1}\phi\bar{\tau})(x) = \bar{\tau}^{-1}(\bar{\tau}(x)) = x$. Luego $\bar{\tau}^{-1}\phi\bar{\tau} \in H_1$.

Recíprocamente, sean $F_1$ y $F_2$ cuerpos intermedios y supongamos que existe $\sigma\colon E \to E$ K-automorfismo tal que $\sigma^{-1}H_2\sigma \subset H_1$. Entonces $\sigma/F_1$ es un K-homomorfismo $F_1 \to F_2$. Para verlo hay que demostrar que $\mathrm{Im}(\sigma/F_1) \subset F_2$ y para esto basta probar que si $x \in F_1$, $\sigma(x)$ es invariante por todo $\tau \in H_2$, o sea, que $\tau\sigma(x) = \sigma(x)$. Por la hipótesis $\sigma^{-1}\tau\sigma = \phi \in H_1$, lo que implica $\tau\sigma(x) = \sigma\phi(x) = \sigma(x)$ cualquiera sea $x \in F_1$.

La demostración de lo que resta en c) queda propuesta como ejercicio.

OBSERVACION. Del teorema resulta que si $K \subset E$ es finita y Galois, cualquiera sea el cuerpo intermedio $K \subset F \subset E$, si $G = G(E/K)$ y $H = G(E/F)$ se tiene

$$[H:1] = [E:F] \qquad y \qquad [G:H] = [F:K].$$

En efecto, $[E:K] = [E:F].[F:K]$

$$[G:1] = [H:1].[G:H]$$

Como E es Galois sobre K y sobre F, $[E:K] = [G:1]$ y $[E:F] = [H:1]$, luego $[G:H] = [F:K]$.

Ejemplo: Sea $E = Q(\sqrt[4]{2}, i)$. E es el cuerpo de raíces sobre Q del polinomio $X^4-2$, luego E es una extensión normal, finita y separable de Q, es decir Galois sobre Q. Sabemos que $[E:Q] = 8$, luego el grupo de Galois G de E sobre Q es de orden 8. Ya se calcularon en un ejemplo anterior los ocho elementos de G.
Es fácil verificar que G está generado por los automorfismos

$$\sigma\begin{cases}\sqrt[4]{2} \to \sqrt[4]{2}\,i \\ i \to i\end{cases} \qquad y \qquad \tau\begin{cases}\sqrt[4]{2} \to \sqrt[4]{2} \\ i \to -i\end{cases}$$

Se ve que $\sigma^4 = 1 = \tau^2$ , $\sigma\tau = \tau\sigma^3$ y $G = \{1,\sigma,\sigma^2,\sigma^3,\tau,\sigma\tau,\sigma^2\tau,\sigma^3\tau\}$. Entonces $G \simeq D_4$ grupo dihedral de orden 8.

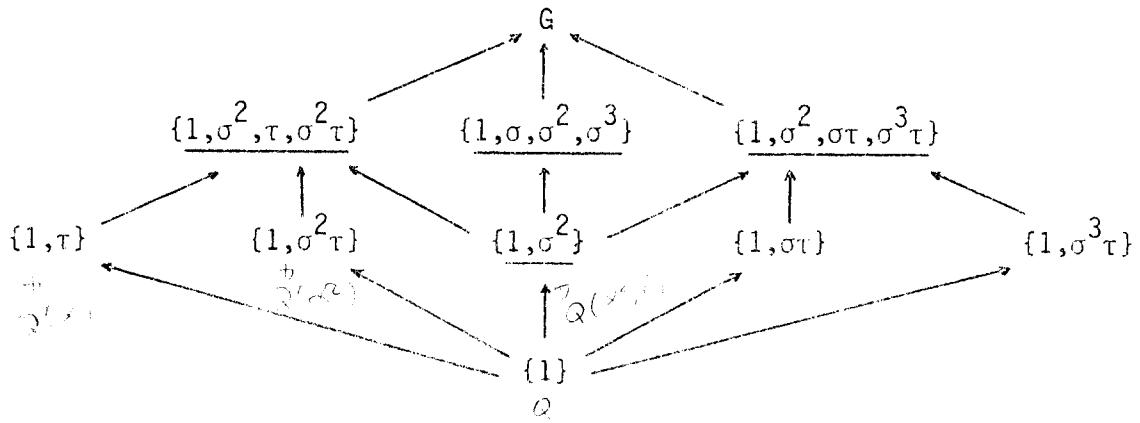
Estudiemos la correspondencia que establece el teorema de Galois. Los subgrupos de G son:

De orden 1: $\{1\}$.

De orden 2: $\{1,\tau\}$ , $\{1,\sigma^2\}$ , $\{1,\sigma\tau\}$ , $\{1,\sigma^2\tau\}$ , $\{1,\sigma^3\tau\}$.

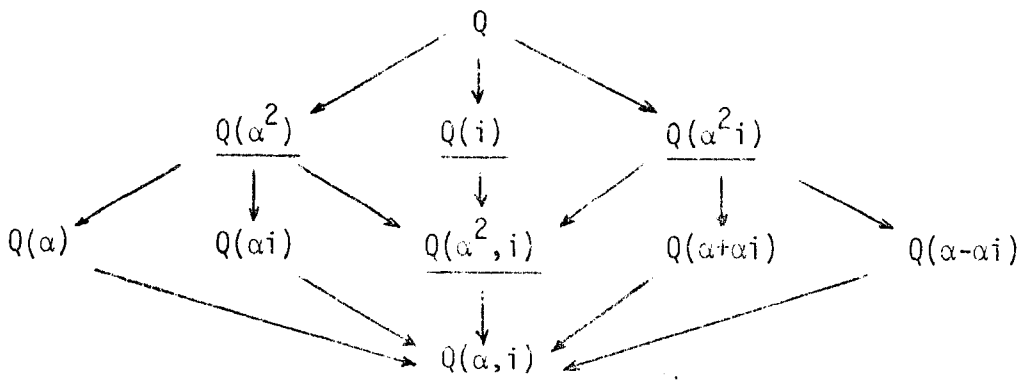
De orden 4: $\{1,\sigma,\sigma^2,\sigma^3\}$ , $\{1,\sigma^2,\tau,\sigma^2\tau\}$ , $\{1,\sigma^2,\sigma\tau,\sigma^3\tau\}$.

Podemos ordenarlos por la relación de inclusión y forman el siguiente reticulado




Los subgrupos normales de G son todos los de orden 4 y el subgrupo $\{1,\sigma^2\}$. Aparecen subrayados en el dibujo.

El reticulado de los cuerpos fijos correspondientes es el siguiente, siendo $\alpha = \sqrt[4]{2}$:




Las extensiones intermedias que son Galois sobre Q aparecen subrayadas. De acuerdo con c) del teorema fundamental, dos extensiones intermedias son isomorfas si y sólo si sus grupos asociados son subgrupos conjugados de G. Se ve que:

$$\sigma\{1,\tau\}\sigma^3 = \{1,\sigma^2\tau\} \quad \Rightarrow \quad Q(\alpha) \simeq Q(\alpha\, i)$$

$$\sigma\{1,\sigma\tau\}\sigma^3 = \{1,\sigma^3\tau\} \quad \Rightarrow \quad Q(\alpha+\alpha i) \simeq Q(\alpha-\alpha i)$$

Señalar las extensiones cíclicas de Q. : $Q(\alpha^2 i)$, $Q(i)$, [illegible]

APLICACIONES

1) Grupo de Galois de un polinomio. Si K es un cuerpo y $f(X) \in K[X]$ es un polinomio de grado $\geqslant 1$, sea E su cuerpo de raíces sobre K. Supongamos que las raíces de f son distintas. Entonces E es una extensión Galois y finita de K. Su grupo de Galois G se llama el grupo de Galois de f sobre K. Sea

$$f(X) = a_n(X-\alpha_1) \ldots (X-\alpha_n)$$

la descomposición de f en producto de polinomios de primer grado en E[X]. Cada K-automorfismo $\sigma \in G$ permuta las raíces $\alpha_1,\ldots,\alpha_n$. Entonces se tiene una aplicación $G \to S_n$ que es un monomorfismo de grupos, y en consecuencia G es isomorfo a un subgrupo de $S_n$. En general no es cierto que ese monomorfismo sea un epimorfismo, es decir, no toda permutación de las raíces proviene de un K-automorfismo de E.

2) Discriminante de un polinomio. Sea f(X) un polinomio con coeficientes en un cuerpo K de característica $\neq 2$, de grado $n \geqslant 1$. Supondremos que las raíces

$\alpha_1,\ldots,\alpha_n$ de f son distintas. Vamos a pensar el grupo de Galois G de f sobre K como un grupo de permutaciones de las raíces, o sea como subgrupo de $S_n$. El elemento

$$\delta = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ \ldots\ (\alpha_{n-1}-\alpha_n) = \prod_{i<j} (\alpha_i-\alpha_j)$$

pertenece al cuerpo de raíces E de f sobre K; cualquier permutación par de las raíces deja fijo a $\delta$ y cualquier permutación impar transforma $\delta$ en $-\delta$. Si $\delta$ queda fijo por todas las permutaciones de G quiere decir que $G \subset A_n$, o sea, $G = G \cap A_n$, y $\delta \in K$; si no, G contiene permutaciones impares, $\delta \notin K$, $A = G \cap A_n$ es un subgrupo normal de G de índice dos, y entonces el cuerpo fijo $E^A$ es una extensión Galois de K de grado dos. Como $\delta \in E^A$ es $K(\delta) = E^A$. Queda probado así

TEOREMA 6.5. Sea K un cuerpo de car $\neq 2$, $f(X) \in K[X]$ un polinomio de grado $n > 0$ con raíces distintas $\alpha_1,\ldots,\alpha_n$, E su cuerpo de raíces, $G = G(E/K)$ su grupo de Galois y

$$\delta = \prod_{1\le i<j\le n} (\alpha_i-\alpha_j).$$

Entonces el cuerpo fijo de $G \cap A_n$ es $K(\delta)$.

COROLARIO. G está formado por permutaciones pares si y sólo si $\delta \in K$, o sea, si y sólo si el elemento $\Delta = \delta^2$ es un cuadrado en K.

$\Delta$ se llama el discriminante de f(X). Es claro que $\Delta = \delta^2$ es invariante por cualquier permutación de $S_n$, en particular por cualquiera de G, luego $\Delta \in K$.

Veamos cómo determinar el grupo de Galois de los polinomios de 2° y 3° grado. Se pueden suponer mónicos.

3) Sea K un cuerpo de car $\neq 2$, $f(X) = X^2+bX+c \in K[X]$. El discriminante de f es $\Delta = b^2-4c$ y el grupo de Galois G de f es un subgrupo de $S_2$. Como el cuerpo de raíces de f es de grado 1 ó 2, G tiene uno o dos elementos, luego $G = \{id\}$ o $G = S_2 \simeq Z_2$ según $\Delta$ es o no un cuadrado en K. $K(\delta)$ es el cuerpo de raíces de f.

4) Sea K un cuerpo de car $\neq 2,3$, $f(X)$ un polinomio irreducible cúbico de $K[X]$. Todo polinomio $X^3+bX^2+cX+d$ se puede escribir $Y^3+pY+q$ completando el cubo, es decir haciendo $X = Y - \frac{b}{3}$. Podemos suponer entonces

$$f(X) = X^3+bX+c .$$

f es separable. Su cuerpo de raíces sobre K es de grado 3 ó 6, luego el grupo de Galois G de f tiene 3 ó 6 elementos, y como G es un subgrupo de $S_3$ es $G = A_3$ o $G = S_3$. Para saber cuál es el caso se puede usar el discriminante:

$$\Delta = \delta^2 = ((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3))^2$$

y haciendo cuentas se ve que

$$\Delta = -4b^3 - 27c^2$$

Si $\Delta$ es un cuadrado en K es $G = A_3 \simeq Z_3$ , si no es $G = S_3$.

Por ejemplo, $f(X) = X^3+X+1$ es irreducible sobre Q. Su discriminante es -31, que no es un cuadrado en Q. Luego el grupo de Galois de f es $S_3$.

Si $f(X) = X^3-3X+1$, f es irreducible sobre Q. El discriminante es $81 = 9^2$, luego el grupo de Galois $G \simeq Z_3$.

$f(X) = X^3-7X+7$ es irreducible sobre Q; $\Delta = 7^2$, luego $G \simeq Z_3$.

En general es difícil determinar el grupo de Galois de un polinomio de grado mayor que tres. Para los de cuarto grado puede verse en I. Kaplansky, Introduçao a la Teoría de Galois, o T.W.Hungerford, Algebra.

5) Un polinomio con grupo de Galois $S_n$.

Dado un cuerpo K, n elementos $t_1,t_2,\ldots,t_n$ de una extensión de K se dicen algebraicamente independientes sobre K si no existe ningún polinomio no nulo $f \in K[X_1,X_2,\ldots,X_n]$ tal que $f(t_1,t_2,\ldots,t_n) = 0$. En ese caso $K[t_1,t_2,\ldots,t_n] \simeq K[X_1,X_2,\ldots,X_n]$ y por lo tanto $K(t_1,t_2,\ldots,t_n) \simeq K(X_1,X_2,\ldots,X_n)$.

Para n=1 esta noción coincide con la de trascendencia.

Se puede pensar que el grupo $S_n$ actúa sobre el anillo $K[t_1,\ldots,t_n]$ permutando $t_1,\ldots,t_n$, es decir, cada $\sigma \in S_n$ define un K-automorfismo de $K[t_1,\ldots,t_n]$, que notaremos también $\sigma$, tal que

$$\sigma(g(t_1,\ldots,t_n)) = g(t_{\sigma(1)},\ldots,t_{\sigma(n)}) \quad \text{cualquiera sea} \quad g \in K[t_1,\ldots,t_n].$$

De esta manera $S_n$ se identifica con un grupo de K-automorfismos de ese anillo.

Un polinomio $g \in K[t_1,\ldots,t_n]$ se dice simétrico si $\sigma(g) = g$ para todo $\sigma \in S_n$.

$S_n$ actúa análogamente sobre $K(t_1,\ldots,t_n)$, $S_n$ es un subgrupo del grupo $G(K(t_1,\ldots,t_n)/K)$ y el cuerpo fijo F de $S_n$ es el que forman las funciones simétricas f/g.

Vamos a ver ahora un ejemplo de un polinomio cuyo grupo de Galois es $S_n$.

Sea K un cuerpo, $t_1,\ldots,t_n$ elementos algebraicamente independientes sobre K.

Consideremos el polinomio

$$f(X) = \prod_{i=1}^{n} (X-t_i) = X^n - s_1X^{n-1} + \ldots + (-1)^n s_n$$

Sus coeficientes $s_i$ son polinomios simétricos en $t_1,\ldots,t_n$:

$$s_1 = t_1+\ldots+t_n \;,\; s_2 = \sum_{1\le i<j\le n} t_it_j \;,\; s_3 = \sum_{1\le i<j<k\le n} t_it_jt_k \;,\; \ldots \;,\; s_n = t_1.t_2\ldots t_n.$$

$s_1,s_2,\ldots,s_n$ se llaman los polinomios o funciones simétricas elementales en $t_1,\ldots,t_n$.

f(X) tiene sus coeficientes en el cuerpo $K(s_1,\ldots,s_n)$, sus raíces son todas distintas, y $E = K(t_1,\ldots,t_n)$ es el cuerpo de raíces de f sobre $K(s_1,\ldots,s_n)$.

Queremos probar que el grupo de Galois de f es $S_n$: $G(E/K(s_1,\ldots,s_n)) = S_n$.

$S_n$ actúa sobre E como dijimos, cada $\sigma \in S_n$ induce un K-automorfismo de E, y si F es el cuerpo fijo de $S_n$, es $G(E/F) = S_n$ (teorema 6.3).

Se trata de probar que $F = K(s_1,\ldots,s_n)$. Es claro que $K(s_1,\ldots,s_n) \subset F \subset E$. Por otro lado, $[E:F] = n!$ y $[E:K(s_1,\ldots,s_n)] \leq n!$ pues E es el cuerpo de raíces de f sobre $K(s_1,\ldots,s_n)$. Luego $F = K(s_1,\ldots,s_n)$.

OBSERVACION. La igualdad $F = K(s_1,\ldots,s_n)$ resulta también de la siguiente propiedad fundamental de los polinomios simétricos elementales, que enunciamos sin demostración:
En general, si A es un anillo conmutativo con unidad se da una definición de n elementos $t_1,\ldots,t_n$ algebraicamente independientes sobre A análoga a la recién vista. $S_n$ actúa sobre $A[t_1,\ldots,t_n]$ y un polinomio $g \in A[t_1,\ldots,t_n]$ se dice simétrico si $\sigma(g) = g$ para todo $\sigma \in S_n$. Los polinomios simétricos forman un subanillo de $A[t_1,\ldots,t_n]$ que contiene a las constantes y a los polinomios simétricos elementales $s_1,\ldots,s_n$. El resultado fundamental sobre polinomios simétricos es que todo polinomio simétrico g se puede escribir de una única manera como

$$g = f(s_1,\ldots,s_n) \quad \text{donde} \quad f \in A[X_1,\ldots,X_n].$$

O lo que es equivalente, el subanillo de los polinomios simétricos está generado sobre A por los polinomios simétricos elementales $s_1,\ldots,s_n$ que son algebraicamente independientes sobre A.

6) Si G es un grupo finito entonces existe un cuerpo y una extensión Galois del mismo con grupo de Galois isomorfo a G.

En efecto, si n es el orden de G, por el teorema de Cayley G es isomorfo a un subgrupo G' de $S_n$. Sea K un cuerpo cualquiera, $F = K(s_1,\ldots,s_n)$, $E = K(t_1,\ldots,t_n)$ como en el ejemplo anterior. Vimos que $S_n = G(E/F)$. Como $G' \subset S_n$, por el teorema fundamental de Galois E es una extensión Galois del cuerpo fijo F' de G' y $G(E/F') = G' \simeq G$.

OBSERVACION. Si K es un cuerpo y G es un grupo finito ¿existe una extensión Galois de K cuyo grupo de Galois es isomorfo a G?. Este es un problema abierto,

ni siquiera resuelto para el cuerpo Q de los racionales.

Más adelante veremos cómo se puede construir un polinomio irreducible de Q[X] de grado primo p cuyo grupo de Galois es $S_p$.

Se demuestra que para todo n se puede construir una extensión de Galois de Q con grupo $S_n$.

En 1954 I.P.Šafarewič probó que la respuesta al problema planteado en el caso racional es afirmativa para todo grupo finito resoluble, y recientemente se han obtenido otros resultados parciales.

7) El cuerpo C de los números complejos es algebraicamente cerrado. (Teorema fundamental del álgebra).

Para probarlo se usan las tres siguientes propiedades del cuerpo R de los números reales: es un cuerpo ordenado, todo elemento positivo tiene una raíz cuadrada y todo polinomio de grado impar de R[X] tiene una raíz en R.
En primer lugar veamos que R no puede tener ninguna extensión de grado impar $> 1$. Supongamos que $R \subset E$ y $[E:R] = n > 1$, n impar. Como R es de característica 0, toda extensión algebraica es separable y por el teorema del elemento primitivo es $E = R(u)$. Entonces si f es el polinomio minimal de u sobre R, f es de grado impar, luego tiene una raíz en R y es reducible. Esta contradicción prueba que toda extensión finita E de R es de grado par.

Veamos ahora que el grado de E es una potencia de 2. Se puede suponer que E es Galois sobre R pues toda extensión finita de R está contenida en una finita y Galois sobre R. Sea G el grupo de Galois de E sobre R. Como 2 divide al orden de G, sea P un 2-subgrupo de Sylow de G y F su cuerpo fijo.

$[F:R]$ = índice de P en G, que es un número impar. Entonces debe ser $F = R$, lo que implica $P=G$. Luego el grado de E sobre R es una potencia de 2.

Consideremos el cuerpo de los complejos $C = R(i)$, donde $i^2 = -1$. Para probar que C es algebraicamente cerrado es suficiente demostrar que toda extensión finita de C coincide con C, pues entonces el cuerpo de raíces de cualquier polinomio $f(X) \in C[X]$ es C. Sea $R(i) \subset E$ una extensión finita. Como E es una extensión finita de R su grado sobre R(i) es una potencia de 2. Podemos suponer que E es

Galois sobre R. Entonces E es Galois sobre R(i). Sea G = G(E/R) y H = G(E/R(i)). Si E ≠ R(i) es H≠1 y el orden de H es una potencia de 2. Luego tiene un subgrupo H' de índice 2, y el cuerpo fijo F de H' es una extensión Galois de R(i) de grado 2. De la fórmula que da las raíces de un polinomio de 2° grado resulta que F= R(i)(α) con $\alpha^2 \in R(i)$.

Pero cualquiera sea a+bi ∈ R(i) se puede escribir

$$a + bi = \left( \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + i \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}} \right)^2$$

donde la raíz cuadrada de $a^2+b^2$ es la positiva, y los signos de las otras dos raíces cuadradas se eligen de modo que su producto sea $\frac{b}{2}$. Estas raíces cuadradas existen en R pues las cantidades subradicales son números no negativos. Luego α ∈ R(i) y F = R(i), lo que contradice que F es de grado 2 sobre R(i). Esta contradicción prueba que E = R(i), lo que termina la demostración.

## EJERCICIOS

1) Decir cuál es el grupo de Galois sobre K de los siguientes polinomios cúbicos:

   $X^3-2X+2$ , $X^3-3X+1$ , $X^3+X-2$ , $X^3+3X^2+X+1$

   siendo: a) K = Q ; b) $K = Z_5$.

2) En un cuerpo de característica ≠ 2, si $f(X) = X^2+bX+c \in K[X]$ y $\alpha_1, \alpha_2$ son las raíces de f, verificar que el discriminante $\Delta = \delta^2 = (\alpha_1-\alpha_2)^2$ de f es $\Delta = b^2-4c$, usando las relaciones que dan los coeficientes de f en función de las raíces.

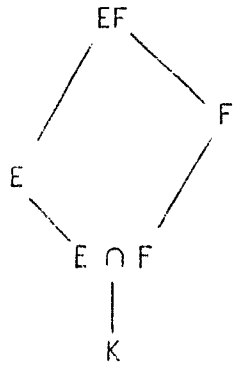
   Enunciar un criterio para determinar el grupo de Galois de una ecuación cuadrática.

3) Sobre un cuerpo K de característica ≠ 2, sea f(X) un polinomio cúbico cuyo discriminante es un cuadrado en K. Probar que f es irreducible o se factoriza completamente sobre K. ¿Por qué no vale este resultado en general si car K = 2?.

4) Probar que cualquiera sea el cuerpo de base K, el polinomio $X^3-3X+1$ es irreducible o se factoriza completamente sobre K.

A continuación veremos algunas propiedades de las extensiones galoisianas.

TEOREMA 6.5. Sea $K \subset E$ una extensión finita y Galois de K, F una extensión arbitraria de K, y E y F contenidos en un mismo cuerpo. Entonces EF es una extensión finita y Galois de F y la aplicación $\sigma \mapsto \sigma/E$ define un isomorfismo $G(EF/F) \simeq G(E/E\cap F)$. Si $E \cap F = K$ entonces $G(EF/F) \simeq G(E/K)$.

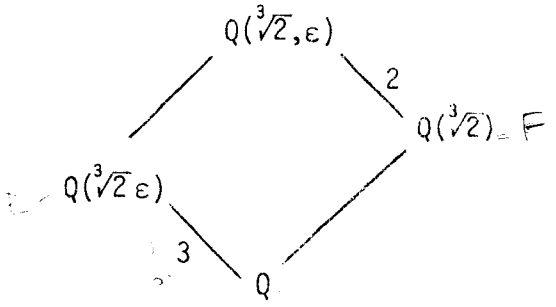



Demostración. EF es finita, normal y separable sobre F por propiedades ya vistas.
Sea $\varphi$: $G(EF/F) \to G(E/E\cap F)$ tal que $\sigma \mapsto \sigma/E$. Es claro que $\sigma/E \in G(E/E\cap F)$. $\varphi$ es un homomorfismo, como se ve sin dificultad y es monomorfismo pues si $\sigma$: $EF \to EF$ es un F-homomorfismo tal que $\sigma/E = id$ entonces $\sigma = id$, ya que los elementos de EF son de la forma $\sum e_i f_i \,/\, \sum e'_j f'_j$. Luego $\varphi$ es un isomorfismo de G(EF/F) sobre Im $\varphi$. Sea $H' = \text{Im}\,\varphi$; $H' \subset G(E/E\cap F)$ implica $E^{G(E/E\cap F)} = E \cap F \subset E^{H'}$. Pero si $x \in E$ es dejado fijo por todos los $\sigma \in H'$, como $\sigma = \overline{\sigma}/E$, con $\overline{\sigma} \in G(EF/F)$, significa que x pertenece al cuerpo fijo de G(EF/F), o sea, $x \in F$, luego $x \in E \cap F$. Entonces $E^{H'} = E \cap F$ y en consecuencia $H' = G(E/E\cap F)$.

COROLARIO. Si E es una extensión finita y Galois de K y F es una extensión arbitraria de K, entonces [EF:F] divide a [E:K].

Demostración. Como [EF:F] = orden G(EF/F) = orden $G(E/E\cap F)$ que es subgrupo de G(E/K), [EF:F]/[E:K].

OBSERVACION. La conclusión del corolario no es en general válida si E no es Galois sobre K. Por ejemplo




$\varepsilon$ = raíz primitiva de tercer orden de 1.

TEOREMA 6.6. Si $E_1$ y $E_2$ son dos extensiones finitas y Galois de un cuerpo K con grupos de Galois $G_1$ y $G_2$ respectivamente, contenidas en un mismo cuerpo, entonces $E_1E_2$ es una extensión finita y Galois de K y la aplicación $G(E_1E_2/K) \to G_1 \times G_2$ tal que $\sigma \mapsto (\sigma/E_1, \sigma/E_2)$ es un monomorfismo. Si $E_1 \cap E_2 = K$ entonces es un isomorfismo.

Demostración. $E_1.E_2$ es finita y Galois sobre K por propiedades ya vistas. La aplicación $\varphi$: $G(E_1E_2/K) \to G_1 \times G_2$ tal que $\varphi(\sigma) = (\sigma/E_1, \sigma/E_2)$ está bien definida y es un homomorfismo. Es monomorfismo pues si $\sigma$ es un K-automorfismo de $E_1E_2$ tal que $\sigma/E_i = id_{E_i}$ $i = 1,2$, por la forma de los elementos de $E_1E_2$ es $\sigma = id$. Si $E_1 \cap E_2 = K$ entonces $\varphi$ es epimorfismo. En efecto, por el teorema anterior cada $\sigma_1 \in G_1$ es la restricción a $E_1$ de un $\sigma \in G(E_1E_2/E_2) \subset G(E_1E_2/K)$, luego $\sigma$ restringido a $E_1$ da $\sigma_1$ y restringido a $E_2$ la identidad. Entonces $G_1 \times (id_{E_2})$ está contenido en Im $\varphi$. Análogamente, $(id_{E_1}) \times G_2$ está contenido en Im $\varphi$. Luego su producto, que es $G_1 \times G_2$, lo que termina la demostración.

COROLARIO 1. Sean $E_1,\ldots,E_n$ extensiones finitas y Galois de K contenidas en un mismo cuerpo y $G_1,\ldots,G_n$ sus grupos de Galois. Supongamos que $E_{i+1} \cap (E_1 \ldots E_i) = K$ para $i = 1,\ldots,n-1$. Entonces $E_1 \ldots E_n$ es Galois y finita sobre K y su grupo de Galois es isomorfo a $G_1 \times \ldots \times G_n$.

COROLARIO 2. Sea E una extensión finita y Galois de K con grupo de Galois G y

supongamos que se puede escribir $G = G_1 \times \ldots \times G_n$. Sea $E_i$ el cuerpo fijo de $G_1 \times \ldots \times (\overset{i}{1}) \times \ldots \times G_n$, $i = 1,\ldots,n$. Entonces $E_i$ es finita y Galois sobre K, $G_i \simeq G(E_i/K)$ y $E_{i+1} \cap (E_1 \ldots E_i) = K$. Además $E = E_1 \ldots E_n$.

Demostración. $E_i$ es finita y Galois sobre K, pues es el cuerpo fijo de un subgrupo normal de G, y $G(E_i/K) \simeq G_i$. $x \in E_{i+1} \cap (E_1 \ldots E_i)$ implica que x queda fijo por todo $\sigma \in G$, luego $x \in K$. Entonces por el corolario anterior el grupo de Galois de $E_1 \ldots E_n$ sobre K es isomorfo a $G_1 \times \ldots \times G_n = G$, lo que implica que $G(E/E_1 \ldots E_n) = id$ y por lo tanto $E = E_1 \ldots E_n$.

Ejemplos

1) Hallar el grupo de Galois de $f(X) = (X^2-3)(X^3-3X+1)$ sobre Q.
Consideremos los factores irreducibles de f: $f_1 = X^2-3$ , $f_2 = X^3-3X+1$, sus respectivos cuerpos de raíces $E_1$ y $E_2$ sobre Q, y sus grupos de Galois $G_1$ y $G_2$.
$E_1 = Q(\sqrt{3})$ y $G_1 \simeq Z_2$.
El discriminante de $f_2$ es $\Delta = 81$, luego $G_2 \simeq Z_3$ y $[E_2:Q] = 3$.
Es claro que el cuerpo de raíces E de f sobre Q es $E = E_1.E_2$. $E_1$ y $E_2$ son dos extensiones de Galois de Q de grados 2 y 3, por lo tanto $E_1 \cap E_2 = Q$. Entonces por el teorema 6.6 el grupo de Galois G de f es isomorfo a $G_1 \times G_2$, es decir $G \simeq Z_2 \times Z_3 \simeq Z_6$. Luego E es una extensión cíclica de Q de grado 6.

2) Sea $f(X) = (X^2-2)(X^2+3)(X^3-5) \in Q[X]$. Hallar su grupo de Galois sobre Q, sobre $Q(\sqrt{3})$ y sobre $Q(\sqrt{-3})$.
f está dado como producto de polinomios irreducibles sobre Q, $f_1 = X^2-2$, $f_2 = X^2+3$ , $f_3 = X^3-5$. Sean $E_1$, $E_2$, $E_3$ sus cuerpos de raíces sobre Q.

$E_1 = Q(\sqrt{2})$ , $E_2 = Q(\sqrt{-3})$ , $E_3 = Q(\sqrt[3]{5},\sqrt{-3})$,
que son extensiones de Q de grado 2, 2 y 6 respectivamente con grupos de Galois

$Z_2$, $Z_2$ y $S_3$.

El cuerpo de raíces de f es $E = Q(\sqrt{2},\sqrt{-3},\sqrt[3]{5})$ y se ve que $E = E_1.E_3$.

$E_1 \cap E_3$ es de grado 1 ó 2. Si fuera de grado 2 sería $E_1 \cap E_3 = E_1$, es decir, $E_1 \subset E_3$. Pero $E_3$ contiene un único subcuerpo de grado 2 sobre Q, que es $Q(\sqrt{-3})$, pues el grupo de Galois $S_3$ de $E_3$ tiene un único subgrupo de orden 3: $A_3$. Entonces debería ser $E_1 = Q(\sqrt{-3})$, absurdo. Luego $E_1 \cap E_3 = Q$ y por el teorema 6.6 el grupo de Galois G de f sobre Q es $G \simeq Z_2 \times S_3$. En este caso E es una extensión Galois de Q de grado 12 no abeliana.

El grupo de Galois de f sobre $Q(\sqrt{3})$ es el mismo que sobre Q.

Si el cuerpo de base es $Q(\sqrt{-3})$ los factores irreducibles de f son $X^2-2$ y $X^3-5$, y el cuerpo de raíces de f es $E = Q(\sqrt{-3})(\sqrt{2},\sqrt[3]{5})$. Razonando análogamente se ve que $G \simeq Z_2 \times Z_3 \simeq Z_6$.

# CAPITULO VII

## LA ECUACION $X^n - 1 = 0$. CUERPOS CICLOTOMICOS

Sea K un cuerpo y supongamos fijada una clausura algebraica $\overline{K}$.

Las raíces de $X^n-1$ forman un grupo multiplicativo $H_n \subset \overline{K}$. Como todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico, $H_n$ es cíclico. ¿Cuántos elementos tiene?.

Si car K = 0, $X^n-1$ tiene n raíces distintas pues $(X^n-1)' = nX^{n-1}$ y m.c.d.$(X^n-1, nX^{n-1}) = 1$. Luego el orden de $H_n$ es n.

Si car $K = p \neq 0$ y $p \nmid n$ se ve como antes que $X^n-1$ tiene todas sus raíces distintas y $H_n$ es de orden n. Pero si $p/n$ entonces $n = p^t.m$ con $(p,m) = 1$ y $t > 0$, $X^n-1 = (X^m-1)^{p^t}$, $X^m-1$ tiene raíces distintas $\varepsilon_1, \ldots, \varepsilon_m$, que son las de $X^n-1$ con multiplicidad $p^t$. Luego las raíces n-ésimas de la unidad coinciden con las raíces m-ésimas y $H_n = H_m$ es de orden m. Por lo tanto si car $K = p \neq 0$ basta considerar el caso $X^n-1$ con $p \nmid n$.

Ejemplo. Dado un cuerpo K, $1 \in K$ es una raíz n-ésima de la unidad para todo $n \geq 1$. Si car $K = p \neq 0$ y $n = p^t$, 1 es la única raíz n-ésima de la unidad.

En todo lo que sigue supondremos car K = 0 o car $K = p \neq 0$ y $p \nmid n$.

Entonces las raíces de la ecuación $X^n-1 = 0$ forman un grupo multiplicativo $H_n$ que es cíclico de orden n.

Un generador de $H_n$ se llama una raíz primitiva de orden n. Hay $\phi(n)$ de estas raíces. ($\phi(n)$ = indicador de Euler). $H_n \subset H_m$ si y sólo si $n/m$.

Si $(m,n) = 1$ es $H_{mn} = H_m.H_n$, todo generador de $H_{mn}$ es producto de un generador de $H_m$ por uno de $H_n$ y recíprocamente. Luego si $(m,n) = 1$ es $\phi(mn) = \phi(m).\phi(n)$.

El cuerpo de raíces E del polinomio $X^n-1$ sobre K se llama el cuerpo ciclotómico de orden n sobre K. Si $\varepsilon \in \overline{K}$ es una raíz primitiva de orden n, $E = K(\varepsilon)$.

$K(\varepsilon)$ es una extensión finita y Galois de K. ¿Cuál es su grupo de Galois?.

TEOREMA 7.1. Dado un cuerpo K, el cuerpo ciclotómico E de orden n sobre K es una extensión abeliana de K y su grupo de Galois es isomorfo a un subgrupo del grupo multiplicativo $U(Z_n)$ de los elementos inversibles de $Z_n$. Luego [E:K] divide a $\phi(n)$.

Demostración. Sea $\varepsilon$ una raíz n-ésima primitiva, $E = K(\varepsilon)$. Todo K-automorfismo $\sigma$ de E aplica biyectivamente el grupo multiplicativo $H_n$ de las raíces n-ésimas sobre sí mismo, aplicando generadores en generadores. Luego $\sigma(\varepsilon) = \varepsilon^i$ con $(i,n) = 1$. La aplicación $\sigma \mapsto \overline{i} \pmod n$ define un monomorfismo de $G(E/K)$ en el grupo multiplicativo $U(Z_n)$ de los elementos inversibles de $Z_n$, como se verifica sin dificultad.

OBSERVACION. $U(Z_n)$ no es en general un grupo cíclico. Se demuestra que $U(Z_n)$ es cíclico si y sólo si $n = 2$, $n = 4$, $n = p^k$ o $n = 2p^k$ donde p es un primo $\neq 2$ y k un entero $\geq 1$.

Dado un cuerpo K no se conoce en general el subgrupo de $U(Z_n)$ que es isomorfo al grupo de Galois del cuerpo ciclotómico de orden n sobre K ni cuántos elementos tiene este grupo de Galois, es decir cuál es el grado del cuerpo ciclotómico. Pero si K = Q se verifica que $G(Q(\varepsilon_n)|Q) \simeq U(Z_n)$ como sigue del siguiente

TEOREMA 7.2. Si $\varepsilon_n$ es una raíz n-ésima primitiva entonces

$$[Q(\varepsilon_n):Q] = \phi(n).$$

Demostración. Sea $f(X) \in Q[X]$ el polinomio minimal de $\varepsilon = \varepsilon_n$ sobre Q. Entonces $X^n-1 = f(X).h(X)$. Como f y h son mónicos, por el lema de Gauss resulta que f y h tienen coeficientes enteros. Vamos a ver que $\varepsilon^p$ es raíz de f para todo primo p que no divide a n. Como $\varepsilon^p$ también es una raíz n-ésima primitiva, de aquí seguirá que todas las raíces primitivas son raíces de f pues cualquier potencia

$\varepsilon^i$, con $(n,i) = 1$, se puede obtener elevando $\varepsilon$ sucesivamente a potencias con exponentè primo p, $p \nmid n$. Luego $gr\ f \geq \phi(n) \geq [Q(\varepsilon):Q] = gr\ f$, de donde sigue $[Q(\varepsilon):Q] = \phi(n)$.

Supongamos por el absurdo que $\varepsilon^p$ no es raíz de f, p primo, $p \nmid n$. Entonces $\varepsilon^p$ es raíz de $h(X)$, luego $\varepsilon$ es raíz de $h(X^p)$, lo que implica $f(X)/h(X^p)$. Entonces $h(X^p) = f(X).g(X)$. Como h y f son mónicos con coeficientes enteros, g también es mónico y tiene coeficientes enteros.

El epimorfismo canónico de anillos $Z \to Z_p$, $a \mapsto \bar{a}$, induce un epimorfismo $Z[X] \to Z_p[X]$ y se tiene

$$\bar{h}(X^p) = \bar{f}(X).\bar{g}(X)$$

Como $\bar{h}(X^p) = \bar{h}(X)^p$ , $\bar{f} / \bar{h}^p$ y $\bar{f}$ y $\bar{h}$ tienen una raíz común. Entonces el polinomio $X^n-\bar{1} = \bar{f}(X).\bar{h}(X)$ tiene una raíz múltiple, imposible pues $X^n-\bar{1}$ es separable ya que $p \nmid n$.

COROLARIO 1. $G(Q(\varepsilon_n)/Q) \simeq U(Z_n)$.

COROLARIO 2. Si $\varepsilon_p$ es una raíz primitiva de la unidad de orden primo p entonces $Q(\varepsilon_p)$ es una extensión cíclica de Q de grado p-1 y el polinomio minimal de $\varepsilon_p$ sobre Q es $X^{p-1} + \ldots + X + 1$.

Demostración. Por el teorema $[Q(\varepsilon_p):Q] = \phi(p) = p-1$.
Como $X^p-1 = (X-1)(X^{p-1} + \ldots + X + 1)$ , $\varepsilon_p$ es raíz del segundo factor. Luego éste es su polinomio minimal.

COROLARIO 3. Si $(m,n) = 1$ y $\varepsilon_m$, $\varepsilon_n$ son raíces primitivas de orden m y n respectivamente entonces

$$Q(\varepsilon_m) \cap Q(\varepsilon_n) = Q \qquad y \qquad Q(\varepsilon_{mn}) = Q(\varepsilon_m).Q(\varepsilon_n).$$

Demostración. Si $(m,n) = 1$, $H_{mn} = H_m.H_n$. Entonces $Q(\varepsilon_{mn}) = Q(\varepsilon_m).Q(\varepsilon_n)$.
Veamos que $Q(\varepsilon_m) \cap Q(\varepsilon_n) = Q$.

$[Q(\varepsilon_{mn}):Q] = \phi(mn) = \phi(m).\phi(n)$

pues $(m,n) = 1$.

Como $[Q(\varepsilon_n):Q] = \phi(n)$ sigue que

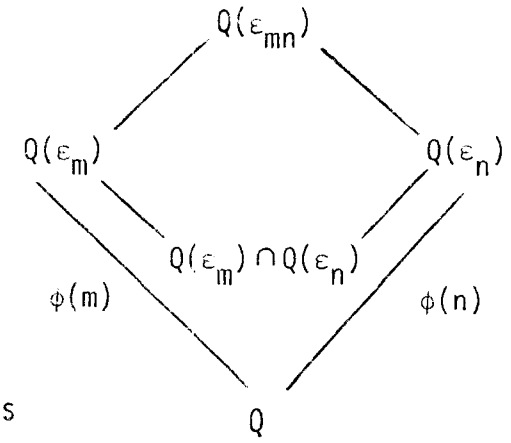
$[Q(\varepsilon_{mn}):Q(\varepsilon_n)] = \phi(m)$.

Por otro lado sabemos que

$G(Q(\varepsilon_{mn})/Q(\varepsilon_n)) \simeq G(Q(\varepsilon_m)/Q(\varepsilon_m) \cap Q(\varepsilon_n))$

luego $[Q(\varepsilon_m):Q(\varepsilon_m) \cap Q(\varepsilon_n)] = \phi(m)$ y entonces

$Q(\varepsilon_m) \cap Q(\varepsilon_n) = Q$.




Volvamos al caso general, K un cuerpo arbitrario, y si car $K = p \neq 0$ suponemos $p \nmid n$. El polinomio

$$f_n(X) = \prod_{i=1}^{\phi(n)} (X-\varepsilon_i)$$

donde $\varepsilon_1,\ldots,\varepsilon_{\phi(n)}$ son las raíces primitivas de la unidad de orden n, se llama el polinomio ciclotómico de orden n sobre K.

De lo visto resulta que si $K = Q$, $f_n$ es irreducible sobre Q pues es el polinomio minimal de cualquier raíz primitiva de orden n. Pero para K arbitrario en general no es así.

El conjunto de las raíces n-ésimas de la unidad se obtiene como reunión de las raíces primitivas de orden d, cuando d recorre el conjunto de los divisores positivos de n. En efecto, si $\varepsilon$ es una raíz n-ésima su orden multiplicativo d (es decir, el menor exponente natural d tal que $\varepsilon^d = 1$) divide a n y $\varepsilon$ es raíz primitiva de orden d. Recíprocamente, toda raíz primitiva de orden d con d/n es una raíz n-ésima de la unidad. Luego

$$X^n - 1 = \prod_{\substack{f_d \text{ pol. ciclotómico de orden } d \\ d/n}} f_d \qquad (1)$$

De aquí resulta la importante fórmula

$$n = \sum_{d/n} \phi(d)$$

(1) proporciona un método recursivo para calcular los polinomios ciclotómicos sobre un cuerpo arbitrario K:

$$f_n(X) = \frac{X^n - 1}{\prod_{\substack{d/n \\ d<n}} f_d(X)}$$

$$f_1(X) = X - 1 \quad , \quad f_2(X) = \frac{X^2 - 1}{f_1(X)} = X + 1 \quad , \quad f_3(X) = \frac{X^3 - 1}{f_1(X)} = X^2 + X + 1 \ ,$$

$$f_4 = \frac{X^4 - 1}{f_1(X)f_2(X)} = \frac{X^4 - 1}{(X - 1)(X + 1)} = X^2 + 1 \ ,$$

$$f_5 = \frac{X^5 - 1}{f_1(X)} = X^4 + X^3 + X^2 + X + 1 \quad , \quad \text{etc.}$$

Se ve que los polinomios ciclotómicos se obtienen recursivamente por división y que los polinomios que se dividen tienen coeficientes en el cuerpo primo de K, que se puede identificar con Q o $Z_p$ según la característica de K. Pensando cómo es el algoritmo de la división, cómo se hace para dividir un polinomio por otro mónico, resulta, razonando por recurrencia, que todos los polinomios ciclotómicos tienen coeficientes enteros:

$f_n(X) \in Z[X]$ si car K = 0 , $f_n(X) \in Z_p[X]$ si car K = p $\neq$ 0.

La construcción de $f_n(X)$ es así universal y válida para cualquier cuerpo K y sólo depende del cuerpo primo de K.

Vimos que <u>todos los polinomios ciclotómicos son irreducibles sobre Q</u>.

En general no es así si car K $\neq$ 0. Por ejemplo, $f_4(X) = X^2+1$ no es irreducible

sobre $Z_5$: $X^2+1 = (X+2)(X+3)$.

Uno estaría tentado de pensar que los coeficientes de cualquier polinomio ciclotómico son 0,1,-1. Así ocurre si $n < 105$. (El coeficiente de $X^7$ en $f_{105}(X)$ es -2. De paso esto muestra que sobre $Z_2$ $f_{105}(X)$ no coincide con el que corresponde a Q). En 1931 Schur demostró que existen polinomios ciclotómicos con coeficientes arbitrariamente grandes en valor absoluto.

Ejercicios

1) ¿Cuál es el polinomio ciclotómico de orden 5 sobre $Z_2$?. ¿Es $f_5(X)$ irreducible sobre $Z_2$?. ¿Y para orden 7?. ¿Y para orden 6?. ¿Y para orden 4?.

2) Dado un entero positivo n, cuál es el cuerpo ciclotómico de orden n sobre $Z_p$?.

Dado un cuerpo K, una extensión F de K se dice una extensión ciclotómica de K si F está contenida en un cuerpo ciclotómico de orden n sobre K, para algún n. Por el teorema 7.1 todo cuerpo ciclotómico sobre K es una extensión abeliana de K, luego toda extensión ciclotómica de K es abeliana. (pero no cíclica en general si car K = 0).

Queda propuesto como ejercicio probar que: Toda extensión ciclotómica de un cuerpo K de característica $p \neq 0$ es cíclica.

En particular, toda extensión ciclotómica de Q es abeliana. Y recíprocamente, toda extensión abeliana finita de Q es ciclotómica. La demostración, hecha por Kronecker (1823-1891) usa técnicas que no veremos.

Pero sí probaremos que

TEOREMA 7.3. Toda extensión cuadrática de Q es ciclotómica.

Antes de demostrarlo definiremos el símbolo de Legendre.
Si $F_q$ es un cuerpo finito con q elementos, $q = p^n$ con p primo impar, el grupo

multiplicativo $F_q^*$ es un grupo cíclico de orden q-1. $F_q^{*2}$ es un subgrupo de $F_q^*$ de índice 2. Luego la mitad de los elementos de $F_q^*$ son cuadrados y la otra no.

Para todo entero no nulo n se define el llamado símbolo de Legendre

$$\left(\frac{n}{p}\right) = \begin{cases} 1 \text{ si } n \text{ es un cuadrado módulo } p \\ -1 \text{ si no lo es.} \end{cases}$$

Demostración del teorema. Sea $Q \subset E$ una extensión cuadrática. Sabemos que E se puede escribir $E = Q(\delta)$ con $\delta^2 \in Z$, $\delta \notin Z$.

Sea $\delta^2 = \pm p_1 \cdot p_2 \ldots p_t$ la descomposición en enteros primos positivos, que se pueden suponer todos distintos.

Entonces para probar el teorema es suficiente demostrar que $\sqrt{p}$ está contenido en algún cuerpo ciclotómico sobre Q, para todo primo positivo p, pues $\sqrt{-1}$ lo está.

Si p = 2 es verdadero porque $(1+i)^2 = 2i$, de modo que $\sqrt{2} \in Q(\varepsilon_8)$.

Si p es impar, sea $\varepsilon$ una raíz primitiva de la unidad de orden p y consideremos

$$S = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \varepsilon^n$$

Se trata de probar que $S^2 = \left(\frac{-1}{p}\right)p$ (1)

pues $S^2 = \pm p$ implica $\sqrt{p} \in \begin{cases} Q(S) \subset Q(\varepsilon_p) \\ \text{o} \\ Q(S,i) \subset Q(\varepsilon_{4p}) \end{cases}$

Veamos entonces (1).

$$S^2 = \sum_{n,m} \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \varepsilon_p^{n+m} = \sum_{n,m} \left(\frac{n.m}{p}\right) \varepsilon_p^{n+m} \quad , \quad 1 \leq m,n \leq p-1.$$

Para m fijo, m,2m,...,(p-1)m dan todas las clases no nulas módulo p. Luego se puede reemplazar n por nm:

$$S^2 = \sum_{m=1}^{p-1} \sum_{n=1}^{p-1} \left(\frac{nm^2}{p}\right) \varepsilon^{(n+1)m} = \sum_{m=1}^{p-1} \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \varepsilon^{(n+1)m} =$$

$$= \sum_{m=1}^{p-1} \left(\frac{-1}{p}\right) \varepsilon^{pm} + \sum_{n=1}^{p-2} \left(\frac{n}{p}\right) \sum_{m=1}^{p-1} \varepsilon^{(n+1)m}$$

Pero $\mu = \varepsilon^{n+1}$ es una raíz primitiva de orden p para $n = 1,\ldots,p-2$, y $1 + \mu + \mu^2 + \ldots + \mu^{p-1} = 0$. Luego

$$S^2 = (p-1)\left(\frac{-1}{p}\right) - \sum_{n=1}^{p-2} \left(\frac{n}{p}\right) = p\left(\frac{-1}{p}\right) - \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = p\left(\frac{-1}{p}\right)$$

pues $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0$ ya que en $Z_p^*$ la mitad de los elementos son cuadrados y la otra mitad no.

EJERCICIOS

1- a) Si $(m,n) = 1$ , $\phi(m.n) = \phi(m).\phi(n)$.

b) Si $n > 2$, $\phi(n)$ es un número par.

c) $\phi.(p^e) = p^{e-1}.(p-1)$ , p primo.

Deducir a qué es igual $\phi(n)$ , $\forall\ n \in N$.

d) Dado un entero n, el conjunto de los enteros x tales que $\phi(x) = \phi(n)$ es finito?. (entero = entero positivo).
¿Es $\phi: N \to 2N \cup \{1\}$ epiyectiva?.

2- a) Si $\varepsilon_6$ es una raíz primitiva de la unidad de orden 6 hallar $[Q(\varepsilon_6):Q]$ y el grupo de Galois de $Q(\varepsilon_6)$ sobre Q.
¿Es $Q(\varepsilon_6)$ una extensión cíclica de Q?.

b) Idem para $\varepsilon_9$ y $\varepsilon_{12}$.

3- a) Si n es impar $Q(\varepsilon_n) = Q(\varepsilon_{2n})$.

b) Si $\varepsilon_m$ y $\varepsilon_n$ son raíces primitivas de la unidad de orden m y n respectivamente y h = m.c.m.(m,n), demostrar que existen enteros u,v tales que $e^{2\pi i/h} = \varepsilon_m^u.\varepsilon_n^v$. Concluir que $Q(\varepsilon_m,\varepsilon_n) = Q(\varepsilon_h)$.

c) Demostrar que las únicas raíces de la unidad que hay en $Q(\varepsilon_n)$ son las n-ésimas si n es par, y las 2n-ésimas si n es impar. (Sugerencia: Sea $\varepsilon_k$ una raíz primitiva de la unidad de orden k contenida en $Q(\varepsilon_n)$. Entonces $Q(\varepsilon_k,\varepsilon_n) = Q(\varepsilon_n) = Q(\varepsilon_h)$, h = m.c.m.(n,k).
Deducir la propiedad enunciada demostrando en general que n/m y $\phi(m) \leqslant \leqslant \phi(n)$ implica m=n si n es par, y m=n o m=2n si n es impar).

d) Los cuerpos ciclotómicos de orden n, n par, son todos distintos y no isomorfos dos a dos.

e) Si m es par, $Q(\varepsilon_n) \subset Q(\varepsilon_m)$ si y sólo si n/m.

4- a) Escribir la fórmula que da por recurrencia sobre n el polinomio ciclotómico de orden n. Hallarlo para n=6 y n=10, sobre Q. (Usar las cuentas hechas en teoría).

b) ¿Es cierto que el polinomio ciclotómico $f_n(X)$ es el mismo cualquiera que sea el cuerpo de base K que se considere, siempre que la característica de K no divida a n, si car K ≠ 0?.

c) ¿Cuáles son los cuerpos ciclotómicos de grado 2 sobre Q?. Escribir sus elementos en términos de raíces cuadradas de números racionales. Decir si hay algún cuerpo ciclotómico $Q(\varepsilon_n)$ de grado 3 sobre Q.

d) Decir que raíces de la unidad están en los siguientes cuerpos:

$Q(i)$ , $Q(\sqrt{2})$ , $Q(\sqrt{-2})$ , $Q(\sqrt{-3})$ , $Q(\sqrt{-5})$ , $Q(\sqrt[3]{2})$.

e) En toda extensión finita de los racionales sólo hay un número finito de raíces de la unidad.

5- a) Todo cuerpo ciclotómico sobre un cuerpo cualquiera K es una extensión abeliana de K.

b) Todo cuerpo ciclotómico sobre un cuerpo finito es una extensión cíclica

del mismo.

c) Todo cuerpo ciclotómico sobre un cuerpo de característica $p \neq 0$ es una extensión cíclica del mismo.

6- Hallar el grado del cuerpo ciclotómico de orden 8 sobre $Z_{11}$ y el polinomio ciclotómico correspondiente y decir si es irreducible sobre $Z_{11}$.

# CAPITULO VIII

## EXTENSIONES CICLICAS

En lo que sigue vamos a estudiar extensiones de Galois finitas cuyo grupo de Galois es cíclico.

Comenzaremos por definir la norma y la traza.

Si $K \subset E$ es una extensión finita, sea $[E:K]_i = p^e$, $[E:K]_s = r$. Entonces $[E:K] = p^e.r$.

DEFINICION. Sea $K \subset E$ una extensión finita de K, $\bar{K}$ una clausura algebraica que contiene a E, $\sigma_1,\ldots,\sigma_r$ los distintos K-nomomorfismos $E \to \bar{K}$. Si $\alpha \in E$ se llama:

1) Norma de $\alpha$ al elemento $N_K^E(\alpha) = \left(\prod_{i=1}^{r}\sigma_i(\alpha)\right)^{[E:K]_i} = \prod_{i=1}^{r}\sigma_i(\alpha^{p^e})$.

2) Traza de $\alpha$ al elemento $Tr_K^E(\alpha) = [E:K]_i \cdot \sum_{i=1}^{r}\sigma_i(\alpha)$.

Observar que:

Si E no es una extensión separable de K, $[E:K]_i = p^e > 1$, p = car K, y la traza de cualquier elemento de E es cero.

Si E es separable, entonces $[E:K]_i = 1$ y

$$N_K^E(\alpha) = \prod_{i=1}^{r}\sigma_i(\alpha) \qquad , \qquad Tr_K^E(\alpha) = \sum_{i=1}^{r}\sigma_i(\alpha)$$

siendo $r = [E:K]$.

La traza es el análogo aditivo de la norma.

Ejemplo. Consideremos la extensión $R \subset C$. $\bar{R} = C$ y los R-nomomorfismos $C \to C$ son

dos, la identidad y el que aplica cada número complejo en su conjugado. Entonces

$$N_R^C(a+bi) = (a+bi)(a-bi) = a^2+b^2$$

$$Tr_R^C(a+bi) = (a+bi) + (a-bi) = 2a$$

TEOREMA 8.1. Sea $K \subset E$ una extensión finita. Entonces

a) $N_K^E(\alpha)$ y $Tr_K^E(\alpha)$ son elementos de K, para todo $\alpha \in E$.

b) La norma $N_K^E$ es un homomorfismo multiplicativo de $E^*$ en $K^*$, y la traza $Tr_K^E$ es un homomorfismo aditivo de E en K.

c) Si $K \subset E \subset F$ ambas aplicaciones son transitivas, es decir

$$N_K^F = N_K^E \circ N_E^F \qquad y \qquad Tr_K^F = Tr_K^E \circ Tr_E^F .$$

d) Si $\alpha \in E$ y $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ es el polinomio minimal de $\alpha$ sobre K entonces $N_K^{K(\alpha)}(\alpha) = (-1)^n a_0$ y $Tr_K^{K(\alpha)}(\alpha) = -a_{n-1}$.

Demostración.

a) Si $\alpha \in E$, $\alpha^{p^e}$ es separable sobre K, luego el grado del polinomio minimal f de $\alpha^{p^e}$ sobre K divide a $[E:K]_s = r$. Entonces $\sigma_1(\alpha^{p^e}),\ldots,\sigma_r(\alpha^{p^e})$ son todos los conjugados de $\alpha^{p^e}$, cada uno repetido el mismo número de veces r/gr f (pues cada K-homomorfismo $\tau: K(\alpha^{p^e}) \to \overline{K}$ se extiende a r/gr f K-homomorfismos de $E \to \overline{K}$). Luego el producto $\prod_{i=1}^{r}\sigma_i(\alpha^{p^e})$ da una potencia del término independiente de f, a menos del signo, y por lo tanto $N_K^E(\alpha) = \prod_{i=1}^{r}\sigma_i(\alpha^{p^e}) \in K$.

Para la traza se aplica un razonamiento similar, teniendo en cuenta que es suficiente demostrarlo para E separable sobre K.

b) Se demuestra sin dificultad.

c) Sea $K \subset E \subset F$, $\{\sigma_i\}$ el conjunto de los K-homomorfismos $E \to \overline{K}$ y $\{\tau_j\}$ el de los E-homomorfismos $F \to \overline{K}$. Sabemos que $\{\overline{\sigma}_i\tau_j\}_{i,j}$ son los K-homomorfismos

$F \to \overline{K}$, siendo $\overline{\sigma}_i : \overline{K} \to \overline{K}$ una extensión de $\sigma_i$, para cada i. Es fácil ver que la norma y la traza son transitivas, teniendo en cuenta la multiplicidad del grado de inseparabilidad.

d) Sea $\alpha \in E$, $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$ su polinomio minimal, $[K(\alpha):K]_s = t$, $\sigma_1,\ldots,\sigma_t$ los K-homomorfismos $K(\alpha) \to \overline{K}$. En $\overline{K}[X]$ el polinomio f se escribe

$$f(X) = ((X-\alpha_1) \ldots (X-\alpha_t))^{[K(\alpha):K]_i}$$

siendo $\alpha_1 = \alpha,\ldots,\alpha_t$ las raíces distintas de f. El producto de las n raíces de f da $(-1)^n a_0$ y su suma $-a_{n-1}$. Por otro lado $\sigma_1(\alpha),\ldots,\sigma_t(\alpha)$ son todas las distintas raíces de f. Entonces es claro que

$$N_K^{K(\alpha)}(\alpha) = \Big(\prod_{j=1}^{t} \sigma_j(\alpha)\Big)^{[K(\alpha):K]_i} = (-1)^n a_0$$

y análogamente para la traza.

OBSERVACION. $Tr_K^E : E \to K$ es una aplicación K-lineal, pues además de ser aditiva se verifica $Tr_K^E(c\alpha) = c\, Tr_K^E(\alpha)$ cualquiera sea $c \in K$, $\alpha \in E$.

Vamos a demostrar que n automorfismos distintos cualesquiera de un cuerpo son linealmente independientes. Esta es una propiedad que vale en un contexto más general y lo veremos así.

Un conjunto con una ley de composición interna asociativa y que tiene elemento neutro se llama un monoide.

DEFINICION. Si G es un monoide y K un cuerpo, un homomorfismo $\sigma : G \to K^*$ se llama un caracter de G en K.

El caracter $\sigma(x) = 1$ para todo $x \in G$ se llama trivial.

n caracteres $\sigma_1,\ldots,\sigma_n$ se dicen linealmente independientes sobre K si

$c_1\sigma_1(x) + c_2\sigma_2(x) + \ldots + c_n\sigma_n(x) = 0$ para todo $x \in G$, con $c_i \in K$, implica $c_1 = \ldots = c_n = 0$.

TEOREMA 8.2. (independencia lineal de caracteres).
n caracteres distintos $\sigma_1,\ldots,\sigma_n$ de G en K son linealmente independientes sobre K.

Demostración. Si no son linealmente independientes entonces existen relaciones

$$c_1\sigma_1 + \ldots + c_n\sigma_n = 0$$

con no todos los $c_i$ nulos. Elijamos una con el menor número de coeficientes no nulos. Podemos suponer

$$c_1\sigma_1 + \ldots + c_m\sigma_m = 0 \qquad (1)$$

reordenando convenientemente los $\sigma_i$. Se ve que $m > 1$. Como $\sigma_1 \neq \sigma_2$ existe un $u \in G$ tal que $\sigma_1(u) \neq \sigma_2(u)$. Para todo $x \in G$ se tiene

$$c_1\sigma_1(ux) + \ldots + c_m\sigma_m(ux) = 0$$

Luego

$$c_1\sigma_1(u)\sigma_1(x) + \ldots + c_m\sigma_m(u)\sigma_m(x) = 0 \qquad (2)$$

Por otro lado de (1)

$$c_1\sigma_1(x) + \ldots + c_m\sigma_m(x) = 0$$

Multiplicando por $\sigma_1(u)$ y restando de (2) resulta

$$c_2(\sigma_2(u)-\sigma_1(u))\sigma_2(x)+\ldots+c_m(\sigma_m(u)-\sigma_1(u))\sigma_m(x) = 0$$

para todo $x \in G$. Como $c_2(\sigma_2(u)-\sigma_1(u)) \neq 0$ no todos los coeficientes son nulos, lo que contradice la minimalidad de (1).

COROLARIO. n automorfismos distintos de un cuerpo E son linealmente independientes sobre E.

El siguiente resultado establece una propiedad fundamental que tienen la norma

y la traza en las extensiones cíclicas.

TEOREMA 8.3. Sea E una extensión cíclica de K de grado n, G su grupo de Galois, $\sigma$ un generador de G. Entonces si $\beta \in E$ se verifica:

a) $N_K^E(\beta) = 1$ si y sólo si $\beta = \alpha/\sigma(\alpha)$, para algún $\alpha \in E$. (Teorema 90 de Hilbert).

b) $Tr_K^E(\beta) = 0$ si y sólo si $\beta = \alpha - \sigma(\alpha)$, para algún $\alpha \in E$. (Forma aditiva).

Demostración. Si $\sigma$ es un generador de G, $\sigma^0 = id, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ son los distintos K-automorfismos de E. Como E es separable

$$N_K^E(\beta) = \beta.\sigma(\beta). \ \ldots \ .\sigma^{n-1}(\beta) \quad , \quad Tr_K^E(\beta) = \beta + \sigma(\beta) + \ldots + \sigma^{n-1}(\beta).$$

a) Si $\beta = \frac{\alpha}{\sigma(\alpha)}$ es $N(\beta) = \frac{N(\alpha)}{N(\sigma(\alpha))} = 1$ pues $N(\alpha) = N(\sigma(\alpha))$.

Recíprocamente, sea $N(\beta) = 1$, lo que implica $\beta \neq 0$. Consideremos la aplicación de E en E dada por

$$id + \beta\sigma + (\beta.\sigma(\beta))\sigma^2 + \ldots + (\beta.\sigma(\beta). \ \ldots \ .\sigma^{n-2}(\beta))\sigma^{n-1}$$

No es nula por el teorema de la independencia lineal de caracteres. Luego existe $\theta \in E$ tal que el elemento

$$\alpha = \theta + \beta\sigma(\theta) + (\beta.\sigma(\beta))\sigma^2(\theta) + \ldots + (\beta.\sigma(\beta). \ \ldots \ .\sigma^{n-2}(\beta))\sigma^{n-1}(\theta)$$

es no nulo. Y es fácil ver que $\beta\sigma(\alpha) = \alpha$ usando la hipótesis $N(\beta) = 1$.

Como $\sigma(\alpha) \neq 0$, es $\beta = \alpha/\sigma(\alpha)$.

b) Si $\beta = \alpha - \sigma(\alpha)$ entonces $Tr(\beta) = Tr(\alpha) - Tr(\sigma(\alpha)) = 0$.

Sea ahora $Tr(\beta) = 0$. Que Tr no es una aplicación idénticamente nula resulta de la independencia lineal de caracteres, luego existe un $\theta \in E$ tal que $Tr(\theta) \neq 0$.

Sea $$\alpha = \frac{1}{Tr(\theta)} (\beta\sigma(\theta)+(\beta+\sigma(\beta))\sigma^2(\theta)+\ldots+(\beta+\sigma(\beta)+\ldots+\sigma^{n-2}(\beta))\sigma^{n-1}(\theta))$$

Haciendo cuentas se ve que $\alpha - \sigma(\alpha) = \beta$.

En el caso car $K = p \neq 0$ el siguiente teorema reduce el estudio de una extensión cíclica de K de grado n al de otras de menor grado.

TEOREMA 8.4. Sea car $K = p \neq 0$, E una extensión cíclica de K de grado n, $n = p^t.m$ con $(p,m) = 1$. Entonces existe una cadena de subcuerpos intermedios

$$K = F_0 \subset F_1 \subset \ldots \subset F_t \subset E$$

tal que E es una extensión cíclica de $F_t$ de grado m y $F_i$ es una extensión cíclica de $F_{i-1}$ de grado p, para $1 \leqslant i \leqslant t$.

Demostración. Si G es el grupo de Galois de E sobre K, G es un grupo cíclico de orden n. Como en un grupo cíclico existe un subgrupo (único) de orden d para cada divisor d del orden del grupo, G contiene la siguiente cadena de subgrupos:

$$\{1\} \subset G_t \subset G_{t-1} \subset \ldots \subset G_1 \subset G_0 = G$$

donde $G_i$ es cíclico de orden $p^{t-i}.m$ , $0 \leqslant i \leqslant t$.

Por el teorema fundamental de Galois los cuerpos fijos respectivos forman una cadena

$$K = F_0 \subset F_1 \subset \ldots \subset F_{t-1} \subset F_t \subset E$$

donde E es Galois sobre $F_i$ y $F_i$ es Galois sobre K, $0 \leqslant i \leqslant t$. Luego cada $F_i$ es una extensión finita y Galois de $F_{i-1}$ con grupo de Galois isomorfo a $G_{i-1}/G_i$ , $1 \leqslant i \leqslant t$, que es un grupo cíclico de orden p.

Entonces $[F_i:F_{i-1}] = p$, $1 \leqslant i \leqslant t$, $[E:F_t] = m$, y cada cuerpo en la cadena es una extensión cíclica del anterior, el primero de grado m, primo con p, y los restantes de grado p.

De acuerdo con este resultado vamos a estudiar las extensiones cíclicas de grado n de un cuerpo K en los siguientes casos:

1) car $K = p \neq 0$ , $n = p$.

2) car $K = p \neq 0$ , $(p,n) = 1$.

3) car $K = 0$.

El caso 1) lo estudiaremos en forma completa; 2) y 3) sólo bajo la hipótesis

de que el cuerpo K contiene las raíces n-ésimas de la unidad. El estudio del caso general es más complicado.

TEOREMA 8.5. Si K es un cuerpo de característica $p \neq 0$, E es una extensión cíclica de K de grado p si y sólo si E es el cuerpo de raíces de un polinomio irreducible de la forma $X^p-X-a \in K[X]$. Y $E = K(\alpha)$ siendo $\alpha$ una raíz cualquiera de ese polinomio.

Demostración. Sea $K \subset E$ una extensión cíclica de K de grado p, $\sigma$ un generador de su grupo de Galois G. Se tiene $Tr_K^E(-1) = p(-1) = 0$, y por la forma aditiva del teorema 90 de Hilbert existe $\alpha \in E$ tal que $-1 = \alpha-\sigma(\alpha)$. Luego $\sigma(\alpha) = \alpha+1$, de donde resulta $\sigma^i(\alpha) = \alpha+i$ , $i = 0,1,\ldots,p-1$. Entonces los p elementos $\alpha+i$ son conjugados de $\alpha$, todos distintos. Luego $[K(\alpha):K] \geqslant p$; como $K \subset K(\alpha) \subset E$ y E es de grado p sobre K, es $E = K(\alpha)$.

Además

$\sigma(\alpha^p-\alpha) = \sigma(\alpha^p)-\sigma(\alpha) = (\sigma(\alpha))^p-\sigma(\alpha) = (\alpha+1)^p-\alpha-1 = \alpha^p-\alpha$ lo que implica que $\alpha^p-\alpha$ queda invariante por $\sigma$, y por lo tanto por $\sigma^i$, $i = 0,1,\ldots,p-1$. Luego $\alpha^p-\alpha \in K$.

Llamando $\alpha^p-\alpha = a$, $\alpha$ es raíz del polinomio $X^p-X-a \in K[X]$, que debe ser su polinomio minimal, y por lo tanto irreducible, puesto que $[K(\alpha):K] = p$. Entonces $E = K(\alpha)$ es el cuerpo de raíces del polinomio irreducible $X^p-X-a$.

Recíprocamente, sea E el cuerpo de raíces sobre K de un polinomio irreducible $f(X) = X^p-X-a \in K[X]$. Si $\alpha \in E$ es una raíz cualquiera se ve que $\alpha+i$, $i = 0,1,\ldots,p-1$, son las p raíces de f, pues $i \in Z_p$ cuerpo primo de K y $i^p = i$. Luego $E = K(\alpha)$, y como todas las raíces son distintas, E es una extensión normal y separable de K, es decir Galois. Además $[E:K] = p$, luego su grupo de Galois es de orden primo y en consecuencia cíclico.

Ejercicio. Si K es un cuerpo de característica $p \neq 0$, probar que un polinomio $X^p-X-a \in K[X]$ es irreducible o tiene todas sus raíces en K.

El estudio del cuerpo de raíces y el grupo de Galois de las ecuaciones del tipo $X^p-X-a = 0$ sobre un cuerpo de característica p queda dado por el teorema anterior.

Ahora vamos a considerar las extensiones cíclicas en los casos 2) y 3) antes mencionados, lo que lleva a estudiar las ecuaciones de la forma $X^n-a = 0$, que se suelen llamar ecuaciones puras. El caso particular $X^n-1 = 0$ ya lo hemos visto.

En general, sea K un cuerpo y $X^n-a \in K[X]$. Supongamos fijada una clausura algebraica $\overline{K}$. Si $\alpha \in \overline{K}$ es una raíz de $X^n-a$ y $\varepsilon_1,\ldots,\varepsilon_m \in \overline{K}$ son las raíces distintas de $X^n-1$ (si car K = 0, m=n, y si car K = p $\neq$ 0, $n = p^t.m$ con $p\nmid m$), entonces $\alpha\varepsilon_1,\ldots,\alpha\varepsilon_m \in \overline{K}$ son las distintas raíces de $X^n-a$. En efecto, se ve que estos elementos son raíces de ese polinomio y que son todos distintos. Además si $\beta \in \overline{K}$ es una raíz de $X^n-a$, $(\frac{\beta}{\alpha})^n = 1$, $\frac{\beta}{\alpha} = \varepsilon_i$ para algún índice i y entonces $\beta = \alpha\varepsilon_i$. Luego si car K = p $\neq$ 0 es suficiente considerar el caso $X^n-a = 0$ con (p,n) = 1.

En lo que sigue vamos a trabajar bajo la hipótesis de que el cuerpo de base K contiene las raíces n-ésimas de la unidad.

TEOREMA 8.6. Sea K un cuerpo, n un entero positivo, n relativamente primo con la característica de K si car K $\neq$ 0. Supongamos que en K hay una raíz primitiva n-ésima de la unidad.

a) Si E es una extensión cíclica de K de grado n entonces E = K($\alpha$) donde $\alpha$ es raíz de un polinomio $X^n-a \in K[X]$.

b) Recíprocamente, si $\alpha$ es raíz de un polinomio $X^n-a \in K[X]$ entonces K($\alpha$) es una extensión cíclica de K, de grado d un divisor de n y $\alpha^d \in K$.

Demostración. Sea $\varepsilon \in K$ una raíz primitiva de orden n de la unidad.

a) Sea $K \subset E$ una extensión cíclica de grado n, G su grupo de Galois, $\sigma$ un generador de G. $N(\varepsilon^{-1}) = (\varepsilon^{-1})^n = 1$, luego por el teorema 90 de Hilbert existe un

$\alpha \in E$, $\alpha \neq 0$, tal que $\varepsilon^{-1} = \frac{\alpha}{\sigma(\alpha)}$, $\sigma(\alpha) = \varepsilon\alpha$ lo que implica $\sigma^i(\alpha) = \varepsilon^i\alpha$, $i = 0,1,\ldots,n-1$. Luego los $\varepsilon^i\alpha$ son conjugados de $\alpha$ y son todos distintos; entonces $[K(\alpha):K] \geqslant n$, y como $K \subset K(\alpha) \subset E$, es $E = K(\alpha)$.

Además $\sigma(\alpha^n) = (\sigma(\alpha))^n = \varepsilon^n\alpha^n = \alpha^n$, luego $\alpha^n$ queda fijo por $\sigma$ y en consecuencia por todos los automorfismos de G, de donde resulta que $\alpha^n \in K$. Llamando $\alpha^n = a$, $\alpha$ es raíz de $X^n-a$, $a \in K$.

b) Sea $\alpha$ una raíz de una ecuación $X^n-a = 0$, $a \in K$. Ya vimos que tiene todas sus raíces distintas y que ellas son $\alpha,\alpha\varepsilon,\ldots,\alpha\varepsilon^{n-1}$. Entonces $E = K(\alpha)$ es el cuerpo de raíces de $X^n-a$, es normal y separable y por lo tanto Galois sobre K. Sea G su grupo de Galois. Si $\sigma \in G$ $\sigma(\alpha) = \varepsilon^{i_\sigma}\alpha$. Entonces $\sigma \to \varepsilon^{i_\sigma}$ define un monomorfismo $G \to H_n$ = grupo multiplicativo de las raíces n-ésimas de 1, que es cíclico de orden n. Luego G es un grupo cíclico, y su orden d divide a n. Entonces $E = K(\alpha)$ es una extensión cíclica de K de grado d, d/n. Si $\sigma$ es un generador de G, $\sigma(\alpha^d) = (\sigma(\alpha))^d = (\varepsilon^{i_\sigma}\alpha)^d = \alpha^d$ pues $(\varepsilon^{i_\sigma})^d = 1$. (ya que $\sigma^d = 1$ y $\varepsilon^{i_\sigma}$ es la imagen de $\sigma$ por el homomorfismo $G \to H_n$). De aquí resulta que $\alpha^d$ queda fijo por todos los automorfismos de G y por lo tanto $\alpha^d \in K$. Entonces $\alpha$ es raíz de la ecuación $X^d-b$, $b = \alpha^d \in K$.

EJERCICIO. a) Sea K un cuerpo, E una extensión cíclica de K de grado n, n arbitrario. Suponiendo que K contiene las raíces de la unidad de un cierto orden, decir cómo se obtiene E a partir de K mediante extensiones cíclicas sucesivas.

b) Concluir que si car $K = 0$ o car $K = p \neq 0$ y $(p,n) = 1$, entonces $E = K(\alpha_1,\ldots,\alpha_s)$ donde $\alpha_i = \sqrt[p_{j_i}]{a_i}$ con $a_i \in K(\alpha_1,\ldots,\alpha_{i-1})$ y $p_{j_i}$ primo que divide a n.

c) Dar el resultado correspondiente para el caso que falta: car $K = p \neq 0$ y $(p,n) \neq 1$.

OBSERVACION. La caracterización del cuerpo de raíces de una ecuación $X^n-a \in K[X]$ cuando el cuerpo de base K no contiene a las raíces n-ésimas de la unidad es más complicada. (Ver, por ejemplo, Serge Lang, Algebra).

EJERCICIOS.

1- a) Por Eisenstein el polinomio $X^7-6$ es irreducible sobre Q. Hallar el grado de su cuerpo de raíces sobre Q.

b) Idem para $X^4-12$.

2- a) Sea a un entero, $a \neq 0,1,-1$, a no divisible por cuadrados. Para cada primo p, sea $E_p$ el cuerpo de raíces sobre Q del polinomio $X^p-a$. Demostrar que $[E_p:Q] = p(p-1)$.

b) Para cada entero $m > 0$ no divisibles por cuadrados, sea $E_m = \prod_{p/m} E_p$ el cuerpo generado por los $E_p$, para todos los primos p que dividen a m. Probar que si m es impar $[E_m:Q] = \prod_{p/m} [E_p:Q]$ , y si m es par, $m = 2n$, entonces $[E_m:Q] = [E_n:Q]$ o $[E_m:Q] = 2[E_n:Q]$ según que $\sqrt{a}$ pertenezca o no a $Q(\varepsilon_m)$.

c) Sean $p_1$ y $p_2$ dos primos, $p_2$ impar. Si a es un entero como en a) y $\varepsilon_{p_1}$ es una raíz primitiva de la unidad de orden $p_1$, demostrar que $[Q(\varepsilon_{p_1}, \sqrt[p_2]{a}):Q] = (p_1-1).p_2$.

Si $p_2 = 2$ entonces el grado de esta extensión es $p_1-1$ o $2(p_1-1)$ según $\sqrt{a}$ pertenezca o no al cuerpo $Q(\varepsilon_{p_1})$.

3- Hallar el grupo de Galois de los siguientes polinomios:

a) $X^4-7$ sobre Q.

b) $X^3-15$ sobre Q.

c) $X^4-7$ sobre $Q(\sqrt{7})$, $Q(\sqrt{-7})$, $Q(i)$.

d) $X^3-15$ sobre $Q(\sqrt[3]{5})$, $Q(\sqrt{-3})$.

e) $X^3-13X+13$ sobre Q.

f) $X^3+2X-1$ sobre $Q(\sqrt{-59})$.

g) $X^4+2$ sobre Q, Q(i).

h) $X^4-a$ sobre Q, siendo a un entero $\neq 0,1,-1$ y no divisible por cuadrados.

i) $X^p-a$ sobre Q, p primo, a como en h).

j) $X^n-a$ sobre Q, n producto de primos impares distintos, a como en h).

k) $X^4-6X^2-3$ sobre Q y $Q(\sqrt{3})$.

l) $(X^2-2)(X^2+5)$ sobre Q.

m) $(X^2-3)(X^2+7)(X^2-11)(X^2+31)$ sobre Q.

n) Si $p_1,p_2,\ldots,p_n$ son primos distintos hallar el grupo de Galois de $f(X) = (X^2-p_1)(X^2-p_2)\ldots(X^2-p_n)$ sobre Q.

o) $(X^2-2)(X^2-5)(X^3-15)$ sobre $Q(\sqrt{-2})$.

p) $(X^2-2)(X^2-18)$ sobre Q.

4- Aplicar el teorema fundamental de Galois estableciendo explícitamente la correspondencia subcuerpo a subgrupo y decir qué extensiones intermedias son Galois sobre el cuerpo de base en a), b), e) y l).

5- Hallar un elemento primitivo de las siguientes extensiones:

a) El cuerpo de raíces de $X^4-7$ sobre Q y sobre $Q(\sqrt{7})$.

b) El cuerpo de raíces de $X^3-15$ sobre Q.

c) El cuerpo de raíces de $(X^2-2)(X^2+5)(X^2-7)$ sobre Q.

d) $Q(\sqrt{2},\sqrt{6})$ sobre Q.

e) $Q(\sqrt[3]{24},\sqrt[3]{1/2})$ sobre Q.

6- a) ¿Existe para cada $n \in N$ una extensión de grado n de Q?.

b) Si K es un cuerpo finito ¿existe para cada $n \in N$ una extensión de grado n

de K?.

c) ¿Cualquier cuerpo K admite una extensión de grado n, para todo $n \in N$?.

d) Si $K \subset E \subset F$, E Galois (abeliana, cíclica) sobre K y F Galois (abeliana, cíclica) sobre E implica F Galois (abeliana, cíclica) sobre K?.
F Galois (abeliana, cíclica) sobre K implica que F lo es sobre E y E sobre K?.

e) Indicar dos extensiones Galois de Q de grado 3.

f) Indicar dos extensiones Galois de Q de grado 4, una cíclica y la otra no.

g) ¿Cuántas extensiones intermedias hay entre Q y $Q(\varepsilon_7)$?.
Hallar un elemento primitivo para la de grado 3 sobre Q.

h) Indicar dos extensiones de Galois de grado 5 y una de grado 10 de Q.

i) Indicar dos extensiones Galois de Q de grado 6, una cíclica y una no abeliana. ¿Existe alguna abeliana no cíclica?.

j) Indicar una extensión de Galois de Q de grado 3.200.

# CAPITULO IX

# CRITERIO DE RESOLUBILIDAD POR RADICALES

## GRUPOS RESOLUBLES

La noción de grupo resoluble es una generalización de la de grupo abeliano y apareció en conexión con el problema de la resolubilidad de una ecuación algebraica por radicales. La aplicación clásica de la teoría de Galois es a ese problema y se obtiene como resultado el siguiente criterio: Una ecuación algebraica es resoluble por radicales si y sólo si su grupo de Galois es resoluble.

Un grupo resoluble es un grupo en el que existen cadenas finitas de subgrupos con cierta propiedad.

DEFINICION. Dado un grupo G, una cadena de subgrupos

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_r = \{1\} \qquad (1)$$

se dice una serie normal de G si $G_i$ es un subgrupo normal de $G_{i-1}$ para $1 \leqslant i \leqslant r$. Los grupos $G/G_1, G_1/G_2, \ldots, G_{r-1}/G_r$ se llaman los grupos factores de la serie dada y el número de inclusiones estrictas en (1) la longitud de la serie.

Todo grupo admite una serie normal: $\{1\}$ o $G \supset \{1\}$, según que G sea de orden igual o mayor que uno.

Una serie normal

$$G = H_0 \supset H_1 \supset \ldots \supset H_s = \{1\}$$

se dice un refinamiento de la serie (1) si puede obtenerse a partir de ella insertando un número finito de subgrupos. Un refinamiento se dice propio si su longitud es mayor que la de (1).

DEFINICION. Una serie normal de un grupo G se dice una serie de composición de G si cada $G_i$ es un subgrupo normal maximal de $G_{i-1}$ , $i = 1,\ldots,r$, o lo que es equivalente, si todos los grupos factores $G_{i-1}/G_i$ son simples.

Es decir, una serie normal es una serie de composición si y sólo si no admite ningún refinamiento propio.

DEFINICION. Un grupo G se dice resoluble si existe una serie normal de G con todos los grupos factores abelianos.

Una serie de este tipo se dice una serie de resolubilidad de G.

Ejemplos.

1) Es claro que todo grupo abeliano es resoluble.

2) Se demuestra que todo grupo nilpotente es resoluble.

3) El grupo dihedral $D_n$ es resoluble pues $D_n \supset (a) \supset \{1\}$ es una serie de resolubilidad, siendo a un elemento de orden n.

4) $S_2$, $S_3$ y $S_4$ son resolubles. En efecto, $S_2 \simeq Z_2$ ; $S_3 \supset A_3 \supset \{1\}$ es una serie de resolubilidad de $S_3$ ; $S_4 \supset A_4 \supset V \supset \{1\}$ es una serie de resolubilidad de $S_4$, donde V es el grupo de Klein.

5) Probaremos que $S_n$ no es un grupo resoluble si $n \geqslant 5$.

6) Es claro que un grupo simple no abeliano no es resoluble. Por ejemplo:
El grupo alternado $A_n$ es simple no abeliano si $n \geqslant 5$.

El grupo proyectivo especial $PL(n,R) \simeq SL(n,R)/Z(SL(n,R))$ es simple y no abeliano para $n > 1$.

TEOREMA 9.1.

(i) Todo subgrupo de un grupo resoluble es resoluble.

(ii) Toda imagen homomórfica de un grupo resoluble es resoluble.

(iii) Si $H \triangleleft G$ y H y G/H son resolubles entonces G es resoluble.

Demostración.

(i) Sea G resoluble, H un subgrupo de G, $G = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$ una serie de resolubilidad de G. Entonces
$H = G \cap H = G_0 \cap H \supset G_1 \cap H \supset \ldots \supset G_r \cap H = \{1\}$ es una serie normal tal que los grupos factores son abelianos.

En efecto, se ve sin dificultad que $G_i \cap H \lhd G_{i-1} \cap H$, $i = 1,\ldots,r$, y usando la propiedad: Si A y B son subgrupos de un grupo G, A subgrupo normal, entonces $B/A \cap B \simeq A.B/A$, se tiene
$G_{i-1} \cap H/G_i \cap H = G_{i-1} \cap H/G_i \cap G_{i-1} \cap H \simeq G_i.(G_{i-1} \cap H)/G_i$, que es isomorfo a un subgrupo de $G_{i-1}/G_i$, abeliano por hipótesis; luego $G_{i-1} \cap H/G_i \cap H$ es abeliano.

(ii) Sea $f: G \to G'$ un epimorfismo de grupos, G resoluble. Hay que probar que G' también lo es. Sea $G = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$ una serie de resolubilidad de G. Entonces

$$G' = f(G) = f(G_0) \supset f(G_1) \supset \ldots \supset f(G_r) = \{1\}$$

Veamos que esta es una serie de resolubilidad para G'.

Como $G_i \lhd G_{i-1}$ es $f(G_i) \lhd f(G_{i-1})$, $i = 1,\ldots,r$. Para ver que los grupos cocientes son abelianos consideremos la aplicación $\varphi: G_{i-1}/G_i \to f(G_{i-1})/f(G_i)$ tal que $\overline{g} \mapsto f(\overline{g})$, donde $\overline{g}$ = clase de g módulo $G_i$, $f(\overline{g})$ = clase de f(g) módulo $f(G_i)$.
$\varphi$ está bien definida y es un epimorfismo de grupos. Luego $G_{i-1}/G_i$ abeliano implica $f(G_{i-1})/f(G_i)$ abeliano.

(iii) Supongamos $H \lhd G$, H y G/H resolubles. Sea $G/H = G_0' \supset G_1' \supset \ldots \supset G_r' = \{1\}$ una serie de resolubilidad para G/H.

Si $\pi: G \to G/H$ es el epimorfismo canónico, sea $G_i = \pi^{-1}(G_i')$, $i = 0,1,\ldots,r$.

Entonces

(1) $G = G_0 \supset G_1 \supset \ldots \supset G_r = H$ , $G_i \lhd G_{i-1}$ y $G_{i-1}/G_i \simeq {}^{G_{i-1}/H}\big/_{G_i/H} \simeq$

$\simeq G_{i-1}'/G_i'$ abeliano.

Agregando a (1) una serie de resolubilidad para H se obtiene una para G.

COROLARIO. Si $0 \to G' \to G \to G'' \to 0$ es una sucesión exacta de grupos entonces G es resoluble si y sólo si G' y G'' lo son.

El siguiente teorema da una caracterización de los grupos resolubles finitos.

TEOREMA 9.2. Un grupo finito es resoluble si y sólo si tiene una serie de composición con todos los grupos factores cíclicos de orden primo.

Demostración. Sea G finito y resoluble, $G = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$ (1)
una serie de resolubilidad de G. Esta serie se puede refinar a una serie de composición con los grupos factores abelianos, y por lo tanto cíclicos de orden primo.

En efecto, si $G_{i-1}/G_i$ no es simple, sea H un subgrupo normal de $G_{i-1}$ tal que $G_{i-1} \supsetneq H \supsetneq G_i$. Entonces $G_i$ es un subgrupo normal de H, y $H/G_i$ y $G_{i-1}/H$ son abelianos pues $G_{i-1}/G_i$ lo es por hipótesis, $H/G_i$ es isomorfo a un subgrupo de $G_{i-1}/G_i$ y $G_{i-1}/H \simeq {}^{G_{i-1}/G_i}\big/_{H/G_i}$.

Luego intercalando H en la serie (1) se obtiene una serie de resolubilidad de G.

Reiterando este procedimiento se puede obtener una serie de composición de G con los grupos factores abelianos simples.

La otra implicación es trivial.

CRITERIO DE RESOLUBILIDAD POR RADICALES.

Vamos a ver el criterio de resolubilidad por radicales de una ecuación algebraica $f(X) = 0$, $f(X) \in K[X]$, K cuerpo arbitrario.

El problema fue estudiado originalmente para polinomios con coeficientes numéricos. A partir del hallazgo en el siglo XVI de las fórmulas que permiten calcular

las raíces de los polinomios de 3° y 4° grados, se trató de encontrar una para los de 5° grado, y en general para los de grado n, $n \geq 5$. A principios del siglo XIX los esfuerzos realizados por numerosos matemáticos culminaron con los trabajos de Paolo Ruffini y Niels Abel, quienes en forma independiente demostraron que no existe tal fórmula para los polinomios de 5° grado. Muy poco tiempo después Évariste Galois obtuvo un resultado más preciso: una condición necesaria y suficiente para que una ecuación algebraica dada sea resoluble por radicales, proporcionando como consecuencia una demostración de la irresolubilidad por radicales de la ecuación general de grado n, si $n \geq 5$. Galois demostró que una ecuación algebraica es resoluble por radicales si y sólo si su grupo de Galois es resoluble.
Este resultado vale para polinomios con coeficientes en un cuerpo K cualquiera, si se da una definición conveniente de lo que significa "ser resoluble por radicales". Supondremos que se trabaja en una clausura algebraica fija $\overline{K}$.

Si car K = 0 corresponde la siguiente: Una ecuación $f(X) = 0$, $f(X) \in K[X]$, se dice resoluble por radicales sobre K si sus raíces se pueden escribir (en $\overline{K}$) en términos de elementos de K y un número finito de radicales.
En el caso general hay que dar una un poco más amplia.

Por razones de simplicidad consideraremos primero polinomios con coeficientes en un cuerpo K de característica cero. Para polinomios separables el caso general no difiere esencialmente de éste.

En lo que sigue supondremos car K = 0.
Comenzaremos por formular la noción de resolubilidad por radicales en términos de extensiones del cuerpo K para precisar la dada más arriba. En primer término definiremos "extensión radical" de K.

DEFINICION 1. Una extensión F de K se dice una extensión radical de K si F posee una torre de subcuerpos

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m = F$$

tal que $K_i = K_{i-1}(\beta_i)$ y $\beta_i^{n_i} \in K_{i-1}$, es decir $\beta_i$ es raíz de un polinomio

$X^{n_i} - a_i \in K_{i-1}[X]$, para $i = 1,\ldots,m$.

O lo que es equivalente $F = K(\beta_1,\beta_2,\ldots,\beta_m)$ donde alguna potencia de $\beta_1$ está en K y alguna potencia de $\beta_i$ está en $K(\beta_1,\ldots,\beta_{i-1})$, para $i = 2,\ldots,m$.
(Toda extensión radical de K es una extensión finita de K).

Es decir, una extensión radical de K se obtiene por la adjunción sucesiva de un número finito de radicales de ciertos órdenes. Por ejemplo, si K = Q el número

$$\frac{3}{7}\sqrt[5]{12}\cdot\sqrt[3]{\frac{-1+\sqrt[6]{-4}}{2}} - 14.\sqrt{2-\sqrt[4]{3}}$$

pertenece a una extensión radical de Q: $Q(\alpha,\beta,\gamma,\delta,\varepsilon)$ siendo $\alpha^5 = 12$, $\beta^6 = -4$, $\gamma^3 = \frac{-1+\beta}{2}$, $\delta^4 = 3$, $\varepsilon^2 = 2-\delta$.

Si $F = K(\beta_1,\ldots,\beta_m)$ es una extensión radical de K es claro que todos los elementos de F se pueden escribir en términos de elementos de K y $\beta_1,\ldots,\beta_m$ mediante operaciones del cuerpo.

DEFINICION 2. Dado un polinomio $f(X) \in K[X]$, se dice que f(X) (o la ecuación algebraica $f(X) = 0$) es resoluble por radicales sobre K si existe una extensión radical F de K que contiene al cuerpo de raíces E de f sobre K.

$$K \subset E \subset F$$

Con esta definición se está pidiendo que los elementos de E, en particular las raíces de f, se escriban en función de elementos de K y un número finito de ciertos radicales mediante operaciones racionales (las del cuerpo $\overline{K}$).
(Pero notar que no todas las expresiones radicales de ese tipo pertenecen necesariamente a E, que en general no es una extensión radical de K).

La definición 2 implica entonces la de resolubilidad por radicales dada al principio. Y recíprocamente, pues si $f(X) \in K[X]$ es un polinomio cuyas raíces se pueden escribir en términos de elementos de K y radicales, lo mismo sucede

con todos los elementos de su cuerpo de raíces E. En particular con $\theta$, si $E = K(\theta)$. Sean $\beta_1,\ldots,\beta_t$ los radicales que figuran en la expresión de $\theta$ ordenados de modo que $\beta_1^{n_1} \in K$ , $\beta_2^{n_2} \in K(\beta_1),\ldots,$ $\beta_t^{n_t} \in K(\beta_1,\ldots,\beta_{t-1})$. Entonces la torre

$$K = K_0 \subset K(\beta_1) \subset K(\beta_1,\beta_2) \subset \ldots \subset K(\beta_1,\ldots,\beta_t) = F$$

es radical y $E \subset F$.

OBSERVACIONES.

1) Si $F = K(\beta_1,\ldots,\beta_m)$ es una extensión radical de K, siempre que convenga se puede suponer que los $\beta_i$ son radicales de orden primo $p_i$. En efecto, en general si $\beta^n \in K$, y $n = r.s$ tomando $\alpha = \beta^s$ se tiene $K \subset K(\alpha) \subset K(\alpha,\beta)$ , con $\alpha^r \in K$ , $\beta^s \in K(\alpha)$.

2) Una extensión radical de un cuerpo K no es necesariamente normal, ni los polinomios $X^{n_i} - a_i$ son irreducibles. Por ejemplo, $Q \subset Q(\varepsilon_3,\sqrt[7]{2})$ con $\varepsilon_3$ raíz cúbica primitiva de la unidad no es una extensión normal y $\varepsilon_3$ es raíz del polinomio $X^3-1$, que no es irreducible sobre Q.

3) Recíprocamente, una extensión normal de K no es necesariamente radical. Por ejemplo, una extensión normal de Q grado 3 no puede ser radical. En efecto, sea $Q \subset E$ una extensión normal, $[E:Q] = 3$. Si fuera radical sería $E = Q(\beta)$ con $\beta^n = a \in Q$, es decir $\beta$ es raíz de $X^n-a$. El polinomio minimal f de $\beta$ sobre Q divide a $X^n-a$, luego las raíces de f son tres de las raíces de $X^n-a$: $\beta$, $\beta\varepsilon^i$, $\beta\varepsilon^j$ donde $\varepsilon$ es una raíz primitiva n-ésima de 1, i,j enteros, $1 \leqslant i \neq j \leqslant n-1$. E normal implica $\beta,\beta\varepsilon^i,\beta\varepsilon^j \in E$, de donde $\varepsilon^i,\varepsilon^j \in E$; luego $Q(\varepsilon^i) \subset E$ y entonces $Q(\varepsilon^i) = Q$ o $Q(\varepsilon^i) = E$. Si $\varepsilon^i$ es primitiva de orden m, $[Q(\varepsilon^i):Q] = \phi(m)$.

$Q(\varepsilon^i) = E$ implica $\phi(m) = 3$, imposible pues $\phi(1) = \phi(2) = 1$ y $\phi(n)$ es par si $n > 2$. Luego $Q(\varepsilon^i) = Q$ y entonces $\varepsilon^i = 1$ ó $-1$. Razonando análogamente para $\varepsilon^j$ se tiene $\varepsilon^j = 1$ ó $-1$. Imposible, pues por las hipótesis hechas es $\varepsilon^i \neq 1$, $\varepsilon^j \neq 1$ y $\varepsilon^i \neq \varepsilon^j$.

Consideremos, por ejemplo, el polinomio $f(X) = X^3 - 7X + 7 \in Q[X]$. Su discriminante $\Delta = -4p^3 - 27q^2 = 49$ es un cuadrado en Q, luego el grupo de Galois del cuerpo de raíces E de f sobre Q es $A_3 \simeq Z_3$ y $[E:Q] = 3$. Entonces es normal de grado 3 sobre Q y por lo recién visto no es radical. Veamos una extensión radical que contiene a E.

Las raíces de un polinomio $X^3 + pX + q$ son $u+v$, $\varepsilon u+\varepsilon^2 v$ y $\varepsilon^2 u+\varepsilon v$ siendo $\varepsilon \neq 1$ una raíz cúbica de la unidad y

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad , \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

donde las raíces cúbicas u y v se eligen de modo que $uv = -\frac{p}{3}$.

Calculando u y v para nuestro ejemplo se ve que $F = Q(\sqrt{-3}, u, v)$ es una extensión radical de Q tal que $E \subset F$.

4) Toda extensión radical de un cuerpo K está contenida en una extensión radical normal de K. Más precisamente, si F es una extensión radical de K y N es la clausura normal de F en $\overline{K}$, $K \subset F \subset N \subset \overline{K}$, entonces N es una extensión radical de K.

En efecto, si $F = K(\beta_1, \ldots, \beta_m)$ y $\{\sigma_i\}_{1 \leq i \leq r}$ son los K-homomorfismos de F en $\overline{K}$, sabemos que $N = K(\{\sigma_i(\beta_j)\}_{i,j})$ y es claro que N es una extensión radical de K.

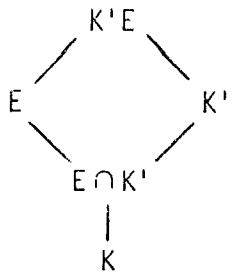
A continuación veremos una demostración del criterio de resolubilidad de Galois en característica cero que puede adaptarse sin dificultad para el caso general.

TEOREMA 9.3. Un polinomio $f(X) \in K[X]$ es resoluble por radicales si y sólo si su grupo de Galois es resoluble.

Demostración. Sea car K = 0.

($\Leftarrow$) Supongamos que el grupo de Galois de f(X) es resoluble, sea E su cuerpo de raíces sobre K, $G = G(E/K)$. Sea m el producto de todos los primos que dividen a $[E:K]$ y $K' = K(\varepsilon)$ donde $\varepsilon$ es una raíz m-ésima primitiva de la unidad.

Por el teorema 6.5, K'E es Galois sobre K' y $G(K'E/K') \simeq G(E/E \cap K') \subset G(E/K)$ que es un grupo resoluble, luego $G' = G(K'E/K')$ es resoluble. Sea




$G' = G'_0 \supset G'_1 \supset \ldots \supset G'_r = \{1\}$

una serie de composición de G'. Por la correspondencia fundamental de Galois existe una torre de subcuerpos

$K' = K_0 \subset K_1 \subset \ldots \subset K_r = K'E$

tal que $G'_i = G(K'E/K_i)$ , $i = 0,1,\ldots,r$.

En cada escalón $K_{i-1} \subset K_i \subset K'E$ , K'E es Galois sobre $K_{i-1}$ y como $G'_i$ es un subgrupo normal de $G'_{i-1}$ resulta que $K_i$ es Galois sobre $K_{i-1}$ y $G(K_i/K_{i-1}) \simeq$ $\simeq G'_{i-1}/G'_i$ que es un grupo cíclico de orden primo $p_i$. Luego $K_i$ es una extensión cíclica de $K_{i-1}$ de grado $p_i$. Como

$p_i$ / orden de $G'_{i-1}$ / orden de G' / orden de G , y $K' \subset K_{i-1}$ , $K_{i-1}$ contiene las raíces $p_i$-ésimas de la unidad de donde resulta que $K_i = K_{i-1}(\beta_i)$ con $\beta_i^{p_i} = a_i \in K_{i-1}$ , es decir $\beta_i$ es raíz del polinomio $X^{p_i} - a_i$, (teorema 8.6), $i = 1,\ldots,r$.

Luego K'E es una extensión radical de K' y por lo tanto de K. Como $K \subset E \subset K'E$, f es resoluble por radicales.

(⇒) Sea f(X) resoluble por radicales, E su cuerpo de raíces, F una extensión radical de K que contiene a E; sea N la clausura normal de F en $\overline{K}$. Es claro que N también es una extensión radical de K y Galois sobre K. Sea m el producto de los primos que dividen al grado [N:K] y sea $K' = K(\varepsilon)$ donde $\varepsilon$ es una raíz primitiva de la unidad de orden m.

Consideremos K'N, que es Galois sobre K (teorema 6.6). Como $K \subset E \subset K'N$ y E es Galois sobre K es $G(E/K) \simeq G(K'N/K) \,/\, G(K'N/E)$. Entonces para probar que G(E/K) es resoluble es suficiente ver que G(K'N/K) lo es.

Como N es radical sobre K, K'N es radical sobre K: Si

$K = K_0 \subset K_1 \subset \ldots \subset K_r = N$ es una torre radical entonces

$K = K'_{-1} \subset K'_0 = K' = K_0(\varepsilon) \subset K'_1 = K_1(\varepsilon) \subset \ldots \subset K'_r = K_r(\varepsilon) = K'N$

es una torre radical, $K'_0$ es una extensión abeliana de K, y $K'_i$ es una extensión abeliana de $K'_{i-1}$ , $i = 1,\ldots,r$.

Por la correspondencia fundamental de Galois existe una cadena de subgrupos

$$G(K'N/K) = G_{-1} \supset G_0 \supset \ldots \supset G_r = \{1\} \qquad (1)$$

tal que $G_i = G(K'N/K'_i)$ , $i = -1,0,1,\ldots,r$. Cada $G_i$ es un subgrupo normal de $G_{i-1}$ y $G_{i-1} / G_i \simeq G(K'_i/K'_{i-1})$ que es un grupo abeliano. Luego (1) es una serie de resolubilidad de $G(K'N/K)$, lo que termina la demostración.

Analizando la demostración de ($\Leftarrow$) recién hecha para tratar de generalizarla al caso car K = p ≠ 0, y suponiendo f separable para que su cuerpo de raíces E sea una extensión Galois de K, se ve que si p divide a [E:K], en la torre de subcuerpos de K'E van a aparecer extensiones $K_{i-1} \subset K_i$ donde $K_i$ es una extensión cíclica de grado p de $K_{i-1}$.

Entonces hay que modificar la definición de extensión radical dando cabida también a ese tipo de extensiones, que se obtienen adjuntando una raíz de un polinomio de la forma $X^p - X - a$. (Teorema 8.5).

Luego la definición de extensión radical para un cuerpo K cualquiera en el caso f separable es como sigue:

DEFINICION. Dado un cuerpo K, una extensión F de K se dice una extensión radical si posee una torre de subcuerpos

$$K = K_0 \subset K_1 \subset \ldots \subset K_m = F$$

tal que cada extensión $K_{i-1} \subset K_i$ es de uno de los siguientes tipos:

(a) Se obtiene adjuntando una raíz de un polinomio de la forma $X^n - a$ con $a \in K_{i-1}$ y n primo con la característica p de K si p ≠ 0.

(b) Se obtiene adjuntando una raíz de un polinomio de la forma $X^p - X - a$,

$a \in K_{i-1}$, $p = \text{car } K$.

Se ve que una extensión radical así definida es finita y separable sobre K. Es claro que si car K = 0 esta definición coincide con la anteriormente dada. La definición de polinomio resoluble por radicales es la misma.

TEOREMA 9.4. Un polinomio separable $f(X) \in K[X]$ es resoluble por radicales si y sólo si su grupo de Galois es resoluble.

Demostración. A cargo del lector, tomando m igual al producto de todos los primos $\neq p$ que dividen a $[E:K]$ (a $[N:K]$), si car $K = p \neq 0$.

Un teorema análogo se puede demostrar para f(X) no separable. En ese caso hay que considerar extensiones normales en lugar de extensiones de Galois y ampliar la definición de extensión radical para incorporar raíces de ecuaciones del tipo $X^p - a$, con $p = \text{car } K$. (Ver S.Lang, Algebra, 2nd. ed., pág.328).

## POLINOMIOS NO RESOLUBLES POR RADICALES.

De acuerdo con el criterio de Galois para exhibir un polinomio no resoluble por radicales es suficiente encontrar uno cuyo grupo de Galcis no sea resoluble.

Vamos a mostrar uno con coeficientes racionales y a indicar un método para construir polinomios de Q[X] no resolubles por radicales.

Después estudiaremos el polinomio general de grado n, probando que no es resoluble por radicales si $n \geqslant 5$.

En primer término

$S_n$ no es un grupo resoluble para $n \geqslant 5$.

Esto resulta inmediatamente de que si $n \geqslant 5$, el grupo alternado $A_n$ es simple y no abeliano, luego la única serie normal que admite es $A_n \supset \{1\}$, y $A_n$ no es resoluble. Entonces $S_n$ tampoco lo es, pues todo subgrupo de un resoluble es resoluble.

Otra demostración de este resultado sin hacer uso de la simplicidad de $A_n$ es la que da Emil Artin en su libro Teoría de Galois:

LEMA. Si $n \geq 5$, G y H son dos subgrupos de $S_n$ tales que G contiene a todos los triciclos, H es un subgrupo normal de G y G/H es abeliano, entonces H contiene a todos los triciclos.

Demostración. Sea $\varphi$: $G \to G/H$ el homomorfismo canónico, $a = (ijk)$, $b = (krs)$ dos elementos de G, i, j, k, r, s cinco números distintos. Como G/H es abeliano $\varphi(a^{-1}b^{-1}ab) = \varphi(a)^{-1}\varphi(b)^{-1}\varphi(a)\varphi(b) = 1$, luego $a^{-1}b^{-1}ab \in H$. Pero $a^{-1}b^{-1}ab = (kji)(srk)(ijk)(krs) = (kjs)$. Por lo tanto $(kjs) \in H$ cualesquiera sean $1 \leq j \neq s \neq k \leq n$.

TEOREMA 9.5. El grupo simétrico $S_n$ no es resoluble para $n \geq 5$.

Demostración. Supongamos que existe una serie normal de $S_n$ con todos los grupos factores abelianos: $S_n = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$.
Como $S_n$ contiene a todos los triciclos, por el lema anterior lo mismo sucede con todos los subgrupos $G_i$ y la sucesión no puede terminar en $\{1\}$.

COROLARIO. $A_n$ no es resoluble si $n \geq 5$.

Demostración. Si $A_n$ fuera resoluble, $n \geq 5$, como $A_n$ es un subgrupo normal de $S_n$ y $S_n/A_n \simeq Z_2$ es resoluble, entonces sería $S_n$ resoluble.

Vamos a dar anora un método para obtener polinomios de Q[X] no resolubles por radicales.

TEOREMA 9.6. Sea $f(X) \in Q[X]$ un polinomio irreducible de grado primo p. Si f(X) tiene exactamente dos raíces no reales en el cuerpo C de los complejos, entonces su grupo de Galois es $S_p$.

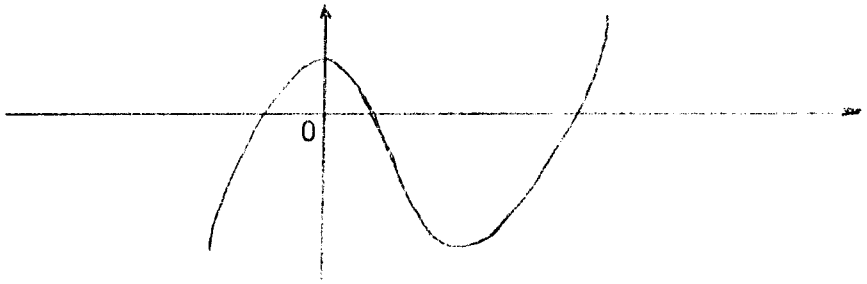
Para demostrarlo se hace uso del siguiente

LEMA. Si G es un subgrupo de $S_p$ , p primo, y G contiene una trasposición y una permutación de orden p entonces $G = S_p$.

Demostración. Recordemos que un sistema de generadores de $S_n$ es $\{(12), (123...n)\}$. Sea $G \subset S_p$ en las condiciones del enunciado. Podemos suponer que G contiene a (12). Teniendo en cuenta que toda permutación es producto de ciclos disjuntos y que su orden es el mínimo común múltiplo de los órdenes de esos ciclos, se ve que en $S_p$, un elemento de orden p es un p-ciclo. Una de sus potencias aplica 1 en 2, y podemos suponer que ella es el ciclo (123...p), modificando la numeración si es preciso. Entonces G contiene a (12) y (123...p), y es $G = S_p$.

Demostración del teorema 9.6. Como f es irreducible tiene p raíces distintas, las que por hipótesis son todas reales, excepto dos que son complejas conjugadas. Sea E el cuerpo de raíces de f y G su grupo de Galois, considerado como grupo de permutaciones de las raíces, es decir como subgrupo de $S_p$. La conjugación define un automorfismo de C, que restringido a E da un automorfismo de E que deja fijas las raíces reales y permuta las dos complejas conjugadas. Luego G contiene una trasposición.
Por otro lado, como f(X) es irreducible de grado p, p divide a [E:Q] = orden de G, y entonces G contiene un elemento de orden p. Por el lema $G = S_p$.

Por ejemplo el polinomio $X^5 - 20X^2 + 6$ llena las condiciones del teorema, luego su grupo de Galois es $S_5$, y por lo tanto no es resoluble por radicales.
En efecto, es irreducible por el criterio de Eisenstein. Estudiando el gráfico de la función real continua $f(x) = x^5 - 20x^2 + 6$ , analizando el signo de la derivada $f'(x) = 5x^4 - 40x$, se ve que f(x) es creciente en los intervalos $(-\infty,0)$ y $(2,+\infty)$, y decreciente en (0,2), y que su gráfico es del tipo



y por lo tanto tiene exactamente tres raíces reales.

Veremos una forma de construir polinomios de Q[X] que verifican las hipótesis del teorema 9.6. (método de R.Brauer):

Sea m un entero positivo par, $u_1 < u_2 < \ldots < u_{r-2}$ enteros pares, r impar $> 3$. Consideremos el polinomio $g(X) = (X^2 + m)(X - u_1)\ldots(X - u_{r-2})$ que tiene r-2 raíces reales y dos complejas, pero que en general no será irreducible. A partir de él vamos a obtener uno irreducible con el mismo tipo de raíces.

La función real g(x) tiene $\frac{r-3}{2}$ máximos relativos, y como $|g(a)| > 2$ para todo entero impar a, el valor de la función en los máximos relativos es $> 2$.

Sea $f(X) = g(X) - 2$; f(x) tiene $\frac{r-3}{2}$ máximos relativos en el intervalo $(u_1, u_{r-2})$, y por lo tanto hay r-3 raíces reales en ese intervalo. Como $f(u_{r-2}) = -2$ y $f(+\infty) = +\infty$, existe otra raíz real en el intervalo $(u_{r-2}, +\infty)$. Luego f(X) tiene r-2 raíces reales. Veamos que las otras dos son complejas.

Sean $\alpha_1, \ldots, \alpha_r$ las raíces de f(X). Los coeficientes de $X^{r-1}$ y $X^{r-2}$ son:

$$\sum_{i=1}^{r} \alpha_i = \sum_{i=1}^{r-2} u_i \qquad \text{y} \qquad \sum_{i<j} \alpha_i\alpha_j = \sum_{i<j} u_iu_j + m. \quad \text{Luego}$$

$$\sum_{i=1}^{r} \alpha_i^2 = \Big(\sum_{i=1}^{r} \alpha_i\Big)^2 - 2\sum_{i<j} \alpha_i\alpha_j = \Big(\sum_{i=1}^{r-2} u_i\Big)^2 - 2\Big(\sum_{i<j} u_iu_j + m\Big) = \sum_{i=1}^{r-2} u_i^2 - 2m.$$

Eligiendo m suficientemente grande es $\sum_{i=1}^{r} \alpha_i^2 < 0$, lo que implica que no todos los $\alpha_i$ son reales, luego hay dos raíces complejas conjugadas.

f(X) tiene todos sus coeficientes pares, excepto el principal, y el término independiente no es divisible por 4 pues el de g(X) lo es. Por el criterio de Eisenstein f(X) es irreducible y verifica entonces las condiciones del teorema.

De aquí resulta que para cada grado n, $n \geq 5$, existen polinomios en Q[X] no resolubles por radicales sobre Q: si p es un primo tal que $5 \leq p \leq n$ y $f(X) \in Q[X]$

es de grado p no resoluble por radicales entonces el polinomio $g(X) = f(X).(X - a)^{n-p}$, $a \in Q$, tiene el mismo grupo de Galois que $f(X)$.

UN CRITERIO DE IRREDUCIBILIDAD.

Vamos a ver un criterio de irreducibilidad para un polinomio $f(X) \in K[X]$ en términos de su grupo de Galois G. En lo que sigue se identifica a G con el correspondiente grupo de permutaciones de las raíces de $f(X)$.

DEFINICION. Un grupo de biyecciones G de un conjunto A se dice transitivo si para todo par de elementos $x,y \in A$ existe un $\sigma \in G$ tal que $\sigma(x) = y$.

TEOREMA 9.7. Sea $f(X) \in K[X]$ un polinomio sin raíces múltiples. Entonces $f(X)$ es irreducible sobre K si y sólo si su grupo de Galois es un grupo de permutaciones transitivo.

Demostración. Supongamos que $f(X) \in K[X]$ es irreducible y separable. Sea E un cuerpo de raíces de f, $\alpha_1,\alpha_2 \in E$ dos raíces de f. Como f es irreducible existe un K-isomorfismo $\varphi: K(\alpha_1) \to K(\alpha_2)$ que aplica $\alpha_1$ en $\alpha_2$. $\varphi$ se extiende a un K-automorfismo de E $\overline{\varphi} \in G(E/K)$ tal que $\overline{\varphi}(\alpha_1) = \alpha_2$. Luego G es transitivo.

Recíprocamente, supongamos $f(X)$ sin raíces múltiples y con grupo de Galois G transitivo. Sea $g(X)$ un factor irreducible de $f(X)$ y $\alpha$ una raíz de $g(X)$, $\beta$ una cualquiera de $f(X)$. Por hipótesis existe $\sigma \in G$ tal que $\sigma(\alpha) = \beta$. Entonces $g(\beta) = g(\sigma(\alpha)) = \sigma(g(\alpha)) = \sigma(0) = 0$, lo que prueba que toda raíz de f es raíz de g. Luego $f = g$ y f es irreducible.

LA ECUACION GENERAL DE GRADO n.

Como ejemplo motivador consideremos el caso de ecuaciones algebraicas con coeficientes racionales, $f(X) = 0$. Sin pérdida de generalidad puede suponerse que

el polinomio f(X) es mónico.

La ecuación $X^2 + a_1X + a_0 = 0$, donde $a_1$ y $a_0$ son dos indeterminadas, se llama la ecuación general de 2° grado sobre Q. Tiene sus coeficientes en el cuerpo $Q(a_1,a_0)$, y sus raíces (en una clausura algebraica $\overline{Q(a_1a_0)}$) son

$$\frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2} \qquad (*).$$

Cualquier ecuación algebraica de 2°grado con coeficiente en Q (mónica) se obtiene especializando $a_1$ y $a_0$ en la ecuación general, es decir, reemplazando $a_1$ y $a_0$ por los números correspondientes, y sus raíces se calculan a partir de (*).

Análogamente, $X^3 + a_2X^2 + a_1X + a_0 = 0$ es la ecuación general de 3° grado, donde $a_2$, $a_1$, $a_0$ son tres indeterminadas y sus raíces están dadas por las fórmulas de Cardano:

Si $p = a_1 - \frac{a_2^2}{3}$ y $q = \frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0$ sean

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad , \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

donde las raíces cúbicas u y v se eligen de modo que $u.v = -\frac{p}{3}$. Entonces las raíces de la ecuación $X^3 + a_2X^2 + a_1X + a_0 = 0$ son:

$$u + v - \frac{a_2}{3} \quad , \quad \varepsilon u + \varepsilon^2 v - \frac{a_2}{3} \quad , \quad \varepsilon^2 u + \varepsilon v - \frac{a_2}{3}$$

siendo $\varepsilon$ una raíz cúbica primitiva de la unidad.

Cualquier ecuación cúbica con coeficientes en Q resulta de la general especializando $a_2$, $a_1$, $a_0$ y así las fórmulas anteriores dan sus raíces.

Para polinomios de 4° grado hay también una fórmula que da las raíces en función de los coeficientes mediante operaciones racionales y radicales de 2° y 3° grado.

Si sucediera lo mismo para las ecuaciones de grado n, $n \geqslant 5$, es decir, si existiera una fórmula que permitiera calcular las raíces de cualquier ecuación alge-

braica de grado $n > 4$ a partir de los coeficientes mediante una sucesión finita de operaciones racionales y radicales entonces la ecuación general $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = 0$ sería resoluble por radicales sobre el cuerpo $Q(a_{n-1},\ldots,a_0)$ de sus coeficientes. Pero vamos a demostrar que esto no es así probando que su grupo de Galois es $S_n$.

Estas ideas se pueden aplicar a ecuaciones algebraicas con coeficientes en un cuerpo arbitrario K, y estudiar la resolubilidad por radicales de la ecuación general para cada grado n.

Sea entonces K un cuerpo, n un entero positivo. El polinomio

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 ,$$

donde $a_{n-1},\ldots,a_0$ son n indeterminadas, se llama el polinomio general de grado n sobre K. $f(X)$ es un polinomio con coeficientes en el cuerpo $K(a_{n-1},\ldots,a_0)$.

Sean $t_1,\ldots,t_n$ sus raíces en una clausura algebraica de $K(a_{n-1},\ldots,a_0)$.

$$f(X) = \prod_{i=1}^{n} (X - t_i) \quad \text{y de aquí sigue que}$$

$$-a_{n-1} = \sum_{i=1}^{n} t_i = s_1 \quad , \quad a_{n-2} = \sum_{i<j} t_i t_j = s_2 \quad , \ \ldots \ , \quad (-1)^n a_0 = \prod_{i=1}^{n} t_i = s_n$$

donde $s_1,\ldots,s_n$ son las funciones simétricas elementales de $t_1,\ldots,t_n$. Luego

$$f(X) = X^n - s_1X^{n-1} + s_2X^{n-2} - \ldots + (-1)^n s_n .$$

El cuerpo de raíces de $f(X)$ sobre $F = K(a_{n-1},\ldots,a_0) = K(s_1,\ldots,s_n)$ es $E = K(a_{n-1},\ldots,a_0,t_1,\ldots,t_n) = K(t_1,\ldots,t_n)$. Queremos probar que $G(E/F) = S_n$, lo que resultaría de un ejemplo ya estudiado si se supiera que $t_1,\ldots,t_n$ son algebraicamente independientes sobre K.

En pág. 76 vimos que si $u_1,\ldots,u_n$ son elementos de una extensión de K alge-

braicamente independientes sobre K entonces el grupo de Galois del polinomio

$$f^*(X) = \prod_{i=1}^{n}(X - u_i) = X^n - s_1^*X^{n-1} + s_2^*X^{n-2} - \ldots + (-1)^n s_n^*$$

donde $s_1^*,\ldots,s^*_n$ son las funciones simétricas elementales de $u_1,\ldots,u_n$, es $G(E^*/F^*) = S_n$, siendo $E^* = K(u_1,\ldots,u_n)$ el cuerpo de raíces de $f^*$ sobre $F^* = K(s_1^*,\ldots,s_n^*)$.

Se trata de probar que $G(E/F) \simeq G(E^*/F^*)$.

Para lo que es suficiente demostrar que existe un isomorfismo $\varphi\colon F \to F^*$ tal que el isomorfismo inducido $\tilde{\varphi}\colon F[X] \to F^*[X]$ aplica $f(X)$ en $f^*(X)$, pues entonces por la unicidad del cuerpo de raíces, (Teorema 4.4), $\varphi$ se extiende a un isomorfismo $\overline{\varphi}\colon E \to E^*$ y en consecuencia $G(E/F) \simeq G(E^*/F^*)$.

Sea $\varphi\colon F \to F^*$ tal que $\varphi\left(\dfrac{g(s_1,\ldots,s_n)}{h(s_1,\ldots,s_n)}\right) = \dfrac{g(s_1^*,\ldots,s_n^*)}{h(s_1^*,\ldots,s_n^*)}$.

Para ver que $\varphi$ está bien definido y que es un isomorfismo basta ver que restringido al anillo $K[s_1,\ldots,s_n]$ es un isomorfismo sobre el anillo $K[s_1^*,\ldots,s^*_n]$, puesto que F y F* son los respectivos cuerpos de cocientes. Y es claro que la restricción de $\varphi$ es un epimorfismo de anillos. Además es inyectivo pues $g(s_1^*,\ldots,s_n^*) = 0$ implica $g = 0$ ya que las funciones simétricas elementales $s_1^*,\ldots,s_n^*$ son algebraicamente independientes sobre K.

Queda probado así que $G(E/F) = S_n$ y que $t_1,\ldots,t_n$ son algebraicamente independientes sobre K. Además el polinomio general $f(X)$ es irreducible sobre $K(a_{n-1},\ldots,a_0)$, lo que resulta del Teorema 9.7. Luego

TEOREMA 9.8. El polinomio general de grado n sobre un cuerpo K, $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ es irreducible y separable sobre $K(a_{n-1},\ldots,a_0)$ y su grupo de Galois es $S_n$.

De aquí sigue el famoso teorema

TEOREMA 9.9. (Abel-Ruffini). La ecuación general de grado n sobre un cuerpo K es resoluble por radicales si y sólo si $n \leqslant 4$.

De este teorema sigue que si $n \geqslant 5$ las raíces del polinomio general de grado n no son expresables por radicales y por lo tanto no existe una "fórmula" para calcular por radicales las raíces de todos los polinomios de grado n con coeficientes en un cuerpo K. Pero podría suceder que cada uno de ellos fuera resoluble por radicales aunque sin ser posible expresar todas las soluciones mediante una "fórmula" única. El resultado obtenido por Galois es más completo.

En el caso K = Q permite mostrar la existencia de polinomios no resolubles por radicales para cada grado $n \geqslant 5$.

Si K = R, de acuerdo con la definición 2, todo polinomio no constante de R[X] es resoluble por radicales puesto que $C \supset R$ es una extensión radical de R.
Si K es un cuerpo finito entonces todo polinomio no constante f con coeficientes en K es resoluble por radicales ya que si E es un cuerpo de raíces de f, E es una extensión finita de K, luego una extensión cíclica y el grupo de Galois G(E/F) es resoluble. También puede verse así: como $E = K(\theta)$ y $\theta$ verifica la ecuación $X^{q-1} - 1 = 0$, donde q es el número de elementos de E, E es una extensión radical de K y por lo tanto cada raíz de f tiene una expresión radical.

EJERCICIOS.

Decir si las siguientes proposiciones son verdaderas:

1) Si K es un cuerpo finito, existe una extensión Galois de K de grado n, $\forall\ n \in N$.

2) Para todo $n \in N$ existe una extensión Galois de Q de grado n.

3) Cualquier cuerpo K tiene una extensión Galois de grado n.

4) Toda extensión radical de un cuerpo K es finita.

5) Toda extensión finita es radical.

6) Toda extensión finita está contenida en un radical.

7) El orden del grupo de Galois de un polinomio de grado n divide a n!.

8) Ninguna ecuación de quinto grado es resoluble por radicales. Es consecuencia del teorema de Abel-Ruffini.

9) El grupo de Galois de un polinomio cúbico de Q[X] es $A_3$ o $S_3$.

10) Si $K \subset E$ es una extensión algebraica y separable de K, existe una extensión Galois de K que contiene a E.

11) Si $K \subset E$ es una extensión algebraica y separable de K, existe una única extensión Galois de K que contiene a E. (a menos de K-isomorfismos).

12) Si $K \subset E$ es una extensión finita tal que el número de K-automorfismos de E es [E:K] entonces E es Galois sobre K.

13) Si $K \subset E$ es una extensión Galois, dos extensiones intermedias entre K y E del mismo grado son isomorfas.

14) Si $f(X) \in K[X]$ es separable y resoluble por radicales su cuerpo de raíces es una extensión radical de K.

15) Todo polinomio irreducible de Q[X] de grado 13 tiene grupo de Galois $S_{13}$.

16) El producto directo de n grupos resolubles es un grupo resoluble.

## BIBLIOGRAFIA


1. ADAMSON I., Introduction to field theory, Edinburgh, Oliver and Boyd, 1964.
2. ARTIN E., Galois theory, Notre Dame Mathematical Lectures, N°2, 1964.
3. AUSLANDER M. and BUSCHBAUM D., Groups, rings and modules, Harper and Row Publishers, N.Y., 1974.
4. BOURBAKI N., Éléments de Mathématique, Algèbre, Chapitres IV et V, Hermann et Cie, Paris, 1950.
5. EDWARDS H.M., Galois theory, Springer-Verlag, 1984.
6. GAAL L., Classical Galois theory, Chelsea Publishing Co., N.Y., 1971.
7. HUNGERFORD T.W., Algebra, Springer-Verlag, revised printing, 1980.
8. JACOBSON N., Lectures in abstract algebra, Vol. 3: Theory of fields and Galois theory, Van Nostrand Co., 1964.
9. KAPLANSKY I., Fields and rings, The University Chicago Press, 1972.
10. KAPLANSKY I., Introduçao a la Teoría de Galois, Río de Janeiro, 1958.
11. LANG S., Algebra, Addison-Wesley Publishing Co., Reading, Mass., 1965.
12. NAGATA M., Field theory, Pure and Applied Mathematics, Marcel Dekker, 1977.
13. STEWART I., Galois theory, Chapman and Hall, London, 1973.
14. VAN DER WAERDEN B.L., Modern algebra, Vol.I, Van Nostrand, Princeton, N.J., 1958.
15. WINTER D.J., The structure of fields, Springer-Verlag, 1974.
16. ZARISKI O. and SAMUEL P., Commutative algebra, Vol.I, Van Nostrand, 1958.


## ASPECTOS HISTORICOS


17. BOURBAKI N., Éléments d'histoire des mathématiques, Hermann et Cie, Paris, 1960.
18. BOYER C., A history of mathematics, John Wiley & Sons, 1968.

19. DUPUY P., La vie d'Évariste Galois, Ann. de l'Éc. Norm. (3), 13 (1896), 197-266.

20. KIERNAN B.M., The development of Galois theory from Lagrange to Artin, Arch. Hist. Exact Sci. 8 (1971), 40-154.

21. ROTHMAN T., Genius and biographers: The fictionalization of Évariste Galois, Amer. Math. Montnly 89 (1982), 84-106.

22. STRUIK D., A concise history of mathematics, Dover Publications, 1948.

# INDICE