Teoría de Galois.

José Cruz García Zagal (el líder).

Mayo de 2002

Contenido

Introducción

En el presente trabajo se tratará de dar un panorama general de la *Teoría de Galois*. Este texto está diseñado para un primer acercamiento a la teoría de campos, así como el de establecer la importancia y relevancia historica que ha tenido el desarrollo de dicha teoría.

En este texto existen capítulos que pueden ser considerados como 'no escenciales' para la comprensión de el material. Tales capítulos son el 6, ...

Capítulo 1

Preliminares.

El objetivo de este capítulo es el de introducir los fundamentos de la teoría de Galois desarrollada posteriormente, conceptos como: 'anillo', 'campo', 'dominio entero', 'ideal', 'polinomio' y 'máximo común divisor '; y las técnicas del algoritmo de Euclides para encontrar el máximo común factor de dos polinomios. El lector que encuentre estas ideas como obvias puede omitir esta parte de la lectura.

Se asumirá que el lector está familiarizado con las propiedades de factorización en el anillo de los números enteros, así como también la parte de la teoría de anillos y anillos cociente, para consultar está parte ver [1] . A continuación introduciremos la notación estándar a utilizar.

1.1 Propiedades generales de anillos.

Se le dará el nombre de *anillo* a un conjunto R junto con dos operaciones binarias $+$, (suma), y $\times$, (multiplicación), de tal forma que R forme un grupo abeliano con la operación suma, la multiplicación sea asociativa y se satisfagan las leyes distributivas, es decir, para toda $a, b, c \in R$

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

y

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

La identidad aditiva de R será denotada por el símbolo 0. Se escribirá ab en lugar de $a \times b$.

Un *dominio entero* es un anillo D con tres propiedades adicionales:

a) La multiplicación en D es conmutativa.

b) Existe un elemento $1 \in D$ tal que $a1 = 1a = a$, para toda $a \in D$.

c) Si $ab = 0$ para $a, b \in D$, entonces $a = 0$ ó bien $b = 0$.

Un *campo*, es un anillo F tal que $F - \{0\}$ es un grupo abeliano bajo la multiplicación. Esto es todo elemento no cero $a \in F$ tiene un inverso multiplicativo a^{-1}. Escribiremos a/b o $\frac{a}{b}$ para denotar a ab^{-1}. Observemos que todo campo es un dominio entero, pues si F es un campo y $ab = 0$ con $a \neq 0$, entonces como sabemos que existe $a^{-1} \in F$ tal que

$$aa^{-1} = a^{-1}a = 1$$

por lo que

$$a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$$

por lo tanto $b = 0$. Por lo tanto F es un dominio entero.A el elemento 1 de F se le llamara también identidad multiplicativa

Ejemplos importantes de tales estructuras son el dominio entero $\mathbb{Z}$ de números enteros y los campos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ de números racionales, números reales y números complejos respectivamente.

Un *subanillo* de un anillo R es un subconjunto no vacío S, tal que si $a, b \in S$ entonces $a + b \in S$, $a - b \in S$ y $ab \in S$.

Un *subcampo* de un campo F es un subconjunto de F que contiene al 0 y al 1, tal que si $a, b \in S$ entonces $a + b \in S$, $a - b \in S$, $ab \in S$ y si $a \neq 0$ entonces $a^{-1} \in S$.

Un *ideal* de un anillo R es un subanillo I de R, de tal manera que si $i \in I$, $r \in R$ entonces tanto ri como ir son elementos de I.

Por ejemplo, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, $\mathbb{R}$ es un subcampo de $\mathbb{C}$, además $2\mathbb{Z}$ es un ideal para $\mathbb{Z}$.

Si I es un ideal de un anillo R se puede formar el *anillo cociente* R/I el cual consiste de las clases laterales de I en R con las operaciones:

$$(I + r) + (I + s) = I + (r + s)$$

y

$$(I + r)(I + s) = I + (rs)$$

donde $r, s \in R$ y $I + r$ es la clase lateral $\{i + r : i \in I\}$. Por ejemplo, sea $n\mathbb{Z}$ el anillo de los enteros que es divisible por un entero fijo n. Este es un ideal de $\mathbb{Z}$, y el anillo cociente $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ es el *anillo* de los enteros módulo n.

Mostraremos la siguiente propiedad para $\mathbb{Z}_n$.

Teorema 1.1.1. *El anillo $\mathbb{Z}_n$ es un campo si, y solamente si, n es un número primo.*

Prueba. Primero supongamos que n no es un número primo. Si $n = 1$ entonces $\mathbb{Z}_n = \mathbb{Z}/\mathbb{Z}$ el cual tiene sólo un elemento, por lo que no puede ser un campo. Si $n > 1$ entonces $n = rs$ para enteros menores que n, si llamamos $I = n\mathbb{Z}$ se tiene que

$$(I + r)(I + s) = I + rs = I.$$

Pero I es el cero de $\mathbb{Z}/I$, donde tanto $I + r$ como $I + s$ son distintos de cero. Dado que todo campo es un dominio entero, tenemos que $\mathbb{Z}/I$ no es un campo. Por lo tanto n es un número primo.

Recíprocamente ahora supongamos que n es primo. Sea $I + r$ un elemento no cero en $\mathbb{Z}/I$. Dado que r y n son primos relativos entonces, existen enteros a y b tales que $1 = ar + bn$ (por propiedades básicas de los enteros). Entonces

$$(I+a)(I+r) = (I+1) - (I+n)(I+b) = I+1$$

de manera similar

$$(I+r)(I+a) = I+1$$

Dado que $I+1$ es la identidad de $\mathbb{Z}/I$ se tiene que encontramos un inverso multiplicativo para el elemento no cero $I+r$, por lo tanto todo elemento no cero de $\mathbb{Z}/I$ tiene inverso. Por lo tanto $\mathbb{Z}_n = \mathbb{Z}/I$ es un campo. □

De ahora en adelante adoptaremos la convención de que en $\mathbb{Z}_n$ los elementos los escribiremos como $0, 1, 2, \ldots, n-1$ en lugar de $n\mathbb{Z}, n\mathbb{Z}+1, n\mathbb{Z}+2, \ldots, n\mathbb{Z}+n-1$.

1.2 La característica de un campo.

Definición 1.2.1. El *subcampo primo* de un campo K es la intersección de todos los subcampos de K.

Es fácil de ver que la intersección de una colección de subcampos de un campo K es un subcampo de K. (que contiene al cero y al elemento unitario del campo) Así pues tenemos que el subcampo primo de un campo K es el único y más pequeño subcampo de K. Por ejemplo para $\mathbb{Q}$ y $\mathbb{Z}_p$ (p primo) se tiene que ellos mismos son su subcampo primo (pues ellos no tienen subcampos propios). El siguiente teorema muestra que estos son los únicos subcampos primos.

Teorema 1.2.2. *Todo subcampo primo es isomorfo al campo de los números racionales $\mathbb{Q}$, ó bien a el campo de los enteros módulo p, $\mathbb{Z}_p$.*

Prueba. Si K es un campo y P es su subcampo primo, entonces P contiene al 0 y al 1 de K y mas aún contiene a los elementos n^* ($n \in \mathbb{Z}$) definidos por

$$n^* = \begin{cases} \underbrace{1 + \cdots + 1}_{n} & n > 0 \\ 0 & n = 0 \\ -(-n)^* & n < 0 \end{cases}$$

Un pequeño calculo utilizando las leyes distributivas muestra que la función

$$^* : \mathbb{Z} \longrightarrow P$$

define un homomorfismo de anillos. Examinaremos los posibles casos que tenemos.

Caso 1. Si $n^* = 0$ para alguna $n \neq 0$. Dado que $(-n)^* \neq 0$ entonces existe un entero positivo p menor que n tal que $p^* = 0$. Si p es compuesto, digamos $p = rs$ donde r y s son enteros positivos menores que p, tenemos que $r^*s^* = p^* = 0$, por lo que $r^* = 0$ o $s^* = 0$ lo que contradice la definición de p. Por lo tanto p es primo. Los elementos n^* forman un anillo isomorfo a $\mathbb{Z}_p$, el cual es un campo (teorema 1.1) y por definición de P tenemos que $\mathbb{Z}_p$ es el subcampo primo de K.

Caso 2. Si $n^* \neq 0$ entonces P debe contener a todos los elementos de la forma $\frac{m^*}{n^*}$ donde m, n son enteros y $n \neq 0$. Pero estos elementos forman un capo isomorfo a $\mathbb{Q}$ (mediante la función que manda $\frac{m^*}{n^*}$ a $\frac{m}{n}$). Por lo tanto el subcampo primo de K es isomorfo a $\mathbb{Q}$. □

Definición 1.2.3. Si el subcampo primo del campo K es isomorfo a $\mathbb{Q}$ se dice que K es de *caracteristica* 0. Si el subcampo primo de K es isomorfo a $\mathbb{Z}_p$ se dice que K es de *caracteristica p.*

Por ejemplo, los campos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, todos tienen característica cero, dado que en cada caso su subcampo primo es $\mathbb{Q}$. El campo $\mathbb{Z}_p$ (p primo) tiene característica p, más adelante veremos que existen otros campos de característica p.

Los elementos n^* definidos en la prueba del teorema anterior son de gran importancia en lo que sigue. convenimos ahora en omitir el asterisco y escribir solamente n en lugar de n^*. Este abuso de notación no debe de causar confusión, ya que podemos encontrarnos en un campo donde n puede ser cero, sin que el campo tenga al cero como elemento. Por ejemplo, en $\mathbb{Z}_5$ se tiene que $2 = 7 = -3$ etc.

Esta dificultad no se tiene en campos de característica cero. Con esta convención el producto nk ($n \in \mathbb{Z}$, $k \in K$) tiene sentido, pues

$$n = \pm(\underbrace{1 + \cdots + 1}_{n-veces})$$

Lema 1.2.4. *Si K es un subcampo de L entonces, K y L tienen la misma característica.*

Prueba. Es claro que K y L tienen el mismo subcampo primo. □

Lema 1.2.5. *Si k es un elemento no cero de un campo K, y si n es un entero tal que $nk = 0$ entonces, n es un múltiplo de la característica de K.*

Prueba. Podemos tener que $n = 0$ en K, es decir en notación anterior $n^* = 0$. Si la característica es cero esto implica que $n = 0$ (como entero). Si la característica es p, con $p > 0$ entonces esto implica que n es un múltiplo de p. □

1.3 Campo de fracciones.

Algunas veces es posible el envolver a un anillo R en un campo; esto es, encontrar un campo que contenga a un anillo isomorfo a R. Por ejemplo, $\mathbb{Z}$ puede ser envuelto en el campo de los números racionales $\mathbb{Q}$. Este ejemplo tiene la particularidad de que todo elemento de $\mathbb{Q}$ es una fracción cuyo numerador y denominador pertenecen a $\mathbb{Z}$. Buscamos generalizar esta situación.

Definición 1.3.1. Un *campo de fracciones* de un anillo R, es un campo K que contiene un subanillo R' isomorfo a R, de tal manera que cada elemento de K pueda ser expresado de la forma $\frac{r}{s}$ para $r, s \in R$ con $s \neq 0$.

Un análisis en la forma en la que $\mathbb{Z}$ puede ser envuelto por $\mathbb{Q}$ establece el siguiente teorema.

Teorema 1.3.2. *Todo dominio entero tiene campo de fracciones.*

Prueba. Sea pues R un dominio entero, y S el conjunto de todas las parejas ordenadas (r, s) donde $r, s \in R$ y $s \neq 0$. Definimos la relación $\sim$ en S como:

$$(r, s) \sim (t, u) \Longleftrightarrow ru = st$$

Es fácil verificar que $\backsim$ así definida es una relación de equivalencia; denotaremos la clase de equivalencia de (r, s) por $[r, s]$. El conjunto F de todas las clases de equivalencia es el que llamaremos campo de fracciones. Definiendo las operaciones suma y producto en F por:

$$[r, s] + [t, u] = [ru + ts, su]$$

y

$$[r, s]\,[t, u] = [rt, su]$$

Una serie de cálculos muestra que F así definido satisface las propiedades requeridas. Dado que estos cálculos son rutina se le pedirá al lector que lo demuestre, señalándole a continuación los puntos a demostrar.

a) Las operaciones están bien definidas. Es decir si

$$(r, s) \sim (r', s')$$

y

$$(t, u) \sim (t', u')$$

entonces

$$[r, s] + [t, u] = [r', s'] + [t', u']$$

y

$$[r,s]\,[t,u] = [r',s']\,[t',u']\,.$$

b) Las operaciones son operaciones binarias en F.

c) F es un campo.

d) El mapeo $R \longrightarrow F$ dado por $r \to [r,1]$ es un monomorfismo.

e) $[r,s] = [r,1] \,/\, [s,1]\,.$ □

Se puede mostrar (ver ejercicio 1.16) que dado un dominio entero R, cualesquiera dos campos de fracciones de R son isomorfos. Por ello nos podemos referir a el campo construido en el teorema 1.3.2, como el campo de fracciones de R. Y podemos identificar cada elemento $r \in R$ con su imagen $[r,1]$ en F; denotaremos a $[r,s] = r/s$.

1.4 Polinomios.

Existe una considerable confusión respecto a que es un polinomio. Una precisa y lógica definición puede ser dada de manera formal, pero preferimos no hacerlo de esta manera (ver Hartley y Hawkes [14] pag.37). Si R es un anillo en el que la multiplicación es conmutativa. Se define un *polinomio sobre R en la indeterminada t* a una expresión de la forma:

$$r_0 + r_1 t + ... + r_n t^n$$

donde $r_0, ..., r_n \in R$, $0 \leq n \in \mathbb{Z}$, y t es la indeterminada. los elementos $r_0, ..., r_n$ serán llamados los coeficientes del polinomio. De manera natural el termino $0t^m$ puede ser omitido o simplemente ser escrito por 0, y $1t^m$ puede ser remplazado por t^m.

Dos polinomios son definidos como *iguales* si, y sólo si los coeficientes correspondientes son iguales (con la convención de que los coeficientes de el polinomio sean todos cero excepto a lo más un número finito). Esta convención es la que puede llegar a causar un poco de confusión. La suma y el producto de dos polinomios son definidas de la siguiente manera: escribiremos

$$\sum_{\mathbb{N}} r_i t^i$$

en lugar de

$$r_0 + r_1 t + ... + r_n t^n$$

donde la suma es considerada sobre todos los enteros $i \geq 0$, y r_k es definido como cero si $k \geq n$. Entonces si

$$r = \sum_{i \in \mathbb{N}} r_i t^i$$

$$s = \sum_{i \in \mathbb{N}} s_i t^i$$

se define:

$$r + s := \sum_{i \in \mathbb{N}} (r_i + s_i) t^i$$

y

$$rs := \sum_{i \in \mathbb{N}} q_j t^j$$

donde

$$q_j := \sum_{h+i=j} r_h s_i t^i$$

Es fácil de verificar que bajo estas operaciones, el conjunto de todos los polinomios en una indeterminada sobre R forma un anillo.

El *anillo de polinomios sobre R en una indeterminada t* que se denotara por el símbolo $R[t]$. Para diferentes indeterminadas $u, v, w, ...$ se obtienen los anillos de polinomios $R[u], R[v], R[w], ...$ los cuales son isomorfos de manera natural. Se pueden definir polinomios en muchas indeterminadas $t_1, t_2, ...$ y obtenemos el anillo de polinomios $R[t_1, t_2, ...]$ de una manera análoga.

Un elemento de $R[t]$ será denotado con una sola letra digamos f siempre que sea claro que la indeterminada t esta involucrada. Si existe ambigüedad escribiremos $f(t)$ para enfatizar el papel que juega la indeterminada t. Esta notación tiene un efecto desafortunado, parece ser que f es una función con t como una 'variable'. Esto no es cierto, sin embargo cada polinomio define una función de R en R, que actúa de la siguiente manera: si

$$f = \sum_{i \in \mathbb{N}} r_i t^i$$

y $\alpha \in R$ entonces α es transformado en

$$\sum_{i \in \mathbb{N}} r_i \alpha^i$$

Este es un elemento de R y no un polinomio, si además utilizamos el mismo símbolo f para denotar a la función anterior se tiene que $f(\alpha) = \sum_{i \in \mathbb{N}} r_i \alpha^i$. Nuevamente abusamos de el lenguaje tradicional y tendremos cuidado de no causar confusión.

El principal punto en mente es el de distinguir que dos polinomios distintos sobre R puedan dar la misma función sobre R. Por ejemplo, en $\mathbb{Z}_2$ los polinomios t y t^2 dan la misma función. Esta es una de las razones por la que no vemos a los polinomios como funciones. Otra de las razones es la de que un polinomio puede dividir a otro, sin embargo que una función divida a otra no tiene sentido (el que nosotros le vamos a dar).

Lema 1.4.1. *Si R es un dominio entero y t es una indeterminada entonces $R[t]$ es un dominio entero.*

Prueba. Supóngase que $f = f_0 + f_1 t + ... + f_n t^n$, $g = g_0 + g_1 t + ... + g_m t^m$ donde $f_n \neq 0 \neq g_m$ y todos los coeficientes pertenecen a R. El coeficiente de t^{m+n}, en fg, es $f_n g_m$ el cual es distinto de cero dado que R es un dominio entero. Por lo tanto si f, g son no cero, entonces fg es no cero. Esto implica que $R[t]$ es un dominio entero como queríamos. $\square$

El Teorema 1.3.2, implica que $R[t]$ tiene campo de fracciones, el cual llamaremos *el campo de expresiones racionales* ó *campo de funciones racionales en t sobre R* y lo denotaremos por $R(t)$. Similarmente $R[t_1, ..., t_n]$ tiene su campo de fracciones $R(t_1, ..., t_n)$.

1.5 El algoritmo de Euclides.

Primeramente necesitamos de una:

Definición 1.5.1. Si f es un polinomio en un anillo conmutativo R y $f \neq 0$ entonces *el grado* de f es la mayor potencia de t que ocurre en f con coeficiente no cero.

Esto es si

$$f = \sum_{i \in \mathbb{N}} r_i t^i$$

con $r_n \neq 0$ y $r_m = 0$ para $m > n$, entonces f tiene grado n. Escribiremos ∂f para denotar a el grado de f.

Para el caso en que $f = 0$ adoptaremos la convención de que $\partial f = -\infty$ (el cual es un símbolo con las siguientes propiedades:

$-\infty < n$ para todo entero n, $-\infty + n = -\infty, -\infty \cdot n = -\infty, (-\infty)^2 = -\infty$).
El siguiente resultado es inmediato de la definición anterior.

Proposición 1.5.2. *Si R es un dominio enero y f, g son polinomios sobre R, entonces*

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

y

$$\partial(fg) = \partial f + \partial g.$$

(la desigualdad en la primera linea se da por la posibilidad de que los términos mayores se cancelen)

Muchos de los resultados importantes en la teoría de la factorización se derivan de el hecho de que un polinomio puede ser dividido por otro.

Proposición 1.5.3. *Sean f y g polinomios sobre un campo K; y supóngase que f es no cero. Entonces existen polinomios únicos q y r sobre K tal que*

$$g = fq + r, \text{ donde } r \text{ tiene grado menor que el grado de } f.$$

Prueba. Se hará por inducción sobre el grado de g.

Si $\partial g = 0$ entonces $g = k \in K$. Si también $\partial f = 0$ entonces $f = j \in K$ y tomamos a $q = \frac{k}{j}$ y a $r = 0$. En otro caso si $\partial f > 0$ podemos tomar a $q = 0$ y a $r = g$. Por lo que el primer paso de la inducción esta probado.

Ahora asumiremos que el resultado es valido para polinomios de grado menor que n, sea g un polinomio sobre K tal que $\partial g = n > 0$. Si $\partial f > \partial g$, podemos tomar a $q = 0$, $r = g$. En el otro caso se tiene que:

$$f = a_m t^m + ... + a_0$$

y

$$g = b_n t^n + ... + b_0$$

donde $a_m \neq 0 \neq b_n$ y $m \leq n$. Ahora elegimos a

$$g_1 = b_n a_m^{-1} t^{n-m} f - g$$

Dado que que los términos de grado mayor se cancelan se tiene que $\partial g_1 < \partial g$. Por hipótesis de inducción podemos encontrar polinomios q_1 y r_1 tal que $g_1 = fq_1 + r_1$ con $\partial r_1 < \partial f$. Ahora tenemos que los polinomios buscados para f y g son:

$$q = b_n a_m^{-1} t^{n-m} - q_1;$$

y

$$r = r_1$$

Finalmente probaremos la unicidad. Supongamos que $g = fq_1 + r_1 = fq_2 + r_2$ donde $\partial r_1, \partial r_2 < \partial f$. Entonces $f(q_1 - q_2) = r_1 - r_2$. Por la Proposición 1.5.2, el polinomio de el lado izquierdo tiene grado mayor que el polinomio de el lado derecho, por lo que ambos lados de la igualdad son cero. Dado que $f \neq 0$ se tiene que $q_1 = q_2$ y que $r_1 = r_2$. Por lo tanto q y r son únicos. □

Con la notación anterior q sera llamado el *cociente* y r será llamado el *residuo* (de dividir g por f). El proceso de encontrar q y r es llamado el *Algoritmo de la División*. Nuestro siguiente paso es introducir nociones de divisibilidad para polinomios. En particular la idea de 'máximo común factor', que será de suma importancia para la 'aritmetíca' de polinomios que veremos en el siguiente capítulo.

Definición 1.5.4. Sean f y g dos polinomios sobre un campo K. se dice que f *divide* a g (o f es un *factor* de g, o g es un *múltiplo* de f) si existe algún polinomio h sobre K tal que $g = fh$.

La notación $f \mid g$ significara que f divide a g, donde $f \nmid g$ significara que f no divide a g (esta notación fue introducida primeramente por *Gauss*).

Un polinomio d sobre K es un *máximo común factor* (mcf) de f y g si $d \mid f$ y $d \mid g$ y siempre que $e \mid f$ y $e \mid g$ se tiene que $e \mid d$.

Note que decimos que d es un máximo común factor y no el máximo común factor, esto es pues los máximos comunes factores no son únicos. El siguiente lema prueba que estos son únicos salvo una constante, es decir salvo un polinomio de grado cero.

Lema 1.5.5. *Si d es un máximo común factor de los polinomios f, g sobre un campo K, si $0 \neq k \in K$, entonces kd es también un mcf de f y g.*

Más aún si d y e son máximos comunes factores de f y g. Entonces existe un elemento no cero $k \in K$ tal que $e = kd$.

Prueba. Claramente $kd \mid f$ y $kd \mid g$. Si $e \mid f$ y $e \mid g$ entonces $e \mid d$ por lo tanto $e \mid kd$. Por lo que kd es un mcf.

Ahora d y e son máximos comunes factores, entonces por definición $e \mid d$ y $d \mid e$. Por lo que $e = hd$ para algún polinomio h dado que $e \mid d$ el grado de e es menor o igual al grado de d esto implica que el grado de $h \leq 0$. Por lo que $h = k \in K$. Por lo tanto $0 \neq e = kd$, por lo que $k \neq 0$. $\square$

A continuación daremos un algoritmo el cual es útil para encontrar el mcf para dos polinomios distintos de cero. Este algoritmo es una generalización de el dado por Euclides para calcular el mcf de dos números enteros y es llamado también *algoritmo de Euclides.*

Algoritmo 1. *Ingredientes.* Dos polinomios f y g ambos no cero, sobre un campo K.
Receta. Por convención llamaremos a $f = r_{-1}$, $g = r_0$. Usando repetidamente el algoritmo de la división encontramos polinomios q_i y r_i sobre K tal que.

$$\begin{aligned} r_{-1} &= q_1 r_0 + r_1 \qquad con \quad \partial r_1 < \partial r_0 \\ r_0 &= q_2 r_1 + r_2 \qquad con \quad \partial r_2 < \partial r_1 \\ r_1 &= q_3 r_2 + r_3 \qquad con \quad \partial r_3 < \partial r_2 \\ &\;.. \\ &\;.. \\ r_i &= q_{i+2} r_i + r_{i+2} \qquad con \quad \partial r_{i+2} < \partial r_{i+1} \end{aligned} \tag{1.1}$$

Dado que los grados de r_i decrecen, eventualmente este proceso termina y de este modo sólo podemos tener que $r_{s+2} = 0$ para algún s y la última ecuación en la lista es de la forma

$$r_s = q_{s+2} r_{s+1} \tag{1.2}$$

Teorema 1.5.6. *Con la anterior notación r_{s+1} es el mcf para f y g sobre K.*

Prueba. Primero mostraremos que r_{s+1} divide tanto a f como a g. Se usara inducción descendente para mostrar que $r_{s+1} \mid r_i$ para toda i.
Claramente $r_{s+1} \mid r_{s+1}$, por la ecuación 1.2, tenemos que $r_{s+1} \mid r_s$. Usando la ecuación 1.1, se tiene que $r_{s+1} \mid r_{i+2}$ y $r_{s+1} \mid r_{i+1}$ entonces $r_{s+1} \mid r_i$. Por

lo tanto $r_{s+1} \mid r_i$ para toda i; en particular $r_{s+1} \mid r_0 = g$ y $r_{s+1} \mid r_{-1} = f$.

Ahora supongamos que $e \mid f$ y $e \mid g$. Por la ecuación 1.2, se sigue inductivamente que $e \mid r_i$. Por lo tanto $e \mid r_{s+1}$. De donde r_{s+1} es un mcf de f y g. $\square$

Ejemplo. Sea $f = 2t^7 + t^3 - 1$, $g = t^3 + 4$ sobre $\mathbb{Q}$. Se calcula el mcf de f y g como sigue:

$$2t^7 + t^3 - 1 = \left(t^3 + 4\right)\left(2t^4 - 8t + 1\right) + (-32t - 5)$$

$$\begin{aligned} t^3 + 4 &= (-32t - 5)\left(\frac{t^2}{32} + \frac{5t}{1024} - \frac{25}{32768}\right) + \frac{139937}{32768} - 32t - 5 \\ &= \frac{139937}{32768}\left(\frac{32768}{139937}(-32t - 5)\right) + 0. \end{aligned}$$

Por lo tanto (139937/32768) es un mcf. Esto es salvo un múltiplo irracional el mcf es 1. Finalizamos este capítulo deduciendo de el algoritmo euclidiano una propiedad importante de el mcf entre dos polinomios.

Teorema 1.5.7. *Sean f y g dos polinomios no cero sobre un campo K y sea d un mcf para f y g. Entonces existen polinomios a y b sobre K tal que $d = af + bg$.*

Prueba. Dado que los máximos comunes divisores son únicos salvo un factor constante, podemos asumir que $d = r_{s+1}$ donde d esta dado por las ecuaciones 1.1 y 1.2 de el algoritmo anterior. De manera inductiva por la hipótesis tenemos que existen polinomios a_i y b_i tales que $d = a_i r_i + b_i r_{i+1}$. Esto claramente es cierto para $i = s+1$, para estos podemos tomar $a_i = 1$, $b_i = 0$. Ahora por la ecuación 1.1, tenemos que $r_{i+1} = r_{i-1} - q_{i+1} r_i$. Por lo tanto por inducción tenemos que $d = a_i r_i + b_i\left(r_{i-1} - q_{i+1}\right)$. Por lo que si elegimos a $a_{i-1} = b_i$, $b_{i-1} = a_i - b_i q_{i+1}$ se tiene $d = a_{i-1} r_{i-1} + b_{i-1} r_i$. Utilizando inducción descendente tenemos que $d = a_{-1} r_{-1} + b_{-1} r_0 = af + bg$ donde $a = a_{-1}$, $b = b_{-1}$. Lo anterior completa la prueba. $\square$

Los pasos de inducción anteriores establecen un método practico para calcular a y b en un caso particular.

1.6 Ejercicios.

1.1 Muestra que $15\mathbb{Z}$ es un ideal de $5\mathbb{Z}$ y que $5\mathbb{Z}/15\mathbb{Z}$ es isomorfo a $\mathbb{Z}_3$.

1.2 ¿Serán los anillos $\mathbb{Z}$ y $2\mathbb{Z}$ isomorfos ?

1.3 Escribe las tablas de suma y multiplicación para $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$. ¿Cuales de estos anillos son dominios enteros y cúales son campos ?

1.4 ¿Cuales de las tablas de suma y multiplicación de el ejercicio 1.3 son simétricas respecto de su diagonal ?

1.5 Definimos un campo *primo* como un campo que no tiene subcampos propios. Muestra que los únicos campos primos son precisamente (salvo isomorfismo) $\mathbb{Q}$ y $\mathbb{Z}_p$ (p un número primo).

1.6 Muestra que las siguientes tablas definen un campo.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Encuentra su subcampo primo y su característica. ¿ Es isomorfo a $\mathbb{Z}_4$? ¿ Cuantos campos hay (salvo isomorfismo) que tengan 4 elementos?.

1.7 Verifica todos los detalles omitidos en la prueba de el teorema 1.3.2.

1.8 Consideremos los polinomios $3t$ y $2t$ sobre $\mathbb{Z}_6$ muestra que la segunda parte de la proposición 1.1.2 falla si R es un anillo que no es dominio entero ¿ Que pasa con la primera parte de la proposición bajo estas circunstancias

?.

1.9 Para los siguientes pares de polinomios f y g encuentra el cociente y el residuo de dividir g por f.

a) $g = t^7 - t^3 + 5$, $f = t^3 + 7$ sobre $\mathbb{Q}$.

b) $g = t^2 + 1$, $f = t^2$ sobre $\mathbb{Q}$.

c) $g = 4t^3 - 17t^2 + t - 3$, $f = 2t + 5$ sobre $\mathbb{R}$.

d) $g = t^3 + 2t - t + 1$, $f = t + 2$ sobre $\mathbb{Z}_3$.

e) $g = t^7 - 4t^6 + t^3 - 3t + 5$, $f = 2t^3 - 2$ sobre $\mathbb{Z}_7$.

1.10 Encuentre los máximos comunes factores para los pares de polinomios de el ejercicio anterior, verifica que tus resultados sean factores comunes tanto de f como de g.

1.11 Expresa los máximos comunes factores de el ejercicio anterior de la forma $af + bg$.

1.12 Un elemento x en un anillo R con identidad multiplicativa 1 se dice que es unidad en R si tiene un inverso multiplicativo en R. Muestra que las unidades de R forman un grupo bajo la multiplicación.

1.13 Encuentra la estructura del grupo de las unidades de $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{24}$.

1.14 ¿ Para que valores de n es cierto que el grupo de las unidades de $\mathbb{Z}_n$ tiene orden dividido por 2 ?.

1.15 Marca verdadero o falso según sea el caso en los siguientes incisos

a) Dado un par de polinomios este par tiene siempre mcf.

b) La función grado $\partial : R[t] \longrightarrow \mathbb{Z}$ que manda $f \to \partial f$ es un homomorfismo de anillos.

c) Todo anillo tiene un campo de fracciones.

d) Todo campo es isomorfo a su campo de fracciones.

e) $\mathbb{Z}_n$ es un dominio entero si y sólo si es campo.

f) Todo dominio entero es campo.

g) Todo campo es un dominio entero.

h) Un polinomio sobre K es una función de K en K.

i) Si K es un campo entonces $K[t]$ es un campo.

1.16 Sea D un dominio entero con campo de fracciones F. Si K es un campo. Pruebe que un monomorfismo $\phi : D \to K$ tiene una única extensión a un monomorfismo $\psi : F \to K$ definido por

$$\psi\left(\frac{a}{b}\right) = \frac{\phi(a)}{\phi(b)}$$

para $a, b \in D$.

Capítulo 2

Factorización de Polinomios.

Las ecuaciones polinomiales $f(x) = 0$ (donde f es un polinomio) han tenido una trascendencia histórica en las matemáticas. Para un polinomio f el problema de encontrar una solución es un simple cálculo, pero la teoría en general requiere técnicas mucho más refinadas. Si tenemos que f es el producto de dos polinomios g y h de grado menor, entonces las soluciones $f(x) = 0$ son precisamente aquellas donde $g(x) = 0$ y $h(x) = 0$.

Esta idea surge de la *aritmética* de polinomios, con particular referencia a lo desarrollado con la aritmética de los números enteros. El algoritmo euclidiano estudiado en el capítulo anterior es precisamente el punto de partida.

En este capítulo se definirán las cuestiones básicas con respecto a la divisibilidad y mostraremos que existen un cierto tipo de polinomios específicos, los polinomios 'irreducibles' los cuales juegan un papel fundamental en esta teoría, así como lo hacen los números primos en el anillo de los números enteros. Todo polinomio sobre un campo puede siempre ser expresado como el producto de polinomios irreducibles esencialmente de manera única.

También definiremos los 'ceros' de polinomios en relación con la teoría de factorización. En la sección final se investigara como reconstruir un polinomio a partir de sus ceros.

2.1 Irreducibilidad.

Definición 2.1.1. Un polinomio sobre un anillo conmutativo es *reducible* si es el producto de dos polinomios de grado menor. En otro caso diremos que el polinomio es *irreducible*.

Ejemplos.

1. Todos los polinomios de grado cero y uno son irreducibles, dado que ciertamente no pueden ser expresados como el producto de dos polinomios de grado menor.

2. El polinomio t^2-2 es irreducible sobre $\mathbb{Q}$. Para mostrar esto procederemos por contradicción, esto es supongamos que es reducible. Entonces

$$t^2 - 2 = (at + b)(ct + d)$$

Donde a, b, c, d son elementos de $\mathbb{Q}$. Dividiendo sí fuera necesario, podemos suponer que $a = 1 = c$. Entonces $b + d = 0$ y $bd = 2$, por lo que $b^2 = 2$, pero no existe un número racional tal que su cuadrado sea 2.

3. Sin embargo $t^2 - 2$ es reducible sobre $\mathbb{R}$, puesto que

$$t^2 - 2 = \left(t - \sqrt{2}\right)\left(t + \sqrt{2}\right).$$

Lo anterior muestra que polinomios irreducibles sobre un campo, pueden ser reducibles en un campo más grande.

Un polinomio reducible puede escribirse como producto de dos polinomios de grado menor y estos a su vez pueden ser reducibles y por tanto dividirse en factores de grado menor y continuar de esta manera. Este es un proceso terminal dado que los grados de los polinomios no pueden decrecer infinítamente.

Teorema 2.1.2. *Un polinomio no cero sobre K es el producto de polinomios irreducibles sobre K.*

Prueba. Si g es un polinomio no cero sobre K. Se procede por inducción sobre el grado de g. Si $\partial g = 0$ ó 1 entonces g es automáticamente reducible. Si $\partial g > 1$ entonces g es irreducible ó $g = hj$ donde $\partial h, \partial j < \partial g$. Por la hipótesis inductiva h y j son el producto de polinomios irreducibles cuyo producto es g. El teorema se sigue por inducción. $\square$

La importancia de los números primos en el anillo de los números enteros es que un entero se descompone como el producto de potencias de primos y resulta que dicha descomposición es única. Sin embargo en el anillo de los polinomios en una indeterminada sobre un campo no es cierto que la descomposición de un polinomio como producto de polinomios irreducibles sea única. Sin embargo, si podremos probar cierta unicidad y a ello dedicaremos el resto de esta sección.

Definición 2.1.3. Si f y g son polinomios sobre un campo K con mcf igual a 1, se dice que f y g son *coprimos* (ó f es primo a g).

Lema 2.1.4. *Si K es un campo, f un polinomio irreducible sobre K, y h, g polinomios sobre K tal que f divide a gh, entonces f divide a g ó f divide a h.*

Prueba. Supongamos que f no divide a g. Haremos ver que f y g son coprimos. Para esto consideramos d un mcf de f y g, entonces dado que f es irreducible y d divide a f tenemos que $d = kf$ (para algún $k \in K$). En primer caso se tiene que si $\partial d > 0$ entonces f divide a g contrario a lo que supusimos. En segundo caso tenemos que 1 es mcf de f y g. Por lo que f y g son co-primos. Por el teorema 1.5.7, existen polinomios a y b sobre K tal que

$$1 = af + bg.$$

Entonces

$$h = haf + hbg.$$

Ahora f divide a haf y f divide a hbg pues f divide a gh. Por lo que f divide a h. □

Teorema 2.1.5. *Para un campo K, la factorización de los polinomios sobre K en polinomios irreducibles es única salvo constantes y el orden en el cual aparecen escritos.*

Prueba. Supongamos que $f = f_1 \cdots f_r = g_1 \cdots g_s$ donde f es un polinomio sobre K y $f_1, ..., f_r, g_1, ..., g_s$ son polinomios irreducibles sobre K. Si todos los f_i son constantes, entonces $f \in K$, por lo que las g_i también son constantes. En el otro caso podemos asumir que los polinomios f_i son polinomios no constantes (si alguno lo fuera entonces dividimos por los términos constantes). Así pues tenemos que $f_1 \mid g_1 \cdots g_s$. Ahora aplicando una inducción obvia basada en el lema 2.1.4, tenemos que $f_1 \mid g_i$ Para algún i. Además podemos reordenar las $g_i^{'}s$ de tal manera que dicho i sea igual a 1, y entonces $f_1 \mid g_1$. Dado que f_1 y g_1 son irreducibles y f_1 no es constante tenemos que $f_1 = k_1 g_1$ para alguna constante $k_1 \in K$. De manera similar $f_2 = k_2 g_2, ..., f_r = k_r g_r$ donde $k_2, ..., k_r \in K$. Las restantes g_j $(j > r)$ tienen que ser constantes pues si no lo fueran tendríamos que el grado de $f = g_1 \cdots g_s$ sería mayor que el grado de $f = f_1 \cdots f_r$. □

2.2 Criterios de irreducibilidad.

En general es muy difícil el decir si un polinomio dado es o no irreducible. Como ejemplo considérese el polinomio

$$t^{15} + t^{14} + t^{13} + t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$$

(este no es un ejemplo sencillo y habremos de considerar este ejemplo en el capítulo 17.).

En esencia la gran mayoría del trabajo a realizar es el de poder factorizar polinomios como el anterior, aunque en términos generales no siempre podremos hacer esto, pero si daremos algunos criterios para saber cuando un polinomio (sobre algunos campos) es irreducible. Uno de los criterios más importantes es el *criterio de Esestein* su aplicación es de gran importancia para los polinomios sobre $\mathbb{Z}$. Sin embargo la siguiente proposición muestra que si un polinomio es irreducible sobre $\mathbb{Z}$ entonces ese polinomio es irreducible sobre $\mathbb{Q}$. (este resultado fue probado primeramente por *Gauss*).

Proposición 2.2.1. *Si f es un polinomio irreducible sobre $\mathbb{Z}$. Entonces f, considerado como polinomio sobre $\mathbb{Q}$ también es irreducible sobre $\mathbb{Q}$.*

Prueba. Supongamos que f es irreducible sobre $\mathbb{Z}$ pero reducible sobre $\mathbb{Q}$, esto es $f = gh$ donde g, h son polinomios sobre $\mathbb{Q}$, de grado menor que el grado de f. Multiplicando por el producto de los denominadores de los coeficientes de g y h al reescribir a f tenemos que $nf = g'h'$ donde $n \in \mathbb{Z}$ y g', h' son polinomios sobre $\mathbb{Z}$, mostraremos ahora que podemos cancelar los factores primos de n sin que nos salgamos de $\mathbb{Z}[t]$.
Supongamos que p es un factor primo que divide a n, entonces si g' y h' tienen la forma:

$$g' = g_0 + g_1 t + ... + g_r t^r$$

$$h' = h_0 + h_1 t + ... + h_s t^s$$

tenemos que p divide a todos los coeficientes de g' o p divide a todos los coeficientes de h'. Pues si no fuera el caso tenemos que existen valores i, j tal que $p \nmid g_i$ y $p \nmid h_j$. Sin embargo p divide al coeficiente de t^{i+j} en $g'h'$ que son

$$h_0 g_{i+j} + h_1 g_{i+j-1} + ... + h_j g_i + ... + h_{i+j} g_0.$$

y por la elección de i, j el primo p divide a todos los términos de la expresión anterior excepto quizás a $h_j g_i$. Pero p divide a toda la expresión, por lo que p divide a $h_j g_i$. Pero $p \nmid h_j$ y $p \nmid g_i$ lo que produce una contradicción. Por lo que sin perdida de generalidad podemos suponer que p divide a cada coeficiente g_i, entonces $g' = pg''$ donde g'' es un polinomio sobre $\mathbb{Z}$ de el mismo grado que g' (ó g). Sea $n = pn_1$, entonces

$$pn_1 f = pg''h', \text{ esto es, } n_1 f = g''h'$$

Procediendo de esta manera podemos remover todos los factores de n, y tener una ecuación de la forma $f = \widehat{g}\widetilde{h}$ donde $\widehat{g}$, $\widetilde{h}$ son polinomios sobre $\mathbb{Z}$ que además son múltiplos de los polinomios originales g, h. pero esto contradice la irreducibilidad de f sobre $\mathbb{Z}$.
Por lo tanto la suposición de la rediciblilidad de f sobre $\mathbb{Q}$ es falsa y por lo tanto f es irreducible sobre $\mathbb{Q}$. □

Con base al resultado anterior podemos probar el siguiente.

Teorema 2.2.2 (Criterio de *Einseistein*). *Sea $f(t) = a_0 + a_1 t + ... + a_n t^n$ un polinomio sobre $\mathbb{Z}$.*
(1) *Supóngase que existe un número primo q tal que : $q \nmid a_n$*
(2) $q \mid a_i$ $(i = 0, 1, ..., n-1)$
(3) $q^2 \nmid a_0$.
Entonces f es un polinomio irreducible sobre $\mathbb{Q}$.

Prueba. Por la proposición 2.2.1, es suficiente con probar que f es irreducible sobre $\mathbb{Z}$. Para ello supongamos que $f = gh$ con

$$g = b_0 + b_1 t + ... + b_r t^r$$

y

$$h = c_0 + c_1 t + ... + c_s t^s$$

donde h, g son polinomios sobre $\mathbb{Z}$, de grado menor que el grado de f. Entonces $r + s = n$. Ahora $b_0 c_0 = a_0$ que por hipótesis (2) tenemos que $q \mid b_0$ ó $q \mid c_0$. Por (3) de la hipótesis q no puede dividir a ambos, por lo que sin perdida de generalidad podemos asumir que $q \mid b_0$, pero $q \nmid c_0$. Si todos los coeficientes b_i son divisibles por q entonces a_n sería divisible por q, contrario a (1). Si b_i es el primer coeficiente de g que no es divisible por q, entonces $a_i = b_i c_0 + ... + b_0 c_i$ donde $i < n$. esto implica que q divide a c_0, dado que q divide a $a_i, b_0, ..., b_{i-1}$, pero no a b_i. Esto es una contradicción. Por lo tanto f es irreducible. □

Ejemplos

(**1**) Consideremos $f(t) = \frac{2}{9}t^5 + \frac{5}{3}t^4 + t^3 + \frac{1}{3}$ sobre $\mathbb{Q}$. Este polinomio es irreducible si, y sólo si $9f(t) = t^5 + 15t^4 + 9t^3 + 3$ es irreducible sobre $\mathbb{Q}$. El criterio de Einseistein aplicado a $q = 3$ muestra que f es irreducible.

(**2**) Consideremos $f(t) = t^{16} + t^{15} + ... + 1$ sobre $\mathbb{Q}$, (el polinomio que ya consideramos anteriormente). Según el criterio de Einseistein a f no le podemos aplicar dicho criterio, pero notemos que $f(t)$ es irreducible si y sólo si $f(t+1)$ lo es. Expandiendo el comentario anterior tenemos que $f(t)$ es irreducible si y sólo si $f(t+n)$ es irreducible para cada $n \in \mathbb{N}$. Por lo que aplicando el criterio de Einseistein a $q = n = 17$ tenemos que el polinomio f es irreducible sobre $\mathbb{Q}$.

Existe otro muy utilizado criterio de irreducibilidad que es explicado de forma sencilla mediante un ejemplo, la idea es la siguiente:

El Homomorfismo natural de $\mathbb{Z} \to \mathbb{Z}_n$ se extiende de manera obvia a un homomorfismo de $\mathbb{Z}[t] \to \mathbb{Z}_n[t]$. De este modo un polinomio f reducible sobre $\mathbb{Z}$ es un producto gh de polinomios de grado menor; y su factorización se preserva bajo el homomorfismo. Además cuando un polinomio es irreducible sobre $\mathbb{Z}_n$ el polinomio original es también irreducible sobre $\mathbb{Z}$. Dada n que no divida al coeficiente del exponente de grado mayor de f tenemos también que f es irreducible sobre $\mathbb{Z}_n$. Por lo tanto si la imagen de un polinomio sobre $\mathbb{Z}$, es un polinomio irreducible sobre $\mathbb{Z}_n$ entonces el polinomio original es irreducible sobre $\mathbb{Z}$. *Dado que en $\mathbb{Z}_n$ sólo hay un número finito de elementos es fácil de verificar si un polinomio es irreducible, este parece ser un buen procedimiento para saber si un polinomio sobre $\mathbb{Z}$ es irreducible.* Aunque en la practica no es muy sencillo encontrar el valor correcto de n.

(**3**) Consideremos $f(t) = t^4 + 15t^3 + 7$ sobre $\mathbb{Z}$. Considerando el mismo polinomio sobre $\mathbb{Z}_5$ tenemos que $f(t) = t^4 + 2$. Si este polinomio es irreducible sobre $\mathbb{Z}_5$ entonces tiene un factor de grado 1, ó es el producto de dos polinomios de grado 2. En el primer caso tenemos que existe un elemento $x \in \mathbb{Z}_5$ tal que $x^4 + 2 = 0$. Pero no existe uno de tales elementos (esto es fácil de verificar pues sólo tenemos cinco posibilidades para la x). En el segundo caso se tiene que sin perdida de generalidad

$$t^4 + 2 = (t^2 + at + b)(t^2 + ct + d)$$

De este modo tenemos que (haciendo talacha) $a + c = 0$, $ac + b + d = 0$, $b + d = 2$. Por lo tanto $b + d = a^2$, que puede tomar únicamente los valores 0, 1, 4 dado que estos nùmeros son las únicas raíces en $\mathbb{Z}_5$. Por lo que $b(1 - b) = 2$, ó -$b^2 = 2$, ó $b(4 - b) = 2$. Haciendo todas estas posibilidades para los valores $0, 1, 2, 3, 4$ para b, se tiene que ninguna de las ecuaciones anteriores se satisface. Por lo tanto $t^4 + 2$ es irreducible sobre $\mathbb{Z}_5$, de esta manera tenemos que el polinomio original $f(t)$ es irreducible sobre $\mathbb{Z}$. Por lo tanto irreducible sobre $\mathbb{Q}$.

Sin embargo note que si hubiéramos hecho el análisis anterior pero ahora sobre $\mathbb{Z}_3$ tendríamos que $f(t) = t^4 + 1$ que es igual a $(t^2 + t - 1)(t^2 - t - 1)$ por lo que es reducible sobre $\mathbb{Z}_3$. Por lo que al trabajar sobre módulo 3 tenemos que nuestra prueba de irreducibilidad falla.

Este método produce un gran conflicto para saber en cual de los $\mathbb{Z}_n$ debemos de trabajar y no siempre es muy recomendable. Sin embargo tanto el criterio de Einseistein como el método descrito anteriormente son muy útiles para saber cuando es reducible un polinomio. Un problema no resuelto aún es el de encontrar un método para saber si dado un polinomio sobre $\mathbb{Q}$ este polinomio es irreducible.

2.3 Ceros de polinomios.

Iniciaremos este sección con una definición formal.

Definición 2.3.1. Sea R un anillo conmutativo y f un polinomio sobre R. A un elemento $\alpha \in R$ con la propiedad de que $f(\alpha) = 0$ le llamaremos un *cero* de f en R.

Por el momento consideraremos solamente polinomios sobre el campo de los números reales. Así pues podemos dibujar la gráfica $y = f(x)$ (gráfica en el sentido estándar) que en un caso típico se ve como en la siguiente figura.

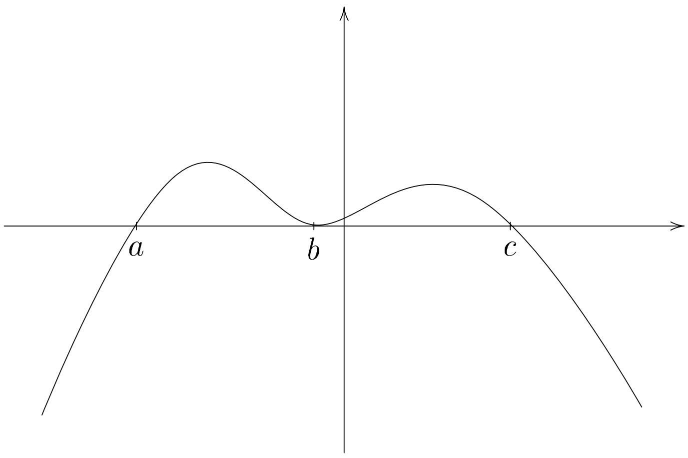

Figura 1.

Los ceros de $f(t)$ son los puntos en los cuales la curva cruza al eje X. Consideremos los tres ceros marcados en a, b, c de la figura, notemos que en b la curva toca al eje x, pero no lo cruza y en el punto c la gráfica es parte de el eje real. Este fenómeno es muy distinguido y se dice que b, c son 'ceros múltiples' de $f(t)$. El cero de b puede ser que sea dos ceros (ó más). Pero, si estos son iguales entonces que queremos decir con dos ceros (ó más). Para clarificar un poco estas ideas tendremos que analizar los *factores lineales* (es decir factores de grado uno) de f.

Lema 2.3.2. *Sea f un polinomio sobre un campo K. Un elemento $\alpha \in K$ es un cero de f si, y sólo si $(t - \alpha) \mid f(t)$.*

Prueba. Si $(t - \alpha) \mid f(t)$ entonces $f(t) = (t - \alpha) g(t)$ para algún polinomio g sobre K, por lo que $f(\alpha) = (\alpha - \alpha) g(\alpha) = 0$.

Reciprocamente, supongamos que $f(\alpha) = 0$. Por el algoritmo de la división existen polinomios q, r sobre K tal que:

$$f(t) = (t-\alpha)\,q(t) + r(t) \text{ donde } \partial r < 1.$$

Por lo que $r(t) = r$ con $r \in K$. Substituyendo α por t encontramos que

$$0 = f(\alpha) = (\alpha - \alpha)\,q(\alpha) + r$$

Por lo que $r = 0$. Por lo tanto $(t-\alpha) \mid f(t)$. □

Buscaremos ahora decir algo acerca de los ceros múltiples.

Definición 2.3.3. Si f es un polinomio sobre un campo K. Un elemento $\alpha \in K$ es un cero *simple* de f si $(t-\alpha) \mid f(t)$ pero $(t-\alpha)^2 \nmid f(t)$.

El elemento α es un cero de *multiplicidad* m si $(t-\alpha)^m \mid f(t)$ pero $(t-\alpha)^{m+1} \nmid f(t)$. A los ceros de multiplicidad mayor que 1 les llamaremos ceros *múltiples.*

Por ejemplo, t^3+3t+2 sobre $\mathbb{Q}$ tiene como ceros a $\alpha = 1, -2$. Su factorización es $(t-1)^2(t+2)$. Por lo tanto -2 es un cero simple, mientras que 1 es un cero de multiplicidad dos.

Cuando $K = \mathbb{R}$ y dibujamos la gráfica de los polinomios como en la figura 1, tenemos que a es un cero simple, b es un cero de multiplicidad par, mientras que c es un cero de multiplicidad mayor que 1. Para otros campos distintos de $\mathbb{R}$ (excepto $\mathbb{Q}$ u otros subcampos de $\mathbb{R}$) una gráfica no puede ser interpretada de la forma en que lo hicimos anteriormente.

Lema 2.3.4. *Sea f un polinomio no cero sobre un campo K, sean $\alpha_1, ..., \alpha_r$ los distintos ceros de f con multiplicidades $m_1, ..., m_r$ respectivamente. Entonces*

$$f(t) = (t-\alpha_1)^{m_1} \cdots (t-\alpha_r)^{m_r}\, g(t) \tag{2.1}$$

donde g no tiene ceros en K.

Recíprocamente, si la ecuación 2.1, se satisface y g no tiene ceros en K, entonces los ceros de f en K son $\alpha_1, ..., \alpha_r$ con multiplicidades $m_1, ..., m_r$ respectivamente.

Prueba. Para un $\alpha \in K$ el polinomio $t-\alpha$ es irreducible. Por lo tanto para distintos $\alpha, \beta \in K$ los polinomios $t-\alpha$ y $t-\beta$ son coprimos. Por la unicidad de la factorización (teorema 2.1.5) la ecuación 2.1, se satisface; y g no puede tener más ceros en K, pues si fuera el caso, entonces f tendría más ceros (ó ceros de multiplicidad mayor) en K.

El inverso se sigue de manera inmediata de la forma en que esta factorizado f. □

De este lema podemos ahora deducir un famoso teorema.

Teorema 2.3.5. *El número de ceros de un polinomio sobre un campo contados con todo y su multiplicidad es menor o igual a el grado de el polinomio.*

Prueba. En la ecuación 2,1, tenemos que $m_1 + ... + m_r < \partial f$. □

2.4 Polinomios simétricos.

Usualmente nos encontraremos en la situación de encontrar los ceros de un polinomio dado. Pero también es posible el trabajar en la dirección contraria, es decir, dados los ceros (con multiplicidad) reconstruir el polinomio. Este es un problema fácil el cual tiene una solución general completa, pero es tal vez debido a su simplicidad que es de considerable importancia teórica.

Consideremos un polinomio de grado n que tiene sus n ceros (contando sus multiplicidades). El es pues el producto de n factores lineales

$$f(t) = k(t-\alpha_1)\cdots(t-\alpha_n)$$

donde $k \in K$ y los α_i son los ceros de f sobre K (no necesariamente distintos). Supóngase que

$$f(t) = a_0 + a_1 t + ... + a_n t^n.$$

Si se expande el primer producto e igualamos sus coeficientes con la segunda expresión tenemos que

$$
\begin{gathered}
a_n = k \\
a_{n-1} = -k\left(\alpha_1 + ... + \alpha_n\right) \\
a_{n-2} = k\left(\alpha_1\alpha_2 + \alpha_1\alpha_3 + ... + \alpha_{n-1}\alpha_n\right) \\
.... \\
a_0 = k\left(-1\right)^n \alpha_1\alpha_2 \cdots \alpha_n.
\end{gathered}
$$

La expresión en $\alpha_1, ..., \alpha_n$ en el lado derecho de las igualdades anteriores, recibe un nombre especial.

Definición 2.4.1. El *r-ésimo polinomio simétrico elemental* denotado por:

$$s_r\left(t_1, ..., t_n\right)$$

en las indeterminadas $t_1, .., t_n$ es la suma de todos los posibles productos distintos tomados r veces, de los elementos $t_1, ..., t_n$.

Abusando un poco de el lenguaje, el resultado de substituir elementos $\alpha_1, ..., \alpha_n$ para $t_1, ..., t_n$ sera llamado el $r-$ésimo polinomio elemental simétrico en $\alpha_1, ..., \alpha_n$. Las ecuaciones pueden ser sumadas y así obtener que

$$a_{n-r} = k\left(-1\right)^r s_r\left(\alpha_1, ..., \alpha_n\right)$$

Este polinomio es simétrico en el sentido de que es el resultado de intercambiar bajo alguna permutación de las indeterminadas t_i. Existen otros polinomios simétricos además de los elementales, por ejemplo, $t_1^2 + ... + t_n^2$; estos polinomios pueden ser expresados en términos de polinomios elementales simétricos. (Una fórmula para $t_1^m + ... + t_n^m$ fue calculada por *Isaac Newton.*)

Teorema 2.4.2. *Sobre un campo K, un polinomio simétrico en $t_1, ..., t_n$ puede ser expresado como un polinomio de menor o igual grado en los polinomios simétricos elementales $s_r\left(t_1, ..., t_n\right)$ donde $(r = 0, ..., n)$.*

Una versión débil de este resultado la probaremos en el corolario 15.1.2. Necesitaremos el teorema anterior para probar que π es trascendental (capítulo 6) el resto de la prueba de el teorema 2.4.2, es por inducción aplicada al corolario 15.1.2 y se encuentra en muchos textos de álgebra (por ejemplo, Salomón [25] pag.57, Van der Warden [5] pag.81). Como un ejemplo de el teorema tenemos la ecuación.

$$t_1^2 + t_2^2 = (t_1 + t_2)^2 - 2t_1t_2 = s_1^2 - 2s_2.$$

2.5 Ejercicios.

2.1 Decir si los siguientes polinomios son o no irreducibles:

(a) $t^4 + 1$, sobre $\mathbb{R}$.

(b) $t^4 + 1$, sobre $\mathbb{Q}$.

(c) $t^7 + 11t^3 - 33t + 22$, sobre $\mathbb{Q}$.

(d) $t^4 + t^3 + t^2 + t + 1$, sobre $\mathbb{Q}$.

(e) $t^3 - 7t^2 + 3t + 3$, sobre $\mathbb{Q}$.

(f) $t^4 + 7$, sobre $\mathbb{Z}_{17}$.

(g) $t^3 - 5$, sobre $\mathbb{Z}_{11}$.

(h) $t^2 - \alpha t + \beta$ sobre el campo de el ejercicio 1.6.

2.2 En cada uno de los casos de el ejercicio 2.1, factorizar el polinomio dado en polinomios irreducibles.

2.3 Si K es un campo con un número infinito de elementos y f, g son polinomios sobre k tal que $f(\alpha) = g(\alpha)$ para todo $\alpha \in K$ pruebe que $f \equiv g$ (f es idénticamente g) ¿ Pueden debilitarse más los hipótesis ?.

2.4 Sea K un campo. Decimos que un polinomio f sobre K es *primo* si siempre que $f \mid gh$ entonces, $f \mid g$ ó $f \mid h$. Muestra que un polinomio $f \neq 0$ es primo si, y sólo si es irreducible (el inverso de este ejercicio en general no es cierto).

2.5 Encuentra los ceros de los siguientes polinomios, primero sobre $\mathbb{Q}$ y luego sobre $\mathbb{R}$ y luego sobre $\mathbb{C}$.

(a) $t^3 + 1$.

(b) $t^3 - 6t^2 + 11t - 6$.

(c) $t^5 + t + 1$.

(d) $t^2 + 1$.

(e) $t^4 + t^3 + t^2 + t + 1$.

(f) $t^4 - 6t^2 + 11$.

2.6 Escribe todos los posibles polinomios de la forma $t^2 + at + b$ sobre $\mathbb{Z}_5$. Encuentra cuales de ellos son irreducibles. En cada caso trabajado notaras que aparece $a^2 - 4b$. ¿ Que es lo que notas ?, ¿ Podrias probarlo ?.

2.7 Da un criterio de irreducibilidad de un polinomio cuadrático (de grado dos) sobre un campo de característica distinta de 2.

2.8 Muestra que para cada número primo p, el campo $\mathbb{Z}_p(t)$ tiene característica p. ¿ Son $\mathbb{Z}_p$ y $\mathbb{Z}_p(t)$ isomorfos ?.

2.9 Expresen se en términos de polinomios simétricos elementales de α, β y γ los siguientes polinomios:

(a) $\alpha^2 + \beta^2 + \gamma^2$.

(b) $\alpha^3 + \beta^3 + \gamma^3$.

(c) $\alpha^2\beta + \alpha^2\gamma + \beta^2\alpha + \beta^2\gamma + \gamma^2\alpha + \gamma^2\beta$.

(d) $\alpha^2\beta^2\gamma^2$.

(e) $(\alpha - \beta)^2 + (\beta - \gamma)^2 + (\gamma - \alpha)^2$.

(f) $(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2$.

(g) $\alpha^2 + \beta\gamma$.

2.10

2.11 Verificar si las siguientes afirmaciones son verdaderas o falsas.

(a) Todo polinomio sobre un campo K tiene un cero en K.

(b) Todo polinomio irreducible sobre $\mathbb{Q}$, es también irreducible sobre $\mathbb{R}$.

(c) Todo polinomio irreducible sobre $\mathbb{Z}$, es también irreducible sobre $\mathbb{Q}$.

(d) Los polinomios lineales son irreducibles.

(e) Todo polinomio simétrico, es elemental.

(f) Dado un polinomio que esta expresado como un arreglo numérico de polinomios elementales simétricos, él mismo es simétrico.

(g) Existe un número infinito de polinomios irreducibles sobre $\mathbb{Q}$.

(h) Los polinomios que son coprimos tienen diferentes grados.

(i) Un polinomio de grado primo, es irreducible.

(j) Un polinomio de grado compuesto, es irreducible.

Capítulo 3

Extensiones de Campos.

La teoría de Galois ha sido expresada originalmente en términos de polinomios sobre el campo de los números complejos. Los métodos usados en la actualidad son una consecuencia de los utilizados en los años 1920 y 1930 (aproximadamente) para generalizar la teoría sobre campos arbitrarios. Desde este punto de vista el principal objetivo de estudio serán siempre los polinomios y así mismo será necesario introducir el concepto de 'extensión de campo' para un polinomio dado. Todo polinomio f sobre un campo K define a su vez a otro campo L que contiene a K (más bien a un campo isomorfo a K). Existe una considerable ventaja al desarrollar teoría de campos desde este punto de vista.

En el capítulo se definirán extensiones de campo en términos de encontrar ceros de polinomios. Mostraremos también ciertas clasificaciones básicas de extensiones y daremos métodos de construcción de dichas clasificaciones.

3.1 Extensiones de campos.

En general, diremos un campo L es una extensión de el campo K, si K es un subcampo de L. Por razones técnicas está definición esta un poco restringida en el sentido de que L puede contener un subcampo isomorfo a K pero no necesariamente igual.

Definición 3.1.1. Una *extensión de campos*, es un monomorfismo $\iota : K \to L$, donde K y L son campos. Diremos que K es el campo *menor* y que L es el campo *mayor*.

Ejemplos.
1. Las inclusiones $i_1 : \mathbb{Q} \to \mathbb{R}$; $i_2 : \mathbb{R} \to \mathbb{C}$; $i_3 : \mathbb{Q} \to \mathbb{C}$ son extensiones de campos.

2. Si K es un campo y $K(t)$ es el campo de las expresiones racionales sobre K, entonces existe un monomorfismo natural $\iota : K \to K(t)$ el cual manda a cada elemento de K en el correspondiente polinomio constante, así pues ι es también una extensión de campos.

3. Sea P el conjunto de números reales de la forma $p + q\sqrt{2}$ donde $p, q \in \mathbb{Q}$, así P es un subcampo de $\mathbb{R}$ donde

$$\left(p + q\sqrt{2}\right)^{-1} = \tfrac{p}{p^2-2q^2} - \tfrac{q}{p^2-2q^2}\sqrt{2}, \text{ (si } p, q \text{ son ambos distintos de cero.)}$$

La inclusión $\iota : \mathbb{Q} \to P$ es una extensión de campos.

Si $\iota : K \to L$ es una extensión de campos, usualmente identificaremos a K con su imagen, (pues ι puede ser considerada como una inclusión). De este modo K puede ser visto como un subcampo de L. Bajo estas circunstancias utilizaremos la notación $(L : K)$ para indicar la extensión y simplemente diremos que L es una extensión de K.

Usualmente haremos la identificación de K con $\iota(K)$ (sólo cuando sea posible). El siguiente concepto es uno de los cuales es trascendental en el álgebra abstracta.

Definición 3.1.2. Sea K un campo y $X \subseteq K$, X no vacío. Entonces el subcampo de K *generado* por X es la intersección de todos los subcampos de K que contienen a X.

El lector podrá convencerse fácilmente que la definición anterior es equivalente a cada una de las siguientes condiciones:

a) El menor subcampo de K que contiene a X.

b) El conjunto de todos los elementos de K que pueden obtenerse de elementos de X mediante una sucesión *finita* de operaciones del campo.

Ejemplo.

En este ejemplo lo que buscamos es encontrar el menor subcampo de $\mathbb{C}$ generado por $\{1, i\}$. (siempre que trabajemos en $\mathbb{C}$ el símbolo i denotara a $\sqrt{-1}$) Llamemosle L a dicho subcampo. Entonces L contiene como subcampo primo a $\mathbb{Q}$ (pues $\mathbb{Q}$ es el subcampo primo de $\mathbb{C}$) dado que L es cerrado bajo las operaciones de campo, entonces L debe contener a todos los elementos de la forma $p+qi$ donde $p, q \in \mathbb{Q}$. Llamemos le M al conjunto de tales elementos.

Afirmamos que M ya es un campo. En efecto claramente M es cerrado bajo productos, sumas y

$$(p+q)^{-1} = \frac{p}{p^2+q^2} - \frac{q}{p^2+q^2}i.$$

por lo que todo elemento distinto de cero de M tiene su inverso multiplicativo en M. Por lo tanto M es un campo que contiene a X. Dado que L es el menor subcampo que contiene a X tenemos que $L \subseteq M$, además por definición de M tenemos que $M \subseteq L$. Por lo tanto $M = L$. Por lo tanto encontramos una descripción de el campo generado por X.

En el caso de una extensión de campos $(L : K)$ resulta muy importante estudiar los campos intermedios entre L y K.

Definición 3.1.3. Sea $(L : K)$ una extensión, $Y \subseteq L$, entonces el *subcampo de L generado por $K \cup Y$* que denotaremos por $K(Y)$ es el campo que se obtiene K adjuntándole Y.

Note que $K(Y)$ es en general mayor que $K \cup Y$. La siguiente notación esta un poco sujeta a algunos abusos de notación. Si Y tiene un único elemento escribiremos $K(y)$en lugar de $K(\{y\})$ y $K(y_1, ..., y_n)$ en lugar de

$K(\{y_1, ..., y_n\})$.

Ejemplos.

1. El subcampo $\mathbb{R}(i)$ de $\mathbb{C}$, contiene todos los elementos de la forma $x + iy$ donde $x, y \in \mathbb{R}$. Por lo que $\mathbb{C} = \mathbb{R}(i)$.

2. Sea K un campo, $K(t)$ el campo de expresiones racionales en t sobre K. La notación anterior puede parecer un tanto ambigua, pues $K(t)$ también denota al subcampo $K \cup \{t\}$. Pero resulta ser que como este subcampo es cerrado bajo las operaciones de campo, entonces debe de contener a todas las expresiones racionales en t, así este subcampo es precisamente el campo de las expresiones racionales. Por lo tanto $K(t)$ resulta ser el mismo campo bajo cualquiera de las dos interpretaciones.

3. El subcampo de $\mathbb{R}$ consistente de todos los elementos de la forma $p + q\sqrt{2}$ donde $p, q \in \mathbb{Q}$. Resulta fácil ver que este campo es $\mathbb{Q}\left(\sqrt{2}\right)$.

4. No siempre es cierto que dado un campo de la forma $K(\alpha)$ este campo consiste de los elementos de la forma $j + k\alpha$ donde $j, k \in K$. Lo que siempre es cierto es que dicho subcampo debe de contener a tales elementos, aunque no necesariamente dichos elementos forman un campo. Por ejemplo, en $(\mathbb{R} : \mathbb{Q})$ consideramos α como la raíz cubica de 2 y consideramos a $\mathbb{Q}(\alpha)$. Este campo es de hecho el conjunto de los elementos de $\mathbb{R}$ de la forma $p + q\alpha + r\alpha^2$, donde $p, q, r \in \mathbb{Q}$. Para probar esto lo que se hace es probar que que el conjunto anterior forma un campo. La única dificultad es encontrar el inverso multiplicativo y dejaremos que el lector se divierta buscando dicho inverso.

3.2 Extensiones simples.

Definiremos primeramente una clase especial de las extensiones de campos.

Definición 3.2.1. Una *extensión simple* es una extensión $(L : K)$ que tiene la propiedad que $L = K(\alpha)$ para alguna $\alpha \in L$.

Los ejemplos discutidos anteriormente son todos de extensiones simples. Un ejemplo de una extensión que no es simple es $(\mathbb{Q}:\mathbb{R})$ (ver ejercicio 3.6). *Nótese que una extensión no necesariamente esta presentada de manera que sea sencillo el saber si es simple.*

Por ejemplo, $\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\right)$ es una extensión simple aunque le estamos adjuntado dos elementos y no uno. para ver esto consideremos el campo $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$.

Este campo contiene al elemento $\left(\sqrt{2}+\sqrt{3}\right)^2 = 5+2\sqrt{6}$, por tanto contiene a $\sqrt{6}$; por lo tanto a $\sqrt{6}\left(\sqrt{2}+\sqrt{3}\right) = 2\sqrt{3}+3\sqrt{2}$; por lo tanto a $\sqrt{2}$ y a $\sqrt{3}$. Por lo tanto $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$. Lo que haremos el resto de el capítulo es clasificar todas las posibles extensiones simples. Primero formularemos el concepto de isomorfismo de extensiones, con ello desarrollaremos las técnicas para la construcción de extensiones simples y finalmente mostraremos (hasta isomorfismo) todas las posibles construcciones de extensiones simples.

Definición 3.2.2. Un *isomorfismo* entre dos extensiones de campo $i: K \to K^*$, $j: L \to L^*$ es una pareja (λ,μ) de isomorfismos de campos $\lambda: K \to L$, $\mu: K^* \to L^*$ tal que para toda $k \in K$ se tiene que $j(\lambda(k)) = \mu(i(k))$. Es decir que el siguiente diagrama *conmuta.*

$$\begin{array}{ccc} K & \xrightarrow{i} & K^* \\ \lambda\big\downarrow & & \big\downarrow\mu \\ L & \xrightarrow[j]{} & L^* \end{array}$$

Es decir las trayectorias que van de K a L^* dan la misma aplicación.

La razón de hacer la definición de esta forma es que la estructura de campo se preserva bajo isomorfismo y los términos 'menor' subcampo y 'mayor' subcampo también se preservan bajo isomorfismo.

Varias identificaciones podemos hacer ahora. Primeramente identificamos a K con $i(K)$ y a L con $j(L)$, entonces i,j son inclusiones y de la condición de conmutatividad resulta ser que tenemos que $\mu\mid_K = \lambda$ donde $\mu\mid_K$ denota la restricción de μ a K. En un futuro identificaremos (sólo cuando sea posible) a K y a L con sus respectivas imágenes, entonces λ será la identidad asì como $\mu \mid_K$sera también la identidad. Aunque en ocasiones (notablemente en el teorema 8.1) habremos de necesitar todas las generalidades de la definición anterior.

3.3 Construcción de extensiones simples.

Primeramente daremos una definición que será de gran utilidad de aquí en adelante.

Definición 3.3.1. Sea $(K(\alpha) : K)$ una extensión simple. Si existe un polinomio no cero p sobre K tal que $p(\alpha) = 0$ entonces diremos que α es un elemento *algebraico* sobre K y diremos que la extensión es una *extensión algebraica simple.* Si no pasa lo anterior diremos que α es *trascendental* sobre K y diremos que la extensión $(K(\alpha) : K)$ es una *extensión trascendental simple.*

El siguiente resultado nos da una forma de construir extensiones trascendentales simples sobre un campo.

Teorema 3.3.2. *El campo de las expresiones racionales $K(t)$ es una extensión trascendental simple de el campo K.*

Prueba. Claramente $K(t)$ es una extensión simple. si p es un polinomio sobre K tal que $p(t) = 0$ entonces $p = 0$ por definición de $K(t)$. □

La construcción de una extensión algebraica simple es mucho más delicada y para ello necesitaremos algunas definiciones previas.

Definición 3.3.3. Un polinomio $f(t) = a_0 + a_1 t + ... + a_n t^n$ sobre un campo K es *mónico* si $a_n = 1$.

Claramente todo polinomio es un múltiplo de algún polinomio monico y dado un polinomio, el polinomio monico asociado a esté polinomio resulta ser único. Más aún el producto de dos polinomios monicos es nuevamente un polinomio monico.

Supongamos ahora que $(K(\alpha) : K)$ es una extensión algebraica simple entonces hay un polinomio p sobre K tal que $p(\alpha) = 0$, además podemos suponer que este polinomio es monico. Así pues tenemos que existe un polinomio de grado menor para el que α es un cero (pues si p, q son dos polinomios distintos de el mismo grado entonces $p(\alpha) - q(\alpha) = 0$. Como p es distinto de q tenemos que existe un polinomio múltiplo de $p - q$ tal que es monico y de grado menor que el grado de p para el cual α también es cero, contrario a la definición de polinomio monico. Por lo tanto existe un único polinomio monico p de menor grado tal que $p(\alpha) = 0$.

Definición 3.3.4. Sea $(L : K)$ una extensión de campos y supongamos que $\alpha \in L$ es algebraico sobre K. Entonces el polinomio *mínimo* de α sobre K es el único polinomio monico m sobre K de menor grado tal que $p(\alpha) = 0$

Por ejemplo, $i \in \mathbb{C}$ es algebraico sobre $\mathbb{R}$. Para ver esto tomamos a $m(t) = t^2+1$, así $m(i) = 0$. Claramente m es monico y los únicos polinomios monicos de grado menor que el grado de m sobre $\mathbb{R}$ son de la forma $t + r$ (con $r \in \mathbb{R}$) ó el polinomio constante 1. Pero i no puede ser cero de ninguno de estos polinomios, pues si esto pasara se tendría que $i \in \mathbb{R}$. Por lo tanto el polinomio mínimo de i sobre $\mathbb{R}$, es $t^2 + 1 = m$.

Lema 3.3.5. *Si α es un elemento algebraico sobre K, entonces el polinomio mínimo de α sobre K es irreducible sobre K. Además este polinomio mínimo divide a cualquier otro polinomio para el cual α sea un cero.*

Prueba. Supongamos que el polinomio mínimo m de α sobre K es reducible sobre K, por lo que $m = fg$ donde f y g son de grado menor que el grado de m. Además podemos asumir que f y g son monicos. Dado que $m(\alpha) = 0$ tenemos que $f(\alpha) g(\alpha) = 0$ lo que implica que $f(\alpha) = 0$ ó $g(\alpha) = 0$. Pero en cualquiera de los dos casos se contradice la definición de m. Por lo tanto m es irreducible sobre K.

Ahora supongamos que p es un polinomio sobre K, tal que $p(\alpha) = 0$. Por el algoritmo de la división existen polinomios q y r sobre K tal que $p = mq + r$ con $\partial r < \partial m$. Entonces $0 = p(\alpha) = 0 + r(\alpha)$. Si $r \neq 0$ entonces un múltiplo constante de r es monico. Lo que contradice la definición de m. Por lo tanto $r = 0$, por lo tanto m divide a p. $\square$

Una observación un poco sofisticada es que utilizando una maquinaria muy poderosa podemos expresar lo dicho en esta sección más sutilmente. El anillo $K[t]$ es un dominio de ideales principales y $\{p : p(\alpha) = 0\}$ es un ideal de $K[t]$, por lo tanto un ideal principal. Y su único generador monico resulta ser precisamente m Para ver detalles de esto consulte *Hartley and Hawkes* [14] pag.59.

Dado un campo K y un polinomio monico irreducible se construye la más pequeña extensión $(K(\alpha) : K)$ tal que α tiene como polinomio mínimo asociado a m sobre K (para probar esto necesitaremos los siguientes dos lemas).

Lema 3.3.6. *Si ψ es un homomorfismo de anillos de un campo K en un anillo R y $\psi \neq 0$ (ψ no es el homomorfismo cero) entonces ψ es un monomorfismo.*

Prueba. El núcleo de ψ ($\mathbf{Nuc}(\psi)$) es un ideal de K. Pero como K es un campo y un campo no tiene ideales propios no triviales tenemos que $\mathbf{Nuc}(\psi) = \{0\}$ ó $\mathbf{Nuc}(\psi) = K$, por hipótesis ψ no es el morfismo cero. Por lo tanto $\mathbf{Nuc}(\psi) = \{0\}$. Por lo tanto ψ es monomorfismo. $\square$

Note que esté lema no es cierto si K es un anillo; el homomorfismo natural $\mathbb{Z} \to \mathbb{Z}_n$ no es cero y no es un monomorfismo.

Lema 3.3.7. *Si m es un polinomio irreducible sobre el campo K, e I es el ideal de $K[t]$ consistente de todos los múltiplos de m, entonces el anillo cociente $K[t] \diagup I$ es un campo.*

Prueba. Sea $I + f$ una clase lateral no cero en $S = K[t] \diagup I$. Dado que m es irreducible y m, f son coprimos, tenemos que por la proposición 1.5.3, existen polinomios a, b sobre K tal que

$$af + bm = 1.$$

Entonces

$$(I + a)(I + f) + (I + b)(I + m) = I + 1.$$

Pero $I + m = I$ es el elemento cero de S, y $I + 1$ es el elemento identidad en S, por lo que

$$(I + a)(I + f) = I + 1$$

y por lo que $I+f$ tiene como inverso a $I+a$. Por lo tanto S es un campo. □

Ahora ya podemos probar el siguiente teorema.

Teorema 3.3.8. *Si K es un campo y m es un polinomio monico irreducible sobre K, entonces existe una extensión $(K(\alpha) : K)$ tal que α tiene como polinomio mínimo a m sobre K.*

Prueba. Existe un monomorfismo natural $i : K \to K[t]$. Sea I el ideal de $K[t]$ consistente de todos los múltiplos de m. Llamemosle $S := K[t] \diagup I$, y sea:

$$\eta : K[t] \longrightarrow S = K[t] \diagup I$$

la proyección natural (que es claramente un homomorfismo) de $K[t] \to S$. Por el lema 3.3.6, la composición de homomorfismos ηi es un monomorfismo.

Ahora identificamos a K con su imagen $\eta(i(K))$. Sea $\alpha = x + I \in S$. Claramente $S = K(\alpha)$. Dado que $m \in I$ tenemos que $m(\alpha) = I$, pero I es el elemento cero de S y dado que m es irreducible y monico tenemos que esté es el polinomio mínimo de α, puesto que si fuera p el polinomio mínimo, entonces por el lema 3.3.5, tendríamos que $p \mid m$. Por lo que$p = m$. Por lo tanto el resultado ha sido probado □

Existe otro camino para está construcción. Que es a cada clase lateral $I + f$ le podemos seleccionar un único polinomio de grado menor que ∂m. La estructura de campo en S induce operaciones en el conjunto de polinomios representantes de cada una de las clases de equivalencia con la suma usual y la multiplicación usual excepto quizás que después de multiplicar es necesario el tomar el residuo de la división por m. Es posible además el *definir* $K(\alpha)$ de está manera.

3.4 Clasificación de extensiones simples.

Habremos de mostrar que el método anterior es suficiente para dar todas las construcciones posibles de las extensiones simples (salvo isomorfismo). De nuevo dar extensiones trascendentales es fácil con el siguiente.

Teorema 3.4.1. *Toda extensión trascendental simple* $(K(\alpha) : K)$ *es isomorfa a la extensión* $(K(t) : K)$ *de expresiones racionales en* t *sobre* K. *El isomorfismo puede ser elegido además que mande a* t *en* α.

Prueba. Definamos la función $\psi : K(t) \to K(\alpha)$ dado por $\psi\left(\frac{f(t)}{g(t)}\right) = \frac{f(\alpha)}{g(\alpha)}$. Como $g \neq 0$, entonces $g(\alpha)$ es distinto de cero (dado que α es trascendental) por lo que la definición anterior tiene sentido. Esta función es claramente un homomorfismo por el lema 3.3.5, este es un monomorfismo. Además este monomorfismo es claramente sobre y por lo tanto un isomorfismo. Más aún $\psi\mid_K$ es el mapeo identidad, por lo tanto ψ define un isomorfismo de extensiones, y es claro que $\psi(t) = \alpha$. □

Lema 3.4.2. *Si* $(K(\alpha) : K)$ *es una extensión algebraica, donde* α *tiene como polinomio mínimo a* m *sobre* K. *Entonces un elemento de* $K(\alpha)$ *tiene una única expresión de la forma* $p(\alpha)$ *donde* p *es un polinomio sobre* K *y* $\partial p < \partial m$.

Prueba. Cada elemento de $K(\alpha)$ puede ser expresado de la forma $f(\alpha)/g(\alpha)$ donde $f, g \in K[t]$ y $g(\alpha) \neq 0$ (dado que el conjunto de tales elementos es un campo que contiene a K y a α y por lo tanto contiene a $K(\alpha)$). Dado que $g(\alpha) \neq 0$, m no divide a g; y dado que m es irreducible se tiene que m y g son coprimos. Por el teorema 1.5.7, existen polinomios a, b sobre K tal que

$ag + bm = 1$. Por lo tanto $a(\alpha) g(\alpha) + b(\alpha) m(\alpha) = 1$, como $m(\alpha) = 0$ entonces se tiene que $a(\alpha) g(\alpha) = 1$ así que $f(\alpha)/g(\alpha) = f(\alpha) a(\alpha) = h(\alpha)$ para algún polinomio h sobre K. Si r es el residuo de dividir h ente m. Entonces $r(\alpha) = h(\alpha)$. Dado que $\partial r < \partial m$, entonces la existencia de tal expresión está probada.

Acontinuación probaremos la unicidad. Supongamos que $f(\alpha) = g(\alpha)$ donde $\partial f, \partial g < \partial m$. Si $e = f - g$ entonces $e(\alpha) = 0$ y $\partial e < \partial m$. Por definición de m tenemos que $e = 0$. Por lo tanto $f = g$. $\square$

Ejemplo. Supongamos que $K = \mathbb{R}$, $m(t) = t^2 + t + 1$. Acordándonos de el lema anterior tenemos que si α tiene polinomio mínimo m sobre K entonces cada elemento de $K(\alpha)$ es un polinomio en α de grado menor que dos. Por ejemplo, consideremos el elemento $(3\alpha^2 + 2)/(\alpha + 4)$. Observemos que:

$$1 = \frac{1}{11}\left(t^2 + t + 1\right) + \frac{t-3}{11}(t+4)$$

Por lo que

$$\frac{1}{(\alpha+4)} = \frac{(\alpha+3)}{11}$$

Así que

$$\begin{aligned}\frac{(3\alpha^2+2)}{(\alpha+4)} &= \frac{1}{11}\left(3\alpha^2+2\right)(\alpha-3)\\ &= \frac{1}{11}\left(3(-\alpha-1)+2\right)(\alpha-3)\\ &= \frac{1}{11}\left(-3\alpha^2+8\alpha+3\right)\\ &= \frac{1}{11}(11\alpha+6)\\ &= \alpha + \frac{6}{11}.\end{aligned}$$

Ahora podemos probar una versión preliminar de el resultado que ente K y m determinan la extensión $K(\alpha)$.

Teorema 3.4.3. *Supongamos que $(K(\alpha) : K)$ y $(K(\beta) : K)$ son extensiones algebraicas simples, tal que α y β tienen el mismo polinomio mínimo m sobre*

K. Entonces las dos extensiones son isomorfas y el isomorfismo de los campos de extensión puede ser tomado de tal manera que transforme a α en β.

Prueba. Por el lema 3.3.7, cada elemento $x \in K(\alpha)$ es expresado de manera única en la forma

$$x = x_0 + x_1\alpha + ... + x_n\alpha^n \ (x_0, ..., x_n \in K)$$

Donde $n = \partial m - 1$. Definimos la transformación:

$$\psi : K(\alpha) \to K(\beta)$$

como

$$\psi(x) = x_0 + x_1\beta + ... + x_n\beta^n$$

Por el lema 3.3.6, ψ es sobre y uno a uno. Claramente

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

Solamente falta probar que

$$\psi(xy) = \psi(x)\psi(y).$$

Sean pues $x, y \in K(\alpha)$. Entonces tenemos que $x = f(\alpha)$, $y = g(\alpha)$, $xy = h(\alpha)$; donde f, g, h son polinomios sobre K de grado menor que el grado de m. Entonces

$$f(\alpha)g(\alpha) - h(\alpha) = xy - xy = 0.$$

Por el lema 3.3.6, m divide a $fg - h$, por lo que existe un polinomio q sobre K tal que $fg = mq + h$. Dado que $\partial h < \partial m$. Entonces se sigue que h es el residuo de dividir fg entre m. Por el mismo razonamiento tenemos que $f(\beta)g(\beta) = h(\beta)$. Por lo que $\psi(xy) = h(\beta) = f(\beta)g(\beta) = \psi(x)\psi(y)$, por lo tanto ψ es un isomorfismo. Dado que ψ es la identidad en K las dos extensiones son isomorfas. Y claramente $\psi(\alpha) = \beta$. $\square$

Para posteriores aplicaciones necesitaremos una versión más fuerte de el teorema anterior, por lo que ahora daremos una definición y terminaremos está sección con dicho resultado.

Definición 3.4.4. Sea $i : K \to L$ un monomorfismo de campos. Entonces existe de manera naturalun monomorfismo

$$\widehat{i} : K\left[t\right] \to L\left[t\right]$$

definido por

$$\widehat{i}\left(k_0 + k_1 t + ... + k_n t^n\right) = i\left(k_0\right) + i\left(k_1\right) t + ... + i\left(k_n\right) t^n.$$

Para $k_0, \ldots, k_n \in K$). Además si i es un isomorfismo entonces también $\widehat{i}$ lo es.

En lo sucesivo utilizaremos la notación de el mapeo i para denotar el mapeo de campos y para denotar el mapeo entere sus anillos de polinomios. Esto no debe causar confusión dado que $\widehat{i}\left(k\right) = i\left(k\right)$ para cualquier $k \in K$

Teorema 3.4.5. *Supóngase que K y L son campos e $i : K \to L$ es un isomorfismo. Sean $K\left(\alpha\right)$ y $L\left(\beta\right)$ extensiones algebraicas simples de K y L respectivamente, tal que α tiene como polinomio mínimo a $m_\alpha\left(t\right)$ sobre K y β tiene como polinomio mínimo a $m_\beta\left(t\right)$ sobre L. Supóngase además que $m_\beta\left(t\right) = i\left(m_\alpha\left(t\right)\right)$. Entonces existe un isomorfismo $j : K\left(\alpha\right) \to L\left(\beta\right)$ tal que $j\mid_K = i$ y $j\left(\alpha\right) = \beta$.*

Prueba. Tenemos el siguiente diagrama.

$$\begin{tikzcd}
K \arrow[r] \arrow[d, "i"'] & K(\alpha) \arrow[d, dashed, "j"] \\
L \arrow[r, "j"'] & L(\beta)
\end{tikzcd}$$

(donde la flecha punteada en el diagrama indica que la función j aún no ha sido definida). Usando la prueba de el teorema 3.4.3, como guia, definimos j como sigue: cada elemento de $K\left(\alpha\right)$ es de la forma $p\left(\alpha\right)$ para algún polinomio p sobre K de grado menor que el grado de m_α. Definimos $j\left(p\left(\alpha\right)\right) = \left(i\left(p\right)\right)\left(\beta\right)$ donde $i\left(p\right)$ está definido como antes. Los demás detalles de la prueba se siguen de el teorema 3.4.3 y se dejan estos al lector. $\square$

La parte interesante de este teorema es que dado un mapeo i este puede ser extendido a una función j entre campos más grandes. Tales funciones dan origen a lo que se conoce de manera general como los *teoremas de extensión* que dicen que bajo ciertas condiciones, relaciones entre subobjetos pueden ser extendidos a relaciones entre objetos y tales teoremas son de gran importancia en las matemáticas.

El teorema 3.3.8, implica que bajo ciertas hipótesis las extensiones $(K(\alpha) : K)$ y $(L(\beta) : L)$ son isomorfas. Esto se sigue de identificar a K con L y a $K(\alpha)$ con $L(\beta)$ vía i y j respectivamente.

Los lemas 3.3.5 y 3.3.6, dan una caracterización completa de las extensiones algebraicas simples en términos de polinomios. A cada extensión le corresponde un polinomio irreducible que también es monico y viceversa dado el campo menor y este polinomio podemos reconstruir la extensión.
Notemos además que la correspondencia no es estrictamente 1-1: es decir extensiones isomorfas pueden dar diferentes polinomios, dado que hay una gran amplitud de la elección de α.

3.5 Ejercicios.

3.1 Pruebe que la relación de isomorfismo entre campos de extensión es una relación de equivalencia.

3.2 Encuentre los subcampos de.

(a) $\{0,1\}$

(b) $\{0\}$

(c) $\{0,1,i\}$

(d) $\{i,\sqrt{2}\}$

(e) $\{\sqrt{2},\sqrt{3}\}$

(f) $\mathbb{R}$

(g) $\mathbb{R} \cup \{i\}$

3.3 Describa los subcampos de $\mathbb{C}$ de la forma

(a) $\mathbb{Q}\left(\sqrt{2}\right)$

(b) $\mathbb{Q}(i)$

(c) $\mathbb{Q}(\alpha)$ donde α es la raíz cubica real de 2

(d) $\mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right)$

(e) $\mathbb{Q}\left(\sqrt{11}\right)$

3.4 Sea $K = \mathbb{Z}_2$. Describa los subcampos de la forma $K(t)$ donde:

(a) $K(t^2)$

(b) $K(t+1)$

(c) $K(t^5)$

(d) $K(t^2+1)$

3.5 De las extensiones definidas en los ejercicios 3.3 y 3.4, ¿ Cuáles de ellas son algebraicas simples ?, ¿ Cuáles de ellas son trascendentales simples ?

3.6 Muestra que $\mathbb{R}$ no son una extensión simple de $\mathbb{Q}$ de la siguiente manera:

(a) $\mathbb{Q}$ es numerable.

(b) Una extensión simple de un campo numerable es numerable.

(c) $\mathbb{R}$ no es numerable.

3.7 Pruebe una versión trascendental de el teorema 3.4.5, modificando los teoremas 3.4.1 y 3.3.2.

3.8 Encuentra el polinomio mínimo sobre los campos menores de los siguientes elementos en las siguientes extensiones:

(a) i en $(\mathbb{C} : \mathbb{Q})$

(b) i en $(\mathbb{C} : \mathbb{R})$

(c) $\sqrt{2}$ en $(\mathbb{R} : \mathbb{Q})$

(d) $\left(\sqrt{5}+1\right)/2$ en $(\mathbb{C} : \mathbb{Q})$

(e) $\left(i\sqrt{3}-1\right)/2$ en $(\mathbb{C} : \mathbb{Q})$

(f) α en $(K : P)$ donde K es el campo de el ejercicio 1.6 y P es su subcampo primo.

(g) α en $(\mathbb{Z}_3(t)(\alpha) : \mathbb{Z}_3(t))$ donde t es una indeterminada y $\alpha^2 = t+1$.

3.9 Muestra que si α tiene como polinomio mínimo a t^2-2 sobre $\mathbb{Q}$ y β tiene como polinomio mínimo a t^2-4t+2 sobre $\mathbb{Q}$, entonces las extensiones $(\mathbb{Q}(\alpha) : \mathbb{Q})$ y $(\mathbb{Q}(\beta) : \mathbb{Q})$ son isomorfas.

3.10 ¿ Para cuales de los siguientes valores de $m(t)$ no existen extensiones $K(\alpha)$ de K para el cual α tiene polinomio mínimo $m(t)$?

(a) $m(t) = t^2-4$, $K = \mathbb{R}$

(b) $m(t) = t^2+1$, $K = \mathbb{Z}_3$

(c) $m(t) = t^2+1$, $K = \mathbb{Z}_5$

(d) $m(t) = t^7-3t^6+4t^3-t-1$, $K = \mathbb{R}$.

3.11 Sea K un campo de característica distinta de 2 y $m(t)$ un polinomio cuadrático sobre K (i.e. $\partial m = 2$). Muestra que si $m(t)$ tiene ambos ceros en un campo de extensión $K(\alpha)$ de K donde $\alpha^2 = k \in K$. Entonces las 'raíces cuadradas' $\sqrt{k}$ solucionan todas las ecuaciones cuadráticas sobre K.

3.12 Muestra que para un campo de característica dos existen ecuaciones cuadráticas que no son solubles vía adjuntando raíces cuadradas de elementos en el campo. (Sugerencia: Hacer el ejercicio primero sobre $\mathbb{Z}_2$).

3.13 Muestra que se pueden resolver ecuaciones cuadráticas sobre un campo de característica dos, si podemos adjuntarle a el campo de extensión elementos ${}^*\sqrt{k}$ definidos como la solución de la ecuación

$$\left({}^*\sqrt{k}\right)^2 +^* \sqrt{k} = k.$$

3.14 Muestra que los ceros de el polinomio $t^2 + t + k = 0$ en el campo de el ejercicio anterior son ${}^*\sqrt{k}$ y $1 +^* \sqrt{k}$.

3.15 Sea $K = \mathbb{Z}_3$. Encuentra todos los elementos irreducibles que a su vez son cuadráticos sobre K, y construye todos las posibles extensiones de K por un elemento con polinomio mínimo cuadrático.

3.16 Construyanse extensiones $(\mathbb{Q}(\alpha) : \mathbb{Q})$ donde α tiene como polinomio mínimo sobre $\mathbb{Q}$:

(a) $t^2 - 5$

(b) $t^4 + t^3 + t^2 + t + 1$

(c) $t^3 + 2$.

3.17. Encuentra un campo con ocho elementos.

3.18. Es $\left(\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right) : \mathbb{Q}\right)$ una extensión simple.

3.19 Supóngase $m(t)$ irreducible sobre K, y α tiene polinomio mínimo $m(t)$ sobre K. ¿ Será cierto que $m(t)$ se puede factorizar sobre $K(\alpha)$ en polinomios lineales (de grado 1)? (Sugerencia: pruebe con $K = \mathbb{Q}$, $\alpha =$ la raíz real cubica de 2).

3.20 Decir si las siguiente afirmaciones son verdaderas o falsas.

(a) Todo campo tiene extensiones no triviales.

(b) Todo campo tiene extensiones algebraicas no triviales.

(c) Toda extensión simple es algebraica.

(d) Toda extensión es simple.

(e) Todas las extensiones algebraicas simples son isomorfas.

(f) Todas las extensiones trascendentales simples sobre un campo dado son isomorfas.

(g) Todo polinomio mínimo es monico.

(h) Los polinomios monicos son siempre irreducibles.

(i) Todo polinomio es un múltiplo constante de un polinomio irreducible.

Capítulo 4

El grado de una extensión.

Una técnica que ha sido muy utilizada en las matemáticas es el de asociarle a una estructura dada otra estructura y con ello poder obtener información de una a través de la otra y viceversa. Este método recién aparicio en topología algebraica y con ello se tuvo qu formalizarlo.

En este capítulo explotaremos la técnica de asociarle a una extensión de campo un espacio vectorial. Esto hace que dispongamos de una herramienta muy utilizada en la actualidad, como lo es el álgebra lineal. La herramienta que aquí desarrollaremos ha resuelto problemas notables los cuales tenían más de 2000 años sin ser resueltos. Habremos de discutir algunos de estos problemas en el siguiente capítulo y en este capítulo desarrollaremos la teoría a utilizar.

No es difícil definir la estructura de espacio vectorial en una extensión de campos.

4.1 El grado de una extensión.

Iniciaremos esta sección dando un resultado que nos permitirá más adelante dar la definición de lo que entenderemos por el grado de una extensión.

Teorema 4.1.1. *Si* $(L : K)$ *es una extensión de campos entonces las opera-*

ciones

$$(\lambda, \mu) \to \lambda\mu \qquad\qquad (\lambda \in K,\ \mu \in L)$$

y

$$(u, v) \to uv \qquad\qquad (u, v \in L)$$

definen en L una estructura de espacio vectorial sobre K.

Prueba. Cada axioma de espacio vectorial es un axioma de campo ó es la restricción de un axioma de campo. □

Las operaciones que hacen de $(L : K)$ un espacio vectorial sobre K nos da un ejemplo, de lo que se ha dado por llamar *el funtor que olvida* que es simplemente el no considerar alguna de las estructuras que se tengan.

Un espacio vectorial sobre un campo esta únicamente determinado (hasta isomorfismo) por su dimensión. La siguiente definición es la terminología tradicional en el contexto de extensiones de campo.

Definición 4.1.2. El *grado* $(L : K)$ de una extensión de campos que denotaremos como: $[L : K]$, es la dimensión de L como K espacio vectorial.

Ejemplos.

1. Los números complejos $\mathbb{C}$ son de dimensión dos sobre los números reales $\mathbb{R}$, $\{1, i\}$ forman una base. Por lo tanto $[\mathbb{C} : \mathbb{R}] = 2$.

2. $[\mathbb{C}(t) : \mathbb{C}]$ es infinito, dado que los elementos $1, t, t^2, \ldots$son linealmente independientes sobre $\mathbb{C}$.

3. Sea K el campo con cuatro elementos de el ejercicio 1.6 y sea P el subcampo primo, que es isomorfo a $\mathbb{Z}_2$. Los elementos $\{1, \alpha\}$ forman una base para K sobre P. Por lo que $[K : P] = 2$.

Es claro que extensiones isomorfas tienen el mismo grado. El siguiente teorema nos permite calcular el grado de algunas extensiones en casos muy particulares.

Teorema 4.1.3. *Si L, M, K son campos y $K \leq M \leq N$ entonces*

$$[M:K] = [M:L]\,[L:K]$$

Cuando en la fórmula haya una extensión que tenga grado infinito, no necesitamos extenderla es decir, si

$$[M:L] = \infty$$

ó

$$[L:K] = \infty$$

entonces

$$[M:K] = \infty$$

y si

$$[M:K] = \infty$$

entonces

$$[M:L] = \infty$$

ó

$$[L:K] = \infty.$$

Prueba. Sea $(x_i)_{i\in I}$ una base para L como espacio vectorial sobre K, y sea $(y_j)_{j\in J}$ una base para M como espacio vectorial sobre L. Para toda $i \in I$, $j \in J$ se tiene que $x_i \in L$, $y_j \in M$. Habremos de mostrar que $(x_i y_j)_{i\in I,\, j\in J}$ es una base de M como K espacio vectorial. (donde $x_i y_j$ es el producto en el campo M) Y dado que que la dimensión es el producto de los cardinales de las bases respectivas, entonces el resultado se sigue.

Así pues primeramente mostraremos la independencia lineal. supongamos que alguna combinación lineal finita de las $(x_i y_j)_{i\in I,\, j\in J}$ es cero, i.e.

$$\sum_{i,j} k_{ij} x_i y_j = 0 \qquad\qquad (k_{ij} \in K)$$

Podemos reordenar la suma anterior como sigue

$$\sum_j \left(\sum_i k_{ij} x_i \right) y_j = 0$$

Dado que los coeficientes $\sum\limits_i k_{ij} x_i$ pertenecen al L y los y_j son linealmente independientes sobre L se tiene que

$$\sum_i k_{ij} x_i = 0.$$

Repitiendo este argumento pero ahora pare L tenemos que $k_{ij} = 0$ para todo i, j. Por lo tanto los elementos $x_i y_j$ son linealmente independientes sobre K.

Finalmente se mostrara que los $x_i y_j$ generan a M sobre K. Sea pues $x \in M$ podemos escribir x como

$$x = \sum_j \lambda_j y_j$$

donde $\lambda_j \in L$ y puesto que los y_j generan a M sobre L. De manera similar para $j \in J$ tenemos que

$$\lambda_j = \sum_i \lambda_{ij} x_i \qquad \textit{con} \quad \lambda_{ij} \in K.$$

Y finalmente uniendo las piezas tenemos que

$$x = \sum_{i,j} \lambda_{ij} x_i y_j.$$

Por lo tanto $(x_i y_j)_{i \in I,\, j \in J}$ generan a M sobre K. $\square$

Ejemplo.

Supongamos que queremos encontrar $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right]$. Es fácil ver que $\left\{1, \sqrt{2}\right\}$ es una base para $\mathbb{Q}\left(\sqrt{2}\right)$ sobre $\mathbb{Q}$. Y también es fácil ver que $\left\{1, \sqrt{3}\right\}$

es una base de $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ sobre $\mathbb{Q}\left(\sqrt{2}\right)$. Por lo que

$$\begin{aligned}\left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\right] &=\\ \left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right] &=\\ 2\cdot 2 &=\\ 4\end{aligned}$$

El teorema anterior también nos permite dar una base, digamos en este caso $\beta=\left\{1,\sqrt{2},\sqrt{3},\sqrt{6}\right\}$. En el caso de las extensiones simples podemos encontrar fácilmente su grado.

Proposición 4.1.4. *Sea $(K(\alpha):K)$ una extensión simple. Si la extensión es trascendental, entonces $[K(\alpha):K]=\infty$.*

Si es algebraico entonces $[K(\alpha):K]=\partial m$ donde m es el polinomio mínimo de α sobre K.

Prueba. Para el caso en que la extensión es trascendental es suficiente con notar que los elementos $1,\alpha,\alpha^2,\dots$ son linealmente independientes sobre K.

Para el caso algebraico exhibiremos una base. Si $\partial m=n$, consideremos los elementos $1,\alpha,\dots,\alpha^{n-1}$. Por el lema 3.4.2, estos elementos generan a $K(\alpha)$ sobre K y por la condición de unicidad también del lema 3.4.2, ellos son linealmente independientes. Por lo tanto ellos forman una base para $K(\alpha)$ sobre K. Por lo tanto $[K(\alpha):K]=n=\partial m$. □

El resultado anterior lo podemos ilustrar mediante un ejemplo muy sencillo, tomemos $\mathbb{C}=\mathbb{R}(i)$ donde i tiene como polinomio mínimo t^2-1 de grado dos, por la proposición anterior tenemos que $[\mathbb{C}:\mathbb{R}]=2$, como ya habiamos visto en el primer ejemplo a la definición 4.1.2.

Definición 4.1.5. a) Una *extensión finita* es una extensión cuyo grado es finito. La proposición 4.1.4, implica que una extensión algebraica simple es finita. Nota; El recíproco de esta afirmación no es cierto.

b) Una extensión $(L : K)$ es *algebraica* si cada elemento de L es un elemento algebraico sobre K.

Las extensiones algebraicas no necesariamente son finitas, más adelante veremos que por ejemplo, los números algebraicos no forman una extensión finita, aunque lo que si es cierto es que cada extensión finita es algebraica.

Lema 4.1.6. *$(L : K)$ es una extensión finita si, y sólo si L es algebraico sobre K y existe un número finito de elementos $\alpha_1, ..., \alpha_s \in L$ tal que $L = K(\alpha_1, ...\alpha_s)$.*

Prueba. Una simple inducción usando el teorema 4.1.3 y la proposición 4.1.4 muestran que una extensión algebraica $(K(\alpha_1, \ldots, \alpha_s) : K)$ es finita.

Recíprocamente sea $(L : K)$ una extensión finita. Entonces existe una base $\{\alpha_1, ..., \alpha_s\}$ para L sobre K, donde $L = K(\alpha_1, ..., \alpha_s)$. Por lo cual sólo falta mostrar que $(L : K)$ es algebraica. Sea x un elemento de L y sea $n = [L : K]$. El conjunto $\{1, x, ..., x^n\}$ contiene $n - 1$ elementos, por lo que este conjunto es linealmente independiente sobre K. Por lo tanto existe una combinación lineal de el conjunto $\{1, x, ..., x^n\}$ igual a cero sin que todos los coeficientes sean cero, es decir

$$k_0 + k_1 x + ... + k_n x^n = 0$$

Para algunos $k_0, ..., k_n \in K$. Por lo tanto x es algebraico sobre K. □

4.2 Números algebraicos.

Si $\mathcal{A}$ denota al conjunto de todos los números complejos que son algebraicos sobre $\mathbb{Q}$. Los elementos de $\mathcal{A}$ son llamados números algebraicos. En seguida haremos uso de las técnicas desarrolladas en este capítulo para demostrar que $\mathcal{A}$ es un campo.

Por el lema 4.1.6, un elemento $\alpha \in \mathbb{C}$, está en$\mathcal{A}$ si, y sólo si $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$. Sean $\alpha, \beta \in \mathcal{A}$. Entonces tenemos que

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty.$$

Por lo que
$$[\mathbb{Q}(\alpha+\beta):\mathbb{Q}]<\infty$$
también
$$[\mathbb{Q}(-\alpha):\mathbb{Q}]<\infty$$
y
$$[\mathbb{Q}(\alpha\beta):\mathbb{Q}]<\infty$$
y si $\alpha \neq 0$ entonces
$$\left[\mathbb{Q}\left(\alpha^{-1}\right):\mathbb{Q}\right]<\infty.$$
Por lo tanto $\alpha+\beta$, -α, $\alpha\beta$, α^{-1} pertenecen a $\mathcal{A}$, por lo tanto $\mathcal{A}$ es un campo.

Notemos que $\mathcal{A}$ es obviamente una extensión algebraica de $\mathbb{Q}$. Pero podemos probar (ver ejercicio 4.8) que $\mathcal{A}$ tiene grado infinito sobre $\mathbb{Q}$. Por lo tanto no toda extensión algebraica es finita.

4.3 Ejercicios.

4.1 Encuentra los grados de las siguientes extensiones:

a) $(\mathbb{C}:\mathbb{Q})$

b) $(\mathbb{Z}_5(t):\mathbb{Z}_5)$

c) $\left(\mathbb{R}\left(\sqrt{5}\right):\mathbb{R}\right)$

d) $(\mathbb{Q}(\alpha):\mathbb{Q})$ donde α es la raíz real cubica de 2

e) $\left(\mathbb{Q}\left(\sqrt{3},\sqrt{5},\sqrt{11}\right):\mathbb{Q}\right)$

f) $\left(\mathbb{Q}\left(\sqrt{6}\right):\mathbb{Q}\right)$

g) $(\mathbb{Q}(\alpha):\mathbb{Q})$ donde $\alpha^7=3$.

4.2 Muestra que todo elemento de $\mathbb{Q}\left(\sqrt{5},\sqrt{7}\right)$ puede ser expresado de manera única en la forma
$$p+q\sqrt{5}+r\sqrt{7}+s\sqrt{35}$$
donde $p,q,r,s\in\mathbb{Q}$. Calcula explícitamente el inverso de tales elementos.

4.3 Si $[L:K]$ es un número primo muestra que los únicos campos M tal que $K \subseteq M \subseteq L$ son solamente L y K.

4.4 Si $[L:K]=1$ muestra que $L=K$.

4.5 Si $K=K_0 \subseteq K_1 \subseteq ... \subseteq K_r = L$ son campos, muestra que

$$[L:K] = [K_r : K_{r-1}] \cdots [K_2 : K_1] [K_1 : K_0] .$$

4.6 Pruebe que $[L:K]$ es finita si, y sólo si $L = K(\alpha_1, ..., \alpha_r)$ donde r es finito y cada α_i es algebraico sobre K.

4.7 De el hecho que $\mathbb{R}$ es un espacio vectorial sobre $\mathbb{Q}$ muestre que hay funciones $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x+y) = f(x) + f(y)$ para todo $x, y \in \mathbb{R}$, pero tal que $f(x)$ no sea un múltiplo constante de x. ¿ Si tales funciones existen serán estas, funciones continuas?.

4.8 Sea $\mathcal{A}$ el campo de los números algebraicos. Pruebe que $[\mathcal{A} : \mathbb{Q}] = \infty$ (use el criterio de einseistein para mostrar que existen polinomios irreducibles sobre $\mathbb{Q}$ de grado arbitrario).

4.9 Asumiendo que cada polinomio sobre $\mathbb{C}$ tiene por lo menos un cero en $\mathbb{C}$, pruebe que cada polinomio en $\mathcal{A}$ tiene por lo menos un cero en $\mathcal{A}$.

4.10 Utilizando el ejercicio anterior muestra que cada extensión algebraica en $\mathcal{A}$ es justamente $\mathcal{A}$.

4.11 Sea $(L:K)$ una extensión. Muestra que la multiplicación por un elemento fijo de L es una transformación lineal de L en si mismo considerando a L como K espacio vectorial ¿Cuándo esta transformación es no singular?.

4.12 Si $(L:K)$ es una extensión finita y si p es un polinomio irreducible sobre K. Muestra que si ∂p y $[L:K]$ son primos relativos entonces p no tiene ceros en L.

4.13 ¿Si $(L:K)$ es algebraica y $(M:L)$ es algebraica entonces $(M:K)$ algebraica?, note que no se puede asumir que las extensiones sean finitas.

4.14 Pruebe que $\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right)=\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$ ¿se puede generalizar este resultado.?

4.15 Pruebe que las raíces cuadradas de todos los números primos forman un conjunto linealmente independiente sobre $\mathbb{Q}$.

4.16 Encuentra una base para $\mathbb{Q}\left(\sqrt{1+\sqrt{3}}\right)$ sobre $\mathbb{Q}$ y encuentra el grado de $\left(\mathbb{Q}\sqrt{1+\sqrt{3}}:\mathbb{Q}\right)$.

4.17 Si $[L:K]$ es un número primo muestra que L es una extensión simple de K.

4.18 Di si las siguientes afirmaciones son verdaderas o falsas, argumenta tu respuesta.

a) Extensiones de el mismo grado son isomorfas.

b) Extensiones isomorfas tienen el mismo grado.

c) Toda extensión algebraica es finita.

d) Toda extensión trascendental es infinita.

e) Todo elemento de $\mathbb{C}$ es algebraico sobre $\mathbb{R}$.

f) Toda extensión de $\mathbb{R}$ es finita.

g) Toda extensión algebraica de $\mathbb{Q}$ es finita.

h) $\mathcal{A}$ es el mayor subcampo de $\mathbb{C}$ que es algebraico sobre $\mathbb{Q}$.

i) Todo espacio vectorial es isomorfo a el espacio vectorial correspondiente a una extensión de campo.

j) Toda extensión de un campo finito es finita.

Capítulo 5

Construcciones con regla y compás.

Acordándonos de como en la antigua Grecia consideraban como figuras perfectas, aquellas formadas solamente por rectas y círculos.

Los Griegos construlleron instrumentos para construir dichas figuras y a tales construcciones son a las que en la actualidad se les conoce con el nombre de construcciones con regla y compás.

Con estos instrumentos es posible mejorar algunas construcciones. Las lineas pueden ser divididas en un número desegmentos iguales, los ángulos pueden bisectarse, las lineas paralelas pueden ser dibujadas. Así como dado un polígono es posible construir un cuadrado que tenga la misma área que el polígono. Sin embargo existen muchos conceptos geométricos que intuitivamente su construcción con regla y compás parece ser imposible.

Existen tres famosos problemas que los Griegos no pudieron resolver, que son: la duplicación de el cubo, la trisección de un ángulo y la cuadratura de el circulo. Es decir, dado un cubo construir un cubo que tenga área el doble que el original, dado un ángulo dividirlo en tres ángulos iguales y dado un circulo construir un cuadrado que tenga área igual al área de el circulo.

No es una sorpresa que los Griegos encontraran estas construcciones muy difíciles, (pues resulta que estas construcciones son imposibles) pero los Griegos no tenían métodos para probar está imposibilidad y ellos suponían que la solución de tales construcciones si existía. En consecuencia ellos expresaron una notable ingenuidad en la búsqueda de tales soluciones.

Arquímedes trabajo en el problema de la cuadratura de el circulo de manera un tanto ingenua, probando un resultado que en la actualidad podemos escribir como $3\frac{10}{71} < \pi < 3\frac{1}{7}$.

Con la maquinaria con que ahora disponemos nos será relativamente simple el dar una solución completa a los tres problemas mencionados anteriormente. Usaremos coordenadas geométricas para expresar dichos problemas en términos algebraicos y aplicaremos la teoría de extensión de campos para resolver los problemas que ya están expresados de manera algebraica.

5.1 Formulación algebraica.

El primer paso sera formalizar la idea intuitiva de construcciones con regla y compás. Asumiremos que un conjunto P_0 de puntos en el plano euclidiano ($\mathbb{R}^2$) está dado y consideraremos las siguientes operaciones.

Operación 1. (Regla) Dados dos puntos en P_0 podemos dibujar la recta que los une.

Operación 2. (Compás) Dibujar un circulo, cuyo centro es un punto en P_0 y cuyo radio es igual a la distancia entre algún par de puntos de P_0.

(Los Griegos tenían una restricción a la operación dos, decían: Dibujar un circulo centrado en algún punto de P_0, y que pase por otro punto de P_0).

Definición 5.1.1. Los puntos de intersección de dos lineas distintas, rectas ó círculos que se pueden dibujar usando la operación 1 ó 2, se dice que son *construibles en un paso* en P_0.

Un punto $r \in \mathbb{R}^2$ es *construible* en P_0 si existe una sucesión finita $r_1, ..., r_n$ de puntos en $\mathbb{R}^2$ tal que para cada $i = 1, ..., n$ el punto r_i es construible en un paso en el conjunto $P_0 \cup \{r_1, \ldots, r_{i-1}\}$.

Ejemplo. Habremos de construir el punto medio de una linea dada. Supongamos pues que nos dan dos puntos $p_1, p_2 \in P_0$.

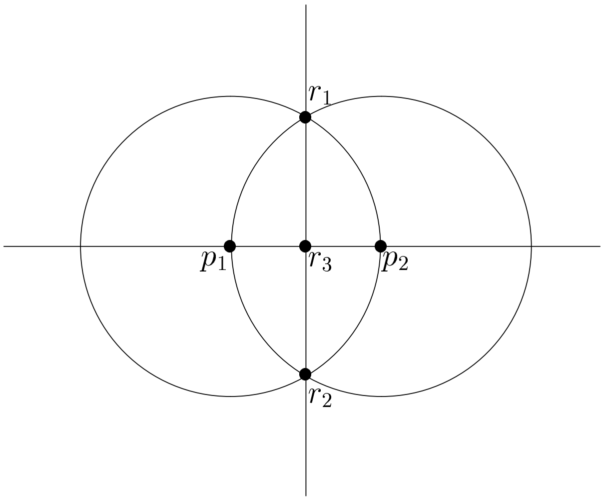

Figura 2.

Sea $P_0 = \{p_1, p_2\}$

1) Dibuja la linea p_1p_2 (operación 1).

2) Dibuja el circulo con centro en p_1 y radio p_1p_2 (operación 2).

3) Dibuja el circulo con centro en p_2 y radio p_1p_2 (operación 2).

4) Sean r_1 y r_2 los puntos de intersección de estos dos círculos.

5) Dibuja la linea r_1r_2 (operación 1).

6) Sea r_3 la intersección de las lineas p_1p_2 y r_1r_2.

Entonces la sucesión r_1, r_2, r_3 define una construcción de el punto medio de la linea p_1p_2.

Dado que una linea está determinada por dos puntos que están en la misma y una circunferencia por su centro y un punto en la circunferencia, entonces todas las construcciones geométricas tradicionales de la geometría euclidiana las podemos hacer con definiciones formales.

La teoría de campos ingresa de una manera muy natural, pues a cada etapa de una construcción le asociaremos el subcampo de $\mathbb{R}$ generado por las coordenadas de el punto construido. Por lo que si K_0 es el subcampo de $\mathbb{R}$ generado por las $x\acute{}s$ y las $y\acute{}s$ de las coordenadas de los puntos de P_0. Ahora si r_i tiene coordenadas (x_i, y_i) entonces inductivamente definimos K_i como el subcampo obtenido de K_{i-1} adjuntándole x_i, y_i esto es $K_i = K_{i-1}(x_i, y_i)$. Claramente obtenemos la sucesión de campos $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \mathbb{R}$.

El siguiente teorema formaliza algebraicamente lo mencionado anteriormente.

Lema 5.1.2. *Con la notación anterior x_i, y_i son ceros en K_i de polinomios cuadráticos sobre K_{i-1}.*

Prueba. Hay tres casos a considerar, linea intersección linea, linea intersección circulo y circulo intersección circulo. Cada caso se trabaja de manera similar y como ejemplo haremos el caso de linea intersección circulo.

Sean A, B, C puntos cuyas coordenadas son $(p, q), (r, s), (t, u)$ que pertenecen a K_{i-1}. Dibujamos la linea AB y el circulo con centro en C y radio w donde $w^2 \in K_{i-1}$ como en la figura 3.

(Note que w^2 esta en K_{i-1} dado que w es la distancia entre dos puntos cuyas coordenadas están en K_{i-1}. Usando pitagoras).

La ecuación de la linea AB es

$$\frac{x-p}{r-p} = \frac{y-q}{s-q} \tag{5.1}$$

y la ecuación de el circulo es

$$(x-t)^2 + (y-u)^2 = w^2 \tag{5.2}$$

resolviendo (5.1) y (5.2) tenemos que $(x-t)^2 + \left(\frac{s-q}{r-p}(x-p) + q - u\right)^2 = w^2$.

Por lo tanto la coordenada en el eje $\overline{X}$ de los puntos de intersección X, Y son ceros de los polinomios cuadráticos sobre K_{i-1}. Lo mismo se satisface para las coordenadas en el eje $\overline{Y}$.

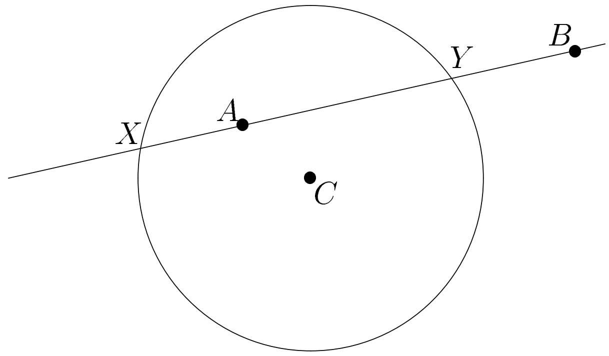

Figura 3.

Por lo que el resultado ha sido probado. □

Podemos ahora deducir una consecuencia algebraica de la existencia de una construcción para un punto dado.

Teorema 5.1.3. *Si $r = (x, y)$ es construible de el subconjunto de P_0 de $\mathbb{R}^2$ y K_0 es el subcampo generado por las coordenadas de los puntos en P_0, entonces los grados $[K_0(x) : K_0]$ y $[K_0(y) : K_0]$ son potencias de dos.*

Prueba. Utilizaremos la notación usada en las pruebas de el lema 5.1.2 y la proposición 4.1.4, así pues tenemos que $[K_0(x_i) : K_0] = 1$ ó 2 (El valor 2 ocurre cuando el polinomio cuadrático sobre K_{i-1} del cual x_i es cero, es irreducible; en el otro caso toma el valor de 1). Similarmente $[K_{i-1}(x_i) : K_{i-1}] = 1$ ó 2. Así pues $[K_{i-1}(x_i, y_i) : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)]\,[K_{i-1}(x_i) : K_{i-1}] = 1, 2$ ó 4. El valor uno nunca se toma, (se deja este detalle de la prueba a el lector).

Por lo tanto $[K_i : K_{i-1}]$ es una potencia de 2. Por inducción (ver ejercicio 4.5) se tiene que $[K_n : K_0]$ es una potencia de 2. Por lo tanto como

$$[K_n : K_0(x)]\,[K_0(x) : K_0] = [K_n : K_0]$$

se sigue que $[K_0(x) : K_0]$ es una potencia de 2. Similarmente $[K_0(y) : K_0]$ es también una potencia de 2. $\square$

5.2 Pruebas de imposibilidad.

Ahora haremos uso de la teoría desarrollada para probar que no existen construcciones con regla y compás para los problemas anteriores. (los mencionados en la introducción de el capítulo) Para los expertos dibujantes se enfatiza que la discusión de estos problemas es para construcciones exactas. Pues existen muchas aproximaciones para la construcción de la trisección de el ángulo, pero ningún método exacto.

Teorema 5.2.1. *El cubo no puede ser duplicado usando regla y compás para su construcción.*

Prueba. Consideremos un cubo dado, por lo que todos los lados del cubo están dados, los cuales además podemos asumir que son de longitud 1 y uno de los lados está sobre el eje $\overline{X}$. Así podemos asumir que $P_0 = \{(0,0), (1,0)\}$ por lo que $K_0 = \mathbb{Q}$. Si se puede duplicar dicho cubo entonces podemos construir el punto $(\alpha, 0)$ donde $\alpha^3 = 2$. Por el teorema 5.1.3, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de dos. Pero α es un cero de el polinomio $t^3 - 2$ sobre $\mathbb{Q}$ el cual es irreducible sobre $\mathbb{Q}$ (por el criterio de Einseinstein). Por lo tanto $t^3 - 2$ es el polinomio mínimo de α sobre $\mathbb{Q}$ y por la proposición 4.1.4, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Lo cual es una contradicción. Así pues el cubo no puede ser duplicado.

$\square$

Teorema 5.2.2. *El ángulo $\frac{\pi}{3}$ no puede ser trisecado usando construcciones con regla y compás.*

Prueba. Para construir un ángulo trisecado de $\frac{\pi}{3}$ es equivalente construir un punto $(\alpha, 0)$ dados $(0,0)$ y $(1,0)$ donde $\alpha = \cos\left(\frac{\pi}{3}\right)$ (ver figura 4).

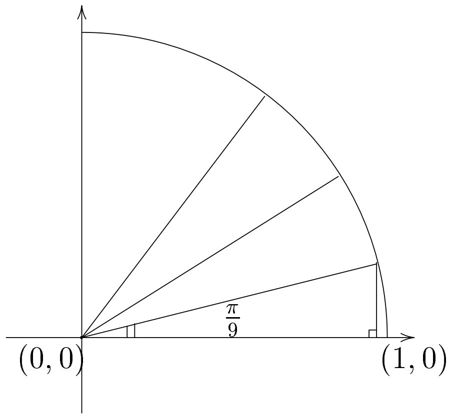

Figura 4.

Se construye $(\beta, 0)$ donde $\beta = 2\cos\left(\frac{\pi}{9}\right)$ de la trigonometría elemental tenemos que $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ si ponemos $\theta = \frac{\pi}{9}$ entonces $\cos(3\theta) = \frac{1}{2}$ y tenemos que $\beta^3 - 3\beta - 1 = 0$.
Ahora como $f(t) = t^3 - 3t - 3$ es irreducible sobre $\mathbb{Q}$ dado que $f(t+1) = t^3 - 3t - 3$ es irreducible (por el criterio de Einseinstein). Como en el teorema previo tenemos que $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$ lo cual es también una contradicción. $\square$

Teorema 5.2.3. *El circulo no se puede 'cuadrar' usando construcciones con regla y compás.*

Prueba. Si tal construcción fuera posible esta sería equivalente a poder construir el punto $(0, \sqrt{\pi})$ a partir de el conjunto $\{(0,0), (1,0)\}$. Pero si esto es posible entonces fácilmente podemos construir $(0, \pi)$. Por lo tanto $[\mathbb{Q}(\pi) : \mathbb{Q}]$ es una potencia de dos, y en particular π sería algebraico sobre $\mathbb{Q}$. Pero un poco más adelante probaremos un famoso teorema conocido con el nombre de teorema de Lindemann que afirma que π no es algebraico sobre $\mathbb{Q}$. Y con esto se sigue el resultado. $\square$

Falta choro...

5.3 Ejercicios.

5.1 Exprese en el lenguaje de este capítulo los métodos de construcción con regla y compás de:

a) La perpendicular de un segmento de linea que pase por el punto medio de la linea dada.

b) Los puntos de trisección de un segmento de recta.

c) La división de un segmento de recta en n partes igual

d) La tangente a un circulo en un punto dado (de el circulo).

e) Las tangentes comunes a dos círculos.

5.2 Estime los grados que corresponden a las extensiones de campos y de una razonable aproximación en los incisos del ejercicio anterior.

5.3 Verifique la siguiente construcción de la trisección de un ángulo usando una regla marcada (ver figura 5). La regla tiene una marca de longitud r.

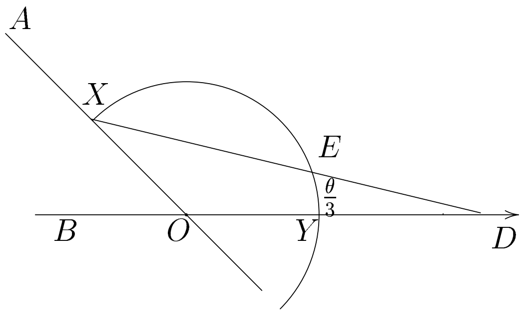

Figura 5.

Dado $\measuredangle AOB = \theta$ dibuja un circulo con centro en O y radio r, sea X el punto de intersección de OA y Y el punto de intersección de OB.

5.4 Puede el ángulo $\frac{2\pi}{5}$ ser trisecado usando regla y compás.

5.5 Muestra que es imposible el construir un 9-agono regular usando regla y compás.

5.6 Considerando la fórmula para $cos(5\theta)$ encuentra una construcción para el pentágono regular.

5.7 Pruebe que el angúlo θ puede ser trisecado usando regla y compás si y sólo si el polinomio

$$4t^3 - 3t - cos\theta$$

es irreducible sobre $\mathbb{Q}(cos\theta)$.

5.8 Discuta la quintisecsión (división en 5 partes iguales) de los ángulos.

5.9 Verifique la siguiente construcción aproximada para π (dada por *Ramanujan*[24]pag 35)

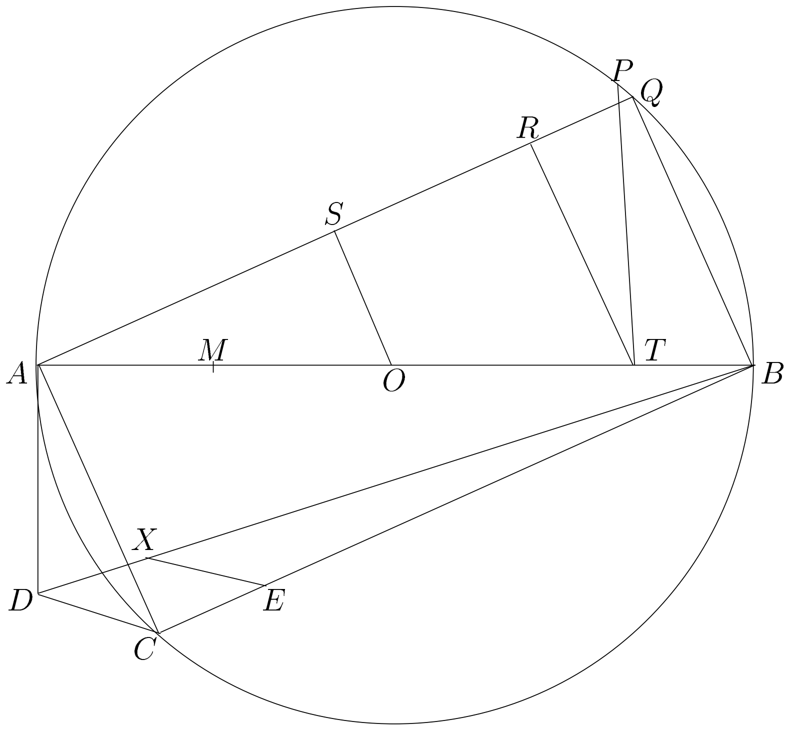

Figura 6

Sea AB el diámetro de el circulo centrado en O. Bisecamos AO digamos en el punto M, trisecamos OB digamos en T. Dibujamos TP perpendicular a AB intersectando al circulo en P. Dibujamos $BQ = PT$ y unimos AQ.

Trazamos OS y TR paralela a BQ. Trazamos $AD = AS$ y $AC = RS$ tangente a el circulo en A. Unimos BC, BD, CD. Hacemos $BE = BM$. Luego trazamos $BE = BM$. Trazamos además EX paralela a CD. Entonces el cuadrado de BX tiene aproximadamente la misma área que el circulo.

5.10 Diga si las siguientes afirmaciones son verdaderas o falsas.

a) Existen construcciones que trisecan el ángulo de cualquier grado aproximación.

b) Las coordenadas de un punto construible pertenecen a un subcampo de $mathbbR$ cuyo grado sobre el subcampo generado por las coordenadas de el punto dado es una potencia de dos.

c) El ángulo π no puede ser trisecado usando regla y compás.

d) Una linea de longitud π no puede ser construida de $\{(0,0),(1,0)\}$ usando regla y compás.

e) Es imposible el triplicar el cubo usando regla y compás.

f) El número real π es trascendente sobre $\mathbb{Q}$.

g) El número real π es trascendente sobre $\mathbb{R}$.

h) Si $(0, \alpha)$ no puede ser construido de $\{(0,0),(1,0)\}$ usando regla y compás entonces α es trascendente sobre $\mathbb{Q}$.

i) Los problemas geométricos no siempre pueden ser resueltos geométricamente.

Capítulo 6

Números trascendentales.

El material de este capítulo no será utilizado en los posteriores capítulos así que puede ser omitido por el lector.

Las técnicas involucran una parte de la teoría de diferenciación y de integración, así como la manipulación de algunas desigualdades.

No es de ninguna manera obvia, que los números trascendentales existan dentro de el campo de números complejos. La existencia de estos números fue primeramente probada por *Louville* en 1844, él considero la aproximación de números reales por números racionales (ver ejercicios 6.6 y 6.8). El encontrar un número trascendental se reduce a encontrar un número que puede ser aproximado más rapídamente que el utilizado para calcular números algebraicos. Louville mostró que este es el caso para el número real

$$\xi = \sum_{n=1}^{\infty} 10^{-n!} = .110010000000000.....$$

En 1873 *Hermíte* probo que el número e "la base de los logaritmos naturales" es trascendente, utilizando métodos similares a los usados por *Lindeman* el cual probo la trascendencia de π en 1882.

Cantor en 1874 produjo una prueba revolucionaría de la existencia de los números trascendentes (aunque no construyo ninguno), en dicha prueba se utilizaron métodos de la teoría de conjuntos. Y este es uno de los primeros triunfos de la teoría de cardinales infinitos.

Habremos de probar cuatro teoremas en este capítulo, en cada caso el procedimiento de las pruebas será por contradicción.

6.1 Irracionalidad.

iniciaremos esta sección con un resultado que será de gran importancia en el desarrollo de este capítulo.

Lema 6.1.1. *Una función $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ que tiende a cero cuando la variable tiende a infinito tiene que ser la función idénticamente cero en todo punto.*

Prueba. Dado que $f(n)$ tiende a cero cuando n tiende a infinito se tiene que $\mid f(n) - 0 \mid < \frac{1}{n}$ si $n \geqslant N$ para algún entero N. Dado que $f(n)$ es entero, lo anterior implica que $f(n)$=0 para toda $n \in \mathbb{N}$. $\square$

A continuación probaremos que π es un número racional, la prueba es la que dio Lindeman.

Teorema 6.1.2. *El número real π es irracional.*

Prueba. Consideremos

$$I_n = \int_{-1}^{1} (1 - x^2)^n \cos(\alpha x) dx$$

integrando por partes tenemos que

$$\alpha^2 I_n = 2n(n-1)I_{n-1} - 4n(n-1)I_{n-2} \tag{6.1}$$

ahora si $n \geqslant 2$. Por inducción sobre n se sigue que:

$$\alpha^{2n+1} I_n = n!(P sen\alpha + Q cos\alpha) \tag{6.2}$$

donde P, Q son polinomios en α de grado menor que $2n+1$ con coeficientes enteros. El término n! entra en el factor $n(n-1)$ de la ecuación 6.1. Terminaremos la prueba por contradicción, para ello supongamos que π es racional, esto es $\pi = \frac{a}{b}$ donde $a, b \in \mathbb{Z}$ y $b \neq 0$.

Entonces

$$J_n = b^{2n+1} \frac{I_n}{n!}$$

es un entero. Ahora bien

$$J_n = \frac{b^{2n+1}}{n!} \int_{-1}^{1} (1 - x^2)^n cos(\frac{\pi}{2}x) dx$$

donde el integrando es positivo puesto que $x \in (-1, 1)$ por lo tanto $J_n > 0$. Por lo que $J_n \neq 0$ para toda n. Pero además tenemos que

$$|J_n| = \frac{|b|^{2n+1}}{n!} \left| \int_{-1}^{1} cos(\frac{\pi}{2}x) dx \right| \leqslant c \frac{|b|^{2n+1}}{n!}$$

donde c es una constante. Por lo que J_n tiende a cero cuando n tiende a infinito, lo cual contradice el lema 6.0.1. Por lo tanto la afirmación de que π es racional es falsa. □

El siguiente resultado fue probado por *Legendre* en 1794 en sus *Elementos de Geometría* (esté es uno de los libros que tuvo gran influencia en la juventud de *Galois*).

Teorema 6.1.3. *El número real π^2 es irracional.*

Prueba. Supongamos que π^2 es racional es decir es un número de la forma

$$\pi^2 = \frac{a}{b}$$

donde $a, b \in \mathbb{Z}$ y $b \neq 0$. Definimos ahora las funciones:

$$f(x) = x^n \frac{(1 - x)^n}{n!}$$

y

$$G(x) = b^n \left[\pi^{2n} f(x) - \pi^{2n-2} f^{(2)}(x) + ... + (-1)^n \pi^0 f^{(2n)}(x) \right]$$

donde los supraindices en f indican las derivadas de f. Afirmamos que una derivada de G toma valores en los enteros (es ó bien cero ó bien uno). Pues recordando la regla de *leibniz* para la derivada de un producto tenemos que

$$\frac{d^m}{dx^m}(uv) = \sum_{r=1}^{m} \left[\binom{m}{r} \frac{d^r u}{dx^r} \frac{d^{m-r}}{dx^{m-r}} \right]$$

y ambos factores x^n o $(1-x^n)$ son diferenciables al menos n-veces y además el valor que toman en la respectiva n-ésima derivada es $x=0$ ó $x=1$. Ahora bien si un factor es diferenciado n o más veces entonces, el denominador $n!$ es cancelado por lo que $G(0)$ y $G(1)$ ambos son enteros. Como:

$$\begin{aligned} \frac{d}{dx}\left[G'(x)sen(\pi x) - \pi G(x)cos(\pi x)\right] &= \left[G''(x) + \pi^2 G(x)\right] sen(\pi x) \\ &= b^n \pi^{2n-2} f(x) sen(\pi x) \end{aligned}$$

dado que $f(x)$ es un polinomio en x de grado $2n$, tenemos que $f^{(2n+2)}(x) = 0$. Además esta expresión es igual a $\pi^2 a^n sen(\pi x) f(x)$.

Así pues

$$\pi \int_0^1 a^n sen(\pi x) f(x) dx = \left[\frac{G'(x)sen(\pi x)}{\pi} - G(x)cos(\pi x)\right]_0^1 = G(0) + G(1)$$

el cual es un número entero, así pues la integral anterior es no cero. Pero

$$\begin{aligned} \left| \int_0^1 a^n sen(\pi x) f(x) dx \right| &\leqslant |a|^n \int_0^1 |sen(\pi x)||f(x)| dx \\ &\leqslant |a|^n \int_0^1 \frac{|x^n(1-x)^n|}{n!} dx \\ &\leqslant \frac{1}{n!} \int_0^1 |(ax)^n (1-x)^n| dx \end{aligned}$$

y lo cual tiende a cero cuando n tiende a infinito, nuevamente por el lema 6.1.1 obtenemos una contradicción. $\square$

6.2 La trascendencia de e.

La prueba de la trascendencia de e primeramente fue dada por *Hermite*, después dicha prueba fue simplificada por *Weiestrass, Hilbert, Hurwitz y Gordan*(la prueba simplificada es la que daremos aquí.

Teorema 6.2.1 (Hermite). *El número real e es trascendente sobre* $\mathbb{Q}$

Prueba. Supongamos que e no es trascendente. Entonces

$$a_m e^m + ... + a_1 e + a_0 = 0$$

donde sin perdida de generalidad podemos suponer que $a_i \in \mathbb{Z}$ para toda i y $a_0 \neq 0$. Definimos

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p \cdots (x-m)^p}{(p-1)!}$$

Donde p es un número primo arbitrario. Ahora observamos que f es un polinomio en x de grado $mp + (p-1)$ sobre $\mathbb{Q}$. Así pues en la función

$$F(x) := f(x) + f'(x) + ... + f^{(mp+p-1)}(x)$$

notamos que $f^{(mp+p)} = 0$. Haciendo algunos cálculos obtenemos que

$$\frac{d}{dx}\left[e^{-x}F(x)\right] = e^{-x}\left[F'(x) - F(x)\right] = -e^{-x}f(x)$$

por lo que dada j tenemos que

$$a_j \int_0^j e^{-x} f(x)dx = a_j \left[-e^{-x}F(x)\right]_0^j = a_j F(0) - a_j e^{-j} F(j)$$

multiplicando por e^j y sumando sobre $j = 0, ..., m$ se tiene que

$$\begin{aligned} \sum_{j=0}^{m} \left(a_j e^j \int_0^j e^{-x} f(x)dx \right) &= F(0) \sum_{j=0}^{m} a_j e^j - \sum_{j=0}^{m} a_j F(j) && (6.3) \\ &= - \sum_{i=0}^{mp+p-1} a_j f^{(i)}(j) && (6.4) \end{aligned}$$

la ecuación anterior es satisfecha por e. Afirmamos ahora que cada $f^{(i)}(j)$ es un número entero y además que es divisible por p, salvo para $j = 0$ y para $i = p - 1$.

Para probar esto usaremos nuevamente la regla de *Leibniz*; el único término no cero en el factor $(x - j)^p$ ocurre cuando $j = 0$. Dado que $p!/(p-1)! = p$ tales términos son enteros divisibles por p. En el único caso cuando $j = 0$ el único término es cuando $i = p - 1$ y entonces

$$f^{(p-1)}(0) = (-1)^p \cdots (-m)^p$$

El valor en la ecuación 6.3, es entonces

$$kp + a_0(-1)^p \cdots (-m)^p \text{ para algún } k \in \mathbb{Z}$$

Ahora si $p > max\{m, |a_0|\}$ entonces el entero $a_0(-1)^p \cdots (-m)^p$ no es divisible por p. Por lo tanto para un primo suficientemente grande p el valor en la ecuación 6.3, es un entero divisible por p por lo tanto no cero.

Ahora estimando la integral tenemos que si $0 \leq x \leq m$ entonces:

$$|f(x)| \leq m^{mp+p-1}/(p-1)!$$

por lo que

$$\begin{aligned}\left[\sum_{J=0}^{m} a_j e^j \int_0^j e^{-x} f(x)dx\right] &\leq \sum_{j=0}^{m} |a_j e^j| \int_0 j \frac{m^{mp+p-1}}{(p-1)!} dx \\ &\leq \sum_{j=0}^{m} \left(|a_j e^j| j \frac{m^{mp+p-1}}{(p-1)!}\right)\end{aligned}$$

y lo anterior tiende a cero cuando p tiende a infinito, lo cual es una contradicción. Por lo tanto e es trascendente □

6.3 La trascendencia de π

Una prueba de que π es trascendental involucra algunos resultados previos, uno de los puntos importantes que usaremos están basados en las propiedades de los polinomios simétricos (capítulo 2).

Teorema 6.3.1 (Lindemann). *El número real π es trascendente sobre $\mathbb{Q}$.*

Prueba. Nuevamente procederemos por contradicción, así pues supongamos que π es cero de algún polinomio no cero sobre $\mathbb{Q}$.

De este modo también $i\pi$ es cero de un polinomio no cero sobre $\mathbb{Q}$ donde

$$i = (-1)^{\frac{1}{2}} = \sqrt{-1}$$

Sea $\Theta_1 \in \mathbb{Q}[x]$ un polinomio con ceros $\alpha_1 = i\pi, \alpha_2, ..., \alpha_n$. Por el 'famoso' teorema de *Euler* se tiene que

$$e^{i\pi} + 1 = 0$$

por lo que

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdots (e^{\alpha_n} + 1) = 0 \tag{6.5}$$

Construimos ahora un polinomio con coeficientes enteros cuyos ceros sean los exponentes $\alpha_{i_1} + ... + \alpha_{i_r}$ de e que aparecen en la expresión de el producto en la ecuación 6.5. Por ejemplo, términos de la forma

$$e^{\alpha_s} e^{\alpha_t} \cdot 1 \cdots 1$$

dan exponentes $\alpha_s + \alpha_t$. Tomando sobre todas las parejas s, t obtenemos que los polinomios simétricos elementales de

$$\alpha_1 + \alpha_2, \ldots, \alpha_{n-1} + \alpha_n$$

son también simétricos en

$$\alpha_1, ..., \alpha_n,$$

por lo que por el teorema 2.4.2 estos polinomios pueden ser expresados como polinomios en los polinomios simétricos elementales de $\alpha_1, ..., \alpha_n$. Estos a su vez son expresados en términos de los coeficientes de el polinomio Θ_1 cuyos ceros son $\alpha_1, ..., \alpha_n$. Por lo que las parejas $\alpha_s + \alpha_t$ satisfacen una ecuación polinomial $\Theta_2(x) = 0$ donde Θ_2 tiene coeficientes racionales. De manera similar las sumas de k $\alpha's$ son ceros de un polinomio $\Theta_k(x)$ sobre $\mathbb{Q}$. Entonces

$$\Theta_1(x)\Theta_2(x)\cdots\Theta_n(x)$$

es un polinomio sobre $\mathbb{Q}$ cuyos ceros son los exponentes de e en la fórmula 6.3. Dividiendo ahora por una adecuada potencia de x y multiplicando por un entero adecuado obtenemos un polinomio $\Theta(x)$ sobre $\mathbb{Z}$ cuyos ceros son los exponentes no cero en la ecuación 6.3. Ahora la ecuación 6.3 toma la forma

$$e^{\beta_1} + ... + e^{\beta_r} + e^0 + ... + e^0 = 0$$

esto es

$$e^{\beta_1} + ... + e^{\beta_r} + k = 0 \tag{6.6}$$

donde $k \in \mathbb{Z}$. El término $1 + \ldots + 1$ ocurre en la ecuación 6.5, por lo que $k > 0$

Supongamos que $\Theta(x) = cx^r + c_1x^{r-1} + ... + c_r$ donde $c_r \neq 0$, dado que 0 no es un cero de Θ. Definimos

$$f(x) = c^s x^{p-1}[\Theta(x)]^p/(p-1)!$$

donde $s = r(p-1)$ y p es un número primo. Definamos también

$$F(x) = f(x) + f'(x) + ... + f^{(s+p+r-1)}(x)$$

y notemos que $f^{(s+r+p)}(x) = 0$. Por un procedimiento similar al usado en el teorema anterior tenemos que

$$\frac{d}{dx}[e^{-x}F(x)] = -e^{-x}f(x)$$

por lo que

$$e^{-x}F(x) - F(0) = \int_0^x e^{-y}f(y)dy$$

haciendo $y = \lambda x$ se tiene

$$F(x) - e^x F(0) = -x \int_0^1 e^{(1-\lambda)x} f(\lambda x) d\lambda$$

y el rango de x está sobre $\beta_1, ..., \beta_r$, ahora sumando de la ecuación 6.5, obtenemos

$$\sum_{j=1}^{r} f(\beta_j) + kF(0) = -\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda \beta_j) d\lambda \tag{6.7}$$

Afirmamos que para un primo suficientemente grande p el lado izquierdo de la ecuación 6.7, es un entero no cero.

Para probar esto consideremos la siguiente suma que sabemos que es igual a cero

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = 0 \qquad si \quad 0 < t < p$$

Cada derivada $f^{(t)}(\beta_j)$ con $t \geq p$ tiene un factor p, esto es dado que $(\Theta(x))^p$ puede ser diferenciado al menos p-veces para con ello obtener un término no cero. Para cada t tenemos que

$$\sum_{j=1}^{r} f^{(t)}(\beta_j)$$

es un polinomio simétrico en las β_j de grado menor o igual a s. Por lo que este es un polinomio de grado menor o igual a s en los coeficientes c_i/c, nuevamente por el teorema 2.4.2, el factor c^s en la definición de $f(x)$ hace de este un entero. Por lo que para $p \geq s$ se tiene

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = pk_t$$

para alguna constante $k_t \in \mathbb{Z}$. Ahora observamos que pasa con $F(0)$ para ello tenemos que

$$f^{(t)}(0) = \begin{cases} 0 & (t \leq p-2) \\ c^s c_r^p & (t = p-1) \\ l_t p & (t \geq p) \end{cases}$$

para una constante adecuada $l_t \in \mathbb{Z}$. Consecuentemente el lado izquierdo en la ecuación 6.7, es $Kp + kc^s c_r^p$ para alguna $K \in \mathbb{Z}$.

Ahora bien como $k \neq 0, c \neq 0.c_r \neq 0$, consideramos a un primo p tal que $p > max\{k, |c|, |c_r|\}$entonces el lado izquierdo de 6.7, es un entero no divisible por p y por lo cual no es cero. La última parte de la prueba es rutina, así pues estimando el tamaño de el lado derecho en la ecuación 6.7, sabemos que

$$|f(\lambda\beta_j)| \leq |c|^s (m(j))^p/(p-1)!$$

donde

$$m(j) = \sup_{0 \leq \lambda \leq 1} \{|\Theta(\lambda\beta_j)|\}$$

por lo que

$$\left| -\sum j = 1^r \beta_j \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda\beta_j) d\lambda \right| \leq \sum_{j=1}^{r} |\beta_j||c^s||m(j)|^p B/(p-1)!$$

donde

$$B = |max_j\{\int_0^1 e^{(1-\lambda)\beta_j} d\lambda\}|$$

pero está expresión tiende a cero cuando p tiende a infinito, lo cual es una contradicción y por lo tanto π es trascendente. □

6.4 Ejercicios.

Los cuatro primeros ejercicios constituyen una prueba de la existencia de los números trascendentes (esta prueba es conocida con el nombre de *Cantor*)

6.1 Pruebe que el campo $\mathbb{R}$ de los números reales es no numerable.

6.2 Definimos para el polinomio

$$f(t) = a_0 + ... + a_n t^n \in \mathbb{Z}[t]$$

su *altura* como:

$$h(f) := n + |a_0| + ... + |a_n|$$

Pruebe que existe sólo un número finito de polinomios sobre $\mathbb{Z}$ los cuales tienen altura fija.

6.3 Muestra que un número algebraico satisface una ecuación polinomial sobre $\mathbb{Z}$. (sugerencia: usando el ejercicio 6.2, muestra que los números algebraicos forman un conjunto numerable)

6.4 Combinando 6.1 y 6.3 prueba que el conjunto de los números trascendentes es no numerable.

6.5 Dibujo

Los siguientes tres ejercicios dados por *Liouville* prueban la existencia de los números trascendentes.

6.6 Supóngase que x es irracional y que $f(x) = a_n x^n + ... + a_0 = 0$ donde $a_0, ..., a_n \in \mathbb{Z}$. Muestra que si $p, q \in \mathbb{Z}$, $q \neq 0$ y $f(p/q) \neq 0$ entonces;

$$|f(p/q)| \geq \frac{1}{q^n}.$$

6.7 Ahora supongamos que $x - 1 < p/q < x + 1$ y p/q es un número racional cercano a x más que cualquier cero de f, entonces existe una constante M tal que $|f'(y)| < M$ si $x - 1 < y < x + 1$. Use el teorema de el valor medio para probar que que $|p/q - x| \geq M^{-1} q^{-n}$.

Por lo que para una $r > n$ y $k > 0$ existe sólo un número finito p y q tal que $|p/q - x| < kq^{-r}$.

6.8 Use este resultado para probar que $\sum_{n=1}^{\infty} 10^{-n!}$ es trascendente.

6.9 Marque verdadero o falso.

a) π es irracional.

b) Todo número irracional es trascendental.

c) Algún múltiplo racional de π es trascendente.

d) Algunas veces el único camino para probar un teorema es a trote de asno.

e) e es irracional.

f) Si α y β son trascendentes entonces también lo es $\alpha + \beta$.

g) Los números trascendentes forman un subanillo de $\mathbb{C}$.

h) El campo $\mathbb{Q}(\pi)$ es isomorfo a $\mathbb{Q}(t)$ para alguna indeterminada t.

i) $\mathbb{Q}(\pi)$ y $\mathbb{Q}(e)$ son campos no isomorfos.

j) $\mathbb{Q}(\pi)$ es isomorfo a $\mathbb{Q}(\pi^2)$.

Capítulo 7

La idea principal de la teoría de Galois.

En este capítulo daremos las ideas principales de la teoría de Galois, es de gran importancia tener siempre presente cuando se trabaja sobre algún problema, el no perder de vista el objetivo fundamental, por ello en este momento habremos de establecer, los puntos atratar más adelante.

Definición 7.0.1. Sea k un subcampo de un campo L. Un automorfismo α de L es un *K-automorfismo de L* si $\alpha(k) = k$ para toda $k \in K$.

La idea de considerar automorfismos de un objeto matemático relativa a un subobjeto es usada de manera general en las distintas ramas de la matemática, por ejemplo; en el famoso programa *Erlanger Programm* de *Felix Klein*, la idea de Klein fue la de considerar a cada "geometría" como la teoría de invariantes de una particular transformación de grupos. Por lo que a la *geometría euclidiana* la considero como el estudio de transformaciones de grupos que son invariantes bajo preservar distancias (la distancia en el plano euclidiano); la *geometría proyectiva* bajo transformaciones proyectivas; en *topología* el estudio de invariantes es sobre todos los mapeos continuos que tienen inversa continua (llamados *homeomorfismos o transformaciones topólogicas*). De este modo tenemos que la interpretación de una extensión de campos es una geometría y hacemos simplemente el estudio de figuras geométricas.

Teorema 7.0.2. *Si (L:K) es una extensión de campos entonces el conjunto de todos los K-automorfismos de L forman un grupo bajo la composición de automorfismos.*

Prueba. Supongamos que α, β son $K - automorfismos$ de L (para simplificar notación, simplemente le llamaremos $K - aut$ a un $K - automorfismo$) entonces claramente $\alpha \circ \beta$ es un automorfismo de L; más aún si $k \in K$ entonces $\alpha\beta(k) = \alpha(\beta(k)) = \alpha(k) = k$, por lo que $\alpha \circ \beta$ es un $K - automorfismo$ de L. El mapeo identidad de L es claramente un $K - automorfismo$ de L. Finalmente α^{-1} es un automorfismo de L y dada $k \in K$ se tiene que $k = \alpha^{-1}\alpha(k) = \alpha^{-1}(k)$ por lo que α^{-1} es un $K - automorfismo$ de L. Como la composición de automorfismos es asociativa, tenemos que el conjunto de todos los $K - automorfismos$ $(K - aut)$ de L forman un grupo. $\square$

Definición 7.0.3. El grupo de todos los $K - aut$ de L bajo la composición de automorfismos de la extensión $(L : K)$, será llamado *el grupo de Galois* de la extensiín $(L : K)$ y lo denotaremos por$\Gamma(L : K)$.

Ejemplos

1. En la extensión $(\mathbb{C} : \mathbb{R})$ supongamos que α es un $\mathbb{R}$-aut de $\mathbb{C}$, sea $j = \alpha(i)$ donde $i = \sqrt{-1}$. Entonces,

$$j^2 = (\alpha(i))^2 = \alpha(i^2) = \alpha(-1) = -1$$

dado que $\alpha(r) = r$, para toda $r \in \mathbb{R}$ tenemos que $j = i$ o $j = -i$. Ahora para $x, y \in \mathbb{R}$ tenemos que

$$\alpha(x + iy) = \alpha(x) + \alpha(i)\alpha(y) = x + jy$$

Por lo que los únicos dos candidatos para ser $\mathbb{R}$-aut de $\mathbb{C}$ son

$$\alpha_1 : x + iy \longmapsto x + iy$$

$$\alpha_2 : x + iy \longmapsto x - iy$$

α_1 es la identidad y por lo tanto un $\mathbb{R}-aut$ de $\mathbb{C}$, el morfismo α_2 se le conoce como la conjugación compleja y mostraremos que también es un $\mathbb{R}$-aut de $\mathbb{C}$ como sigue:

$$\alpha_2[(x+iy)+(u+iv)] = (x+u)-(y+v)i = \alpha_2(x+iy)+\alpha_2(u+iv)$$

$$\begin{aligned}\alpha_2[(x+iy)(u+iv)] &= \alpha_2(xu-yv+i(xv+yu)) \\ &= xu-yv-i(xv+yu) \\ &= (x-iy)(u-iv) \\ &= \alpha_2(x+iy)\alpha_2(u+iv)\end{aligned}$$

Por lo tanto α_2 es un $\mathbb{R}$-aut de $\mathbb{C}$. Obviamente $\alpha_2^2 = \alpha_1$ por lo que el grupo de Galois $\Gamma(\mathbb{C}:\mathbb{R})$ es un grupo de orden dos.

2. Consideremos ahora $c = 2^{(\frac{1}{3})}$ la raíz cubica de el número real 2 y consideremos la extensión $(\mathbb{Q}(c):\mathbb{Q})$ si α es un $\mathbb{Q}$-aut de $\mathbb{Q}(c)$ entonces

$$(\alpha(c))^3 = \alpha(c^3) = \alpha(2) = 2$$

Dado que $\mathbb{Q}(c) \subseteq \mathbb{R}$ se tiene que $\alpha(c) = c$. Por lo que α es la identidad y $\Gamma(\mathbb{Q}(c):\mathbb{Q})$ tiene orden uno.

De la misma manera tenemos que en las pruebas anteriores probamos que el conjunto de todos los automorfismos de un campo L forman un grupo bajo la composición de automorfismos. Uno de los usos principales de el grupo de Galois es que esté refleja parte de la estructura de $(L:K)$. La idea principal que tuvo Galois (expresada en términos de polinomios) es que bajo ciertas condiciones existe una correspondencia uno a uno entre:

1. Los subgrupos de el grupo de Galois de $(L:K)$.

2. Los subcampos M de L que contienen a K.

Si $(L:K)$ es una extensión de campos diremos que un campo M es *intermedio* si $K \leqslant M \leqslant L$. A cada campo intermedio le asociamos el grupo $M^* = \Gamma(L:M)$ de todos los $M-automorfismos$ de L. Por lo que con esta notación K^* es el grupo de Galois $\Gamma(L:K)$. A L^* que consiste solamente de el automorfismo identidad de L lo denotaremos por $L^* = 1_L$.

Claramente si $M \subseteq N$ entonces, tenemos que $N^* \subseteq M^*$, pues cada automorfismo de L que deje fijos los elementos de N también deja fijos todos elementos de M.

Recíprocamente a cada subgrupo H de $\Gamma(L:K)$ le asociamos el conjunto $H^\dagger$ de todos los elementos $x \in L$ tal que $\alpha(x) = x$ para toda $\alpha \in H$. Que además resulta ser un campo intermedio por el siguiente lema.

Lema 7.0.4. *Si H es un subgrupo de $\Gamma(L:K)$ entonces, $H^\dagger$ es un subcampo de L que contiene a K.*

Prueba. Sean $x, y \in H^\dagger$ y $\alpha \in H$ entonces $\alpha(x+y) = \alpha(x)+\alpha(y) = x+y$. de manera similar se tiene que $H^\dagger$ es cerrado bajo la otra operación de campo, es pura rutina probar que $H^\dagger$ satisface los axiomas de campo y se dejan a el lector los detalles de esto. Dado que para $\alpha \in \Gamma(L:K)$ tenemos que $\alpha(k) = k$ para toda $k \in K$ entonces $K \subseteq H^\dagger$. □

Definición 7.0.5. Con la notación anterior $H^\dagger$ es el *campo fijo* de H.

Claramente si $H \subseteq G$ entonces $G^\dagger \subseteq H^\dagger$. Es también fácil de verificar que si M es un campo intermedio y H es un subgrupo de el grupo de Galois entonces

$$M \subseteq M^{*\dagger}$$

y

$$H \subseteq H^{\dagger *}$$

El ejemplo 2 de está sección muestra que estas inclusiones son no necesariamente igualdades pues por ejemplo, tenemos que

$$\mathbb{Q}^{*\dagger} = \mathbb{Q}(c).$$

Si $\mathfrak{F}$ denota al conjunto de todos los campos intermedios y $\mathfrak{G}$ al conjunto de subgrupos de el grupo de Galois entonces, tenemos dos transformaciones como sigue.

$$* : \mathfrak{F} \longrightarrow \mathfrak{G}$$

$$\dagger : \mathfrak{G} \longrightarrow \mathfrak{F}$$

Cuya inclusión inversa se satisface por lo dicho anteriormente. La idea principal de Galois se puede interpretar de la siguiente manera:

Bajo que condiciones * y † son inversas naturales o bien, cuando se tiene una biyección entre $\mathfrak{F}$ y $\mathfrak{G}$. Algunas de las condiciones extra que necesitamos son llamadas condiciones de *separabilidad* y *normalidad* y estas serán discutidas en el siguiente capítulo.

7.1 Ejercicios.

7.1 Encuentra los $K - aut$ de L para las siguientes extensiones $(L : K)$.

a) $(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$

b) $(\mathbb{Q}(\sqrt[5]{7}) : \mathbb{Q})$

c) $(\mathbb{Q}(\sqrt{2}), \sqrt{3} : \mathbb{Q})$

7.2 Encuentre el grupo de Galois correspondiente a las extensiones del ejercicio anterior.

7.3 En cuales de los casos del ejercicio anterior el grupo de Galois correspondiente a las extensiones da una biyección.

7.4 Sea K es el campo de cuatro elementos definido en el ejercicio 1.6 y P su subcampo primo. ¿Cual es el grupo de Galois de $(L : K)$?. ¿Es la correspondencia de Galois una biyección?.

7.5 Sea $(K(\alpha) : K)$ una extensión algebraica simple y supóngase que γ es un elemento de el grupo de Galois. Pruebe que $\gamma(\alpha)$ tiene el mismo polinomio mínimo que α sobre K. Por lo que este ejercicio muestra que el grupo de Galois actúa como permutaciones de los ceros de este polinomio.

7.6 Encuentra todos los campos intermedios para la extensión $\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}\right)$. Encuentre el grupo de Galois.¿Que observas?.

7.7 Di si las siguientes afirmaciones son falsas ó verdaderas.

a) Cada K-aut de L es un automorfismo de L.

b) Cada L-aut de L es la identidad.

c) El grupo de Galois de $(L : K)$ es un grupo cíclico.

d) El grupo de Galois de $(\mathbb{C} : \mathbb{R})$ es abeliano.

e) Los mapeos * y † son siempre uno inverso de el otro.

f) Los mapeos * y † preservan inclusiones.

g) Si $\Gamma(L : K) = 1$ entonces $L = K$.

h) Si $L = K$ entonces $\Gamma(L : K) = 1$.

i) $K(t)$ tiene sólo un K-aut.

Capítulo 8

Normalidad y Separabilidad.

En este capítulo habremos de definir los conceptos importantes de *normalidad* y *separabilidad* así como el de desarrollar algunos resultados importantes respecto a estos.

También describiremos el fenómeno en el cual un polinomio puede no tener ceros en un campo pero el mismo polinomio tener ceros en un campo mayor (más grande). Por ejemplo, el polinomio $t^2 + 1$ no tiene ceros sobre $\mathbb{R}$ pero tiene a $i, -i$ como ceros en $\mathbb{C}$. También hablaremos de la descomposición de un polinomio como producto de factores lineales (y por lo tanto tener todos sus ceros) esto es lo que llamaremos el *campo de descomposición.* Habremos de estudiar estos campos de descomposición y mostraremos que dichos campos son muy parecidos al concepto de normalidad.

Daremos también ejemplos que usan propiedades muy especiales de el campo de los números complejos $\mathbb{C}$, así como también un resultado que quedara abierto (por ahora) que es el conocido *Teorema Fundamental de el Álgebra* que dice que todo polinomio con coeficientes en $\mathbb{C}$ puede ser expresado como producto de factores lineales, dicho resultado lo probaremos en el capítulo 18.

8.1 Campos de descomposición.

Comenzaremos esta sección con la siguiente:

Definición 8.1.1. Si K es un campo y F es un polinomio sobre K entonces, diremos que F se *divide* sobre K, si F puede ser expresado como un producto de factores

$$f(t) = k(t - \alpha_1) \cdots (t - \alpha_n)$$

donde $k, \alpha_1, ..., \alpha_n \in K$.

En este caso tenemos que los ceros de F en K son precisamente $\alpha_1, ..., \alpha_n$.

Si F es un polinomio sobre K y L es una extensión de K entonces un polinomio f sobre K lo es también sobre L. Mostraremos que dado un campo K y un polinomio f sobre este campo, podemos construir siempre una extensión Ξ de K tal que f se divide sobre Ξ, habremos de tener también que f no se divida sobre un campo menor que Ξ para de esta manera tener a Ξ como un campo lo más económico (pequeño) posible.

Definición 8.1.2. El campo Ξ es un *campo de descomposición* para un polinomio f sobre un campo K si $K \subseteq \Xi$ y
(1) f se divide sobre Ξ.
(2) Si $K \subseteq \Xi' \subseteq \Xi$ y f se divide sobre Ξ', entonces $\Xi' = \Xi$

esta segunda condición es equivalente a:
(2') $\Xi = K(\sigma_1, ..., \sigma_n)$ donde $\sigma_1, ..., \sigma_n$ son los ceros de f en Ξ.

Construiremos el campo de descomposición mediante la adjunción de elementos al campo K y estos elementos serán precisamente los ceros de f, para esto habremos de utilizar polinomios irreducibles (teorema 3.3.8)

Teorema 8.1.3. *Si K es un campo y f es un polinomio sobre K entonces, existe un campo de descomposición para f sobre K.*

Prueba. La prueba la haremos por inducción sobre el grado de f, ∂f. Si $\partial f = 1$ entonces no tenemos nada que probar pues f claramente se divide sobre K. Ahora bien si f no se divide sobre K entonces tomamos un factor irreducible f_1 de grado mayor que 1. Usando el teorema 3.3.8 le agregamos σ_1 a K donde $f(\sigma_1) = 0$. Entonces en $K(\sigma_1)(t)$ tenemos que $f = (t-\sigma_1)g$ donde $\partial g = \partial f - 1$. Por hipótesis de inducción tenemos que existe un campo de descomposición Ξ para g sobre $K(\sigma_1)$ por lo que este mismo Ξ es un campo de descomposición de f sobre K. $\square$

En la prueba anterior tenemos una observación muy importante pues en la construcción de el campo de descomposición de un polinomio f sobre un campo K podemos obtener diferentes campos de descomposición ya que al tomar la descomposición de el polinomio en producto de factores irreducibles, posiblemente lleguemos a distintos campos de descomposición. Pero no nos alarmemos demasiado ya que dichos campos son isomorfos y habremos de probar esto a continuación para ello utilizaremos resultados de el capítulo tres así como de una pequeña inducción.

Lema 8.1.4. *Supóngase que $\imath : K \longrightarrow K'$ es un isomorfismo de campos. Sea f un polinomio sobre K y Ξ un campo de descomposición de f sobre K. Si L es una extensión de el campo K' tal que $\imath(f)$ se divide sobre L. Entonces existe un monomorfismo $\jmath : \Xi \longrightarrow L$ tal que $\jmath|_K = \imath$*

Prueba. Consideremos el siguiente diagrama;

$$\begin{tikzcd} K \arrow[r] \arrow[d, "\imath"'] & \Xi \arrow[d, dashed, "\jmath"] \\ K' \arrow[r] & L \end{tikzcd}$$

donde $\jmath$ es el monomorfismo que buscamos.

Ahora usaremos inducción sobre ∂f. Como Ξ es un campo de descomposición de f sobre K tenemos que

$$f = k(t-\sigma_1)\cdots(t-\sigma_n).$$

Para $\sigma_1, \ldots, \sigma_n \in \Xi$ y $k \in K$. El polinomio mínimo m de σ_1 sobre K es un factor irreducible de f. Ahora $\imath(m)$ divide a $\imath(f)$ el cual se divide sobre L, por lo que sobre L tenemos que

$$\imath(m) = (t - \alpha_1) \cdots (t - \alpha_r)$$

donde $\alpha_1, ..., \alpha_r \in L$. Dado que $\imath(m)$ es irreducible sobre K' se tiene que es el polinomio mínimo de α_1 sobre K'. Por lo que por teorema 3.4.5, existe un isomorfismo

$$\jmath_1 : K(\sigma_1) \longrightarrow K'(\alpha_1)$$

tal que

$$\jmath_1|_K = \imath$$

y

$$\jmath_1(\sigma_1) = \alpha_1.$$

Ahora Ξ es un campo de descomposición de el polinomio

$$g = \frac{f}{(t - \sigma_1)}$$

sobre $K(\sigma_1)$. Por inducción tenemos que existe un monomorfismo

$$\jmath : \Xi \longrightarrow L$$

tal que

$$\jmath|_{K(\sigma_1)} = \jmath_1.$$

Pero entonces tenemos que $\jmath|_K = \imath$, con lo cual concluye la prueba. $\square$

Este resultado establece una cierta unicidad que probaremos en el siguiente teorema.

Teorema 8.1.5. *Sea $i : K \longrightarrow K'$ un isomorfismo de campos. Sea T un campo de descomposición de un polinomio f sobre K, T' un campo de descomposición para $i(f)$ sobre K'. Entonces existe un isomorfismo $j : T \longrightarrow T'$ tal que $j|_K = i$. Dicho de otra manera las extensiones $(T : K)$ y $(T' : K')$ son isomorfas.*

Prueba. Nuevamente consideremos el siguiente diagrama

$$\begin{tikzcd} K \arrow[r] \arrow[d, "i"'] & T \arrow[d, dashed, "j"] \\ K' \arrow[r] & T' \end{tikzcd}$$

Nosotros necesitamos encontrar j para hacer conmutativo el diagrama anterior. Por el lema 8.1.4, tenemos que existe un monomorfismo

$$j : T \longrightarrow T'$$

tal que $j|_K = i$. Pero $j(T)$ es un campo de descomposición para $i(f)$ sobre K' y este está contenido en T'. Dado que T' es también un campo de descomposición para $i(f)$ sobre K' se tiene que $j(T) = T'$, por lo que j es suprayectivo. Por lo tanto j es un isomorfismo. $\square$

Ejemplos.

1 Sea $f(t) = (t^2 - 3)(t^3 + 1)$ sobre $\mathbb{Q}$. Podemos construir un campo de descomposición de f como sigue: dentro de $\mathbb{C}$, f se descompone en factores lineales de la siguiente manera.

$$f(t) = (t+1)\left(t + \sqrt{3}\right)\left(t - \sqrt{3}\right)\left(t - \frac{-1 + i\sqrt{3}}{2}\right)\left(t - \frac{-1 - i\sqrt{3}}{2}\right)$$

Por lo que existe un campo de descomposición dentro de $\mathbb{C}$ que es:

$$\mathbb{Q}\left(\sqrt{3}, \frac{-1 + i\sqrt{3}}{2}\right)$$

y es claro que está extensión es la misma que $\mathbb{Q}\left(\sqrt{3}, i\right)$.

2 Sea $f(t) = (t^2 - 2t - 2)(t^2 + 1)$ sobre $\mathbb{Q}$. Los ceros de f en $\mathbb{C}$ son $1 \pm \sqrt{3}, \pm i$. Por lo que un campo de descomposición es $\mathbb{Q}\left(1 + \sqrt{3}, i\right)$ el cual es igual a $\mathbb{Q}\left(\sqrt{3}, i\right)$. Este es el mismo campo que en el ejemplo anterior, !pero están involucrados polinomios distintos!

3 También es posible que tengamos dos polinomios irreducibles con el mismo campo de descomposición. Por ejemplo, $t^2 - 3$ y $t^2 - 2t - 2$ ambos tienen el mismo campo de descomposición, a saber $\mathbb{Q}\left(\sqrt{3}\right)$ sobre $\mathbb{Q}$.

4 Ahora consideremos $f(t) = t^2 + t + 1$ sobre $\mathbb{Z}_2$. En esta ocasión no podemos auxiliarnos con el campo de los números complejos $\mathbb{C}$, sin embargo haremos la construcción de su campo de descomposición de una manera ilustrativa. Primeramente recordemos que el campo $\mathbb{Z}_2$ solamente tiene dos elementos a saber 0 y 1. Notemos ahora que f es irreducible, por lo que tenemos que adjuntarle un elemento ζ a $\mathbb{Z}_2$ tal que ζ tenga como polinomio mínimo a f sobre $\mathbb{Z}_2$. De esta manera tenemos que $\zeta^2 + \zeta + 1 = 0$ por lo que $\zeta^2 = 1 + \zeta$. Nuestra primera afirmación es que los siguientes cuatro elementos forman un campo.

$$0, 1, \zeta, 1 + \zeta.$$

Para probar esto solamente tenemos que verificar las siguientes tablas de suma

$+$	0	1	ζ	$1+\zeta$
0	0	1	ζ	$1+\zeta$
1	1	0	$1+\zeta$	ζ
ζ	ζ	$1+\zeta$	0	1
$1+\zeta$	$1+\zeta$	ζ	1	0

y multiplicación.

$\cdot$	0	1	ζ	$1+\zeta$
0	0	0	0	0
1	0	1	ζ	$1+\zeta$
ζ	0	ζ	$1+\zeta$	1
$1+\zeta$	0	$1+\zeta$	1	ζ

Se sigue, que $\mathbb{Z}_2(\zeta)$ es un campo con cuatro elementos. Además tenemos que f se divide sobre $\mathbb{Z}_2(\zeta)$ pues

$$t^2 + t + 1 = (t - \zeta)(t - (1 + \zeta))$$

y además no puede dividirse sobre un campo más pequeño. Por lo tanto $\mathbb{Z}_2(\zeta)$ es un campo de descomposición de f sobre $\mathbb{Z}_2$.

8.2 Normalidad.

La idea de una extensión normal fue expuesta primeramente por Galois (aunque esta fue dada en términos de polinomios sobre el campo de los números complejos). En el lenguaje moderno está idea toma la siguiente forma.

Definición 8.2.1. Una extensión $(L : K)$ es *normal* si cada polinomio irreducible f sobre K que tiene al menos un cero en L entonces este polinomio se divide en L.

Por ejemplo, la extensión $(\mathbb{C} : \mathbb{R})$ es normal ya que cada polinomio (irreducible o no) se divide en $\mathbb{C}$. En el otro sentido podemos encontrar extensiones que no sean normales por ejemplo, consideremos la extensión $\left(\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right)$. Un polinomio irreducible que tiene por cero a $\sqrt[3]{2}$ en $\mathbb{Q}\left(\sqrt[3]{2}\right)$ es $t^3 - 2$, pero este polinomio no se divide sobre $\mathbb{Q}\left(\sqrt[3]{2}\right)$ pues si lo hiciera tendríamos tres raíces distintas, de 2 lo cual es absurdo.

Comparando estos ejemplos con los grupos de Galois dados en el capítulo anterior, la extensión normal $(\mathbb{C} : \mathbb{R})$ tiene un 'buen' grupo de Galois asociado en el sentido de que la correspondencia de Galois es una biyección. Mientras que extensión no normal $\left(\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right)$ no tiene un buen grupo de Galois asociado en el mismo sentido.

Existe una conexión importante entre extensiones normales y campos de descomposición que tiene que ver con el rango de la extensión normal.

Teorema 8.2.2. *Una extensión $(L : K)$ es normal y finita si, y sólo si L es el campo de descomposición para algún polinomio sobre K.*

Prueba. Primeramente supongamos que $(L : K)$ es normal y finita por la proposición 4.1.5, $L = K(\alpha_1, ..., \alpha_s)$ para ciertos números algebraicos α_i sobre

K. Si m_i es el polinomio mínimo de α_i sobre K entonces f se escribe como $f = m_1 \cdots m_s$.

Cada m_i es irreducible sobre K y tiene como cero a α_i sobre L, por la normalidad de la extensión tenemos que cada m_i se divide sobre L y por lo tanto f se divide sobre L. Dado que L esta generado por K y los ceros de f tenemos que L mismo es un campo de descomposición de f sobre K.

Recíprocamente supongamos que L es un campo de descomposición para algún polinomio g sobre K. La extensión $(L : K)$ es entonces obviamente finita; por lo que solamente resta probar que esta extensión es normal. Para ello consideremos un polinomio irreducible f sobre K con un cero en L, mostraremos que este polinomio se divide sobre L.

Sea $M \supseteq L$ un campo de descomposición para fg sobre K. Supóngase que θ_1 y θ_2 son ceros de f en M. Afirmamos que

$$[(L(\theta_1) : L)] = [(L(\theta_2) : L)]$$

Tenemos ahora una *retícula* importante de subcampos de M, ilustrada mediante el siguiente diagrama.

$$\begin{tikzcd}
 & M & \\
L(\theta_1) \arrow[ur] & & L(\theta_2) \arrow[ul] \\
 & L \arrow[uu] & \\
K(\theta_1) \arrow[uu] \arrow[ur] & & K(\theta_2) \arrow[uu] \arrow[ul] \\
 & K \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

donde todas las flechas en el diagrama indican inclusiones. La afirmación se sigue de cálculos simples respecto de los grados. Así pues par $j = 1, 2$

tenemos.

$$[(L(\theta_j):L)]\,[(L:K)] = [(L(\theta_j):K)] = [(L(\theta_j):K(\theta_j))]\,[(K(\theta_j):K)] \quad (8.1)$$

Ahora por el teorema 4.1.4 $[(K(\theta_1):K)] = [(K(\theta_2):K)]$.

Claramente $L(\theta_j)$ es un campo de descomposición de g sobre $K(\theta_j)$ y por el teorema 3.4.3, tenemos que $K(\theta_1)$ es isomorfo a $K(\theta_2)$ y por el teorema 8.1.3, las extensiones

$$[(L(\theta_j):K(\theta_j))]$$

son isomorfas para $j = 1, 2$; por lo tanto tienen el mismo grado. Substituyendo en la ecuación 8.1 y haciendo unos cálculos obtenemos que

$$[(L(\theta_1):L)] = [(L(\theta_2):L)$$

Pero entonces si $\theta_1 \in L$ se tiene $[(L(\theta_1):L)] = 1$.

Por lo que también$[(L(\theta_2):L)] = 1$ y por lo que $\theta_2 \in L$. Por lo tanto $(L:K)$ es normal. □

8.3 Separabilidad.

Aunque Galois no dio explícitamente el concepto de separabilidad, dado que él únicamente trabajo con el campo de los números complejos (donde como veremos más adelante la separabilidad es automática). Los conceptos de separabilidad y las pruebas de los resultados respecto de este tema involucran el estudio de campos de característica cero.

Definición 8.3.1. Un polinomio irreducible f sobre un campo K es *separable* sobre K, si no tiene ceros múltiples en su campo de descomposición.

Esto hace que f tenga la siguiente forma en su campo de descomposición

$$f(t) = k(t - \sigma_1)\cdots(t - \sigma_n)$$

donde todos los σ_i son distintos.

Definición 8.3.2. Un polinomio irreducible sobre K es *inseparable* sobre K si dicho polinomio no es separable sobre K.

Ejemplos.

1 Un polinomio separable. El polinomio $t^4+t^3+t^2+t+1$ es separable sobre $\mathbb{Q}$, pues este tiene su campo de descomposición dentro de $\mathbb{C}$ donde sus ceros son

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

y todos ellos son diferentes.

2 Un polinomio inseparable. Sea $K_0 = \mathbb{Z}_p$ para algún primo p y $K = K_0(u)$ donde u es trascendental sobre K_0. Sea $f(t) = t^p - u \in K[t]$. Consideremos Ξ un campo de descomposición de f sobre K y sea τ un cero de f en Ξ. Entonces $\tau^p = u$. Tenemos ahora

$$(t-\tau)^p = t^p + \binom{p}{1} t^{p-1}(-\tau) + ... + (-\tau)^p$$

por el teorema del binomio. Pero todos los coeficientes binomiales $\binom{p}{r}$ donde $0 < r < p$ son divisibles por p, dado que en

$$\binom{p}{r} = \frac{p!}{r!(p-r)!}$$

el factor p en el numerador no ocurre en el denominador y como en K cualquier múltiplo de p es cero tenemos que

$$(t-\tau)^p = t^p - \tau^p = t^p - u = f(t)$$

Por lo tanto si $\sigma^p - u = 0$, entonces $(\sigma - \tau)^p = 0$, por lo que $\sigma = \tau$. Por lo tanto todos los ceros de f en Ξ son iguales.

Por lo tanto, solamente nos resta probar que f es irreducible sobre K. Supongamos para ello que no es el caso, es decir $f = gh$ donde $g, h \in K[t]$, y tanto g como h tienen grado menor que f. Por la unicidad de la factorización tenemos que $g(t) = (t-\tau)^s$ donde $0 < s < p$ así pues tenemos que el coeficiente constante de τ^s de g esta en K. Lo anterior implica que $\tau \in K$ pues tenemos que como s y p son primos relativos, entonces existen enteros a, b tal que $as + bp = 1$ y dado que $\tau^{as+bp} \in K$ entonces se sigue que $\tau \in K$, de este modo tenemos que $\tau = v(u)/w(u)$ donde $v, w \in K_0[u]$, por lo tanto

$$v(u)^p - u(w(u))^p = 0$$

Pero los términos de grado menor no se cancelan. Por lo tanto f es irreducible. Por lo tanto f es inseparable sobre K.

8.4 Diferenciación formal.

Para polinomios sobre $\mathbb{R}$ existe un método estándar para detectar ceros múltiples mediante la diferenciación. Este método se puede generalizar a campos arbitrarios pero para ello tenemos que definir la derivada de manera formal.

Definición 8.4.1. Supongamos que $f(t) = a_0 + ... + a_n t^n \in K[t]$, para un campo K. Entonces la *derivada formal* de f es el polinomio

$$Df = a_1 + 2a_2 t + ... + na_n t^{n-1}$$

Cuando $K = \mathbb{R}$ esta definición coincide con la derivada usual, además algunas de las propiedades que satisface la derivada en $\mathbb{R}$ lo sigue cumpliendo nuestra definición. Por ejemplo:

Sean f, g polinomios sobre un campo K entonces tenemos

$$D(f+g) = Df + Dg$$

$$D(f \cdot g) = Df \cdot g + f \cdot Dg$$

y si $\lambda \in K$ entonces

$$D(\lambda) = 0$$

en particular

$$D(\lambda f) = \lambda Df$$

estas propiedades de el pperador D nos dan ahora un criterio para la existencia de ceros múltiples, aunque este criterio no nos dice como encontrarlos.

Lema 8.4.2. *Un polinomio f no cero sobre un campo K, tiene un cero múltiple en un campo de descomposición de f si, y solamente si f y Df tienen un factor común en $K[t]$ de grado mayor o igual a uno.*

Prueba. Primeramente supongamos que f tiene un cero repetido en (de multiplicidad mayor o igual a dos) un campo de descomposición Ξ para f, por lo que en Ξ, f se descompone como

$$f(t) = (t - \alpha)^2 g(t)$$

con $\alpha \in \Xi$, derivando tenemos que

$$Df = (t - \alpha)\left[(t - \alpha)Dg + 2g\right]$$

por lo que f y Df tienen como factor común a $(t-\alpha)$ en $\Xi[t]$, por lo tanto f y Df tienen un factor común en $K[t]$ a saber el polinomio mínimo de α sobre K.

Recíprocamente, ahora supongamos que f no tiene ceros repetidos. Mostraremos por inducción sobre el grado de f que Df y f son coprimos en $\Xi[t]$ y por tanto en $K[t]$.

Si $\partial f = 1$ no hay nada que probar. En otro caso $f(t) = (t - \alpha)g(t)$ donde $(t - \alpha) \nmid g(t)$ por lo que

$$Df = (t - \alpha)Dg + g$$

Ahora bien si un factor de g divide a Df este mismo factor también divide a Dg y como $(t - \alpha)$ no divide a $g(t)$ entonces por hipótesis de inducción como g y Dg son coprimos se tiene que no existen tales factores, por lo tanto f y Df son coprimos. □

Podemos dar ahora condiciones necesarias y suficientes para la separabilidad de un polinomio irreducible.

Proposición 8.4.3. *Si K es un campo de característica cero entonces, cada polinomio irreducible sobre K es separable sobre K. Si K tiene característica $p > 0$ entonces, un polinomio irreducible f sobre K es inseparable si y sólo si*

$$f(t) = k_0 + k_1 t^p + ... + k_r t^{rp}$$

donde $k_0, ..., k_r \in K$.

Prueba. Un polinomio irreducible f sobre K es inseparable si, y sólo si f y Df tienen un factor común de grado mayor o igual a uno. Dado que f es irreducible y Df tiene grado menor que f tenemos que $Df = 0$. Entonces si $f = a_0 + ... + a_n t^n$ tenemos que $na_n = 0$ para todo entero mayor que cero. Para característica cero lo anterior implica que $a_n = 0$ para toda n. Para característica p lo anterior implica que $a_n = 0$ si p no divide a n. Sea $k_i = a_{i_p}$ y el resultado se sigue. □

Definiremos ahora tres usos más del concepto de 'separable'

Definición 8.4.4. Un polinomio sobre un campo K es *separable* sobre K si todos sus factores irreducibles son separables sobre K.

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

Una extensión algebraica $(L : K)$ es una *extensión separable* si cada $\alpha \in L$ es separable sobre K.

Finalmente mostraremos que las extensiones algebraicas separables se 'comen' a los campos intermedios.

Lema 8.4.5. *Sea $(L : K)$ una extensión algebraica separable y M un campo intermedio, es decir $K \subseteq M \subseteq L$. Entonces $(M : K)$ y $(L : M)$ son separables.*

Prueba. Claramente $(M : K)$ es separable. Ahora sea $\alpha \in L$ con m_K y m_M su polinomio mínimo sobre K y M respectivamente. Sabemos que $m_M \mid m_K$

en $M[t]$. Pero α es separable sobre K por lo cual m_K es separable sobre K y esto hace que m_M sea separable sobre M, con ello tener que $(L : M)$ es una extensión separable. □

8.5 Ejercicios.

8.1 Construya subcampos de $\mathbb{C}$ que sean campos de descomposición sobre $\mathbb{Q}$ para los polinomios $f(t) = t^3 - 1$, $g(t) = t^4 + 5t^2 + 6$, $h(t) = t^6 - 8$.

8.2 Encuentre los grados de estas extensiones de campo de $\mathbb{Q}$.

8.3 Construya un campo de descomposición para $t^3 + 2t + 1$ sobre $\mathbb{Z}_3$.

8.4 Construya un campo de descomposición para $t^3 + t^2 + t + 2$ sobre $\mathbb{Z}_3$. ¿Es isomorfa esta construcción a la construcción dada en el ejercicio anterior?.

8.5 Da una lista de todos los polinomios cuadráticos sobre $\mathbb{Z}_5$. ¿Cuales de estos son irreducibles? Construye un campo de descomposición para algunos de estos polinomios irreducibles. ¿Son estos campos isomorfos?.

8.6 Muestra que se puede extender la definición de derivada formal a $K(t)$ definiéndola como

$$D(\frac{f}{g}) = \frac{(f \cdot Dg - g \cdot Df)}{f^2}$$

8.7 ¿Cuales de los polinomios

$f(t) = t^3 + 1$,

$t^2 + 2t - 1$,

$t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$,

$7t^5 + t - 1$

son separables,considerados como polinomios sobre $\mathbb{Q}, \mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{19}$.?

8.8 ¿Cuales de las siguientes extensiones son normales?

a) $(\mathbb{Q}(t):\mathbb{Q})$

b) $\big(\mathbb{Q}(\sqrt{-5}):\mathbb{Q}\big)$

c) $\big(\mathbb{Q}(\sqrt[7]{5}):\mathbb{Q}\big)$

d) $\big(\mathbb{Q}(\sqrt{5},\alpha):\mathbb{Q}\big)$ donde α es como en c)

e) $\big(\mathbb{R}(\sqrt{7}):\mathbb{R}\big)$.

8.9 Muestra que cada extensión de grado dos es normal. ¿Esto es cierto para alguna extensión de grado mayor que dos?.

8.10 Si Ξ es un campo de descomposición para f sobre K, y $K \subseteq L \subseteq \Xi$. Muestra que Ξ es un campo de descomposición para f sobre L.

8.11 Sea f un polinomio de grado n sobre K, y sea Ξ un campo de descomposición de f sobre K. Muestra que $[\Xi:K]$ divide a $n!$.

8.12 Dí si las siguientes afirmaciones son verdaderas o falsas.

a) Todo polinomio se divide sobre algún campo.

b) El polinomio t^3+5 es separable sobre $\mathbb{Z}_7$.

c) Los campos de descomposición son únicos salvo isomorfismo.

d) Toda extensión finita es normal.

e) Toda extensión separable es normal.

f) Toda extensión normal finita es el campo de descomposición de algún polinomio.

g) $(\mathbb{Q}(\sqrt{19}):\mathbb{Q})$ es una extensión normal separable.

h) $(\mathbb{Q}(\sqrt{21}):\mathbb{Q})$ es una extensión normal separable.

i) Un polinomio irreducible no puede ser separable.

j) Si $Df=0$ entonces $f=0$, para un polinomio f sobre un campo.

Capítulo 9

Grado de un campo y orden de un grupo.

En la prueba de el *Teorema Fundamental de la Teoría de Galois* dado en el capítulo 11 necesitaremos mostrar que si H es un subgrupo de el grupo de Galois de una extensión normal separable $(L : K)$, entonces $H^{\dagger *} = H$. El método a utilizar es probar que tanto H como $H^{\dagger *}$ son grupos finitos y tienen el mismo orden y dado que $H \subseteq H^{\dagger *}$ entonces los dos grupos son el mismo (Es muy importante el trabajar con *extensiones finitas* y grupos *finitos.* pues podemos tener el caso en que un conjunto infinito este contenido en otro de la misma cardinalidad pero estos no sean iguales (en cuanto a alguna estructura dada). Por ejemplo $\mathbb{Z} \subseteq \mathbb{Q}$ y ambos conjuntos tienen la misma cardinalidad).

El objetivo de este capítulo es el de establecer técnicas para calcular el orden de $H^{\dagger *}$, además encontraremos el grado de $\left[(H^{\dagger} : K)\right]$ en términos de el orden de H. En el siguiente capítulo encontraremos el orden de $H^{\dagger *}$ en términos de su grado y juntando estas piezas daremos el resultado deseado.

Este primer resultado se debe a *Dedekind* que hizo el estudio sistemático de el estudio de los automorfismos de campo.

Lema 9.0.1 (Dedekind). *Si K y L son campos, entonces cada conjunto de* *monomorfismos de $K \longrightarrow L$ distintos es linealmente independiente sobre L.*

Prueba. Sean $\lambda_1, \ldots, \lambda_n$ distintos monomorfismos de $K \longrightarrow L$, decir que este conjunto es linealmente independiente sobre L, es lo mismo que decir que no existen elementos $a_1, ..., a_n \in L$ tal que

$$a_1\lambda_1(x) + ... + a_n\lambda_n(x) = 0 \tag{9.1}$$

para toda $x \in K$, salvo que todas las a_i sean cero.

Supongamos lo contrario, es decir que la ecuación 9.1 se satisface, donde alguna de las a_i es no cero. Sin perdida de generalidad podemos suponer que todas las a_i son distintas de cero (las que no ean cero podemos excluirlas). De todas las ecuaciones de la forma de la ecuación 9.1, que se satisfacen con todas las $a_i \neq 0$ existe una que es menor ó para la cual el número n de términos es menor. Elegimos esta expresión y supongamos que es la misma que la dada en la ecuación 9.1.

Por lo que podemos asumir que no existe una ecuación que satisface 9.1, con menos de n términos. Haremos ahora una deducción por contradicción.

Sabemos que existe $0 \neq y \in K$ tal que $\lambda_1(y) \neq \lambda_n(y)$ pues $\lambda_1 \neq \lambda_n$. Ahora bien 9.1 se satisface también si remplazamos a x por xy, por lo que:

$$a_1\lambda_1(xy) + ... + a_n\lambda_n(xy) = 0$$

para todo $x \in K$ por lo que:

$$a_1\lambda_1(y)\lambda_1(x) + \cdots + a_n\lambda_n(y)\lambda_n(x) = 0 \tag{9.2}$$

para toda $x \in K$ si multiplicamos 9.1 por $\lambda_1(y)$ y se la restamos a 9.2 obtenemos que

$$a_2(\lambda_2(x)\lambda_1(y) - \lambda_2(x)\lambda_2(y)) + ... + a_n(\lambda_n(x)\lambda_1(y) - \lambda_n(x)\lambda_n(y)) = 0$$

El coeficiente de $\lambda_n(x)$ es $a_n\,[\lambda_1(y) - \lambda_n(y)]$. Por lo que tenemos una ecuación de la forma 9.1, con menos términos, lo cual contradice la suposición hecha anteriormente.

Consecuentemente no existe ninguna ecuación de la forma 9.1 y esto implica que los monomorfismos son linealmente independientes. ☐

Para un primer resultado importante necesitamos dos lemas. El primero es un resultado estándar de el álgebra lineal motivo por el cual omitiremos la prueba.

Lema 9.0.2. *Un sistema de m ecuaciones homogéneas*

$$a_{m1}x_1 + ... + a_{mn}x_n = 0$$

en n variables $x_1, ...x_n$ con coeficientes a_{ij} tomados en un campo tiene una solución (que no sea con $x_i = 0$ para toda i) si $n > m$.

Este teorema se prueba en al menos un primer curso de álgebra lineal (ver Halmos[11]pag.91).

El segundo lema es un principio muy general.

Lema 9.0.3. *Si G es un grupo finito cuyos elementos distintos son $g_1, ..., g_n$. Entonces para un elemento fijo $g \in G$ se tiene que la función $f_g : G \longrightarrow G$ dada por $f_g(h) = gh$ para $h \in G$ es un isomorfismo de grupos (en este caso un automorfismo de grupos).*

Prueba. Es mera rutina probar que la función dada y la función $f_{g^{-1}} : G \longrightarrow G$ (donde g^{-1} es el inverso de g en G), dada por $f_{g^{-1}}(h) = g^{-1}(h)$ son homomorfismos de grupo, donde f_g y $f_{g^{-1}}$ son uno el inverso de el otro. ☐

Requerimos ahora una notación.

Notación. La *cardinalidad* de un conjunto S será denotada por $|S|$. Por lo que si G es un grupo entonces $|G|$ denotará el orden de G.

Estamos en condiciones de poder probar el teorema principal de este capítulo.

Teorema 9.0.4. *Sea G un subgrupo finito de el grupo de automorfismos de un campo K, y sea K_0 el campo fijo de G. Entonces*

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

Prueba. Sea $n = |G|$, y supongamos que los elementos de G son $g_1, \ldots, g_n$, donde g_1 denota al elemento neutro en G.

Primeramente supongamos que $[(K : K_0)] = m < n$. Consideramos una base $\{x_1, ..., x_m\}$ para K sobre K_0. Por el lema 9.0.2 podemos encontrar $y_1, ..., y_n$ en K no todos cero, tal que

$$g_1(x_j)y_1 + ... + g_n(x_j)y_n = 0 \tag{9.3}$$

para $j = 1, ...m$. Tomamos en elemento a en K entonces

$$a = \alpha_1 x_1 + ... + \alpha_m x_m$$

donde $\alpha_1, ..., \alpha_m \in K$. Por lo que

$$\begin{aligned} g(a)y_1 + ... + g_n(a)y_n &= g_1\left(\sum_l \alpha_l x_l\right) y_1 + ... + g_n\left(\sum_l \alpha_l x_l\right) y_n \\ &= \sum_l \alpha\left(g_1(x_l)y_1 + ... + g_n(x_l)y_n\right) \\ &= 0 \end{aligned}$$

usando la ecuación 9.3. Por lo que los distintos monomorfismos $g_1, ..., g_n$ son linealmente dependientes, contrario a el lema 9.0.1. Por lo tanto tenemos que $m \geq n$.

Para la segunda desigualdad nuevamente supongamos que $[(K : K_0)] = m > n$. Por lo que tenemos que existe un conjunto de $n + 1$ elementos de K que son linealmente independientes sobre K_0, consideremos tal conjunto $\{x_1, ..., x_{n+1}\}$. Por el lema 9.0.2, tenemos que existen $y_1, ..., y_{n+1} \in K$, no todos cero, tal que para $j = 1, ..., n$

$$g_j(x_1)y_1 + ... + g_j(x_{n+1})y_{n+1} = 0. \tag{9.4}$$

Habremos de utilizar un procedimiento similar al utilizado en la prueba de el lema 9.0.1. De esta manera elegimos de todas las combinaciones de n elementos de K que satisfacen la ecuación 9.4, aquella que tiene el menor número posible de elementos no cero. Así pues tenemos elementos $y_1, ..., y_{n+1} \in K$ con

$$y_1, ..., y_r \neq 0, \quad y_{r+1}, ..., y_{n+1} = 0$$

De esta manera la ecuación 9.4 se convierte en

$$g_j(x_1)y_1 + ... + g_j(x_r)y_r = 0. \tag{9.5}$$

Ahora tomemos $g \in G$ y lo aplicamos en la ecuación 9.5. Esto nos da un sistema de ecuaciones.

$$gg_j(x_1)g(y_1) + ... + gg_j(x_r)g(y_r) = 0.$$

Por el lema 9.0.3, como j es la variable en este sistema tenemos que, el sistema anterior de ecuaciones es equivalente a

$$g_j(x_1)g(y_1) + ... + g_j(x_r)g(y_r) = 0. \tag{9.6}$$

Si multiplicamos la ecuación 9.5, por $g(y_1)$ y la ecuación 9.6, por y_1, y las restamos obtenemos que

$$g_j(x_2)(y_2 g(y_1) - g(y_2)y_1) + ... + g_j(x_r)(y_r g(y_1) - g(y_1)y_r) = 0.$$

Este sistema de ecuaciones es similar a la ecuación 9.5, pero con menos términos lo cual da una contradicción salvo que todos los términos

$$y_i g(y_1) - y_1 g(y_i)$$

sean cero. Pero si esto sucede entonces

$$y_i y_1^{-1} = g(y_i y_1^{-1})$$

para todo $g \in G$, por lo que $y_i y_1^{-1} \in K_0$. Por lo que existen $z_1, ..., z_r \in K_0$ y un elemento $k \in K$, tal que $y_i = kz_i$ para toda i. Entonces la ecuación 9.5, toma la forma

$$x_1 k z_1 + ... + x_r k z_r = 0$$

y dado que $k \neq 0$ podemos dividir por k, lo que muestra que las x_i son linealmente dependientes sobre K_0. Lo que es una contradicción. Por lo que $[(K : K_0)] = m \leq n$ y por la primera parte de la prueba tenemos que:

$$[(K : K_0)] = m = n = |G|.$$

□

Corolario 9.0.5. Si G es el grupo de Galois de la extensión finita $(L : K)$ y H es un subgrupo finito de G entonces

$$\left[(H^\dagger : K)\right] = \frac{[(L : K)]}{|H|}.$$

Prueba.

$$\left[(H^\dagger : K)\right] = \frac{[(L : K)]}{[(L : H^\dagger)]} = \frac{[(L : K)]}{|H|}$$

la última desigualdad se da por el teorema anterior. □

Ejemplos.

Ilustraremos el teorema 9.0.4 mediante dos ejemplos, uno que es muy simple y el otro un poco más de complejidad.

1. Sea G el grupo de automorfismos de $\mathbb{C}$ consistente de el automorfismo identidad y la conjugación compleja. El campo fijo de G es $\mathbb{R}$ pues si $x - yi = x + yi$ (con $x, y \in \mathbb{R}$) entonces $y = 0$, y el reciproco también se vale. Por lo tanto $[\mathbb{C} : \mathbb{R}] = |G| = 2$.

2 Sea $K = \mathbb{Q}(\omega)$ donde $\omega = e^{2\pi i/5} \in \mathbb{C}$. Como $\omega^5 = 1$ y $\mathbb{Q}(\omega)$ consiste de todos los elementos de la forma

$$p + q\omega + r\omega^2 + s\omega^3 + t\omega^4 \tag{9.7}$$

donde $p, q, r, s, t \in \mathbb{Q}$. El grupo de Galois de $(\mathbb{Q}(\omega) : \mathbb{Q})$ es fácil de encontrar, puesto que si α es un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\omega)$ entonces $(\alpha(\omega))^5 = \alpha(\omega^5) = \alpha(1) = 1$, por lo que $\alpha(\omega) = \omega, \omega^2, \omega^3$ ó ω^4. esto da solamente cuatro candidatos para ser $\mathbb{Q}$-automorfismo:

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

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

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

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

Es fácil de verificar que todos estos mapeos son todos los $\mathbb{Q}$-automorfismos. Por lo que el grupo de Galois de $(\mathbb{Q}(\omega) : \mathbb{Q})$ tiene orden cuatro. El campo fijo de este grupo de Galos es fácil de calcular, por lo que se pide al lector verificar que dicho campo es $\mathbb{Q}$. De este modo por el teorema 9.4, tenemos que $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$.

Un primer 'staik' cometido es el hecho de que en vista de la ecuación 9.7, cada elemento de la extensión puede ser escrito en términos de los cinco elementos de la base; es decir el grado de la extensión es cinco, el 'supuesto' error que se cometió es el de considerar a ω como un cero de el polinomio $t^5 - 1$, un lector astuto pudo darse cuenta que aquí esta el problema pues, $t^5 - 1$ *no* es el polinomio mínimo de ω sobre $\mathbb{Q}$, dado que este polinomio es reducible, el polinomio mínimo de hecho es

$$t^4 + t^3 + t^2 + t + 1$$

el cual tiene grado cuatro. Así pues la ecuación 9.7, se satisface pero los elementos de la supuesta base son linealmente dependientes ya que

$$\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$$

Por lo que cada elemento de $\mathbb{Q}(\omega)$ puede ser expresado de manera única de la forma

$$p + q\omega + r\omega^2 + s\omega^3$$

donde $p, q, r, s \in \mathbb{Q}$. Dimos este ejemplo de esta manera, para poder ilustrar al lector acerca de los errores que son comunes en la realización de los cálculos.

9.1 Ejercicios.

9.1 Verifique el teorema 9.04 para la extensión de el Ejercicio 7.1 y sus grupos de Galois.

9.2 Encuentra el campo fijo de el subgrupo $\{\alpha_1, \alpha_4\}$ para el segundo de los ejemplos anteriores. Verifique que el teorema 9.04 se satisfaga.

9.3 Desarrolle de manera similar al ejemplo 2 de la sección anterior, pero ahora para $\omega = e^{2\pi i/7}$.

9.4 Encuentre todos los monomorfismos de $\mathbb{Q} \longrightarrow \mathbb{C}$.

9.5 Encuentre todos los monomorfismos de anillos de $\mathbb{Z} \longrightarrow \mathbb{Q}$.

9.6 Muestra que un monomorfismo de anillos de $\mathbb{Z} \longrightarrow K$, donde K es un campo, extiende a un único monomorfismo de campos entre $\mathbb{Q} \longrightarrow K$. ¿Sera cierto lo anterior si K no es un campo.?

9.7 Diga si las siguientes afirmaciones son verdaderas ó falsas.

a) Si $S \subseteq T$ es un conjunto finito y $|S| = |T|$ entonces $S = T$.

b) Será cierto el ejercicio anterior para conjuntos infinitos.

c) Existe un único monomorfismo de $\mathbb{Q} \longrightarrow \mathbb{Q}$.

d) Hay precisamente p automorfismos de $\mathbb{Z}_p$.

e) Si K y L son campos existe al menos un monomorfismo de $K \longrightarrow L$.

f) Si K y L son campos y existe un monomorfismo entre ellos, entonces ambos tienen la misma característica.

g) Si K y L son campos con la misma característica entonces existe un monomorfismo entre ellos.

h) Si K es un campo de característica p entonces existe un monomorfismo de $\mathbb{Z}_p \longrightarrow K$.

i) Automorfismos distintos de un campo son linealmente independientes sobre K.

j) Monomorfismos linealmente independientes son distintos.

Capítulo 10

Monomorfismos y cerradura normal.

El tema de este capítulo, es el de la construcción de automorfismos, para dar con estos algunos resultados técnicos. Iniciaremos con la generalización de K-automorfismo, con los K-monomorfismos. Para extensiones normales usaremos los K-monomorfismos en lugar de los K-automorfismos. Usando esto podremos calcular el orden de el grupo de Galois de una extensión normal separable finita, este resultado combinado con los resultados de el capítulo 9, forman una parte crucial de el Teorema Fundamental de el capítulo 11.

También introduciremos el concepto de *cerradura normal* de una extensión finita. El uso de esta cerradura normal radica en que existen obstrucciones de el tipo técnico causadas por las extensiones no normales.

10.1 K-monomorfismos

Iniciaremos con la generalización de la idea de K-automorfismo de un campo L.

Definición 10.1.1. Supongamos que K es un subcampo de M y también es subcampo de L. Entonces un K-*monomorfismo* de M en L es una función

$\phi : M \longrightarrow L$ la cual es un monomorfismo de campo tal que para cada $k \in K$, $\phi(k) = k$.

En general si $K \subseteq M \subseteq L$ entonces un K-automorfismo de L restringe a un K-monomorfismo de $M \longrightarrow L$. De particular interés es cuando este proceso puede ser invertido.

Teorema 10.1.2. *Supongamos que $(L : K)$ es una extensión normal finita y $K \subseteq M \subseteq L$. Si τ es un K-monomorfismo de $M \longrightarrow L$. Entonces existe un K-automorfismo σ de L tal que $\sigma|_M = \tau$.*

Prueba. Por el teorema 8.2.2, L es un campo de descomposición sobre K para algún polinomio f sobre K, por lo que simultáneamente también es campo de descomposición sobre M para f y sobre $\tau(M)$ para f. Pero $\tau|_K$ es la identidad por lo que $\tau(f) = f$. Se tiene además el diagrama

$$\begin{array}{ccc} M & \longrightarrow & L \\ {\scriptstyle\tau}\Big\downarrow & & {\scriptstyle\sigma}\Big\downarrow \\ \tau(M) & \longrightarrow & L \end{array}$$

Por el teorema 8.1.5, existe un isomorfismo $\sigma : L \longrightarrow L$ tal que $\sigma|_M = \tau$. Por lo cual σ es un automorfismo de L y dado que $\sigma|_K = \tau|_K$ es la identidad, se tiene que σ es un K-automorfismo de L. $\square$

Este resultado puede ser usado para construir K-automorfismos de la siguiente manera.

Proposición 10.1.3. *Supongamos que $(L : K)$ es una extensión normal finita y que α, β son ceros en L de el polinomio irreducible p sobre K. Entonces existe un K-automorfismo σ de L tal que $\sigma(\alpha) = \beta$.*

Prueba. Por el teorema 3.4.5, existe un isomorfismo $\tau : K(\alpha) \longrightarrow K(\beta)$ tal que $\tau|_K$ es la identidad y $\sigma(\alpha) = \beta$. Por el teorema anterior τ extiende a un K-automorfismo σ de L. $\square$

10.2 Cerradura normal.

Cuando las extensiones no son normales podemos recobrar la normalidad mediante una extensión mayor.

Definición 10.2.1. Sea L una extensión normal algebraica de K. Una *cerradura normal* de $(L : K)$ es una extensión N de L tal que

(1) $(N : K)$ es normal.

(2) Si $L \subseteq M \subseteq N$ y $(M : K)$ es normal entonces $M = N$.

Por lo que N es la más pequeña extensión de L que es normal sobre K.

El siguiente teorema garantiza la suficiencia de cerraduras normales.

Teorema 10.2.2. *Si $(L : K)$ es una extensión finita entonces existe una cerradura normal N que es una extensión finita sobre K, Si M es otra cerradura normal entonces las extensiones $(M : K)$ y $(N : K)$ son isomorfas.*

Prueba. Sea $\{x_1, ..., x_r\}$ una base para L sobre K, y m_i el polinomio mínimo de x_i sobre K. Sea N un campo de descomposición de el polinomio $f = m_1 \cdots m_r$ sobre L. Entonces N es también un campo de descomposición para f sobre K por lo que por el teorema 8.2.2, la extensión $(N : K)$ es normal y finita.

Supongamos que $L \subseteq P \subseteq N$ donde $(P : K)$ es normal. Cada polinomio m_i tiene un cero $x_i \in P$, por la normalidad tenemos que f se divide en P. Dado que N es un campo de descomposición para f tenemos que $P = N$. Así pues N es una cerradura normal.

Ahora supongamos que M y N ambas son cerraduras normales. El polinomio anterior f se divide en M y en N, por lo que M y N contienen un campo de descomposición de f sobre K. Este campo de descomposición contiene a L y es normal sobre K. Por lo que es igual a M y a N respectivamente. La unicidad de los campos de descomposición (teorema 8.1.5) nos dice que $(M : K)$ y $(N : K)$ son isomorfos. □

Por ejemplo, consideremos $(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ esta extensión no es normal, como podemos ver. Si consideramos a K como un campo de descomposición para $t^3 - 2$ sobre $\mathbb{Q}$ contenido en $\mathbb{C}$, entonces

$$K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$$

donde $\omega = -1 + i\sqrt{3}/2$ es una raíz cubica compleja de 2. Ahora tenemos que K es una cerradura normal, adjuntándole todos los ceros que le faltan.

Lema 10.2.3. *Supongamos que $K \subseteq L \subseteq N \subseteq M$ donde $(L : K)$ es finita y N es una cerradura normal de $(L : K)$. Si τ es un K-monomorfismo de L en M. Entonces $\tau(L) \subseteq N$.*

Prueba. Sea $\alpha \in L$. Entonces α tiene un polinomio mínimo m sobre K. Entonces $0 = m(\alpha) = \tau(m(\alpha)) = m(\tau(\alpha))$ por lo que $\tau(\alpha)$ es un cero de m, y además esta dentro de N ya que $(N : K)$ es normal. Des este modo tenemos que $\tau(L) \subseteq N$. $\square$

Este resultado marca un poco la importancia de la cerradura normal de una extensión dada. El siguiente resultado es un recíproco al resultado anterior un tanto debíl.

Teorema 10.2.4. *Para una extensión finita $(L : K)$ las siguientes condiciones son equivalentes:*

(1) $(L : K)$ es normal.

(2) Existe una extensión normal N de K que contiene a L tal que cada K-monomorfismo $\tau : L \longrightarrow N$ es un K-automorfismo de L

(3) Para cada extensión normal M de K que contiene a L cada K-monomorfismo $\tau : L \longrightarrow M$ es un K-automorfismo de L.

Prueba. Probaremos (1) implica, (3) implica, (2) implica, (1).
(1) $\Longrightarrow$ (3) Si $(L : K)$ es normal, entonces L es una cerradura normal de $(L : K)$ por lo que por el lema 10.2.3, $\tau(L) \subseteq L$. Pero τ es un mapeo K-lineal definido en el espacio vectorial dimensionalmente finito L sobre K y es

un monomorfismo, por lo que $\tau(L)$ tiene la misma dimensión que L. Por lo tanto $\tau(L) = L$ y de este modo τ es un K-automorfismo de L.
(3) $\Longrightarrow$ (2) Sea N una cerradura normal de $(L : K)$ que existe por teorema 10.2.2.
(2) $\Longrightarrow$ (1) Supongamos que f es un polinomio irreducible sobre K con un cero $\alpha \in L$. Entonces f se divide sobre N por normalidad, y si β es un cero de f en N entonces por la proposición 10.1.3, tenemos que existe un automorfismo σ de N tal que $\sigma(\alpha) = \beta$. Por hipótesis σ es un K automorfismo de L, por lo que $\beta = \sigma(\alpha) \in \sigma(L) = L$. De este modo f se divide sobre L y $(L : K)$ es normal. □

Nuestro siguiente resultado requiere hacer unos cálculos.

Teorema 10.2.5. *Supongamos que $(L : K)$ es una extensión finita separable de grado n. Entonces existen precisamente n distintos K-monomorfismos de L en una cerradura normal N (y por lo tanto para cada extensión normal M de K que contenga a L.*

Prueba. La prueba la haremos por inducción sobre $[L : K]$. Si $[L : K] = 1$ el resultado es claro. Supongamos que $[L : K] = k > 1$. Sea $\alpha \in L/K$ con polinomio mínimo m sobre K. Entonces $\partial m = [K(\alpha) : K] = r > 1$. Ahora m es un polinomio irreducible separable con un cero en la extensión normal N, por lo que m se divide en N y sus ceros $\alpha_1, ..., \alpha_r$ son distintos. Por hipótesis de inducción existen precisamente $'s'$ distintos $K(\alpha)$-monomorfismos digamos $\rho_1, ..., \rho_s : L \longrightarrow N$, donde $s = [L : K(\alpha)] = k/r$. Por la proposición 10.1.3, existen r distintos K-automorfismos $\tau_1, ...\tau_r$ de N, tal que $\tau_i(\alpha) = \alpha_i$. Los mapeos

$$\phi_{ij} = \tau_i \rho_j$$

dan $k = rs$ distintos K-monomorfismos de L en N. Mostraremos que estos son todos los distintos K-monomorfismos de L en N.

Sea $\tau : L \longrightarrow N$ un K-monomorfismo. Entonces $\tau(\alpha)$ es un cero de m en

N, por lo que $\tau(\alpha) = \alpha_i$ para algún i. El mapeo $\phi = \tau_i^{-1}\tau$ es un $K(\alpha)$-monomorfismo de L en N, por lo que por hipótesis de inducción $\phi = \rho_j$ para algún j. Esto hace que $\tau = \tau_i\rho_j = \phi_{ij}$, lo cual termina la prueba. □

Estamos en este momento en posición de calcular el orden de el grupo de Galois de una extensión normal separable finita.

Corolario 10.2.6. Si $(L : K)$ es una extensión normal separable finita de grado n entonces existen precisamente n distintos K-automorfismos de L, por lo que $|\Gamma(L : K)| = n$.

Prueba. Es consecuencia inmediata de los teoremas 10.2.4 y 10.2.5 □

De este corolario se deduce un importante

Teorema 10.2.7. *Sea $(L : K)$ es una extensión finita con grupo de Galois G. Si $(L : K)$ es normal y separable entonces K es el campo fijo de G.*

Prueba. Sea K_0 el campo fijo de G, y sea $[L : K] = n$. Por el corolario 10.2.6, tenemos que $|G| = n$. Por el teorema 9.0.4, $[L : K] = n$. Dado que $K \subseteq K_0$ tenemos que $K = K_0$. □

Existe un recíproco de este resultado el cual muestra que podemos considerar extensiones normales y separables en algún orden para tener la correspondencia de Galois como una biyección. Más adelante probaremos este recíproco.

Teorema 10.2.8. *Supongamos que $K \subseteq L \subseteq M$, con $(M : K)$ finita, y que $[L : K] = n$. Entonces existen a lo más n, K-monomorfismos de L en M.*

Prueba. Sea N una cerradura normal de $(M : K)$. Entonces $(N : K)$ es finita por el teorema 10.2.2, y cada K-monomorfismo de L en M es también un K-monomorfismo de L en N. Por lo que podemos asumir que M es una extensión normal de K, solamente reemplazamos M por N. El argumento restante de la prueba se sigue por inducción sobre $[L : K]$ como en la prueba de el teorema 10.2.5, excepto que lo que podemos deducir es que existen s'

$K(\alpha)$-monomorfismos de L en N, donde $s' \leq s$ (por inducción) y que existen r' distintos K-automorfismos de N, donde $r' \leq r$ (dado que los ceros de m en N no son necesariamente distintos). Y el resto de el argumento es verdadero. □

Note que si $(L : K)$ no es separable entonces existen menos de n K-monomorfismos de L en M, dado que r' es definitivamente menor que r para alguna elección de α.

Teorema 10.2.9. *Si $(L : K)$ es una extensión finita con grupo de Galois G y si K es el campo fijo de G entonces $(L : K)$ es normal y separable.*

Prueba. Por el teorema 9.0.4, $[L : K] = |G| = n$. Entonces hay exactamente n, distintos K-monomorfismos de L en L que son los elementos de el grupo de Galois. Pero como notamos en la prueba de 10.2.8, si $(L : K)$ no es separable entonces hay menos de n, K-monomorfismos de L en L. Por lo que $(L : K)$ es separable.
Ahora probaremos la normalidad, usando 10.2.4. Consideremos a N una extensión normal de K que contiene a L y sea τ un K-monomorfismo de L en N. Dado que cada elemento de el grupo de Galois de $(L : K)$ define un K-homomorfismo de L en N hay n K-monomorfismos de L en N que son automorfismos de L. Pero por el teorema 10.2.8, τ puede tomar a lo más n valores pero τ es uno de estos monomorfismos. Por lo tanto τ es un automorfismo de L. Por el teorema 10.2.4, tenemos que $(L : K)$ es normal. □

Si la correspondencia de Galois es una biyección entonces K es el campo fijo de el grupo de Galois de $(L : K)$, por lo anterior sabemos que $(L : K)$ es separable y normal. De este modo tenemos que estas condiciones son suficientes para que la correspondencia de Glois sea una biyección y esto será probado en el siguiente capítulo.

10.3 Ejercicios.

10.1 Supongamos que $(L : K)$ es finita. Muestre que cada K-monomorfismo de L en L es un automorfismo. ¿Será cierto este resultado si la extensión no es finita.?

10.2 Construya cerraduras normales N para las siguientes extensiones:

a) $(\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q})$.

b) $(\mathbb{Q}(\sqrt[7]{2}) : \mathbb{Q})$.

c) $(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$.

d) $(\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) : \mathbb{Q})$.

e) $(\mathbb{Q}(\gamma) : \mathbb{Q})$ donde γ es cero de $t^3 - 3t^2 + 3$.

10.3 Encuentra los grupos de Galois de las extensiones (a), (b), (c) y (d) de el ejercicio anterior.

10.4 Encuentra el grupo de Galois de las extensiones $(N : \mathbb{Q})$ par las cerraduras normales N.

10.5 Muestra que el lema 10.2.3, no es cierto si no asumimos que $(N : K)$ es normal. Pero es cierto para una extensión N de L tal que $(N : K)$ es normal, justamente para una cerradura normal.

10.6 Use el corolario 10.2.6, para encontrar el orden de el grupo de Galois de $(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q})$.

10.7 Marque verdadero o falso según sea el caso.

a) Cada K-monomorfismo es un K-automorfismo.

b) Toda extensión finita tiene una cerradura normal.

c) Si $K \subseteq L$ y σ es un K-automorfismo de L, entonces $\sigma|_K$ es un K-automorfismo de K.

d) Toda extensión en un campo de característica cero es normal.

e) Una extensión que tiene grupo de Galois de orden uno es normal.

f) Una extensión normal y separable tiene grupo de Galois finito.

g) Todo grupo de Galois es abeliano.

h) La correspondencia de Galois falla para extensiones no normales.

i) Una extensión finita y separable de grado n tiene grupo de Galois de orden n.

j) El grupo de Galois de una extensión normal es cíclico.

Capítulo 11

La correspondencia de Galois.

Estamos en este momento en condiciones de establecer las propiedades de la correspondencia de Galois entre una extensión de campos y su grupo de Galois. Mucho de el trabajo para reunir estas propiedades ya está hecho en los capítulos anteriores y en este capítulo principalmente uniremos las piezas.

Recordaremos alguna notación cada en el capítulo 7. Si $(L : K)$ es una extensión de campos con grupo de Galois G, el cual consiste de todos los K-automorfismos de L.

$\mathfrak{F}$ denota al conjunto de todos los campos intermedios M entre K y L

$\mathfrak{G}$ denota al conjunto de todos los subgrupos H de G.

Tenemos además definidas las transformaciones.

$$* : \mathfrak{F} \longrightarrow \mathfrak{G}$$

y

$$\dagger : \mathfrak{G} \longrightarrow \mathfrak{F}$$

de la siguiente manera:

Para $M \in \mathfrak{F}$ entonces M^* es el grupo de todos los M-automorfismos de L.

Y para $H \in \mathfrak{G}$ entonces $H^\dagger$ es el campo que fijan los elementos de H.

También habíamos visto que los mapeos * y † son inclusiones inversas, es decir que $M \subseteq M^{*\dagger}$, y $H \subseteq H^{\dagger *}$.

Daremos un último resultado de tipo técnico antes de dar el *Teorema Fundamental de la Teoría de Galois.*

Lema 11.0.1. *Supóngase que $(L : K)$ es una extensión finita, separable y normal, M un campo intermedio, y τ un K-automorfismo de L. Entonces*

$$(\tau(M))^* = \tau M^* \tau^{-1}$$

Prueba. Llamemosle $M' = \tau(M)$ y tomemos $\gamma \in M^*$, $x_1 \in M'$. Entonces $x_1 = \tau(x)$ para algún $x \in M$. Entonces

$$(\tau\gamma\tau^{-1})(x) = \tau\gamma(x) = \tau(x) = x_1$$

por lo que

$$\tau M^* \tau^{-1} \subseteq {M'}^*.$$

De manera similar

$$\tau^{-1} {M'}^* \tau \subseteq M^*,$$

por lo que

$$\tau M^* \tau^{-1} \supseteq {M'}^*,$$

lo cual concluye la prueba. □

Teorema 11.0.2 (Fundamental de la Teoría de Galois). *Sea $(L : K)$ una extensión de campos finita, separable y normal de grado n con grupo de Galois G; si $\mathfrak{F}$, $\mathfrak{G}$ están definidos como antes entonces:*

(1) El grupo de Galois G tiene orden n.

(2) Los mapeos * y † son inversas naturales y es una correspondencia 1-1 que preserva el orden entre $\mathfrak{F}$ y $\mathfrak{G}$.

(3) Si M es un campo intermedio entonces.

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

y

$$[M:K] = \frac{|G|}{|M^*|}.$$

(4) Un campo intermedio M es una extensión normal de K si, y solamente si M^* es un subgrupo normal de G (normal en el sentido usual de la teoría de grupos).

(5) Si un campo intermedio M es una extensión normal de K entonces el grupo de Galois de $(M : K)$ es isomorfo a el grupo cociente G/M^*.

Prueba. La primera parte es precisamente el corolario 10.2.6. Para la segunda parte, tenemos por el teorema 8.4.5, que $(L : M)$ es separable y por el teorema 8.2.2, $(L : M)$ claramente es normal. Por el teorema 10.2.7, M es el campo fijo de M^*. De este modo

$$M^{*\dagger} = M. \tag{11.1}$$

Ahora consideremos $H \in \mathfrak{G}$. Sabemos que $H \subseteq H^{\dagger *}$, de donde:

$$H^{\dagger * \dagger} = (H^\dagger)^{*\dagger} = HH^\dagger$$

por la ecuación 11.1.

Por el teorema 9.0.4, tenemos que:

$$|H| = [K : H^\dagger].$$

por lo que

$$|H| = [K : H^{\dagger * \dagger}]$$

nuevamente por el teorema 9.0.4 se tiene que

$$[K : H^{\dagger * \dagger}] = |H^{\dagger *}|$$

por lo que

$$|H| = |H^{\dagger *}|.$$

Dado que H y $H^{\dagger *}$ son grupos finitos y $H \subseteq H^{\dagger *}$ tenemos que

$$H = H^{\dagger *}.$$

Por lo tanto la segunda parte de el teorema se sigue.

Para la tercera parte, notemos de nuevo que $(L : M)$ es separable y normal. Por el corolario 10.2.6, $[L : M] = |M^*|$, y la otra igualdad se sigue inmediatamente.

Note que $|G|/|M^*|$ es el índice de M^* en G en el sentido usual de la teoría de grupos.

Ahora probaremos la cuarta parte de el teorema. Si $(M : K)$ es normal, y $\tau \in G$. Entonces $\tau|_M$ es un K-monomorfismo de M en L, por lo que por el teorema 10.2.4, τ es también un K-automorfismo de M. Por lo tanto $\tau(M) = M$. Por el lema 11.0.1, tenemos que $\tau M^* \tau^{-1} = M^*$, esto implica que M^* es un subgrupo normal de G.

Recíprocamente supongamos que M^* es un subgrupo normal de G. Y sea σ un K-monomorfismo de M en L. Por el teorema 10.1.2, existe un K-automorfismo τ de L tal que $\tau|_M = \sigma$. Ahora $\tau M^* \tau^{-1} = M^*$ dado que M^* es un subgrupo normal de G, por lo que por el lema 11.0.1, $(\tau(M))^* = M^*$. Por la parte dos de este teorema tenemos que $\tau(M) = M$. Por lo tanto $\sigma(M) = M$. De este modo tenemos que σ es un K-automorfismo de M. Por el teorema 10.2.4, $(M : K)$ es normal.

Finalmente probaremos la parte 5 de el teorema, sea G' el grupo de Galois de $(M : K)$. Podemos definir una función $\phi : G \longrightarrow G'$ dado por

$$\phi(\tau) = \tau|_M \quad (\tau \in G).$$

Esta función es claramente un homomorfismo de grupos de G a G', por el teorema 10.2.4, $\tau|_M$ es un$K$-automorfismo de M, por el teorema 10.1.2, ϕ es suprayectivo. El núcleo de ϕ es claramente M^*. Por lo que por un resultado estándar de teoría de grupos se sigue que

$$G' = im(\phi) \cong G/Nuc(\phi) = G/M.$$

□

Capítulo 12

Un ejemplo importante.

En este capítulo daremos un ejemplo, para ver un poco los alcances de el teorema dado en el capítulo anterior. Es de considerable importancia verificar todas las hipótesis dadas en el teorema pues si no lo hacemos con cuidado podemos pensar que la información obtenida es muy sencilla, por lo que enumeraremos los pasos desarrollados.

1. Consideremos el polinomio $f(t) = t^4 - 2$ sobre $\mathbb{Q}$, y sea K un campo de descomposición para f tal que $K \subseteq \mathbb{C}$. En $\mathbb{C}$ podemos factorizar a f de la siguiente manera

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

donde $\xi = \sqrt[4]{2}$ es la raíz cuarta (positiva) de 2. De manera obvia tenemos que $K = \mathbb{Q}(\xi, i)$. La característica de este campo es cero y de este modo vemos que K es un campo de descomposición, por lo que la extensión $(K : \mathbb{Q})$ es finita, separable y normal.

2. Ahora vamos a calcular el grado de $(K : \mathbb{Q})$. Primeramente veamos que

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

el polinomio mínimo de $\mathbb{Q}(\xi)$, es t^2+1, dado que $i^2+1 = 0$, pero $i \notin \mathbb{R} \supseteq \mathbb{Q}(\xi)$. Por lo tanto

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

Ahora ξ es un cero de f sobre $\mathbb{Q}$ y f es irreducible por el criterio de Einseinstein. Por lo que f es el polinomio mínimo ξ sobre $\mathbb{Q}$, y

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

así que

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

3. Ahora encontraremos los elementos de el grupo de Galois de (K:$\mathbb{Q}$). Mediante un cálculo directo (o una aplicación directa de el teorema 3.4.5). Se tiene que existe un $\mathbb{Q}$-automorfismo σ de K tal que

$$\sigma(i) = i \qquad\qquad \sigma(\xi) = i\xi$$

y otro τ, tal que

$$\tau(i) = -i \qquad\qquad \tau(\xi) = \xi$$

y productos de estos dos dan ocho distintos $\mathbb{Q}$-automorfismos de K que ilustraremos en la siguiente tabla.

Aut.	efecto en ξ	efecto en i
1	ξ	i
σ	$i\xi$	i
σ^2	$-\xi$	i
σ^3	$-i\xi$	i
τ	ξ	$-i$
$\sigma\tau$	$i\xi$	$-i$
$\sigma^2\tau$	$-\xi$	$-i$
$\sigma^3\tau$	$-i\xi$	$-i$

y otros productos no producen nuevos automorfismos, dado que $\sigma^4 = 1$, $\tau^2 = 1$, $\tau\sigma = \sigma^3\tau$, $\tau\sigma^2 = \sigma^2\tau$, $\tau\sigma^3 = \sigma\tau$ (las últimas dos relaciones se siguen de las primeras tres).

Ahora bien un $\mathbb{Q}$-automorfismo de K transforma a i en algún cero de t^2+1 por lo que $i \longmapsto \pm i$; de manera similar ξ es transformado en ξ, $i\xi$, $-\xi$ ó

$-i\xi$ todas las posibles combinaciones (ocho en número) aparecen en la lista anterior, por lo que estos son precisamente los $\mathbb{Q}$-automorfismos de K.

4. La estructura de el grupo de Galois G puede ser encontrada formando al grupo como una relación, es decir

$$G = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle$$

y se sigue que G es el grupo diedrico de orden ocho, que habremos de denotar como $\mathbf{D_8}$.

5. Un ejercicio muy fácil de hacer, es encontrar los subgrupos de G. Si denotamos por $\mathbf{C_n}$ al grupo cíclico de orden n y $\times$ al producto directo de grupos, entonces los subgrupo de G son los siguientes.

Orden 8 :

$$G \qquad\qquad G \backsimeq \mathbf{D_8}$$

Orden 4

$$\left\{1, \sigma, \sigma^2, \sigma^3\right\} \qquad S \backsimeq \mathbf{C_4}$$

$$\left\{1, \sigma^2, \tau, \sigma^2\tau\right\} \qquad T \backsimeq \mathbf{C_2} \times \mathbf{C_2}$$

$$\left\{1, \sigma, \sigma\tau, \sigma^3\tau\right\} \qquad U \backsimeq \mathbf{C_2} \times \mathbf{C_2}$$

Orden 2

$$\left\{1, \sigma^2\right\} \qquad A \backsimeq \mathbf{C_2}$$

$$\{1, \tau\} \qquad B \backsimeq \mathbf{C_2}$$

$$\{1, \sigma\tau\} \qquad C \backsimeq \mathbf{C_2}$$

$$\left\{1, \sigma^2\tau\right\} \qquad D \backsimeq \mathbf{C_2}$$

$$\left\{1, \sigma^3\tau\right\} \qquad E \backsimeq \mathbf{C_2}$$

Orden 1

$$\{1\} \qquad I \backsimeq \mathbf{C_1}$$

6. Las relaciones de los subgrupos de G pueden ser observadas en el siguiente diagrama reticular.

$$
\begin{tikzcd}
 & & G & & \\
 & T \arrow[ur] & S \arrow[u] & U \arrow[ul] & \\
D \arrow[ur] & B \arrow[u] & A \arrow[ul] \arrow[u] \arrow[ur] & C \arrow[u] & E \arrow[ul] \\
 & & I \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}
$$

Donde si hay flecha de X a Y significa que como conjuntos (además de ser subgrupos) esta contenido uno en el otro.

Bajo la correspondencia de Galois se obtienen los campos intermedios. Pero tenemos ahora inclusiones que invierten las flechas, así pues obtenemos un diagrama reticular de campos que se ve de la siguiente manera.

$$
\begin{tikzcd}
 & & I^\dagger & & \\
D^\dagger \arrow[urr] & B^\dagger \arrow[ur] & A^\dagger \arrow[u] & C^\dagger \arrow[ul] & E^\dagger \arrow[ull] \\
 & T^\dagger \arrow[ul] \arrow[u] \arrow[ur] & S^\dagger \arrow[u] & U^\dagger \arrow[ul] \arrow[u] \arrow[ur] & \\
 & & G^\dagger \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}
$$

Donde $G^\dagger = \mathbb{Q}$ y $K = I^\dagger$.

7. Ahora describiremos los elementos de los campos intermedios. Existen tres subcampos de K (de manera obvia) de grado dos sobre $\mathbb{Q}$ digamos $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt[2]{2})$, $\mathbb{Q}(i\sqrt[2]{2})$. Estos claramente son los subcampos fijos de $S^\dagger$, $T^\dagger$ y $U^\dagger$ respectivamente. Los otros subcampos fijos no son tan obvios. Para ilustrar esto calculemos $C^\dagger$.

Un elemento x de K puede ser expresado de la forma

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3 i\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3$$

donde $a_0, ..., a_7 \in \mathbb{Q}$, así pues tenemos que

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

De este modo tenemos que x queda fijo por $\sigma\tau$ (y por lo tanto por C) si, y sólo si $a_0 = a_0$, $a_1 = a_5$, $a_2 = -a_2$, $a_3 = -a_7$, $a_4 = -a_4$, $a_5 = a_1$, $a_6 = a_6$, $a_7 = -a_3$ por lo que a_0 y a_6 los podemos tomar de manera arbitraria, $a_2 = 0 = a_4$, $a_1 = a_3$ y $a_5 = -a_7$, así pues tenemos que:

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

De este modo tenemos que $C^\dagger = \mathbb{Q}((1+i)\xi)$. De manera similar tenemos que:

$$A^\dagger = \mathbb{Q}(i, \sqrt[2]{2}); \quad B^\dagger = \mathbb{Q}((\xi); \quad D^\dagger = \mathbb{Q}(i) \quad ; E^\dagger = \mathbb{Q}((1-i)\xi).$$

Es en este momento fácil el verificar las relaciones de inclusión (las determinadas por las flechas) determinadas en el diagrama reticular de el punto 6.

8. El lector puede verificar (de manera muy sencilla) que estos son los únicos campos intermedios.

9. Los subgrupos normales de G son G, S, T, U, A, I. Por la teoría desarrollada $G^\dagger$, $S^\dagger$, $T^\dagger$, $U^\dagger$, $A^\dagger$, $I^\dagger$ son las únicas extensiones normales de $\mathbb{Q}$, que están contenidas en K. Dado que estos son todos los campos de descomposición sobre $\mathbb{Q}$, para los polinomios t, t^2+1, t^2-2, t^2+2, t^4-t^2-2, t^4+2 (respectivamente) estos son extensiones normales de $\mathbb{Q}$.

En otro sentido $(B^\dagger : \mathbb{Q})$ no es normal, dado que t^4-2 tiene un cero, digamos ξ en $B^\dagger$, pero este polinomio no se divide en $B^\dagger$. Similarmente $C^\dagger$, $D^\dagger$ y $E^\dagger$ no son extensiones normales de $\mathbb{Q}$.

10. Acordándonos de la teoría desarrollada cuando vimos el grupo de Galois tenemos que $(A^\dagger : \mathbb{Q})$ es isomorfo a G/A. Además G/A es isomorfo a $\mathbf{C_2} \times \mathbf{C_2}$, para probar esto haremos lo siguiente. Como $A^\dagger$ es isomorfo a $\mathbb{Q}(i, \sqrt[2]{2})$ hay cuatro automorfismos de K, que ilustraremos en la siguiente tabla.

Aut.	efecto en i	efecto en $\sqrt[2]{2}i$
1	i	$\sqrt[2]{2}$
α	i	$-\sqrt[2]{2}$
β	$-i$	$\sqrt[2]{2}$
$\alpha\beta$	$-i$	$-\sqrt[2]{2}$

Dado que $\alpha^2 = \beta^2 = 1$ y $\alpha\beta = \beta\alpha$, este grupo es precisamente $\mathbf{C_2} \times \mathbf{C_2}$ como esperábamos.

12.1 Ejercicios.

12.1 Encuentre el grupo de Galois de las siguientes extensiones.

a) $(\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}$.

b) $(\mathbb{Q}(\alpha) : \mathbb{Q})$ donde $\alpha = e^{2\pi i/3}$

c) $(K : \mathbb{Q})$ donde K es el campo de descomposición sobre $\mathbb{Q}$ para el polinomio $t^4 - 3t^2 + 4$.

12.2 Encuentra los subcampos intermedios de el grupo de Galois para las extensiones de el ejercicio anterior.

12.3 Encuentra los correspondientes campos fijos.

12.4 Encuentra los subgrupos normales de el grupo de galois para las extensiones de el ejercicio 12.1.

12.5 Verifique que las extensiones sean normales.

12.6 Verifique que los grupos de Galois de estas extensiones normales son los grupos factor (ó grupos cociente).

Capítulo 13

Algo de Teoría de Grupos.

Para las siguientes aplicaciones de el teorema de la correspondencia de Galois necesitaremos resultados de la teoría general de grupos. Habremos de asumir que el lector esta familiarizado con conceptos tales como: subgrupos, subgrupos normales, grupos cociente (ó grupos factor), conjugados, permutaciones (descomposición en ciclos) y los teoremas de isomorfismo.

En la primera parte de este capítulo desarrollaremos algunas propiedades básicas de los grupos solubles. Los grupos solubles son de gran importancia en la solución de ecuaciones por radicales, en la segunda sección discutiremos acerca de los grupos simples y el principal objetivo será probar que la simplicidad de el grupo alternante (que denotaremos $\mathbf{A_n}$) para n mayor que cuatro. Por último en la tercer sección daremos una pequeña introducción a la teoría de p-grupos y a los teoremas de Sylow.

13.1 Grupos solubles.

Los grupos solubles fueron primeramente definidos y estudiados por Galois en su trabajo para encontrar la solución de una ecuación dada por radicales. Estos grupos tienen desde entonces una gran importancia en muchas ramas de las matemáticas (principalmente en teoría de grupos). En la siguiente definición habremos de adoptar la notación $H \trianglelefteq G$ para indicar que H es un subgrupo *normal* de G.

Definición 13.1.1. Un grupo es *soluble*, si tiene una serie finita de subgrupos

$$1 = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G \tag{13.1}$$

tal que se cumplan

1. $G_i \trianglelefteq G_{i+1}$ para toda i

2. G_{i+1}/G_i es un grupo abeliano, para toda i.

Note que en la condición (1) de la definición anterior no se implica que $G_i \trianglelefteq G$ dado que $G_i \trianglelefteq G_{i+1} \trianglelefteq G_{i+2}$ no implica que $G_i \trianglelefteq G_{i+2}$.

Ejemplos.

1. Todo grupo abeliano G es soluble, con serie de composición $1 \trianglelefteq G$ donde 1 representa el subgrupo trivial de G.

2. El grupo simétrico $\mathbf{S_3}$ de grado 3 es soluble, dado que tiene un subgrupo normal de orden 3 (que es el generado por el ciclo $(1\ 2\ 3)$), cuyo grupo cociente es cíclico de orden 2.

3. El grupo diedrico $\mathbf{D_8}$ de orden ocho es soluble, con la notación de el capítulo 12 este tiene un subgrupo normal S de orden cuatro cuyo grupo cociente tiene orden dos.

4. El grupo simétrico $\mathbf{S_4}$ de grado 4 es soluble, tiene serie.

$$1 \trianglelefteq V \trianglelefteq \mathbf{A_4} \trianglelefteq \mathbf{S_4}.$$

donde $\mathbf{A_4}$ es el grupo alternante (que tiene orden 12), y V consiste de las permutaciones $1, (12)(34), (13)(24), (14)(23)$, este grupo V además es un producto directo de grupos cíclicos de orden dos (el símbolo V fue dado por *Klein* por el termino de Vieregruppe (que significa 4-grupo)) los grupos cociente son.

$V/1 \backsimeq V$ abeliano de orden cuatro.

$\mathbf{A_4}/V \backsimeq \mathbf{C_3}$ abeliano de orden tres.

$\mathbf{S_4}/\mathbf{A_4} \backsimeq \mathbf{C_2}$ abeliano de orden dos.

5. El grupo simétrico $\mathbf{S_5}$ de grado 5 no es soluble (la prueba de este hecho será dada más adelante).

A continuación enunciaremos los teoremas de isomorfismo (aunque no los probaremos).

Lema 13.1.2. *Sean G, H y A grupos.*

1) Si $H \trianglelefteq G$ y $A \subseteq G$ entonces $H \cap A \trianglelefteq A$ y $A/H \cap A \backsimeq HA/H$.

2) Si $H \trianglelefteq G$ y $H \subseteq A \trianglelefteq G$ entonces:

a) $H \trianglelefteq A$,

b) $(A/H) \trianglelefteq (G/H)$ y

c) $(G/H)/(A/H) \backsimeq G/A$.

La parte 1) y 2) en son conocidas en la literatura como el primer y segundo teorema de isomorfismo respectivamente.

Teorema 13.1.3. *Sea G un grupo y H un subgrupo de G si N es un subgrupo normal de G entonces se cumple.*

1) Si G es soluble entonces H es soluble.

2) Si G es soluble entonces G/N es soluble.

3) Si N y G/N son solubles entonces G es soluble.

Prueba. 1) Sea $1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ una serie para G con grupos factores G_{i+1}/G_i abelianos. Consideremos $H_i = G_i \cap H$ entonces es claro que H tiene serie

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_n = H.$$

Solamente resta probar que los grupos factores (o simplemente factores) son abelianos, pero por los teoremas de isomorfismo tenemos que

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

Pero el grupo anterior es un subgrupo de G_{i+1}/G_i que es abeliano y por tanto H_{i+1}/H_i es abeliano. Por lo tanto H es soluble.

2) Definiendo los G_i como antes tenemos que G/N tiene serie

$$N/N = G_0N/N \trianglelefteq G_iN/N \trianglelefteq ..... \trianglelefteq G_nN/N = G/N.$$

cuyos factores son:

$$\frac{G_{i+1}N/N}{G_iN/N}$$

y por el segundo teorema de isomorfismo tenemos que

$$\frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \backsimeq \frac{G_{i+1}}{G_{i+1} \cap G_iN} \backsimeq \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))G_i}$$

que es un cociente de el grupo abeliano G_{i+1}/G_i y por tanto G/N es soluble.

3) Existen series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_r = N$$

y

$$N/N = G_0/N \trianglelefteq G_1/N \trianglelefteq ... \trianglelefteq G_s/N = G/N.$$

con factores abelianos . Consideremos la serie de G dada por

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_s = G.$$

Los grupos cociente son N_{i+1}/N_i (que es abeliano) ó bien G_{i+1}/G_i el cual es isomorfo a

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

y este cociente es abeliano. Por lo tanto G es soluble. $\square$

Se dice que un grupo G es una extensión de un grupo A por un grupo B si G tiene un subgrupo normal N isomorfo a A tal que G/N es isomorfo a B. De este modo podemos resumir las tres propiedades de teorema anterior diciendo que *la clase de los grupos solubles es cerrada bajo subgrupos, cocientes y extensiones.* Aquí hay una observación importante sabemos que la clase de los grupos abelianos es cerrada bajo subgrupos, cocientes, pero de hecho no es cerrada bajo extensiones, así que podemos pensar que los grupos solubles pudieron haber tenido su origen precisamente en este sentido (que de hecho así sucedio).

13.2 Grupos simples.

En esta sección hablaremos en cierto sentido a lo opuesto a los grupos solubles que son precisamente los grupos simples.

Definición 13.2.1. Un grupo G es *simple*, si sus únicos subgrupos normales son el trivial (que denotaremos por 1) y G mismo.

Todo grupo cíclico de orden primo es simple, dado que no tiene subgrupos (y por lo tanto no tiene subgrupos normales) distintos de el trivial y de el mismo. Estos grupos son además abelianos, por lo que también son solubles. De hecho estos son los únicos grupos solubles simples.

Teorema 13.2.2. *Un grupo soluble es simple si, y solamente si es cíclico y de orden primo.*

Prueba. Si G es un grupo simple y soluble este tiene una serie de la forma

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$$

donde podemos considerar que no hay repeticiones es decir $G_i \neq G_{i+1}$. De este modo tenemos que G_{n-1} es un subgrupo normal propio de G, que es simple, por lo que $G_{n-1} = 1$ y $G = G_n/G_{n-1}$ que es abeliano. Dado que todo subgrupo de un grupo abeliano es normal y todo elemento de G genera un grupo cíclico y como G no tiene subgrupos normales propios no triviales, tenemos que G es cíclico de orden primo. El recíproco de este resultado esta probado en la discusión previa al teorema. $\square$

Los grupos simples juegan un papel importante en la teoría de grupos finitos. estos son en cierto sentido los unidades fundamentales que constituyen a todos los grupos finitos. específicamente todo grupo finito tiene una serie de subgrupos como en la ecuación 13.1, cuyos grupos cocientes son simples; y estos grupos simples dependen únicamente de el grupo y no de la serie elegida (esto no es más que el conocido teorema de *Jordan-Hölder*).

Teorema 13.2.3. *Si n es mayor que cuatro entonces el grupo alternante $\mathbf{A_n}$ es simple.*

Prueba. Supongamos que $1 \neq N \trianglelefteq \mathbf{A_n}$. Primeramente probaremos que si N contiene un 3-ciclo entonces contiene a todos los tres ciclos y con ello probaremos despues que todos los 3-ciclos generan a $\mathbf{A_n}$, entonces tendríamos que $N = \mathbf{A_n}$.

Supongamos pues que N contiene un 3-ciclo; sin perdida de generalidad podemos suponer que N contiene al ciclo $(1\ 2\ 3)$. Ahora para $k > 3$ el ciclo $(12k)$ es una permutación par, por lo que pertenece a $\mathbf{A_n}$ y de este modo tenemos que $(23k)^{-1}(123)(23k) = (1k2)$ pertenece a N, por tanto N contiene a $(1k2)^2 = (12k)$ para todo $k \geq 3$. Ahora el grupo simétrico es el generado por todos los 2-ciclos de la forma $(1i)$ para $i \in \{1, ..., n\}$. Dado que $\mathbf{A_n}$ es el conjunto de los productos pares de estos 2-ciclos tenemos que $\mathbf{A_n}$ esta generado por todos los elementos de la forma

$$(1i)(1j) = (1ij)$$

pero para $i \neq 2$ tenemos:

$$(1ij) = (12j)(12i)(12j)$$

Por lo que $\mathbf{A_n}$ esta generado por todos los ciclos de la forma $(12k)$, lo que muestra que $N = \mathbf{A_n}$.

Solamente falta probar que N contiene al menos un 3-ciclo, para hacer esto lo dividiremos en casos.

Primero. Supongamos que N contiene un elemento de la forma

$$x = abc....$$

donde $a, b, c, ...$ son ciclos disjuntos y $a = (a_1, , , a_m)$ $(m \geq)4$. Sea $t = (a_1 a_2 a_3)$. Entonces N contiene a $t^{-1}xt$. Dado que t conmuta con $b, c, ...$ (por ser ciclos disjuntos) se sigue que

$$t^{-1}xt = (t^{-1}at)bc... = z$$

por lo que N contiene a, $zx^{-1} = (a_1 a_3 a_m)$ el cual es un tres ciclo.

Segundo. Ahora supongamos que N contiene un elemento que esta compuesto con por lo menos un producto de 3-ciclos. Sin perdida de generalidad N contiene a $x = (123)(456)y$ donde y es una permutación que fija a $1, 2, 3, 4, 5$ y 6, sea $t = (254)$. Entonces N contiene a $(t^{-1}xt)x^{-1} = (123456)$ y por el primer caso N contiene un 3-ciclo.

Tercero. Si N no contiene contiene elementos como en los casos previos entonces N esta compuesto de un tres ciclo ó es un producto de 2-ciclos disjuntos, para la primera posibilidad podemos considerar un elemento x en N de la forma $x = (123)y$ donde y conmuta con x y $y^2 = 1$. Entonces N contiene a $x^2 = (132)y^2 = (132)$ el cual es un tres ciclo.

Cuarto. El caso restante es cuando todo elemento de N es un producto de 2-ciclos disjuntos (esto puede ocurrir cuando $n = 4$). Pero como $n \geq 5$ podemos asumir que N contiene a

$$x = (12)(34)y$$

donde y fija a 1,2,3 y 4. Si escogemos a $t = (234)$ entonces N contiene a

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

y si $u = (145)$ entonces N contiene a

$$(u^{-1}xu)x^{-1} = (45)(23).$$

por lo que N contiene a $(45)(23)(14)(23) = (145)$ contradiciendo el hecho de que N es el producto de 2-ciclos disjuntos. Por lo tanto $\mathbf{A_n}$ es simple para $n \geq 5$. $\square$

El hecho de que $\mathbf{A_5}$ es el menor grupo simple no abeliano fue primeramente probado por Galois. De este teorema podemos deducir fácilmente

Corolario 13.2.4. El grupo simétrico $\mathbf{S_n}$ no es soluble para $n \geq 5$.

Prueba. Si $\mathbf{S_n}$ fuera soluble, entonces $\mathbf{A_n}$ es soluble (teorema 13.1.3) y simple por el teorema 13.2.3, por lo tanto de orden primo (por teorema 13.2.2) pero el orden de $\mathbf{A_n}$ es $\frac{1}{2}n!$ que no es primo para $n \geq 5$. $\square$

Con tópicos de el estilo anterior se puede probar un resultado simple que será usado en el capítulo 14.

Lema 13.2.5. *Para un número natural n el grupo simétrico $\mathbf{S_n}$ está generado por los ciclos $(1\ 2\ \ldots\ n)$ y $(1\ 2)$.*

Prueba. Sea c=$(1\ 2\ \ldots\ n)$ y t=$(1\ 2)$, consideremos al subgrupo G de $\mathbf{S_n}$ generado por c y t. Entonces G contiene a $c^{-1}tc$ =$(2\ 3)$ y por tanto también contiene a $c^{-1}(2\ 3)c$=$(3\ 4)$,... y por tanto a todas las transposiciones de la forma $(m\ m+1)$.

Así pues G contiene a $(1\ 2)(2\ 3)(1\ 2)$=$(1\ 5)$, $(1\ 3)(3\ 4)(1\ 3)$=$(1\ 4)$,... y por lo tanto contiene a todas las transposiciones de la forma $(1\ m)$. Pero entonces G contiene a todos los elementos de la forma $(1\ m)(1\ r)(1\ m)$=$(m\ r)$. Y como cada elemento de $\mathbf{S_n}$ es un producto de transposiciones tenemos que $G = \mathbf{S_n}$. $\square$

13.3 P-grupos

Primeramente recordemos las ideas principales de esta teoría.

Definición 13.3.1. Dos elementos a, b de un grupo G son *conjugados* en G si existe $g \in G$ tal que $a = g^{-1}bg$.

La conjugación antes definida es una relación de equivalencia; las clases de equivalencia serán llamadas *clases de conjugación* de G. Si las clases de conjugación de G son $C_1, ..., C_r$ entonces una de ellas digamos C_1 contiene únicamente al elemento identidad de G. por lo que $|C_1| = 1$, dado que las clases de conjugación constituyen una partición de G tenemos que

$$|G| = 1 + |C_2| + ... + |C_n| \tag{13.2}$$

la cual es llamada la ecuación de clase para G.

Definición 13.3.2. Si G es un grupo y $x \in G$ entonces el *centralizador* $C_G(x)$ de x en G es el conjunto de todos los elementos $g \in G$ que conmutan con x, es decir $gx = xg$.

Siempre es cierto que $C_G(x)$ es un subgrupo de G. Existe una conexión muy usada entre los centralizadores y las clases de conjugación.

Lema 13.3.3. *Sea G es un grupo y $x \in G$ entonces el número de elementos en la clase de conjugación de x es el índice de $C_G(x)$ en G.*

Prueba. La ecuación $g^{-1}xg = h^{-1}xh$ se satisface si, y sólo si $hg^{-1}x = xhg^{-1}$ es decir, si $hg^{-1} \in C_G(x)$, es decir, que tanto h como g pertenezcan a la misma clase lateral $C_G(x)$ en G. El número de estas clases laterales es precisamente el índice de $C_G(x)$ en G. □

Corolario 13.3.4. El número de elementos en una clase de conjugación de un grupo finito G divide al orden de el grupo.

Ahora introduciremos la clase de los *p-grupos.*

Definición 13.3.5. Sea p un número primo. Un grupo finito G es un *p-grupo*, si su orden es una potencia de p.

Por ejemplo, el grupo diedrico $\mathbf{D_8}$ es un $2-grupo$. Si $n \geq 3$ entonces el grupo simétrico $\mathbf{S_n}$ no es nunca un $p-grupo$ para ningún primo p.

Definición 13.3.6. El *centro* $Z(G)$ de un grupo G es el conjunto de elementos de $x \in G$ tal que $xg = gx$ para toda $g \in G$.

Como una primera observación tenemos que el centro de un grupo siempre es un subgrupo normal. Muchos grupos tienen centro trivial, por ejemplo, $Z(\mathbf{S_3}) = 1$ mientras que si un grupo G es abeliano se tiene que $Z(G) = G$; la existencia de centro no trivial es de suma importancia en los $p-grupos$.

Teorema 13.3.7. *Sea $1 \neq G$ un $p-grupo$ finito entonces G tiene centro no trivial.*

Prueba. La ecuación de clase (13.2) de G nos dice que

$$p^n = |G| = 1 + |C_2| + ... + |C_r|$$

y por el corolario 13.3.4, tenemos que $|C_i| = p^{n_i}$ para algún $n_i \geq 0$. Ahora bien p divide al lado derecho de la ecuación anterior por lo que al menos $p-1$ valores de las n_i tienen que ser igual a 1. Pero si x esta en la clase de conjugación con un solo elemento entonces, $g^{-1}xg = x$ para toda $x \in G$, es decir $xg = gx$, por lo que $x \in Z(G)$ así pues $Z(G)$ es no trivial □

De el resultado anterior deducimos fácilmente

Lema 13.3.8. *Si G es un $p-grupo$ finito de orden p^n, entonces G tiene una serie de subgrupos normales*

$$1 = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

tal que $|G_i| = p^i$ para todo $i = 1, ..., n$.

Prueba. Usaremos inducción sobre n. Si $n = 0$ todo es claro. Si no, sea $Z = Z(G) \neq 1$. Dado que Z es abeliano de orden p^m, tenemos que Z tiene un elemento de orden p. El grupo cíclico generado por tales elementos llamemosle K tiene orden p y es normal en G dado que $K \subseteq Z$. Ahora bien el grupo cociente G/K es un $p-grupo$ de orden p^{n-1} y por hipótesis de inducción existe una serie de subgrupos normales.

$$K/K = G_1/K \subseteq ... \subseteq G_n/K$$

donde $|G_i/K| = p^{i-1}$ pero entonces $|G_i| = p^i$ y $G \trianglelefteq G_{i+1}$ tomando $G_0 = 1$ el resultado se sigue. □

Corolario 13.3.9. Todo $p - grupo$ finito es soluble.

Prueba. Los grupos cociente G_{i+1}/G_i de serie dada en el lema anterior son de orden p y por lo tanto cíclicos y abelianos. □

En 1872 el Matemático Noruego *L. Sylow* descubrió algunos teoremas fundamentales acerca de la existencia de $p - grupos$ dentro de grupos finitos, en el siguiente capítulo necesitaremos algunos de estos resultados. Solamente probaremos la primera parte de el siguiente teorema.

Teorema 13.3.10 (Sylow). *Sea G un grupo finito de orden $p^\alpha r$ donde p es un número primo que no divide a r. Entonces se satisface lo siguiente.*

1) G tiene al menos un subgrupo de orden p^α.

2) Todos los subgrupos de orden p^α son conjugados.

3) Un $p-$ subgrupo de G está contenido en uno de orden p^α.

4) El número de subgrupos de G de orden p^α deja residuo 1 en la división por p.

Este resultado motiva la siguiente

Definición 13.3.11. Si G es un grupo finito de orden $p^\alpha r$ donde p no divide a r entonces, un *p-subgrupo de sylow* de G es un subgrupo de G de orden p^α.

Para dar la prueba que prometimos de la parte 1 de el teorema anterir necesitaremos de un resultado que probaremos a continuación.

Lema 13.3.12. *Si A es un grupo abeliano finito cuyo orden es divisible por un primo p entonces, A tiene un elemento de orden p.*

Prueba. Usaremos inducción sobre $|A|$, si $|A|$ es primo el resultado se sigue. En otro caso tomamos un subgrupo propio M de A cuyo orden (digamos m) sea máximo. Si p divide a m entonces por hipótesis de inducción ya acabamos. Así que supongamos que p no divide a m. Y consideremos un elemento $t \in A$ tal que $t \notin M$, y sea T el subgrupo cíclico generado por t. Entonces MT es un subgrupo de A más grande que M y por la máximalidad de M tenemos que $MT = A$. Por el primer teorema de isomorfismo tenemos

$$|MT| = |M||T| \diagup |M \cap T|.$$

Por lo que p divide al orden de T digamos que este orden es r. Dado que T es cíclico el elemento $t^{\frac{r}{p}}$ tiene orden p. Por lo tanto el lema ha sido probado. □

Prueba. Usaremos nuevamente inducción sobre $|G|$. El teorema es obviamente claro para $|G| = 1$ ó 2. Sean $C_1, ..., C_s$ las clases de conjugación de G y sea $c_i = |C_i|$. Por la ecuación de clase tenemos que

$$p^\alpha r = c_1 + ... + c_s. \tag{13.3}$$

Si Z_i denota el centralizador de G para algún elemento $x_i \in C_i$ y $n_i = |Z_i|$ entonces por el lema 13.3.3, tenemos.

$$n_i = p^\alpha r \diagup c_i. \tag{13.4}$$

Supongamos ahora que c_i es mayor que uno y no divisible por p, entonces por la ecuación 13.4, $n_i < p^\alpha r$ y es divisible por p^α. Por hipótesis de inducción Z_i contiene un subgrupo de orden p^α. De este modo tenemos que podemos asumir que para todo, $i \in \{1, ..., s\}$ $c_i = 1$, ó bien, p divide a c_i. Sea $z = Z(G)$

como en el teorema 13.3.7, z es el número de valores i tal que $c_i = 1$ por lo que

$$p^\alpha r = z + kp.$$

para algún entero k. Por lo que p divide a z y G tiene centro no trivial Z tal que p divide a z. por el lema 13.3.12, Z tiene un elemento de orden p que genera un subgrupo P de G de orden p. Dado que $P \subseteq Z$ se tiene que $P \trianglelefteq G$. Por hipótesis de inducción G/P contiene un subgrupo S/P de orden $p^{\alpha-1}$ y como S es un subgrupo de G de orden $p\alpha$ hemos probado la primer parte de el teorema. □

De este resultado podemos probar el teorema de *Cauchy* (que históricamente siempre precede al teorema de *Sylow*).

Teorema 13.3.13 (Cauchy). *Si p es un número primo que divide al orden de un grupo finito G entonces G tiene un elemento de orden p.*

Prueba. Consideremos S un $p-subgrupo$ de sylow de G, por lo que $S \neq 1$ por el lema 13.3.8, S tiene un subgrupo normal de orden p. □

Ejemplo. Sea $G = \mathbf{S_4}$ así $|G| = 24$ acordándonos de el teorema de sylow G tiene subgrupos de orden 3 y de orden 8. Los subgrupos de orden 3 son fáciles de calcular pues un tres ciclo tal como (1 2 3) ó (1 3 4) ó (2 3 4) generan tales subgrupos. Ahora encontremos los subgrupos de orden 8. Consideremos V el grupo de Klein el cual es normal en G y sea t un 2-ciclo el cual genera un subgrupo T de G de orden dos. Entonces $V \cap T = 1$ y VT es un subgrupo de orden ocho.

13.4 Ejercicios.

13.1 Muestre que el grupo general diedrico

$$\mathbf{D_{2n}} = \langle a, b : a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle$$

13.2 Pruebe que $\mathbf{S_n}$ no es soluble para $n \geq 5$ usando la simplicidad de $\mathbf{A_n}$.

13.3 Pruebe que un subgrupo normal de un grupo es una unión de clases de conjugación. Encuentre las clase de conjugación de $\mathbf{A_5}$ (usando el tipo de ciclos de una permutación). Y finalmente de otra prueba que $\mathbf{A_5}$ es simple.

13.4 Pruebe que $\mathbf{S_n}$ esta generado por los 2-ciclos (1 2),...,(1 n).

13.5 Encuentre los 2-, 3- y 5-subgrupos de sylow de $\mathbf{S_5}$.

13.6 Pruebe que un grupo finito G es un $p-grupo$ si, y sólo si todo elemento de G tiene orden alguna potencia de p.

13.7 Si el punto (α, β) es construible con regla y compás de (0,0) y (1,0) muestra que los grupos de Galois de $(\mathbb{Q}(\alpha) : \mathbb{Q})$ y $(\mathbb{Q}(\beta) : \mathbb{Q})$ son 2-grupos.

13.8 Muestra que $\mathbf{A_5}$ no tiene subgrupos de orden 15.

13.9 Muestra que un subgrupo ó un grupo cociente de un $p - grupo$ es también un $p - grupo$. Muestra que una extensión de un $p - grupo$ por un $p - grupo$ es un $p - grupo$.

13.10 Muestra que $\mathbf{S_n}$ tiene centro trivial si $n \geq 3$.

13.11 Pruebe que todo grupo de orden p^2 (p un número primo) es abeliano. Con esto muestra que existen exactamente dos grupos no isomorfos de orden p^2 para un primo p.

13.12 Encuentra las clases de conjugación de el grupo diedrico $\mathbf{D_{2n}}$.

13.13 Si $x, g \in G$ muestre que $C_G(g^{-1}xg) = g^{-1}C_G(x)g$.

13.14 Diga si las siguientes afirmaciones son verdaderas o falsas.

a) Todo grupo soluble es un $p - grupo$.

b) Todo subgrupo de sylow de un grupo finito es soluble.

c) Un producto directo de grupos solubles es soluble.

d) Un grupo soluble simple es cíclico.

e) Todo grupo cíclico es simple.

f) El grupo simétrico $\mathbf{S_n}$ es simple si $n \geq 5$.

g) Las clases de conjugación de un grupo G son subgrupos de G.

h) Todo grupo finito tiene $p - subgrupos$ de sylow para un primo p.

i) Todo $p - grupo$ finito no trivial tiene centro no trivial.

j) Todo $p - grupo$ simple es abeliano.

Capítulo 14

Solución de ecuaciones por radicales.

Los aspectos de el problema de resolver una ecuación por radicales ya han sido discutidos en la introducción. El objetivo de este capítulo es usar la correspondencia de Galois para dar una condición que debe de satisfacer una ecuación para ser soluble por radicales. Dicha condición será que el grupo de Galois de cierta extensión tiene que ser soluble (en el sentido de el capítulo anterior). Con ello construiremos un polinomio de grado cinco (o un polinomio quintico) cuyo grupo de Galois no es soluble, lo cual probará que la ecuación de grado cinco no siempre es soluble por radicales.

La solubilidad de el grupo de Galois es también una condición suficiente para que una ecuación sea soluble por radicales. Postergaremos este resultado hasta el capítulo siguiente.

14.1 Extensiones radicales.

Iniciaremos dando algunas definiciones para con ellas poner en términos de la teoría desarrollada lo que entenderemos por la frase 'soluble por radicales'.

Definición 14.1.1. Una extensión $(L : K)$ es *radical* si $L = K(\alpha_1, ..., \alpha_m)$

donde para cada $i \in \{1, ..., m\}$ existe un número entero $n(i)$ tal que

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

los elementos α_i se dicen que forman una *sucesión radical* para $(L : K)$.

Informalmente, una extensión radical es obtenida mediante la adjunción de una sucesión de raíces. Por ejemplo la extensión radical de el elemento.

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt[2]{3}}{2}} + \sqrt[4]{1+\sqrt[3]{4}}$$

esta contenida en la extensión radical $\mathbb{Q}(\alpha, \beta.\gamma, \delta, \epsilon)$ de $\mathbb{Q}$ donde:

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

Es claro que una expresión radical en el sentido de la introducción está contenida en alguna extensión radical. Un polinomio es soluble por radicales siempre que todos sus ceros sean expresiones radicales sobre algún campo.

Definición 14.1.2. Sea f un polinomio sobre un campo K de característica cero y sea Ξ un campo de descomposición para f sobre K. Se dice que f es *soluble por radicales* si existe un campo M contenido en Ξ tal que $(M : K)$ es una extensión radical.

Existen algunas observaciones importantes a esta definición. La primera de ellas es que está restringida solamente a campos con característica cero: por razones técnicas la definición de que un polinomio sea soluble por radicales no abarca los campos de característica p para un primo.

A lo largo de este capítulo iremos mencionando el hecho de no considerar campos con esta característica. La segunda observación es el hecho de que $(\Xi : K)$ no necesariamente es una extensión radical. De hecho lo que queremos es que todo campo de descomposición lo podamos expresar como extensiones racionales. La última observación a realizar es que todos los ceros de f puedan ser expresados por radicales, es posible que algunos ceros puedan ser expresados por radicales sin que otros lo sean (simplemente consideremos el producto de dos polinomios uno de ellos soluble por radicales y el otro no). Sin embargo si un polinomio irreducible f tiene un cero expresable por radicales entonces, los demás ceros de el polinomio también son expresables por radicales (por un argumento simple basado en el teorema 3.4.3)

El principal teorema que probaremos es el siguiente.

Teorema 14.1.3. *Si K es un campo de característica cero y $K \subseteq L \subseteq M$ donde $(M : K)$ es una extensión radical entonces, el grupo de Galois de $(L : K)$ es un grupo soluble.*

La prueba de este resultado requiere todavía de algunos resultados previos que comenzaremos a desarrollar.

Lema 14.1.4. *Supongamos que $(L : K)$ es finita y M es una cerradura normal de $(L : K)$. Entonces M esta generado por los subcampos $L_1, ..., L_s$ que contienen a K tal que cada extensión $(L_i : K)$ es isomorfa a $(L : K)$.*

Prueba. Por el lema 4.0.6, se tiene que $L = K(\alpha_1, ..., \alpha_r)$ para elementos algebraicos $\alpha_1, ..., \alpha_s$ sobre K. Sea m_i el polinomio mínimo de α_i sobre K y N un campo de descomposición para $f = m_1 \cdots m_r$ sobre K que contiene a L. Entonces N es una cerradura normal de $(L : K)$ (por la prueba de el teorema 10.2.2). También por el teorema 10.2.2 las extensiones $(M : K)$ y $(N : K)$ son isomorfas, por lo que podemos asumir que $M = N$. Ahora si β_i es un cero de m_i se sigue de el teorema 3.4.5, que las extensiones $(K(\alpha_1, ..., \alpha_i, ..., \alpha_r) : K)$ y $(K(\alpha_1, ..., \beta_i, ..., \alpha_r))$ son isomorfas pero como β_i e i varían de 1 a r las extensiones anteriores generan a M y entonces se sigue el resultado. $\square$

Con este resultado probaremos el siguiente

Lema 14.1.5. *Si $(L : K)$ es una extensión radical y M es una cerradura normal de $(L : K)$ entonces $(M : K)$ es radical.*

Prueba. Sabemos que M esta generado por $L_1, ..., L_s$ (como en el lema 14.1.4) y las extensiones $(L_i : K)$ son todas ellas isomorfas a $(L : K)$ de este modo tenemos que $(L_i : K)$ es una extensión radical para toda i. Por indicción, es suficiente con probar que si R esta generado por $(R_1 : K)$ y $(R_2 : K)$ y estas son extensiones radicales, entonces $(R : K)$ es una extensión radical. Así pues consideremos que nos encontramos en la situación anterior, sea $R_1 = K(\alpha_1, ..., \alpha_m)$ y $R_2 = K(\beta_1, ..., \beta_n)$ donde α_i y β_j son sucesiones radicales, entonces la sucesión combinada

$$\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_n$$

es una sucesión radical, por lo que $(K(\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_n) : K)$ es una extensión radical. Pero esta extensión es precisamente $(R : K)$. $\square$

Los siguientes dos lemas muestran que ciertos grupos de Galois son abelianos.

Lema 14.1.6. *Sea K un campo de característica cero y sea L un campo de descomposición para el polinomio $t^p - 1$ sobre K, donde p es un número primo. Entonces el grupo de Galois de $(L : K)$ es abeliano.*

Prueba. la derivada de $t^p - 1$, es pt^{p-1}, por lo que el polinomio no tiene ceros múltiples en L. Claramente los ceros de $t^p - 1$ forman un grupo bajo la multiplicación; este grupo tiene orden p dado que todos sus ceros son distintos y por lo tanto es un grupo cíclico. Sea ε un generador de este grupo. Entonces $L = K(\varepsilon)$ por lo que un K-automorfismo de L esta determinado por el efecto que este tenga sobre ε. Más aún un K-automorfismo de L es de la forma

$$\alpha_j : \varepsilon \longmapsto \varepsilon^j$$

Pero entonces $\alpha_i\alpha_j$ y $\alpha_j\alpha_i$ ambos automorfismos mandan a ε a ε^{ij}. Por lo tanto el grupo de Galois de $(L : K)$ es abeliano. $\square$

Lema 14.1.7. *Sea K un campo de característica cero en el cual el polinomio $t^n - 1$ se divide. Sea $a \in K$ y sea L un campo de descomposición para $t^n - a$ sobre K. Entonces el grupo de Galois de $(L : K)$ es abeliano.*

Prueba. Sea α un cero de $t^n - a$. Dado que $t^n - 1$ se divide en K un cero general de $t^n - a$ es de la forma, εa donde ε es un cero de $t^n - 1$ en K, dado que $L = K(\alpha)$ un K-automorfismo de L esta determinado por el efecto que este tenga sobre α. De este modo consideremos dos K-automorfismos de L

$$\phi : \alpha \longrightarrow \varepsilon\alpha$$

y

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

donde $\varepsilon, \eta \in K$, de este modo tenemos que $\phi\psi(\alpha) = (\varepsilon\eta)\alpha = (\eta\varepsilon)\alpha = \psi\phi(\alpha)$. Por lo tanto el grupo de galois de $(L : K)$ es abeliano. □

En este momento nos encontramos en condiciones de dar la prueba de el teorema 14.1.3. Dicha prueba la haremos por inducción.

Prueba.*(*De el teorema 14.1.3*)*. La prueba la realizaremos siguiendo una serie de pasos que iremos enumerando.

Primero. Sea K_0 el campo fijo de el grupo de Galois $\Gamma(L : K)$ y supongamos por el momento que podemos probar el teorema remplazando K por K_0. Dado que el grupo de Galois $\Gamma(L : K_0)$ es el mismo que $\Gamma(L : K)$ entonces por definición y dado que M es claramente radical (ver M en la hipótesis de el teorema) $(K \subseteq K_0)$ se deduce (de el Teorema 14.1.3) que podemos remplazar K por K_0. Pero $(L : K_0)$ es normal (por el teorema 10.2.9), dado que K_0 es el campo fijo de $\Xi(L : K) = \Gamma(L : K_0)$. La conclusión de todo esto es que podemos asumir que $(L : K)$ es normal.

Segundo. Si N es una cerradura normal de $(M : K)$ entonces por el lema 14.1.5 $(N : K)$ es radical, así que remplazado M por N podemos asumir que $(M : K)$ es normal.

Tercero. El grupo de Galois $\Gamma(L : K)$ es un grupo cociente de $\Gamma(M : K)$ (lo anterior es consecuencia de el teorema 11.0.2, parte (5)). Si probamos que $\Gamma(M : K)$ es un grupo soluble entonces de el teorema 13.1.3, parte (2) se tendrá que $\Gamma(L : K)$ es soluble. Por lo cual asumiremos que $M = L$ y el resultado general se seguirá de este caso especial.

Cuarto. Hemos reducido la prueba de el teorema a considerarnos dentro de la siguiente situación: $(L : K)$ es una extensión normal y radical, que además es separable puesto que la característica de K es cero. Ahora mostraremos que bajo estas condiciones $\Gamma(L : K)$ es soluble. Supongamos pues que:

$$L = K(\alpha_1, ..., \alpha_n) \tag{14.1}$$

donde

$$\alpha_i^{n(i)} \in K(\alpha_1, ..., \alpha_{i-1}). \tag{14.2}$$

Añadiéndole posiblemente más α_i's (de ser necesario) podemos asumir que $n(i)$ es un número primo para toda i y que las ecuaciones 14.1 y 14.2 se satisfacen. En particular existe un número primo p tal que $\alpha_1^p \in K$.

Quinto. Ahora usaremos inducción sobre el número entero n que ocurre en la ecuación 14.1. Consideremos M_0 un campo de descomposición para $t^p - 1$ sobre L y sea M_1 el subcampo de M_0 generado por K y los ceros de $t^p - 1$ en M_0.

$$\begin{tikzcd}
& M_0 & \\
M \arrow[ur] & & M_1 \arrow[ul] \\
& K \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Dado que $\Gamma(M : K)$ es un grupo cociente de $\Gamma(M_0 : K)$ es suficiente con probar que $\Gamma(M_0 : K)$ es soluble. Ahora bien como M_1 es una extensión normal de K y $\Gamma(M_1 : K)$ es abeliano (por el lema 14.1.6, es abeliano) pero también $\Gamma(M_1 : K) \trianglelefteq \Gamma(M_0 : K)$ (por el teorema 11.0.2, parte (4)) y como el grupo $\Gamma(M_0 : K)$ es isomorfo al grupo cociente $\Gamma(M_0 : K) \diagup \Gamma(M_1 : K)$, se seguirá de el teorema 13.1.3 que si podemos probar que el grupo cociente anterior es soluble entonces también lo es $\Gamma(M_0 : K)$.

Llamemosle $G = \Gamma(M_0 : M_1)$ como $M_0 = M_1(\alpha_1, ..., \alpha_n)$, consideremos $H = (M_1(\alpha_1))^*$, el subgrupo de G correspondiente a $M(\alpha_1)$ bajo la correspondencia de Galois. Como $t^p - 1$ se divide en M_1, por lo que $M_1(\alpha_1)$ es un campo de descomposición para $t^p - \alpha_1^p$ de M_1. Por lo que esta es una extensión normal de M_1 (por el teorema 8.2.2) y tiene grupo de Galois abeliano (por el lema 14.1.7). Por lo tanto $H \trianglelefteq G$ por el teorema 11.0.2 parte (4). Los siguientes grupos y campos se corresponden.

$$\begin{array}{ccc} M_1 & \longrightarrow & 1 \\ \downarrow & & \downarrow \\ M_1(\alpha_1) & \longrightarrow & H \\ \downarrow & & \downarrow \\ M_0 & \longrightarrow & G \end{array}$$

Por la parte (5) de el teorema 11.0.2, G/H es el grupo de Galois de la extensión $(M_0 : M_1(\alpha_1))$ pero

$$M_0 = M_1(\alpha_1)(\alpha_2, ..., \alpha_n)$$

dado que $(M_0 : M_1(\alpha_1))$ es normal se sigue por inducción que G/H es soluble, pero además H es abeliano por lo que la parte (3) de el teorema 13.1.3, implica que G es soluble, lo cual completa la prueba. $\square$

La idea principal de esta prueba es simple: una extensión radical es una serie de extensiones por n-raíces; tales extensiones tienen grupos de Galois abelianos; Por lo que el grupo de Galois de una extensión radical esta formado por una sucesión propia de grupos abelianos. Desafortunadamente hay algunos problemas técnicos en la prueba anterior: Necesitamos raíces de la unidad y tuvimos que hacer varias extensiones normales y hasta después de todo esto pudimos usar la correspondencia de Galois.

Ahora nos trasladaremos de el uso de campos a polinomios y observaremos la idea general (ó el punto de vista original) de Galois.

Definición 14.1.8. Sea f un polinomio sobre un campo K, con campo de descomposición Ξ sobre K; *El grupo de Galois de f sobre K* es el grupo de Galois de $(\Xi : K)$, $(\Gamma(\Xi : K))$.

Sea G el grupo de Galois de un polinomio f sobre K, si $\alpha \in \Xi$ es un cero de f entonces $f(\alpha) = 0$, por lo que para alguna $g \in G$ se tiene que $f(g(\alpha)) = g(f(\alpha)) = 0$. Por lo cual cada elemento $g \in G$ induce una permutación g' de el conjunto de ceros de f en Ξ. Distintos elementos de G inducen distintas permutaciones dado que Ξ esta generado por los ceros de f.

Se sigue fácilmente que la transformación

$$g \longmapsto g'$$

es un monomorfismo (de grupos) de G sobre el grupo de todas las permutaciones de los ceros de f. Dicho de otra manera podemos pensar a G como un grupo de permutaciones de los ceros de f.

Teorema 14.1.9. *Sea f un polinomio sobre un campo K de característica cero. Si f es soluble por radicales entonces, el grupo de Galois de f sobre K es un grupo soluble.*

Por lo tanto para encontrar un polinomio no soluble por radicales es suficiente encontrar un polinomio cuyo grupo de Galois no sea soluble. Existen dos caminos principalmente para llevar esto a cabo, uno de ellos es el buscar la llamada 'Ecuación general de grado n' ó el 'Polinomio general de grado n' (que será discutida en el siguiente capítulo). Este camino tiene cierta desventaja pues no muestra que exista un polinomio con coeficientes *racionales* que no sea *soluble por radicales.* Sin embargo la otra alternativa (que adoptaremos en este momento) sera la de exhibir un polinomio especifico con coeficientes racionales cuyo grupo de Galois no sea soluble. Dado que calcular un grupo de Galois no es en general sencillo, necesitaremos de algún trabajo con el grupo simétrico y también de recurrir al "*Teorema Fundamental del Álgebra*".

14.2 Una ecuación quintica no soluble.

Lema 14.2.1. *Sea p un número primo y f un polinomio irreducible de grado p sobre $\mathbb{Q}$. Supongamos que f tiene exactamente dos ceros no reales en $\mathbb{C}$. Entonces el grupo de Galois de f sobre $\mathbb{Q}$ es el grupo simétrico $\mathbf{S_p}$.*

Prueba. Por el teorema fundamental de el álgebra, $\mathbb{C}$ contiene a un campo de descomposición Ξ para f. Sea G el grupo de Galois de f sobre $\mathbb{Q}$ considerado como grupo de permutaciones de los ceros de f. Estos ceros son distintos entre ellos pues la característica de $\mathbb{Q}$ es cero, por lo que G es un subgrupo de $\mathbf{S_p}$. Para la construcción de un campo de descomposición para un polinomio f lo primero que hicimos fue al campo original adjuntarle un elemento de grado p, por lo que $[\Xi : \mathbb{Q}]$ es divisible por p. Por el teorema 11.0.2, parte (1) tenemos que p divide al orden de G y por el teorema 13.3.13, se tiene que G tiene un elemento de orden p, pero los únicos elementos de orden p en $\mathbf{S_p}$ son los p-ciclos.

Por otro lado la conjugación compleja es un $\mathbb{Q}$-automorfismo de $\mathbb{C}$ y esta induce un $\mathbb{Q}$-automorfismo de Ξ dicho automorfismo inducido deja los $(p-2)$ ceros reales de f fijos y permuta los dos ceros no reales. Por lo tanto G contiene un 2-ciclo.

Para simplificar la notación podemos tomar una potencia de el p-ciclo para poder asumir que G contiene al 2-ciclo $(1\ 2)$ y al p-ciclo $(1\ 2\ \dots\ p)$. Pero por el lema 13.2.5, estas permutaciones generan todo $\mathbf{S_p}$. Así que $G = \mathbf{S_p}$. $\square$

En este momento nos encontramos en condiciones de poder exhibir un polinomio de grado cinco el cual no es soluble por radicales

Teorema 14.2.2. *El polinomio $t^5 - 6t + 3$ sobre $\mathbb{Q}$ no es soluble por radicales.*

Prueba. Por el criterio de Einseinstein tenemos que el polinomio $f(t) = t^5 - 6t + 3$ es irreducible sobre $\mathbb{Q}$. Habremos de mostrar que f tiene exactamente tres ceros reales cada uno de ellos de multiplicidad uno y por lo tanto tendrá dos ceros no reales. Dado que 5 es un número primo por el lema 14.2.1, el grupo de Galois de f sobre $\mathbb{Q}$ es $\mathbf{S_5}$ y por el corolario 13.2.4, $\mathbf{S_5}$ no es un grupo soluble, así pues por el teorema 14.1.9, f no es soluble por radicales. Lo que nos resta probar es que f tiene exactamente tres ceros reales, cada uno de ellos de multiplicidad uno. Como $f(-2) = -17$, $f(-1) = 8$, $f(0) = 3$, $f(1) = -2$, $f(2) = 23$ se sigue de el *teorema de el valor medio* que f tiene por lo menos tres ceros reales (pues f pensada como función real es continua) Un dibujo de la gráfica $y = f(x)$ se da en la siguiente figura.

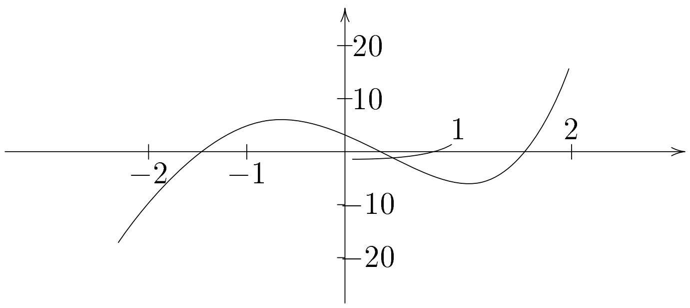

Figura 7.

En la gráfica solamente aparecen tres ceros reales pero esto lo argumentaremos de manera más rigurosa. Por el teorema de *Rolle* los ceros de f están 'separados' por los ceros de la derivada de f (Df) y $Df = 5t^4 - 6$ que solamente tiene dos ceros distintos en $\pm\sqrt{\frac{6}{5}}$. Ahora bien como f y Df son primos relativos (coprimos) se sigue que f no tiene ceros múltiples ó repetidos (esto se sigue de la irreducibilidad de f y la característica de $\mathbb{Q}$). Por lo que f tiene a lo más tres ceros reales. Por lo tanto f tiene exactamente tres ceros reales. $\square$

En cierto sentido este no es el fin de la historia, pues existen muchos caminos para probar que una ecuación quintica no puede ser soluble por radicales. Otro camino que usaremos en el siguiente capítulo es el de dar otra forma para probar que la ecuación de grado cinco no necesariamente es soluble por radicales. Este problema fue uno de los principales que resolvio Galois (posiblemente este resultado fue el que realmente lo encumbro a la fama).

14.3 Ejercicios.

14.1 Podrías construir un método (si es que no lo conoces) para resolver las ecuaciones cuarticas por radicales.

14.2 Encuentra extensiones radicales de $\mathbb{Q}$ que contengan los siguientes elementos de $\mathbb{C}$.

a) $\frac{\sqrt{11}-\sqrt[7]{23}}{\sqrt[4]{5}}$.

b) $(\sqrt{6}+2\sqrt[3]{5})^4$.

c) $\frac{2\sqrt[5]{5}-4}{\sqrt{1+\sqrt{99}}}$.

14.3 ¿Cuál es el grupo de Galois de t^p-1 sobre $\mathbb{Q}$ para un primo p?.

14.4 Muestra que los polinomios

t^5-4t+2

t^5-4t^2+2

t^5-6t^2+3

$t^7-10t^5+15t+5$

sobre $\mathbb{Q}$ son solubles por radicales.

14.5 Resuelve la ecuación de grado seis

$$t^6+2t^5-5t^4+9t^3-5t^2+2t+1=0$$

por radicales (sugerencia: realiza el cambio de variable $u=\frac{i}{t}$).

14.6 El grupo de permutaciones G de un conjunto X es *transitivo* si para cada par de elementos x,y en X existe un elemento $g\in G$ tal que $g(x)=y$. Muestra que el grupo de Galois de un polinomio irreducible es transitivo pensado como el grupo de permutaciones de los ceros del polinomio.

14.7 Si $(L:K)$ es un extensión radical y M es un campo intermedio, muestra que $(M:K)$ no necesariamente es una extensión radical.

14.8 Si p es un polinomio irreducible sobre K con un cero expresable por radicales, pruebe que cada cero de p es expresable por radicales.

14.9 Diga si las siguientes afirmaciones son verdaderas o falsas.

a) Toda ecuación cuartica sobre un campo de característica cero puede ser resuelta por radicales.

b) Toda extensión radical es finita.

c) Toda extensión finita es radical.

d) El orden de el grupo de Galois de un polinomio de grado n divide a $n!$.

e) Un polinomio quintico reducible es soluble por radicales.

f) Existen ecuaciones cuarticas con grupo de Galois $\mathbf{S_4}$.

g) Un polinomio irreducible de grado 11 con exactamente dos ceros no reales tiene grupo de Galois $\mathbf{S_{11}}$.

h) La cerradura normal de una extensión radical es radical.

i) $\mathbf{A_5}$ tiene 60 elementos.

Capítulo 15

La ecuación general.

El prefijo "General" en la frase la ecuación general no es en realidad más que un polinomio especifico, este prefijo es dado a un polinomio cuando los coeficientes de este satisfacen algunas relaciones algebraicas especificas. Estas propiedades hace simple el trabajo sobre los polinomios en $\mathbb{Q}$ y es que en este particular es fácil encontrar su grupo de Galois. Uno de los resultados que probaremos es que la ecuación (polinomio) quintico general no es soluble por radicales sin asumir la teoría desarrollada en el capítulo 14. Efectivamente esto implica que no existe una fórmula general mediante la cual todas las ecuaciones quinticas sean solubles por radicales.

Se puede predecir de lo anterior que el grupo de Galois de el polinomio general de grado n es el grupo simétrico $\mathbf{S_n}$. Esto muestra inmediatamente la no solubilidad de la ecuación quintica por radicales. Mientras que las estructuras de $\mathbf{S_2}, \mathbf{S_3}$ y $\mathbf{S_4}$ pueden ser usadas para encontrar métodos que resuelvan las ecuaciones generales cuadráticas, cubicas y cuarticas.

15.1 Grados de trascendencia.

Hasta este momento no hemos hablado mucho acerca de las extensiones trascendentes, hemos usado muchas veces la condición de finitud de las extensiones (la mayoría de las pruebas de los teoremas importantes las hemos hecho por inducción) en la teoría desarrollada. Necesitaremos en lo sucesivo el considerar otra clase de extensiones que definiremos ahora.

Definición 15.1.1. Una extensión de campos $(L : K)$ es una extensión *finitamente generada* si $L = K(\alpha_1, ..., \alpha_n)$ para n finito.

Note sin embargo que α_i puede ser tanto algebraico como trascendente sobre K.

Definición 15.1.2. Si $t_1, ..., t_n$ son elementos trascendentes sobre un campo K y todos ellos están dentro de alguna extensión L de K entonces decimos que las $t_i's$ son *independientes* si existe un polinomio no trivial p sobre K (en n-indeterminadas) tal que $p(t_1, ..., t_n) = 0$ en L.

Por ejemplo, si t es trascendental sobre K y u es trascendental sobre $K(t)$, entonces $K(t, u)$ es una extensión finitamente generada de K y t, u son independientes. En otro sentido t y $t + 1$ son ambos trascendentes sobre K pero ellos están conectados por una ecuación polinomial, por tal motivo ellos no constituyen un conjunto independiente.

El siguiente resultado nos da información acerca de la estructura de una extensión finitamente generada.

Lema 15.1.3. *Si $(L : K)$ es finitamente generada entonces existe un campo intermedio M tal que:*

1) $M = K(\alpha_1, : .., \alpha_r)$ donde las α_i son elementos trascendentes independientes sobre K.

2) $(L : M)$ es una extensión finita.

Prueba. Supongamos que $L = K(\beta_1, ..., \beta_n)$. Si todas las β_j son algebraicos sobre K entonces $(L : K)$ es finita por el lema 4.0.6 y podemos hacer la ellección de $M = K$.

En otro caso algún β_i es trascendente sobre K. Digamos que es α_1. Si la extensión $(L : K(\alpha_1))$ no es finita, entonces existe algún β_s trascendente sobre $K(\alpha_1)$. Digamos α_2. Continuamos este proceso hasta obtener $M = K(\alpha_1, ..., \alpha_r)$ tal que $(L : K)$ es finita. Por construcción las α_i son elementos trascendentes independientes sobre K. $\square$

Un resultado debido a *Steinitz* dice que el entero r de el lema anterior es independiente de la elección de M.

Lema 15.1.4 (Steinitz). *Con la notación de el lema anterior. Si existen otros campos intermedios $N = K(\beta_1, ..., \beta_s)$ tal que $\beta_1, ..., \beta_s$ son elementos trascendentes independientes sobre K y $(L : N)$ es finita, entonces $r = s$.*

Prueba. Dado que $[L : M]$ es finita entonces tenemos que β_1 es algebraico sobre M_1 por lo cual existe una ecuación polinomial tal que

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

Alguno de los α_i ocurre en la ecuación anterior digamos α_1 de este modo tenemos que α_1 es algebraico sobre $K(\beta_1, \alpha_2, ..., \alpha_r)$ y $(L : K((\beta_1, \alpha_2, ..., \alpha_r))$ es finita. Inductivamente podemos remplazar sucesivamente (como en el lema 15.1.3) a α_i por β_i. Por lo tanto $L : K(\beta_1, ..., \beta_r)$ es finita. Si $s > r$ entonces β_{r+1} es trascendente sobre $K(\beta_1, ..., \beta_r)$ lo cual no puede ser posible, así que $s \leq r$ intercambiando papeles tenemos también que $r \leq s$ por lo que $s = r$. $\square$

El resultado anterior nos dice que tenemos una buena elección para r, formularemos esto en la siguiente definición.

Definición 15.1.5. El entero r definido en el lema 15.3.1, es llamado el *grado de trascendencia* de $(L : K)$.

Por ejemplo, consideremos $(K(t, \alpha, u) : K)$ donde t es trascendente sobre K $\alpha^2 = t$ y u es trascendente sobre $K(t, \alpha)$. Entonces $M = K(t, u)$ donde t, u son elementos trascendentes independientes sobre K y la extensión

$$(K(t, \alpha, u) : M) = (M(\alpha) : M)$$

es finita, su grado de trascendencia es 2.

Un argumento de inducción prueba que la extensión $(K(\alpha_1, ..., \alpha_r) : K)$ por elementos trascendentes independientes α_i es isomorfa a $(K(t_1, ..., t_r) : K)$ donde $K(t_1, ..., t_r)$ es el campo de expresiones racionales en las indeterminadas $t_1, \ldots t_r$.

15.2 La ecuación general.

Si K es un campo y si $t_1, ..., t_n$ son elementos trascendentes independientes sobre K, entonces a el grupo simétrico $\mathbf{S_n}$ lo podemos hacer actuar como un grupo de K-automorfismos de $K(t_1, ..., t_n)$ definiendo

$$\sigma(t_i) = t_{\sigma(i)}.$$

para cada $\sigma \in \mathbf{S_n}$ y extendiendo de manera obvia esta acción a un K-aut.

Es también claro que distintos elementos de $\mathbf{S_n}$ dan distintos K-automorfismos. El campo fijo F de $\mathbf{S_n}$ obviamente contiene a todos los polinomios simétricos elementales $s_r = s_r(t_1, .., t_n)$. A continuación mostraremos que estos polinomios simétricos elementales generan a todo el campo fijo F.

Lema 15.2.1. *Con la notación anterior* $F = K(s_1, ..., s_n)$.

Prueba. Primero probaremos por inducción sobre n que

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

Para ello consideremos la doble extensión

$$K(t_1, ..., t_n) \supseteq K(s_1, ..., s_n t_n) \supseteq K(s_1, ..., s_n)$$

Ahora bien sabemos que $f(t_n) = 0$, donde

$$f(t) = t^n - s_1 t^{n-1} + ... + (-1)^n s_n$$

por lo que

$$[K(s_1, ..., s_n, t_n) : K(t_1, ..., t_n)] \leq n \tag{15.1}$$

Si renombramos por $s_1^{'}, ..., s_{n-1}^{'}$ a los polinomios simétricos elementales en las variables $t_1, ..., t_{n-1}$ tenemos que

$$s_j = t_n s_{j-1}^{'} + s_j^{'}$$

y de este modo

$$K(s_1, ..., s_n, t_n) = K(t_n, s_1^{'}, ..., s_{n-1}^{'})$$

Utilizando ahora la hipótesis de inducción tenemos que

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

Por lo que multiplicando por el grado en la ecuación 15.1, en el paso inductivo, obtenemos lo que queremos.

Ahora $K(s_1, ..., s_n)$ esta claramente contenida en el campo fijo F de $\mathbf{S_n}$. Por el teorema 9.0.4, tenemos que

$$[K(t_1, ..., t_n) : F] = \mid \mathbf{S_n} \mid = n!$$

y por lo anterior tenemos que $F = K(s_1, ..., s_n)$. □

Corolario 15.2.2. Todo polinomio simétrico contenido en $t_1, ..., t_n$ sobre K puede ser escrito como una expresión racional en $s_1, ..., s_n$.

Prueba. Es inmediata ya que los polinomios simétricos están "dentro" de el campo fijo F. □

Lema 15.2.3. *Con la notación anterior $s_1, ..., s_n$ son elementos trascendentes independientes sobre K.*

Prueba. Como $K(t_1, ..., t_n)$ es una extensión finita de $K(s_1, ..., s_n)$ y por lo tanto tienen el mismo grado de trascendencia sobre K, digamos n. De este modo tenemos que los s_i son independientes pues si no lo fueran tendríamos que el grado de trascendencia de $[K(s_1, ..., s_n) : K]$ sería menor que n. □

Definición 15.2.4. Sea K un campo si $s_1, ..., s_n$ son elementos trascendentes independientes sobre K. Definimos *el polinomio general de grado n 'sobre' K* como

$$t^n - s_1 t^{n-1} + s_2 tn - 2 - \ldots (-1)^n s_n.$$

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

Teorema 15.2.5. *Para un campo K, sea g el polinomio general de grado n 'sobre' K y sea Ξ un campo de descomposición para g sobre $K(s_1, ..., s_n)$. Entonces los ceros $t_1, ..., t_n$ de g en Ξ son elementos trascendentes independientes sobre K y el grupo de Galois de $[\Xi : K(s_1, ..., s_n)]$ es todo el grupo simétrico $\mathbf{S_n}$.*

Prueba. La extensión $[\Xi : K]$ es finita por el teorema 8.2.2, por lo que el grado de trascendencia es igual al grado de $(K(s_1, ..., s_n) : K)$ digamos que este grado es n. Dado que $\Xi = K(t_1, ..., t_n)$ se sigue que las t_i son elementos trascendentes independientes sobre K, dado que cualquier relación algebraica entre estos tendría un grado de trascendencia menor. Consideremos a s_i los polinomios simétricos (como en el capítulo 2) en $t_1, ..., t_n$. Como antes $\mathbf{S_n}$ actúa en el grupo de automorfismos de $\Xi = K(t_1, ..., t_n)$ y por el lema 15.2.1, el campo fijo es $K(s_1, ..., s_n)$. Por el teorema 10.2.9, $(\Xi : K(s_1, ..., s_n))$ es separable y normal (la normalidad también se sigue de la definición de Ξ como un campo de descomposición) y por el teorema 9.0.4, este grado es $\mid \mathbf{S_n} \mid = n!$. Entonces por el teorema 11.0.2, parte 1) el grupo de Galois tiene orden$n!$ y contiene a $\mathbf{S_n}$. Por lo tanto es $\mathbf{S_n}$. □

De el teorema 14.1.9 y de el corolario 13.2.4, podemos fácilmente deducir.

Teorema 15.2.6. *Si K es un campo de característica cero y $n \geq 5$ entonces la ecuación general de grado n 'sobre' K no es soluble por radicales.*

15.3 Solución de ecuaciones cuadráticas.

Dos importantes preguntas en este momento son las siguientes. ¿Cuando la ecuación general de grado n 'sobre' K puede ser soluble por radicales?, ¿Es fácil deducir una solución por radicales de un polinomio de grado n sobre K? Una respuesta parcial a estos cuestionamientos es la siguiente; Si substituimos elementos de K por los polinomios simétricos elementales, obtenemos una solución a la segunda pregunta (de este hecho toma precisamente su nombre la ecuación general (ó polinomio general)). De el teorema 15.2.6, tenemos una buena aproximación para poder resolver polinomios de grado menor o igual a cuatro. Dedicaremos el resto de este capítulo a encontrar dichas soluciones.

Definición 15.3.1. Sea $(L : K)$ una extensión normal finita con grupo de Galois G. la *norma* de un elemento $\alpha \in L$ es

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

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

Claramente $N(a)$ esta en el campo fijo de G (por el lema 9.0.3) por lo tanto si la extensión es también separable entonces $N(a) \in K$.

El siguiente es un resultado importante debido a *Hilbert* y referido como el teorema 90 de *Hilbert* (su aparición fue presentada en un reporte de números algebraicos publicada en 1893).

Teorema 15.3.2. *Sea $(L : K)$ una extensión finita, normal con grupo de Galois G cíclico generado por τ. Entonces $a \in L$ tiene norma 1 si, y solamente si $a = \frac{b}{\tau(b)}$ para algún $b \in L$ con $b \neq 0$.*

Prueba. Si $a = \frac{b}{\tau(b)}$ con $b \neq 0$ entonces, si $\mid G \mid = n$ tenemos que

$$N(a) = a\tau(a)\tau^2(a)\cdots\tau^{n-1}(a) = \frac{b}{\tau(b)}\frac{\tau(b)}{\tau^2(b)}\cdots\frac{\tau^{n-1}(b)}{\tau^n(b)} = 1$$

pues $\tau^n(b) = 1$.

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

$$d_0 = ac, d_1 = (a\tau(a))\tau(c), ..., d_i = (a\tau(a)\cdots\tau^i(a))\tau^i(c)$$

para $0 \leq i \leq n-1$. Entonces $d_{n-1} = N(a)\tau^{n-1}(c) = \tau^{n-1}(c)$ así que

$$d_{i+1} = a\tau(d_i)$$

para $0 \leq i \leq n-2$.

Definimos ahora $b = d_0 + d_1 + ... + d_{n-1}$. Además podemos elegir a c de tal manera que $b \neq 0$. Para justificar esto supongamos lo contrario es decir que $b = 0$ para cualquier elección posible de c. Entonces para algún $c \in L$ tenemos que $\lambda_0\tau^0(c) + \lambda_1\tau(c) + ... + \lambda_{n-1}\tau n - 1(c) = 0$, donde $\lambda_i = a\tau(a)\cdots\tau^i(a)$ es un elemento de L. Por lo tanto los distintos automorfismos τ^i son linealmente independientes sobre L. Lo cual contradice el lema 9.0.1. Por lo que podemos elegir a c tal que $b \neq 0$. pero

$$\begin{aligned}
\tau(b) &= \tau(d_0) + \cdots + \tau(d_{n-1}) \\
&= \frac{1}{a}(d_1 + \ldots + d_{n-1} + \tau^n(c)) \\
&= \frac{1}{a}(d_1 + \ldots + d_n) \\
&= \frac{b}{a}
\end{aligned}$$

de este modo $a = \frac{b}{\tau(b)}$. □

Teorema 15.3.3. *Supongamos que $(L : K)$ es una extensión finita separable y normal con grupo de Galois cíclico de orden primo p, generado por τ. Supongamos que la característica de K es cero ó la característica de K es el primo p y que $t^p - 1$ se divide en K. Entonces $L = (\alpha)$ donde α es un cero de un polinomio irreducible $t^p - a$ sobre K, para algún $a \in K$.*

Prueba. Sabemos que los p ceros de $t^p - 1$ forman un grupo de orden p que tiene que ser cíclico por lo que los ceros de $t^p - 1$ son las potencias de algún $\epsilon \in K$, donde $\epsilon^p = 1$. Pero entonces $N(\epsilon)\epsilon\cdots\epsilon = 1$. Dado que $\epsilon \in K$ tenemos que $\tau^i(\epsilon) = \epsilon$ para toda i, por el teorema 15.3.2, tenemos que $\epsilon = \frac{\alpha}{\tau(\alpha)}$ para algún $\alpha \in L$.

Se sigue que $\tau(\alpha) = \epsilon^{-1}\alpha$, $\tau^2 = \epsilon^{-2}\alpha$,... y $a = \alpha^p$ queda fijo por todo elemento de G por tal motivo $a \in K$. Ahora como $K(\alpha)$ es un campo de descomposición sobre K. Los K-automorfismos $1, \tau, \ldots \tau^{p-1}$ transforman a α a elementos distintos, por lo que estos dan distintos K-automorfismos de $K(\alpha)$. Por el teorema 11.0.2 parte (1) $[K(\alpha) : K] \geq p$. Pero $[L : K] = \mid G \mid = p$, por lo que $L = K(\alpha)$. Por lo tanto $t^n - a$ es el polinomio mínimo de α sobre K (en otro caso tendríamos que $[K(\alpha) : K] < n$) por lo tanto irreducible sobre K. $\square$

En este momento nos encontramos en condiciones de probar el recíproco de el teorema 14.1.9.

Teorema 15.3.4. *Sea K un campo de característica cero y $(L : K)$ una extensión normal finita con grupo de Galois soluble G. Entonces existe una extensión R de L tal que $[R : K]$ es radical.*

Prueba. Todas las extensiones son separables dada que la característica de K es cero. Así pues haremos la prueba por inducción sobre $\mid G \mid$. El resultado es trivial cuando $\mid G \mid = 1$.

Ahora bien si $\mid G \mid \neq 1$ entonces tomamos un subgrupo normal máximo H de G (el cual existe dado que G es un grupo finito). De donde tenemos que G/H es simple y soluble por el teorema 13.1.3, parte (2). Por el teorema 13.2.2, G/H es cíclico de orden primo p. Consideremos ahora un campo de descomposición N sobre L de el polinomio $t^p - 1$. Entonces $(N : K)$ es normal; de el teorema 8.2.2, tenemos que L es un campo de descomposición sobre K de algún polinomio f y por tanto N es también un campo de de descomposición sobre L de el polinomio $(t^p - 1)f$, nuevamente por el teorema 8.2.2, tenemos que $(N : K)$ es normal. Como el grupo de Galois de $(N : L)$ es abeliano por el lema 14.1.6 y el teorema 11.0.2, parte (5) $\Gamma(L : K)$ es isomorfo a $\Gamma(N : K)/\Gamma(N : L)$. Por el teorema 13.1.3, parte (3) tenemos que $\Gamma(N : K)$ es soluble. Por ultimo si M es el subcampo de N generado por K y los ceros de $t^p - 1$ entonces $(M : N)$ es una extensión normal. Ahora bien $(M : K)$ es claramente una extensión radical y dado que $L \subseteq N$ el resultado deseado lo obtenemos probando que podemos encontrar una extensión R de

N tal que $(R : M)$ sea radical.

Para ello probaremos primero la siguiente afirmación. El grupo de Galois de $(N : M)$ es isomorfo a un subgrupo de G. Para probar esto consideremos τ un M-automorfismo de N τ, como la restricción $\tau\mid_L = L$ dado que $(L : K)$ es normal $\tau\mid_L$ es un K-automorfismo de L. De esta manera tenemos un homomorfismo de grupos

$$\Phi : \Gamma(N : M) \longrightarrow \Gamma(L : K)$$

Observemos que si τ esta en el núcleo de Φ entonces τ fija todos los elementos de L y de M y estos a su vez generan a todo N. Así pues τ en el núcleo de Φ implica que $\tau = 1$, por lo que Φ es un monomorfismo y por tanto $\Gamma(N : M)$ es isomorfo a un subgrupo J de $\Gamma(L : K)$

Si $J = \Phi(\Gamma(N : M))$ es un subgrupo propio de G entonces por hipótesis de inducción tenemos que existe una extensión R de N tal que $(R : M)$ es radical. Solamente nos resta ver que sucede cuando $J = G$. En este caso consideramos $I = \Phi^{-1}(H)$ y de este modo tenemos que $I \trianglelefteq \Gamma(N : M)$. Sea P el campo fijo de $I^{\dagger}$. Entonces $[P : M] = p$ (por el teorema 11.0.2 parte (3)). $(P : M)$ es normal (par el teorema 11.0.2 parte (4)) y $t^p - 1$ se divide en M. Por el teorema 15.3.3 $P = M(\alpha)$ donde $\alpha^p = a \in M$. Pero $(N : P)$ es una extensión normal que tiene grupo de Galois soluble de orden menor que $\mid G \mid$, nuevamente por hipótesis de inducción tenemos que existe una extensión R de N tal que $(R : P)$ es radical. Pero entonces $(R : M)$ es radical. □

Observemos que cuando trabajemos en campos de característica $p > 0$ tenemos que definir una extensión radical de otra manera, esta es adjuntándole al campo elementos α tal que α^n pertenezca al campo dado, pero también adjuntándole los elementos α tal que α^p pertenezca también al campo dado (donde p es la característica de el campo). De esta manera tenemos que un polinomio es soluble por radicales si, y sólo si su grupo de Galois es soluble. La prueba de este hecho difiere de la otra en considerar extensiones de grado p sobre campos de característica p y la prueba de el teorema 15.3.3, no funciona para extensiones de este segundo tipo. Si modificamos la definición de solubilidad por radicales entonces aunque cada polinomio soluble tiene grupo soluble el recíproco no necesariamente es cierto, algunos polinomios cuadráticos tienen grupo de Galois abeliano y no solubles por radicales (ver ejercicios 13.12 y 13.13).

Dado que un campo de descomposición es siempre una extensión normal se tiene:

Teorema 15.3.5. *Sobre un campo de característica cero, un polinomio es soluble por radicales si, y sólo si tiene grupo de Galois soluble.*

Prueba. Es inmediata usando los teoremas 14.1.9 y 15.3.4. □

La ecuación general (ó polinomio general) de grado n tiene grupo de Galois $\mathbf{S_n}$ y sabemos que para $n \leq 4$ este grupo es soluble (ver ejemplos al inicio de el capítulo 13). Por lo tanto, resulta ser que para un campo de característica cero el polinomio general de grado menor o igual a cuatro puede ser resuelto por radicales (también se dice que un polinomio de grado menor o igual a cuatro es soluble por radicales).

Además podemos usar la estructura de el grupo simétrico para encontrar dicha solución, a continuación daremos los métodos para encontrar la solución por radicales de un polinomio de grado menor o igual a cuatro.

1. Si el polinomio es lineal, es decir de grado 1 entonces el polinomio tiene la forma $t - s_1$ el cual trivialmente tiene como única solución (ó único cero) a $t_1 = s_1$.

2. Si el polinomio es de grado dos (ó la ecuación es cuadrática) digamos.

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

Entonces, si los ceros de este polinomio son t_1, t_2 se tiene que el grupo de Galois de $\mathbf{S_2}$ consiste solamente de el morfismo identidad y de el morfismo que intercambia a t_1 con t_2. Por lo tanto $(t_1 - t_2)^2$ queda fijo por todo $\mathbf{S_2}$, por lo que dicho elemento esta en $K(s_1, s_2)$. Mediante un calculo explicito tenemos que $(t_1 - t_2)^2 = s_1^2 - 4s_2$. Por lo tanto tenemos las siguientes ecuaciones

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

y

$$t_1 + t_2 = s_1.$$

con esto obtenemos la fórmula conocida

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

3. Si el polinomio es de grado tres, (ó la ecuación es cubica) digamos

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

Entonces, si los ceros de este polinomio son t_1, t_2, t_3 se tiene que el grupo de Galois $\mathbf{S_3}$ tiene como serie de composición a

$$1 \trianglelefteq \mathbf{A_3} \trianglelefteq \mathbf{S_3}.$$

con cocientes abelianos. Adjuntándole un elemento $\omega \neq 1$ tal que $\omega^3 = 1$ consideramos a

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

y como los elementos de $\mathbf{A_3}$ permutan a t_1, t_2 y t_3 cíclicamente. Por lo tanto y^3 queda fijo por $\mathbf{A_3}$. Similarmente si

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

entonces z^3 queda fijo por $\mathbf{A_3}$

Ahora cualquier permutación impar de $\mathbf{S_3}$ intercambia y^3 y z^3 por lo que

$$y^3 + z^3$$

y

$$y^3 z^3$$

quedan fijos por todo $\mathbf{S_3}$ por lo que están en $K(s_1, s_2, s_3)$ (Explícitamente la fórmula esta dada en la sección final de este capítulo). Por lo tanto y^3 y z^3 son los ceros de un polinomio cuadrático sobre $K(s_1, s_2, s_3)$ que puede ser resuelto como en la parte **2** y tomando raíces cubicas obtenemos a y y z. Pero dado que $s_1 = t_1 + t_2 + t_3$ de sigue que

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

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

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

4. Si el polinomio es de grado tres (ó la ecuación es cuartica) digamos,

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

Entonces, si los ceros de este polinomio son t_1, t_2, t_3 y t_4. Como el grupo de Galois de el polinomio anterior es $\mathbf{S_4}$, y este tiene serie de composición

$$1 \trianglelefteq V \trianglelefteq \mathbf{A_4} \trianglelefteq \mathbf{S_4}$$

con grupos cocientes abelianos y donde:

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

Es además natural el considerar las expresiones

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

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

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

Estas a su vez son permutadas por los elementos de $\mathbf{S_4}$ por lo que los polinomios simétricos elementales en y_1, y_2, y_3 están en $K(s_1, s_2, s_3, s_4)$ (una fórmula explicita esta dada más adelante). Entonces tenemos que por lo anterior y_1, y_2, y_3 son ceros de una cierta raíz cubica sobre $K(s_1, s_2, s_3, s_4)$ llamada la *resolvente cubica.* Dado que

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

podemos encontrar tres polinomios cuadráticos cuyos ceros son $t_1 + t_2$ y $t_3 + t_4$, $t_1 + t_3$ y $t_2 + t_4$, $t_1 + t_4$ y $t_2 + t_3$. De estos polinomios es fácil encontrar t_1, t_2, t_3, t_4.

Para completar las fórmulas explicitas antes aludidas referimos par ver detalles a *Van der Warden* [5] pag.177.

Cubica. Por la transformación de *Tschirnhaus* tenemos que si hacemos

$$u = t + \frac{1}{3}s_1$$

entonces la ecuación general toma la forma

$$u^3 + pu + q.$$

Si podemos encontrar los ceros de este polinomio será fácil de encontrar los ceros de la ecuación cubica general. Siguiendo el procedimiento anterior resolveremos este polinomio de manera explicita, así pues tenemos que

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

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

para el cual se sigue y^3 y z^3 son ceros de el polinomio cuadrático

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

Lo cual resuelve el problema.

Cuartica. Nuevamente consideremos la transformación de *Tschirnaus*

$$u = t + \frac{1}{4}s_1$$

la cual reduce al polinomio cuartico a uno de la forma

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

y en este caso procedemos como antes y obtenemos

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

$$y_1y_2 + y_1y_3 + y_2y_3 = p^2 - 4r$$
$$y_1y_2y_3 = -q^2$$

así pues la resolvente cubica toma la forma

$$t^3 - 2pt^2 + (p^2 - 4r)t + q^2$$

cuyos ceros son y_1, y_2, y_3 y se tiene que

$$2t_1 = \sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}$$

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

las raíces cuadradas elegidas existen puesto que $\sqrt{-y_1}, \sqrt{-y_2}, \sqrt{-y_3} = -q$.

15.4 Ejercicios.

15.1 Si K es un campo con un número numerable de elementos y $(L : K)$ es finitamente generada, muestra que L es numerable. Por lo tanto $(\mathbb{R} : \mathbb{Q})$ y $(\mathbb{C} : \mathbb{Q})$ no son finitamente generadas.

15.2 Calcula el grado de trascendencia de las siguientes extensiones

a) $(\mathbb{Q}(t, u, v, w) : \mathbb{Q})$ donde t, u, v, w son elementos trascendentes independientes sobre $\mathbb{Q}$

b) $(\mathbb{Q}(t,u,v,w):\mathbb{Q})$ donde $t^2=2$ es trascendente sobre $\mathbb{Q}(t)$, $v^3=t+5$ y w es trascendente sobre $\mathbb{Q}(t,u,v)$.

c) $(\mathbb{Q}(t,u,v):\mathbb{Q})$ donde $t^2=u^3=v^4=7$.

15.3 Muestra que en el lema 15.1.3, el grado $[L:M]$ no es independiente a la elección de M. (Sugerencia: considera $K(t^2)$ como un subcampo de $K(t)$).

15.4 Supón que $K\subseteq L\subseteq M$ y las extensiones $(M:K)$ y $(L:K)$ son finitamente generadas. Entonces muestra que las extensiones anteriores tienen el mismo grado de trascendencia si y sólo si $(M:L)$ es finita.

15.5 Usando el resultado que cada grupo finito es isomorfo a un subgrupo de $\mathbf{S_n}$ para algún n, muestra que un grupo finito es isomorfo al grupo de Galois de alguna extensión finita (Un problema no resuelto aún es que dado un grupo este sea el grupo de Galois de una extensión normal finita de $\mathbb{Q}$).

15.6 Dado un campo K muestra que x^3-3x+1 es irreducible ó se divide en K (Sugerencia: Muestra que un cero es una expresión racional de algún otro cero).

15.7 Sea K un campo de característica cero y supóngase que $(L:K)$ es normal y finita con grupo de Galois G. Dada $a\in L$ definamos la *traza*

$$T(a)=\tau_1(a)+\ldots\tau_n(a)$$

donde $\tau_1,\ldots,\tau_n$ son los distintos elementos de G. Muestra que $T(a)\in K$ y que

$$T:L\longrightarrow K$$

es una transformación suprayectiva.

15.8 Si en el ejercicio anterior G es cíclico con generador τ, muestra que $T(a)=0$ si, y sólo si $a=b-\tau(b)$ para algún $b\in L$.

15.9 Resuelve por radicales los siguientes polinomios sobre $\mathbb{Q}$

a) t^3-7t+5.

b) $t^3 - 7t + 6$.

c) $t^4 + 5t^3 - 2t - 1$.

d) $t^4 + 4t + 2$.

15.10 Muestra que una extensión algebraica finitamente generada es finita y encuentra una extensión algebraica que no sea finitamenta generada.

15.11 Di si las siguientes afirmaciones son verdaderas o falsas.

a) Toda extensión finita es finitamente generada.

b) Toda extensión finitamente generada es algebraica.

c) El grado de trascendencia de una extensión finitamente generada es invariante bajo isomorfismos.

d) Si $t_1, \ldots, t_n$ son elementos trascendentes independientes entonces sus polinomios simétricos son también elementos trascendentes independientes.

e) El grupo de Galois de el polinomio general de grado n es soluble para todo número n.

f) La ecuación general quintica es soluble por radicales.

g) La transformación de la *norma* es un homomorfismo de campos.

h) Los únicos subgrupos propios de $\mathbf{S_3}$ son 1 y $\mathbf{A_3}$.

i) El polinomio general de grado n 'sobre' K es un polinomio en una indeterminada sobre K.

j) El grado de trascendencia de $(\mathbb{Q}(t) : \mathbb{Q})$ es uno.

Capítulo 16

Campos finitos.

Los campos que solamente tienen un número finito de elementos juegan un papel fundamental en muchas ramas de las matemáticas, tales como; teoría de números, teoría de grupos, geometría proyectiva y muchas más. Los ejemplos más comunes de estos campos son los $\mathbb{Z}_p$ para p un número primo, pero estos no son todos los campos finitos. En este capítulo daremos una clasificación completa de todos los campos finitos y se probará que los campos finitos están determinados de manera única (hasta isomorfismo) por el número de elementos que tienen; y además dicho número debe de ser una potencia de algún número primo, pero además para cada numero n existe un campo con p^n elementos.

16.1 Campos finitos.

Iniciaremos esta sección probando la segunda de las condiciones mencionas anteriormente.

Teorema 16.1.1. *Si F es un campo finito entonces F tiene característica $p > 0$ y el número de elementos de F es p^n, donde n es el grado de F sobre su subcampo primo.*

Prueba. Sea P el subcampo primo de F. Sabemos que P no es isomorfo a

$\mathbb{Q}$, pues $\mathbb{Q}$ tiene un número infinito de elementos, por lo que P es isomorfo a algún $\mathbb{Z}_p$ (para algún número primo p) y por el teorema 1.2.2, tenemos que F tiene característica p. Por el teorema 4.0.1, se tiene que F es un espacio vectorial sobre P y además este espacio vectorial tiene solamente un número finito de elementos, por lo que es dimensionalmente finito. Por lo tanto $[F : P] = n$ es finita. Consideremos $\beta = \{x_1, \ldots, x_n\}$ base de F sobre P. De este modo tenemos que cualquier elemento de F puede ser expresado de manera única de la forma.

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots \lambda_n x_n$$

donde λ_i esta en P para toda i y como $|P| = p$ entonces λ_1 solamente puede ser elegida de p-distintas maneras, así pues como solamente hay p^n expresiones de la manera descrita anteriormente, se tiene que $|F| = p^n$ $\square$

De este resultado se sigue que no existen campos con $6, 10, 12, 14, \ldots$ elementos. Notemos el contraste de este hecho con lo que sucede en la teoría de grupos, donde hay por lo menos un grupo para de cualquier orden dado. Sin embargo en la teoría de grupos existen grupos no isomorfos que tienen el mismo orden. Este es un hecho que no sucede en los campos finitos y para probarlo primeramente probaremos un lema, el cual es un resultado que esta implícito en el capítulo 8.

Lema 16.1.2. *Sea K un campo de característica $p > 0$. Entonces la función*

$$\phi : K \longrightarrow K$$

definida como $\phi(k) = k^p$ para $k \in K$, es un monomorfismo de campos. Si K es finito entonces ϕ es un automorfismo.

Prueba. Sean $x, y \in K$ entonces

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$$

y también

$$\phi(x + y) = (x + y)^p = x^p + px^{p-1}y + (\frac{p!}{(p-2)!2!})x^{p-2}y^2 + \cdots + pxy^{p-1} + y^p.$$

lo anterior es por el teorema de el binomio. Como observamos en el capítulo 8, cuando dimos el ejemplo de un polinomio no separable (inseparable) los coeficientes binomiales necesariamente son divisibles por p. Por lo que la suma anterior se reduce a

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

Por lo tanto ϕ es un homomorfismo de campos. Pero $\phi(1) = 1 \neq 0$ por lo que por el lema 3.2.6, tenemos que ϕ es un monomorfismo.

Ahora bien si K es un campo finito, entonces cualquier monomorfismo de K en si mismo es automáticamente un epimorfismo. Por lo tanto un automorfismo. $\square$

Definición 16.1.3. Si K es un campo de característica $p > 0$. Entonces el monomorfismo

$$\phi : K \longrightarrow K$$

dada por $\phi(k) = k^p$ para $k \in K$ es llamado el *monomorfismo de Frobenius* de K. Si K es finito entonces para referir al monomorfismo anterior le llamaremos el *automorfismo de Frobenius.*

Por ejemplo, para el campo $\mathbb{Z}_5$ tenemos que ϕ es el homomorfismo identidad, para el campo de el ejercicio 1.6 se tiene que $\phi(0) = 0, \phi(1) = 1, \phi(\alpha) = \beta$ y $\phi(\beta) = \alpha$. Motivo por el cual ϕ no siempre es el homomorfismo identidad.

Teorema 16.1.4. *Sea p un número primo y n un número entero mayor que cero. Un campo F tiene $q = p^n$ elementos si, y sólo si este es un campo de descomposición para el polinomio $f(t) = t^q - t$ sobre el subcampo primo $P \simeq \mathbb{Z}_p$ de F.*

Prueba. Supongamos que $|F| = q$. Consideremos el conjunto $F - \{0\}$ este conjunto forma un grupo bajo la multiplicación de orden $q - 1$; por lo que si $0 \neq x \in F$ entonces $x^{q-1} = 1$. Por lo que $x^q - x = 0$. Dado que $0^q - 0 = 0$ entonces todo elemento de F es un cero de el polinomio $t^q - t$, por tanto $f(t)$ se divide en F. Dado que los ceros de f son todos los elementos de F

tenemos que F es un campo de descomposición de f sobre P.

Recíprocamente, sea K un campo de descomposición de f sobre $\mathbb{Z}_p$. Dado que $Df = -1$ se tiene que f y Df son coprimos, por lo que todos los ceros de f en K son distintos, de este modo tenemos que f tiene exactamente q ceros. Supongamos que x, y son ceros de f. Entonces $x^q = \phi^n(\alpha)$ donde ϕ es el monomorfismo de Frobenius. Como ϕ^n es también un monomorfismo (es fácil de verificar) se tiene que los ceros de f cumplen;

$$(xy)^q - xy = x^q y^q - xy = xy - xy = 0$$

$$(x + y)^q - (x + y) = x^q + y^q - (x + y) = 0$$

$$(x^{-1})^q - x^{-1} = x^{-q} - x^{-1} = x^{-1} - y^{-1} = 0$$

Por lo tanto, los ceros de f forman un campo en K que además tiene que ser el campo de descomposición (pues están todos los ceros distintos que son q). Por lo tanto $|K| = q$. $\square$

Dado que los campos de descomposición son únicos salvo isomorfismo fácilmente se deduce el siguiente

Teorema 16.1.5. *Un campo finito tiene exactamente $q = p^n$ elementos para algún número primo p y algún número entero mayor que cero, además para cada uno de estos tales q existe un único campo salvo isomorfismo con q elementos que además puede ser construido como el campo de descomposición para el polinomio $t^q - t$ sobre $\mathbb{Z}_p$.*

Notación:
Al campo con q elementos de el teorema anterior lo denotaremos por $\mathbb{F}_q$.

16.2 El grupo multiplicativo.

La anterior clasificación de campos finitos, no da una gran información respecto a las diferentes tipos de estructuras que hemos analizado antes, como lo son ¿Como son los campos intermedios?, ¿Cuantos de estos campos intermedios hay?, ¿Cuales son sus respectivos grupos de Galois?. A continuación probaremos un resultado muy importante, usando la estructura de grupo multiplicativo $F - \{0\}$ para un campo finito F. Necesitaremos algunos resultados de la teoría de grupos que daremos a continuación.

Definición 16.2.1. El *exponente* $e(G)$ de un grupo finito G es el mínimo común múltiplo de los ordenes de los elementos de G.

Claramente $e(G)$ divide al orden de G. En general G no necesariamente tiene un elemento de orden $e(G)$; por ejemplo, si $G = \mathbf{S_3}$ entonces $e(G) = 6$ pero G no tiene elementos de orden 6. Resulta un hecho muy interesante que los grupos abelianos si se comportan bien con respecto a la observación hecha anteriormente y este es el primer resultado que probaremos.

Lema 16.2.2. *Un grupo abeliano finito G contiene un elemento de orden $e(G)$.*

Prueba. Sea $e = e(G) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ donde los p_i son números primos distintos y $\alpha_1 \geq 1$. Entonces G tiene un elemento g_i de orden $p_i^{\alpha_1}$ (por la definición de $e(G)$), así que alguna potencia a_i de g_i tiene orden $p_i^{\alpha_i}$. Definamos

$$g = a_1 a_2 \cdots a_n$$

Supongamos que $g^m = 1$ donde $n \geq 1$ entonces

$$a_i^m = a_1^{-1} \cdots a_{i-1}^{-m} a_{i+1}^{-m} \cdots a_n^{-m}$$

Por lo que si

$$q = p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n}$$

entonces $a_i^{mq} = 1$. Pero q es coprimo a el orden de a_i, por lo que $p_i^{\alpha_i}$ divide a m. Por lo tanto e divide a m. Pero claramente $g^e = 1$. Por lo tanto g tiene orden e, que es lo que queríamos probar. □

Corolario 16.2.3. Sea G un grupo abeliano finito tal que $e(G) = |G|$ entonces G es cíclico.

Prueba. El elemento g construido en el lema anterior, genera a G. $\square$

Aplicando este resultado tenemos.

Teorema 16.2.4. *Sea G un subgrupo finito de el grupo multiplicativo $K-\{0\}$ de un campo K, entonces G es cíclico.*

Prueba. Dado que la multiplicación en K es conmutativa, entonces G es un grupo abeliano, llamemosle $e = e(G)$. Entonces para $x \in G$ se tiene que $x^e = 1$, por lo que x es un cero del polinomio $t^e - 1$ sobre K. Por el teorema 2.3.5, hay a lo más e ceros de este polinomio, por lo tanto $|G| \leq e$, pero $e \leq |G|$. Por lo tanto $|G| = e$ y por el corolario anterior se tiene que G es cíclico. $\square$

Corolario 16.2.5. El grupo multiplicativo de un campo finito es cíclico.

Resumiendo, para un campo finito F existe al menos un elemento x tal que cada elemento no cero de F es una potencia de x. A continuación daremos dos ejemplos.

1. En el campo $\mathbb{F}_{11}$, las potencias de 2, en orden, son;

$$1, 2, 4, 5, 10, 9, 7, 3, 6, 1$$

así que 2 genera a el grupo multiplicativo $\mathbb{F}_{11}-\{0\}$. Sin embargo las potencias de cuatro son;

$$1, 4, 5, 9, 3, 1$$

así que el 4 no genera a $\mathbb{F}_{11} - \{0\}$.

2. El campo $\mathbb{F}_{25}$ puede ser construido como un campo de descomposición para el polinomio $t^2 - 2$ sobre $\mathbb{Z}_5$, dado que $t^2 - 2$ es irreducible y de grado dos, podemos representar los elementos de $\mathbb{F}_{25}$ como $a + b\alpha$ con $\alpha^2 = 2$. Aunque no hemos escrito $\alpha = \sqrt{2}$, no nos alarmemos de este hecho, pues esta propiedad caracteriza a α. Consideremos ahora el elemento $2 + \sqrt{2}$ sus potencias sucesivas son;

$$1, 2+\sqrt{2}, 1+4\sqrt{2}, 4\sqrt{2}, 3+3\sqrt{2}, 2+4\sqrt{2}, 2, 4+2\sqrt{2}, 2+3\sqrt{2},$$

$$3\sqrt{2}, 1+\sqrt{2}, 4+3\sqrt{2}, 4, 3+\sqrt{2}, 4+\sqrt{2}, \sqrt{2}, 2+2\sqrt{2}, 3+\sqrt{2}, 3,$$
$$1+3\sqrt{2}, 3+2\sqrt{2}, 2\sqrt{2}, 4+4\sqrt{2}, 1+2\sqrt{2}, 1$$

Por lo tanto, $2+\sqrt{2}$ genera a el grupo multiplicativo $\mathbb{F}_{25} - \{0\}$.

En general no existe un procedimiento para encontrar un generador de $\mathbb{F}_q - \{0\}$ que no sea a prueba y error. Afortunadamente la existencia de un generador es casi siempre información suficiente.

16.3 Ejercicios.

16.1 ¿Para cuáles de los siguientes valores de n existe un campo con n elementos?

1, 2, 3, 4, 5, 6, 17, 24, 312, 65536, 65537, 83521, 103823,$2^{528} - 1$.

16.2 ¿Cuáles de los resultados de este capítulo implican revisar los teoremas 8.1.5 y 8.2.2?.

16.3 Construyanse campos que tienen 8, 9 y 16 elementos.

16.4 Sea ϕ el automorfismo de Frobenius de $\mathbb{F}_{p^n}$. Encuentre el mínimo valor $m > 0$ tal que ϕ^m es el automorfismo identidad.

16.5 Muestre que los subcampos de $\mathbb{F}_{p^n}$ son isomorfos a $\mathbb{F}_{p^r}$ donde r divide a n.

16.6 Muestre que el grupo de Galois de $(\mathbb{F}_{p^n} : \mathbb{F}_p)$ es cíclico de orden n, generado además por el automorfismo de Frobenius ϕ. Muestra que para campos finitos la correspondencia de Galois es una biyección y encuentra el grupo de Galois de $(\mathbb{F}_{p^n} : \mathbb{F}_{p^m})$ siempre que m divide a n.

16.7 ¿Existe siempre un número compuesto r que divida a los coeficientes binomiales $\binom{r}{s}$, para $1 \leq s \leq r-1$?

16.8 Encuentre generadores para los grupos multiplicativos $\mathbb{F}_{p^n}$ cuando $n =$

8, 9, 13, 17, 19, 23, 29, 31, 37, 41 y 44.

16.9 Muestre que el grupo aditivo de $\mathbb{F}_{p^n}$ es un producto directo de n-grupos cíclicos de orden p.

16.10 Considerando el campo $\mathbb{Z}_2(t)$ muestra que el monomorfismo de Frobenius no siempre es un automorfismo.

16.11 Para cada valor n, pruebe que $\mathbf{S_n}$ no contiene un elemento de orden $s(\mathbf{S_n})$. (Sugerencia; use la descomposición cíclica para estimar el máximo orden de un elemento de $\mathbf{S_n}$ y compare esto con una estimación de $e(\mathbf{S_n})$)

16.12 Marque verdadero ó falso según sea el caso.

a) Existe un campo finito con 124 elementos.

b) Existe un campo finito cuyo grupo multiplicativo tiene 124 elementos

c) Existe un campo finito con 125 elementos.

d) El grupo multiplicativo de $\mathbb{F}_9$ contiene un elemento de orden 3.

e) Todos los campos con 121 elementos son isomorfos.

f) $\mathbb{F}_{2401}$ tiene un subcampo isomorfo a $\mathbb{F}_{49}$.

g) Un monomorfismo de un campo finito en si mismo es un automorfismo.

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

i) El grupo multiplicativo de un campo es cíclico.

j) El exponente de un grupo, es el máximo de los ordenes de sus elementos.

Capítulo 17

Polígonos regulares.

En este momento regresaremos a trabajar (ahora con herramientas más sofisticadas) los problemas con regla y compás. La principal pregunta en este momento es : ¿Para cuáles valores de n puede ser construido con regla y compás el polígono regular con n lados?.

En la antigua Grecia se conocía la construcción para los 3-agonos, 5-agonos y 15-agonos; y también se conocía una construcción de el $2n$-agono, dado un n-agono, dicha construcción es muy sencilla, solamente hay que bisecar el ángulo.

Por cerca de 2000 años se hicieron pocos progresos en cuanto a este problema. Finalmente el 30 de marzo de 1796, *Gauss* realizo un importante descubrimiento para construir el 17-agono. Gauss contaba con solamente 19 años de edad cuando resolvió este problema. En su *Disquisitions Arithmeticae [39]* Gauss estableció condiciones necesarias y suficientes para la construcción de el n-agono regular y probo la suficiencia de estas condiciones. Aunque se dice que el también tenia la prueba de la necesidad esta nunca fue publicada.

17.1 Construcciones posibles.

Para obtener las condiciones de necesidad y suficiencia para las construcciones con regla y compás de dichos n-agonos, tendremos que probar teoremas más detallados que los realizados en le sección 5.2.

Lema 17.1.1. *Sea $P \subseteq \mathbb{R}^2$, talque P contiene los puntos $(0,0)$ y $(0,1)$, entonces el punto (x,y) es construible a partir de P siempre que x,y estén en el subcampo R generado por las coordenadas de los puntos en P.*

Prueba. Dado un punto (x_0, y_0) es obvio que podemos construir $(0, x_0)$ y $(0, y_0)$. De $(0,0)$ y $(1,0)$ podemos construir los ejes coordenados y entonces procedemos como se muestra en la siguiente figura.

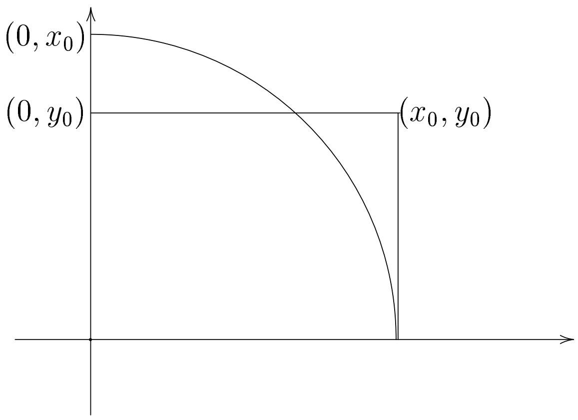

Figura 9.

Así que si $(0, x_0)$ y $(0, y_0)$ están dados, entonces la misma construcción en (sentido inverso) da una construcción de (x_0, y_0). Por lo que para probar el lema es suficiente con mostrar que dados $(0,x)$ y $(0,y)$ se pueden construir los puntos $(0, x+y)$, $(0, x-y)$, $(0, xy)$ y $(0, \frac{x}{y})$ para $y \neq 0$. Las construcciones de $(0, x+y)$ y $(0, x-y)$ son obvias; pues si se se traza un arco de radio y y centro en $(0,x)$ estos cortan a el eje Y en los puntos $(0, x+y)$ y $(0, x-y)$. Para las otras construcciones procedemos de la siguiente manera:

Unamos (1,0) con $(0,y)$ y dibujemos la linea paralela a esta recta que pase por $(0, x)$. Esta linea corta a el eje X en el punto $(u, 0)$. Por semejanza de triángulos tenemos que

$$\frac{u}{x} = \frac{1}{y}$$

por lo que

$$u = \frac{x}{y}$$

tomando $x = 1$ (pues el punto(1,0) es claramente construible) entonces construimos el punto $(\frac{1}{y}, 0)$, por lo tanto el punto $(0, \frac{1}{y})$. Cambiando $\frac{1}{y}$ en lugar de y tenemos que $(xy, 0)$ es construible. Con este punto podemos ahora construir los puntos $(0, xy)$ y $(0, \frac{x}{y})$ (ver figura 10)

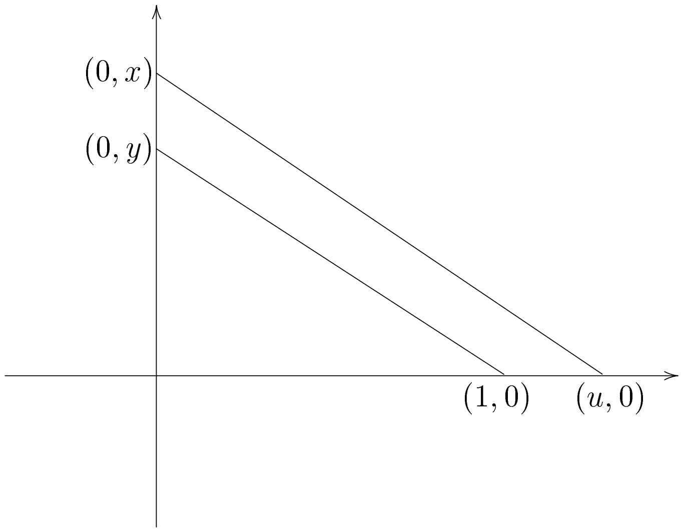

Figura 10.

□

Lema 17.1.2. *Supongamos que $(K(\alpha) : K)$ es una extensión de grado 2, tal que $K(\alpha) \subseteq \mathbb{R}$. Entonces un punto (z, t) de $\mathbb{R}^2$ cuyas coordenadas $z, t \in \mathbb{R}$ puede ser construido de algún conjunto finito de puntos cuyas coordenadas estén en K.*

Prueba. Si tenemos que $\alpha^2 + p\alpha + q = 0$ donde $p, q \in K$. Entonces se sigue que

$$\alpha = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

y dado que $K(\alpha) \subseteq \mathbb{R}$ entonces $p^2 - 4q$ tiene que ser positivo.

Usando el lema 17.1.1, el resultado se seguirá si podemos construir el punto $(0, \sqrt{k})$ para $0 < k \in K$ a partir de un número finito de puntos (x_r, y_r) donde x_r, y_r están en K.

A partir de $(-1, 0)$ y $(k, 0)$. Dibujamos el semicirculo con estos puntos como extremos opuestos de el diámetro (de dicho semicirculo). Dicha semicircunferencia intersecta al eje Y en el punto $(0, v)$. Por el teorema anterior tenemos que $v^2 = 1k$, por lo que $v = \sqrt{k}$ (ver figura 11).

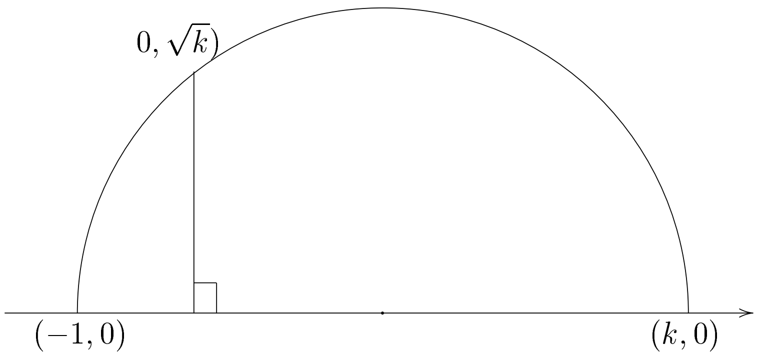

Figura 11.

□

Teorema 17.1.3. *Supongamos que K es un subcampo de $\mathbb{R}$ generado por las coordenadas de los puntos de algún subconjunto $P \subseteq \mathbb{R}^2$. Sean α, β en alguna extensión L de K contenida en $\mathbb{R}$, tal que exista una serie finita de subcampos*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L$$

con

$$[K_{i+1} : K_i] = 2$$

para $i = 0, \ldots, r-1$. Entonces (α, β) es construible a partir de P.

Prueba. La demostración la haremos por inducción sobre r. El caso $r = 0$ esta probado en el lema 17.1.1, supongamos ahora que el punto (α, β) es construible de un número finito de puntos cuyas coordenadas están en K_{r-1} (es posible por el lema 17.1.2). Por la hipótesis de inducción estos puntos son construibles a partir de P. Así pues (α, β) es construible a partir de P. □

De la prueba de el teorema 5.1.3, se sigue que la existencia de tales campos K_i es también una condición de necesidad para que el punto (α, β) sea construible a partir de P. Existe una versión muy usada de el teorema anterior, aunque en cierto sentido un poco más débil.

Proposición 17.1.4. *Sea K un subcampo de $\mathbb{R}$ generado por las coordenadas de los puntos de algún subconjunto $P \subseteq \mathbb{R}^2$, si α, β están en una extensión normal L de K, tal que $L \subseteq \mathbb{R}$ y $[L : K] = 2^r$ para algún entero r. Entonces (α, β) es construible a partir de p.*

Prueba. Como $(L : K)$ es separable (dado que la característica de K es cero). Sea G el grupo de Galois de $(L : K)$. Por el teorema 11.0.2 parte (1) tenemos que $|G| = 2^r$, por lo que G tiene un 2-grupo. Por el lema 13.3.8, G tiene una serie de subgrupos normales

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G$$

tal que $|G_i| = 2^i$. Sea K_i el campo fijo de $G^{\dagger}_{i-1}$. Entonces por el teorema 11.0.2 parte (3) tenemos que $[K_{j+1} : K_j] = 2$ para toda j, por el teorema 17.1.3, tenemos que (α, β) es construible a partir de P. □

17.2 Polígonos regulares.

En esta sección usaremos conceptos de álgebra y geometría para determinar los valores n para los cuales los $n-$agonos regulares son construibles.

Definición 17.2.1. A un entero positivo n le llamaremos *construible* si el $n-$agono regular es construible con regla y compás.

El primer paso es reducir el problema para la descomposición de n como producto de potencias de números primos.

Lema 17.2.2. *Si n es construible y m divide a n entonces m es construible. Si n, m son coprimos y construibles entonces mn es construible.*

Prueba. Si m divide a n entonces podemos construir un m-agono uniendo los d-ésimos vértices de un n-agono regular, donde $d = \frac{n}{m}$.

Ahora si n, m son primos relativos, entonces existen números enteros a y b tal que

$$am + bn = 1$$

así pues

$$\frac{1}{mn} = a\frac{1}{n} + b\frac{1}{m}$$

y como los ángulos $\frac{2\pi}{m}$ y $\frac{2\pi}{n}$ pueden ser construidos tenemos que $\frac{2\pi}{mn}$ también puede ser construible y de esta manera podemos construir un mn-agono. □

Corolario 17.2.3. Supongamos que $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ donde $p_1, \ldots p_r$ son números primos distintos. Entonces n es construible si, y sólo si $p_i^{\alpha_i}$ es construible.

Un resultado obvio resulta ser

Lema 17.2.4. *Para un entero positivo α el número 2^α es construible.*

Prueba. Como cualquier ángulo puede ser bisecado usando solamente regla y compás, el resultado se sigue usando inducción. □

Este resultado nos permite reducir el problema a solamente considerar potencias de números primos impares. Para ello usaremos un poco de álgebra en el plano complejo. En el plano complejo el conjunto de las n-raíces de la unidad forman un n-agono regular (dichas raíces son precisamente los vértices). Más aún estas raíces de la unidad son los ceros en $\mathbb{C}$ de el polinomio

$$t^n - 1 = (t-1)(t^{n-1} + t^{n-2} + \ldots + t + 1)$$

Nos concentraremos ahora en el segundo factor de el lado derecho de la expresión anterior.

Lema 17.2.5. *Sea p un número primo, tal que p^n es construible. Sea ς una raíz p-ésima de la unidad en $\mathbb{C}$. Entonces el grado de el polinomio mínimo de ς sobre $\mathbb{Q}$ es una potencia de 2.*

Prueba. Primero consideremos $\varsigma = e^{\frac{2\pi i}{p^n}}$. Dado que p^n es construible entonces podemos construir el punto (α, β) donde $\alpha = cos(\frac{2\pi}{p^n})$ y $\beta = sen(\frac{2\pi}{p^n})$, para hacer esto solamente basta con proyectar un vértice de el p^n-agono regular en los ejes coordenados.

Por lo tanto por el teorema 5.1.3, tenemos que

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^r$$

Para algún entero r, así que

$$[\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] = 2^{r+1}.$$

Pero $\mathbb{Q}(\alpha, \beta, i)$ contiene a $\alpha + i\beta = \varsigma$, por lo que

$$[\mathbb{Q}(\varsigma) : \mathbb{Q}]$$

es una potencia de 2, dado que $\mathbb{Q}(\varsigma) \subseteq \mathbb{Q}(\alpha, \beta, i)$ se tiene que el grado de el polinomio de ς sobre $\mathbb{Q}$ es una potencia de 2. $\square$

El siguiente paso a realizar es el calcular el polinomio mínimo respecto a encontrar sus grados. Sera suficiente considerar solamente p y p^2.

Lema 17.2.6. *Si p es un número primo y ς es una raíz p-ésima primitiva de la unidad en $\mathbb{C}$. Entonces el polinomio mínimo de ς sobre $\mathbb{Q}$ es*

$$f(t) = 1 + t + \ldots + t^{p-1}.$$

Prueba. Notemos que

$$f(t) = \frac{(t^p - 1)}{(t - 1)}$$

primero veamos que $f(\varsigma) = 0$, pero dado que$\varsigma^p - 1 = 0$ y $\varsigma \neq 1$, se sigue que $f(\varsigma) = 0$. Ahora mostraremos que $f(t)$ es irreducible, para ello hagamos $t = 1 + u$ donde u es una indeterminada. Entonces $f(t)$ es irreducible si, y sólo si $f(1+u)$ es irreducible, pero

$$f(1+t) = \frac{(1+u)^{p-1} - 1}{p} = u^{p-1} + ph(u)$$

donde h es un polinomio en la variable u sobre $\mathbb{Z}$ con termino constante 1, (esto se debe a las observaciones constantemente hechas acerca de los coeficientes binomiales). Por el criterio de Einseinstein se tiene que $f(1+u)$ es irreducible en $\mathbb{Q}$. $\square$

Lema 17.2.7. *Sea p un número primo y ς una raíz p^2-ésima primitiva de la unidad en $\mathbb{C}$. Entonces el polinomio mínimo de ς sobre $\mathbb{Q}$ es*

$$g(t) = 1 + t^p + \ldots + t^{p(p-1)}.$$

Prueba. Nuevamente notamos que

$$g(t) = \frac{t^{p^2} - 1}{t^p - 1}$$

y sabemos que $\varsigma^{p^2} - 1 = 0$ con $\varsigma^p - 1 \neq 0$, por lo que $g(\varsigma) = 0$. Por lo que solamente resta probar que $g(t)$ es irreducible $\mathbb{Q}$. Como en la prueba de el lema anterior hacemos $t = 1 + u$ y entonces tenemos que

$$g(1+u) = \frac{(1+u)^{p^2} - 1}{(1+u)^p - 1}$$

y módulo p lo anterior es igual a

$$\frac{(1+u^{p^2}) - 1}{(1+u)^p - 1} = u^{p(p=1)} + pk(u)$$

así que

$$g(1+u) = u^{p(p-1)} + pk(u)$$

donde k es un polinomio en la variable u sobre $\mathbb{Z}$. De la expresión alternativa tenemos que

$$g(1+u) = 1 + (1+u)^p + \ldots + (1+u)^{p(p-1)}$$

k tiene termino constante 1. Nuevamente por el criterio de Enseintein tenemos que $g(1+u)$ es irreducible sobre $\mathbb{Q}$. $\square$

Estamos en este momento preparados para dar el resultado principal de esta sección.

Teorema 17.2.8 (Gauss). *El n-agono regular es construible con regla y compás si, y sólo si $n = 2^r p_1 \cdots p_s$ donde r, s son enteros positivos y $p_1, \ldots, p_s$ son primos impares de la forma*

$$p_i = 2^{2^{r_i}} + 1$$

para enteros positivos r_i.

Prueba. Si n es construible entonces

$$n = 2^r p_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

donde p_i son primos impares distintos para toda i. Por el corolario 17.2.3, cada uno de los $p_i^{\alpha_i}$ es construible. Si $\alpha_i \geq 2$ entonces p_i^2 es construible (por la proposición 17.1.4). Por lo tanto el grado del polinomio mínimo de una p_i^2-raíz de la unidad sobre $\mathbb{Q}$ es una potencia de 2 (por el lema 17.2.5). Por el lema 17.2.7, $p_i(p_i - 1)$ es una potencia de 2 la cual no puede ser tomada ya que p_i es impar. Así pues $\alpha_i = 1$ para toda i. Por lo que p_i es construible. Por el lema 17.2.6, $p_i - 1 = 2^{s_i}$ para algún s_i. Supongamos ahora que s_i tiene un divisor impar $a > 1$, por lo que $s_i = ab$. Entonces

$$p_i = (2^b)^a + 1$$

el cual es divisible por $2^b + 1$ dado que

$$t^a + 1 = (t+1)(t^{a-1} - t^{a-2} - \ldots - 1)$$

cuando a es impar. Por lo que p_i no puede ser primo. Por lo tanto s_i no tiene factores impares, así que

$$s_i = 2^r$$

para algún $r > 0$. Lo anterior establece la necesidad para la n-ada.

Ahora probaremos la suficiencia. Por el corolario 17.2.3, solamente necesitamos considerar las potencias de los factores primos de n. Por el lema 17.2.4, 2^r es construible, mostraremos ahora que cada p_i es construible. Sea ς una raíz p_i-ésima primitiva de la unidad en $\mathbb{C}$, entonces tenemos que

$$[\mathbb{Q}(\varsigma) : \mathbb{Q}] = p_i - 1 = 2^a$$

para alguna a (esto es por el lema 17.2.6). Ahora $\mathbb{Q}(\varsigma)$ es un campo de descomposición para el polinomio

$$f(t) = 1 + t + \ldots + t^{p-1}$$

sobre $\mathbb{Q}$ por lo cual la extensión

$$(\mathbb{Q}(\varsigma) : \mathbb{Q})$$

es una extensión normal y además es separable puesto que $\mathbb{Q}$ es de característica cero. Por el lema 14.1.6, el grupo de Galois $\Gamma(\mathbb{Q}(\varsigma) : \mathbb{Q})$ es abeliano. sea $K = \mathbb{R} \cap \mathbb{Q}(\varsigma)$, entonces $cos(\frac{2\pi}{p_i}) = \frac{(\varsigma + \varsigma^{-1})}{2} \in K$. Como $(\mathbb{Q}(\varsigma) : K)$ es de grado 2 y por el teorema 11.0.2

$$\Gamma(\mathbb{Q}(\varsigma) : K)$$

es un subgrupo de

$$G = \Gamma(\mathbb{Q}(\varsigma) : \mathbb{Q})$$

de orden 2 y más aún es un subgrupo normal ya que G es abeliano. De este modo tenemos que $(K : \mathbb{Q})$ es una extensión normal de grado 2^{a-1}. Por la proposición 17.1.4, el punto $(0, cos(\frac{2\pi}{p_i}))$ es construible. Por lo tanto p_i es construible, lo cual finaliza la prueba. $\square$

17.3 Números de Fermat.

Analizaremos ahora nuestro problema desde el punto de vista de la teoría de números, para ello necesitaremos una definición previa.

Definición 17.3.1. El n-ésimo *número de Fermat* es $F_n = 2^{2^n} + 1$

Así pues la pregunta ahora es ¿cuándo F_n es primo?.

En 1640 *Pierre Fermat* noto que $F_0 = 3$, $F_1 = 2$, $F_2 = 17$ $F_3 = 257$, $F_4 = 65537$ todos estos números son primos y se conjeturo que F_n es un número primo para todo $n \in \mathbb{N}$. Es decir se conjeturo que teníamos una función generadora de números primos. Desafortunadamente (ó afortunadamente) en 1732 *Euler* probo que la conjetura no es cierta, es decir encontró un número natural n para el cual F_n no es número primo. A continuación daremos una tabla en la cual se vera para algunos valores n cuando F_n es un número primo.

n	k		m	fecha	descubridor
0		primo		1640	Fermat
1		primo		1640	Fermat
2		primo		1640	Fermat
3		primo		1640	Fermat
4		primo		1640	Fermat
5	5		7	1732	Euler
6		compuesto		1878	Lucas
7		compuesto		1905	Morehead, Western
8		compuesto		1909	Morehead, Western
9	37		16	1903	Western
10	11131		12	1953	Selfridge
11	39		13	1899	Cunningham
12	7		14	1877	Lucas, Pervusin
13		compuesto		1961	Paxons (IBM 7090)
14		compuesto		1963	Paxons,Hurwitz (IBM 7090)
15	579		21	1925	Kraitcik
16	1575		19	1953	Selfridge (SWAC)
18	13		20	1903	Western
23	5		25	1878	Pervusin
36	5		39	1886	Seelhoff
38	3		41	1903	Cullen,Cunningham,Western
39	21		41	1956	Robinson (SWAC)
55	29		57	1956	Robinson (SWAC)
58	95		61	1957	Robinson (SWAC)
63	9		67	1956	Robinson (SWAC)
73	5		75	1906	Morehead
n	k		m	fecha	descubridor
77	425		79	1957	Robinson,Selfridge (SWAC)
81	271		84	1957	Robinson,Selfridge (SWAC)
117	7		120	1956	Robinson (SWAC)
125	5		127	1956	Robinson (SWAC)
144	17		147	1956	Robinson (SWAC)
150	1575		157	1956	Robinson (SWAC)
207	3		209	1956	Robinson (SWAC)
226	15		229	1956	Robinson (SWAC)
228	29		231	1956	Robinson (SWAC)
250	403		252	1957	Robinson,Selfridge (SWAC)
267	177		271	1957	Robinson,Selfridge (SWAC)
268	21		276	1956	Robinson (SWAC)

Donde en la primera columna va el valor n de F_n, en la segunda columna va el número de números compuestos que tiene F_n, en la cuarta columna va el numero m de factores de la forma $k2^m + 1$ de F_n, en la quinta columna va la fecha en que fueron descubiertos por primera vez tales datos y finalmente en la ultima columna va el nombre de el descubridor.

Una inspección a la tabla anterior revela que los únicos números primos (que hay en la tabla) son los que el propio Fermat había propuesto, hasta la fecha no se ha encontrado otro número n para el cual F_n sea primo.

Un vistazo más a la tabla anterior revela la siguiente:

Proposición 17.3.2. *Los únicos primos $p < 10^{40000}$ para los cuales el p-agono regular es construible son 2, 3, 5, 17, 257, 56537.*

17.4 Construcciones.

Muchas construcciones para el 17-agono han sido encontradas, la primera de estas que se publico fue dada por *Huguenin* (Ver *Klein* [41]) en 1803. En algunas de las construcciones dadas, solamente esta usada la geometría euclidiana sin coordenadas rectangulares.

Una serie de notas publicada por *Richelut* [46] en 1832, da una construcción para el 257-agono.

En [28] *Bell* estableció un proyecto reuniendo estudiantes para dar la construcción de el 65537-agono, el cual concluyeron 20 años después a su inicio Falta choro....

Un camino para construir el 17-agono es el siguiente (que emplea la teoría desarrollada con anterioridad) este proceso fue tomado de *Hardy and Wright* [13]

Nuestro primer objetivo será el de encontrar expresiones radicales para los ceros de el polinomio

$$\frac{t^{17}-1}{t-1} = t^{16} + t^{15} + \ldots + 1 \tag{17.1}$$

Sobre $\mathbb{C}$, consideremos

$$\theta = \frac{2\pi}{17}$$

y

$$\epsilon = e^{ki\theta} = cos(k\theta) + isen(k\theta)$$

notemos que los ceros en la ecuación 17.1, en $\mathbb{C}$ son los elementos $\epsilon_1, \ldots \epsilon_{16}$. Las potencias de 3 reducidas módulo 17 son las siguientes

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^m	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Definimos

$$x_1 = \epsilon_1 + \epsilon_9 + \epsilon_{13} + \epsilon_{15} + \epsilon_{16} + \epsilon_9 + \epsilon_2$$

$$x_2 = \epsilon_3 + \epsilon_{10} + \epsilon_5 + \epsilon_{11} + \epsilon_{14} + \epsilon_7 + \epsilon_{12} + \epsilon_6$$

$$y_1 = \epsilon_1 + \epsilon_{13} + \epsilon_{16} + \epsilon_4$$

$$y_2 = \epsilon_4 + \epsilon_{15} + \epsilon_8 + \epsilon_2$$

$$y_3 = \epsilon_3 + \epsilon_5 + \epsilon_{14} + \epsilon_{12}$$

$$y_4 = \epsilon_{10} + \epsilon_{11} + \epsilon_7 + \epsilon_6$$

y observamos que se tiene

$$\epsilon_k + \epsilon_{17-k} = 2cos(k\theta) \tag{17.2}$$

para $k = 1, \ldots, 16$, por lo que

$$x_1 = 2(cos(\theta) + cos(8\theta) + cos(4\theta) + cos(2\theta))$$

$$x_2 = 2(cos(3\theta) + cos(7\theta) + cos(5\theta) + cos(6\theta))$$

$$y_1 = 2(cos(\theta) + cos(4\theta))$$

$$y_2 = 2(cos(8\theta) + cos(2\theta))$$

$$y_3 = 2(cos(3\theta) + cos(5\theta))$$

$$y_4 = 2(cos(7\theta) + cos(6\theta)) \tag{17.3}$$

de la ecuación 17.1, se sigue que

$$x_1 + x_2 = -1$$

Usando ahora la ecuación

$$2cos(m\theta) = cos[(m+n)\theta] + cos[(m-n)\theta]$$

tenemos que

$$\begin{aligned} x_1 x_2 =& 2[cos4\theta + cos3\theta + cos8\theta + cos6\theta + cos4\theta + cos6\theta + cos5\theta + cos7\theta \\ &+ cos11\theta + cos5\theta + cos15\theta + cos\theta + cos13\theta + cos14\theta + cos2\theta + cos7\theta \\ &+ cos\theta + cos3\theta + cos11\theta + cos\theta + cos9\theta + cos2\theta + cos10\theta + cos5\theta \\ &+ cos\theta + cos9\theta + cos5\theta + cos7\theta + cos3\theta + cos9\theta + cos8\theta] = -4 \end{aligned}$$

usando la ecuación 17.2. Por lo tanto x_1 y x_2 son ceros de el polinomio cuadratico

$$t^2 + t - 4 \tag{17.4}$$

Más aún como $x_1 > 0$ se tiene que $x_1 > x_2$. Por una expresión trigonométrica similar a la anterior tenemos que

$$y_1 + y_2 = x_1$$

y

$$y_1 y_2 = -1$$

Así que y_1, y_2 son los ceros de el polinomio

$$t^2 - x_1 t - t \tag{17.5}$$

De manera similar como $y_1 > y_2$ tenemos que y_3 y y_4 son ceros de el polinomio

$$t^2 - x_2 t - 1 \tag{17.6}$$

Además $y_3 > y_4$. Ahora bien como

$$2cos\theta + 2cos(4\theta) = y_1$$

y

$$4cos\theta cos(4\theta) = 2(cos(5\theta) + cos(3\theta))$$

se tiene que

$$z_1 = 2cos\theta$$

y

$$z_2 = 2cos(4\theta)$$

son los ceros de el polinomio

$$t^2 - y_1 t + y_3 \tag{17.7}$$

y $z_1 > z_2$.

Resolviendo ahora las series cuadráticas (es decir las ecuaciones 17.4, 17.5, 17.6, 17.7) y usando las igualdades para ver que cero se obtiene en la ecuación correspondiente, obtenemos la ecuación

$$\begin{aligned} cos\theta =& \frac{1}{16}[-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} \\ &+ \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2(1 - \sqrt{17})(\sqrt{34 - 2\sqrt{17}})}] \end{aligned}$$

donde todas las raíces cuadradas en la expresión, son tomadas positivas.

De todo lo anterior podemos deducir la construcción geométrica para el 17-agono, construyendo las raíces cuadradas anteriores.

Teniendo un poco de ingenuidad podemos obtener construcciones más satisfactorias (aunque en cierto sentido un tanto más antiestéticas). El siguiente método se debe a $Richmond$[17].

Sea ϕ el ángulo positivo más pequeño (acute) tal que $tan(4\phi) = 4$. Entonces $\phi, 2\phi$ y 4ϕ son todos (acute). La ecuación 17.4, puede ahora escribirse como

$$t^2 + 4tcot(4\theta) - 4$$

cuyos ceros son

$$2tan(2\theta)$$

y

$$-2cot(2\theta)$$

Por lo que si $x_1 = 2tan(2\theta)$ y $x_2 = -2cot(2\theta)$ entonces formamos las siguientes expresiones

$$y_1 = tan\left(\theta + \frac{\pi}{4}\right)$$

$$y_2 = tan\left(\theta - \frac{\pi}{4}\right)$$

$$y_3 = tan\theta$$

$$y_4 = -cot\theta$$

Entonces $2(cos(3\theta) + cos(5\theta)) = tan\theta$, así que

$$4cos(3\theta)cos(5\theta) = tan\left(\theta - \frac{\pi}{4}\right) \tag{17.8}$$

Ahora como en la figura 12. Sean OA, OB los 2 radios perpendiculares de un circulo: Hacemos $OI = \frac{1}{4}OB$ y el ángulo OIE igual aun cuarto de el ángulo

OIA. Encontrando F en AO producido al hacer el ángulo EIF igual a $\frac{\pi}{4}$.

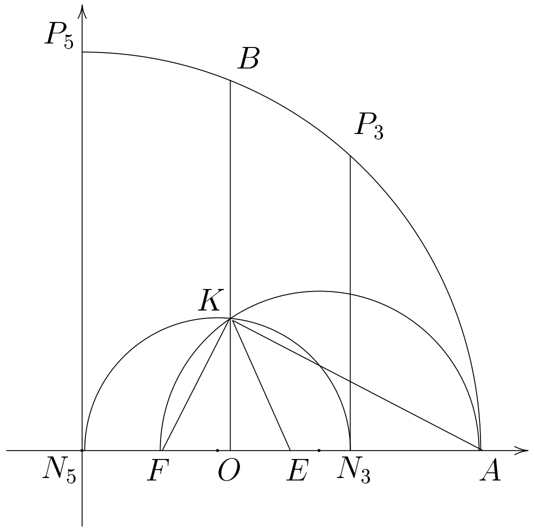

Figura 12.

Consideremos el circulo con diámetro AF que corte OB en K, y tracemos el circulo con centro en E que pase por K y que corte a OA en N_3 y N_5, como se muestra en la figura 12. Ahora dibujemos N_3P_3 y N_5P_5 perpendiculares a OA.

Entonces el ángulo entre OIA es igual a 4ϕ y el ángulo entre OIE es igual a ϕ. También

$$2\left(cos(\measuredangle AOP_3) + cos(\measuredangle AOP_5)\right) = 2\frac{ON_3 - ON_5}{OA \cdot OA} = 4\frac{OE}{OA} = \frac{OE}{OI} = tan\theta$$

y

$$\begin{aligned} 4cos(\measuredangle AOP_3)cos(\measuredangle AOP_3) &= -\,4\frac{ON_3 \cdot ON_5}{OA \cdot OA} = -4\frac{(OK)^2}{(OA)^2} \\ &= -4\frac{OF}{OA} = -\frac{OF}{OI} = tan(\theta - \frac{\pi}{4}) \end{aligned}$$

comparando estos resultados con la ecuación 17.8, se tiene que

$$\measuredangle AOP_3 = 3\theta$$

y

$$\measuredangle AOP_5 = 5\theta$$

Por lo que A, P_3, P_5 son el primer, tercer y quinto vertice de el 17-agono regular inscrito en el circulo dado. Los demás vértices son fáciles de calcular a partir de estos.

17.5 Ejercicios.

17.1 Verifique las siguientes construcciones (aproximadas) para los siguientes n-agonos regulares. (estas construcciones fueron dadas por *Oldrogd*[23]).

a) 7-agono. Construir de $cos^{-1}(\frac{4+\sqrt{5}}{10})$ dado un ángulo aproximado de $\frac{2\pi}{7}$.

b) 9-agono. Construir el ángulo $cos^{-1}(\frac{5\sqrt{3}-1}{10})$.

c) 11-agono. Construir los ángulos $cos^{-1}(\frac{9}{9})$, $cos^{-1}(\frac{1}{2})$ y tomar su diferencia.

d) 13-agono. Construir los ángulos $tan^{-1}(1)$, $tan^{-1}(\frac{4+\sqrt{5}}{20})$ y luego tomar su diferencia.

17.2 Muestra que para n impar, las únicas 'buenas' construcciones de n-agonos regulares son para los cuales n es un divisor de $2^{32} - 1 = 4294967295$.

17.3 Trata de dar una aproximación de el tamaño de F_{1945}. Explica por que no es fácil encontrar factores de los números de Fermat.

17.4 Usa la ecuación $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ para mostrar que 641 divide a F_5.

17.5 Muestra que

$$F_{n+1} = 2 + F_n \cdot F_{n-1} \cdots F_0$$

y deduce que si $m \neq n$ entonces F_m y F_n son coprimos. Por lo tanto hay una infinidad de números primos.

17.6 Enliste los valores $n \leq 100$ para los cuales el n-agono regular, puede ser construido usando regla y compás.

17.7 Verifique la siguiente construcción para el pentágono regular.

Dibuja el circulo centrado en O con dos radios perpendiculares OP_0, OB. Sea D el punto medio de OB y une P_0D. Luego biseca el ángulo ODP_0 cortando OP_0 en N. Dibuja NP_1 perpendicular a OP_0 que corte a el circulo en P_1. Entonces P_0 y P_1 son los dos primeros vértices de el pentágono regular inscrito en el circulo.

17.8 Diga si las siguientes afirmaciones son verdaderas o falsas.

a) $2^n + 1$ no es primo salvo que n sea una potencia de 2.

b) Si n es una potencia de 2 entonces $2^n + 1$ es primo.

c) El 771-agono regular es construible usando regla y compás.

d) El 768-agono regular es construible usando regla y compás.

e) El 25-agono regular es construible usando regla y compás.

f) Para un primo impar p el p^2-agono nunca puede ser construido usando regla y compás.

g) Si n es un número entero positivo, entonces la linea de longitud $\sqrt{n}$ siempre puede ser construida usando regla y compás.

h) Un punto cuyas coordenadas pertenecen a una extensión normal de $\mathbb{Q}$ de grado alguna potencia de 2 es construible usando regla y compás.

i) El 51-agono regular es construible usando regla y compás.

j) Si p es un número primo entonces $t^{p^2} - 1$ es irreducible sobre $\mathbb{Q}$.

Capítulo 18

El 'Teorema Fundamental' de el Álgebra.

Iniciaremos este capítulo dando una definición en este primer parrafo. Decimos que un campo es *algebraicamente cerrado* si cada polinomio sobre el se divide. El resultado referido en el titulo de este capítulo establece que el campo de los números complejos es algebraicamente cerrado.

La primera prueba dada de este resultado fue hecha por *Gauss* en su disertación doctoral en 1799 cuyo titulo es ´Una nueva prueba de que cada función racional integral de una variable puede ser resuelta en factores reales de primer y segundo grado´. Gauss comenzó el titulo de su disertación doctoral con la palabra ´nueva´, aunque el fue el primero que dio una prueba genuina. La prueba que dio Gauss puede ser consultada en [12] pag.492.

Existen otras pruebas de el teorema antes mencionado, una de ellas usa parte de la teoría de funciones de variable compleja (ver *Remert*) y esta es una de las pruebas más comunes. Existe también una prueba dada por *Clifford* [34] pag.20, la cual es casi puramente algebraica; la idea principal de esta prueba, es mostrar que un polinomio irreducible sobre $\mathbb{R}$ es de grado uno ó dos. La prueba que nosotros vamos a dar es esencialmente la dada por *Legendre*. Aunque su idea en general no utiliza teoría de Galois.

Es poco razonable poder dar una prueba algebraica de dicho teorema, dado que el campo de los números reales (y por lo tanto el de los números complejos) están definidos en términos de conceptos analíticos, tales como las sucesiones de *Cauchy*, cortaduras de *Dedekind*, ó la completes de acuerdo a un orden dado.

Definición 18.0.1. Un *campo ordenado* es un campo K con una relación $\leq$ tal que:

(1) $k \leq k$ para todo elemento $k \in K$.

(2) Si $k \leq l$ y $l \leq m$ entonces $k \leq m$ para $k, l, m \in K$.

(3) Si $k \leq l$ y $l \leq k$ entonces $k = l$ para $k, l \in K$.

(4) Si $k, l \in K$ entonces $k \leq l$ ó $l \leq k$.

(5) Si $k, l, m \in K$ y $k \leq l$ entonces $k + m \leq l + m$.

(6) Si $k, l, m \in K$, $k \leq l$ y $0 \leq m$ entonces $km \leq lm$.

La relación $\leq$ se dice que es un *orden* para K. Las relaciones $<, \geq, >$ están definidas de manera obvia. De manera obvia resultan también los conceptos, tales como *positivo* ó *negativo*.

Ejemplos de campos ordenados, son $\mathbb{Q}, \mathbb{R}$. En seguida probaremos un par de consecuencias que se desprende de la definición de campo ordenado.

Lema 18.0.2. *Sea K un campo ordenado. Para un elemento $k \in K$ se tiene que $k^2 \geq 0$. La característica de K además tiene que ser cero.*

Prueba. Si $k \geq 0$ entonces $k^2 \geq 0$ (por la propiedad (6)). Por lo que por la propiedad (3) podemos asumir que $k < 0$. Si sucediera en este caso también que $-k < 0$ se seguiría que

$$0 = k + (-k) < k + 0 = k$$

lo cual no puede suceder, por lo que $-k \geq 0$. Así que $k^2 = (-k)^2 \geq 0$. Esto concluye la primer parte de la prueba.

Ahora bien como $1 = 1^2 > 0$ entonces para cualquier número finito n tenemos que

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n-veces} > 0$$

por lo que $n \neq 0$ ya así K tiene característica cero. $\square$

Enunciaremos a continuación algunas propiedades de $\mathbb{R}$

Lema 18.0.3. *$\mathbb{R}$ con su orden usual, es un campo ordenado. Cada elemento positivo de $\mathbb{R}$ tiene una raíz cuadrada en $\mathbb{R}$. Todo polinomio de grado impar sobre $\mathbb{R}$ tiene un cero en $\mathbb{R}$.*

Todas las propiedades anteriores son probadas en un curso de Cálculo de nivel superior y sus pruebas dependen únicamente de que un polinomio pensado como función polinomial, es una función continua de variable real.

El siguiente paso a seguir es el de desarrollar un poco de herramienta respecto a la teoría de Galois, para después aplicar esta a nuestro objetivo.

Lema 18.0.4. *Sea K un campo de característica cero, tal que para algún número primo p toda extensión finita M de K con $M \neq K$ tiene $[M : K]$ divisible por p. Entonces cada extensión finita de K tiene grado alguna potencia de p.*

Prueba. Sea N una extensión finita de K. Como la característica de K es cero entonces $(N : K)$ es una extensión separable. Módulo una cerradura normal, podemos asumir que $(N : K)$ es normal, por lo que la correspondencia de Galois es una biyección. Sea G el grupo de Galois de $(N : K)$ y sea P un p-subgrupo de Sylow de G. El campo fijo $P^\dagger$ tiene grado $[P^\dagger : K]$ igual a el índice de P en G (por el teorema 11.0.2 parte 1), pero este grado debe ser primo relativo a $|P|$. Por la hipótesis tenemos que $p^\dagger = K$, por lo que $P = G$. Entonces $[N : K] = |G| = p^n$ para alguna n. $\square$

Teorema 18.0.5. *Sea K un campo ordenado en el que cada elemento positivo tiene raíz cuadrada y cada polinomio de grado impar tiene un cero. Entonces $K(i)$ es algebraicamente cerrado, donde $i^2 = -1$.*

Prueba. Una primera observación es que K no puede tener extensiones de grado impar finitas mayores que 1. Pues si $[M : K] = r > 1$ donde r es impar, entonces consideramos a $\alpha \in M - \{K\}$ y digamos que m es su polinomio mínimo, entonces el grado de m divide a r por lo que el grado de m es impar. Por la hipótesis m tiene un cero en K, por lo que m es reducible sobre K, lo cual no puede ser cierto. Por lo tanto toda extensión finita de K tiene grado par sobre K. Como la característica de K es cero por el lema 18.0.2 y por 18.0.4 toda extensión finita de K tiene grado alguna potencia de 2.

Consideremos ahora $M = K(i)$ una extensión finita de K, donde $i^2 = -1$. Tenemos que módulo una cerradura normal podemos asumir que $(M : K)$ es normal, por lo que el grupo de Galois de $(M : K)$ es un 2-grupo. Usando el lema 13.3.8 y la correspondencia de Galois, podemos encontrar una extensión N de $K(i)$ de grado $[N : K(i)] = 2$. Por la fórmula general para resolver ecuaciones cuadráticas tenemos

$$N = K(i)(\alpha)$$

donde $\alpha^2 \in K(i)$. Pero si $a, b \in K$ se tiene que

$$\sqrt{a+ib} = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$$

donde la raíz cuadrada de de $a^2 + b^2$ es tomada positiva y los signos de las otras dos raíces son elegidos de tal manera que su producto sea igual a 1. Las raíces cuadradas de el lado derecho están siempre en K, dado que los elementos sobre los que se esta tomando la raíz siempre son positivos.

De este modo tenemos que $\alpha \in K$, por lo que $K(i) = N$, lo cual contradice la definición de N. Por lo tanto $M = K(i)$ y por lo tanto $K(i)$ no tiene extensiones finitas de grado mayor que 1. Por lo tanto un polinomio irreducible en $K(i)$ tiene grado 1. Pues si no fuera el caso, un campo de descomposición tendría grado finita mayor que 1 sobre $K(i)$. Por lo tanto $K(i)$ es algebraicamente cerrado. $\square$

Corolario 18.0.6 (Teorema Fundamental de el Álgebra). El campo de los números complejos $\mathbb{C}$ es algebraicamente cerrado.

18.1 Ejercicios.

18.1 Muestra que un campo K es algebraicamente cerrado si, y sólo si $(L : K)$ algebraica implica que $L = K$.

18.2 Muestra que cada extensión algebraica de $\mathbb{R}$ es isomorfa a $(\mathbb{R} : \mathbb{R})$ ó $(\mathbb{C} : \mathbb{R})$.

18.3 Pruebe por inducción transfinita que cada campo K tiene una extensión L donde L ya es algebraicamente cerrado.

18.4 Muestre que $\mathbb{C}$ con las operaciones comunes de campo no tiene estructura de campo ordenado. Si damos operaciones de campo diferentes. ¿Puede el conjunto $\mathbb{C}$ ser un campo ordenado?.

18.5 Pruebe el teorema cuyas condiciones están dadas en el primer parrafo de este capítulo.

18.6 Supóngase que $(K : \mathbb{Q})$ es una extensión finitamente generada. Pruebe que existe un $\mathbb{Q}$-monomorfismo de $K \longrightarrow \mathbb{C}$. (Sugerencia: Use consideraciones acerca de la cardinalidad al adjuntarle elementos trascendentes y la cerradura de $\mathbb{C}$ al adjuntarle elementos algebraicos). ¿Es cierto este resultado si cambiamos a $mathbbQ$ por $\mathbb{R}$ o por $\mathbb{C}$?.

18.7 Sea K un campo ordenado. Un subconjunto S de K esta *acotado superiormente*, si existe un elemento $k \in K$ tal que para cada $s \in S$ se tiene que $s \leq k$ (en este caso se dice que k es una cota superior). Un elemento l es un *supremo* para S, si es una cota superior de S y para cualquier otra cota superior m de S se tiene que $l \leq m$. Muestre que existen K y S tal que S tiene cota superior, pero no supremo.

18.8 Un campo ordenado se llama *completo* si cada subconjunto S de K que este acotado superiormente tiene supremo. Pruebe que todo campo ordenado completo es isomorfo a el campo $\mathbb{R}$ de los números reales, dando un isomorfismo que preserve el orden. (Sugerencia: K contiene como subcampo primo a $\mathbb{Q}$ con su orden natural. Ahora bien sea T el subconjunto de K formado por todos los supremos de los subconjuntos de $\mathbb{Q}$. Muestre que T es isomorfo a $\mathbb{R}$ y que T es el mismo K).

18.9 De la definición de que $\mathbb{R}$ es un campo ordenado completo, deduce las propiedades de el lema 18.0.3.

18.10 Diga si las siguientes afirmaciones son verdaderas o falsas.

a) El campo $\mathbb{C}$ es algebraicamente cerrado.

b) El campo $\mathbb{A}$ de los números algebraicos es algebraicamente cerrado.

c) El campo $\mathbb{A}$ es un campo ordenado.

d) No existe ningún orden en $\mathbb{C}$ que lo haga ser un campo ordenado.

e) Todo polinomio sobre $\mathbb{R}$ se divide en $\mathbb{C}$.

f) Si f es un polinomio sobre $\mathbb{R}$ y K es un campo de descomposición para f, entonces $K = \mathbb{R}$ ó bien $K = \mathbb{C}$.

g) Todo campo ordenado tiene característica cero.

h) Todo campo de característica cero puede ser ordenado.

i) En un campo ordenado, cada raíz cuadrada es positiva.

j) Si todo elemento de un campo K tiene raíz cuadrada en K, entonces K no puede ser un campo algebraicamente cerrado.