I saber de mis hijos
hará mi grandeza"

UNIVERSIDAD DE SONORA

División de Ciencias Exactas y Naturales

Programa de Licenciatura en Matemáticas

"Teoría de Galois
Aplicada a construcciones geométricas"

T E S I S

Que para obtener el título de:

Licenciado en Matemáticas

Presenta:

Carol Yaneth Corral López

Director de Tesis:

Dr. Rafael Roberto Ramos Figueroa

Hermosillo, Sonora. México. 29 de Noviembre, 2011.

SINODALES

Dr. Guzmán Partida Martha
Universidad de Sonora

Dr. Ramos Figueroa Rafael Roberto
Universidad de Sonora

M.C. Robles Corbalá Carlos Alberto
Universidad de Sonora

M.C. Vargas Castro Jorge Ruperto
Universidad de Sonora

Dedicatoria

A todos los que creyeron en mí.

Agradecimientos

Gracias a mis padres, Leonel Corral y Amalia López, por

Su apoyo y amor incondicional.

A Alfredo, por acompañarme siempre.

A mis hermanos, Leo y Dory, por darme el ejemplo y

Ser mi motivación para seguir preparándome día a día.

A mis compañeros y amigos: Adriana, Mamu,
Daniela, Angélica, Arling ,Alma Delia, Lina,
Angelita, Beto, Dante y Sergio, por su paciencia.

A mis maestros de la licenciatura, con los

que les estaré eternamente agradecida, especialmente

al profesor Tellechea y su esposa Gaby.

A mi director de tesis Rafa Ramos, por

su paciencia y consejos.

A mis sinodales Carlos Robles,

Ruperto Vargas y Martha Guzmán.

Gracias por su apoyo.

A cada una de las personas con las que tuve el honor de convivir en esta hermosa etapa de mi vida, GRACIAS...!

Índice general

0.1. Introducción

En el siguiente trabajo se muestran algunos aspectos interesantes acerca de la aplicación de la teoría de extensiones de campos y de teoría de Galois a las construcciones con regla y compás. Dichas construcciones se remontan a los tiempos de Euclides y Platón, planteándose en esas épocas tres problemas geométricos que interesaron tanto a los griegos de la antigüedad que trascendieron a través de los siglos y se han conocido como los tres problemas famosos de la geometría elemental. Estos problemas son: la trisección del ángulo, la duplicación del cubo y la cuadratura del círculo. Dichos problemas no tuvieron respuesta por más de 2000 años, hasta que tuvieron una formulación algebraica.

Esta tesis tiene como propósito desarrollar la teoría de Galois para aplicarla a la geometría. El trabajo se divide en cuatro capítulos, en los cuales se demuestran cada uno de los teoremas planteados y además se proporcionan una serie de ejemplos donde se aplican de forma inmediata los conceptos teóricos expuestos. Comenzamos introduciendo en el primer capítulo los conceptos básicos de la teoría de anillos y polinomios sobre campos. Posteriormente se abordan temas de campos y sus extensiones, todos necesarios para el desarrollo de la teoría de Galois.

Al final del trabajo se concluye con una aplicación de la teoría de Galois en la posibilidad e imposibilidad de ciertas construcciones geométricas con regla y compás (tales como los tres problemas griegos).

Capítulo 1

Preliminares

1.1. Homomorfismos de anillos.

Sean R y R' anillos.

Definición 1.1.1 *Una función $\Phi : R \to R'$ es un homomorfismo de anillos si cumple:*

$$\begin{aligned} \Phi(a+b) &= \Phi(a) + \Phi(b) \\ \Phi(ab) &= \Phi(a)\Phi(b) \qquad \forall\ a, b \in R \end{aligned}$$

Teorema 1.1.2 *Si N es un ideal de un anillo R, entonces la proyección canónica γ es un homomorfismo de anillos*

$$\begin{array}{rccc} \gamma: & R & \to & R/N \\ & a & \mapsto & a+N \end{array}$$

Demostración.
$\gamma(a+b) = a+b+N = (a+N)+(b+N) = \gamma(a)+\gamma(b)$ por teoría de grupos

$\gamma(ab) = ab+N = (a+N)(b+N) = \gamma(a)\gamma(b)$ ■

Definición 1.1.3 *El Kernel de un homomorfismo de anillos $\Phi : R \to R'$ es $Ker\Phi = \{a \in R | \Phi(a) = 0'\}$ donde $0'$ es la identidad aditiva de R'.*

Teorema 1.1.4 *Sea $\Phi : R \to R'$ un homomorfismo de anillos.*

1. *Si 0 es el elemento neutro aditivo en R entonces $\Phi(0) = 0'$ es el elemento neutro de R' .*
2. *Si $a \in R$ entonces $\Phi(-a) = -(\Phi(a))$.*
3. *Si S es subanillo de R entonces $\Phi(S)$ subanillo de R'.*

4. *Si S es ideal de R entonces $\Phi(S)$ es ideal de $\Phi(R)$.*

   Por otra parte

5. *Si S' es un subanillo de R' entonces $\Phi^{-1}(S')$ es un subanillo de R.*

6. *Si S' es un ideal de $\Phi(R)$ entonces $\Phi^{-1}(S')$ es un ideal de R.*

7. *Si R tiene unitario 1 y $\Phi(1) \neq 0'$ entonces $\Phi(1) = 1'$ es unitario de $\Phi(R)$.*

Demostración. Por teoría de grupos solo necesitamos verificar las propiedades multiplicativas.
3).–
Sea S un subanillo de R y $\Phi(s_1), \Phi(s_2) \in \Phi(S)$.
Entonces $\Phi(s_1)\Phi(s_2) = \Phi(s_1 s_2) \in \Phi(S)$, por tanto, $\Phi(S)$ es cerrado bajo multiplicación y así $\Phi(S)$ es subanillo de R'.

4).–
Sea S un ideal de R y sea $\Phi(s) \in \Phi(S)$, $\Phi(r) \in \Phi(R)$.
Notemos que $s \cdot r \in S$ y $r \cdot s \in S$ pues S es ideal de R. Así

$$\Phi(s)\Phi(r) = \Phi(sr) \in \Phi(S) \quad y \quad \Phi(r)\Phi(s) = \Phi(rs) \in \Phi(S)$$

por tanto tenemos que $\Phi(S)$ es un ideal de $\Phi(R)$.

5).–
Sea S' subanillo de R' entonces por teoría de grupos $\langle \Phi^{-1}(S), + \rangle$ es un subgrupo de $\langle R, + \rangle$. Sean $x, y \in \Phi^{-1}(S') \subseteq R'$
$\Rightarrow \Phi(x), \Phi(y) \in S' \Rightarrow \Phi(xy) = \Phi(x)\Phi(y) \in S'$
$\Rightarrow xy \in \Phi^{-1}(S') \therefore \Phi^{-1}(S')$ es cerrado bajo multiplicación
Así $\Phi^{-1}(S')$ es un subanillo de R.

6).–
Sea S' un ideal de $\Phi(R)$. Sea $r \in R$ y sea $x \in \Phi^{-1}(S')$
$\Rightarrow \Phi(rx) = \Phi(r)\Phi(x) \in S'$, pues $\Phi(r) \in \Phi(R)$, $\Phi(x) \in S'$ y S' es un ideal de $\Phi(R)$.
$\Rightarrow rx \in \Phi^{-1}(S')$, por tanto, $\Phi^{-1}(S')$ es ideal en R.

7).–
Si R tiene unitario 1 entonces $\forall\, r \in R$ se tiene,
$\Phi(r) = \Phi(1r) = \Phi(1)\Phi(r)$ y

$\Phi(r) = \Phi(r1) = \Phi(r)\Phi(1)$
$\therefore 1' = \Phi(1)$ es identidad multiplicativa de $\Phi(R)$
(En particular si $1' \neq 0'$ entonces $1'$ es unitario para $\Phi(R)$). ■

Nota 1.1.5 *Enfatizamos que si $\Phi : R \to R'$ es homomorfismo de anillo y A es un ideal de R, entonces no necesariamente $\Phi(A)$ es un ideal de R', sólo un ideal de $\Phi(R)$.*

Ejemplo 1.1.6 *$2\mathbb{Z}$ es un ideal de $\mathbb{Z}$.*

Sea $\begin{array}{rccc} \Phi: & \mathbb{Z} & \to & \mathbb{Z}\times\mathbb{Z}, \\ & n & \to & (n,n) \end{array}$ *entonces Φ es homomorfismo de anillos*

$\Rightarrow \Phi(2\mathbb{Z}) = \{(2n, 2n) | n \in \mathbb{Z}\}$ *no es un ideal de $\mathbb{Z}\times\mathbb{Z}$ pues por ejemplo*

$$(1,2) \in \mathbb{Z}\times\mathbb{Z}, \qquad (4,4) \in \Phi(2\mathbb{Z})$$

y

$$(1,2)(4,4) = (4,8) \notin \Phi(2\mathbb{Z})$$

Corolario 1.1.7 *Sean R y R' anillos. $\Phi : R \to R'$ un homomorfismo de anillos. Entonces $Ker\Phi = \Phi^{-1}(\{0'\})$ es un ideal de R.*

Demostración. $\{0'\}$ es un ideal trivial de $\Phi(R)$ y aplicamos el teorema 1.1.4 punto 6. ■

Teorema 1.1.8 *Sean R y R' anillos. Sea $\Phi : R \to R'$ un homomorfismo de anillos con $Ker\Phi = K$. Entonces $\Phi(R)$ es un anillo y existe un isomorfismo canónico de $\Phi(R)$ con R/K.*

Demostración. Por el teorema 1.1.4 $\Phi(R)$ es anillo. Sea

$$\begin{array}{rccc} \lambda: & R/K & \to & \Phi(R) \\ & a+K & \to & \Phi(a) \end{array}$$

Es isomorfismo de grupos abelianos (por el teorema fundamental de isomorfismos para grupos). Así basta probar que

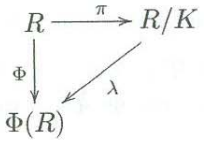
$$\lambda((a+K)(b+K)) = \lambda(a+K)\lambda(b+K).$$

Tenemos que:

$$\begin{aligned} \lambda((a+K)(b+K)) &= \lambda((a+K)(b+K)) \\ &= \lambda(ab+K) \\ &= \Phi(ab) \\ &= \Phi(a)\Phi(b) \\ &= \lambda(a+K)\lambda(b+K) \end{aligned}$$

■

Nota 1.1.9 Φ *es canónico en el sentido de que hace conmutar el diagrama.*



$\Phi(R) \subseteq R'$

1.2. Ideales maximales y primos.

Definición 1.2.1 *Un ideal maximal de un anillo R es un ideal M propio de R tal que si N es un ideal de R tal que $M \subseteq N \subsetneq R$ entonces $M = N$.*

Definición 1.2.2 *Sea R un anillo conmutativo con unitario y sea $a \in R$. El ideal $\{ra|r \in R\}$ de todos los múltiplos de a es el ideal generado por a y se denota por $\langle a \rangle$. Un ideal N de R es un ideal principal de R si $N = \langle a \rangle$ para alguna $a \in R$.*

Teorema 1.2.3 *Sea R un anillo conmutativo con unitario. Entonces M es un ideal maximal de R si y sólo si R/M es un campo.*

Demostración. ($\Rightarrow$)
Supongamos que R es un anillo conmutativo con unitario.
$\Rightarrow R/M$ también tiene unitario ($1 + M$ es el unitario de R/M).
Sea $a + M \neq \overline{0}$ en R/M, P.D. que $a + M$ tiene un inverso.

$a + M \neq \overline{0} \Rightarrow a \notin M$ Considere N el ideal generado por a y M.

(es decir, $N = \langle \{\{a\}, M\} \rangle$). Entonces $M \subsetneq N \subseteq R$. Como M es maximal,

$$N = R. \text{ Así } 1 \in N \quad = \langle \{\{a\}M\} \rangle \quad = \{r_1 a + r_2 m | m \in M \text{ y } r_1, r_2 \in R\}$$
$$= \{ra + m | m \in M\}$$

Donde la última igualdad se da por que M es ideal de R.
Entonces $1 = ra + m$ para algún $r \in R$ y $m \in M$.
Así $1 + M = ra + m + M = ra + M = (r + M)(a + M)$, por tanto, $a + M$ tiene inverso multiplicativo.

($\Leftarrow$) Supongamos que R es un anillo conmutativo con unitario y que M es un ideal de R tal que R/M es un campo.
Sea N ideal de R tal que $M \subseteq N \subsetneq R$

Consideremos la proyección canónica $\pi : R \twoheadrightarrow R/M$
Tenemos que

$$\pi(N) \ \textit{ideal de} \ R/M \Rightarrow \begin{cases} \pi(N) = 0 \Rightarrow N \subseteq M \therefore N = M \\ \qquad \acute{o} \\ \pi(N) = R/M \end{cases}$$

Pero $\pi(N) = R/M$ no es posible, pues de ser así:

$$\begin{aligned} \pi(N) = R/M \ &\Rightarrow 1 + M \in \pi(N) = \{n + M \in R/M | n \in N\} \\ &\Rightarrow 1 + M = n + M \ \textit{para algún} \ n \in N \\ &\Rightarrow 1 - n \in M \\ &\Rightarrow 1 - n = m \ \textit{para algún} \ m \in M \\ &\Rightarrow 1 = n + m \in N \ \textit{pues por hipótesis} \ M \subseteq N. \end{aligned}$$

Pero $1 \in N \Rightarrow N = R$ lo cual es una contradicción pues supusimos que $N \subsetneq R$. ■

Corolario 1.2.4 *Un anillo conmutativo con unitario es un campo si y sólo si no contiene ideales propios no triviales.*

Demostración. ($\Rightarrow$) Sabemos que si R es un anillo conmutativo con unitario y N es un ideal que contiene una unidad entonces N=R.
$\Rightarrow$ Un campo no contiene ideales propios no triviales.

($\Leftarrow$) Supongamos que R es un anillo conmutativo con unitario tal que no contiene ideales propios no triviales.
Entonces $\{0\}$ es un ideal maximal de R, y por el teorema 1.2.3 tenemos que $R/\{0\}$ es un campo, pero $R/\{0\} \cong R$, por tanto, R es un campo. ■

Observación 1.2.5 *Sea $N \neq R$. R anillo conmutativo con unitario y N ideal de R.*

$$\begin{aligned} R/N \ \textit{es dominio de entero} \ &\Leftrightarrow R/N \ \textit{no tiene divisores de cero (por definición).} \\ &\Leftrightarrow ((a+N)(b+N) = 0 \Rightarrow a + N = N \ \ \acute{o} \ \ b + N = N) \\ &\Leftrightarrow (ab + N = N \Rightarrow a \in N \ \ \acute{o} \ \ b \in N) \\ &\Leftrightarrow (ab \in N \Rightarrow a \in N \ \ \acute{o} \ \ b \in N) \end{aligned}$$

Ejemplo 1.2.6 *Los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ (Ver ejemplo 28.1 en [1] pp. 253). Además $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ es dominio entero $\Leftrightarrow$ n es primo (ver ejemplo 28.2 en [1] pp. 253).*

Así los ideales $n\mathbb{Z}$ tales que $\mathbb{Z}/n\mathbb{Z}$ es dominio entero, son de la forma $p\mathbb{Z}$ donde p es primo.
Se tiene que $\mathbb{Z}/p\mathbb{Z}_p$ es un campo por ser dominio entero finito (ver ejemplo 28.2 en [1] pp. 253).
$\Rightarrow p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$.

Observación 1.2.7 *Por la observación 1.2.5 tenemos que $r, s \in p\mathbb{Z} \Leftrightarrow p|r$ ó $p|s$. Lo cual inspira la siguiente definición.*

Definición 1.2.8 *Un ideal $N \neq R$ en un anillo conmutativo R, es un ideal primo si $ab \in N$ implica que $a \in N$ ó $b \in N \ \ \forall\, a, b \in \mathbb{R}$.*

De la observación 1.2.5 obtenemos lo siguiente:

Teorema 1.2.9 *Sea R un anillo conmutativo con unitario y sea $N \neq R$ un ideal en R. Entonces R/N es un dominio entero $\Leftrightarrow$ N es ideal primo de R.*■

Corolario 1.2.10 *Todo ideal maximal en un anillo conmutativo R con unitario, es un ideal primo.*

Demostración. Por el teorema 1.2.3 M es maximal en $R \Leftrightarrow R/M$ es campo. En particular R/M es dominio entero. Pero R/M es dominio entero $\Leftrightarrow$ M es primo, esto por el teorema 1.2.9. ■

Definición 1.2.11 *Sea R cualquier anillo con unitario 1 y sea $n \in \mathbb{Z}$. La operación $n \cdot 1$ significa $1 + 1 + \cdots + 1$ con n sumandos para $n > 0$, y $(-1)+(-1)+\cdots+(-1)$ para $|n|$ sumandos con $n < 0$, mientras que $n \cdot 1 = 0$ para $n < 0$.*

Teorema 1.2.12 *Sea R anillo con unitario 1. Entonces la función*

$$\begin{array}{rccl} \Phi: & \mathbb{Z} & \longrightarrow & R \\ & n & \longmapsto & n \cdot 1 \end{array} \quad \textit{es un homomorfismo de anillos.}$$

Demostración.

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

usando la ley distributiva en R

$$\underbrace{(1+1+\cdots+1)}_{\text{n-sumandos}}\underbrace{(1+1+\cdots+1)}_{\text{m-sumandos}}=\underbrace{(1+1+\cdots+1)}_{\text{nm-sumandos}}$$

Así

$$(n\cdot 1)(m\cdot 1)=(nm)\cdot 1$$

para $m,n>0$. Es fácil probar que $\forall\ m,n\in\mathbb{Z}$

$$(n\cdot 1)(m\cdot 1)=(nm)\cdot 1$$

Entonces

$$\Phi(nm)=(nm)\cdot 1=(n\cdot 1)(m\cdot 1)=\Phi(n)\Phi(m).$$

■

Corolario 1.2.13 *Sea R anillo con unitario y característica $n>1$ (ver definición de* ***característica*** *de un anillo en [1] pp. 219), entonces R contiene un subanillo isomorfo a $\mathbb{Z}_n$. Si R tiene característica cero, entonces R contiene un anillo isomorfo a $\mathbb{Z}$.*

Demostración.
$\Phi:\mathbb{Z}\longrightarrow R\Rightarrow Ker\Phi$ es un ideal en $\mathbb{Z}$
$m\longmapsto m\cdot 1$
sabemos que todos los ideales en $\mathbb{Z}$ son de la forma $s\mathbb{Z}$ para $s\in\mathbb{Z}$
Si $n=CharR>0$ entonces notemos que $Ker\Phi=n\mathbb{Z}$:

Por definición $Ker\Phi=\{s\in\mathbb{Z}|s\cdot 1=0\}$. Dado que $n\cdot 1=0$

$$\begin{aligned}&\Rightarrow n\in Ker\Phi\\&\Rightarrow\langle n\rangle\leq Ker\Phi\\&\Rightarrow n\mathbb{Z}\leq Ker\Phi.\end{aligned}$$

Veamos que $Ker\Phi\subseteq n\mathbb{Z}$:
Sea $s\in Ker\Phi\Rightarrow s\cdot 1=0$. Dado que $0<n$ tenemos por el algoritmo de la división en $\mathbb{Z}$ que $s=nq+r,\quad 0\leq r<n$

$$\begin{aligned}&\Rightarrow s-nq=r\\&\Rightarrow r\cdot 1=(s-nq)\cdot 1=s\cdot 1-(nq)\cdot 1=0-0=0\\&\Rightarrow r\cdot 1=0\\&\Rightarrow r=0\end{aligned}$$

pues $n > 0$ es el mínimo entero tal que $n \cdot 1 = 0.$,

$$\Rightarrow s = nq \Rightarrow s \in n\mathbb{Z}. \ Por \ tanto \ Ker\phi = n\mathbb{Z}$$
$$\Rightarrow \mathbb{Z}/Ker\Phi = \mathbb{Z}/n\mathbb{Z} \cong \Phi(\mathbb{Z}) \subseteq R$$
$$\therefore \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \ es \ isomorfo \ a \ un \ subanillo \ de \ R.$$

Si $CharR = 0$ entonces $m \cdot 1 \neq 0 \ \forall \ m \neq 0$
$\Rightarrow Ker\Phi = \{s \in \mathbb{Z} \ s \cdot 1 = 0\} = \{0\} \Rightarrow \mathbb{Z} \cong \mathbb{Z}/\{0\} \cong \Phi(\mathbb{Z}) \subseteq \mathbb{R}$. ■

Teorema 1.2.14 *Todo campo F, o es de característica p para p algún primo y contiene un subcampo isomorfo a $\mathbb{Z}_p$ o bien es de característica cero y contiene un subcampo isomorfo a $\mathbb{Q}$.*

Demostración.
CASO 1: $CharF \neq 0$. Por el corolario 1.2.13 se tiene que F contiene un subanillo isomorfo a $\mathbb{Z}_n$. Notemos que n debe ser un primo p de lo contrario F tendría divisores de cero.

CASO 2: $CharF = 0$. Por el corolario 1.2.13 F contiene un anillo isomorfo a $\mathbb{Z}$, y F contiene al campo de cocientes de este anillo que debe ser $\mathbb{Q}$ (esto último por el teorema que afirma que si $CharF \neq 0$ entonces F contiene un subcampo isomorfo a $\mathbb{Q}$) (ver teorema 29.7 en [1] pp. 263). ■

Nota 1.2.15 *Los campos $\mathbb{Z}_p$ y $\mathbb{Q}$ son las piezas constitutivas fundamentales en la que descansan todos los campos.*

Definición 1.2.16 *Los campos $\mathbb{Z}_p$ y $\mathbb{Q}$ se llaman campos primos.*

Definición 1.2.17 *Sea R un anillo. Un polinomio $f(x)$ con coeficientes en R es una suma formal infinita*

$$\sum_{i=0}^{\infty} a_i x^i$$

donde $a_i \in R$ y $a_i = 0$ para todos, excepto un número finito de valores de i.

Definición 1.2.18 *Las a_i se llaman coeficientes de $f(x)$. Si $a_i \neq 0$ para alguna $i > 0$, el mayor de dichos valores de i es el grado de $f(x)$. De no existir dicha i diremos que $f(x)$ es de grado cero.*

Definición 1.2.19 *La suma y la multiplicación de polinomios con coeficientes en un anillo R se define como sigue. Sean $f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} a_i x^i$ polinomios. Definimos:*

$$f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

y definimos

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} d_i x^i \quad donde \quad d_i = \sum_{j=0}^{i} a_j b_{i-j} \quad para \quad cada \quad i = 0, 1, ...$$

Nota 1.2.20

$\sum_{j=0}^{i} a_j b_{i-j}$ *no necesariamente es igual a* $\sum_{j=0}^{i} b_j a_{i-j}$ *si R no es conmutativo.*

Teorema 1.2.21 *El conjunto $R[x]$ de todos los polinomios de una indeterminada x con coeficientes en un anillo R es un anillo bajo la suma y la multiplicación polinomial. Si R es conmutativo, también lo es $R[x]$ y si R tiene unitario 1 entonces 1 es también unitario en $R[x]$.*

Demostración. Aunque sencilla, la demostración es tediosa y por tanto no se incluye en esta tesis. Para la demostración ver [1] pp. 268-269. ■

Ejemplo 1.2.22 *$\mathbb{Z}[x]$ es el anillo de polinomios con indeterminada x con coeficientes en $\mathbb{Z}$. $\mathbb{Q}[x]$ es el anillo de polinomios en x con coeficientes racionales y así sucesivamente.*

Ejemplo 1.2.23 *En $\mathbb{Z}_2[x]$ tenemos*

$$\begin{aligned} (x+1)^2 &= (x+1)(x+1) \\ &= x^2 + (1+1)x + 1 \\ &= x^2 + 0x + 1 \\ &= x^2 + 1 \end{aligned}$$

También en $\mathbb{Z}_2[x]$ tenemos

$$\begin{aligned} (x+1) + (x+1) &= (1+1)x + (1+1) \\ &= 0x + 0 \\ &= 0 \end{aligned}$$

Definición 1.2.24 *Sea R un anillo y $\boldsymbol{x,y}$ indeterminadas, podemos formar en anillo $(R[x])[y]$; es decir, el anillo de polinomios en y con coeficientes que son polinomios en x.*

Observación 1.2.25

$$\begin{array}{ccc} (R[x])[y] & \cong & (R[y])[x] \\ r & \mapsto & r \\ x & \mapsto & x \\ y & \mapsto & y \end{array}$$

Es un isomorfismo canónico. Todo polinomio en y con coeficientes que son polinomios en x, pueden reescribirse de manera natural, como un polinomio en x con coeficientes en y. ■

Nota 1.2.26 *Identificaremos los anillos anteriores mediante el isomorfismo canónico y lo denotaremos por $R[x,y]$ a cualquiera de los dos anillos $(R[x])[y]$ y $(R[y])[x]$. Llamaremos a $R[x,y]$ el anillo con indeterminadas en x y y.*

Definición 1.2.27 *Análogamente definimos en anillo $R[x_1,...,x_n]$ de polinomios en n indeterminadas x_i con coeficientes en R.*

Observación 1.2.28 *Si D es un dominio entero, entonces también lo es $D[x]$.*
Recordemos que si

$$f(x) = \sum_{n=0}^{\infty} a_n x^n, g(x) = \sum_{n=0}^{\infty} b_n x^n$$

entonces

$$f(x)g(x) = \sum_{n=0}^{\infty} d_n x^n; \quad donde \quad d_n = \sum_{i=0}^{n} a_i b_{n-i}$$

Demostración. (por inducción)
Si $f(x)$ y $g(x)$ son polinomios cualquiera de grado tal que
$grad\ g(x) \leq grad\ f(x) = 0$ con $f(x) \neq 0$
entonces
$0 = f(x)g(x) = a_0 b_0$ con $a_0 \neq 0$ implica que $b_0 = 0$.
Supongamos que dados dos polinomios

$$f(x) = \sum_{n=o}^{n_0} a_n x^n \quad y \quad g(x) = \sum_{n=o}^{n_0} b_n x^n$$

tales que $f(x) \neq 0$ y $grad\ g(x) \leq grad\ f(x) \leq n_0$, se cumple que $0 = f(x)g(x) = \sum_{n=0}^{2n_0} d_n x^n$ entonces $b_n = 0\ \forall\ n \leqslant n_0$, donde $d_n = \sum_{i=0}^{n} a_i b_{n-i}\ \forall\ n \leqslant 2n_0$, es decir, se cumple que:

$$d_n = 0 \ \ \forall\ n \leq 2n_0$$
$$\Rightarrow b_n = 0 \ \ \forall n \leq n_0$$

Sean

$$f(x) = \sum_{n=0}^{n_0+1} a_n x^n, \quad g(x) = \sum_{n=0}^{n_0+1} b_n x^n$$

polinomios cualquiera tales que $f(x) \neq 0$ y $grad\ g(x) \leq grad\ f(x) \leq n_0 + 1$.
Demostraremos que $(d_n = 0 \ \ \forall n \leq 2n_0 + 2 \ \ \Rightarrow b_n = 0 \ \ \forall n \leq n_0 + 1)$
CASO 1: Si $grad\ f(x) \leq n_0$ ya está demostrado por la hipótesis de inducción.

CASO 2: Si $grad\ g(x) \leq grad\ f(x) = n_0 + 1 \Rightarrow a_{n_0+1} \neq 0$.
Dado que $d_n = 0 \ \ \forall n \leq 2n_0 + 2$ por la hipótesis de inducción tenemos que esto implica que $b_n = 0 \ \ \forall n \leq n_0$.
Nos queda demostrar que $b_{n_0+1} = 0$
Tenemos que $d_{2n_0+1} = d_{2n_0+2} = 0$

$$\Leftrightarrow \begin{cases} 0 = d_{2n_0+1} & = \sum_{i=0}^{2n_0+1} a_i b_{(2n_0+2)-i} \\ & = \sum_{i=0}^{n_0-1} a_i b_{(2n_0+1)-i} + \sum_{i=n_0+1}^{2n_0+1} a_i b_{(2n_0+1)-i} + a_{n_0} b_{(2n_0+1)-i} + a_{n_0} b_{(2n_0+1)-n_0} \\ & = a_{n_0} b_{n_0+1} \end{cases} \quad \textbf{(I)}$$

$$\Leftrightarrow \begin{cases} y \end{cases}$$

$$\begin{cases} 0 = d_{2n_0+2} & = \sum_{i=0}^{2n_0+2} a_i b_{(2n_0+2)-i} \\ & = \sum_{i=0}^{n_0} a_i b_{(2n_0+2)-i} + \sum_{i=n_0+2}^{2n_0+2} a_i b_{(2n_0+2)-i} + a_{n_0+1} b_{(2n_0+2)-(n_0+1)} \\ & = a_{n_0+1} b_{n_0+1} \end{cases} \quad \textbf{(II)}$$

donde la primera sumatoria en la expresión **(I)** anterior es cero por definición y la segunda sumatoria en la expresión **(I)** también es cero por hipótesis de inducción. Así obtenemos que $0 = d_{2n_0+1} = a_{n_0} b_{n_0+1}$.
Similarmente, la primera sumatoria en la expresión **(II)** es cero por definición y la segunda sumatoria en la expresión **(II)** también es cero por hipótesis de inducción. Así obtenemos que $0 = d_{2n_0+2} = a_{n_0+1} b_{n_0+1}$.

$$\Leftrightarrow \begin{cases} 0 = a_{n_0} b_{n_0+1} \\ \quad y \\ \\ 0 = a_{n_0+1} b_{n_0+1} \Rightarrow b_{n_0+1} = 0 \quad pues \quad a_{n_0+1} \neq 0 \end{cases}$$

■

A continuación se presenta una prueba corta de la observación 1.2.28.
(Si D es un dominio entero, también lo es $D[x]$).
Demostraremos que ($f(x) \neq 0$ y $g(x) \neq 0 \Rightarrow f(x)g(x) \neq 0$).

Demostración. Primero demostraremos que $f(x) \neq 0$ y $g(x) \neq 0$
$\Rightarrow grad(f(x)g(x)) = grad\ f(x) + grad\ g(x)$.
Sean

$$f(x) = \sum_{n=0}^{\infty} a_n x^n, \qquad g(x) = \sum_{n=0}^{\infty} b_n x^n$$

$grad(f(x)) = n_0$, $grad(g(x)) = m_0$ $\Rightarrow a_{n_0} \neq 0$ y $b_m \neq 0$. Por definición

$$f(x)g(x) = \sum_{n=0}^{\infty} d_n x^n \quad con \quad d_n = \sum_{i=0}^{n} a_i b_{n-i}$$

Consideremos el factor $d_{m_0+n_0}$

$$\begin{aligned} d_{m_0+n_0} &= a_0 b_{m_0+n_0} + a_1 b_{(m_0+n_0)-1} + \cdots + a_{n_0-1} b_{(m_0+n_0)-(n_0-1)} + a_{n_0} b_{(m_0+n_0)-n_0} \\ &\quad + a_{n_0+1} b_{(m_0+n_0)-(n_0+1)} + \cdots + a_{m_0+n_0} b_0 \\ &= \underbrace{a_0 b_{m_0+n_0} + a_1 b_{(m_0+n_0)-1} + \cdots + a_{n_0-1} b_{(m_0+1)}}_{\| \ 0} + a_{n_0} b_{m_0} \\ &\quad + \underbrace{a_{n_0+1} b_{(m_0+n_0)-(n_0+1)} + \cdots + a_{m_0+n_0} b_0}_{\| \ 0} \end{aligned}$$

Donde las expresiones marcadas son ceros por definición de $f(x)$ y $g(x)$.
Entonces tenemos que:

$$d_{m_0+n_0} = a_{n_0} b_{m_0}$$

Dado que $a_{n_0} \neq 0$ y $b_{m_0} \neq 0$ y que D es dominio entero se tiene que

$$a_{n_0} b_{m_0} \neq 0$$

Por tanto

$$grad(f(x)g(x)) \geqslant m_0 + n_0 = grad\ f(x) + grad\ g(x).$$

Para ver que

$$grad(f(x)g(x)) \leqslant grad\ f(x) + grad\ g(x)$$

Basta notar que por definición de $f(x)$ y $g(x)$ se tiene que

$$a_{n_0+i}b_{m_0+j} = 0 \ \ \forall\, i \geqslant 0, \ \ j \geqslant 0.$$

Por tanto

$$f(x) \neq 0 \ \ y \ \ g(x) \neq 0 \Rightarrow grad(f(x)g(x)) = grad\ f(x) + grad\ g(x).$$

Si $f(x) \neq 0$ y $g(x) \neq 0$ son tales que

$$grad\ f(x) = grad\ g(x) = 0 \quad entonces \quad f(x) = a_0, \ \ g(x) = b_0$$

$$\Rightarrow f(x)g(x) = a_0b_0 \neq 0 \ \ pues \ \ D \ \ es \ \ dominio \ \ entero.$$

Si al menos uno de ellos es mayor que cero,

$$\Rightarrow grad\ (f(x)g(x)) = grad\ f(x) + grad\ g(x) > 0 \Rightarrow f(x)g(x) \neq 0.$$

■

De la observación anterior tenemos como corolario:

Corolario 1.2.29 *Si F es un campo entonces F[x] es un dominio entero.*

Observación 1.2.30 *Notemos que F[x] no es un campo; pues x no es una unidad en F[x], es decir, no existe polinomio $f(x) \in F[x]$ tal que $xf(x) = 1$.*

Teorema 1.2.31 *Cualquier dominio entero D puede agrandarse en un campo F, tal que todo elemento de F puede expresarse como cociente de dos elementos de D.(Dicho campo F es un* ***campo de cocientes*** *de D.)*

Demostración. La demostración es análoga a la construcción de los racionales a partir de $\mathbb{Z}$, la cual no se presenta en esta tesis (para detalles de la demostración ver en [1] pp. 242). ■

Nota 1.2.32 *Por el teorema 1.2.31 podemos construir el campo de cocientes F(x) de F[x].*
Cualquier elemento de F(x) se puede expresar como un cociente $f(x)/g(x)$ de los polinomios en F[x] con $g(x) \neq 0$. Análogamente definimos

$$F(x_1, \cdots, x_n)$$

como el campo de cocientes de

$$F[x_1 \cdots x_n].$$

El campo $F(x_1,\cdots,x_n)$ se llama el campo de funciones racionales en n indeterminadas sobre F. Estos campos desempeñan un papel muy importante en geometría algebraica (ver ejemplo 30.1 en [1] pp. 269-270).

Teorema 1.2.33 *Sea F un subcampo de E, sea α cualquier elemento de E y sea x una indeterminada. La función $\Phi_\alpha : F[x] \to E$ definida por*

$$\Phi_\alpha(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

para $(a_0 + a_1x + \cdots + a_nx^n) \in F[x]$ es un homomorfismo de anillos.
Además $\Phi_\alpha|_F : F \hookrightarrow E$ el homomorfismo inclusión.
Así tenemos el siguiente diagrama conmutativo donde las flechas verticales son inclusiones.

$$\begin{array}{ccc} & & E \\ & & \uparrow \\ F[x] & \xrightarrow{\Phi_\alpha} & \Phi_\alpha(F[x]) \\ \uparrow & & \uparrow \\ F & \xrightarrow[Id]{} & F \end{array}$$

Demostración. Sea

$$f(x) \in F(x) \Rightarrow f(x) = a_0 + a_1x + \cdots + a_nx^n$$

$f(x)$ solo puede modificarse insertando términos de la forma $0x^i$. Lo cual claramente no afecta

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

Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + \cdots + b_mx^m$,
$h(x) = f(x) + g(x) = c_0 + c_1x + \cdots + c_rx^r$ Entonces
$\phi_\alpha(f(x) + g(x)) = \phi_\alpha(h(x)) = c_0 + c_1\alpha + \cdots + c_r\alpha^r$
Por otra parte,

$$\begin{aligned} \phi_\alpha(f(x)) + \phi_\alpha(g(x)) &= (a_0 + a_1\alpha + \cdots + a_n\alpha^n) + (b_0 + b_1\alpha + \cdots + b_m\alpha^m) \\ &= (a_0 + b_0) + (a_1 + b_1)\alpha + \cdots + (a_r + b_r)\alpha^r; \quad r = máx\{n, m\} \\ &= c_0 + c_1\alpha + \cdots + c_r\alpha^r \end{aligned}$$

■

Ejemplo 1.2.34 *Sean* $F = \mathbb{Q}$, $E = \mathbb{R}$
Sea

$$\begin{array}{rccc} \Phi_0: & \mathbb{Q}[x] & \longrightarrow & \mathbb{R} \\ & (a_0 + a_1 + \cdots + a_n x^n) & \mapsto & a_0 + a_1 0 + \cdots + a_n 0^n. \end{array}$$

Observación:

$$\begin{aligned} Ker\Phi_0 &= \{f(x) \in \mathbb{Q}[x] | \Phi_0(f(x)) = 0\} \\ &= \{\textstyle\sum_{i=0}^{\infty} a_i x^i \in \mathbb{Q}[x] | \Phi(\sum_{i=0}^{\infty} a_i x^i) = 0\} \\ &= \{\textstyle\sum_{i=0}^{\infty} a_i x^i \in \mathbb{Q}[x] | a_0 = 0\} \\ &= \{\textstyle\sum_{i=1}^{\infty} a_i x^i \in \mathbb{Q}[x]\} \\ &= \{x \textstyle\sum_{i=1}^{\infty} a_i x^{i-1}\} \\ &= \{xf(x) | f(x) \in \mathbb{Q}[x]\} \end{aligned}$$

Notamos que $\Phi_0(\mathbb{Q}[x]) = \mathbb{Q}$, *pues*

$$\begin{aligned} (\subseteq) \quad Sea \quad f(x) \in \Phi_0(\mathbb{Q}[x]) \quad &\Rightarrow f(x) = \Phi_0(g(x)) \quad p.a \quad g(x) \in \mathbb{Q}[x] \\ &\Rightarrow f(x) = a_0 \in \mathbb{Q} \therefore \Phi_0(\mathbb{Q}[x]) \subseteq \mathbb{Q} \end{aligned}$$

$(\supseteq)$ *Sea* $a \in \mathbb{Q}$ *y dado que* $\mathbb{Q} \subseteq \mathbb{Q}[x] \Rightarrow a \in \mathbb{Q}[x] \Rightarrow a = \Phi_0(a) \in \Phi_0(\mathbb{Q}[x])$
Por el teorema de isomorfismo tenermos que

$$\mathbb{Q}[x]/Ker\Phi_0 \cong \mathbb{Q}$$

Notando que una clase lateral $a + Ker\Phi_0 \in \mathbb{Q}[x]/Ker\Phi_0$ *consta de todos los polinomios en* $\mathbb{Q}[x]$ *que tienen término constante fijo* a.

Ejemplo 1.2.35 *Sean* $F = \mathbb{Q}, E = \mathbb{R}$. *Sea*

$$\Phi_2 : \mathbb{Q}[x] \longrightarrow \mathbb{R}$$

dada por:

$$\Phi_2(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 2 + \cdots + a_n 2^n$$

Notemos que $\Phi_2(\mathbb{Q}[x]) = \mathbb{Q}$ *pues*
$(\subseteq)$ $f(x) \in \mathbb{Q}[x] \Rightarrow \Phi_2(f(x)) = f(2) \in \mathbb{Q}$
$(\supseteq)$ *Sea* $q \in \mathbb{Q}, \Phi_2(x + (q-2)) = 2 + q - 2 = q \Rightarrow q \in \Phi_2(\mathbb{Q}[x])$

Tenemos que $(x-2) \in Ker\Phi_2$ *pues* $\Phi_2(x-2) = 2 - 2 = 0$
Así $\langle (x-2) \rangle \subseteq Ker\Phi_2$ *donde*
$N = \langle (x-2) \rangle = \{(x-2)f(x) | f(x) \in \mathbb{Q}[x]\}$
Demostraremos mas adelante que $N = Ker\Phi_2$
Y así tenemos por el teorema de isomorfismo que $\mathbb{Q}[x]/N \cong \mathbb{Q}$ *canónicamente.*

Ejemplo 1.2.36 *$F = \mathbb{Q}, E = \mathbb{C}$. Sea*

$$\Phi_i : \mathbb{Q}[x] \longrightarrow \mathbb{C}$$

dada por:

$$\Phi_i(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1i + \cdots + a_ni^n$$

Notemos que $\Phi_i(x^2+1) = i^2 + 1 = 0 \quad \therefore x^2 + 1 \in Ker\Phi_i$.
Así $\langle x^2+1\rangle \subseteq Ker\Phi_i$.
Por tanto $N = \langle x^2+1\rangle = \{(x^2+1)f(x) | f(x) \in \mathbb{Q}[x]\} \subseteq Ker\Phi_i$.
Demostraremos más adelante que $Ker\Phi_i = N$ Así tenemos que $\Phi_i(\mathbb{Q}[x]) \cong \mathbb{Q}[x]/N$.
Demostraremos también que $\Phi_i(\mathbb{Q}[x]) = \{q_1 + q_{2i} | q_1, q_2 \in \mathbb{Q}\}$
y que es un subcampo de $\mathbb{C}$.

Ejemplo 1.2.37 *$F = \mathbb{Q}, E = \mathbb{R}$. Sea*

$$\Phi_\pi : \mathbb{Q}[x] \longrightarrow \mathbb{R}$$

dada por:

$$\Phi_\pi(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\pi + \cdots + a_n\pi^n$$

$\therefore Ker\Phi_\pi = 0 \Rightarrow \mathbb{Q}[x] \cong \Phi_\pi(\mathbb{Q}[x])$. Donde hemos usado el hecho de que $(a_0 + a_i\pi + \cdots + a_n\pi^n = 0 \Leftrightarrow a_i = 0 \ \ \forall \ \ i = 0, \cdots, n)$.

Definición 1.2.38 *Sea F un subcampo de un campo E y sea $\alpha \in E$.*
Sea

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \ \ en \ \ F[x] \ \ y \ \ sea \ \ \Phi_\alpha : F[x] \to E$$

el homomorfismo de evaluación. Denotemos por

$$f(\alpha) \ \ a \ \ \Phi_\alpha(f(x)) = a_0 + a_1\alpha^1 + \cdots + a_n\alpha^n$$

Si $f(\alpha) = 0$, entonces diremos que α es un cero de $f(x)$.

Nota 1.2.39 *En términos de la definición anterior podemos replantear al problema de encontrar todas las soluciones a la ecuación polinomial*

$$r^2 + r - 6 = 0$$

Tomando $F = \mathbb{Q}$ y $E = \mathbb{R}$, lo replanteamos pidiendo encontrar todas las $\alpha \in \mathbb{R}$ tales que

$$\Phi_\alpha(x^2 + x - 6) = 0$$

Ambos problemas tienen la misma respuesta:

$$\begin{aligned}\{\alpha \in \mathbb{R} | \Phi_\alpha(x^2 + x - 6) = 0\} &= \{\alpha \in \mathbb{R} | (\alpha^2 + \alpha - 6) = 0\} \\ &= \{r \in \mathbb{R} | (r^2 + r - 6) = 0\}.\end{aligned}$$

Nota 1.2.40 *Si $f(x) \in F[x]$ no tiene un cero en F, tenemos que construir un campo E con $F \leqslant E$ tal que $\exists\ \alpha \in E$ tal que $f(\alpha) = \phi_\alpha(f(x)) = 0$. Para construir E se tiene que E debe contener $\phi_\alpha(F[x])$ bajo el homomorfismo valuación $\phi_\alpha : F[x] \to E$ y recordemos que por el teorema de isomorfismo de anillos $\phi_\alpha(F[x]) \cong F[x]/Ker\phi_\alpha$. Esto sugiere que debemos tratar de costruir E construyendo un anillo cociente $F[x]/N$ para cierto ideal N de $F[x]$.*
Por el teorema 1.2.3 tenemos que $F[x]/N$ es un campo $\Leftrightarrow$ N es un ideal maximal de $F[x]$.
Así que debemos estudiar los ideales de $F[x]$.

1.3. Factorización de polinomios sobre un campo.

Teorema 1.3.1 *(Algoritmo de la divisiòn para $F[x]$). Sea F un campo. Sean*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

Dos elementos en $F[x]$ con $a_i, b_i \in F$, $a_n \neq 0$, $b_m \neq 0$ y $m > 0$.
Entonces existen polinomios únicos $q(x)$ y $r(x)$ en $F[x]$ tales que

$$f(x) = g(x)q(x) + r(x)$$

Donde grad $r(x) <$ grad $g(x) = m$.

Demostración. Sea

$$S = \{f(x) - g(x)s(x) | s(x) \in F[x]\}$$

Sea $r(x) \in S$ un elemento de grado minimal.
$\Rightarrow r(x) = f(x) - g(x)q(x)$ para algún $q(x) \in F[x]$. Demostraremos primero que $grad(r(x)) < m = grad(g(x))$ por contradicción:
Supongamos que $grad\ r(x) \geq m$ entonces

$$r(x) = c_t x^t + c_{t-1}x^{t-1} + \cdots + c_0$$

Con $t \geq m$ y $c_t \neq 0$. consideremos la expresión

$$r(x) - (\frac{c_t}{b_m} x^{t-m}) g(x)$$

por una parte

$$r(x) - (\frac{c_t}{b_m} x^{t-m}) g(x) = r(x) - (c_t x^t + \ términos \ de \ grado \ menor)$$

$$\Rightarrow grad(r(x) - (\frac{c_t}{b_m} x^{t-m}) g(x)) < grad\ r(x)$$

por otra parte,

$$\begin{aligned} r(x) - (\tfrac{c_t}{b_m} x^{t-m}) g(x) &= (f(x) - g(x)q(x)) - (\tfrac{c_t}{b_m} x^{t-m}) g(x)) \\ &= f(x) - g(x)(q(x) + \tfrac{c_t}{b_m} x^{t-m}) \in S \end{aligned}$$

Lo cual contradice que $r(x) \in S$ es de grado minimal.

$$\therefore grad\ r(x) < m = grad\ g(x)$$

Demostraremos ahora la unicidad de $q(x)$ y $r(x)$:
Supongamos que

$$f(x) = g(x)q_1(x) + r_1(x)$$

y que

$$f(x) = g(x)q_2(x) + r_2(x)$$

sustrayendo las dos ecuaciones anteriores obtenemos

$$0 = g(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x)) \Rightarrow g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

Dado que

$$grad(r_2(x) - r_1(x)) < grad(g(x))$$

Esto solo es posible si

$$q_1(x) - q_2(x) = 0 \Rightarrow 0 = r_2(x) - r_1(x) \Rightarrow r_1(x) = r_2(x) \ \ y \ \ q_1(x) = q_2(x)$$

■

Corolario 1.3.2 *Sea F un campo.*
$a \in F$ es cero de $f(x) \in F[x] \Leftrightarrow x - a$ es factor de $f(x)$ en $F[x]$.

Demostración. ($\Rightarrow$) Supongamos que $f(a) = 0$.
Aplicando el teorema 1.3.1 del Algoritmo de la división tenemos que

$$f(x) = (x-a)q(x) + r(x)$$

con

$$\begin{aligned} grad\ r(x) < 1 = grad\ (x-a) &\Rightarrow grad\ r(x) = 0 \\ &\Rightarrow r(x) = c \in F \ \ (para\ \ algún\ \ c \in F) \\ &\Rightarrow f(x) = (x-a)q(x) + c \end{aligned}$$

Dado que $f(a) = 0 \Rightarrow 0 = f(a) = (a-a)q(a) + c \Rightarrow 0 = c$

$$\Rightarrow f(x) = (x-a)q(x)$$

$$\therefore (x-a)\ \ es\ \ factor\ \ de\ \ f(x).$$

($\Leftarrow$) Supongamos que $f(x) = (x-a)q(x)$.
Aplicando el homomorfismo valuación Φ_a tenemos que

$$f(a) = \phi_a(f(x)) = \phi_a(x-a)\phi_a(q(x)) = (a-a)q(a) = 0$$

Por tanto a es cero de $f(x)$. ■

Corolario 1.3.3 *Sea $f(x) \in F[x]$ un polinomio tal que grad $f(x) = n$ y $f(x) \neq 0$. Entonces $f(x)$ tiene a lo mas n ceros en un campo F.*

Demostración. Por el corolario anterior, si $a_1 \in F$ es un cero de $f(x)$ entonces

$$f(x) = (x-a_1)q_1(x) \ \ con\ \ grad(q_1(x)) = n-1$$

si a_2 es un cero de $q_1(x)$ entonces

$$f(x) = (x-a_1)(x-a_2)q_2(x) \ \ con\ \ grad(q_2(x)) = n-2$$

Continuando con este proceso llegamos a que

$$f(x) = (x-a_1)\cdots(x-a_r)q_r(x) \ \ con\ \ grad\ q_r(x) = n-r$$

y $q_r(x)$ no tiene mas ceros en F. Claramente $r \leq n$.
Además si $b \neq a_i \ \ \forall\ i = 1, \cdots, r$ con $b \in F$ entonces

$$f(b) = (b-a_1)\cdots(b-a_r)q_r(b) \neq 0$$

Pues F es campo $\Rightarrow$ F dominnio entero $\Rightarrow$ F no tiene divisores de cero y por construcción $b - a_i$ y $q_r(b)$ son distintos de cero. ■

Ejemplo 1.3.4 *trabajaremos con polinomios de* $\mathbb{Z}_5[x]$ *y dividamos*

$$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$$

entre

$$g(x) = x^2 - 2x + 3$$

para encontrar $q(x)$ *y* $r(x)$ *del teorema 1.3.1 (algoritmo de la división).*

$$\begin{array}{rl|l} & & x^2 - x - 3 \\ \cline{3-3} x^2 - 2x + 3 & | & x^4 - 3x^3 + 2x^2 + 4x - 1 \\ & & -(x^4 - 2x^3 + 3x^2) \\ \cline{3-3} & & \quad - x^3 - x^2 + 4x - 1 \\ & & \quad -(-x^3 + 2x^2 - 3x) \\ \cline{3-3} & & \quad\quad - 3x^2 + 7x - 1 \\ & & \quad\quad -(-3x^2 + 6x - 9) \\ \cline{3-3} & & \quad\quad\quad x + 8 \quad \equiv \quad x + 3 \end{array}$$

Por tanto tenemos que $x^4-3x^3+2x^2+4x-1 = (x^2-2x+3)(x^2-x-3)+(x+3)$
Así obtenemos

$$q(x) = x^2 - x - 3$$
$$r(x) = x + 3$$

Ejemplo 1.3.5 *Sea* $f(x) = x^4 + 3x^3 + 2x + 4 \in \mathbb{Z}_5[x]$.
Notemos que 1 es un cero:
$\phi_1(f(x)) = \phi_1(x^4 + 3x^3 + 2x + 4) = 1 + 3 + 2 + 4 = 10 = \bar{0} \in \mathbb{Z}_5[x]$ *por lo tanto podemos factorizar* $f(x) = x^4 + 3x^3 + 2x + 4$ *en* $(x - 1)q(x)$. *Usando la división*

$$\begin{array}{rl|l} & & x^3 + 4x^2 + 4x + 1 \\ \cline{3-3} x - 1 & | & x^4 + 3x^3 \quad\quad + 2x + 4 \\ & & -(x^4 - x^3) \\ \cline{3-3} & & \quad 4x^3 + \quad 2x + 4 \\ & & \quad -(\ 4x^3 - 4x^2) \\ \cline{3-3} & & \quad\quad 4x^2 + 2x + 4 \\ & & \quad\quad -(4x^2 - 4x) \\ \cline{3-3} & & \quad\quad\quad 6x + 4 \\ & & \quad\quad\quad\quad \| \\ & & \quad\quad\quad\quad x + 4 \\ & & \quad\quad\quad\quad -(x - 1) \\ \cline{3-3} & & \quad\quad\quad\quad\quad 5 \equiv 0 \end{array}$$

Por tanto se tiene que $x^4 - 3x^3 + 2x + 4 = (x-1)(x^3 + 4x^2 + 4x + 1) \in \mathbb{Z}_5[x]$
Notemos que 1 también es un cero de $x^3 + 4x^2 + 4x + 1$ *pues*

$$\phi_1(x^3 + 4x^2 + 4x + 1) = 1 + 4 + 4 + 1 = 10 = \bar{0} \in \mathbb{Z}_5[x]$$

Así podemos dividir $x^3 + 4x^2 + 4x + 1$ *entre* $x - 1$

$$\begin{array}{r|l}
 & \underline{\quad x^2 + 4 \qquad\qquad\quad} \\
x - 1 & x^3 + 4x^2 + 4x + 1 \\
 & \underline{-(x^3 - x^2) \qquad\qquad} \\
 & \quad 5x^2 + 4x + 1 \\
 & \qquad \parallel \\
 & \qquad \underline{0 + 4x + 1} \\
 & \qquad \underline{\quad -(4x - 4)} \\
 & \qquad\qquad\quad 5 \;\equiv\; 0
\end{array}$$

Entonces

$$x^3 + 4x^2 + 4x + 1 = (x-1)(x^2 + 4)$$

Y como nuevamente 1 *es cero de* $x^2 + 4$ *podemos hacer la siguiente división:*

$$\begin{array}{r|l}
 & \underline{\quad x + 1 \qquad\quad} \\
x - 1 & x^2 + \quad 4 \\
 & \underline{-(x^2 - x) \quad} \\
 & \qquad x + 4 \\
 & \quad \underline{-(x - 1)} \\
 & \qquad\quad 5 \;\equiv\; 0
\end{array}$$

Por lo tanto $x^2 + 4 = (x-1)(x+1)$
Y así tenemos que $x^2 + 3x^3 + 2x + 4 = (x-1)^3(x+1) \in \mathbb{Z}_5[x]$.

1.4. Polinomios irreducibles.

Definición 1.4.1 *Un polinomio no constante* $f(x) \in F[x]$ *es irreducible sobre* F *o es un polinomio irreducible en* $F[x]$ *si* $f(x)$ *no puede expresarse como producto* $g(x)h(x)$ *de dos polinomios* $g(x)$ *y* $h(x)$ *en* $F[x]$, *ambos de grado menor que el grado de* $f(x)$.

Tomando en cuenta que las unidades en $F[x]$ son los elementos distintos de cero en F (ver teorema 31.8 en [1] pp. 287-288) tenemos la siguiente definición que es equivalente a la anterior:

Definición 1.4.2 *Un polinomio no constante $f(x) \in F[x]$ es irreducible sobre F o es un polinomio irreducible en $F[x]$ si para toda factorización $f(x) = g(x)h(x)$ en $F[x]$, $g(x)$ o $h(x)$ es unidad.*

Nota 1.4.3 *La definición anterior trata del concepto de irreducible sobre F y no solo irreducible, como se ilustra en el siguiente*

Ejemplo 1.4.4 *x^2-2 visto en $\mathbb{Q}[x]$ no tiene ceros en $\mathbb{Q}$. Esto muestra que x^2-2 es irreducible sobre $\mathbb{Q}$ pues no existe una factorización $(ax+b)(cx+d)$ para $a,b,c,d \in \mathbb{Q}$ que de lugar a ceros de x^2-2 en $\mathbb{Q}$.*
Sin embargo x^2-2 visto en $\mathbb{R}[x]$ no es irreducible sobre $\mathbb{R}$ pues x^2-2 se factoriza sobre $\mathbb{R}$ como $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.

Ejemplo 1.4.5 *$f(x) = x^3+3x+2$ visto en $\mathbb{Z}_5[x]$ es irreducible en $\mathbb{Z}_5$.*
Supongamos que $f(x)$ se factoriza en $\mathbb{Z}_5[x]$ en polinomios de grado menor. Entonces tenemos un polinomio de grado 2 y otro de grado 1 (pues grad $(f(x)g(x)) =$ grad $f(x)+$ grad $g(x)$) en el dominio entero $D = \mathbb{Z}_5[x]$.
Así tenemos que $x-a$ es un factor de $f(x)$ para algún a en $\mathbb{Z}_5$. Pero por el corolario 1.3.2 ésto ocurre si y sólo si a es un cero de $f(x)$, con $a \in \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\} = \mathbb{Z}_5$, sin embargo se tiene que:

$$\begin{aligned} f(\bar{0}) &= 2 \\ \\ f(\bar{1}) &= 1+3+2 \\ &= 6 \\ &= \bar{1} \\ \\ f(\bar{2}) &= 8+6+2 \\ &= 16 \\ &= \bar{1} \\ \\ f(-2) &= -8-6+2 \\ &= -12 \\ &= -\bar{2} = \bar{3} \end{aligned}$$

Lo que muestra que $f(x)$ no tiene ceros en $\mathbb{Z}_5$, por tanto $f(x)$ es irreducible sobre $\mathbb{Z}_5$. ■

1.5. Criterios de irreducibilidad.

Inspirados por la técnica de los dos ejemplos anteriores tenemos el siguiente

Teorema 1.5.1 *Sea $f(x) \in F[x]$ y sea $f(x)$ de grado 2 o 3. Entonces $f(x)$ es reducible sobre $F \Leftrightarrow f(x)$ tiene un cero en F.*

Demostración. ($\Rightarrow$) Supongamos que $f(x)$ es reducible, es decir, se factoriza de la siguiente manera:

$$f(x) = g(x)h(x)$$

tal que

$$grad\ g(x) < grad\ f(x) \quad y \quad grad\ h(x) < grad\ f(x).$$

Esto implica que por lo menos un factor es de grado 1.
Digamos que

$$grad\ g(x) = 1 \Rightarrow g(x) = (x - a) \quad para \quad algún \quad a \quad en \quad F.$$

$$\Rightarrow g(a) = 0 \Rightarrow f(a) = g(a)h(a) = 0 \ con\ g(a) = 0 \Rightarrow f(a) = 0.$$

Por tanto $f(x)$ tiene un cero en F.

($\Leftarrow$) Supongamos que $f(x)$ tiene un cero en F. Por el corolario 1.3.2
$f(a) = 0$ para $a \in F$ si y sólo si $x - a$ es un factor de $f(x) \in F[x]$. Entonces $f(x) = (x - a)g(x)$ y por tanto $f(x)$ es reducible. ■

Teorema 1.5.2 *Sea $f(x) \in \mathbb{Z}[x]$. Entonces $f(x)$ se factoriza en un producto de dos polinomios de grado menor r y s en $\mathbb{Q}[x]$ si y sólo si tiene dicha factorización con polinomios de los mismos grados r y s en $\mathbb{Z}[x]$.*

Demostración. Para detalles de la demostración ver [1] pp. 283. ■

Corolario 1.5.3 *Si*

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

está en $\mathbb{Z}[x]$ con $a_0 \neq 0$, y si $f(x)$ tiene un cero en $\mathbb{Q}$ entonces tiene un cero $m \in \mathbb{Z}$ y $m|a_0$.

Demostración. Por el corolario 1.3.2 $f(a) = 0$ para algún $a \in \mathbb{Q}$ si y sólo si $f(x) = (x - a)g(x)$ para algún $g(x) \in \mathbb{Q}[x]$. Por el teorema 1.5.2 ésto pasa si y sólo si $f(x)$ tiene una factorización con un factor lineal en $\mathbb{Z}[x]$.
$\Rightarrow f(x) = (x - m)(x^{n-1} + \cdots + c_0)$ pero $c_0 = -\frac{a_0}{m} \therefore \frac{a_0}{m} \in \mathbb{Z} \Rightarrow m|a_0$ ■

Ejemplo 1.5.4 *El corolario anterior nos da una demostración de la irreducibilidad de* $x^2 - 2$ *sobre* $\mathbb{Q}$.

Demostración. Como $x^2 - 2$ es de grado 2, por el teorema 1.5.2 $x^2 - 2$ se factoriza de manera no trivial $\Leftrightarrow x^2 - 2$ tiene un cero en $\mathbb{Q} \Leftrightarrow x^2 - 2$ tiene un cero en $\mathbb{Z}$. Pero los únicos divisores de $a_0 = 2$ son $\pm 1, \pm 2$ y ninguno de éstos es cero de $x^2 - 2$. ■

Ejemplo 1.5.5 *Demuestre que* $f(x) = x^4 - 2x^2 + 8x + 1$ *visto en* $\mathbb{Q}[x]$ *es irreducible sobre* $\mathbb{Q}$.

Demostración. Tenemos dos casos: $f(x)$ tiene un factor lineal o $f(x)$ se factoriza en dos términos cuadráticos.
CASO 1: $f(x)$ tiene un factor lineal $x - a$ en $\mathbb{Q}[x]$ si y sólo si a es un cero de $\mathbb{Q}$, entonces por el corolario 1.5.3 $f(x)$ tiene un cero $m \in \mathbb{Z}$ y $m|a_0 = 1$. Así se tiene que $m = \pm 1$, pero $f(1) = 8$ y $f(-1) = -8$. Por tanto $f(x)$ no puede tener un factor lineal.

CASO 2: Supongamos que $f(x)$ se factoriza en dos factores cuadráticos en $\mathbb{Q}[x]$. Entonces por el teorema 1.5.2 tenemos que $f(x)$ se factoriza en dos factores cuadráticos en $\mathbb{Z}[x]$ es decir:

$$\begin{aligned} f(x) &= (x^2 + ax + b)(x^2 + cx + d) \ \ en \ \ \mathbb{Z}[x] \\ &= x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd \end{aligned}$$

(Notemos que en la primera igualdad hemos tomado el coeficiente de las x^2 como 1 sin pérdida de generalidad. Pues en general $x^4 = x^2 \cdot x^2$ o bien $x^4 = (-x^2)(-x^2)$ pero podemos suponer que los signos negativos son absorbidos por uno de los dos factores). Igualando términos con $f(x) = x^4 - ax^2 + 8x + 1$ obtenemos:
(1) $a + c = 0$
(2) $ac + b + d = -2$
(3) $ad + bc = 8$
(4) $bd = 1 \Rightarrow b = d = 1$ ó $b = d = -1$

CASO 1: $b = d = 1$
de (1) y (2) tenemos que: a+c=0 y ac+1+1=-2.
Entonces se obtiene que $a + c = 0$ y $ac = -4 \Rightarrow a = -c$ y $ac = -4$
$\Rightarrow a = -c = \pm 2$ pero $b = d = 1$ y (3) $\Rightarrow a + c = 8$ lo cual no es posible.
CASO 2: $b = d = -1$
Entonces por (3) y por $b = d = -1$ se tiene que $-a - c = 8$, por tanto

$a + c = -8$ y por otra parte por (1) $a + c = 0$ lo cual no es posible. Así se tiene que $f(x)$ es irreducible en $\mathbb{Q}[x]$. ■

Teorema 1.5.6 *(Eisenstein) Sea $p \in \mathbb{Z}$ un primo. Supongamos que*

$$f(x) = a_n x^n + \cdots + a_0$$

es un polinomio en $\mathbb{Z}[x]$ y $a_n \not\equiv 0 \pmod{p}$, pero $a_i \equiv 0 \pmod{p}$ para $i < n$ con $a_0 \not\equiv 0 \pmod{p^2}$. Entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

Demostración. Por el teorema 1.5.2 solo necesitamos demostrar que $f(x)$ no se factoriza en polinomios de grado menor en $\mathbb{Z}[x]$.

Supongamos que $f(x)$ es reducible en $\mathbb{Z}[x]$, entonces $f(x)$ se puede factorizar como:

$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$ *con* $b_r \neq 0, c_s \neq 0$ *tal que* $r, s < n$.

La hipótesis nos dice que, $p|a_0$ y $p^2 \nmid a_0$ *y* $a_0 = b_0 c_0$. Por lo tanto $(p \nmid b_0$ *y* $p|c_0)$ ó $(p|\, b_0$ *y* $p \nmid c_0)$.

Digamos que $p \nmid b_0$ *y* $p|c_0$.
por otra parte la hipótesis, $p \nmid a_n$ *y* $a_n = b_r c_s \Rightarrow p \nmid b_r$ *y* $p \nmid c_s$.
Sea m el menor valor de los $k = 0, 1, ..., s$ tal que $p \nmid c_k$ (m existe pues al menos para s tenemos que $p \nmid c_s$), así $0 \leq m \leq s$. Entonces

$$a_m = \sum_{j=0}^{m} c_j b_{m-j} = c_0 b_m + c_1 b_{m-1} + \cdots + c_{m-1} b_1 + c_m b_0$$

con $p|c_0, p|c_1, \cdots, p|c_{m-1}$ y $p \nmid c_m b_0$
$\Rightarrow p|(c_0 b_m + c_1 b_{m-1} + \cdots + c_{m-1} b_1)$ y $p \nmid c_m b_0$
Entonces concluimos que $p \nmid a_m$
(pues $p|a_m \Rightarrow p|(a_m - (c_0 b_m + c_1 b_{m-1} + \cdots + c_{m-1} b))) \Rightarrow p|c_m b_0!) \therefore p \nmid a_m$.
Las hipótesis del teorema implican que $m = n$, así $0 \leq n \leq s \Rightarrow s = n$
lo cual contradice que $s < n$. ■

Ejemplo 1.5.7 *Sea $p = 3$, por el teorema 1.5.6*

$$25x^2 - 9x^4 + 3x^2 - 12 \quad \textit{es irreducible sobre } \mathbb{Q}.$$

Demostración.

$$3 \nmid 25, \quad 3|-9, \quad 3|3, \quad 3|-12 \quad \textit{pero} \quad 3^2 \nmid -12$$

■

Corolario 1.5.8 *El polinomio ciclotómico*

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

es irreducible sobre $\mathbb{Q}$ *para cualquier primo* p.

Demostración. Nuevamente, por el teorema 1.5.2 solo necesitamos considerar factorizaciones en $\mathbb{Z}[x]$. Sea

$$g(x) = \Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x^{p-(p-1)} + \binom{p}{0}x^0) - 1}{x}$$

$$= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-2}x^2 + \binom{p}{p-1}x^1}{x}$$

$$= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-2}x^2 + px}{x}$$

$$\Rightarrow g(x) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + p$$

Notemos que $g(x)$ satisface el criterio de Eisentein para el primo p pues $p \nmid 1$ y $p|\binom{p}{1}$, $p|\binom{p}{2}$, $p|\binom{p}{p-2}$, $p|p$ pero $p^2 \nmid p$, (pues $p|\binom{p}{i}$ $\forall$ $1 \leq i \leq (p-2)$ porque

$$\binom{p}{i} = \frac{p!}{(p-i)!i!} = p\frac{(p-1)!}{(p-i)!i!} \text{ para } 1 \leq i \leq (p-2)$$

y notemos que

$$(p-i) \nmid p \ \forall \ i, \text{ y que } i \nmid p \ \forall \ i.$$

Por tanto, $(p-i)!i! \nmid p$ $\therefore p|\binom{p}{i}$ $\forall$ $1 \leq i \leq (p-2)$). Así $g(x)$ es irreducible sobre $\mathbb{Q}$.

Pero claramente, si $\Phi_p(x) = h(x)r(x)$ fuera una factorización no trivial de $\Phi_p(x)$ en $\mathbb{Z}[x]$ entonces

$$\Phi_p(x+1) = g(x) = h(x+1)r(x+1)$$

Sería una factorización no trivial de $g(x)$ en $\mathbb{Z}[x]$, pero ya vimos que $g(x)$ es irreducible, por tanto $\Phi_p(x)$ debe ser también irreducible sobre $\mathbb{Q}$. ■

Teorema 1.5.9 *Si* F *es un campo entonces todo ideal en* $F[x]$ *es principal.*

Demostración. Sea N un ideal en $F[x]$.
CASO (trivial): Si $N = \{0\}$ entonces $N = \langle 0 \rangle \therefore N$ es principal.

Supongamos que $N \neq \{0\}$ y sea $0 \neq g(x) \in N$ tal que $grad\ g(x)$ es minimal.

CASO 1: $grad\ g(x) = 0$ entonces $g(x) \in F - \{0\} \therefore g(x)$ es una unidad en F y tenemos que $N = F[x] = \langle 1 \rangle$ (ver teorema 28.4 en [1] pp. 254), por tanto N es principal.

CASO 2: $grad\ g(x) \geq 1$.
Sea $f(x) \in N$ un elemento arbitrario. Por el Teorema 1.3.1 (Algoritmo de la división en $F[x]$) se tiene que $f(x) = g(x)q(x) + r(x)$ con $grad\ r(x) < grad\ g(x)$.
Tenemos $f(x) \in N$ y claramente $g(x)q(x) \in N$ (pues $g(x) \in N$ y N es ideal), de donde tenemos que $r(x) = f(x) - g(x)q(x) \in N$ con $grad\ r(x) < grad\ g(x)$.
Como $0 \neq g(x) \in N$ es de grado minimal ésto obliga a que $r(x) = 0$, por tanto, $f(x) = g(x)q(x)$ y entonces $N = \langle g(x) \rangle$. Así N es ideal principal. ■

Ahora caracterizaremos los ideales maximales de $F[x]$.

Teorema 1.5.10 *Un ideal $\langle p(x) \rangle \neq \{0\}$ en $F[x]$ es maximal $\Leftrightarrow$ $p(x)$ es irreducible sobre F.*

Demostración.
($\Rightarrow$) Supongamos que $\langle p(x) \rangle \neq 0$ es un ideal maximal en $F[x]$
(recordemos que por definición M ideal de R es maximal $\Leftrightarrow M \subsetneq R$ y si N es ideal propio de R, tal que $M \subseteq N \subsetneq R$ entonces $M = N$). En particular $\langle p(x) \rangle \subsetneq F[x] \Rightarrow p(x) \notin F$ (pues si $p(x) \in F$ y $p(x) \neq 0$ entonces $\langle p(x) \rangle = F[x]$).
Por otra parte si $\langle p(x) \rangle$ es maximal, entonces por el corolario 1.2.10 $\langle p(x) \rangle$ es un ideal primo. Sea

$$p(x) = f(x)g(x)$$

una factorización de $p(x)$, entonces $f(x)g(x) \in \langle p(x) \rangle$ Entonces por definición de ideal primo tenemos que $f(x) \in \langle p(x) \rangle ó\ g(x) \in \langle p(x) \rangle$. De esta manera se tendría que $f(x) = p(x)q_1(x)\ ó\ g(x) = p(x)q_2(x)$ para $q_1(x), q_2(x)$ en $F[x]$ por lo que $grad\ f(x) \geq grad\ p(x) ó\ grad\ g(x) \geq grad\ p(x)$, por tanto, $p(x)$ es irreducible sobre F.

($\Leftarrow$) Supongamos que $p(x)$ es irreducible sobre F.
Supongamos que N es un ideal de $F[x]$ tal que $\langle p(x)\rangle \subseteq N \subseteq F[x]$.
Por el teorema 1.5.9 N es un ideal principal, esto es,
$N = \langle g(x)\rangle$ para algún $g(x) \in N$.

Por otra parte como $\langle p(x)\rangle \subseteq N$ se tiene que $p(x) \in N$, por tanto
$p(x) = g(x)q(x)$ para algún $q(x) \in F[x]$, pero por hipótesis $p(x)$ es irreducible sobre F $\Rightarrow$ $g(x)$ o $q(x)$ es de grado cero.

CASO 1: si *grad* $g(x) = 0$ entonces $g(x) = c \in F$ con $c \neq 0$ (pues $c = 0 \Rightarrow p(x) = g(x)q(x) = cq(x) = 0$!).
Así $g(x) \in F - \{0\}$, es decir, $g(x)$ es una unidad y entonces
$N = \langle g(x)\rangle = F[x]$.

CASO 2: si *grad* $q(x) = 0$ entonces $q(x) = c \in F$, $c \neq 0 \Rightarrow g(x) = \frac{1}{c}p(x) \in \langle p(x)\rangle$
$\Rightarrow N = \langle g(x)\rangle \subseteq \langle p(x)\rangle \therefore N = \langle p(x)\rangle$.
Así no es posible tener que $\langle p(x)\rangle \subsetneq N \subsetneq F[x] \therefore \langle p(x)\rangle$ es maximal. ■

Ejemplo 1.5.11 *Demostramos en el ejemplo 1.4.5 que el polinomio* x^3+3x+2 *es irreducible sobre* $\mathbb{Z}_5[x]$, *entonces por el teorema 1.2.3,* $\mathbb{Z}[x]/\langle x^3+3x+2\rangle$ *es un campo.*
También el polinomio x^2-2 *es irreducible sobre* $\mathbb{Q}[x]$ *y por tanto* $\mathbb{Q}[x]/\langle x^2-2\rangle$ *es un campo.*
Se examinarán dichos campos con mas detalles posteriormente.

Definición 1.5.12 *Sean* $f(x), g(x) \in F[x]$. *Decimos que* $g(x)$ *divide a* $f(x)$ *en* $F[x]$ *si existe un polinomio* $q(x) \in F[x]$ *tal que* $f(x) = g(x)q(x)$.

Teorema 1.5.13 *Sea* $p(x)$ *un polinomio irreducible en* $F[x]$. *Si* $p(x)$ *divide a* $r(x)s(x)$ *para* $r(x), s(x) \in F[x]$, *entonces* $p(x)$ *divide a* $r(x)$ *o* $p(x)$ *divide a* $s(x)$.

Demostración. supongamos que $p(x)|r(x)s(x) \Rightarrow p(x)q(x) = r(x)s(x)$ para algún $q(x) \in F[x]$, entonces $r(x)s(x) \in \langle p(x)\rangle$. Por el teorema 1.5.10 $\langle p(x)\rangle$ es un ideal maximal, y entonces $\langle p(x)\rangle$ es un ideal primo, por tanto, $r(x) \in \langle p(x)\rangle$ ó $s(x) \in \langle p(x)\rangle$, así se tiene que $p(x)|r(x)$ ó $p(x)|s(x)$. ■

Corolario 1.5.14 *Si* $p(x)$ *es irreducible en F[x] y p(x) divide al producto* $r_1(x)\cdots r_n(x)$ *para* $r_i(x) \in F[x]$ *entonces p(x) divide* $r_i(x)$ *para almenos una* i.

Demostración. Usar teorema 1.5.13 e inducción. ■

Teorema 1.5.15 *Sea F un campo, entonces todo polinomio no constante $f(x) \in F[x]$ se puede factorizar en $F[x]$ en un producto de polinomios irreducibles, además los polinomios irreducibles son únicos, excepto por el orden y por factores que son unidades (esto es, constantes distintas de cero) en F.*

Demostración. Sea $f(x) \in F[x]$ un polinomio no constante.
Si f(x) no es irreducible entonces $f(x) = g(x)h(x)$ con $grad\ g(x)$ y $grad\ h(x)$ ambos menores que $grad\ f(x)$. Si $g(x)$ y $h(x)$ son irreducibles nos detenemos aquí. De no ser así, almenos uno de ellos se factoriza en polinomios de grado menor. continuando este proceso (en realidad es un proceso de inducción), llegamos a la factorización

$$f(x) = p_1(x)p_2(x)\cdots p_r(x)$$

donde p_i es irreducible para toda i.
Demostremos la unicidad. Supongamos que

$$f(x) = p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x)$$

son dos factorizaciones de $f(x)$ en polinomios irreducibles, entonces por el corolario 1.5.14 se tiene que $p_1(x)|q_j(x)$ para alguna j, $1 \leq j \leq s$, supongamos sin pérdida de generalidad que $j = 1$ así $p_1(x)|q_1(x)$.
Como $q_1(x)$ es irreducible, $q_1(x) = u_1p_1(x)$, donde $u_1 \neq 0$ y $u_1 \in F$, i.e. u_1 es unidad.
Sustituyendo en la igualdad $q_1(x)$ por $u_1p(x)$ tenemos

$$p_1(x)p_2(x)\cdots p_r(x) = u_1p_1(x)q_2(x)\cdots q_s(x)$$

Todos los factores son distintos de cero (pues si no $f(x) = 0$!) además ya probamos que $F[x]$ es un dominio entero por lo que podemos cancelar,

$$\Rightarrow p_2(x)\cdots p_r(x) = u_1q_2(x)\cdots q_s(x)$$

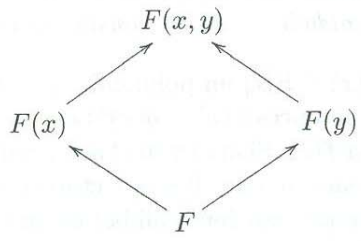
Al continuar de esta forma llegamos a que

$$\begin{aligned}
&1 = u_1u_2\cdots u_rq_{r+1}(x)\cdots q_s(x)\\
&\Rightarrow q_{r+1}(x)\cdots q_s(x) = 1\cdot(u_1u_2\cdots u_r)^{-1} \ \textit{es una unidad } u\\
&\Rightarrow r = s\\
&\textit{con}\ \ 1 = u_1u_2\cdots u_ru
\end{aligned}$$

por tanto, los factores $p_i(x)$ y $q_j(x)$ fueron los mismos excepto quizá por el orden y por factores unidades. ■

Definición 1.5.16 *Un campo E es un campo de extensión de un campo F si F es subcampo de E.*

Ejemplo 1.5.17



(donde todas las flechas son inclusiones)

Teorema 1.5.18 *(Kronecker)(objetivo fundamental)*
Sea F un campo y sea $f(x)$ un polinomio no constante en $F[x]$.
Entonces existe un campo de extensión E de F y alguna $\alpha \in E$ tal que $f(\alpha) = 0$.

Demostración. Por el teorema 1.5.15 $f(x)$ tiene factorización en polinomios que son irreducibles en F. Sea $p(x)$ un polinomio irreducible que aparece en dicha factorización, entonces por el teorema 1.5.10 $\langle p(x)\rangle$ es un ideal maximal de $F[x]$. Pero ésto ocurre si y sólo si, $E = F[x]/\langle p(x)\rangle$ es un campo, ésto por el teorema 1.2.3. Sea

$$\begin{aligned} \Psi : F &\longrightarrow F[x]/\langle p(x)\rangle \\ a &\longmapsto a + \langle p(x)\rangle \end{aligned}$$

Notemos que Ψ en la composición $F \hookrightarrow^{i} F[x] \to^{\Pi} F[x]/\langle p(x)\rangle$, por tanto, Ψ es un homomorfismo de anillos.
Veamos que Ψ es uno a uno.
Sea $a \in F$ tal que $\Psi(a) = 0$ entonces $a + \langle p(x)\rangle = \langle p(x)\rangle$ si y sólo si $a \in \langle p(x)\rangle$. Así, $a = g(x)p(x)$ para algún $g(x) \in F[x]$, entonces $grad\ (a) \geqslant grad\ p(x) \geqslant 1$ ó $a = 0$. Entonces $grad(a) = 0$, pues $a \in F$, por tanto, $a = 0$.

Y por tanto Ψ es uno a uno.

Así $\Psi : F \longrightarrow \Psi(F) = \{a + \langle p(x)\rangle | a \in F\}$ con $\Psi(F)$ subcampo de $F[x]/\langle p(x)\rangle = E$.
Identificando F con el subcampo $\{a + \langle p(x)\rangle | a \in F\}$ tenemos que si $p(y) = a_0 + a_1 y + \cdots + a_n y^n \in F[y]$ entonces $p(y) = \overline{a_0} + \overline{a_1} y + \cdots + \overline{a_n} y^n \in F[y]$ bajo nuestra identificación en $E[y]$ donde $\overline{a_i} = a_i + \langle p(x)\rangle$. Sea $\alpha = x + \langle p(x)\rangle \in E$, aplicando $\Phi_\alpha : F[y] \longrightarrow E$ a $p(y)$ obtenemos:

$$\begin{aligned} p(\alpha) = \Phi_\alpha(p(y)) &= \overline{a_0} + \overline{a_1}(x + \langle p(x)\rangle) + \cdots + \overline{a_n}(x + \langle p(x)\rangle)^n \ \ en \ \ E. \\ &= a_0 + a_1 x + \cdots + a_n x^n + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle \\ &= 0 \ \ en \ \ E. \end{aligned}$$

■

Ejemplo 1.5.19 *Sean $F = \mathbb{R}$ y $f(x) = x^2 + 1$ (sabemos que $f(x)$ no tiene ceros en $\mathbb{R}$ y por tanto $f(x)$ es irreducible sobre $\mathbb{R}$).$\Rightarrow \langle x^2 + 1\rangle$ es un ideal maximal en $\mathbb{R}[x]$. Entonces $\mathbb{R}[x]/\langle x^2 + 1\rangle$ es un campo.*
Identificando $r \in \mathbb{R}$ con $r + \langle x^2 + 1\rangle$ en $\mathbb{R}[x]/\langle x^2 + 1\rangle$ podemos considerar a $\mathbb{R}$ como un subcampo de $E = \mathbb{R}[x]/\langle x^2 + 1\rangle$.
Sea $\alpha = x + \langle x^2 + 1\rangle$ tenemos que
$\Phi_\alpha : \mathbb{R}[x] \longrightarrow \mathbb{R}[x]/\langle x^2 + 1\rangle = E$ y evaluando en $f(x) = x^2 + 1$ tenemos que

$$\begin{aligned} f(\alpha) = \Phi_\alpha(x^2 + 1) &= \Phi_\alpha((x^2 + 1) + \langle x^2 + 1\rangle) \\ &= (x + \langle x^2 + 1\rangle)^2 + 1 + \langle x^2 + 1\rangle \\ &= x^2 + 1 + \langle x^2 + 1\rangle \\ &= 0 \quad en \quad E. \end{aligned}$$

por tanto, $\alpha \in E$ es un cero de $x^2 + 1$.
Identificaremos en la sección 2 del próximo capítulo a $\mathbb{R}[x]/\langle x^2 + 1\rangle$ con $\mathbb{C}$.

Ejemplo 1.5.20 *Sea $F = \mathbb{Q}$ y sea $f(x) = x^4 - 5x^2 + 6$. Ahora, f(x) se factoriza como $f(x) = (x^2 - 2)(x^2 - 3)$ en $\mathbb{Q}[x]$ y ambos factores son irreducibles sobre $\mathbb{Q}$ como vimos antes. Podemos tomar $E = \mathbb{Q}[x]/\langle x^2 - 2\rangle$*
y entonces $\alpha = x + \langle x^2 - 2\rangle$ es tal que $\alpha^2 - 2 = 0$ ó podemos tomar
$E' = \mathbb{Q}[x]/\langle x^2 - 3\rangle$ con $\alpha' = x + \langle x^2 - 3\rangle$ y tendremos que $\alpha'^2 - 3 = 0$
En ambos casos la construcción es como en el ejemplo anterior.

1.6. Elementos algebraicos y trascendentes.

Definición 1.6.1 *Sea E un campo de extensión de F.*
Decimos que $\alpha \in E$ es algebraico sobre F si $f(\alpha) = 0$ para algún $f(x) \in F[x]$ con $f(x) \neq 0$. Si α no es algebraico sobre F, diremos que α es trascendente sobre F.

Ejemplo 1.6.2 *$\mathbb{Q}$ subcampo de $\mathbb{C}$. $\sqrt{2}$ es cero de $x^2 - 2 \in \mathbb{Q}[x]$. Por tanto, $\sqrt{2} \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$.*

También $i \in \mathbb{C}$ es un elemento algebraico sobre $\mathbb{C}$ pues i es cero del polinomio $x^2 + 1 \in \mathbb{Q}[x]$.

Ejemplo 1.6.3 *Los números reales π y e son trascendentes sobre $\mathbb{Q}$. Para la demostración de este ejemplo ver [2] pp. 207-2010.*

Ejemplo 1.6.4 *$\pi \in \mathbb{R}$ es trascendente sobre $\mathbb{Q}$, sin embargo π es algebraico sobre $\mathbb{R}$ pues es cero del polinomio $x - \pi \in \mathbb{R}[x]$.*

Ejemplo 1.6.5 *El número real $\sqrt{1+\sqrt{3}}$ es algebraico sobre $\mathbb{Q}$.*
Sea $\alpha = \sqrt{1+\sqrt{3}} \Rightarrow \alpha^2 = 1+\sqrt{3}$ y entonces $\alpha^2 - 1 = \sqrt{3}$ y así, $(\alpha^2-1)^2 = 3$ $\Rightarrow \alpha^4 - 2\alpha^2 + 1 = 3 \Rightarrow \alpha^4 - 2\alpha^2 - 2 = 0$, por tanto, $\alpha = \sqrt{1+\sqrt{3}}$ es un cero de un polinomio sobre $\mathbb{Q}[x]$.

La siguiente definición es una definición usada en teoría de números.

Definición 1.6.6 *Un elemento en $\mathbb{C}$ que es algebraico sobre $\mathbb{Q}$ es un número algebraico.*
Un número trascendente es un elemento en $\mathbb{C}$ que es trascendente sobre $\mathbb{Q}$.

Teorema 1.6.7 *Sea E un campo de extensión de F y sea $\alpha \in E$. Sea*

$$\Phi_\alpha : F[x] \longrightarrow E$$

el homomorfismo evaluación ($\Phi_\alpha(a) = a \ \forall \ a \in F$ y $\Phi_\alpha(x) = \alpha$).
Entonces α es trascendente sobre $F \Leftrightarrow \Phi_\alpha$ es monomorfismo.

Demostración. ($\Rightarrow$)$Ker\ \Phi_\alpha = \{f \in F[x] | \Phi_\alpha(f) = 0\}$ pero por definición $\Phi_\alpha(f) \neq 0 \ \ \forall\ 0 \neq f(x) \in F[x]$, por tanto $Ker\ \Phi_\alpha = 0$.

($\Leftarrow$) Si Φ_α monomorfismo, se tiene que $Ker\ \Phi_\alpha = \{0\} \Leftrightarrow \{f \in F[x] | f(\alpha) = 0\} = 0$, por tanto, $f(\alpha) \neq 0 \ \forall\ 0 \neq f(x) \in F[x]$
$\therefore \alpha$ es trascendente sobre $F[x]$. ■

1.7. El polinomio irreducible asociado a un elemento algebraico α sobre F.

Motivación: $\mathbb{Q}$ subcampo de $\mathbb{R}$. Sabemos que $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$ y $\sqrt{2}$ es un cero de x^2-2. También $\sqrt{2}$ es cero de por ejemplo los polinomios x^3-2x y de $x^4-3x^2+2=(x^2-2)(x^2-1)$. Todos estos polinomios que tienen a $\sqrt{2}$ como cero, son múltiplos del polinomio x^2-2.

El siguiente teorema muestra que esto siempre se da en el caso general.

Teorema 1.7.1 *Sea E un campo de extensión de F y sea $\alpha \in F$ tal que α es algebraico sobre F. Entonces existe (por definición) algún polinomio irreducible $p(x) \in F[x]$ tal que $p(\alpha)=0$. Además $p(x)$ está determinado de manera única salvo un factor constante en F y es un polinomio de grado minimal mayor o igual que 1 en $F[x]$ que tiene a α como un cero. También si $f(\alpha)=0$ para algún $f(x) \in F[x]$ con $f(x) \neq 0$ entonces $p(x)|f(x)$.*

Demostración. Consideremos el homomorfismo valuación

$$\Phi_\alpha : F[x] \longrightarrow F$$

$\Rightarrow Ker\Phi_\alpha = \{f \in F[x] | f(\alpha)=0\}$. Dado que α es algebraico sobre F tenemos que $\exists \ \ 0 \neq f(x) \in F[x] \ \ tal \ \ que \ \ f(\alpha)=0 \ \therefore Ker\Phi_\alpha \neq 0$. Ya probamos anteriormente que $F[x]$ es un DIP $\therefore Ker\Phi_\alpha = \langle p(x) \rangle$ para algún $p(x) \in F[x]$. Además dado que $Ker\Phi_\alpha \neq 0 \Rightarrow p(x) \neq 0$.
Notemos también que $p(x)$ no puede ser una constante c distinta de cero pues tendríamos que $c=p(\alpha)=0 \therefore grad\ p(x) \geq 1$.
Sea $0 \neq f(x) \in F[x] \ \ tal \ \ que \ \ f(\alpha)=0. \Rightarrow f(x) \in Ker\Phi_\alpha \Rightarrow f(x) = g(x)p(x) \ para \ algún \ g(x) \in F[x] \Rightarrow p(x)|f(x) \ \forall \ f(x) \in F[x]$ tal que $f(\alpha)=0$. Además $p(x)$ es de grado minimal tal que $f(\alpha)=0$ pues $p(x)|f(x) \ \forall \ f(x) \in F[x]$ tal que $f(\alpha)=0 \Rightarrow p(x)g(x)=f(x) \Rightarrow grad\ p(x) \leq grad\ f(x)$.

-$p(x)$ es irreducible-
$p(x)=r(x)s(x) \Rightarrow 0=p(\alpha)=r(\alpha)s(\alpha) \Rightarrow r(x)$ es una constante o $s(x)$ es una constante pues de no ser así se constradice la minimalidad del grado de p(x). ■

El teorema anterior nos permite dar la siguiente

Definición 1.7.2 *Sea E un campo de extensión del campo F y sea $\alpha \in E$ algebraico sobre F. El único polinomio mónico $p(x)$ del teorema 1.7.1 será llamado el polinomio irreducible para α sobre F y se denotará por $irr(\alpha, F)$. El grado de $irr(\alpha, F)$ se llama el grado de α sobre F y se denotará por grad (α, F).*

Ejemplo 1.7.3 *a).-* $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$.
b).- En el ejemplo 1.6.5 vimos que $\alpha = \sqrt{i + \sqrt{3}} \in \mathbb{R}$ *es un cero de* $x^4 - 2x - 2 \in \mathbb{Q}[x]$. *Por Eisenstein (con* $p = 2$*) vemos que* $x^4 - 2x - 2$ *es irreducible sobre* $\mathbb{Q}$
$\therefore irr(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2$
y grad $(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = 4$.

Ejemplo 1.7.4 $\sqrt{2} \in \mathbb{R}$ *es algebraico de grado 2 sobre* $\mathbb{Q}$, *pues* $\sqrt{2}$ *es cero del polinomio mónico irreducible* $x^2 - 2$ *en* $\mathbb{Q}[x]$.
$\sqrt{2} \in \mathbb{R}$ *es algebraico de grado 1 sobre* $\mathbb{R}$ *pues es* $x - \sqrt{2}$ *es un polinomio mónico irreducible en* $\mathbb{R}[x]$ *que tiene a* $\alpha = \sqrt{2}$ *como un cero.*

Capítulo 2

Extensiones de campos.

2.1. Extensiones simples.

Observación 2.1.1 *Sea F subcampo de E y sea $\alpha \in E$. Sea*

$$\Phi_\alpha : F[x] \longrightarrow E$$

el homomorfismo evaluación.

Entonces sólo existen dos posibilidades, que α sea algebraico sobre F o que α sea trascendente sobre F.
CASO 1: α es algebraico sobre F. En la demostración del teorema 1.7.1, vimos que

$$Ker\ \Phi_\alpha = \langle irr(\alpha, F)\rangle$$

Por el teorema 1.5.10 se tiene que $\langle irr(\alpha, F)\rangle$ es un ideal maximal de $F[x]$. Y por el teorema 1.2.3 tenemos que $F[x]/\langle irr(\alpha, F)\rangle$ es un campo.
Por otra parte, por el **primer teorema de isomorfismo de anillos** (ver teorema en [1] pp. 141-142), tenemos el isomorfismo canónico de anillos

$$\overline{\Phi}_\alpha : F[x]/\langle irr(\alpha, F)\rangle \longrightarrow \Phi_\alpha(F[x]) \subseteq E.$$

Dado que $\overline{\Phi}_\alpha$ es isomorfismo de anillos y $F[x]/\langle irr(\alpha, F)\rangle$ es campo, entonces $\Phi_\alpha(F[x])$ es subcampo de E.
Por otra parte,

$$\Phi_\alpha(F[x]) = \{f(\alpha) | f(x) \in F[x]\} \equiv \{ \sum_{i,finita} a_i \alpha^{i_k} | a_i \in F\},$$

notemos que cualquier campo que contenga a F y a α debe contener al conjunto anterior que es un campo, por lo tanto $\Phi_\alpha(F[x])$ es el menor subcampo de E que contiene a F y a α. Denotaremos este campo por $F(\alpha)$.

CASO 2: α es trascendente sobre F. Por el teorema 1.6.7, $\Phi_\alpha : F[x] \longrightarrow E$ es monomorfismo de anillos.
Entonces $\Phi_\alpha : F[x] \longrightarrow \Phi_\alpha(F[x])$ es isomorfismo de anillos (pues $F[x]$ es dominio entero y no es campo). Entonces $\Phi_\alpha(F[x])$ es dominio entero y no es campo. Denotaremos a $\Phi_\alpha(F[x])$ por $F[\alpha]$.
Pero se tiene que cualquier campo E que contiene a un dominio entero $F[\alpha]$ contiene al campo de cocientes de $F[\alpha]$ (ver corolario en [1] pp. 244) así E contiene un campo de cocientes de $F[\alpha]$ y por lo tanto dicho campo de cocientes es el menor subcampo de E que contiene al campo F y a α. Como en el CASO 1 denotaremos este campo por $F(\alpha)$.

Definición 2.1.2 *Un campo de extensión E de un campo F es una extensión simple de F si $E = F(\alpha)$ para algún $\alpha \in E$.*

Teorema 2.1.3 *Sea E una extensión simple $F(\alpha)$ de un campo F y sea α algebraico sobre F. Sea $n \geq 1$ el grado de $irr(\alpha, F)$. Entonces todo elemento β de $E = F(\alpha)$ se puede expresar de manera única como:*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \quad \textit{donde} \quad b_i \in F \ \ \forall\, i = 0, \cdots, n-1$$

Demostración. Como α algebraico sobre F, y por el CASO 1 anterior,

$$F(\alpha) = \Phi_\alpha(F[x])$$

Entonces todo elemento en $F(\alpha)$ es de la forma $\Phi_\alpha(f) = f(\alpha)$, un polinomio en α con coeficiente en F. Sea el polinomio:

$$p(x) = irr(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

Por definición de $p(x)$ tenemos que $p(\alpha) = 0$, de donde obtenemos

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$$

Usando la ecuación anterior podemos expresar cualquier monomio α^m con $m = n + k$
en términos de potencias de α que son menores que n, por ejemplo:

$$\begin{aligned} \alpha^{n+1} = \alpha\alpha^n &= \alpha(-a_{n-1}\alpha^{n-1} - \cdots - a_0) \\ &= -a_{n-1}\alpha^n - \cdots - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_0) - \cdots - a_0\alpha \end{aligned}$$

Así, si $\beta = f(\alpha)$ es posible expresar a β de la forma requerida

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$

Veamos que dicha expresión es única. Si

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = b'_0 + b'_1\alpha + \cdots + b'_{n-1}\alpha^{n-1}$$

para $b'_i \in F$, entonces

$$(b_0 - b'_0) + (b_1 - b'_1)x + \cdots + (b_{n-1} - b'_{n-1})x^{n-1} = g(x) \in F[x]$$

con $g(\alpha) = 0$ y con $grad(g(x)) < grad(irr(\alpha, F))$. Con $irr(\alpha, F)$ un polinomio distinto de cero y minimal, por tanto, $g(x) = 0$ y así

$$b_i = b'_i \ \ \forall \ \ i = 0, 1, \cdots, n-1.$$

■

Corolario 2.1.4 *Sea F subcampo de E y sea $\alpha \in E$ algebraico sobre F. Si $grad(\alpha, F) = n$, entonces $F(\alpha)$ es un espacio vectorial n-dimensional sobre F, con base $\{1, \alpha, ..., \alpha^{n-1}\}$. Más aún todo elemento $\beta \in F(\alpha)$ es algebraico sobre F y además,*

$$grad(\beta, F) \leqslant grad(\alpha, F).$$

Demostración. Que $F(\alpha)$ es espacio vectorial sobre F con base $\{1, \alpha, ..., \alpha^{n-1}\}$ es por consecuencia directa del teorema 2.1.3. Veamos que para β en $F(\alpha)$ tenemos que β algebraico sobre F y que

$$grad(\beta, F) \leqslant grad(\alpha, F).$$

Consideremos la colección de elementos

$$1, \beta, \beta^2, \cdots, \beta^n$$

tal colección es linealmente dependiente en $F(\alpha)$. Entonces, existen b_i en F tales que:

$$b_0 + b_1\beta + ... + b_n\beta^n = 0$$

con no todas las $b_i = 0$. Tenemos entonces que el polinomio

$$f(x) = b_0 + b_1x + ... + b_nx^n$$

es tal que

$$0 \neq f(x) \in F[x] \ \ y \ \ f(\beta) = 0.$$

Por lo que β es algebraico sobre F y además

$$deg(\beta, F) \leqslant n = deg(\alpha, F).$$

■

Ejemplo 2.1.5

$$p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$$

es un polinomio irreducible sobre $\mathbb{Z}_2$ *pues ni* $\overline{0}$ *ni* $\overline{1}$ *son raíces, y grad* $(p(x)) \leqslant 3$ *(ver el teorema 1.5.1).*
Aplicando el teorema 1.5.18 tenemos que existe un campo de extensión E *de* $\mathbb{Z}_2$ *que contiene algún cero* α *de* $p(x)$. *Por el teorema 2.1.3*

$$\mathbb{Z}_2(\alpha) = \{0 + 0\alpha, 1 + 0\alpha, 0 + 1\alpha \ \ y \ \ 1 + 1\alpha\} = \{0, 1, \alpha, 1 + \alpha\}$$

Hemos obtenido un nuevo campo finito de 4 elementos. Calculemos las tablas de adición y multiplicación para este campo, notemos que para calcular el producto $(1 + \alpha)(1 + \alpha)$ *en* $\mathbb{Z}_2(\alpha)$, *tenemos que* $p(\alpha) = \alpha^2 + \alpha + 1 = 0$, *entonces*

$$\begin{aligned}(1+\alpha)(1+\alpha) &= 1 + 1\cdot\alpha + 1\cdot\alpha + \alpha^2 \\ &= 1 + (1+1)\alpha + \alpha^2 \\ &= 1 + \alpha^2 \quad \textit{pues } 1+1 = 0 \textit{ en } \mathbb{Z}_2 \\ &= 1 - 1 - 1\alpha \quad \textit{pues } 0 = p(\alpha) = \alpha^2 + \alpha + 1 \Rightarrow \alpha^2 = \alpha - 1 \\ &= 1 + \alpha + 1 \quad \textit{pues } -1 = 1 \textit{ en } \mathbb{Z}_2 \\ &= \alpha \quad \textit{pues } 1+1 = 0 \textit{ en } \mathbb{Z}_2\end{aligned}$$

$$\therefore (1+\alpha)(1-\alpha) = \alpha$$

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

2.2. Estensiones finitas.

Definición 2.2.1 *Sea* F *subcampo de* E. *Si* E *es de dimensión finita* n *como espacio vectorial sobre* F, *entonces diremos que* E ***es una extensión finita*** *de grado* n *sobre* F. *Denotaremos por* $[E : F]$ *al grado de* E *sobre* F.

Observación 2.2.2 *Sea F subcampo de E tal que E es una extensión finita sobre F.*

$$[E : F] = 1 \Leftrightarrow E = F.$$

Demostración. ($\Rightarrow$) Dado que $[E : F] = 1$ tenemos que E es un espacio vectorial de dimensión finita sobre F. Por álgebra lineal tenemos que para $\alpha \in E$ tal que $\alpha \neq 0$, $\{\alpha\}$ se puede extender a una base de E sobre F. En particular tomemos $0 \neq 1 \in E$, tenemos que $\{1\}$ se puede extender a una base de E sobre F. Dado que $[E : F] = 1$ entonces $\{1\}$ es una base para E sobre F, así:

$$\begin{aligned} E &= \{\textstyle\sum_{i,finita} a_i 1^{k_i} | a_i \in F\} = \{f(1) | f(x) \in F[x]\} \\ &= F(1) \text{ pues 1 es algebraico sobre F y aplicamos el CASO 1 de la observación 2.1.1} \\ &= F \ \textit{pues} \ 1 \in F. \end{aligned}$$

por tanto

$$E = F.$$

($\Leftarrow$) Ahora consideremos $E = F \Rightarrow [E : F] = 1$. ■

Ejemplo 2.2.3 *Retomando el ejemplo 1.5.19 demostraremos que:*

$$\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}.$$

Demostración. Recordemos que $\mathbb{R}[x]/\langle x^2 + 1\rangle$ es una extensión de $\mathbb{R} = \{r + \langle x^2 + 1\rangle \in \mathbb{R}[x]/\langle x^2 + 1\rangle | r \in \mathbb{R}\}$, tal que el elemento $\alpha = x + \langle x^2 + 1\rangle \in \mathbb{R}[x]/\langle x^2 + 1\rangle$ es un cero del polinomio $x^2 + 1 \in \mathbb{R}[x]$. Tenemos que $\mathbb{C}$ es un campo de extensión de $\mathbb{R}$ (esto es, $\mathbb{R}$ es subcampo de $\mathbb{C}$) y que $i \in \mathbb{C}$ es un elemento algebraico sobre $\mathbb{R}$, pues i es cero de $x^2 + 1 \in \mathbb{R}[x]$.
Por el CASO 1 de la observación 2.1.1 tenemos un isomorfismo

$$\overline{\Phi_i} : \mathbb{R}[x]/\langle x^2 + 1\rangle \longrightarrow \Phi_i(\mathbb{R}[x]) \equiv \mathbb{R}[i] \equiv \mathbb{R}(i),$$

con $\mathbb{R}(i)$ subcampo de $\mathbb{C}$, tal que para $f(x) + \langle x^2 + 1\rangle \in \mathbb{R}[x]/\langle x^2 + 1\rangle$ se tiene

$$\overline{\Phi_i}(f(x) + \langle x^2 + 1\rangle) = \Phi_i(f(x)) = f(i),$$

con $f(i) \in \mathbb{R}(i)$.
Por el teorema 2.1.3 tenemos que una base de $\mathbb{R}(i)$ sobre $\mathbb{R}$ es $\{1, i\}$, entonces:

$$\mathbb{R}(i) = \{a + bi | a, b \in \mathbb{R}\} = \mathbb{C},$$

por tanto tenemos un isomorfismo de anillos

$$\begin{array}{rcl} \overline{\Phi}_i : \mathbb{R}[x]/\langle x^2+1\rangle & \longrightarrow & \mathbb{C} \\ f(x)+\langle x^2+1\rangle & \longmapsto & f(i) \end{array}$$

(Notemos además que si $r+\langle x^2+1\rangle \in \{r+\langle x^2+1\rangle \in \mathbb{R}[x]/\langle x^2+1\rangle | r \in \mathbb{R}\} \cong \mathbb{R}$ entonces $\overline{\Phi}_i(r+\langle x^2+1\rangle) = \Phi_i(r) = r$ y $\overline{\Phi}_i(\alpha) = \overline{\Phi}_i(x+\langle x^2+1\rangle) = \Phi_i(x) = i$). ■

2.3. Extensiones algebraicas.

Definición 2.3.1 *Un campo de extensión E de un campo F, es una* ***extensión algebraica*** *de F si todo elemento en E es algebraico sobre F.*

Teorema 2.3.2 *Sea F subcampo de E, tal que $[E:F] < \infty$, entonces E es una extensión algebraica sobre F.*

Demostración. Sea $\alpha \in E$. Sea $n = [E:F]$. Consideremos la colección

$$1, \alpha, \cdots, \alpha^n \in E$$

Notemos que tal colección no es linealmente independiente en E, por lo que existen elementos a_i en F tales que

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$$

con no todas las a_i iguales a cero. Entonces

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

es tal que $f(x) \neq 0$, $f(x) \in F[x]$ y $f(\alpha) = 0$, por tanto, α es algebraico sobre F. ■

Corolario 2.3.3 *Sea F subcampo de E y $\alpha \in E$, tal que α es algebraico sobre $F \Rightarrow F(\alpha)$ es una extensión algebraica sobre F.*

Demostración. Dado que α es algebraico sobre F, entonces por el corolario 2.1.4 tenemos que $[F(\alpha):F] = grad(\alpha, F) < \infty$. Aplicando el teorema 2.3.2, se tiene que $F(\alpha)$ es una extensión algebraica sobre F. ■

Corolario 2.3.4 *Sea F subcampo de E y $\alpha \in E$. α es algebraico sobre $F \Leftrightarrow F(\alpha)$ es una extensión finita sobre F en E.*

Demostración. ($\Rightarrow$) Inmediato del teorema 2.3.2.
($\Leftarrow$) Es el corolario 2.1.4. ■

Teorema 2.3.5 *Sea F subcampo de E y E subcampo de K, tal que $[E:F]$ y $[K:E]$ son finitos $\Rightarrow$ K es una extensión finita de F y*

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

Más aún si

$$\{\alpha_i\}_{i=1}^{n} \subseteq E,\ \{\beta_j\}_{j=1}^{m} \subseteq K$$

son bases de E sobre F y K sobre E respectivamente, entonces el conjunto de los productos en K

$$\{\alpha_i\beta_j\}_{1\leq i\leq n,\ 1\leq j\leq m}$$

es una base de K sobre F.

Demostración. Sea $\gamma \in K$, entonces γ se puede escribir como

$$\gamma = \sum_{j=1}^{m} b_j\beta_j$$

con b_j elementos de E. Dado que $\{\alpha_i\}_{i=1}^{n}$ es una base de E sobre F tenemos que

$$b_j = \sum_{i=1}^{n} a_{ij}\alpha_i$$

para cada b_j con $j = 1, \cdots, m$, con $a_{ij} \in F\ \forall\ i = 1, \cdots, n$ y $j = 1 \cdots, m$.
Así tenemos que

$$\gamma = \sum_{j=1}^{m}(\sum_{i=1}^{n} a_{ij}\alpha_i)\beta_j = \sum_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m} a_{ij}(\alpha_i\beta_j)$$

por tanto el conjunto $\{\alpha_i\beta_j\}$ genera a K sobre F.
Supongamos que

$$\sum_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m} c_{ij}(\alpha_i\beta_j) = 0 \ \ con\ \ c_{ij}\ en\ F,$$

entonces

$$\sum_{j=1}^{m}\sum_{i=1}^{n}(c_{ij}\alpha_i)\beta_j = 0 \quad con \quad \sum_{i=1}^{n} c_{ij}\alpha_i \ \ en\ \ E\ \ para\ cada\ \ j = 1, \cdots, m$$

Dado que $\{\beta_j\}_{j=1}^m$ es linealmente independiente sobre E, entonces se tiene que:

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0 \ \ para\ cada\ j = 1, \cdots, m$$

Pero por hipótesis el conjunto$\{\alpha_i\}_{i=1}^n$ también es linealmente independiente sobre F, por consiguiente se tiene que $c_{ij} = 0 \ \ \forall\ i, j$, por tanto, $\{\alpha_i\beta_j\}$ es linealmente independiente.

$$Base\ \{\alpha_i\beta_j\} \left\{ \begin{array}{c} K \\ \uparrow \text{Base } \{\beta_j\} \\ E \\ \uparrow \text{Base } \{\alpha_i\} \\ F \end{array} \right.$$

■

Nota 2.3.6 *En el sentido de las bases, el teorema 2.3.5 también es válido cuando las extensiones son de grado infinito, es decir, si $\{\alpha_i\}_{i\in I}$ es base para E sobre F y $\{\beta_j\}_{j\in J}$ es base para K sobre E entonces $\{\alpha_i\beta_j\}_{i\in I,\ j\in J}$ es base para K sobre F.*

Corolario 2.3.7 *Si F_i es un campo para $i = 1, \cdots, n$ y F_{i+1} es una extensión finita para F_i, entonces F_r es una extensión finita de F_1 y además*

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1]$$

Demostración. Usar el teorema 2.3.5 e inducción matemática. ■

Corolario 2.3.8 *Sea F subcampo de E, sea $\alpha \in E$ algebraico sobre F y sea $\beta \in F(\alpha)$, entonces*

$$grad\ (\beta, F) | grad(\alpha, F).$$

Demostración. Dado que $\alpha \in E$ es algebraico sobre F, por el cololario 2.1.4 se tiene que

$$grad\ (\alpha, F) = [F(\alpha) : F] \ \ (que\ es\ finito) \qquad \textbf{(I)}$$

Por otra parte, si α en E es algebraico sobre F, entonces por el corolario 2.4.6, se tiene que $F(\alpha)$ es una extension algebraica sobre F. Dado que

por hipótesis β es un elemento de $F(\alpha)$, entonces por definición $\beta \in E$ es algebraico sobre F. Aplicando el corolario 2.1.4 se tiene que

$$grad\ (\beta, F) = [F(\beta) : F]\ \ (que\ es\ finito) \qquad \textbf{(II)}.$$

Además, dado que $F(\beta)$ es el menor subcampo de E que contiene a F y a β y tenemos que $\beta \in F(\alpha)$ con $F \subseteq F(\alpha)$, concluímos que $F(\beta)$ es un subcampo de $F(\alpha)$.

Notemos también que β es elemento de $F(\alpha)$ con $F(\beta)$ subcampo de $F(\alpha)$ y con β algebraico sobre F. Por lo que β satisface un polinomio con coeficientes en F, lo que implica, que β es cero de un polinomio con coeficientes en $F(\beta)$. Por lo que β esta en $F(\alpha)$, con $F(\beta)$ subcampo de $F(\alpha)$ y con β algebraico sobre $F(\beta)$. Aplicando el corolario 2.3.3 obtenemos que:

$$[F(\alpha) : F(\beta)] < \infty \qquad \textbf{(III)}$$

Por **(I),(II),(III)** y por el teorema 2.3.5 se obtiene,

$$[F(\alpha) : F(\beta)][F(\beta) : F] = [F(\alpha) : F],$$

por tanto,

$$grad(\beta, F) | grad(\alpha, F).$$

■

Ejemplo 2.3.9 *No hay elemento de* $\mathbb{Q}(\sqrt{2})$ *que sea un cero de* $x^3 - 2$.

Demostración. Supongamos que existe β en $\mathbb{Q}(\sqrt{2})$ tal que $\beta^3 - 2 = 0$. Usando el teorema 1.5.6 (criterio de Einstein) con $p = 2$, tenemos que $x^3 - 2$ es irreducible sobre $\mathbb{Q}$ y además es mónico, por lo que,

$$\begin{aligned} grad\ (\beta, \mathbb{Q}) &= grad\ (x^3 - 2) \\ &= 3. \end{aligned}$$

Por otra parte:

$$grad\ (\sqrt{2}, \mathbb{Q}) = grad\ (x^2 - 2) = 2.$$

Por el corolario 2.3.8 se tendría que:

$$grad\ (\beta, \mathbb{Q}) | grad\ (\sqrt{2}, \mathbb{Q}).$$

Pero $3 \not| 2$. Por lo que no existen elementos en $\mathbb{Q}(\sqrt{2})$ que sean ceros del polinomio $x^3 - 2$. ■

Observación 2.3.10 *Sea F subcampo de E y $\alpha_1, \alpha_2 \in E$ algebraicos o no sobre F. Sea $F(\alpha_1, \alpha_2)$ el menor subcampo de E que contiene α_1 y a α_2.*

Entonces

$$F(\alpha_1, \alpha_2) \subseteq (F(\alpha_1))(\alpha_2).$$

pues $(F(\alpha_1))(\alpha_2)$ es un campo que contiene a $F(\alpha_1)$ y a α_2 pero $F(\alpha_1)$ contiene a F y a α_1, por lo que:

$$F(\alpha_1)(\alpha_2) \supseteq F \cup \{\alpha_1\} \cup \{\alpha_2\}$$

Por otra parte también se tiene que $F(\alpha_1) \subseteq F(\alpha_1, \alpha_2)$ pues $F(\alpha_1)$ es el menor subcampo que contiene a F y a α_1

$$\Rightarrow F(\alpha_1) \cup \{\alpha_2\} \subseteq F(\alpha_1, \alpha_2)$$

pues $\alpha_2 \in F(\alpha_1, \alpha_2)$. $\Rightarrow F(\alpha_1)(\alpha_2) \subseteq F(\alpha_1, \alpha_2)$ pues $F(\alpha_1)(\alpha_2)$ es el menor subcampo de E que contiene a $F(\alpha_1)$ y a α_2. Por tanto

$$F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2).$$

Análogamente $F(\alpha_1, \alpha_2) = F(\alpha_2)(\alpha_1)$, por tanto,

$$F(\alpha_1)(\alpha_2) = F(\alpha_1, \alpha_2) = F(\alpha_2)(\alpha_1).$$

De la misma forma para $\alpha_i \in E$ con $i = 1, \cdots, n$ se tiene que

$$F(\alpha_1, \cdots, \alpha_n)$$

es el menor subcampo de E que contiene a $\alpha_1, \cdots, \alpha_n$ y podemos obtener el campo $F(\alpha_1, \cdots, \alpha_n)$ a partir del campo F, agregando a F uno por uno los elementos $\alpha_i \in E$.

Ejemplo 2.3.11 *Consideremos el campo $\mathbb{Q}(\sqrt{(2)})$. Dado que*

$$irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \quad \Rightarrow \quad grad(\sqrt{2}, \mathbb{Q}) = 2.$$

Por el corolario 2.1.4 tenemos que $\{1, \sqrt{2}\}$ es una base para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.
Por otra parte consideremos el elemento $\sqrt{2}+\sqrt{3} \in \mathbb{R}$, calculando obtenemos que

$$irr(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1.$$

(pues $\alpha = \sqrt{2}+\sqrt{3} \Rightarrow \alpha - \sqrt{2} = \sqrt{3} \Rightarrow (\alpha-\sqrt{2})^2 = 3 \Rightarrow \alpha^2 - 2\alpha\sqrt{2} + 2 = 3 \Rightarrow 2\alpha\sqrt{2} = \alpha^2 - 1 \Rightarrow 4\alpha^2 \cdot 2 = (\alpha^2-1)^2 \Rightarrow 8\alpha^2 = \alpha^4 - 2\alpha^2 + 1 \Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0 \Rightarrow \alpha = \sqrt{2}+\sqrt{3}$ *es cero del polinomio* $x^4 - 10x^2 + 1$ *que es mónico e irreducible sobre* $\mathbb{Q}$*). Aplicando el corolario 2.1.4 se tiene que*

$$4 \equiv grad(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}]$$

por lo que $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ *(pues* $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ *implica, por el corolario 2.1.4, que* $\sqrt{2}+\sqrt{3}$ *es algebraico sobre* $\mathbb{Q}$ *tal que por el corolario 2.3.8* $4 \equiv grad(\sqrt{2}+\sqrt{3}, \mathbb{Q}) | grad(\sqrt{2}, \mathbb{Q}) = 2$ *pero* $4 \nmid 2$*!* $\therefore \sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$*). Lo que implica que* $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ *(pues* $\sqrt{3} \in \mathbb{Q}(\sqrt{2}) \Rightarrow \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ *lo cual vimos que no es posible), entonces* $\{1, \sqrt{3}\}$ *es una base para* $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ *sobre* $\mathbb{Q}(\sqrt{2})$ *(pues dado que* $\sqrt{3} \notin \mathbb{Q}(\sqrt{(2)})$ *tenemos que* $irr(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3 \Rightarrow grad(\sqrt{3}, \mathbb{Q}(\sqrt{(2)}) = 2$ *pero por el corolario 2.1.4 el* $grad(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = [\mathbb{Q}(\sqrt{(2)})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \therefore [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$*. Así por el corolario 2.1.4* $\{1, \sqrt{3}\}$ *es base).*
Por el teorema 2.3.5 los productos

$$\{1 \cdot 1, 1 \cdot \sqrt{2}, \sqrt{3} \cdot 1, \sqrt{3}\sqrt{2}\} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\},$$

son una base para $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ *pero por la observación 2.3.10* $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$*, así* $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *es una base para* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *sobre* $\mathbb{Q}$*.*

$$\text{Base } \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} \begin{cases} \mathbb{Q}(\sqrt{2})(\sqrt{3}) \equiv \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \quad \uparrow \text{Base } \{1, \sqrt{3}\} \\ \mathbb{Q}(\sqrt{2}) \\ \quad \uparrow \text{Base } \{1, \sqrt{2}\} \\ \mathbb{Q} \end{cases}$$

Observación 2.3.12 *Notamos que* $F \leqslant E \leqslant K$ *tal que* $[K : F] < \infty \Rightarrow [K : E] < \infty$*, pues sea* $\gamma \in K$

$$\Rightarrow \gamma = \sum_{i=1}^{n} a_i k_i \text{ con } a_i \in F,\ k_i \in K$$

pero notemos que $a_i \in E$ *pues* $F \subseteq E$*. Así* $\{k_1, \cdots, k_n\}$ *genera a* K *sobre* $E \therefore [K : E] < \infty$*.*

Observación 2.3.13 *Tenemos por la observación anterior que*

$$\infty > \left\{ \begin{array}{l} K \\ \uparrow {\scriptstyle <\infty} \\ E \\ \uparrow \\ F \end{array} \right.$$

veamos que esto implica que $[E : F] < \infty$. *Supongamos que* $[E : F] = \infty$. *Sea* $\{\alpha_i\}_{i\in I}$ *una base infinita para* E *sobre* F *y sea* $\{\beta_j\}_{j=1,\cdots,n}$ *una base para* K *sobre* F. *Por la nota 2.3.6* $\Rightarrow \{\alpha_i\beta_j\}_{i\in I, j=1,\cdots,n}$ *es una base para* K *sobre* $F \Rightarrow [K : F] = \infty !\therefore [E : F] < \infty$.

Ejemplo 2.3.14 *Sea* $\sqrt[3]{2}, \sqrt{2} \in \mathbb{R}$. *Notemos que* $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$ *(pues si* $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2})$, *por el corolario 2.3.7 tendríamos que* $grad(\sqrt[3]{2}, \mathbb{Q})|grad(\sqrt{2}, \mathbb{Q})$ *pero* $irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ *que es irreducible sobre* $\mathbb{Q}$ *por Einsenstein para* $p = 2$ *además* $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \Rightarrow grad(\sqrt[3]{2}, \mathbb{Q}) = 3$ *y* $grad(\sqrt{2}, \mathbb{Q}) = 2$ *pero* $3 \nmid 2$ *! ∴* $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2}) \Rightarrow [(\mathbb{Q}(\sqrt{2}))(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] = grad(\sqrt[3]{2}, \mathbb{Q}(\sqrt{2})) = grad(x^3 - 2) = 3$ *(pues* $\sqrt[3]{2}$ *es raíz de* $x^3 - 2$ *con* $x^3 - 2$ *irreducible sobre* $\mathbb{Q}(\sqrt{2})$ *porque* $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$*y las demás raíces de* $x^3 - 2$ *no están en* $\mathbb{R} \supseteq \mathbb{Q}(\sqrt{2})$.
Entonces una base para $\mathbb{Q}(\sqrt{2})$ *sobre* $\mathbb{Q}$ *es* $\{1, \sqrt{2}\}$ *y una base para* $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ *sobre* $\mathbb{Q}(\sqrt{2})$ *es* $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$.

$$\begin{array}{c} \mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) \\ \uparrow {\scriptstyle \text{Base } \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}} \\ \mathbb{Q}(\sqrt{2}) \\ \uparrow {\scriptstyle \text{Base } \{1, \sqrt{2}\}} \\ \mathbb{Q} \end{array}$$

Más aún por el teorema 2.3.5 el conjunto de productos

$$\begin{aligned} \{1 \cdot 1, 1 \cdot \sqrt{2}, \sqrt[3]{2} \cdot 1, \sqrt[3]{2}\sqrt[3]{2}, (\sqrt[3]{2})^2 \cdot 1, (\sqrt[3]{2})^2\sqrt{2}\} &= \{1, 2^{\frac{1}{2}}, 2^{\frac{1}{3}}, 2^{\frac{1}{3}+\frac{1}{2}}, 2^{\frac{2}{3}}, 2^{\frac{2}{3}+\frac{1}{2}}\} \\ &= \{1, 2^{\frac{1}{2}}, 2^{\frac{1}{3}}, 2^{\frac{5}{6}}, 2^{\frac{2}{3}}, 2^{\frac{7}{6}}\} \end{aligned}$$

es una base para $\mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) \equiv \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ *sobre* $\mathbb{Q} \therefore [\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}] = 6$.
Notemos que $\frac{1}{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ *(pues* $\frac{1}{2} \in \mathbb{Q}$*) y* $2^{\frac{7}{6}} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ *pues* $2^{\frac{7}{6}}$

es uno de los elementos de la base de $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ *sobre* $\mathbb{Q}(\sqrt{2}) \Rightarrow \frac{1}{2}(2^{\frac{7}{6}}) \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. *Pero* $\frac{1}{2}(2^{\frac{7}{6}}) = \frac{1}{2}(2 \cdot 2^{\frac{1}{6}}) = 2^{\frac{1}{6}} \therefore 2^{\frac{1}{6}} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ *y notemos que* $2^{\frac{1}{6}}$ *es cero del polinomio* $x^6 - 2 \in \mathbb{Q}[x]$ *el cual es irreducible sobre* $\mathbb{Q}$ *(por el criterio de Einsenstein para* $p = 2$*) entonces*

$$grad(2^{\frac{1}{6}}, \mathbb{Q}) = 6 \ \therefore \ [\mathbb{Q}(2^{\frac{1}{6}}), \mathbb{Q}] = 6.$$

Además

$$\begin{aligned} \mathbb{Q} &\leqslant \mathbb{Q}(2^{\frac{1}{6}}) \\ &\leqslant \mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) \text{ pues } 2^{\frac{1}{6}} \in \mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}). \end{aligned}$$

Por tanto,

$$\infty > \left\{ \begin{array}{c} \mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) \\ \uparrow \\ \mathbb{Q}(2^{\frac{1}{6}}) \\ \infty > \uparrow \\ \mathbb{Q} \end{array} \right. \Longrightarrow \begin{array}{c} \mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) \\ \infty > \uparrow \\ \mathbb{Q}(2^{\frac{1}{6}}) \\ \uparrow \\ \mathbb{Q} \end{array}$$

Por tanto podemos aplicar el teorema 2.3.5

$$\Rightarrow \underbrace{[\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}]}_{\shortparallel} = [\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}(2^{\frac{1}{6}})] \underbrace{[\mathbb{Q}(2^{\frac{1}{6}}) : \mathbb{Q}]}_{\shortparallel}$$

$$6 \qquad\qquad 6$$

$$\Rightarrow 6[\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}(2^{\frac{1}{6}})] = 6 \Rightarrow [\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}(2^{\frac{1}{6}})] = 1$$

$$\Leftrightarrow \mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) = \mathbb{Q}(2^{\frac{1}{6}}) \text{ ésto por la observación 2.2.2.}$$

Nota 2.3.15 *El ejemplo 2.3.14 muestra que es posible que una extensión* $F(\alpha_1, \cdots, \alpha_n)$ *de un campo* F*, en realidad, sea una extensión simple. Aunque* $n > 1$*. A continuación caracterizaremos las extensiones de la forma* $F(\alpha_1, \cdots, \alpha_n)$ *para el caso en que todas las* α_i *son algebraicas sobre* F*.*

Teorema 2.3.16 *Sea* F *subcampo de* E*, tal que* E *es una extensión algebraica de* F*.*
Existe un número finito de elementos $\alpha_1, \alpha_2, \cdots, \alpha_n$*, en* E *tal que* $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ *si y sólo si* $[E : F]$ *es finito.*

Demostración. ($\Rightarrow$) Supongamos que $E = F(\alpha_1, \cdots, \alpha_n)$, con $\alpha_i \in E$.
Dado que E es una extensión algebraica de F, por definición tenemos que α_i es algebraico sobre F. Claramente cada α_i es algebraico sobre todo campo de extensión de F en E. Usando esta observación y el corolario 2.3.3 se tiene que $F(\alpha_1)$ es algebraico sobre F pues $\alpha_1 \in E$ es algebraico sobre F. De la misma manera $F(\alpha_1, \alpha_2) = (F(\alpha_1))(\alpha_2)$ es algebraica sobre $F(\alpha_1)$ pues α_2 en E es algebraico sobre $F(\alpha_1)$.
$F(\alpha_1, \alpha_2, \alpha_3) = (F(\alpha_1, \alpha_2))(\alpha_3)$ es algebraica sobre $F(\alpha_1, \alpha_2)$ pues α_3 en E es algebraico sobre $F(\alpha_1, \alpha_2)$. Continuando de esa forma se llega a que:
$F(\alpha_1, \cdots, \alpha_n) = (F(\alpha_1, \cdots, \alpha_{n-1}))(\alpha_n)$ es algebraica sobre $F(\alpha_1, \cdots, \alpha_{n-1})$ pues α_n en E es algebraica sobre $F(\alpha_1, \cdots, \alpha_n)$.
Por el corolario 2.1.4 tenemos que:
$[F(\alpha_1) : F] < \infty$
$[F(\alpha_1, \alpha_2) : F(\alpha_1)] < \infty$
$[F(\alpha_1, \alpha_2, \alpha_3) : F(\alpha_1, \alpha_2)] < \infty$
$\vdots$
$[F(\alpha_1, \cdots, \alpha_n) : F(\alpha_1, \cdots, \alpha_{n-1})] < \infty$

Usando el corolario 2.3.7 tenemos que

$$E \equiv [F(\alpha_1, \cdots, \alpha_n) : F] = [F(\alpha_1, \cdots, \alpha_n) : F(\alpha_1, \cdots, \alpha_{n-1})] \cdots [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) :$$

por lo que $[E : F]$ es finito.

($\Leftarrow$) Dado que $[E : F] < \infty$ existe una base $\{\alpha_1, \cdots, \alpha_n\} \subseteq E$. Así $E = \{a_1\alpha_1 + \cdots + a_n\alpha_n | a_i \in F\} \subseteq F(\alpha_1, \cdots, \alpha_n)$ donde la contención anterior se tiene porque $F(\alpha_1, \cdots, \alpha_n)$ contiene a F y a $\alpha_1, \cdots, \alpha_n$ y porque $F(\alpha_1, \cdots, \alpha_n)$ es campo.
Por otra parte, también se tiene que $F(\alpha_1, \cdots, \alpha_n) \subseteq E$ pues $F(\alpha_1, \cdots, \alpha_n)$ es el menor campo que contiene a F y a $\alpha_1, \cdots, \alpha_n$. F es subcampo de E por hipótesis y $\{\alpha_1, \cdots, \alpha_n\} \subseteq E$. Por tanto $F(\alpha_1, \cdots, \alpha_n) = E$. ■

2.4. Campos algebraicamente cerrados y cerraduras algebraicas.

Teorema 2.4.1 *Sea E un campo de extensión de F. Entonces*

$$\overline{F_E} = \{\alpha \in E | \ \alpha \text{ es algebraico sobre } F\}$$

es un subcampo de E, el cual llamaremos la ***cerradura algebraica*** *de F en E.*

Demostración. Sean α, β en $\overline{F_E}$. Dado que α, β son elementos de E algebraicos sobre F, entonces por el corolario 2.3.4 $[F(\alpha) : F] < \infty$.
Veamos que $[F(\alpha)(\beta) : F(\alpha)] < \infty$.
Como β en E es algebraico sobre F, se tiene que β es algebraico sobre todo campo de extensión de F en E. Por lo que β es algebraico sobre $F(\alpha)$, entonces por el corolario 2.3.4 $[(F(\alpha))(\beta) : F(\alpha)] < \infty$ y por el corolario 2.3.7 tenemos que:

$$[(F(\alpha))(\beta) : F] = [F(\alpha)(\beta) : F(\alpha)][F(\alpha) : F] < \infty$$

Por tanto $[F(\alpha, \beta) : F] < \infty$. Por el teorema 2.3.2 $F(\alpha, \beta)$ es una extensión algebraica sobre F, por lo que todo elemento de $F(\alpha, \beta)$ es algebraico sobre F y usando la definición de $\overline{F_E}$ tenemos que $F(\alpha, \beta) \subseteq \overline{F_E}$.
Así $\overline{F_E}$ contiene a $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$, y $\frac{\alpha}{\beta}$ para $\beta \neq 0$. Por lo tanto $\overline{F_E}$ es un subcampo de E. ■

Corolario 2.4.2 *Si F es subcampo de E y $\alpha, \beta \in E$ son algebraicos sobre F, entonces $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ y $\frac{\alpha}{\beta}$ si $\beta \neq 0$ son algebraicos sobre F.*

Demostración. Se sigue del teorema 2.4.1. ■

Nota 2.4.3 *Es bien sabido que todo polinomio no constante en $\mathbb{C}[x]$ tiene un cero en $\mathbb{C}$ (Teorema fundamental del Álgebra). La siguente definición generaliza este concepto a otros campos.*

Definición 2.4.4 *Un campo **F es algebraicamente cerrado** si todo polinomio no constante en $F[x]$ tiene algún cero en F.*

Teorema 2.4.5 *Un campo F es algebraicamente cerrado $\Leftrightarrow$ todo polinomio no constante en $F[x]$ se puede factorizar en $F[x]$ en factores lineales.*

Demostración. ($\Rightarrow$) Supongamos que F es algebraicamente cerrado. Sea $f(x)$ en $F[x]$ un polinomio no constante por lo tanto, $f(x)$ tiene un cero α en F. Por el corolario 1.3.2, $x - a$ es un factor de $f(x)$, es decir,

$$f(x) = (x - a)g(x) \text{ para algún } g(x) \text{ en } F[x],$$

con

$$grad\ g(x) = (grad\ f(x)) - 1.$$

Si $g(x)$ es no constante entonces tiene un cero b en F y

$$f(x) = (x - a)(x - b)h(x), \text{ para } h(x) \text{ en } F[x]$$

con

$$grad\ h(x) = (grad\ f(x)) - 2.$$

Continuando este proceso obtenemos una factorización de $f(x)$ en factores lineales.

($\Leftarrow$) Supongamos que todo polinomio no constante tiene una factorización en factores lineales. Si $ax - b$ es un factor lineal de $f(x)$, entonces $\frac{b}{a}$ es un cero de $f(x)$, por tanto, F es algebraicamente cerrado. ■

Corolario 2.4.6 *Sea F un campo algebraicamente cerrado. Si E es una extensión algebraica de F entonces $E = F$, es decir, F no tiene extensiones algebraicas propias.*

Demostración. Sea E una extensión algebraica de F, así F es subcampo de E. Sea α en E. Entonces α es algebraico sobre F. Por el teorema 1.7.1 existe el polinomio irreducible

$$p(x) = irr(\alpha, F).$$

(recordemos que $p(x)$ es irreducible, mónico y $p(\alpha) = 0$).
Por el teorema 2.4.5 todo polinomio no constante en $F[x]$ se factoriza en factores lineales, pero $p(x)$ es irreducible sobre F, por lo que:

$$grad\ p(x) = 1,$$

así

$$p(x) = x - a$$

con a en F. Pero $p(\alpha) = 0$, por lo que

$$\alpha - a = 0.$$

Y finalmente $\alpha = a \in F$, por tanto, $E \subseteq F$ y en consecuencia $E = F$. ■

El siguiente Teorema es fundamental

Teorema 2.4.7 *Todo campo F tiene una cerradura algebraica $\overline{F}$, esto es, una extensión algebraica que es algebraicamente cerrada.*

Demostración. Ver la demostración en [1] pp. 356-357. ■

Damos a continuación algunos ejemplos sin demostración de cerraduras algebraicas de algunos campos.

Ejemplo 2.4.8 $\overline{\mathbb{R}} = \mathbb{C}$

$$\begin{aligned}\overline{\mathbb{Q}} = & \{\alpha \in \mathbb{Q} | \alpha \text{ es cero de un polinomio en } \mathbb{Q}[x]\} \\ \equiv & \{\alpha \in \mathbb{Q} | \alpha \text{ es cero de un polinomio en } \mathbb{Z}[x]\}.\end{aligned}$$

A $\overline{\mathbb{Q}}$ se le llama campo de números algebraicos.

Nota 2.4.9 *Existe una cantidad numerable de campos algebraicamente cerrados en los números complejos que contienen al campo de números algebraicos. Son las cerraduras algebraicas de las extensiones trascendentes de los números racionales (como por ejemplo, de $\mathbb{Q}(\pi)$).*

Ejemplo 2.4.10 *Sea p un primo. $\overline{\mathbb{Z}_p}$ es un campo numerable infinito que contiene una copia del campo de orden p^n para cada entero positivo n (es la unión de dichas copias).*

2.5. Automorfismos de campos.

Sea $\overline{F}$ una cerradura algebraica fija de F.

Definición 2.5.1 *Sea E una extensión algebraica de un campo F. Dos elementos $\alpha, \beta \in E$ se llaman conjugados sobre F cuando*

$$irr(\alpha, F) = irr(\beta, F).$$

Esto es, si α y β son ceros del mismo polinomio irreducible sobre F.

Nota 2.5.2 *La definición anterior generaliza la idea clásica de* ***"números complejos conjugados sobre*** $\mathbb{R}$*"*. *Pues por ejemplo si $a, b \in \mathbb{R}$ y $b \neq 0$, los números complejos conjugados $a+bi$ y $a-bi$ son ambos ceros del polinomio $x^2 - 2ax + a^2 + b^2$, que es un polinomio irreducible en $\mathbb{R}[x]$.*

$$((x-(a+bi))(x-(a-bi)) = x^2 - 2ax + a^2 + b^2).$$

Teorema 2.5.3 *(Isomorfismos básicos de la teoría de campos algebraicos). Sea F un campo y $\alpha, \beta \in \overline{F}$ algebraicos sobre F, con $grad(irr(\alpha, F)) = n$. La función*

$$\Psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$$

definida por:

$$\Psi_{\alpha,\beta}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}$$

para $c_i \in F$, es un isomorfismo de $F(\alpha)$ sobre $F(\beta)$ si y sólo si α y β son conjugados sobre F.

Demostración. ($\Rightarrow$) Supongamos que $\Psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$ es isomorfismo. Sea

$$irr(\alpha, F) = a_0 + a_1 x + \cdots + a_n x^n$$

el polinomio irreducible de α sobre F. Por definición de $irr(\alpha, F)$ tenemos que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Así se tiene que

$$a_0 + a_1\beta + \cdots + a_n\beta^n = \Psi_{\alpha,\beta}(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \Psi_{\alpha,\beta}(0) = 0$$

Por tanto $a_0 + a_1\beta + \cdots + a_n\beta^n = 0$. Por el teorema 1.7.1 obtenemos que:

$$irr(\beta, F) | a_0 + a_1 x + \cdots + a_n x^n = irr(\alpha, F),$$

por tanto,

$$irr(\beta, F) | irr(\alpha, F).$$

Ahora notemos que

$$(\Psi_{\alpha,\beta})^{-1} = \Psi_{\beta,\alpha}.$$

Haciendo un razonamiento análogo tenemos lo siguiente:
Sea

$$irr(\beta, F) = b_0 + b_1 x + \cdots + b_m x^m,$$

entonces

$$b_0 + b_1\beta + \cdots + b_m\beta^m = 0$$

y esto implica que

$$0 = \Psi_{\alpha,\beta}(0) = \Psi_{\alpha,\beta}(b_0 + b_1\beta + \cdots + b_m\beta^m) = b_0 + b_1\alpha + \cdots + b_m\alpha^m$$

entonces

$$irr(\alpha, F) | b_0 + b_1 x + \cdots + b_m x^m = irr(\beta, F),$$

por lo que

$$irr(\alpha, F) | irr(\beta, F)$$

De lo anterior se tiene que:

$$irr(\beta, F) q_1(x) = irr(\alpha, F)$$

para algún $q_1(x)$ en $F[x]$ con $grad\ q_1(x) = 0$ pues $irr(\alpha, F)$ es irreducible.
$\Rightarrow irr(\beta, F)c_1 = irr(\alpha, F)$ donde $q_1(x) = c_1 \in F$.
Análogamente

$$irr(\alpha, F)|irr(\beta, F)$$

y entonces $irr(\alpha, F)c_2 = irr(\beta, F)$ pero notemos que que $c_1 = c_2 = 1$, pues $irr(\beta, F)$ e $irr(\alpha, F)$ son mónicos y por lo tanto:

$$irr(\beta, F) = irr(\alpha, F).$$

($\Leftarrow$) Supongamos que $irr(\alpha, F) = irr(\beta, F) = p(x)$. Dado que α y β son algebraicos sobre F, los homomorfismos evaluación son tales que

$$\Phi_\alpha : F[x] \longrightarrow F[\alpha] \equiv F(\alpha), \quad \Phi_\beta : F[x] \longrightarrow F[\beta] \equiv F(\beta).$$

Por el CASO I de la observación 2.1.1. Por tanto son epimorfismos. También por el CASO I de la observación 2.1.1 tenemos que $\overline{\Phi}_\alpha : F[x]/\langle p(x)\rangle \longrightarrow F(\alpha)$ y $\overline{\Phi}_\beta : F[x]/\langle p(x)\rangle \longrightarrow F(\beta)$ son isomorfismos.

$$Sea \quad \Psi_{\alpha,\beta} := \overline{\Phi}_\beta \circ (\overline{\Phi}_\alpha)^{-1} : F(\alpha) \longrightarrow F(\beta)$$

Entonces $\Psi_{\alpha,\beta}$ es un isomorfismo. Además si tomamos un elemento $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \in F(\alpha)$ entonces:

$$\begin{aligned}\Psi_{\alpha,\beta}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) &= \overline{\Phi}_\beta \circ (\overline{\Phi}_\alpha)^{-1}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) \\ &= \overline{\Phi}_\beta(c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + \langle p(x)\rangle) \\ &= \Phi_\beta(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) \\ &= c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}.\end{aligned}$$

Y así, $\Psi_{\alpha,\beta}$ es justamente el isomorfismo enunciado en el teorema. ■

Corolario 2.5.4 *Sea α algebraico sobre un campo F. Sea $\Psi : F(\alpha) \longrightarrow \overline{F}$ cualquier monomorfismo tal que $\Psi(a) = a\ \forall\ a \in F$ (es decir $\Psi|_F : F \hookrightarrow \overline{F}$ es la inclusión) entonces $\beta = \Psi(\alpha)$ es un conjugado de α sobre F. Recíprocamente, para cada elemento β conjugado sobre F de α existe un único monomorfismo $\Psi_{\alpha,\beta} : F(\alpha) \longrightarrow \overline{F}$ tal que $\Psi_{\alpha,\beta}(\alpha) = \beta$ y $\Psi_{\alpha,\beta}(a) = a\ \forall\ a \in F$.*

Demostración. ($\Rightarrow$) Sea el polinomio

$$irr(\alpha, F) = a_0 + a_1x + \cdots + a_nx^n,$$

entonces se tiene que:

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

$$\begin{aligned} \Rightarrow 0 &= \Psi(0) = \Psi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= a_0 + a_1\Psi(\alpha) + \cdots + a_n\Psi(\alpha)^n \text{ pues } \Psi|_F = F \end{aligned}$$

Sea $\beta = \Psi(\alpha)$, entonces β es cero del polinomio $a_0 + a_1x + \cdots + a_nx^n = irr(\alpha, F)$, así $irr(\alpha, F) = irr(\beta, F)$, por tanto $\beta = \Psi(\alpha)$ es conjugado de α sobre F.

($\Leftarrow$) Sea β conjugado de α sobre F. Entonces el isomorfismo del teorema 2.5.3

$$\Psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta) \leqslant \overline{F}$$

cumple las condiciones deseadas.
Para ver la unicidad, sea

$$\overline{\Psi}_{\alpha,\beta} : F(\alpha) \longrightarrow F,$$

un homomorfismo tal que $\overline{\Psi}_{\alpha,\beta}(a) = a \ \forall \ a \ \in F$ y $\overline{\Psi}_{\alpha,\beta}(\alpha) = \beta$.
Sea

$$\gamma = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \ \in \ F(\alpha),$$

entonces

$$\begin{aligned} \overline{\Psi}_{\alpha,\beta}(\gamma) &= \overline{\Psi}_{\alpha,\beta}(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) \\ &= \overline{\Psi}_{\alpha,\beta}(a_0) + \overline{\Psi}_{\alpha,\beta}(a_1)\overline{\Psi}_{\alpha,\beta}(\alpha) + \cdots + \overline{\Psi}_{\alpha,\beta}(a_{n-1})\overline{\Psi}_{\alpha,\beta}(\alpha^{n-1}) \\ &= a_0 + a_1\overline{\Psi}_{\alpha,\beta}(\alpha) + \cdots + a_{n-1}\overline{\Psi}_{\alpha,\beta}(\alpha^{n-1}) \\ &= a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1} \\ &= \Psi_{\alpha,\beta}(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) \\ &= \Psi_{\alpha,\beta}(\gamma) \end{aligned}$$

Por tanto, se tiene la unicidad. ■

Corolario 2.5.5 *Sea $f(x) \in \mathbb{R}[x]$. Si $f(a + bi) = 0$ para $a + bi \in \mathbb{C}$, donde $a,b \in \mathbb{R}$, entonces también $f(a - bi) = 0$.*

Demostración. Ya probamos en el ejemplo 2.2.3 que $\mathbb{C} = \mathbb{R}(i)$ donde $i^2 = -1$ y claramente $\mathbb{C} = \mathbb{R}(-i)$ (pues por definición $\mathbb{R}(i)$ es el menor subcampo que contiene a $\mathbb{R}$ y a i, esto es, $\mathbb{R}(i)$ contiene a $-i$, por lo que $\mathbb{R}(-i) \subseteq \mathbb{R}(i)$, por otra parte $\mathbb{R}(-i)$ contiene a $\mathbb{R}$ y a $i \Rightarrow \mathbb{R}(i) \subseteq \mathbb{R}(-i) \therefore \mathbb{R}(i) = \mathbb{R}(-i)$). Además notemos que $irr(i, \mathbb{R}) = irr(-i, \mathbb{R}) = x^2+1$ entonces por el teorema 2.5.3 tenemos el isomorfismo

$$\Psi_{i,-i} : \mathbb{C} \equiv \mathbb{R}(i) \longrightarrow \mathbb{R}(-i) \equiv \mathbb{C}$$

tal que

$$\Psi_{i,-i}(a+bi) = a + b(-i) = a - bi.$$

Así

$$\Psi_{i,-i} : \mathbb{C} \longrightarrow \mathbb{C} \text{ es un isomorfismo}$$

tal que

$$\Psi(a+bi) = a - bi.$$

Así, si $f(x) = a_0 + a_1x + \cdots + a_nx^n$ y si para $a, b \in \mathbb{R}$ se tiene que $0 = f(a+b_i)$ entonces

$$0 = f(a+bi) = a_0 + a_1(a+bi) + \cdots + a_n(a+bi)^n$$

y así,

$$\begin{aligned} 0 = \Psi_{i,-i}(f(a+bi)) &= \Psi_{i,-i}(a_0 + a_1(a+bi) + \cdots + a_n(a+bi)^n) \\ &= \Psi_{i,-i}(a_0) + \Psi_{i,-i}(a_1)\Psi_{i,-i}(a+bi) + \cdots + \Psi_{i,-i}(a_n)\Psi_{i,-i}(a+bi)^n \\ &= a_0 + a_1\Psi_{i,-i}(a+bi) + \cdots + a_n\Psi_{i,-i}(a+bi)^n \\ &= a_0 + a_1(a-bi) + \cdots + a_n(a-bi)^n \\ &= f(a-bi). \end{aligned}$$

■

Ejemplo 2.5.6 *Considérese el campo $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Los ceros del polinomio*

$$irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$$

son $\sqrt{2}$ y $-\sqrt{2}$. Entonces se tiene que dichos ceros son conjugados sobre $\mathbb{Q}$. Por el teorema 2.5.3 la transformación

$$\Psi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2})$$

que está dada por

$$\Psi_{\sqrt{2},-\sqrt{2}}(a+b\sqrt{2}) = a + b(-\sqrt{2}) = a - b\sqrt{2}$$

es un isomorfismo de $\mathbb{Q}(\sqrt{2})$ sobre si mismo.

Definición 2.5.7 *Un isomorfismo de un campo sobre si mismo se llama* ***automorfismo*** *del campo.*

Definición 2.5.8 *Sea E un campo. Denotaremos por* ***Aut(E)*** *al conjunto de automorfismos de E.*

Definición 2.5.9 *Sea $\sigma \in Aut(E)$. Decimos que* ***un elemento $a \in E$ queda fijo*** *bajo σ si $\sigma(a) = a$.*

Definición 2.5.10 *Sea $S \subseteq Aut(E)$. Decimos que* ***S deja fijo a un subcampo F de E*** *si para cada $a \in F$ tenemos que $\sigma(a) = a \ \forall \ \sigma \ \in S$.*

Definición 2.5.11 *Sea $S \subseteq Aut(E)$. Definimos el conjunto*

$$E_S = \{a \in E | \sigma(a) = a \ \forall \ \sigma \in S\},$$

es decir, el conjunto de elementos de E que quedan fijos bajo toda $\sigma \in S$.

Definición 2.5.12 *Sea E un campo. Definimos*

$$E^* = E - \{0\}.$$

Afirmación 2.5.13 *E^* es un grupo abeliano bajo la multiplicación.*

■

Afirmación 2.5.14 *Si tenemos un homomorfismo de anillos f entre dos campos E_1 y E_2,*

$$f : E_1 \longrightarrow E_2$$

entonces

$$\overline{f} : E_1^* \longrightarrow E_2^*$$

definido por $\overline{f}(a) = f(a) \ \forall \ a \ \in \ E_1^*$, es homomorfismo de grupos abelianos.

■

Teorema 2.5.15 *Sea $S \subseteq Aut(E)$. Entonces E_S es un subcampo de E.*

Demostración. Sean $a, b \in E_S$, entonces $\sigma(a) = a$ y $\sigma(b) = b \ \forall \ \sigma \in S$.

$$\Rightarrow \begin{cases} \sigma(a \pm b) & = \sigma(a) \pm \sigma(b) & = a \pm b & \forall \ \sigma \in S \\ \sigma(ab) & = \sigma(a)\sigma(b) & = ab & \forall \ \sigma \in S \end{cases}$$

Así se tiene que $a \pm b, ab \in E_S$. Si además $b \neq 0$ con $b \in E_S$ entonces

$$\sigma\left(\frac{a}{b}\right) = \sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}).$$

Pero tenemos que σ es homomorfismo de grupos abelianos por la afirmación 2.5.14 anterior. Así

$$\sigma(a)\sigma(b^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1} = \frac{a}{b} \ \forall \ \sigma \in S$$

$$\therefore \sigma(\frac{a}{b}) = \frac{a}{b} \ \forall \ \sigma \in S$$

además dado que $S \subseteq Aut(E)$, los elementos de S son automorfismos y así,

$$\sigma(0) = 0 \ y \ \sigma(1) = 1 \ \forall \ \sigma \in S,$$

por tanto, E_S es un subcampo de E. ■

Definición 2.5.16 *Llamaremos al campo E_S del teorema 2.5.15, el campo fijo de S. Para un solo automorfismo $\sigma \in Aut(E)$. Llamaremos a $E_{\{\sigma\}}$ el campo fijo de σ y lo denotaremos por E_σ.*

Ejemplo 2.5.17 *Consideremos el automorfismo*

$$\Psi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(-\sqrt{2}) \equiv \mathbb{Q}(\sqrt{2})$$

dado en el ejemplo 2.5.6, tal que,

$$\Psi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2} \ con \ a, b \in \mathbb{Q}.$$

Así

$$\Psi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a + b\sqrt{2} \quad \Leftrightarrow \quad b = 0,$$

por tanto,

$$\mathbb{Q}(\sqrt{2})_{\Psi_{\sqrt{2},-\sqrt{2}}} = \mathbb{Q}.$$

■

Teorema 2.5.18 *Aut(E) es un grupo bajo la composición de automorfismos.*

Demostración. Notemos que $\sigma \in Aut(E)$, por lo que σ es una permutación de E. Así $Aut(E) \subseteq S_E$ donde S_E denota al grupo de permutaciones de E en E.

Basta probar que $Aut(E)$ es un subgrupo de S_E.
Sean $\sigma, \tau \in Aut(E)$ entonces $\sigma\tau \in Aut(E)$ (pues composición de isomorfismos es un isomorfismo). Sea $\sigma \in Aut(E)$ entonces $\sigma^{-1} \in Aut(E)$ (pues el inverso de un ismorfismo es un isomorfismo). Por tanto $Aut(E)$ es subgrupo de S_E y en consecuencia se tiene que $Aut(E)$ es un grupo. ■

Teorema 2.5.19 *Sea E un campo y sea F un subcampo de E. Entonces el conjunto*

$$G(E/F) = \{\sigma \in Aut(E) | \sigma(a) = a \ \forall \ a \in F\}$$

es un subgrupo del grupo $Aut(E)$. Más aún F es un subcampo de

$$E_{G(E/F)} \equiv \{a \in E | \sigma(a) = a \ \forall \ \sigma \in G(E/F)\}.$$

Demostración. Sean $\sigma, \tau \in G(E/F)$ entonces tenemos que

$$\sigma\tau(a) = \sigma(a) = a \ \forall \ a \ \in F,$$

por tanto,

$$\sigma\tau \in G(E/F).$$

Sea $\sigma \in G(E/F)$ entonces $\sigma(a) = a \ \forall \ a \in F$, en consecuencia:

$$a = \sigma^{-1}(\sigma(a)) = \sigma^{-1}(a) \ \forall \ a \in F \Rightarrow \sigma^{-1}(a) = a \ \forall \ a \in F \Rightarrow \sigma^{-1} \in G(E/F).$$

Veamos que F es un subcampo de $E_{G(E/F)}$.
Sea $a \in F$. Sea $\sigma \in G(E/F)$. Así, $\sigma(a) = a$ por definición de $G(E/F)$. Dado que $\sigma \in G(E/F)$ fué tomado arbitrariamente, entonces $\sigma(a) = a$ para todo $\sigma \in G(E/F)$ así $a \in E_{G(E/F)} \therefore F \subseteq E_{G(E/F)}$. Dado que F está contenido en $E_{G(E/F)}$ y $E_{G(E/F)}$ es subcampo de E, tenemos que F es un subcampo de $E_{G(E/F)}$. ■

Definición 2.5.20 *El grupo $G(E/F)$ se llama el* ***grupo de automorfismos de E que deja fijo a F****, o más brevemente, el* ***grupo de E sobre F****.*

El siguiente ejemplo resume la idea de los tres teoremas anteriores.

Ejemplo 2.5.21 *Consideremos el campo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dado que*

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

y aplicando el isomorfismo básico del teorema 2.5.3 se tiene que

$$\Psi_{\sqrt{2},-\sqrt{2}} : (\mathbb{Q}(\sqrt{3}))(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})(-\sqrt{2}) \equiv \mathbb{Q}(\sqrt{3})(\sqrt{2})$$

tal que

$$\Psi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2} \ \ con \ \ a, b \ \in \mathbb{Q}(\sqrt{3}).$$

(dado que $\sqrt{2}$ es conjugado de $-\sqrt{2}$, esto es, $irr(\sqrt{2}, \mathbb{Q}\sqrt{3}) = irr(-\sqrt{2}, \mathbb{Q}\sqrt{3}) = x^2 - 2$ tenemos que en efecto $\Psi_{\sqrt{2},-\sqrt{2}}$ es isomorfismo).

Notemos que $\mathbb{Q}(\sqrt{3})$ *es el campo fijo de* $(\mathbb{Q}\sqrt{3})(\sqrt{2})$ *bajo* $\Psi_{\sqrt{2},-\sqrt{2}}$. *En efecto; por definición se tiene que*

$$(\mathbb{Q}\sqrt{3})(\sqrt{2})_{\Psi_{\sqrt{2},-\sqrt{2}}} = \{a+\sqrt{2}b \in (\mathbb{Q}\sqrt{3})(\sqrt{2}) | \Psi_{\sqrt{2},-\sqrt{2}}(a+\sqrt{2}b) = a+\sqrt{2}b\}.$$

Sea

$$a + \sqrt{2}b \in (\mathbb{Q}\sqrt{3})(\sqrt{2})_{\Psi_{\sqrt{2},-\sqrt{2}}}, \qquad a, b \in \mathbb{Q}(\sqrt{3}),$$

entonces se tiene que:

$$\Psi_{\sqrt{2},-\sqrt{2}}(a + \sqrt{2}b) = a + \sqrt{2}b \quad \Rightarrow \quad a - \sqrt{2}b = a + \sqrt{2}b.$$

y en consecuencia $b = -b$, *pues* $\{1, \sqrt{2}\}$ *es una base para* $\mathbb{Q}(\sqrt{3})(\sqrt{2})$ *sobre* $\mathbb{Q}(\sqrt{3})$. *Así* $b = 0$, *y entonces*

$$a + \sqrt{2}b = a \in \mathbb{Q}(\sqrt{3}),$$

por tanto,

$$(\mathbb{Q}(\sqrt{3}))(\sqrt{2})_{\Psi_{\sqrt{2},-\sqrt{2}}} \quad \subseteq \quad \mathbb{Q}(\sqrt{3}).$$

Por otra parte, claramente $\mathbb{Q}(\sqrt{3})$ *es subcampo de* $(\mathbb{Q}(\sqrt{3}))(\sqrt{2})_{\Psi_{\sqrt{2},-\sqrt{2}}}$ *pues* $a \in \mathbb{Q}(\sqrt{3})$ *implica que*

$$\Psi_{\sqrt{2},-\sqrt{2}}(a) = a \quad \therefore \quad a \in (\mathbb{Q}(\sqrt{3}))(\sqrt{2})_{\Psi_{\sqrt{2},-\sqrt{2}}},$$

por lo que $(\mathbb{Q}(\sqrt{3}))$ *está contenido en* $(\mathbb{Q}(\sqrt{3}))(\sqrt{2})_{\Psi_{\sqrt{2},-\sqrt{2}}}$ *y así*

$$(\mathbb{Q}(\sqrt{3}))(\sqrt{2})_{\Psi_{\sqrt{2},-\sqrt{2}}} = \mathbb{Q}(\sqrt{3}).$$

Análogamente tenemos el automorfismo:

$$\Psi_{\sqrt{3},-\sqrt{3}} : (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) \longrightarrow (\mathbb{Q}(\sqrt{2}))(-\sqrt{3}) \equiv \mathbb{Q}(\sqrt{2})(\sqrt{3})$$

tal que

$$\Psi_{\sqrt{3},-\sqrt{3}}(a + b\sqrt{3}) = a - b\sqrt{3}$$

con

$$\mathbb{Q}(\sqrt{2},\sqrt{3})_{\Psi_{\sqrt{3},-\sqrt{3}}} = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})_{\Psi_{\sqrt{3},-\sqrt{3}}} = \mathbb{Q}(\sqrt{2})$$

como el producto de automorfismos (composición de funciones) es de nuevo un automorfismos, podemos considerar el automorfismo

$$(\Psi_{\sqrt{2},-\sqrt{2}}) \circ (\Psi_{\sqrt{3},-\sqrt{3}}) : \mathbb{Q}(\sqrt{2},\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}).$$

Sean

$$\begin{aligned} Id &= \textit{Automorfismo identidad} \\ \sigma_1 &= \Psi_{\sqrt{2},-\sqrt{2}} \\ \sigma_2 &= \Psi_{\sqrt{3},-\sqrt{3}} \\ \sigma_3 &= (\Psi_{\sqrt{2},-\sqrt{2}}) \circ (\Psi_{\sqrt{3},-\sqrt{3}}) \end{aligned}$$

Por el teorema 2.5.15 se tiene que $Aut(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ *contiene un campo fijo bajo* $\{1,\sigma_1,\sigma_2,\sigma_3\}$ *(esto es* $\mathbb{Q}(\sqrt{2},\sqrt{3})_{\{1,\sigma_1,\sigma_2,\sigma_3\}}$*).*

Notemos que $1 \in \mathbb{Q}(\sqrt{2},\sqrt{3})_{\{1,\sigma_1,\sigma_2,\sigma_3\}}$ *pues todo automorfismo de un campo deja fijo al* 1*, en particular,* $\{1,\sigma_1,\sigma_2,\sigma_3\}$ *deja fijo al* 1 *(como el* 1 *queda fijo, entonces* $\forall\ a \in \mathbb{Q}$ *a se puede escribir como* $a = \frac{b}{c}$ *y* $b = 1 + \cdots + 1$ *ó* $b = -1 \cdots - 1$ *y c de igual forma) por tanto*

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})_{\{1,\sigma_1,\sigma_2,\sigma_3\}}.$$

Ahora veamos que

$$\mathbb{Q} \supseteq \mathbb{Q}(\sqrt{2},\sqrt{3})_{\{1,\sigma_1,\sigma_2,\sigma_3\}}.$$

En el ejemplo 2.3.11 vimos que una base para $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *sobre* $\mathbb{Q}$ *es:*

$$\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}.$$

Dado que

$$\sigma_1(\sqrt{2}) = \Psi_{\sqrt{2},-\sqrt{2}}(\sqrt{2}) = -\sqrt{2},$$

$$\sigma_1(\sqrt{2}\sqrt{3}) = \Psi_{\sqrt{2},-\sqrt{2}}(\sqrt{2}\sqrt{3}) = \Psi_{\sqrt{2},-\sqrt{2}}(\sqrt{2})\Psi_{\sqrt{2},-\sqrt{2}}(\sqrt{3}) = -\sqrt{2}\sqrt{3} = -\sqrt{6},$$

$$\sigma_2(\sqrt{3}) = \Psi_{\sqrt{3},-\sqrt{3}}(\sqrt{3}) = -\sqrt{3},$$

$$\sigma_2(\sqrt{6}) = \Psi_{\sqrt{3},-\sqrt{3}}(\sqrt{2}\sqrt{3}) = \Psi_{\sqrt{3},-\sqrt{3}}(\sqrt{2})\Psi_{\sqrt{3},-\sqrt{3}}(\sqrt{3}) = \sqrt{2}(-\sqrt{3}) = -\sqrt{6}.$$

Sea $x = a_0 \cdot 1 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{2}\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})_{\{1,\sigma_1,\sigma_2,\sigma_3\}}$ *con* $a_0, a_1, a_2, a_3 \in \mathbb{Q}$ *entonces* $\sigma_1(x) = x$*, es decir,*

$$\begin{aligned} x = \sigma_1(x) &= \Psi_{\sqrt{2},-\sqrt{2}}(a_0 \cdot 1 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{2}\sqrt{3}) \\ &= a_0 \cdot 1 + a_1(-\sqrt{2}) + a_2\sqrt{3} + a_3(-\sqrt{6}) \\ &= a_0 \cdot 1 - a_1\sqrt{2} + a_2\sqrt{3} - a_3\sqrt{6}. \end{aligned}$$

Dado que $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ *es una base para* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *sobre* $\mathbb{Q}$*, entonces*

$$a_1 = -a_1,\ a_3 = -a_3 \ \Rightarrow\ a_1 = a_3 = 0. \qquad \textit{(I)}$$

También $\sigma_2(x) = x$, *entonces*

$$\begin{aligned} x = \sigma_2(x) &= \Psi_{\sqrt{3},-\sqrt{3}}(a_0 \cdot 1 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{2}\sqrt{3}) \\ &= a_0 \cdot 1 + a_1\sqrt{2} - a_2\sqrt{3} - a_3\sqrt{6} \end{aligned}$$

Dado que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *es una base para* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *sobre* $\mathbb{Q}$, *entonces*

$$a_2 = -a_2, \quad a_3 = -a_3$$

$$\therefore \quad a_2 = a_3 = 0 \qquad \textbf{(II)}$$

por tanto de **(I)** *y* **(II)** *tenemos que*

$$a_1 = a_2 = a_3 = 0.$$

Lo que implica que $x = a_0 \in \mathbb{Q}$, *concluyendo que*

$$\mathbb{Q}(\sqrt{2}, \sqrt{3})_{\{1,\sigma_1,\sigma_2,\sigma_3\}} = \mathbb{Q}.$$

Sea

$$G = \{1, \sigma_1, \sigma_2, \sigma_3\}$$

Es fácil checar que G *es un grupo bajo la multiplicación de automorfismmos (composición de funciones). Por ejemplo:*

$$\sigma_1\sigma_3 = (\Psi_{\sqrt{2},-\sqrt{2}}) \circ (\Psi_{\sqrt{2},-\sqrt{2}} \circ \Psi_{\sqrt{3},-\sqrt{3}}) = \Psi_{\sqrt{3},-\sqrt{3}} = \sigma_2$$

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

(De hecho el grupo G *es isomorfo al* $4-$*grupo de Klein).*

Veamos que G *es exactamente el grupo* $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. *Recordemos que*

$$G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\sigma \in Aut(\mathbb{Q}(\sqrt{2}, \sqrt{3}))|\sigma(a) = a \ \forall \ a \in \mathbb{Q}\}$$

con $G = \{1, \sigma_1, \sigma_2, \sigma_3\}$. *Claramente, tenemos que* G *es un subgrupo de* $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.

Veamos ahora que $G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \subseteq G$. *Sea* $\tau \in Aut((\mathbb{Q}(\sqrt{2}))(\sqrt{3}))$ *tal que* $\tau(a) = a \ \forall \ a \in \mathbb{Q}$, *esto implica que*

$$\tau : \mathbb{Q}(\sqrt{2})(\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2})(\sqrt{3})$$

es un isomorfismo tal que $\tau|_{\mathbb{Q}}$ *es inclusión. Dado que* $\mathbb{Q}(\sqrt{3})$ *es subcampo* $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ *entonces*

$$\tau|_{\mathbb{Q}(\sqrt{3})} : \mathbb{Q}(\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2})(\sqrt{3})$$

es un monomorfismo que deja fijo a $\mathbb{Q}$ *(*$\tau|_{\mathbb{Q}} = \mathbb{Q}$*). Aplicando el corolario 2.5.4 obtenemos que* $\tau(\sqrt{3})$ *es conjugado de* $\sqrt{3}$, *y así*

$$\tau(\sqrt{3}) = \pm\sqrt{3}.$$

Análogamente se demuestra que

$$\tau(\sqrt{2}) = \pm\sqrt{2}.$$

Dado que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ *es una base para* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *sobre* $\mathbb{Q}$, *tenemos que un automorfismo de* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *que deje fijo a* $\mathbb{Q}$ *está determinado por sus valores en* $\sqrt{2}$ *y* $\sqrt{3}$.
Es fácil checar que $Id, \sigma_1, \sigma_2, \sigma_3$ *son todos los automorfismos posibles de* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *que dejan fijo a* $\mathbb{Q}$. *Más explícitamente tenemos que:*

$$\begin{aligned} Id(\sqrt{2}) &= \sqrt{2} \\ Id(\sqrt{3}) &= \sqrt{3} \end{aligned}$$

$$\begin{aligned} \sigma_1(\sqrt{2}) &= -\sqrt{2} \\ \sigma_1(\sqrt{3}) &= \sqrt{3} \end{aligned}$$

$$\begin{aligned} \sigma_2(\sqrt{2}) &= \sqrt{2} \\ \sigma_2(\sqrt{3}) &= -\sqrt{3} \end{aligned}$$

$$\begin{aligned} \sigma_3(\sqrt{2}) &= -\sqrt{2} \\ \sigma_3(\sqrt{3}) &= -\sqrt{3} \end{aligned}$$

Nota 2.5.22 *En el ejemplo anterior se puede observar que*

$$|G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = 4$$

y

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4.$$

Esto no es coincidencia, sino un ejemplo de una situación bastante general, como veremos más adelante.

2.6. Automorfismo de Frobenius.

Teorema 2.6.1 *(El automorfismo de Frobenius) Sea F un campo finito de característica p. Entonces la función $\sigma_p : F \longrightarrow F$ definida por $\sigma_p(a) = a^p \ \forall \ a \in F$ es un automorfismo que llamaremos* ***el automorfismo de Frobenius de*** *F. Además $F_{\{\sigma_p\}} \cong \mathbb{Z}_p$.*

Demostración. Sea $a, b \in F$. Aplicando el teorema del binomio a $(a+b)^p$ tenemos que:

$$\begin{aligned}
(a+b)^p &= \tbinom{p}{0}a^pb^0 + \tbinom{p}{1}a^{p-1}b^1 + \tbinom{p}{2}a^{p-2}b^2 + \cdots + \tbinom{p}{p-1}ab^{p-1} + \tbinom{p}{p}a^{p-p}b^p) \\
&= a^p + \tfrac{p!}{(p-1)!1!}a^{p-1}b + \tfrac{p!}{(p-2)!2!}a^{p-2}b^2 + \cdots + \tfrac{p!}{(p-(p-1))!(p-1)!}ab^{p-1} + \tfrac{p!}{(p-p)!p!}b^p \\
&= a^p + \underbrace{pa^{p-1}b + (\frac{p(p-1)}{2}\cdot 1)a^{p-2}b^2 + \cdots + (p\cdot 1)ab^{p-1}}_{\shortparallel\ 0} + 1b^p) \\
&= a^p + b^p
\end{aligned}$$

pues todos los sumandos que tienen factor p son iguales a cero. Entonces

$$\begin{aligned}
\sigma_p(a+b) &= (a+b)^p \\
&= a^p + b^p \\
&= \sigma_p(a) + \sigma_p(b).
\end{aligned}$$

y es directo que

$$\begin{aligned}
\sigma_p(ab) &= (ab)^p \\
&= a^pb^p \\
&= \sigma_p(a)\sigma_p(b).
\end{aligned}$$

por tanto, σ_p es homomorfismo de anillos. Veamos que σ_p es uno a uno. Si $\sigma_p(a) = 0$ entonces $a^p = 0$ y así $a \cdots a = 0$ pero como F es campo entonces no tiene divisores de cero, por tanto $a = 0$ y así σ_p es uno a uno.

Verificaremos que σ_p es sobre.
F es finito, digamos $F = \{0, 1, a_1, \cdots, a_n\}$. Consideremos

$$\sigma_p(0), \sigma_p(1), \sigma_p(a_1), \cdots \sigma_p(a_n)$$

como tenemos que σ_p es inyectiva, todos los elementos de la colección anterior son distintos, por lo que $\{\sigma_p(0), \sigma_p(1), \sigma_p(a_1), \cdots \sigma_p(a_n)\}$ tiene la misma

cantidad de elementos que F y con esto aseguramos que σ_p es sobre.
Ahora veremos que $F_{\{\sigma_p\}} \cong \mathbb{Z}_p$.

$$\begin{aligned} F_{\{\sigma_p\}} &= \{c \in F | \sigma_p(c) = 0\} \\ &= \{c \in F | \sigma_p(c) - c = 0\} \\ &= \{c \in F | c^p - c = 0\} \\ &= \{c \in F | c \text{ es cero de } x^p - x\}. \qquad \textbf{(I)} \end{aligned}$$

Por otra parte tenemos por el teorema 1.2.14 que cuando p es un número primo, se tiene que F contiene una copia salvo isomorfismos de $\mathbb{Z}_p$, pues F es de caracaterística p.
Sea $c \in \mathbb{Z}_p \subseteq F$, se tiene que $\sigma_p(c) = c^p = c$ (por el teorema de Fermat que afirma que $a^p \equiv a(mod\ p)\ \forall\ a \in \mathbb{Z}$ y cualquier primo p), por tanto, $\sigma_p(c) = c\ \forall\ c \in \mathbb{Z}_p \subseteq F$, por tanto, el polinomio $x^p - x \in F[x]$ tiene p ceros en F, esto es, todos los elementos de $\mathbb{Z}_p$. Pero el corolario 1.3.3 afirma que un polinomio de grado n sobre un campo tiene a lo más n ceros en el campo. Así los los ceros de $x^p - x \in F[x]$ en F son exactamente los elementos de $\mathbb{Z}_p$, por ésto y por **(I)** se tiene que

$$F_{\{\sigma_p\}} \cong \mathbb{Z}_p.$$

■

2.7. El teorema de extensión de isomorfismos.

Teorema 2.7.1 *(Extensión de isomorfismos).*
Sea F un subcampo de E y sea $\sigma : F \longrightarrow F'$ un isomorfismo de anillos. Con E extensión algebraica de F y sea $\overline{F'}$ una cerradura algebraica de F', entonces existe un monomorfismo

$$\tau : E \longrightarrow \overline{F'}$$

que extiende a σ, es decir

$$\tau(a) = \sigma(a)\ \forall\ a \in F.$$

$$\begin{array}{ccc} E & \overset{\tau}{\rightarrowtail} & \overline{F'} \\ \uparrow & & \uparrow \\ F & \underset{\cong}{\xrightarrow{\sigma}} & F' \end{array} \qquad \textbf{(I)}$$

Demostración. Ver los detalles de la demostración en [1] pp. 384-385. ■

Corolario 2.7.2 *Sea E una extensión algebraica de F y subcampo de $\overline{F}$. Sean $\alpha, \beta \in E$ conjugados sobre F y sea $\Psi_{\alpha,\beta}$ el isomorfismo básico dado por el teorema 2.5.3,*

$$\Psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$$

entonces $\Psi_{\alpha,\beta}$ puede extenderse a un monomorfismo

$$\overline{\Psi}_{\alpha,\beta} : E \rightarrowtail \overline{F}.$$

Demostración. Basta demostrar que $\overline{F}$ es una cerradura algebraica de $F(\beta)$.
Dado que $\overline{F}$ es algebraicamente cerrado sólo resta demostrar que $F(\beta) \subseteq \overline{F}$ y que $\overline{F}$ es extensión algebraica de $F(\beta)$:
Dado que β es algebraico sobre $F \Rightarrow \beta$ es cero de algún polinomio en $F[x]$, dado que $F \subseteq \overline{F}$ tenemos que $F[x] \subseteq \overline{F}[x]$ así β es cero de algún polinomio en $\overline{F}[x]$ y por tanto β es algebraico sobre $\overline{F}$.
$\Rightarrow \overline{F}(\beta)$ es una extensión algebraica sobre $\overline{F}$, entonces por el corolario 2.4.6

$$\overline{F}(\beta) = \overline{F}.$$

Por otra parte $F \subseteq \overline{F} \Rightarrow F(\beta) \subseteq \overline{F}(\beta) \therefore F(\beta) \subseteq \overline{F}$.
Veamos que $\overline{F}$ es una extensión algebraica de $F(\beta)$:
Dado que $\overline{F}$ es extensión algebraica sobre $F \Rightarrow \overline{F}$ es extensión algebraica sobre cualquier campo E tal que $F \leqslant E \leqslant \overline{F}$. Tomando $E = F(\beta)$ tenemos que $\overline{F}$ es extensión algebraica sobre $F(\beta)$.

$$\begin{array}{ccc} E & \rightarrowtail & \overline{F} \\ \uparrow & & \uparrow \\ F(\alpha) & \xrightarrow[\cong]{\Psi_{\alpha,\beta}} & F(\beta) \end{array}$$

■

Corolario 2.7.3 *Sean $\overline{F}$ y $(\overline{F})'$ dos cerraduras algebraicas de F. Entonces $\overline{F}$ es isomorfa a $(\overline{F})'$ bajo un isomorfismo que deja fijo a cada elemento de F.*

Demostración. Por el teorema 2.7.1 tenemos una extensión τ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \overline{F} & \xrightarrow{\tau} & (\overline{F})' \\ \uparrow & & \uparrow \\ F & = & F \end{array} \qquad \textbf{(I)}$$

y además $\tau : \overline{F} \longrightarrow \tau(\overline{F}) \leqslant (\overline{F})'$ es un isomorfismo. Consideremos el isomorfismo

$$\tau^{-1} : \tau(\overline{F}) \longrightarrow \overline{F}$$

aplicando de nuevo el teorema 2.7.1 a τ^{-1} tenemos una extensión $\overline{\tau^{-1}}$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} (\overline{F})' & \xrightarrow{\overline{\tau^{-1}}} & \overline{F} \\ \uparrow & & \uparrow \\ \tau(\overline{F}) & \underset{\cong}{\xrightarrow{\tau^{-1}}} & \overline{F} \end{array} \qquad \textbf{(II)}$$

Dado que τ^{-1} es isomorfismo entonces τ^{-1} es sobreyectiva y como **(II)** conmuta entonces se tiene que $\overline{\tau^{-1}}$ es sobreyectiva y por tanto tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} \overline{F} & \underset{\cong}{\xrightarrow{(\overline{\tau^{-1}})^{-1}}} & (\overline{F})' \\ \uparrow & & \uparrow \\ \overline{F} & \underset{\cong}{\xrightarrow{\tau}} & \tau(\overline{F}) \end{array} \qquad \textbf{(III)}$$

Sea $\Psi = (\overline{\tau^{-1}})^{-1}$. Pegando los diagramas **(I)** y **(III)** se obtiene el diagrama conmutativo

$$\begin{array}{ccc} \overline{F} & \underset{\cong}{\xrightarrow{\Psi}} & (\overline{F})' \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i'} \\ F & = & F \end{array} \qquad \textbf{(IV)}$$

Sea $a \in F. \Rightarrow \Psi(a) = \Psi \circ i(a) = i' \circ Id(a) = i(a) = a$

Por tanto

$$\Psi : \overline{F} \longrightarrow (\overline{F})'$$

es un isomorfismo tal que

$$\Psi(a) = a \; \forall \; a \in F.$$

■

2.8. Índice de un campo de extensión.

Teorema 2.8.1 *Sea F subcampo de E tal que $[E:F] < \infty$. Sea $\sigma : F \longrightarrow F'$ un isomorfismo de F sobre un campo F' y sea $\overline{F'}$ una cerradura algebraica de F'. Entonces el número de extensiones de σ a un monomorfismo $\tau : E \rightarrowtail \overline{F'}$ $(t.q\ \tau|_F = \sigma)$ es finito e independiente de F', $\overline{F'}$ y σ. Esto es, el número de extensiones está completamente determinado por los campos E y F, es intrínseco a ellos.*

$$\begin{array}{ccc} E & \overset{\tau}{\rightarrowtail} & \overline{F'} \\ \uparrow & & \uparrow \\ F & \underset{\cong}{\xrightarrow{\sigma}} & F' \end{array}$$

(dicho de otra forma, el número de extensiones τ del diagrama del teorema 2.7.1 es siempre el mismo independientemente de $F', \overline{F'}$ y σ.)

Demostración. Sean $\sigma_1 : F \longrightarrow F_1'$, $\sigma_2 : F \longrightarrow F_2'$ dos isomorfismos y sean $\overline{F'}_1$ y $\overline{F'}_2$ las cerraduras algebraicas de F_1' y F_2' respectivamente. Afirmamos que existe un isomorfismo

$$\lambda : \overline{F'}_1 \longrightarrow \overline{F'}_2$$

tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \overline{F'}_1 & \underset{\cong}{\xrightarrow{\lambda}} & \overline{F'}_2 \\ \uparrow & & \uparrow \\ F_1' & \underset{\cong}{\xleftarrow{\sigma_1^{-1}}} F \underset{\cong}{\xrightarrow{\sigma_2}} & F_2' \end{array}$$

En efecto; por el teorema 2.7.1 existe:

$$\delta : \overline{F'}_1 \rightarrowtail \overline{F'}_2$$

tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \overline{F'}_1 & \overset{\delta}{\rightarrowtail} & \overline{F'}_2 \\ \uparrow & & \uparrow \\ F_1' & \underset{\cong}{\xrightarrow{\sigma_2\sigma_1^{-1}}} & F_2' \end{array} \qquad \textbf{(I)}$$

Ahora aplicaremos la idea de la prueba del corolario 2.7.3 para construir la λ requerida.

$$\Rightarrow \delta : \overline{F'}_1 \to \delta(\overline{F'}_1) \subseteq \overline{F'}_2 \ \textit{es un isomorfismo.}$$

Consideremos el isomorfismo

$$\delta^{-1} : \delta(\overline{F'}_1) \longrightarrow \overline{F'}_1.$$

Aplicando de nuevo el teorema 2.7.1 tenemos que existe $\overline{\delta^{-1}}$, tal que el siguiente disgrama conmuta:

$$\begin{array}{ccc} \overline{F'}_2 & \xrightarrow{\overline{\delta^{-1}}} & \overline{F'}_1 \\ \uparrow & & \| \\ \delta(\overline{F'}_1) & \xrightarrow[\cong]{\delta^{-1}} & F'_1 \end{array} \qquad \textbf{(II)}$$

Dado que δ^{-1} es isomorfismo, entonces δ^{-1} es epimorfismo y el diagrama **(II)** conmuta y entonces $\overline{\delta^{-1}}$ es epimorfismo, por tanto tenemos el siguiente diagrama conmutativo

$$\textbf{(III)} \qquad \begin{array}{ccc} \overline{F'}_2 & \xrightarrow[\cong]{\overline{\delta^{-1}}} & \overline{F'}_1 \\ \uparrow & & \| \\ \delta(\overline{F'}_1) & \xrightarrow[\cong]{\delta^{-1}} & \overline{F'}_1 \end{array}$$

que a su vez induce el diagrama conmutativo siguiente

$$\begin{array}{ccc} \overline{F'}_1 & \xrightarrow[\cong]{(\overline{\delta^{-1}})^{-1}} & \overline{F'}_2 \\ \uparrow & & \uparrow \\ \overline{F'}_1 & \xrightarrow[\cong]{\delta} & \delta(\overline{F'}_1) \end{array} \qquad \textbf{(IV)}$$

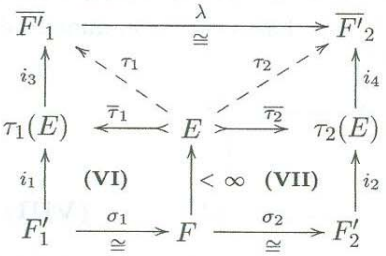
Haciendo $\lambda = (\overline{\delta^{-1}})^{-1}$ y pegando los diagramas **(I)** y **(IV)** obtenemos el diagrama conmutativo siguente

$$\begin{array}{ccc} \overline{F'}_1 & \xrightarrow[\cong]{\lambda} & \overline{F'}_2 \\ \uparrow & & \uparrow \\ F'_1 & \xrightarrow[\cong]{\sigma_2\sigma_1^{-1}} & F'_2 \end{array} \qquad \textbf{(V)}$$

Entonces se tiene que λ es isomorfismo,

$$\lambda : \overline{F'}_1 \longrightarrow F_2 \quad y \quad \lambda|_{F'_1} = \sigma_2\sigma_1^{-1}.$$

Así resulta el siguiente diagrama:



Con referencia al diagrama anterior, por cada monomorfismo $\tau_1 : E \longrightarrow \overline{F'}_1$ que extiende a σ_1, se obtiene un monomorfismo $\tau_2 : E \longrightarrow \overline{F'}_2$ definiendo $\tau_2 = \lambda\tau_1 : E \longrightarrow \overline{F'}_2$.
Notemos que si $a \in F$, entonces,

$$\begin{aligned}
\tau_2(a) = \lambda\tau_1(a) &= \lambda(\tau_1 \circ i)(a) \\
&= \lambda(i_3 \circ i_1\sigma_1)(a) \qquad \textit{pues } \textbf{(VI)} \textit{ conmuta} \\
&= (\lambda i_3 \circ i_1) \circ \sigma_1(a) \\
&= (\lambda|_{F'_1}) \circ \sigma_1(a) \\
&= (\sigma_2 \circ \sigma_1^{-1})(\sigma_1(a)) \\
&= \sigma_2(a).
\end{aligned}$$

$$\therefore \ \tau_2|_F = \sigma_2.$$

Así por cada monomorfismo $\tau_1 : E \rightarrowtail \overline{F'}_1$ que extiende a σ_1 obtenemos un monomorfismo $\tau_2 : E \rightarrowtail \overline{F'}_2$ que extiende a σ_2 definiendo a τ_2 como

$$\tau_2 := \lambda\tau_1 : E \longrightarrow \overline{F'}_2.$$

Análogamente para cada monomorfismo $\tau_2 : E \rightarrowtail \overline{F'}_2$ que extiende a σ_2 podemos obtener un monomorfismo $\tau_1 : E \rightarrowtail \overline{F'}_1$ que extiende a σ_1, definiendo a τ_1 como

$$\tau_1 := \lambda^{-1}\tau_2 : E \longrightarrow \overline{F'}_1.$$

Así tenemos una biyección φ entre el conjunto de monomorfismos $\tau : E \rightarrowtail \overline{F'_1}$ que extienden a σ_1 y el conjunto de monomorfismos $\tau : E \rightarrowtail \overline{F'_2}$ que extienden a σ_2, definida por

$$\varphi(\tau_1) = \lambda\tau_1$$

$$\varphi^{-1}(\tau_2) = \lambda^{-1}\tau_2$$

es claro que $\varphi \circ \varphi^{-1} = Id$ y $\varphi^{-1} \circ \varphi = Id \therefore \varphi$ es biyección.

Veamos que el número de extensiones τ es finito.

Dado que ya probamos que el número de extensiones τ que extiende a σ es independiente de $F', \overline{F'}$ y σ, basta contar el número de extensiones de un isomorfismo $\sigma : F \longrightarrow F'$.

$$\begin{array}{ccc} E \subseteq \overline{F} & \overset{\tau}{\rightarrowtail} & \overline{F'} \\ \uparrow & & \uparrow \\ F & \underset{\cong}{\overset{\sigma}{\longrightarrow}} & F' \end{array} \qquad \textbf{(VIII)}$$

Por hipótesis $[E : F] < \infty$ (así, por el teorema 2.3.2 E es una extensión algebraica de F). Aplicando el teorema 2.3.16 tenemos que existe un número finito de elementos $\alpha_1, \cdots, \alpha_n \in E$ tales que $E = F(\alpha_1, \cdots, \alpha_n)$.
Notemos ahora que dado $\alpha \in E$ tenemos que si

$$irr(\alpha, F) = a_0 + a_1 x + \cdots + a_n x^n \in F[x],$$

entonces

$$irr(\tau(\alpha), F') = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in F'[x]$$

En efecto; pues el diagrama **(VIII)** induce al diagrama conmutativo **(IX)**.

$$\begin{array}{ccc} \overline{F} & \overset{\tau}{\rightarrowtail} & \overline{F'} \\ \uparrow & & \uparrow \\ F & \underset{\cong}{\overset{\sigma}{\longrightarrow}} & F' \end{array} \qquad \textbf{(VIII)}$$

$$\Longrightarrow \qquad \begin{array}{ccc} \overline{F}[x] & \overset{\overline{\tau}}{\rightarrowtail} & \overline{F'}[x] \\ \uparrow & & \uparrow \\ F[x] & \underset{\cong}{\overset{\overline{\sigma}}{\longrightarrow}} & F'[x] \end{array} \qquad \textbf{(IX)}$$

así,

$$\begin{aligned} \overline{\sigma}(irr(\alpha, F)) &= \overline{\sigma}(a_0 + a_1 x + \cdots + a_n x^n) \\ &= \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in F'[x] \end{aligned}$$

Dado que $\overline{\sigma}$ es isomorfismo $\Rightarrow \overline{\sigma}(irr(\alpha, F))$ es irreducible sobre F', además $a_n = 1 \Rightarrow \sigma(a_n) = 1$.
También,

$$\begin{aligned} &\sigma(a_0) + \sigma(a_1)(\tau(\alpha)) + \cdots + \sigma(a_n)(\tau(\alpha))^n \\ &= \tau(a_0) + \tau(a_1)\tau(\alpha) + \cdots + \tau(a_n)(\tau(\alpha))^n \ pues\ \tau|_F = \sigma \\ &= \tau(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \tau(0) \\ &= 0 \in F' \end{aligned}$$

$$\therefore \quad irr(\tau(\alpha), F') = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in F'[x] \qquad \textbf{(X)}$$

Tenemos la siguiente torre de campos de extensiones finitas

$$\begin{array}{c} F(\alpha_1, \cdots, \alpha_n) = E \\ \uparrow {<}\infty \\ F(\alpha_1, \cdots, \alpha_{n-1}) \\ \uparrow {<}\infty \\ \vdots \\ \uparrow {<}\infty \\ F(\alpha_1, \alpha_2) = (F(\alpha_1))(\alpha_2) \\ \uparrow {<}\infty \\ F(\alpha_1) \\ \uparrow {<}\infty \\ F \end{array}$$

(son finitas pues $\alpha_1, \alpha_2, \cdots, \alpha_n$ en E son algebraicos sobre F, en particular son algebraicos sobre cualquier extensión de F. Así tenemos que cada extensión es simple y algebraica sobre la anterior, entonces cada extensión es finita).
Por el corolario 2.3.7 una base para $F(\alpha_1, \cdots, \alpha_n)$ sobre F son todos los productos de las bases para $F(\alpha_1, \cdots, \alpha_i)$ sobre $F(\alpha_1, \cdots, \alpha_{i-1})$ $\forall\, i = 1, \cdots, n$, la cual es finita y a su vez por el teorema 2.1.3 una base para $F(\alpha_1, \cdots, \alpha_i)$ sobre $F(\alpha_1, \cdots, \alpha_{i-1})$ es de la forma $\{1, \alpha_i^1, \cdots, \alpha_i^{n_i - 1}\}$ que es finita.
Así una base finita para $F(\alpha_1, \cdots, \alpha_n)$ sobre F está dada por un conjunto finito de productos de potencias de las α_i con $i = 1, \cdots, n$.
Dado que $\tau|_F = \sigma \Rightarrow \tau : E = F(\alpha_1, \cdots, \alpha_n) \longrightarrow \overline{F'}$ está determinado por los valores $\tau(\alpha_i)$ para $i = 1, \cdots, n$, pero por la afirmación **(X)** anterior

$$irr(\alpha_i, F) = a_{i_0} + a_{i_1}x + \cdots + a_{i_n}x^{n_i}$$

$$\Rightarrow irr(\tau(\alpha_i), F') = \sigma(a_{i_0}) + \sigma(a_{i_1})x + \cdots + \sigma(a_{i_n})x^{n_i}$$

para cada $i = 1, \cdots, n$. Pero por el corolario 1.3.3, el polinomio $irr(\tau(\alpha_i), F')$ tiene a lo mas n_i raíces en cualquier campo de extensión y $\tau(\alpha_i)$ debe ser

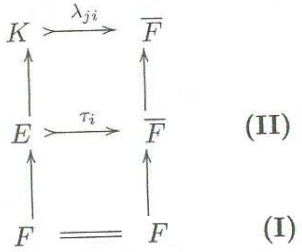
una raíz.
Así para cada $i = 1, \cdots, n$, $\tau(\alpha_i)$ solo puede tomar un número finito de valores y por tanto, el número de extensiones τ es finito. ■

Definición 2.8.2 *Sea E es una extensión finita de un campo F. El número de monomorfismos de E en $\overline{F}$ que dejan fijo a F se llama el* ***índice $\{E:F\}$ de E sobre F.***

Corolario 2.8.3 *Si F es subcampo de E y E es subcampo de K, donde K es un campo de extensión finita del campo F con $[K:F] < \infty$, entonces*

$$\{K:F\} = \{K:E\}\{E:F\}.$$

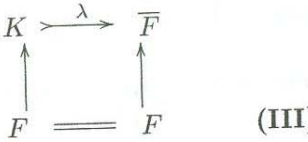
(Notemos que en la prueba de este corolario no es necesario suponer que $[E:F] < \infty$ ni que $[K:F] < \infty$.)
Demostración. Consideremos el siguiente diagrama



(II)

(I)

y el diagrama



(III)

Por el teorema 2.8.1 por cada uno de los $\{E:F\}$ monomorfismos $\tau_i : E \longrightarrow \overline{F}$ que dejan fijo F, se tienen $\{K:E\}$ extensiones $\lambda_{ji} : K \longrightarrow \overline{F}$ tales que, $\lambda_{ji}|_E = \tau_i$

$$\Rightarrow \{K:F\} \geqslant \{K:E\}\{E:F\}.$$

pero notemos que cualquier monomorfismo $\lambda : K \longrightarrow \overline{F}$ que deja fijo a F (es decir, tal que **(III)** conmuta), es una extensión del monomorfismo $\lambda|_E : E \longrightarrow \overline{F}$ que deja fijo a F

$$\therefore \{K:F\} = \{K:E\}\{E:F\}.$$

■

Afirmación 2.8.4 *Más adelante demostraremos que a menos de que F sea un campo infinito de característica $p \neq 0$ siempre tendremos que*

$$[E : F] = \{E : F\}.$$

para todo campo E tal que $[E : F] < \infty$.

Afirmación 2.8.5 *Para el caso $E = F(\alpha)$, las $\{F(\alpha) : F\}$ extensiones de la tranformación identidad*

$$Id : F \longrightarrow F$$

a transformaciones de $F(\alpha)$ en $\overline{F}$, están dadas por los isomorfismos básicos $\Psi_{\alpha,\beta}$ para cada conjugado β en $\overline{F}$ de α sobre F. Así, si $irr(\alpha, F)$ tiene n ceros distintos en $\overline{F}$, tendremos que $\{E : F\} = n$ (para $E = F(\alpha)$).

Afirmación 2.8.6 *Mostraremos también que a menos que F sea infinito y de característica $p \neq 0$ el número de ceros distintos de $irr(\alpha, F)$ es $grad(\alpha, F) = [F(\alpha) : F]$.*

Observación 2.8.7 *Dado que por definición $G(E/F) = \{\sigma \in Aut(E) | \sigma(a) = a \ \forall \ a \in F\}$ tenemos que $\{E : F\} = |G(E/F)|$ en algunos casos (puede suceder que $\tau(E) \neq E$ y $\therefore \tau \notin Aut(E)$. Más adelante veremos en que casos).*

Ejemplo 2.8.8 *Sea $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $F = \mathbb{Q}$. Vimos en el ejemplo 2.5.21 que*

$$|G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = 4.$$

Además como $\mathbb{Q}$ es de característica cero y $[E : F] = 4$, por la afirmación 2.8.4 se tiene que $\{E : F\} = [E : F] = 4$ y así

$$|G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = \{E : F\}.$$

Por otra parte,

$$sea \quad \sigma \in G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma \in Aut(\mathbb{Q}(\sqrt{2})) | \sigma(a) = a \ \forall \ a \in \mathbb{Q}\}$$

$$\Rightarrow \sigma : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}) \ es \ isomorfismo \ con \ \sigma|_{\mathbb{Q}} = inclusión.$$

Por el corolario 2.5.4 $\sigma(\sqrt{2})$ debe ser conjugado a $\sqrt{2}$ sobre $\mathbb{Q}$. Dado que $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ tenemos que $\sigma(\sqrt{2}) = \pm\sqrt{2}$ y no hay más posibilidades,

$$\therefore |G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2.$$

Además, por la afirmación 2.8.4

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

Por otra parte, sea

$$\sigma \in G(\mathbb{Q}(\sqrt{2})(\sqrt{3})/\mathbb{Q}(\sqrt{2})) = \{\sigma \in Aut(\mathbb{Q}(\sqrt{2})(\sqrt{3}))|\sigma(a) = a \; \forall \; a \in \mathbb{Q}(\sqrt{2})\}$$

$$\Rightarrow \sigma : \mathbb{Q}(\sqrt{2})(\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2})(\sqrt{3}) \text{ es isomorfismo y } \sigma|_{\mathbb{Q}(\sqrt{2})} = \text{inclusión.}$$

Por el corolario 2.5.4 $\sigma(\sqrt{3})$ *es conjugado a* $\sqrt{3}$ *sobre* $\mathbb{Q}(\sqrt{2})$. *Dado que demostramos anteriormente que*

$$irr(\mathbb{Q}(\sqrt{2})(\sqrt{3}), \mathbb{Q}(\sqrt{2})) = x^2 - 3$$

$\Rightarrow \sigma(\sqrt{3}) = \pm\sqrt{3}$ *y no hay más posibilidades.*

$$\Rightarrow |G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2}))| = 2.$$

Además,

$$\{E : \mathbb{Q}(\sqrt{2})\} = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2.$$

En conclusión,

$$\{E : F\} = 4 \; , \; \{E : \mathbb{Q}(\sqrt{2})\} = 2 \; y \; \{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = 2$$

con $4 = (2)(2)$ *lo que confirma el teorema 2.8.1.*

Observación 2.8.9 *Sea* E *una extensión algebraica de* F *tal que para cualquier extensión* $\tau : E \rightarrowtail \overline{F}$ *tal que* $\tau(a) = a \; \forall \; a \in F$ *se cumple que* $\tau \in Aut(E)$. *(Es decir,* E *es una extensión algebraica de* F *tal que para cualquier* τ *tal que el siguiente diagrama conmuta*

$$\begin{array}{ccc} E & \overset{\tau}{\rightarrowtail} & \overline{F} \\ {\scriptstyle alg}\uparrow & & \uparrow \\ F & = & F \end{array}$$

se cumple que $\tau \in Aut(E)$.*)*
Si $\alpha \in E$ *y* $\beta \in \overline{F}$ *son tales que*

$$irr(\alpha, F) = irr(\beta, F)$$

entonces $\beta \in E$.

Demostración. Por el teorema 2.5.3 tenemos que si

$$irr(\alpha, F) = irr(\beta, F)$$

entonces existe un isomorfismo

$$\Psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$$

tal que $\Psi_{\alpha,\beta}(a) = a \ \forall \ a \ \in F$, es decir, tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} F(\alpha) & \xrightarrow[\cong]{\Psi_{\alpha,\beta}} & F(\beta) \\ \uparrow & & \uparrow \\ F & = & F \end{array} \qquad \textbf{(I)}$$

Por el corolario 2.7.2 $\Psi_{\alpha,\beta}$ tiene una extensión $\overline{\Psi_{\alpha,\beta}}$ a todo E, esto es, tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} E & \xrightarrow{\overline{\Psi_{\alpha,\beta}}} & \overline{F} \\ \uparrow & & \uparrow \\ F(\alpha) & \xrightarrow[\cong]{\Psi_{\alpha,\beta}} & F(\beta) \end{array} \qquad \textbf{(II)}$$

Dado que **(II)** conmuta (es decir, $\Psi(\alpha) = \beta$ y $\overline{\Psi_{\alpha,\beta}}$ es extensión de $\Psi_{\alpha,\beta}$) $\Rightarrow \overline{\Psi_{\alpha,\beta}}(\alpha) = \beta$.
Por otra parte pegando los diagramas **(I)** y **(II)** tenemos que $\overline{\Psi_{\alpha,\beta}}$ hace conmutar el diagrama siguiente.

$$\begin{array}{ccc} E & \xrightarrow{\overline{\Psi_{\alpha,\beta}}} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \end{array} \qquad \textbf{(III)}$$

Así la hipótesis implica que

$$\overline{\Psi_{\alpha,\beta}} \in Aut(E)$$

$$\Rightarrow \overline{\Psi_{\alpha,\beta}}(E) = E \quad \Rightarrow \quad \beta = \overline{\Psi_{\alpha,\beta}}(\alpha) \in \overline{\Psi_{\alpha,\beta}}(E) = E$$

$$\therefore \beta \in E.$$

■

2.9. Campos de descomposición.

Definición 2.9.1 *Sea F un campo con cerradura algebraica $\overline{F}$. Sea $\{f_i(x)|i \in I\}$ una colección de polinomios en $F[x]$. Un campo $E \leqslant \overline{F}$ es un* ***campo de descomposición de*** *$\{f_i(x)|i \in I\}$* ***sobre*** *F si E es el menor subcampo de $\overline{F}$ que contiene a F y a los ceros en $\overline{F}$ de cada uno de los $f_i(x)$ $\forall\ i \in I$.*

Definición 2.9.2 *Un campo $K \leqslant \overline{F}$ es un* ***campo de descomposición sobre F*** *si es el campo de descomposición de algún conjunto de polinomios en $F[x]$.*

Teorema 2.9.3 *Un campo E tal que $F \leqslant E \leqslant \overline{F}$ es un campo de descomposición sobre $F \Leftrightarrow$ todo automorfismo de $\overline{F}$ que deje fijo a F lleva a E sobre si mismo y así, induce un automorfismo de E que deja fijo a F.*

Demostración. ($\Rightarrow$) Sea $\{f_i(x)|i \in I\} \subseteq F[x]$ tal que E es un campo de descomposición de $\{f_i(x)|i \in I\}$ sobre F. Sea

$$\sigma : \overline{F} \longrightarrow \overline{F}$$

un isomorfismo que deja fijo a F, esto es σ es un isomorfismo de $\overline{F}$ en $\overline{F}$ tal que el diagrama siguiente conmuta

$$\begin{array}{ccc} \overline{F} & \xrightarrow[\cong]{\sigma} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \end{array}$$

Demostraremos que $\sigma(E) = E$.
Sea $\{\alpha_j|j \in J\}$ la colección de todos los ceros en $\overline{F}$ de los $f_i(x)$ para cada $i \in I$. Dado que cada $\alpha_j \in \overline{F}$ es algebraico sobre F, entonces

$$\begin{array}{l} F(\alpha_j) \\ \infty > \Big\uparrow \text{Base } \{\alpha_j^0, \alpha_j^1, \cdots, \alpha_j^{n_j-1}\} \text{ donde } n_j = grad(\alpha_j, F) \\ F \end{array}$$

$\Rightarrow$ para cada $j \in J$ tenemos

$$F(\alpha_j) = \{a_0 + a_1\alpha_j + \cdots + a_{n_j-1}\alpha_j^{n_j-1} | a_k \in F\} \quad y \quad n_j = grad(\alpha_j, F).$$

Sea S el conjunto de sumas finitas de productos finitos de los elementos de $F(\alpha_j)\ \forall\ j \in J$.

$$\Rightarrow S = \{ \sum_{i,\ finita} a_i \alpha_{i_1}^{r_1} \cdots \alpha_{i_k}^{r_k} | \alpha_{i_1}, \cdots, \alpha_{i_k} \in \{\alpha_j\}_{j\in J},\ a_i \in F\}$$

Notemos que dada cualquier colección

$$\alpha_{j_1}, \cdots, \alpha_{j_r} \in \{\alpha_j\}_{j\in J}$$

tenemos que

$$F(\alpha_{j_1}, \cdots, \alpha_{j_r}) \subseteq S,$$

pues se tiene la torre de campos

$$\begin{array}{c} F(\alpha_{j_1}, \cdots, \alpha_{j_r}) \\ \| \\ F(\alpha_{j_1}, \cdots, \alpha_{j_{r-1}})(\alpha_{j_r}) \\ \uparrow_{<\infty} \\ F(\alpha_{j_1}, \cdots, \alpha_{j_{r-1}}) \\ \| \\ F(\alpha_{j_1}, \cdots, \alpha_{j_{r-2}})(\alpha_{j_{r-1}}) \\ \uparrow_{<\infty} \\ \vdots \\ \uparrow_{<\infty} \\ F(\alpha_{j_1}, \alpha_{j_2}) \\ \| \\ (F(\alpha_{j_1}))(\alpha_{j_2}) \\ \uparrow_{<\infty} \\ F(\alpha_{j_1}) \\ \uparrow_{<\infty} \\ F \end{array}$$

Sea

$$n_{j_k} = grad(\alpha_{j_k}, F)$$

$\Rightarrow \{\alpha_{j_k}^0, \alpha_{j_k}^1, \cdots, \alpha_{j_k}^{n_{j_k}-1}\}$ es una base para $F(\alpha_{j_1}, \cdots, \alpha_{j_{k-1}})(\alpha_{j_k})$ sobre $F(\alpha_{j_1}, \cdots, \alpha_{j_{k-1}})$. Así, por el corolario 2.3.7 tenemos que

$$[F(\alpha_{j_1}, \cdots, \alpha_{j_r}) : F] = n_{j_1} \cdots n_{j_r}$$

donde una base para $F(\alpha_{j_1}, \cdots, \alpha_{j_r})$ sobre F esta dada por el conjunto

$$\{\Pi_{k=0}^{r} \alpha_{j_k}^{s_{j_k}} | 0 \leq s_{j_k} \leq n_{j_k - 1}\}$$

que consta de todos los posibles productos de las potencias de los $\alpha_{j_1}, \cdots, \alpha_{j_r}$ y tiene $n_{j_1} \cdots n_{j_r}$ elementos.
Por tanto tenemos que efectivamente $F(\alpha_{j_k}, \cdots, \alpha_{j_r}) \subseteq S$ para cualquier colección finita $\alpha_{j_1}, \cdots, \alpha_{j_r} \in \{\alpha_j\}_{j \in J}$.
Retomando

$$S = \left\{ \sum_{i,\ finita} a_i \alpha_{i_1}^{r_1} \cdots \alpha_{i_k}^{r_k} | \alpha_{i_1}, \cdots, \alpha_{i_k} \in \{\alpha_j\}_{j \in J},\ a_i \in F \right\} \subseteq E$$

Es claro que S es cerrado bajo la suma y bajo la multiplicación y que $0, 1 \in S$. Además $0 \neq y \in S$

$$\Rightarrow y = \sum_{i,\ finita} a_i \alpha_{i_1}^{r_1} \cdots \alpha_{i_k}^{r_k} \in F(\alpha_1, \cdots, \alpha_n) \subseteq S$$

para alguna colección $\alpha_1, \cdots, \alpha_n$ finita donde $\alpha_1, \cdots, \alpha_n$ son todas las α_i's que aparecen en la sumatoria. $\Rightarrow y^{-1} \in F(\alpha_1, \cdots, \alpha_n)$ pues $F(\alpha_1, \cdots, \alpha_n)$ es un campo contenido en E, pero $F(\alpha_1, \cdots, \alpha_n) \subseteq S \Rightarrow y^{-1} \in S \therefore S \leqslant E$, con S tal que contiene a todos los ceros $\{\alpha_j | j \in J\}$ *de* $\{f_i(x) \in F[x] | i \in I\}$ y $F \subseteq S$. Por definición de campo de descomposición tenemos que $S = E$. Por tanto hemos probado que el conjunto de todos los ceros $\{\alpha_j\}_{j \in J}$ de $\{f_i(x) | i \in I\}$ genera a E sobre F en el sentido de que cualquier elemento en E se expresa como suma de productos finitos de potencias de α_i's con coeficientes en F. Así se tiene que el valor de $\sigma|_E$ tal que $\sigma(a) = a\ \forall\ a \in F$ está determinado completamente por la colección de valores $\{\sigma(\alpha_j)\}_{j \in J}$.
Por el corolario 2.5.4 (el cual afirma que si α es algebraico sobre F entonces todo monomorfismo $\Psi : F(\alpha) \rightarrowtail \overline{F}$ tal que $\Psi(a) = a\ \forall\ a \in F$ es tal que $\Psi(\alpha)$ es conjugado de α sobre F.)

$$\Rightarrow irr(\alpha_j, F) = irr(\sigma(\alpha_j), F)\ \ \forall\ j \in J$$

pero por el teorema 1.7.1 $irr(\alpha_j, F)$ divide a aquellos $f_i(x) \in F[x]$ que cumplen $f_i(\alpha_j) = 0$. Pero $irr(\alpha_j, F) = irr(\sigma(\alpha_j), F) \Rightarrow irr(\sigma(\alpha_j), F)$ divide a aquellos $f_i(x) \in F[x]$ tal que $f_i(\alpha_j) = 0$. $\Rightarrow \sigma(\alpha_j)$ es cero de todos los f_i que tienen a α_j como cero y entonces, por definición de campo de descomposición tenemos que $\sigma(\alpha_j) \in E \quad \forall\ j \in J$. Así, dado que $F \leqslant E \leqslant \overline{F}$, tenemos que $\sigma|_E : E \rightarrowtail \overline{F}$ es tal que $\sigma(E) \subseteq E$. Así, $\sigma|_E : E \rightarrowtail E$ y $\sigma|_E$ extiende a F como lo ilustra el siguiente diagrama.

$$\begin{array}{ccc} E & \overset{\sigma}{\rightarrowtail} & E \\ \uparrow & & \uparrow \\ F & = & F \end{array}$$

Repitiendo el razonamiento que se hizo para σ se llega a que $\sigma^{-1}|_E : E \rightarrowtail E$ es monomorfismo y extiende a F como lo ilustra el siguiente diagrama

$$\begin{array}{ccc} E & \overset{\sigma^{-1}}{\rightarrowtail} & E \\ \uparrow & & \uparrow \\ F & = & F \end{array}$$

Usando este hecho podemos demostrar que $\sigma : E \rightarrowtail E$ es sobreyectiva. En efecto; sea $\beta \in E$ arbitrario. $\Rightarrow \sigma^{-1}(\beta) \in E$ pues $\sigma^{-1} : E \rightarrowtail E$,
$\Rightarrow \sigma(\sigma^{-1}(\beta)) = \beta \therefore x = \sigma^{-1}(\beta) \in E$ es tal que $\sigma(x) = \beta \therefore \sigma$ es sobreyectiva y por tanto

$$\sigma \in Aut(E) \ y \ \sigma(a) = a \ \forall \ a \in F.$$

($\Leftarrow$) Claramente si $E = F$ entonces E es un campo de descomposición sobre F. Consideremos el caso en que $F \lneq E \leqslant \overline{F}$. Sea $g(x) \in F[x]$ un polinomio irreducible sobre F, tal que $g(x)$ tiene un cero $\alpha \in E$ (por ejemplo podemos tomar cualquier $\alpha \in E$ y como $E \leqslant \overline{F}$ y por definición de $\overline{F}$ es una extensión algebraica de F algebraicamente cerrada, se tiene que E es algebraica sobre F, entonces $irr(\alpha, F)$ existe y podemos tomar $g(x) = irr(\alpha, F)$, por ejemplo.)
Sea β cualquier cero de $g(x)$ en $\overline{F}$,

$$\Rightarrow irr(\alpha, F) = irr(\beta, F)$$

por el teorema 2.5.3 se tiene

$$\Psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta) \ es \ isomorfismo$$

que deja fijo a F.

$$\begin{array}{ccc} F(\alpha) & \overset{\Psi_{\alpha,\beta}}{\underset{\cong}{\longrightarrow}} & F(\beta) \\ \uparrow & & \uparrow \\ F & = & F \end{array} \qquad \textbf{(I)}$$

Dado que $\overline{F}$ es algebraico sobre F, entonces $\overline{F}$ es algebraico sobre $F(\alpha)$.

$$\begin{array}{c} \overline{F} \\ \uparrow \\ F(\alpha) \\ \uparrow \\ F \end{array}$$

Por el teorema 2.7.1 (teorema de extensión de isomorfismos) se tiene que $\Psi_{\alpha,\beta}$ puede extenderse a un monomorfismo $\tau : \overline{F} \rightarrowtail \overline{F}$, es decir, el diagrama siguiente conmuta

$$\begin{array}{ccc} \overline{F} & \xrightarrow{\tau} & \overline{F} = \overline{F(\beta)} \\ {\scriptstyle alg}\uparrow & & \uparrow \\ F(\alpha) & \xrightarrow[\cong]{\Psi_{\alpha,\beta}} & F(\beta) \end{array} \qquad \textbf{(II)}$$

Aplicando nuevamente el teorema 2.7.1 al isomorfismo

$$\tau^{-1} : \tau(\overline{F}) \longrightarrow \overline{F},$$

τ^{-1} puede extenderse a un monomorfismo

$$\overline{(\tau^{-1})} : \overline{F} \rightarrowtail \overline{F},$$

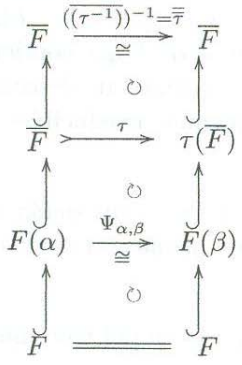
tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \overline{F} & \xrightarrow{\overline{(\tau^{-1})}} & \overline{F} \\ {\scriptstyle alg}\uparrow & & \| \\ \tau(\overline{F}) & \xrightarrow[\cong]{\tau^{-1}} & \overline{F} \end{array} \qquad \textbf{(III)}$$

Dado que τ^{-1} es sobreyectiva $\Rightarrow$ $\overline{(\tau^{-1})}$ es isomorfismo, por lo que invirtiendo el diagrama **(III)**, obtenemos el siguiente diagrama conmutativo:

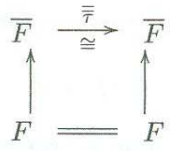
$$\begin{array}{ccc} \overline{F} & \xrightarrow[\cong]{(\overline{(\tau^{-1})})^{-1}=\overline{\overline{\tau}}} & \overline{F} \\ \| & & \uparrow \\ \overline{F} & \longrightarrow & \tau(\overline{F}) \end{array} \qquad \textbf{(IV)}$$

$\Rightarrow$ pegando los diagramas **(I)**,**(II)** y **(IV)** tenemos



(I)

Así obtenemos el siguiente diagrama conmutativo



(V)

por tanto $\overline{\overline{\tau}}$ es un automorfismo de $\overline{F}$ que deja fijo a F.
Por hipótesis, $\overline{\overline{\tau}}(E) = E$. Así $\overline{\overline{\tau}}(\alpha) \in E$.

$$\Rightarrow \beta = \Psi_{\alpha,\beta}(\alpha) = \overline{\overline{\tau}}(\alpha) \in E \therefore \beta \in E.$$

Hemos demostrado que si $g(x)$ es un polinomio irreducible en $F[x]$ con un cero en E, entonces todos los ceros de $g(x)$ están en E.

Sea E' subcampo de $\overline{F}$, tal que E' el campo de descomposición del conjunto $\{g_k(x)\}$ de todos los polinomios irreducibles en F con al menos un cero en E. Claramente $E' \subseteq E$. Veamos que $E = E'$. Tenemos que

Sea $\alpha \in E \leqslant \overline{F}$. Dado que E es una extensión algebraica sobre F (pues $\overline{F}$ la es), entonces α es cero de $irr(\alpha, F) \in \{g_k(x)\} \subseteq F[x]$, pero por definición $\alpha \in E'$ pues E' es el menor subcampo de $\overline{F}$ que contiene a F y a los ceros del conjunto $\{g_k(x)\}$, por tanto, E es el campo de descomposición del conjunto $\{g_k(x)\} \subseteq F[x]$ de todos los polinomios irreducibles sobre F con al menos en cero en E. ■

Corolario 2.9.4 *Si E es campo de descomposición sobre F, entonces todo polinomio irreducible en $F[x]$ con al menos un cero en E, se descompone en E.*

Demostración. Es directa de la prueba del teorema 2.9.3. ■

Corolario 2.9.5 *Sea E un campo de descomposición sobre F, entonces todo monomorfismo $\sigma : E \rightarrowtail \overline{F}$ que deja fijo F, es tal que $\sigma \in Aut(E)$. En particular si E es un campo de descomposición de grado finito sobre F entonces*

$$\{E : F\} = |G(E/F)|.$$

Demostración. Sea $\sigma : E \rightarrowtail \overline{F}$ un monomorfismo que deja fijo a F. Esto es, el siguiente diagrama conmuta

$$\begin{array}{ccc} E & \overset{\sigma}{\rightarrowtail} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \end{array} \qquad \textbf{(I)}$$

Por el teorema 2.7.1 existe τ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \overline{F} & \overset{\tau}{\rightarrowtail} & \overline{F} \\ \uparrow & & \uparrow \\ E & \underset{\cong}{\overset{\sigma}{\rightarrowtail}} & \sigma(E) \subseteq \overline{F} \end{array} \qquad \textbf{(II)}$$

Por **(I)** tenemos que $\tau|_F = Id$ y por **(II)** tenemos que $\tau : \overline{F} \longrightarrow \tau(\overline{F})$ es isomorfismo. Entonces $\tau^{-1} : \tau(\overline{F}) \subseteq \overline{F} \longrightarrow \overline{F}$ es también un isomorfismo y existe $\overline{\tau^{-1}}$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \overline{F} & \underset{\cong}{\overset{\overline{\tau^{-1}}}{\longrightarrow}} & \overline{F} \\ \uparrow & & \| \\ \tau(\overline{F}) & \overset{\tau^{-1}}{\rightarrowtail} & \overline{F} \end{array} \qquad \textbf{(III)}$$

Definiendo $\Psi = (\overline{\tau^{-1}})^{-1}$, tenemos el diagrama conmutativo:

$$\begin{array}{ccc} \overline{F} & \xrightarrow[\cong]{(\overline{\tau^{-1}})^{-1}=\Psi} & \overline{F} \\ \uparrow & & \uparrow \\ \overline{F} & \xrightarrow[\cong]{\tau} & \tau(\overline{F}) \subseteq \overline{F} \end{array} \qquad \textbf{(IV)}$$

de donde tenemos que el monomorfismo $\tau : \overline{F} \rightarrowtail \overline{F}$ hace conmutar el siguiente diagrama

$$\begin{array}{ccc} \overline{F} & \xrightarrow[\cong]{\Psi} & \overline{F} \\ \uparrow & & \uparrow \\ \overline{F} & \xrightarrow{\tau} & \overline{F} \end{array} \qquad \textbf{(V)}$$

pegando el diagrama **(II)** y el **(V)** se tiene el siguiente diagrama que conmuta

$$\begin{array}{ccc} \overline{F} & \xrightarrow[\cong]{\Psi} & \overline{F} \\ \uparrow & & \uparrow \\ E & \xrightarrow{\sigma} & \sigma(E) \subseteq \overline{F} \end{array} \qquad \textbf{(VI)}$$

Dado que por hipótesis E es campo de descomposición sobre F, por el teorema 2.9.3 tenemos que $\sigma = \Psi|_E \in Aut(E)$.

Si $[E : F] < \infty$ entonces recordaremos que para un campo de extensión finita del campo F se definió $\{E : F\}$ como el número de monomorfismos de E en $\overline{F}$ que dejan fijo a F.
Por la primera parte del corolario 2.9.5 que ya demostramos tenemos que

$$\{E : F\} = |\{\sigma \in Aut(E) | \sigma|_F = F\}| = |G(E/F)|.$$

■

Ejemplo 2.9.6 *$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el campo de descomposición de $\{x^2 - 2, x^2 - 3\} \subseteq \mathbb{Q}[x]$ sobre $\mathbb{Q}$, pues $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ contiene a $\mathbb{Q}$, y a todos los ceros de $x^2 - 2$ y $x^2 - 3$ que son: $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$.*
Además $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es por definición el subcampo de $\mathbb{C}$ mas pequeño que contiene a $\sqrt{2}, \sqrt{3}$ y a $\mathbb{Q}$, y por tanto a $-\sqrt{2}$ y $-\sqrt{3}$.

En el ejemplo 2.5.21 se demostró que los automorfismos Id, σ_1, σ_2 y σ_3 son

todos los automorfismos de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *que dejan fijo a* $\mathbb{Q}$, *así* $|G(\mathbb{Q}(\sqrt{2},\sqrt{3}))/\mathbb{Q}| = 4$. *(Aún más notemos que cualquier automorfismo de* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *debe dejar fijo al campo primo* $\mathbb{Q}$ *∴ esos son todos los automorfismos de* $\mathbb{Q}(\sqrt{2},\sqrt{3})$*). Así, por el corolario 2.9.5 se tiene*

$$4 \equiv |G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = \{\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}\}. \quad \blacksquare$$

Deseamos determinar las condiciones para las cuales se cumple que:

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

Para extensiones finitas de E en F ($[E : F] < \infty$). En la siguiente sección demostraremos que $|G(E/F)| = \{E : F\} = [E : F]$ se cumple cuando:
1.- E es un campo de descomposición sobre un campo F de característica cero,
2.- Cuando F es un campo finito.

Nota 2.9.7 $|G(E/F)| = \{E : F\} = [E : F]$ *no necesariamente es cierto cuando* F *es un campo infinito de característica* p *(con* p *un número primo).*

Ejemplo 2.9.8 *Sea* $\sqrt[3]{2}$ *la raíz cúbica real de 2. Notemos que* $x^3 - 2$ *no se descompone en* $\mathbb{Q}(\sqrt[3]{2})$ *pues* $\mathbb{Q}(\sqrt[3]{2}) \leqslant \mathbb{R}$ *y sólo un cero de* $x^3 - 2$ *es real. Así,* $x^3 - 2$ *se factoriza en* $(\mathbb{Q}(\sqrt[3]{2}))[x]$ *en un factor lineal* $x - \sqrt[3]{2}$ *y en un factor cuadrático irreducible* $p(x)$. *Así, si* $\alpha = a + bi$ *es un cero en* $\overline{F} = \mathbb{C}$ *para dicho factor cuadrático* $p(x)$ *irreducible* $\Rightarrow \mathbb{Q}(\sqrt[3]{2})(\alpha)$ *es el menor subcampo de* $\mathbb{C}$ *que contiene a* $\mathbb{Q}(\sqrt[3]{2})$ *y a* α. *Además que* $\alpha = a + bi \in \mathbb{C}$ *sea cero de* $p(x) \in \mathbb{Q}(\sqrt[3]{2})[x] \subseteq \mathbb{R}[x]$, *implica que* $\overline{\alpha} = a - bi \in \mathbb{C}$ *es cero de* $p(x) \in \mathbb{Q}(\sqrt[3]{2})[x] \subseteq \mathbb{R}[x]$, *donde* $a, b \in \mathbb{Q}(\sqrt[3]{2})$. *(Ya se demostró anteriormente). Notemos ahora que*

$$\overline{\alpha} \in \mathbb{Q}(\sqrt[3]{2})(\alpha)$$

pues tenemos que $a, b \in \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2})(\alpha)$ *y* $\alpha = a + bi \in \mathbb{Q}(\sqrt[3]{2})(\alpha) \Rightarrow b_i = -a + (a + b_i) \in \mathbb{Q}(\sqrt[3]{2})(\alpha) \Rightarrow -b_i \in \mathbb{Q}(\sqrt[3]{2})(\alpha) \Rightarrow a + (-bi) \in \mathbb{Q}(\sqrt[3]{2})(\alpha)$ *∴ hemos probado que el campo de descomposición* E *de* $x^3 - 2$ *sobre* $\mathbb{Q}$ *es* $E = \mathbb{Q}(\sqrt[3]{2})(\alpha)$ *y además que*

$$[\mathbb{Q}(\sqrt[3]{2})(\alpha) : \mathbb{Q}(\sqrt[3]{2})] = grad(p(x), \mathbb{Q}) = 2$$

$$\Rightarrow [E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = (2)(3) = 6$$

Por tanto, hemos demostrado que el campo de descomposición E sobre $\mathbb{Q}$ del polinomio x^3-2 es de grado 6 sobre $\mathbb{Q}$ ($[E:\mathbb{Q}]=6$).
Elevando al cubo podemos verificar que:

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

son los ceros del factor cuadrático irreducible $p(x)$ en $\mathbb{C}$.
Así

$$E=\mathbb{Q}(\sqrt[3]{2})\left(\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)\right)$$

o de manera más simplificada notemos que

$$E=\mathbb{Q}(\sqrt[3]{2})(i\sqrt{3})$$

En efecto; claramente $\mathbb{Q}(\sqrt[3]{2})\left(\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)\right)\subseteq\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$.
Veamos que

$$\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})\subseteq\mathbb{Q}(\sqrt[3]{2})\left(\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)\right).$$

Basta probar que

$$i\sqrt{3}\in\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}(\frac{-1+i\sqrt{3}}{2})).$$

pero

$$i\sqrt{3}=1+2\cdot\frac{1}{\sqrt[3]{2}}\left(\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)\right)\in\mathbb{Q}\left(\sqrt[3]{2},\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)\right).$$

$$\therefore E=\mathbb{Q}(\sqrt[3]{2})(i\sqrt{3}).$$

Nota 2.9.9 *$E\neq\mathbb{Q}(\sqrt[3]{2},i,\sqrt{3})$ el cual es de grado 12 sobre $\mathbb{Q}$, ver [1] pp. 391-392).*

2.10. Multiplicidad de los ceros de un polinomio.

Definición 2.10.1 *Sea $f(x)\in F[x]$. Un elemento $\alpha\in\overline{F}$ tal que $f(\alpha)=0$ se llama un cero de $f(x)$ de* ***multiplicidad*** *ν, si ν es el mayor entero tal que $(x-\alpha)^\nu$ es un factor de $f(x)$ en $\overline{F}[x]$.*

Teorema 2.10.2 *Sea $f(x)$ irreducible en $F[x]$. Entonces todos los ceros de $f(x)$ en $\overline{F}$ tienen la misma multiplicidad.*

Demostración. Sean α y β ceros del polinomio $f(x)$ irreducible $\Rightarrow irr(\alpha, F) = irr(\beta, F)$, y por el teorema 2.5.3 se tiene el isomorfismo

$$\Psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$$

tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \overline{F} & & \\ \uparrow & & \\ F(\alpha) & \xrightarrow[\cong]{\Psi_{\alpha,\beta}} & F(\beta) \qquad con \quad \Psi(\alpha) = \beta \\ {\scriptstyle alg}\uparrow & & \uparrow \\ F & = & F \qquad\qquad \textbf{(I)} \end{array}$$

por el corolario 2.7.2 existe una extensión τ, tal que, conmuta el siguiente diagrama

$$\begin{array}{ccc} \overline{F} & \xrightarrow{\tau} & \overline{F} \\ {\scriptstyle alg}\uparrow & & \uparrow \\ F(\alpha) & \xrightarrow[\cong]{\Psi_{\alpha,\beta}} & F(\beta) \qquad\qquad \textbf{(II)} \end{array}$$

pegando los diagramas **(I)** y **(II)** se tiene el diagrama conmutativo siguiente

$$\begin{array}{ccc} \overline{F} & \xrightarrow{\tau} & \overline{F} \\ \uparrow & & \uparrow \\ F(\alpha) & \xrightarrow[\cong]{\Psi_{\alpha,\beta}} & F(\beta) \\ \uparrow & & \uparrow \\ F & = & F \end{array}$$

que induce el diagrama siguiente

$$\begin{array}{ccc} \overline{F}[x] & \xrightarrow{\tau_x} & \overline{F}[x] \\ \uparrow & & \uparrow \\ F(\alpha)[x] & \xrightarrow[\cong]{\overline{\Psi}_{\alpha,\beta}} & F(\beta)[x] \\ \uparrow & & \uparrow \\ F[x] & = & F[x] \end{array}$$

Dado que $f(x)$ por hipótesis pertenece a $F[x]$, entonces

$$\tau_x(f(x)) = f(x).$$

Por otra parte

$$f(x) = (x-\alpha)^\nu g(x)$$

para algún $g(x) \in \overline{F}[x]$, donde ν =multiplicidad de α en $\overline{F}$. Y entonces:

$$\begin{aligned} f(x) &= \tau_x(f(x)) \\ &= \tau_x((x-\alpha)^\nu g(x)) \\ &= (\tau_x(x) - \tau_x(\alpha))^\nu \tau_x(g(x)) \\ &= (x - \Psi_{\alpha,\beta}(\alpha))^\nu \tau_x(g(x)) \\ &= (x-\beta)^\nu \tau_x(g(x)) \quad con \quad \tau_x(g(x)) \in \overline{F}[x] \end{aligned}$$

entonces la multiplicidad de β en $\overline{F}$ es al menos ν. Esto es, la multiplicidad de β en F es mayor o igual a la multiplicidad de α en $\overline{F}$.
Cambiando los papeles de α y β en el razonamiento anterior concluímos que la multiplicidad de α en $\overline{F}$ es mayor o igual a la multiplicidad de β en $\overline{F}$. Por tanto la multiplicidad de α en $\overline{F}$ es igual a la multiplicidad de β en $\overline{F}$.
■

Corolario 2.10.3 *Si $f(x)$ es irreducible en $F[x]$, entonces $f(x)$ tiene una factorización en $\overline{F}[x]$ de la forma:*

$$a\Pi_{i,finita}(x-\alpha_i)^\nu \equiv a(x-\alpha_1)^\nu(x-\alpha_2)^\nu \cdots (x-\alpha_k)^\nu para\ algún\ k$$

donde las α_i son los ceros distintos de $f(x)$ en $\overline{F}$ y $a \in F$.

Demostración. Inmediata del teorema 2.10.2. ■

A continuación mostraremos mediante un ejemplo que puede ocurrir el caso en el que un cero de un polinomio irreducible sea de multiplicidad mayor que 1. Lo que sólo puede suceder para un polinomio sobre un campo infinito de característica $p \neq 0$.

Ejemplo 2.10.4 *Consideremos el campo $E = \mathbb{Z}_p(y)$, donde y es una indeterminada, es decir,*

$$\mathbb{Z}_p(y) = \{\frac{f(y)}{g(y)} | f(y), g(y) \in \mathbb{Z}_p[y] \ con\ g(y) \neq 0\}.$$

Sea $\mathbb{Z}_p(y^p)$ *el subcampo de* $\mathbb{Z}_p(y)$ *definido por*

$$\mathbb{Z}_p(y^p) = \{\frac{f(y^p)}{g(y^p)} | f(y), g(y) \in \mathbb{Z}_p[y] \text{ y } g(y) \neq 0\} \leqslant \mathbb{Z}_p(y) \equiv E.$$

Primero notemos que $\mathbb{Z}_p(y^p)(y) = \mathbb{Z}_p(y)$ *porque tenemos que* $\mathbb{Z}_p(y^p, y) \subseteq \mathbb{Z}_p(y)$ *pues* $\mathbb{Z}_p(y)$ *es un campo que contiene por definición a* $\mathbb{Z}_p$ *y a* y*, además* $y^p \in \mathbb{Z}_p(y)$.
Por otra parte tenemos que

$$\mathbb{Z}_p(y) \subseteq \mathbb{Z}_p(y^p, y)$$

pues $\mathbb{Z}_p(y^p, y)$ *es un campo que contiene a* $\mathbb{Z}_p$ *y a* y*, por tanto*

$$\mathbb{Z}_p(y^p)(y) = \mathbb{Z}_p(y).$$

Además el elemento $y \in \mathbb{Z}_p(y^p)(y)$ *es algebraico sobre* $\mathbb{Z}_p(y^p)$ *pues* y *es cero del polinomio*

$$x^p - y^p \in \mathbb{Z}_p(y^p)[x].$$

Así tenemos que $\mathbb{Z}_p(y^p)(y)$ *es una extensión simple por un elemento y algebraico sobre* $\mathbb{Z}_p(y^p)$ *(por tanto la extensión es finita), por lo que tiene sentido hablar del polinomio* $irr(y, \mathbb{Z}_p(y^p))$.

$$\begin{array}{c} \mathbb{Z}_p(y^p)(y) = \mathbb{Z}_p(y) \\ \Big\uparrow {\scriptstyle <\infty} \\ \mathbb{Z}(y^p) \end{array}$$

Dado que y *es cero del polinomio* $x^p - y^p \in \mathbb{Z}_p(y^p)[x]$ *entonces por el teorema 1.7.1 tenemos*

$$irr(y, \mathbb{Z}_p(y^p)) | x^p - y^p. \qquad \textit{(I)}$$

Además dado que

$$\mathbb{Z}_p(y^p)(y) = \mathbb{Z}_p(y) \neq \mathbb{Z}_p(y^p) \Leftrightarrow [\mathbb{Z}_p(y^p)(y) : \mathbb{Z}_p(y^p)] \neq 1, \textit{por la observación 2.2.2}$$

es decir,

$$grad(y, \mathbb{Z}_p(y^p)) = [\mathbb{Z}_p(y^p)(y) : \mathbb{Z}_p(y^p)] \geq 2 \qquad \textit{(II)}$$

Por otra parte notemos que $x^p - y^p = (x - y)^p$ *en* $\mathbb{Z}_p(y)$*, pues* $\mathbb{Z}_p(y)$ *tiene característica* p *(por la demostración del teorema 2.6.1).* ***(III)***

Por tanto de ***(I)***, ***(II)*** *y* ***(III)*** *se concluye que*

$$irr(y, \mathbb{Z}_p(y^p)) = (x-y)^k \text{ con } 1 < k \leq p$$

con $(x-y)^k | (x-y)^p = x^p - y^p$. *Así* y *es un cero de multiplicidad* $k > 1$. ■

En realidad por el siguiente ejemplo 2.10.5 tenemos que $irr(y, \mathbb{Z}(y^p)) = x^p - y^p \therefore y$ es un cero de multiplicidad p.

Ejemplo 2.10.5 *Demostraremos que*

$$\{1, y, y^2, \cdots, y^{p-1}\}$$

es una base para $\mathbb{Z}_p(y)$ *sobre* $\mathbb{Z}_p(y^p)$, *donde* y *es una indeterminada. Con referencia al ejemplo 2.10.4, concluiremos, mediante un razonamiento de grado, que* $x^p - t$ *es irreducible sobre* $\mathbb{Z}_p(t)$ *donde* $t = y^p$.

Demostración. Tenemos que

$$\begin{array}{c} \mathbb{Z}_p(y) \\ \text{II} \\ Z_p(y^p)(y) \\ \uparrow_{<\infty} \\ \mathbb{Z}_p(y^p) \end{array}$$

Dado que y satisface el polinomio

$$x^p - y^p \in \mathbb{Z}_p(y^p)[x]$$

entonces y es algebraico sobre $\mathbb{Z}_p(y^p)$. Por tanto $\mathbb{Z}_p(y^p)(y)$ es una extensión simple por un elemento algebraico, por tanto la extensión es finita, aún más, una base está dada por

$\{1, y^1, y^2, \cdots, y^{n-1}\}$, *donde* $n = grad(irr(y, \mathbb{Z}_p(y^p)))$, *con* $irr(y, \mathbb{Z}_p(y^p)) \in \mathbb{Z}_p(y^p)[x]$.

Dado $m \in \mathbb{N} \cup \{0\}$, notemos que

$$\begin{aligned} y^m &= y^{pk+r} \text{ para algún } k \in \mathbb{N} \cup \{0\} \text{ y para algún } r \text{ tal que } 0 \leqslant r < p \\ &= y^{pk} y^r \text{ con } y^{pk} \in \mathbb{Z}_p(y^p) \end{aligned}$$

$\Rightarrow \{1, y, y^2, \cdots, y^{p-1}\}$ genera el espacio vectorial $\mathbb{Z}_p(y^p)(y)$ sobre $\mathbb{Z}_p(y^p)$. Veamos que esta colección es linealmente independiente sobre $\mathbb{Z}_p(y^p)$.

Sea

$$0 = b_0 + b_1 y + \cdots + b_{p-1} y^{p-1} \ \ con \ \ b_i \in \mathbb{Z}_p(y^p) = \{\frac{f(y^p)}{g(y^p)} \mid f(y), g(y) \in \mathbb{Z}_p(y) \ con \ g(y) \neq 0\}$$

$$\Rightarrow b_i = \frac{f_i(y^p)}{g_i(y^p)} \ para \ cada \ \ i = 0, \cdots, p-1$$

$$\Rightarrow 0 = \frac{f_0(y^p)}{g_0(y^p)} + \frac{f_1(y^p)}{g_1(y^p)} y + \cdots + \frac{f_{p-1}(y^p)}{g_{p-1}(y^p)} y^{p-1}$$

sacando común denominador,

$$0 = \frac{f_0(y^p)(\widehat{g_0(y^p)} g_1(y^p) \cdots g_{p-1}(y^{p-1})) + f_1(y^p)(g_0(y^p)\widehat{g_1(y^p)} \cdots g_{p-1}(y^p))y + \cdots + f_{p-1}(y^p)(g_0(y^p) \cdots (\widehat{g_{p-1}(y^p)}))y^{p-1}}{g_0(y^p) g_1(y^p) \cdots g_{p-1}(y^p)}$$

$$\Rightarrow 0 = \frac{f_0(y^p)h_0(y^p) + f_1(y^p)h_1(y^p)y + \cdots + f_{p-1}(y^p)h_{p-1}(y^p)y^{p-1}}{h(y^p)}$$

donde

$$h_i(y^p) = g_0(y^p) \cdots \widehat{g_i(y^p)} \cdots g_{p-1}(y^p)$$

$$h(y^p) = g_0(y^p) g_1(y^p) \cdots g_{p-1}(y^p)$$

Dado que cada sumando está compuesto de sumas donde las potencias de y no aparecen en otro sumando distinto $i \neq j$. En cada polinomio $f_i(y^p)h_i(y^p)y^i$ tenemos que si m_i es una potencia de un sumando cualquiera de $f_i(y^p)h_i(y^p)y^i$ entonces $m_i \equiv i \ mod \ p$. Así $i \neq j \Rightarrow m_i \neq m_j$. Por tanto, $f_i(y^p)h_i(y^p)y^i = 0 \ \ \forall \ i = 0, \cdots, p-1$.
Pero recordemos que $h_i(y^p) \neq 0$ (pues $h(y^p) \neq 0$) y obviamente $y^i \neq 0$.
Dado que no hay divisores de cero en $\mathbb{Z}_p(y^p)(y) = \mathbb{Z}_p(y) \Rightarrow f_i(y^p) = 0 \ \ \forall \ i = 0, \cdots, p-1 \therefore \{1, y^1, y^2, \cdots, y^{p-1}\}$ es una base para $\mathbb{Z}_p(y)$ sobre $\mathbb{Z}_p(y^p)$.

Ahora veamos que $(x-y)^p = x^p - y^p \in \mathbb{Z}_p(y^p)[x]$ es irreducible sobre $\mathbb{Z}_p(y^p)$.
Supongamos que $(x-y)^p$ no es irreducible sobre $\mathbb{Z}_p(y^p)$, entonces $(x-y)^k \in \mathbb{Z}_p(y^p)[x]$ para algún k tal que $0 < k < p$.
Por otra parte, $(x-y)^k$ tiene término independiente y^k con $0 < k < p$ pero notemos que $y^k \notin \mathbb{Z}_p(y^p)$ (pues suponiendo que $y^k \in \mathbb{Z}_p(y^p)$ para $0 < k < p \Rightarrow 1 \cdot y^k = y^k$ con $1 \in \{1, y^1, \cdots, y^{p-1}\}$ donde $\{1, y^1, \cdots, y^{p-1}\}$ es una base para $\mathbb{Z}_p(y^p)(y)$ sobre $\mathbb{Z}_p(y) \Rightarrow y^k \in \{1, y^1, \cdots, y^{p-1}\}$ se expresa como combinación lineal (múltiplo de 1) de elementos de la base lo cual no es posible). Entonces $y^k \notin \mathbb{Z}_p(y^p) \forall\ 0 < p < k \Rightarrow (x-y)^k \notin \mathbb{Z}_p(y^p)[x]\ \forall\ 0 < k < p$, contradicción. Por tanto, $(x-y)^p \in \mathbb{Z}_p(y^p)[x]$ es irreducible sobre $\mathbb{Z}_p(y^p)$. ■

Teorema 2.10.6 *Sea F subcampo de E tal que $[E:F] < \infty$ entonces,*

$$\{E:F\} | [E:F].$$

Demostración. Dado que $[E:F] < \infty$, por el teorema 2.3.16 existen

$$\alpha_1, \cdots, \alpha_n \in E$$

tales que

$$E = F(\alpha_1, \cdots, \alpha_n).$$

También $[E:F] < \infty$ implica que E es una extensión algebraica sobre F.
$\Rightarrow F \leqslant E \leqslant \overline{F}$.

$$\Rightarrow \exists\ \alpha_1, \cdots, \alpha_n \in \overline{F}$$

tales que

$$E = F(\alpha_1, \cdots, \alpha_n)$$

entonces para cada $i \in \{1, \cdots, n\}$ fijo, la extensión

$$\begin{array}{ll} F(\alpha_1, \cdots, \alpha_{i-1})(\alpha_i) & \text{con } \alpha_i \in \overline{F} \\ \Big\uparrow{\scriptstyle alg} & \\ F(\alpha_1, \cdots, \alpha_{i-1}) & \end{array}$$

es algebraica.
Así tenemos que para cada i fijo existe el polinomio

$$irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1}))$$

entonces para cada i fijo, α_i es uno de los n_i ceros distintos del polinomio $irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1}))$ que por el teorema 2.10.2 tienen multiplicidad ν_i en $\overline{F}$, es decir, tenemos que el polinomio

$$irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1}))$$

es de la forma

$$irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1})) = (x-\alpha_{1_i})^{\nu_i}(x-\alpha_{2_i})^{\nu_i} \cdots (x-\alpha_{n_i})^{\nu_i} \in \overline{F} \ (donde\ \alpha_{1_i} := \alpha_i).$$

$$\Rightarrow grad(irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1}))) = n_i\nu_i$$

entonces para cada i fijo

$$[F(\alpha_1, \cdots, \alpha_{i-1})(\alpha_i) : F(\alpha_1, \cdots, \alpha_{i-1})] = grad(irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1}))) = n_i\nu_i.$$

Por otra parte, para cada i fijo se tiene por la afirmación 2.8.5 que

$$\{F(\alpha_1, \cdots, \alpha_{i-1})(\alpha_i) : F(\alpha_1, \cdots, \alpha_{i-1})\} = n_i.$$

Así, por el teorema 2.3.5 y el corolario 2.8.3,

$$[E : F] = \Pi_{i=1}^{n} n_i\nu_i$$

$$\{E : F\} = \Pi_{i=1}^{n} n_i$$

$$\therefore \{E : F\} | [E : F].$$

■

2.11. Extensiones separables.

Definición 2.11.1 *Una extensión finita E de F es una extensión separable de F si $\{E : F\} = [E : F]$.*
Un elemento $\alpha \in \overline{F}$ es separable sobre F si $F(\alpha)$ es una extensión separable de F.
Un polinomio irreducible $f(x) \in F[x]$ es separable sobre F si todo cero de $f(x)$ en $\overline{F}$ es separable sobre F.

Observación 2.11.2 *Sea $\alpha \in \overline{F}$.*
α es separable sobre $F \Leftrightarrow irr(\alpha, F)$ tiene todos sus ceros de multiplicidad 1.

Demostración. Primero recordamos que tenemos que $\{F(\alpha) : F\}$ =número de ceros distintos de $irr(\alpha, F)$ en $\overline{F}$ y $[F(\alpha) : F] = grad(\alpha, F)$ =número total de ceros de $irr(\alpha, F)$.

($\Rightarrow$)$\{F(\alpha) : F\} = [F(\alpha) : F] \Rightarrow$ todos los ceros de $irr(\alpha, F)$ en $\overline{F}$ son de multiplicidad 1.
($\Leftarrow$) Todos los ceros de $irr(\alpha, F)$ son de multiplicidad 1 $\Rightarrow \{F(\alpha) : F\} = grad(irr(\alpha, F)) = [F(\alpha) : F]$. ■

Observación 2.11.3 *Sea $f(x) \in F[x]$ un polinomio irreducible sobre F. $f(x)$ es separable sobre $F \Leftrightarrow f(x)$ tiene un cero de multiplicidad 1.*

Demostración. Supongamos que $f(x)$ es separable

$$\Rightarrow [F(\alpha) : F] = \{F(\alpha) : F\} \ \forall\ \alpha \in \overline{F},\ tal\ que\ \alpha\ es\ cero\ de\ f(x).$$

Entonces el grado de $f(x)$ es igual al número de ceros distintos de f(x), es decir,

$$\begin{array}{ccc} [F(\alpha) : F] & = & \{F(\alpha) : F\} \ \forall\ \alpha \in \overline{F}\ con\ \alpha\ cero\ de\ f(x) \\ \| & & \| \\ grad(irr(\alpha, F)) & & \text{número de ceros distintos de } irr(\alpha, F) \\ \| & & \| \\ grad(f(x)) & & \text{número de ceros distintos de } f(x) \end{array}$$

Entonces $grad(f(x))$ =número de ceros distintos de $f(x)$, por lo que todos los ceros de $f(x)$ tienen multiplicidad 1.

($\Leftarrow$) Supongamos que $f(x)$ tiene un cero de multiplicidad 1.
Por el teorema 2.10.2 se tiene que $f(x)$ tiene todos sus ceros $\alpha \in \overline{F}$ de multiplicidad 1.

$$\begin{array}{rcl} \Rightarrow grad(f(x)) = grad(\alpha, F) = [F(\alpha) : F] & = & \text{número total de ceros de } irr(\alpha, F) \\ & = & \text{número de ceros distinto de } irr(\alpha, F) \\ & = & \{F(\alpha, F)\} \end{array}$$

$\Rightarrow [F(\alpha) : F] = \{F(\alpha), F\}$ para todo cero $\alpha \in \overline{F}$, por lo que $f(x)$ es separable sobre F. ■

Equivalentemente tenemos la siguiente

Observación 2.11.4 *Sea $f(x) \in F[x]$ un polinomio irreducible sobre F. $f(x)$ es separable sobre $F \Leftrightarrow f(x)$ tiene todos sus ceros de multiplicidad 1.*
■

Teorema 2.11.5 *Si K es una extensión finita de E y E es una extensión finita de F, esto es , si $F \leqslant E \leqslant K$, entonces K es separable sobre $F \Leftrightarrow K$ es separable sobre E y E es separable sobre F.*

Demostración. Por hipótesis tenemos que:

$$\begin{array}{c} K \\ \uparrow {\scriptstyle <\infty} \\ E \\ \uparrow {\scriptstyle <\infty} \\ F \end{array}$$

($\Rightarrow$) Supongamos que K es separable sobre F, entonces por definición

$$[K:F] = \{K:F\},$$

$$\Rightarrow [K:E] < \infty \ \ y \ \ \{E:F\} < \infty$$

por el teorema 2.10.6 tenemos que

$$\{K:E\} | [K:E] \ \ y \ \ \{E:F\} | [E:F]$$

$$\Rightarrow \begin{cases} \{K:E\}c_1 = [K:E] \ p.a. \ \ 0 \neq c_1 \in \mathbb{N} \cup \{0\} \\ \{E:F\}c_2 = [E:F] \ \ p.a. \ \ 0 \neq c_2 \in \mathbb{N} \cup \{0\} \end{cases} \qquad \textbf{(I)}$$

Por otra parte,

$$\begin{array}{lll} \{K:E\}\{E:F\} & = \{K:F\} & \text{por el corolario 2.8.3} \\ & = [K:F] & \text{por hipótesis} \\ & = [K:E][E:F] & \text{por el teorema 2.3.5} \\ & = \{K:E\}c_1\{E:F\}c_2 & \text{por (I)} \end{array}$$

$$\therefore \{K:E\}\{E:F\} = \{K:E\}c_1\{E:F\}c_2$$

$\Rightarrow c_1c_2 = 1$ con $c_1, c_2 \in \mathbb{N} \Rightarrow c_1 = c_2 = 1$

$$\Rightarrow \begin{cases} \{K:E\} = [K:E] \\ \qquad y \\ \{E:F\} = [E:F] \end{cases}$$

entonces tenemos que K es separable sobre E y E es separable sobre F.
($\Leftarrow$) Supongamos que

$$[K:E] < \infty \ \ y \ \ [E:F] < \infty$$

con K separable sobre E y E separable sobre F. Tenemos por definición que

$$\{K : E\} = [K : E] \;\; y \;\; \{E : F\} = [E : F].$$

$$\Rightarrow \{K : F\} = \{K : E\}\{E : F\} = [K : E][E : F] = [K : F]$$

Por tanto K es separable sobre F. ■

Nota 2.11.6 *El teorema 2.11.5 claramente se puede extender por inducción a cualquier torre finita de extensiones finitas. El campo de arriba es una extensión separable del campo de abajo si y sólo si cada campo es una extensión separable del que está inmediatamente debajo de él.*

Corolario 2.11.7 *Sea E una extensión finita de F. E es separable sobre $F \Leftrightarrow$ cada $\alpha \in E$ es separable sobre F.*

Demostración. ($\Rightarrow$) Supongamos que E es separable sobre F y sea $\alpha \in E$ arbitrario. Tenemos

$$\infty > \left\{ \begin{array}{c} E \\ \uparrow \\ F(\alpha) \\ \uparrow \\ F \end{array} \right.$$

vimos que lo anterior implica que

$$\begin{array}{c} E \\ \uparrow {\scriptstyle <\infty} \\ F(\alpha) \end{array}$$

Además $[E : F] < \infty$ implica que E es algebraica sobre F, $\Rightarrow \alpha \in E$ es algebraico sobre F y entonces,

$$\begin{array}{c} F(\alpha) \\ \uparrow {\scriptstyle <\infty} \\ F \end{array}$$

Dado que por hipótesis E es separable sobre F, por el teorema 2.11.5 $F(\alpha)$ es separable sobre F para cada $\alpha \in E$ y así por definición se tiene que α es

separable sobre F $\forall$ $\alpha \in E$.

$$\infty > \left\{ \begin{array}{c} E \\ \uparrow {\scriptstyle <\infty} \\ F(\alpha) \\ \uparrow {\scriptstyle <\infty} \\ F \end{array} \right.$$

($\Leftarrow$) Supongamos que $[E : F] < \infty$ y que $\forall$ $\alpha \in E$ tenemos que α es separable sobre F. (Notemos que si $[E : F] < \infty$ entonces por el teorema 2.3.2 E es algebraica sobre F y entonces E subcampo de $\overline{F}$).
Dado que $[E : F] < \infty$, entonces tenemos por el teorema 2.3.16 que $\exists$ $\alpha_1, \cdots, \alpha_n \in E \leqslant \overline{F}$ tales que $E = F(\alpha_1, \cdots, \alpha_n)$.
Dado que por hipótesis cada $\alpha_i \in E \leqslant \overline{F}$ es separable sobre F $\forall\, i = 1, \cdots, n$, entonces por la observación 2.11.2 se tiene que

$$irr(\alpha_i, F) \text{ tiene todos sus ceros de multiplicidad 1 en } \overline{F} \qquad \textbf{(I)}$$

Por otra parte, dado que $irr(\alpha_i, F)$ tiene a $\alpha_i \in E$ como un cero y $F \subseteq F(\alpha_1, \cdots, \alpha_{i-1}) \Rightarrow irr(\alpha_i, F) \in F(\alpha_1, \cdots, \alpha_{i-1})[x]$ y también $irr(\alpha_i, F)$ tiene a α_i como cero para cada $i = 1, \cdots, n$. Por el teorema 1.7.1 tenemos que

$$irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1})) | irr(\alpha_i, F) \textit{ para cada } i = 1, \cdots, n,$$

$$\Rightarrow \quad \exists \;\; g_i(x) \in F(\alpha_1, \cdots, \alpha_{i-1})[x] \text{ tal que}$$

$$irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1}))g_i(x) = irr(\alpha_i, F) \textit{ para cada } i = 1, \cdots, n. \qquad \textbf{(II)}$$

Por **(I)** tenemos el factor $(x - \alpha_i)$ aparece exactamente una sola vez en el lado izquierdo de la igualdad **(II)**, por lo que α_i es un cero de multiplicidad 1 en $irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1}))$ entonces por el teorema 2.10.2 se tiene que todos los ceros en $\overline{F(\alpha_1, \cdots, \alpha_{i-1})} = \overline{F}$ de $irr(\alpha_i, F(\alpha_1, \cdots, \alpha_{i-1}))$ tienen multiplicidad 1. Por la observación 2.11.2 se tiene que el elemento $\alpha_i \in F(\alpha_1, \cdots, \alpha_{i-1})(\alpha_i) \leqslant \overline{F}$ es tal que α_i es separable sobre $F(\alpha_1, \cdots, \alpha_{i-1})$ para cada $i = 1, \cdots, n$, con cada extensión simple separable sobre el campo

que está inmediatamente debajo de ella. Así tenemos

$$\begin{array}{c} E \\ \| \\ F(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n) \\ \uparrow_{<\infty} \\ F(\alpha_1, \cdots, \alpha_{n-1}) \\ \| \\ F(\alpha_1, \cdots, \alpha_{n-2})(\alpha_{n-1}) \\ \uparrow_{<\infty} \\ \vdots \\ \uparrow_{<\infty} \\ F(\alpha_1, \alpha_2) \\ \| \\ F(\alpha_1)(\alpha_2) \\ \uparrow_{<\infty} \\ F(\alpha_1) \\ \uparrow_{<\infty} \\ F \end{array}$$

Por el teorema 2.11.5 extendido por inducción, concluímos que $E \equiv F(\alpha_1, \cdots, \alpha_n)$ es una extensión separable sobre F. ■

2.12. Campos perfectos.

Pasamos a la tarea de demostrar:
"Si $\alpha \in F$ no es separable sobre F entonces F es un campo infinito de característica $p \neq 0$ ".
Para esto, necesitamos el siguiente:

Lema 2.12.1 *Sea $\overline{F}$ una cerradura algebraica de un campo F, y sea*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

cualquier polinomio mónico en $\overline{F}[x]$. Si $(f(x))^m \in F[x]$ y $m \cdot 1 \neq 0$ en F, entonces $f(x) \in F[x]$, esto es, todas las $a_i \in F$.

Demostración. Debemos demostrar que $a_i \in F$, procederemos por inducción sobre r, demostraremos que $a_{n-r} \in F$. Para $r = 1$, veremos primero que

$$(f(x))^m = x^{mn} + (m \cdot 1)a_{n-1}x^{mn-1} + \cdots + a_0^m.$$

Sea

$$Z = a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \qquad \textbf{(I)}$$

entonces

$$\begin{aligned}(x^n + Z)^m = \ & \tbinom{m}{0}(x^n)^m Z^0 + \tbinom{m}{1}(x^n)^{(m-1)} Z^1 + \tbinom{m}{2}(x^n)^{(m-2)} Z^2 + \cdots \\ & + \tbinom{m}{m-1}(x^n)^{(m-(m-1))} Z^{m-1} + \tbinom{m}{m}(x^n)^{m-m} Z^m \qquad \textbf{(II)}\end{aligned}$$

donde

$$\begin{array}{lll} Z^1 & = (a_{n-1}x^{n-1} + \cdots + a_1x + a_0)^1 & \text{todos los términos de grado} \leqslant (n-1) \\ Z^2 & = (a_{n-1}x^{n-1} + \cdots + a_1x + a_0)^2 & \text{todos los términos de grado} \leqslant 2(n-1) \\ \vdots & \vdots & \vdots \\ Z^{m-1} & = (a_{n-1}x^{n-1} + \cdots + a_1x + a_0)^{m-1} & \text{todos los términos de grado} \leqslant (m-1)(n-1) \\ Z^m & = (a_{n-1}x^{n-1} + \cdots + a_1x + a_0)^m & \text{todos los términos de grado} \leqslant m(n-1) \end{array}$$

por tanto, en

$$\begin{array}{ll} \tbinom{m}{1}(x^n)^{(m-1)} Z^1 & \text{aparecen sólo términos de grado} \\ & \leqslant (nm-n) + (n-1) = nm-1. \\ En\ \tbinom{m}{2}(x^n)^{(m-2)} Z^2 & \text{aparecen sólo términos de grado} \\ & \leqslant (nm-2n) + (2n-2) = nm-2. \\ \vdots & \vdots \\ En\ \tbinom{m}{m-1}(x^n)^{(m-(m-1))} Z^{m-1} & \text{aparecen sólo términos de grado} \\ & \leqslant nm - n(m-1) + n(m-1) - (m-1) = nm-(m-1). \\ En\ \tbinom{m}{m}(x^n)^{(m-m)} Z^m & \text{aparecen sólo términos de grado} \\ & \leqslant (nm-nm) + (mn-m) = nm-m. \end{array}$$

por tanto,

$$\begin{aligned}(f(x))^m &= (x^n + Z)^m \\ &= (x^n + (a_{n-1}x^{n-1} + \cdots + a_1x + a_0))^m \\ &= x^{nm} + (m \cdot 1)a_{n-1}x^{nm-1} + \cdots + a_0^m.\end{aligned}$$

Dado que por hipótesis $(f(x))^m \in F[x]$, entonces $(m \cdot 1)a_{n-1} \in F$. Además también por hipótesis $(m \cdot 1) \neq 0$ en F, entonces $(m \cdot 1)^{-1} \in F$ y así

$$a_{n-1} = (m \cdot 1)^{-1}((m \cdot 1)a_{n-1}) \in F,$$

por lo que se tiene

$$a_{n-1} \in F$$

Hipótesis de inducción:

Supongamos que $a_{n-r} \in F \ \forall \ r = 1, 2, \cdots, k$. Por demostrar que $a_{n-(k+1)} \in F$ (y por lo tanto demostraremos que $a_{n-r} \in F \ \forall \ r \leqslant k$ implica que $a_{n-r} \in F \ \forall \ r \leqslant k+1$).

Calculemos el coeficiente A de $Ax^{nm-(k+1)}$ del polinomio $(x^n + Z)^m$.
De la ecuación **(II)** obtenemos que:

$$\begin{aligned} Ax^{nm-(k+1)} &= \tbinom{m}{1}x^{mn-n}a_{n-(k+1)}x^{n-(k+1)} \\ &+\tbinom{m}{2}x^{nm-2n}b_2x^{2n-(k+1)} \\ &\vdots \\ &+\tbinom{m}{m-1}x^{nm-(m-1)n}b_{m-1}x^{(m-1)n-(k+1)} \\ &+\tbinom{m}{m}x^{nm-mn}b_mx^{mn-(k+1)} \end{aligned}$$

Donde los $b_ix^{in-(k+1)}$ son los términos que aparecen en Z^i, con $2 \leqslant i \leqslant m$.
Ahora

$$Z^s = (\underbrace{(a_{n-1}x^{n-1} + \cdots + a_{n-k}x^{n-k})}_{h(x)} + \underbrace{(a_{n-(k+1)}x^{n-(k+1)} + \cdots + a_1x + a_0)}_{g(x)})^s$$

Sean

$$h(x) = a_{n-1}x^{n-1} + \cdots + a_{n-k}x^{n-k},$$
$$g(x) = a_{n-(k+1)}x^{n-(k+1)} + \cdots + a_1x + a_0.$$

el $grad(Z) = n-1$ cuando $a_{n-1} \neq 0$ y $grad(Z) < n-1$ cuando $a_{n-1} = 0$ por como se definió en **(I)**. Entonces para $h(x)$ y $g(x)$ se tiene

$$grad(h(x)) \leqslant n-1 \quad y \quad grad(g(x)) \leqslant n-(k+1)$$

para cada s tal que $2 \leqslant s \leqslant m$. Nos interesa encontrar el coeficiente del término $x^{sn-(k+1)}$ de Z^s.

$$\begin{aligned} Z^s &= (h(x)+g(x))^s \\ &= \tbinom{s}{0}(h(x))^s g(x)^0 && \longrightarrow grado = (s(n-1)+0(n-(k+1))) = sn-s \\ &+\tbinom{s}{1}(h(x))^{s-1}g(x)^1 && \longrightarrow grado = (s-1)(n-1)+1(n-(k+1)) = sn-(1k+s) \\ &+\tbinom{s}{2}(h(x))^{s-2}g(x)^2 && \longrightarrow grado = (s-2)(n-1)+2(n-(k+1)) = sn-(2k+s) \\ &\vdots \\ &+\tbinom{s}{s-1}(h(x))^{s-(s-1)}g(x)^{s-1} && \longrightarrow grado = (s-(s-1))(n-1)+(s-1)(n-(k+1)) \\ & && \qquad\quad = sn-((s-1)k+s) \\ &+\tbinom{s}{s}(h(x))^{s-s}g(x)^s && \longrightarrow grado = (s-s)(n-1)+s(n-(k+1)) = sn-(sk+s) \end{aligned}$$

Para $1 \leqslant i \leqslant s$, tenemos que

$$\begin{aligned}(s-i)(n-1)+i(n-(k+1)) &= sn-s-in+i+in-ik-i \\ &= sn-(ik+s).\end{aligned}$$

Concluímos que para $i \geqslant 1$ no hay términos de la forma $x^{sn-(k+1)}$ en Z^s. Sólo pudieran aparecer términos de la forma $x^{sn-(k+1)}$ para $i=0$ en Z^s, es decir, sólo aparecen términos de la forma $x^{sn-(k+1)}$ en el primer sumando de Z^s que es $\binom{s}{0}(h(x))^s = \binom{s}{0}(a_{n-1}x^{n-1}+\cdots+a_{n-k}x^{n-k})^s \ \forall\ 2 \leqslant s \leqslant m$. Entonces el coeficiente A de $x^{mn-(k+1)}$ en $(f(x))^m$ es de la forma:

$$A = (m\cdot 1)a_{n-(k+1)} + g_{k+1}(a_{n-1}, a_{n-2}, \cdots, a_{n-k})$$

Donde $g_{k+1}(a_{n-1}, a_{n-2}, \cdots, a_{n-k})$ es un polinomio formal en $a_{n-1}, a_{n-2}, \cdots, a_{n-k}$, es decir, g_{k+1} es suma finita de productos finitos de los $a_{n-1}, a_{n-2}, \cdots, a_{n-k}$. Entonces por la hipótesis de inducción tenemos que:

$$g_{k+1}(a_{n-1}, a_{n-2}, \cdots, a_{n-k}) \in F$$

y por hipótesis

$$(f(x))^m \in F[x]. \text{ En particular } A \in F.$$

por tanto,

$$(m\cdot 1)a_{n-(k+1)} = A - g_{k+1}(a_{n-1}, a_{n-2}, \cdots, a_{n-k}) \in F.$$

Por lo que

$$(m\cdot 1)a_{n-(k+1)} \in F.$$

Dado que por hipótesis $m\cdot 1 \neq 0$ en F, nuevamente tenemos que $a_{n-(k+1)} \in F$.
■

Definición 2.12.2 *Un* ***campo es perfecto*** *si toda extensión finita es una extensión separable.*

Teorema 2.12.3 *Todo campo de característica cero es perfecto.*

Demostración. Sea F un campo de característica cero. Sea E un campo de extensión de F tal que $[E:F] < \infty$.
Sea $\alpha \in E$ arbitrario. Como $[E:F] < \infty$, por el teorema 2.3.2 tenemos que E es algebraica sobre F, entonces existe el polinomio $irr(\alpha, F)$.
Por el corolario 2.10.3 el polinomio $irr(\alpha, F)$ se factoriza en $\overline{F}[x]$ como

$$\Pi_{i=1}^{n}(x-\alpha_i)^{\nu} \in \overline{F}[x]$$

donde α_i son los ceros distintos de $irr(\alpha, F)$ en $\overline{F}$ y digamos que $\alpha = \alpha_1$.

$$\text{Entonces } irr(\alpha, F) = \Pi_{i=1}^{n}(x - \alpha_i)^{\nu} = (\Pi_{i=1}^{n}(x - \alpha_i))^{\nu} \in \overline{F}[x].$$

Pero F es de característica cero y por definición de característica cero esto implica que $\nu \cdot 1 \neq 0$, por el lema 2.12.1, el polinomio

$$f(x) = \Pi_{i=1}^{n}(x - \alpha_i) \in F[x]$$

con $f(\alpha) = 0$.
Dado que $irr(\alpha, F)$ es irreducible en F y de grado mínimo tal que tiene a α como un cero, entonces $\nu = 1$ y así tenemos que

$$irr(\alpha, F) = \Pi_{i=1}^{n}(x - \alpha_i) \in \overline{F}[x],$$

lo que implica que todos los ceros de $irr(\alpha, F)$ son de multiplicidad 1 en $\overline{F}$. Por la observación 2.11.2 se tiene que α es separable sobre F. Dado que $[E : F] < \infty$ y $\alpha \in E$ fué tomado arbitrario, aplicando el corolario 2.11.7 obtenemos que E es separable sobre F. ■

Teorema 2.12.4 *Todo campo finito es perfecto.*

Demostración. Sea F un campo finito de característica p y sea E una extensión de F tal que $[E : F] < \infty$. Sea $\alpha \in E$ arbitrario. Por el corolario 2.11.7 basta demostrar que α es separable sobre F.
Dado que $[E : F] < \infty$ por el teorema 2.3.2 tenemos que E es algebraica sobre F y por definición se tiene que existe el polinomio $irr(\alpha, F)$ y por el corolario 2.10.3 tenemos que:

$$irr(\alpha, F) = \Pi_{i=1}^{n}(x - \alpha_i)^{\nu} \text{ en } \overline{F}[x],$$

donde los α_i son los ceros distintos de $irr(\alpha, F)$ en $\overline{F}$ y digamos que $\alpha = \alpha_1$.
Como $\nu \in \mathbb{N}$ podemos expresar ν como $\nu = p^t e$ tal que $p \nmid e$ con $t \in \mathbb{N} \cup \{0\}$.

$$\Rightarrow irr(\alpha, F) = \Pi_{i=1}^{n}(x - \alpha_i)^{\nu} = (\Pi_{i=1}^{n}(x - \alpha_i)^{p^t})^{e}$$

Notemos que $e \cdot 1 \neq 0$ en F pues $(e, p) = 1$. Por el lema 2.12.1

$$\Pi_{i=1}^{n}(x - \alpha_i)^{p^t} \in F[x].$$

Dado que $irr(\alpha, F)$ es el polinomio de grado mínimo sobre F, tal que tiene a $\alpha = \alpha_1$ como un cero y $\alpha = \alpha_1$ también es cero de $\Pi_{i=1}^{n}(x - \alpha_i)^{p^t}$, entonces $e = 1$, por tanto,

$$irr(\alpha, F) = \Pi_{i=1}^{n}(x - \alpha_i)^{p^t} \text{ en } F[x]$$

Por otra parte, vimos en la demostración del teorema 2.6.1 que en un campo finito F de característica p se tiene que

$$(a+b)^p = a^p + b^p \quad \forall\, a, b, \in F.$$

Aplicando la observación anterior p^t veces tenemos

$$irr(\alpha, F) = \Pi_{i=1}^{n}(x-\alpha_i)^{p^t} = \Pi_{i=1}^{n}(x^{p^t} - \alpha_i^{p^t}).$$

Entonces podemos expresar a $irr(\alpha, F)$ como:

$$irr(\alpha, F) = g(x^{p^t}) \in F[x] \; donde \; g(x) = \Pi_{i=1}^{n}(x - \alpha_i^{p^t})$$

pero $g(x^{p^t}) \in F[x]$ y entonces por definición todos los coeficientes de $g(x^{p^t})$ están en F. Así $g(x)$ tiene todos sus coeficientes en $F \Rightarrow g(x) \in F[x]$

$$\therefore g(x) = \Pi_{i=1}^{n}(x - \alpha_i^{p^t}) \in F[x].$$

Notemos que también $g(x)$ es irreducible en $F[x]$ (pues si $g(x)$ no fuera irreducible sobre F entonces existiría una factorización de $g(x)$ tal que $g(x) = h(x)k(x)$ con $grad(h(x)) \neq 0$ y $grad(k(x)) \neq 0$ pero entonces tendríamos que $F[x] \ni irr(\alpha, F) = g(x^{p^t}) = h(x^{p^t})k(x^{p^t}) \Rightarrow grad\; h(x^{p^t}) \neq 0$ y $grad\; k(x^{p^t}) \neq 0 \Rightarrow irr(\alpha, F)$ *no es irreducible sobre* F **!**), por tanto, $g(x) = \Pi_{i=1}^{n}(x - \alpha_i^{p^t}) \in F[x]$ es irreducible sobre F y $g(x)$ tiene todos sus ceros de multiplicidad 1 en $\overline{F}$. Por la observación 2.11.3, $g(x) \in F[x]$ es separable sobre F y los ceros distintos de $g(x)$ en $\overline{F}$ son los $\alpha_i^{p^t}$.

Ahora consideremos

$$F(\alpha_1^{p^t}) \equiv F(\alpha^{p^t}).$$

Dado que $\alpha_1^{p^t} \equiv \alpha^{p^t}$ es un cero del polinomio separable $g(x) \in F[x]$ sobre F entonces por definición

$$F(\alpha^{p^t}) \text{ es separable sobre } F. \qquad \textbf{(I)}$$

Por otra parte, dado que $x^{p^t} - \alpha^{p^t} = (x-\alpha)^{p^t}$ entonces

$$\alpha \text{ es el único cero del polinomio } x^{p^t} - \alpha^{p^t} \text{ en } \overline{F} \qquad \textbf{(II)}$$

y $F(\alpha^{p^t})$ es un espacio vectorial de dimensión finita sobre $F \Rightarrow F(\alpha^{p^t})$ es un campo finito y de característica p, pues $1 \in F \subseteq F(\alpha^{p^t})$, $1 + \cdots + 1 = 0$

en $F \subseteq F(\alpha^{p^t}) \therefore 1 + \cdots + 1 = 0$ en $F(\alpha^{p^t})$. Por el teorema 2.6.1 se tiene la transformación

$$\sigma_p : F(\alpha^{p^t}) \longrightarrow F(\alpha^{p^t})$$

tal que

$$\sigma_p(a) = a^p, \text{ es automorfismo}$$

$$\Rightarrow (\sigma_p)^t \equiv \underbrace{\sigma_p \circ \cdots \circ \sigma_p}_{t-veces} : F(\alpha^{p^t}) \longrightarrow F(\alpha^{p^t}) \text{ es automorfismo,}$$

en particular, $(\sigma_p)^t$ es sobreyectiva y por tanto, para el elemento $\alpha^{p^t} \in F(\alpha^{p^t})$ existe $\beta \in F(\alpha^{p^t})$, tal que

$$(\sigma_p)^t(\beta) = \alpha^{p^t}$$

y por otra parte, por la definición de σ_p tenemos

$$(\sigma_p)^t(\beta) = \beta^{p^t}$$

$$\Rightarrow \beta^{p^t} = \alpha^{p^t}$$
$$\Rightarrow \beta^{p^t} - \alpha^{p^t} = 0$$
$$\Rightarrow \beta \textit{ es un cero de } x^{p^t} - \alpha^{p^t}$$

pero en **(II)** vimos que α es el único cero de $x^{p^t} - \alpha^{p^t}$, por tanto $\alpha = \beta$, y dado que $\beta \in F(\alpha^{p^t})$ y $\beta = \alpha$, entonces $\alpha \in F(\alpha^{p^t})$ así:

$$F(\alpha) = F(\alpha^{p^t}) \qquad \textbf{(III)}$$

(**(III)** es verdad pues siempre se cumple que

$$F(\alpha^{p^t}) \subseteq F(\alpha)$$

pues $\alpha^{p^t} \in F(\alpha)$ y

$$F(\alpha) \subseteq F(\alpha^{p^t})$$

debido a que $F(\alpha^{p^t})$ contiene a α y a F). Por **(I)** y **(III)** tenemos que $F(\alpha)$ es separable sobre F, entonces por definición, $\alpha \in E$ es separable sobre F. (Notemos además que $irr(\alpha, F) = \Pi_{i=1}^{n}(x - \alpha_i)^{p^t}$, entonces por la observación 2.11.2 $t = 0$). ■

2.13. Teorema del elemento primitivo.

Teorema 2.13.1 *(Del elemento primitivo)*
*Sea E una extensión separable finita de un campo infinito F. Entonces existe $\alpha \in E$ tal que $E = F(\alpha)$ (dicho elemento α se llama el **elemento primitivo**). Esto es, una extensión separable finita de un campo infinito es una extensión simple.*

Demostración. Lo probaremos para el caso que $E = F(\beta, \gamma)$. El razonamiento de inducción es claro.
$[E : F] < \infty \Rightarrow E$ es algebraico sobre F, entonces existen los polinomios

$$irr(\beta, F),\ irr(\gamma, F)$$

Sean $\beta = \beta_1, \cdots, \beta_n$, todos los ceros distintos de $irr(\beta, F)$ en $\overline{F}$, y sean $\gamma = \gamma_1, \cdots, \gamma_n$ todos los ceros distintos de $irr(\gamma, F)$ en $\overline{F}$.
Dado que E es separable sobre F, por el corolario 2.11.7 y por la observación 2.11.2 todos los ceros de $irr(\beta, F)$ y de $irr(\gamma, F)$ son de multiplicidad 1.
Como F es infinito, entonces existe $a \in F$ tal que

$$a \neq \frac{(\beta_i - \beta)}{(\gamma - \gamma_j)} \in \overline{F}\ \forall\ i, j\ con\ j \neq 1.$$

$$\Rightarrow \beta + a\gamma \neq \beta i + a\gamma_j\ \ \forall\ \ i, j\ con\ j \neq 1$$

(pues $\beta + a\gamma = \beta_i + a\gamma_j \Rightarrow \beta_i - \beta = a\gamma - a\gamma_j \Rightarrow a = \frac{\beta_i - \beta}{\gamma - \gamma_j}$!).
Sea

$$\alpha = \beta + a\gamma \neq \beta_i + a\gamma_j \qquad \textbf{(I)}$$

$$\Rightarrow \alpha - a\gamma_j \neq \beta_i\ \forall\ i, j\ con\ j \neq 1 \qquad \textbf{(II)}$$

Sea

$$f(x) = irr(\beta, F) \in F[x],$$

y sea

$$h(x) = f(\alpha - ax) \in F(\alpha)[x].$$

$$\begin{aligned} \Rightarrow h(\gamma) &= f(\alpha - a\gamma) \\ &= f((\beta + a\gamma) - a\gamma)\ por\ \textbf{(I)} \\ &= f(\beta) = 0 \end{aligned}$$

pero por construcción

$$h(\gamma_j) = f(\alpha - a\gamma_j) \neq 0\ \ \forall\ i, j\ con\ j \neq 1.$$

(por **(II)** y por que los β_i son todos los ceros distintos de $f(x) = irr(\beta, F)$)

$$\therefore h(\gamma_j) \neq 0 \quad \forall\, j \neq 1,$$

por tanto, el polinomio $h(x) \in F(\alpha)[x]$ sólo tiene un cero en común en $\overline{F}$ con $irr(\gamma, F) \in F[x] \subseteq F(\alpha)[x]$, el cual es γ.
Por el teorema 1.7.1

$$irr(\gamma, F(\alpha))|h(x) \in F(\alpha)[x] \;\; y \;\; irr(\gamma, F(\alpha))|irr(\gamma, F) \in F(\alpha)[x].$$

$\Rightarrow irr(\gamma, F(\alpha)) \in F(\alpha)[x]$ debe ser un polinomio lineal en $F(\alpha)[x]$ pues $h(x)$ y $irr(\gamma, F)$ solo tienen a γ como cero en común en $\overline{F}$. Dado que $irr(\gamma, F(\alpha))$ es también mónico $\Rightarrow irr(\gamma, F(\alpha)) = x - \gamma \in F(\alpha)[x] \Rightarrow \gamma \in F(\alpha)$

$$\Rightarrow F(\alpha, \gamma) \subseteq F(\alpha),$$

y siempre se tiene que

$$F(\alpha) \subseteq F(\alpha, \gamma) \therefore F(\alpha) = F(\alpha, \gamma).$$

Sólamente resta probar que $F(\alpha, \gamma) = F(\beta, \gamma)$. Recordaremos que $\alpha = \beta + a\gamma$
($\subseteq$) Notemos que

$$\alpha = \beta + a\gamma \in F(\beta, \gamma) \;\; pues\; a \in F$$

$\therefore F(\beta, \gamma)$ es un campo que contiene a F, γ y α.

$$\therefore F(\alpha, \gamma) \subseteq F(\beta, \gamma)$$

($\supseteq$) Notemos que

$$\beta = \alpha - a\gamma \in F(\alpha, \gamma) \;\; pues\; a \in F.$$

Así $F(\alpha, \gamma)$ es un campo que contiene a F, γ y β

$$\therefore F(\beta, \gamma) \subseteq F(\alpha, \gamma),$$
$$\therefore F(\beta, \gamma) = F(\alpha, \gamma) = F(\alpha)$$
$$\therefore E = F(\beta, \gamma) = F(\alpha),$$

con esto se concluye que E es una extensión simple de F. ■

Corolario 2.13.2 *Una extensión finita de un campo de característica cero es una extensión simple.*

Demostración. Sea F un campo de característica cero y E extensión de F tal que $[E : F] < \infty$. Dado que F es un campo de característica cero entonces $\mathbb{Q} \subseteq F$ y por tanto, F es un campo infinito. También dado que F es de característica cero, por el teorema 2.12.3 F es un campo perfecto, es decir, toda extensión finita de F es separable, y por el teorema 2.13.1 $E = F(\alpha)$ para algún $\alpha \in E$. ■

2.14. Campos finitos.

El objetivo de esta sección es demostrar que dado cualquier primo p y dado cualquier entero positivo n, existe exactamente un campo finito (salvo isomorfismo) de orden p^n. Denotaremos a este campo $CG(p^n)$ y lo llamaremos el campo de Galois de orden p^n.

2.14.1. Estructura de un campo finito.

Teorema 2.14.1 *Sea E una extensión finita de un campo F de grado n, es decir $[E : F] = n < \infty$. Si F tiene q elementos entonces E tiene q^n elementos.*

Demostración. Sea $\{\alpha_1, \cdots, \alpha_n\}$ una base para E sobre F. Entonces cada $\beta \in E$ puede escribirse de manera única como

$$\beta = b_1\alpha_1 + \cdots + b_n\alpha_n^n \text{ con } b_i \in F$$

dado que cada b_i tiene q posibles formas de elegirse en F, entonces el número total de dichas combinaciones lineales es q^n, por tanto, $|E| = q^n$. ■

Corolario 2.14.2 *Sea E un campo finito de característica p, entonces E contiene exactamente p^n elementos para algún entero positivo n.*

Demostración. Tenemos que dado que E es de característica p, entonces por el corolario 1.2.13 $\mathbb{Z}_p \subseteq E$. El conjunto total de elementos de E es un conjunto finito de generadores de E sobre $\mathbb{Z}_p$ (para cada $e \in E$, $e = 1 \cdot e$ para $1 \in \mathbb{Z}_p$ y $e \in E$) $\therefore [E : \mathbb{Z}_p] = n < \infty$ para algún n. Dado que $|\mathbb{Z}_p| = p$ y por el teorema 2.14.1 se tiene que $|E| = p^n$ para algún n. ■

El siguiente teorema mostrará como puede construirse cualquier campo finito a partir del subcampo primo $\mathbb{Z}_p$.

Teorema 2.14.3 *Un campo finito E de p^n elementos es el campo de descomposición del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ sobre $\mathbb{Z}_p$ (salvo isomorfismos). Aún más*

$$E = \{a \in \overline{\mathbb{Z}_p} | a \text{ es cero de } x^{p^n} - x \in \mathbb{Z}_p[x]\}.$$

Demostración. Sea E un campo finito con p^n elementos donde p es la característica de E (véase el corolario 2.14.2).
Sea $E^* = E - \{0\}$. Entonces E^* es un grupo abeliano multiplicativo (por la afirmación 2.5.13) tal que, $|E^*| = p^n - 1$. Por teoría de grupos, tenemos que

para cualquier $\alpha \in E^*$ se tiene que α elevado al orden del grupo E^* es igual a 1, es decir, $\alpha^{p^n-1} = 1 \ \forall \ \alpha \in E^*$,

$$\Rightarrow \alpha^{p^n} = \alpha \ \forall \ \alpha \in E^* \Rightarrow \alpha^{p^n} - \alpha = 0 \ \ \forall \ \alpha \in E^*$$

Así, $\forall \ \alpha \in E^*$ tenemos que α es cero del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$. Notemos que $0 \in E$ también es cero del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x] \ \therefore \ \alpha$ es cero del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x] \ \forall \ \alpha \in E. \ \therefore \ E \subseteq \{a \in \overline{\mathbb{Z}_p} |\ a$ es cero de $x^{p^n} - x \in \mathbb{Z}_p[x]\}$. Además $\mathbb{Z}_p \subseteq E$ pues E es de caractarística p.
Pero $|E| = p^n$ y $x^{p^n} - x$ tiene a lo más p^n ceros en cualquier campo de extensión.
$\therefore \ E = \{a \in \overline{\mathbb{Z}_p} |\ a$ es cero de $x^{p^n} - x \in \mathbb{Z}_p[x]\}$. Así, E es un campo que contiene a $\mathbb{Z}_p$ y a todos los ceros de $\mathbb{Z}_p$. Sea E' el campo de descomposición de $x^{p^n} - x \in \mathbb{Z}_p[x]$, así, por defincón de E', $E' \subseteq E$. Pero por otra parte por definición de E', $\{a \in \overline{\mathbb{Z}_p} |\ a$ es cero de $x^{p^n} - x \in \mathbb{Z}_p[x]\} \subseteq E'$

$$\therefore E = E' = \{a \in \overline{\mathbb{Z}_p} |\ \ a \ \ es \ \ cero \ \ de \ \ x^{p^n} - x\}.$$

■

Definición 2.14.4 *Sea F un campo. Un elemento $\alpha \in F$ se llama una* ***raíz $n-$ésima del unitario*** *si $\alpha^n = 1$. α se llama una* ***raíz n-ésima primitiva del unitario*** *si $\alpha^n = 1$ y $\alpha^m \neq 1$ para $0 < m < n$.*

Observación 2.14.5 *Si E es un campo de característica p finito (y por tanto, por el corolario 2.14.2 E tiene p^n elementos para algún n), entonces todos los elementos de $E^* = E - \{0\}$ son todas las raíces $(p^n - 1)-$ésimas del unitario.*

Demostración. E^* es grupo y $|E^*| = p^n - 1$,

$$\Rightarrow \alpha^{|E^*|} = 1 \ \forall \ \alpha \in E^* \Rightarrow \alpha^{p^n-1} = 1 \ \forall \ \alpha \in E^*.$$

■

Observación 2.14.6 *Sea F cualquier campo y sea U_n el conjunto de todas las raíces n-ésimas del unitario en F. Entonces U_n es un grupo bajo la multiplicación del campo F.*

Demostración. Notemos que $U_n \subseteq F^*$, pues $a \in U_n \Rightarrow a^n = 1 \Rightarrow a \cdot a^{n-1} = 1 \Rightarrow a$ es unidad, por lo que, $a \in F^*$. Demostraremos que U_n es un subgrupo

de $F^* = F - \{0\}$.

$$\begin{aligned} \textit{Sean } a, b \in U_n \Rightarrow (ab)^n &= a^n b^n \textit{ pues } F^* \textit{ es grupo abeliano} \\ &= 1 \cdot 1 \textit{ pues } a^n = 1 \textit{ y } b^n = 1 \\ &\Rightarrow ab \in U_n \end{aligned}$$

Sea $a \in U_n \Rightarrow a^n = 1 \Rightarrow 1 = (a^n)^{-1} a^n = (a^n)^{-1} \cdot 1 \Rightarrow 1 = (a^{-1})^n \therefore a^{-1} \in U_n$.
$\therefore U_n$ es grupo multiplicativo (abeliano). ■

En la demostración del siguiente teorema utilizaremos el **teorema de grupos abelianos finitamente generados** que aqui presentamos sin demostración.

Teorema fundamental de los grupos abelianos finitamente generados: Todo grupo abeliano finitamente generado G es isomorfo al producto directo de los grupos cíclicos de la forma:

$$Z_{(p_1)^{r_1}}, \times Z_{(p_2)^{r_2}} \times \cdots \times Z_{(p_n)^{r_n}} \times Z \times Z \times \cdots \times Z$$

donde las p_i son primos, no necesariamente distintos, y también es isomorfo a un producto de la forma:

$$Z_{m_1}, \times Z_{m_2} \times \cdots \times Z_{m_r} \times Z \times Z \times \cdots \times Z,$$

donde las m_i dividen a m_{i+1}.
En ambos casos el producto directo es único, excepto por posibles rearreglos de los factores, esto es, el número de factores de Z es único. Los coeficientes de torsión m_i de G son únicos y las potencias de primos $(p_i)^{r_i}$ son únicas.

Demostración. Para la demostración ver [1] pp.(184-189). ■

Teorema 2.14.7 *Si G es un subgrupo finito multiplicativo del grupo multiplicativo $\langle F^*, \cdot \rangle$ de los elementos distintos de cero de un campo F, entonces G es cíclico.*

Demostración. Dado que G es un grupo abeliano finito, tenemos por **el teorema fundamental de los grupos abelianos finitamente generados**, que G es isomorfo a un producto directo de grupos cíclicos.

$G \cong Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_r}$, $m_i | m_{i+1}$ $\forall$ i y algún r tal que $1 \leqslant r < \infty$.

Pensemos que cada Z_{m_i} es un grupo de orden m_i en notación multiplicativa. Entonces dado cualquier $a_i \in Z_{m_i} \Rightarrow a_i^{m_i} = 1 \Rightarrow a_i^{m_r} = 1$, pues $m_i | m_r$, $\forall\ i$. Así, dado

$$(a_1, a_2, \cdots, a_r) \in Z_{m_1}, \times Z_{m_2} \times \cdots \times Z_{m_r} \textit{ un elemento arbitrario},$$

tenemos que

$$(a_1, a_2, \cdots, a_r)^{m_r} = (a_1^{m_r}, a_2^{m_r}, \cdots, a_r^{m_r}) = (1, 1, \cdots, 1) = 1.$$

Usando el isomorfismo

$$G \cong Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_r}$$

en G, lo anterior se traduce a lo siguiente. Dado $\alpha \in G$ arbitrario

$$\Rightarrow \alpha^{m_r} = 1 \Rightarrow \alpha^{m_r} - 1 = 0,$$

entonces para todo $\alpha \in G$ tenemos que α es cero del polinomio $x^{m_r} - 1 \in F[x]$. Dado que $x^{m_r} - 1$ a lo más m_r ceros en cualquier campo de extensión de F, entonces $|G| \leqslant m_r$ para algún r, tal que, $1 \leqslant r < \infty$.
Por otra parte tenemos que

$$\begin{aligned} |G| &= |Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_r}| \\ &= |Z_{m_1}||Z_{m_2}| \cdots |Z_{m_r}| \\ &= \Pi_{i=1}^{r} m_i \end{aligned}$$

Así

$$|G| \leqslant m_r \ \ y \ \ |G| = \Pi_{i=1}^{r} m_i \Rightarrow r = 1$$

$\therefore G \cong Z_{m_1}$, por tanto, G es cíclico finito. ■

Corolario 2.14.8 *El grupo multiplicativo de todos los elementos distintos de cero de un campo finito bajo la multiplicación del campo es cíclico.*

Demostración. Inmediato del teorema 2.14.7. ■

Corolario 2.14.9 *Una extensión finita E de un campo finito F es una extensión simple de F.*

Demostración. Por el teorema 2.14.1 y como $[E : F] < \infty$ y F es finito, entonces tenemos que E es un campo finito. Entonces por el corolario 2.14.8

tenemos que $E - \{0\} = E^*$ es un grupo cíclico finito.
Sea α un generador del grupo cíclico finito E^*,

$$\Rightarrow E^* = \{\alpha^0, \alpha^1, \cdots, \alpha^k\} \quad \Rightarrow \quad E = \{0, \alpha^0, \alpha^1, \cdots, \alpha^k\} \subseteq F(\alpha)$$

pero también tenemos que $F(\alpha) \subseteq E$ pues E contiene a F y a α

$$\therefore E = F(\alpha).$$

■

Para el siguiente ejemplo necesitaremos el **teorema de Lagrange**. Recordemos su enunciado:

Teorema de Lagrange: Sea G un grupo de orden finito y sea H un subgrupo de G entonces el orden de H divide al orden de G.

Observación 2.14.10 *a es un generador de algún subgrupo H de orden k de $\mathbb{Z}_{11}^* \Leftrightarrow$ a es raíz k-ésima primitiva de la unidad.*

Demostración. ($\Rightarrow$) Sea a generador de H donde H es un subgrupo de $\mathbb{Z}_{11}^*$ de orden k, entonces $a^m \neq 1 \ \forall \ 0 < m < k$ (de lo contrario a no sería generador de H).

($\Leftarrow$) Tenemos que $a^k = 1$ y $a^m \neq 1 \ \forall \ 0 < m < k$. Notemos que $m_1 \neq m_2$ con $0 < m_1 < m_2 < k \Rightarrow a^{m_1} \neq a^{m_2}$ (pues $a^{m_1} = a^{m_2} \Rightarrow a^{m_2 - m_1} = 1$ con $0 < m_2 - m_1 < k$, contradicción. $\therefore a^{m_1} \neq a^{m_2}$.) $\Rightarrow |\langle a \rangle| = k \therefore a$ genera a un subgrupo de orden k de $\mathbb{Z}_{11}^*$. ■

Ejemplo 2.14.11 *Consideremos el campo finito $\mathbb{Z}_{11}$. Por el corolario 2.14.8 se tiene que $\langle \mathbb{Z}_{11}^*, \cdot \rangle$ es un grupo cíclico finito.*
Encontremos un generador de $\mathbb{Z}_{11}^*$ a prueba y error. Intentemos con $\overline{2} \in \mathbb{Z}_{11}^*$. Dado que $|\mathbb{Z}_{11}^*| = 10$ por el teorema de Lagrange

$$\circ(\overline{2}) | 10 \Rightarrow \circ(\overline{2}) = 2, 5 \text{ ó } 10$$

pero

$$2^2 = 4 \neq 1, 2^5 = \overline{2^4} \cdot \overline{2} = \overline{16} \cdot \overline{2} = \overline{5} \cdot \overline{2} = \overline{10} \neq 1 \text{ en } \mathbb{Z}_{11},$$

por tanto, $\circ(2) = 10 \Rightarrow \langle 2 \rangle = \mathbb{Z}_{11}^* \therefore 2 \in \mathbb{Z}_{11}^*$ es un generador de $\mathbb{Z}_{11}^*$.

Recordaremos ahora dos resultados de la teoría de grupos cíclicos:

***Teorema**: Sea G grupo cíclico con n elementos generado por a. Sea $b \in G$ y sea $b = a^s$. Entonces b genera un subgrupo cíclico H de G con $\frac{n}{d}$ elementos donde d es el m.c.d de n y s, es decir, $(n, s) = d$.*

***Corolario**: Si a es un generador de un grupo cíclico finito G de orden n, entonces los otros generadores de G son elementos de la forma a^r donde r y n son primos relativos $((r, n) = 1)$.*

Usando el corolario anterior tenemos que todos los generadores del grupo cíclico $\mathbb{Z}_{11}^*$ son a^r donde $a = 2$ y $(r, 10) = 1 \Rightarrow r = 1, 3, 7$ y 9.
Entonces todos los generadores de $\mathbb{Z}_{11}^*$ son

$$\overline{2}^1 = \overline{2}, \quad \overline{2}^3 = \overline{8}, \quad \overline{2}^7 = \overline{7}, \quad \overline{2}^9 = \overline{6} \text{ en } \mathbb{Z}_{11}$$

es decir, todas las raíces décimas primitivas del unitario en $\mathbb{Z}_{11}$ son:

$$\overline{2}, \overline{6}, \overline{7}, \overline{8}.$$

Por el teorema enunciado anteriormente en este ejemplo y la observación 2.14.10 tenemos que las raíces quintas primitivas del unitario en $\mathbb{Z}_{11}$ son de la forma $b = a^s$, donde $a = 2$, $n = 10$, $\frac{n}{d} = 5$ y $(n, s) = d$. Es decir, $\frac{10}{d} = 5 \Rightarrow d = 2$, entonces los generadores b de los subgrupos cíclicos H de orden 5 de $\mathbb{Z}_{11}^*$ son tales que $b = 2^s$ con $(10, s) = 2 \Rightarrow s = 2, 4, 6$ y 8. Así por la observación 2.14.10 el total de raíces quintas primitivas del unitario de $\mathbb{Z}_{11}$ son:

$$\overline{2}^2 = \overline{4}, \quad \overline{2}^4 = \overline{5}, \quad \overline{2}^6 = \overline{9}, \quad \overline{2}^8 = \overline{3} \text{ en } \mathbb{Z}_{11}$$

es decir, son

$$\overline{3}, \overline{4}, \overline{5}, \overline{9} \text{ en } \mathbb{Z}_{11}$$

La raíz cuadrada del unitario en $\mathbb{Z}_{11}$ sería $b = a^s$ donde $a = 2$, $n = |\mathbb{Z}_{11}^*| = 10$, $\frac{n}{d} = 2$ y $(n, s) = d$, entonces serían los $b = 2^s$ con s tal que $(10, s) = 5$. $\Rightarrow s = 5$. Así, $b = 2^5 = \overline{10}$ sería la única raíz cuadrada primitiva de la unidad.

2.15. La existencia de $CG(p^n)$.

Pasaremos ahora a la cuestión de la existencia de un campo finito de orden p^r para toda potencia de un primo p, con $r > 0$. Para ello necesitamos el siguiente

Lema 2.15.1 *Sea F un campo de característica p y sea $n > 0$, entonces $x^{p^n} - x$ tiene p^n ceros distintos en el campo de descomposición K (K subcampo de $\overline{F}$) de $x^{p^n} - x$ sobre F.*

Demostración. Demostraremmos que $x^{p^n} - x$ tiene p^n ceros distintos en K. Primero notemos que $0 \in F \leqslant K$ es un cero de multiplicidad 1 de $x^{p^n} - x$ (pues $x^{p^n} - x = x(x^{p^n} - 1)$ y 0 no es cero de $x^{p^{n-1}} - 1$).
Sea α $(\alpha \neq 0)$ un cero del polinomio $x^{p^n-1} - 1$, veamos que α debe ser de multiplicidad 1 y habremos terminado.

Como α ($\alpha \neq 0$) es cero del polinomio $x^{p^n-1} - 1$ tenemos por el corolario 1.3.2 que $(x - \alpha)$ es un factor de $x^{p^n-1} - 1$ en $K[x]$.
Dividiendo $x^{p^n-1} - 1$ por $(x - \alpha)$ tenemos

$$
\begin{array}{l|l}
 & x^{(p^n-1)-1} + \alpha^1 x^{(p^n-1)-2} + \alpha^2 x^{(p^n-1)-3} + \cdots + \alpha^{p^n-3} x^{(p^n-1)-(p^n-3+1)} + \alpha^{p^n-2} x^{(p^n-1)-(p^n-2+1)} \\
x - \alpha & x^{p^n-1} - 1 \\
 & \underline{-(x^{p^n-1} - \alpha x^{(p^n-1)-1})} \\
 & \alpha x^{(p^n-1)-1} - 1 \\
 & \underline{-(\alpha x^{(p^n-1)-1} - \alpha^2 x^{(p^n-1)-2})} \\
 & \alpha^2 x^{(p^n-1)-2} - 1 \\
 & \underline{-(\alpha^2 x^{(p^n-1)-2} - \alpha^3 x^{(p^n-1)-3})} \\
 & \alpha^3 x^{(p^n-1)-3} - 1 \\
 & \vdots \\
 & \underline{\alpha^{p^n-2} x^{(p^n-1)-(p^n-2)} - 1} \\
 & -(\alpha^{p^n-2} x^{(p^n-1)-(p^n-2)} - \alpha^{p^n-1} x^{(p^n-1)-(p^n-1)}) \\
 & \alpha^{p^n-1} x^0 - 1 = \alpha^{p^n-1} - 1 = 0 \text{ pues } \alpha \text{ es cero de } x^{p^n-1}
\end{array}
$$

Así, el polinomio $g(x)$ dado por el cociente

$$g(x) = \tfrac{x^{p^n-1}-1}{x-\alpha} \textit{ es tal que}$$
$$g(x) = x^{(p^n-1)-1} + \alpha^1 x^{(p^n-1)-2} + \alpha^2 x^{(}p^n - 1) - 3 + \cdots + \alpha^{p^n-3} x^{(p^n-1)-(p^n-3+1)} + \alpha^{p^n-2} x^{(p^n-1)-(p^n-2+1)}$$

$g(x)$ tiene $(p^n - 1)$ sumandos y en $g(\alpha)$ cada sumando es

$$\alpha^i x^{(p^n-1)-(i+1)}|_\alpha = \alpha^i \alpha^{(p^n-1)-(i+1)} = \alpha^{p^n-2} = \frac{\alpha^{p^n} - 1}{\alpha} = \frac{1}{\alpha} \quad \forall\, i = 0, \cdots, p^n - 2$$

donde la última igualdad es porque α es cero de

$$x^{p^n-1} - 1 \Rightarrow \alpha^{p^n-1} - 1 = 0 \Rightarrow \alpha^{p^n-1} = 1$$

$$\Rightarrow g(\alpha) = [(p^n - 1) \cdot 1]\frac{1}{\alpha}$$

Dado que F es de característica p, entonces $p^n \cdot 1 = 0$

$$\Rightarrow g(\alpha) = [(p^n - 1) \cdot 1]\frac{1}{\alpha} = [(p^n \cdot 1) - (1 \cdot 1)]\frac{1}{\alpha} = [0 - (1 \cdot 1)]\frac{1}{\alpha} = -\frac{1}{\alpha} \neq 0$$

Así hemos demostrado que cualquier cero α de $x^{p^n-1} - 1$ es de multiplicidad 1 en el campo de descomposición $K \leqslant \overline{F}$ de $x^{p^n} - x$. ■

Teorema 2.15.2 *Dado p un primo y $n > 0$, existe un campo finito $CG(p^n)$ de p^n elementos. Aún más, podemos tomar*

$$CG(p^n) = \{a \in \overline{\mathbb{Z}_p} | a \text{ es cero de } x^{p^n} - x \in \mathbb{Z}_p[x]\}$$

que es un campo de descomposición de $x^{p^n} - x \in \mathbb{Z}_p[x]$ sobre $\mathbb{Z}_p$.

Demostración. Sea K subcampo de $\overline{\mathbb{Z}_p}$ tal que K es el campo de descomposición del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ sobre $\mathbb{Z}_p$. Por definición K es el menor subcampo de $\overline{\mathbb{Z}_p}$ tal que K contiene a $\mathbb{Z}_p$ y a todos los ceros en $\overline{\mathbb{Z}_p}$ del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$.
Sea F el conjunto

$$F = \{a \in \overline{\mathbb{Z}_p} | a \text{ es cero de } x^{p^n} - x\},$$

entonces, por la definición de K se tiene

$$F \subseteq K.$$

Dado que $\mathbb{Z}_p$ tiene característica p, el lema 2.15.1 nos dice que $x^{p^n} - x$ tiene p^n ceros distintos en el campo K de descomposición ($K \leqslant \overline{\mathbb{Z}_p}$) sobre $\mathbb{Z}_p$ del polinomio $x^{p^n} - x$. Así, por definición del conjunto F, se tiene

$$|F| = p^n \qquad \textbf{(I)}$$

Por otra parte afirmamos que F es subcampo de K. Sean $\alpha, \beta \in F$

$$\begin{aligned} \Rightarrow (\alpha \pm \beta)^{p^n} &= \alpha^{p^n} \pm \beta^{p^n} && \text{pues } Char(K) = Char(\mathbb{Z}_p) = p \\ &= \alpha \pm \beta && \text{pues } \alpha, \beta \in F \end{aligned}$$

$$\Rightarrow (\alpha \pm \beta)^{p^n} - (\alpha \pm \beta) = 0 \Rightarrow \alpha \pm \beta \in F$$

también

$$\begin{aligned}(\alpha\beta)^{p^n} &= \alpha^{p^n}\beta^{p^n} \\ &= \alpha\beta \text{ pues } \alpha, \beta \in F\end{aligned}$$

$$\Rightarrow (\alpha\beta)^{p^n} - \alpha\beta = 0 \Rightarrow \alpha\beta \in F.$$

Además $0, 1 \in F$, pues $0, 1 \in \mathbb{Z}_p$ son cero de $x^{p^n} - x$.
También sea $0 \neq \alpha \in F \Rightarrow \alpha^{p^n} - \alpha = 0 \Rightarrow \alpha^{p^n} = \alpha \neq 0 \Rightarrow \frac{1}{\alpha^{p^n}} = \frac{1}{\alpha} \Rightarrow (\frac{1}{\alpha})^{p^n} = \frac{1}{\alpha} \Rightarrow (\frac{1}{\alpha})^{p^n} - (\frac{1}{\alpha}) = 0 \Rightarrow \frac{1}{\alpha} \in F \therefore F$ es subcampo de K y dado que $1 \in F$ $(1 \in \mathbb{Z}_p) \Rightarrow \mathbb{Z}_p \leqslant F$.
Así tenemos que

$$\mathbb{Z}_p \leqslant F \leqslant K \leqslant \overline{\mathbb{Z}}_p.$$

Dado que por definición $K \leqslant \overline{\mathbb{Z}}_p$ es el menor subcampo de $\overline{\mathbb{Z}}_p$ que contiene a $\mathbb{Z}_p$ y al conjunto de todos los ceros de $x^{p^n} - x$ y por otra parte F es el conjunto de todos los ceros de $x^{p^n} - x$, $\mathbb{Z}_p \subseteq F$ y F es campo, entonces $F = K$. Pero por **(I)** tenemos que $|F| = p^n$, por tanto, $|K| = p^n$ y así K es el campo buscado donde

$$K = F = \{a \in \overline{\mathbb{Z}}_p | a \text{ es cero de } x^{p^n} - x\}.$$

■

Corolario 2.15.3 *Sea F un campo finito cualquiera. Dado n un entero positivo cualquiera existe un polinomio irreducible en $F[x]$ de grado n.*

Demostración. F es un campo finito, por lo que la característica de F es p, para algún p primo. Por el corolario 2.14.2, se tiene que $|F| = p^r$ para algún entero positivo r. También dado que F es de característica p, entonces $\mathbb{Z}_p$ es subcampo de F. Tenemos que F es finito, por lo que $[F : \mathbb{Z}_p] < \infty$ y así, por el teorema 2.3.2 F es una extensión algebraica sobre $\mathbb{Z}_p$, y por lo tanto:

$$\mathbb{Z}_p \leqslant F \leqslant \overline{F} \leqslant \overline{\mathbb{Z}}_p$$

Por el teorema 2.15.2 se tiene que:

$$K = \{a \in \overline{\mathbb{Z}_p} | a \text{ es cero de } x^{p^{nr}} - x\}$$

es un subcampo de $\overline{\mathbb{Z}}_p$, tal que, $|K| = p^{nr}$. Además por ser K subcampo de $\overline{\mathbb{Z}}_p$ y $\overline{\mathbb{Z}}_p$ de característica p, entonces K es de característica p y por tanto $\mathbb{Z}_p$ es subcampo de K.

Por otra parte, dado que F es un campo finito con $|F| = p^r$ y por el teorema 2.14.3

$$\Rightarrow F = \{\alpha \in \overline{\mathbb{Z}}_p | \alpha \text{ es cero de } x^{p^r} - x\} \quad \textbf{(I)}$$

Veamos que F es un subcampo de K.
Usando que $p^{rs} = p^r \cdot p^{r(s-1)}$, que $\alpha \in F$ y que por **(I)** $\alpha^{p^r} = \alpha$ tenemos que

$$\begin{aligned}
\alpha^{p^{rn}} &= \alpha^{p^r \cdot p^{r(n-1)}} \\
&= (\alpha^{p^r})^{p^{r(n-1)}} \\
&= \alpha^{p^{r(n-1)}} \\
&= \alpha^{p^r \cdot p^{r(n-2)}} \\
&= (\alpha^{p^r})^{p^{r(n-2)}} \\
&= \alpha^{p^{r(n-2)}} \\
&\vdots \\
&= \alpha^{p^{r(n-(n-1))}} \\
&= \alpha^{p^r} \\
&= \alpha
\end{aligned}$$

Por tanto, $\alpha^{p^{rn}} - \alpha = 0 \Rightarrow \alpha \in K$, lo que implica que F es subcampo de K y así tenemos que

$$\mathbb{Z}_p \leqslant F \leqslant K \leqslant \overline{\mathbb{Z}}_p.$$

Ahora, dado que $|K| = p^{nr}$ tenemos que K es un campo finito y entonces $[K : F] < \infty$, es decir, tenemos que $[K : F] = m$ para algún $m > 0$, y dado que $|F| = p^r$ tenemos por el teorema 2.14.1 que

$$|K| = p^{rm}$$

por tanto

$$p^{rm} = p^{rn} \Rightarrow m = n \quad \therefore \quad [K : F] = n.$$

También dado que $[K : F] = n < \infty$, F es finito y por el corolario 2.14.9, K es una extensión simple de $F \Rightarrow K = F(\beta)$ para algún $\beta \in K$. Así se tiene por el corolario 2.1.4

$$grad(\beta, F) = [F(\beta) : F]$$

$$\Rightarrow grad(\beta, F) = [F(\beta) : F] = [K : F] = n$$

entonces $grad(\beta, F) = n$ por tanto $irr(\beta, F)$ es un polinomio irreducible en $F[x]$ de grado n. ■

Capítulo 3

Teoría de Galois.

3.1. Extensiones normales.

Estaremos interesados en extensiones finitas K de F tales que se cumple

$$|G(K/F)| = \{K : F\} = [K : F]$$

La primera igualdad ya vimos que se cumple $\Leftrightarrow$ K es campo de descomposición sobre F y la segunda igualdad es la definición de que K sea una extensión separable sobre F.
Así, definimos

Definición 3.1.1 *Una extensión finita K de F es una* ***extensión normal finita*** *de F si K es un campo de descomposición separable de F.*

$$|G(K/F)| = \{K : F\} = [K : F].$$

Teorema 3.1.2 *Sea K una extensión normal finita de F y sea E una extensión de F, tal que $F \leqslant E \leqslant K \leqslant \overline{F}$. Entonces K es una extensión normal finita de E y $G(K/E)$ es un subgrupo de $G(K/F)$. Además σ y τ en $G(K/F)$ inducen el mismo monomorfismo de E en $\overline{F}$ (es decir, $\sigma|_E = \tau|_E : E \rightarrowtail \overline{F}$) si y sólo si $\overline{\tau} = \overline{\sigma}$ en el conjunto de clases laterales derechas $G(K/F)/G(K/E)$.*

Demostración. K es extensión normal finita sobre F, en particular por definición K es campo de descomposición de un conjunto $\{f_i(x)|i \in I\}$ en $F[x]$.

Entonces por definición K es el menor subcampo de $\overline{F}$ que contiene a F y a todos los ceros en $\overline{F}$ de la colección $\{f_i(x)|i \in I\} \subseteq F[x]$ **(I)**

Dado que $F \subseteq E$ podemos considerar la colección $\{f_i(x)|i \in I\}$ como subconjunto de $E[x]$. Afirmamos que K es campo de descomposición sobre E

de la colección $\{f_i(x)|i \in I\} \subseteq E(x)$.
En efecto pues sea $K' \leqslant \overline{F}$ el campo de descomposición de la colección $\{f_i(x)|i \in I\} \subseteq E[x]$ sobre E, entonces por definición tenemos que K' es el menor subcampo de $\overline{F}$ que contiene a E y a los ceros en $\overline{F}$ de $\{f_i(x)|i \in I\} \subseteq E[x]$. Dado que por hipótesis $E \subseteq K$, entonces por **(I)**

$$K' \subseteq K.$$

Por otra parte, por hipótesis $F \subseteq E$, entonces K' contiene a F y a los ceros en $\overline{F}$ de $\{f_i(x)|i \in I\} \subseteq E[x]$ así por **(I)**

$$K \subseteq K'$$

por tanto,

$$K = K'$$

por lo que K es campo de descomposición sobre E de la colección

$$\{f_i(x)|i \in I\} \subseteq E[x].$$

Ahora veamos que K es separable sobre E.
Por hipótesis K es una extensión normal finita de F, por lo que K es separable sobre F y $[K : F] < \infty$. Dado que también por hipótesis

$$F \leqslant E \leqslant K$$

entonces tenemos que $[E : F] < \infty$ y $[K : E] < \infty$. Por el teorema 2.11.5 K es separable sobre E.
En conclusión K es campo de descomposición sobre E y K es separable sobre E. Entonces por definición K es extensión normal finita de E.

Veamos que $G(K/E)$ es subgrupo de $G(K/F)$.

Sea $\sigma \in G(K/E) = \{\sigma \in Aut(K)|\sigma|_E = Id\}$. Como $F \subseteq E$ y como $\sigma|_E = Id, \Rightarrow \sigma|_F = Id, \Rightarrow \sigma \in \{\sigma \in Aut(K)|\sigma|_F = Id\} = G(K/F)$, por lo que

$$G(K/E) \subseteq G(K/F)$$

Por el teorema 2.5.18 tenemos que $G(K/E)$ también es un grupo bajo la composición de funciones, entonces

$$G(K/E) \textit{ es subgrupo de } G(K/F).$$

Veamos que σ y τ en $G(K/F)$ inducen el mismo monomorfismo de E en $\overline{F} \Leftrightarrow \overline{\tau} = \overline{\sigma}$ en $G(K/F)/G(K/E)$.

($\Rightarrow$) Sean σ, τ en $G(K/F)$, tal que $\overline{\sigma} = \overline{\tau}$ en $G(K/F)/G(K/E)$.
$\Leftrightarrow \tau^{-1}\sigma \in G(K/E) \Leftrightarrow \tau^{-1}\sigma = \mu$ para algún $\mu \in G(K/E) \Rightarrow \sigma = \tau\mu$.
Sea $\alpha \in E$ arbitrario, entonces

$$\begin{aligned} \sigma(\alpha) &= \tau\mu(\alpha) \\ &= \tau(\alpha) \ \ pues\ \mu \in G(K/E) \end{aligned}$$

$$\therefore \sigma(\alpha) = \tau(\alpha)\ \forall\ \alpha \in E$$

$$\Rightarrow \sigma|_E = \tau|_E : E \rightarrowtail \overline{F}.$$

($\Leftarrow$) Supongamos que $\sigma, \tau \in G(K/F)$ son tales que $\sigma|_E = \tau|_E$, $\Rightarrow \sigma(\alpha) = \tau(\alpha)\ \forall\ \alpha \in E \Rightarrow \tau^{-1}\sigma(\alpha) = \tau(\alpha)\ \forall\ \alpha \in E \Rightarrow \tau^{-1}\sigma \in G(K/E) \Leftrightarrow \overline{\tau} = \overline{\sigma} \in G(K/F)/G(K/E)$.

■

Corolario 3.1.3 *Sea K una extensión normal finita de F y sea E extensión de F, tal que $F \leqslant E \leqslant K \leqslant \overline{F}$. Entonces tenemos una biyección*

$$\varphi:\ G(K/F)/G(K/E) \longrightarrow \left\{ \begin{array}{c} \textit{monomorfismos } \tau \textit{ tales que} \\ \textit{el diagrama conmuta} \\ \begin{array}{ccc} E & \overset{\tau}{\rightarrowtail} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \end{array} \end{array} \right\}$$

definida por $\varphi(\overline{\sigma}) = (\sigma|_E : E \rightarrowtail F)$, donde $\sigma \in G(K/F)$, es decir, σ es tal que el diagrama

$$\begin{array}{ccc} K & \overset{\sigma}{\longrightarrow} & K \\ \uparrow & & \uparrow \\ F & = & F \end{array} \qquad \textit{conmuta}$$

Demostración. φ está bien definida; en efecto, sean $\overline{\sigma}, \overline{\tau}$ en $G(K/F)/G(K/E)$ tales que $\overline{\sigma} = \overline{\tau}$, por el teorema 3.1.2 tenemos que

$$\begin{array}{ccccc} \sigma|_E & = & \tau|_E & : E \rightarrowtail \overline{F} \\ \| & & \| & \\ \varphi(\overline{\sigma}) & & \varphi(\overline{\tau}) & \end{array}$$

φ es 1-1; en efecto, supongamos que $\overline{\sigma},\overline{\tau} \in G(K/F)/G(K/E)$ son tales que, $\varphi(\overline{\sigma}) = \varphi(\overline{\tau}) \Rightarrow \sigma|_E = \tau|_E : E \rightarrowtail F$, nuevamente por el teorema 3.1.2 $\overline{\sigma} = \overline{\tau}$ en $G(K/F)/G(K/E)$.
Veamos que φ es sobreyectiva. Sea τ en el contradominio de φ entonces tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} E & \overset{\tau}{\rightarrowtail} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \end{array} \qquad \textbf{(I)}$$

consideremos el isomorfismo $\tau : E \longrightarrow \tau(E)$. Por el teorema de extensión de isomorfismos tenemos que existe τ_K tal que el siguiente diagrama conmuta.

$$\begin{array}{ccc} & & \overline{F} \\ & & \uparrow \\ K & \overset{\tau_K}{\rightarrowtail} & \overline{F} \\ {\scriptstyle alg}\uparrow & & \uparrow \\ E & \underset{\cong}{\overset{\tau}{\longrightarrow}} & \tau(E) \end{array}$$

$$\Rightarrow \quad \begin{array}{ccc} K & \overset{\tau_K}{\rightarrowtail} & \overline{F} \\ {\scriptstyle alg}\uparrow & & \| \\ E & \underset{\cong}{\overset{\tau}{\rightarrowtail}} & \overline{F} \end{array} \qquad \textit{conmuta} \qquad \textbf{(II)}$$

Pegando los diagramas **(I)** y **(II)** tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} \overline{F} & & \\ \uparrow & & \\ K & \overset{\tau_K}{\rightarrowtail} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \end{array} \qquad \textbf{(III)}$$

Dado que por hipótesis $K \leqslant \overline{F}$ es una extensión normal finita de F, entonces por definición K es un campo de descomposición sobre F y dado que **(III)** conmuta tenemos por el corolario 2.9.5 que $\tau_K \in Aut(K) \Rightarrow \tau_K \in G(K/F)$ y así se tiene que, $\overline{\tau}_K \in G(K/F)/G(K/E)$ con $\varphi(\overline{\tau}_K) = \tau_K|_E = \tau$. ■

Nota 3.1.4 *(Respecto al corolario anterior).*
Dado que no necesariamente E es campo de descomposición sobre F no podemos afirmar en el corolario anterior que los monomorfismos de E en $\overline{F}$ que extienden a la identidad en F son automorfismos de E, es decir, no podemos afirmar que tenemos una biyección

$$G(K/F)/G(K/E) \longrightarrow G(E/F).$$

Veremos más adelante que esto acurrirá $\Leftrightarrow G(K/E) \lhd G(K/F)$ o bien, si y sólo si, E es una extensión normal de F. De hecho dicha biyección resultará ser un isomorfismo de grupos.

Definición 3.1.5 *Si K es una extensión finita de un campo F, entonces $G(K/F)$ se llama* ***grupo de Galois*** *de K sobre F.*

Teorema 3.1.6 *(Teorema principal de la teoría de Galois)*
Sea K una extensión normal finita de un campo F, con grupo de Galois $G(K/F)$. Entonces tenemos una biyección

$$\lambda : \{E | F \leqslant E \leqslant K\} \longrightarrow \{H | H \leqslant G(K/F)\}$$
$$E \longmapsto G(K/E)$$

que cumple además:
$2 : E = K_{G(K/E)} \equiv K_{\lambda(E)}$.

3 : *Si H es subgrupo de $G(K/F)$ entonces $\lambda(K_H) = H$.*

$4 : [K : E] = |\lambda(E)| \equiv |G(K/E)|$;
$[E : F] = \{G(K/E) : \lambda(E)\} \equiv \{G(K/F) : G(K/E)\}$, *el número de clases laterales de $\lambda(E) \equiv G(K/E)$ en $G(K/F)$.*

5 : *E es una extensión normal de $F \Leftrightarrow \lambda(E) \equiv G(K/E)$ es un subgrupo normal de $G(K/F)$ $(G(K/E) \lhd G(K/F))$.*

Demostración. 2- En el teorema 2.5.19 demostramos que E es subcampo de $K_{G(K/E)}$. Veamos que $K_{G(K/E)} \subseteq E$.

Sea $\alpha \in K - E$. Demostraremos que existe $\sigma \in G(K/E)$ tal que $\sigma(\alpha) \neq \alpha$ (y así tendremos que $\alpha \notin K_{G(K/E)}$, esto es, que $\alpha \in K - K_{G(K/E)}$, esto es, que $K - E \subseteq K - K_{G(K/E)}$, y dado que $K - E \subseteq K - K_{G(K/E)} \Leftrightarrow K_{G(K/E)} \subseteq E$, tendremos que $K_{G(K/E)} \subseteq E$).

Dado que K es normal sobre F, por el teorema 3.1.2 tenemos que K es normal sobre E entonces por definición K es separable sobre E,pero esto ocurre si y sólo si, α es separable sobre $E\ \forall\ \alpha \in K$ por el corolario 2.11.7. Así, por la observación 2.11.2 el polinomio $irr(\alpha, E)$ tiene todos los ceros en $\overline{F}$ de multiplicidad 1, es decir, todos los ceros en $\overline{F}$ de $irr(\alpha, E)$ son distintos entre sí.
También dado que $\alpha \notin E \Rightarrow grad(\alpha, E) \geqslant 2$.
Sea $\beta \neq \alpha$, tal que β es otro cero en $\overline{F}$ de $irr(\alpha, E)$. Consideremos el isomorfismo

$$\Psi_{\alpha,\beta} : E(\alpha) \longrightarrow E(\beta).$$

Recordemos que $\Psi_{\alpha,\beta}(\alpha) = \beta$ y tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} E(\alpha) & \xrightarrow{\Psi_{\alpha,\beta}} & E(\beta) \\ \uparrow & & \uparrow \\ E & = & E \end{array} \qquad \textbf{(I)}$$

Por el teorema 2.7.1 (teorema de extensión de isomorfismos), se tiene que existe un monomorfismo $\overline{\Psi_{\alpha,\beta}}$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \overline{F} & & \\ \uparrow & & \\ K & \xrightarrow{\overline{\Psi_{\alpha,\beta}}} & \overline{F} \\ \uparrow & & \uparrow \\ E(\alpha) & \xrightarrow{\Psi_{\alpha,\beta}} & E(\beta) \end{array} \qquad \textbf{(II)}$$

Pegando los diagramas **(I)** y **(II)** se obtiene el siguiente diagrama que conmuta

$$\begin{array}{ccc} K & \xrightarrow{\overline{\Psi_{\alpha,\beta}}} & \overline{F} = \overline{E} \\ \uparrow & & \uparrow \\ E & = & E \end{array} \qquad \textbf{(III)}$$

Dado que K es normal sobre $E \Rightarrow K$ es campo de descomposición sobre E y por el corolario 2.9.5 $\Rightarrow \overline{\Psi_{\alpha,\beta}} \in Aut(K)$. Además,

$$\overline{\Psi_{\alpha,\beta}}|_E = Id \ \therefore\ \overline{\Psi_{\alpha,\beta}} \in G(K/E).$$

También tenemos que $\Psi_{\alpha,\beta}(\alpha) = \beta \neq \alpha$, por tanto, $\alpha \notin K_{G(K/E)}$ y así $\alpha \in K - K_{G(K/E)}$, con lo que se tiene

$$K_{G(K/E)} \subseteq E \quad \therefore \quad K_{G(K/E)} = E,$$

es decir,

$$E = K_{\lambda(E)}.$$

para ver que λ es $1-1$ supongamos que $\lambda(E_1) = \lambda(E_2)$

$$\Rightarrow K_{\lambda(E_1)} = K_{\lambda(E_2)}.$$

pero por la propiedad 2 anterior tenemos que

$$E_1 = K_{\lambda(E_1)} = K_{\lambda(E_2)} = E_2,$$
$$\therefore E_1 = E_2 \ \therefore \ \lambda \ es \ 1-1.$$

4.– Dado que K es extensión normal finita sobre E, entonces

$$[K : E] = \{K : E\} = |G(K/E)| \equiv |\lambda(E)|.$$

Por otra parte, por el corolario 3.1.3 tenemos una biyección

$$\varphi : \ G(K/F)/G(K/E) \longrightarrow \left\{ \begin{array}{c} \text{monomorfismos } \tau \text{ tales que} \\ \text{el diagrama conmuta} \\ \begin{array}{ccc} E & \overset{\tau}{\rightarrowtail} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \end{array} \end{array} \right\}$$

Entonces tenemos

$$\begin{array}{lll} |G(K/F)/G(K/E)| & = \{E : F\} & \text{por definición de } \varphi \\ \| & & \\ \{G(K/F) : G(K/E)\} & & \text{por definición} \\ \| & & \\ \{G(K/F) : \lambda(E)\} & & \end{array}$$

Por el teorema 2.11.5 K es separable sobre $F \Leftrightarrow K$ es separable sobre E y E es separable sobre F, entonces se tiene

$$\{E : F\} = [E : F], \quad \therefore \quad [E : F] = \{G(K/F) : \lambda(E)\}$$

Sólo resta demostrar las propiedades 3 y 5 (note que demostrar 3 equivale a demostrar que λ es sobre), las probaremos en la siguiente sección. ■

3.2. Grupos de Galois sobre campos finitos.

Teorema 3.2.1 *Sea K una extensión finita de grado n de un campo finito F de p^r elementos. Entonces $G(K/F)$ es un grupo cíclico de orden n está generado por σ_{p^r} donde $\sigma_{p^r}(\alpha) = \alpha^{p^r}$ para cada $\alpha \in K$.*

Demostración. Primero veamos que K es extensión normal sobre F.
como F es un campo finito entonces por el teorema 2.12.4 se tiene que F es un campo perfecto, es decir, toda extensión finita de F es una extensión separable. Dado que por hipótesis $[K : F] = n < \infty \Rightarrow K$ es una extensión separable sobre F.
Por otra parte, tenemos por hipótesis que $|F| = p^r$ y $[K : F] = n$. Por el teorema 2.14.1 se tiene que $|K| = (p^r)^n = p^{rn}$, del teorema 2.14.3 se tiene que K es el campo de descomposición de $x^{p^{nr}} - x \in \mathbb{Z}_p[x]$ sobre $\mathbb{Z}_p$, entonces K es el campo de descomposición de $x^{p^{nr}} - x \in F[x]$ sobre F, por tanto, K es una extensión normal de F

$$\Rightarrow |G(K/E)| = \{K : F\} = [K : F] \Rightarrow$$

$$|G(K/F)| = [K : F] = n \qquad \textbf{(I)}$$

Dado a que K es un campo finito de característica p, por el teorema 2.6.1 tenemos el siguiente automorfismo (automorfismo de Frobenius)

$$\sigma_p : K \longrightarrow K$$

$$a \longmapsto a^p$$

$$\Rightarrow \sigma_{p^r} = \underbrace{(\sigma_p \circ \cdots \circ \sigma_p)}_{r - veces} : K \longrightarrow K, \text{ es un automorfismo tal que}$$

$$a \longmapsto a^{p^r}$$

además notemos que σ_{p^r} deja fijo al subcampo F de K pues si $a \in F$ es tal que $a = 0$, entonces $\sigma_{p^r}(0) = 0$. Si $0 \neq a \in F$ entonces $a \in F - \{0\} = F^*$ y F^* es un grupo multiplicativo abeliano tal que $|F^*| = p^r - 1 \Rightarrow a^{|F^*|} = 1 \Rightarrow a^{p^r-1} = 1 \Rightarrow a \cdot a^{p^r-1} = a \cdot 1 \Rightarrow a^{p^r} = a \Rightarrow \sigma_{p^r}(a) = a$

$$\therefore \sigma_{p^r}(a) = a \ \forall \ a \in F \quad \therefore \quad \sigma_{p^r} \in G(K/F).$$

Ahora demostraremos que el orden de $\sigma_{p^r} \in G(K/F)$ debe ser mayor o igual que n y dado que por **(I)** $|G(K/F)| = n$, tendremos que $\langle \sigma_{p^r} \rangle = G(K/F)$.

Procederemos:
Notemos que dado cualquier $i > 0$ y dado que cualquier $\alpha \in K$ tenemos que $(\sigma_{p^r})^i(\alpha) = (\sigma_{p^r} \circ \cdots \circ \sigma_{p^r})(\alpha) = \alpha^{p^{ri}}$.
Debemos analizar como es el menor $i > 0$ tal que $(\sigma_{p^r})^i = Id$. Pero $(\sigma_{p^r})^i = Id \Leftrightarrow (\sigma_{p^r})^i(\alpha) = \alpha \ \forall \ \alpha \in K \Leftrightarrow \alpha^{p^{ri}} = \alpha \ \forall \ \alpha \in K \Leftrightarrow \alpha^{p^{ri}} - \alpha = 0 \ \forall \ \alpha \in K \Leftrightarrow \alpha$ es cero de $x^{p^{ri}} - x \in F[x] \ \forall \ \alpha \in K$.
Por tanto debemos analizar como es el menor $i > 0$ tal que α es cero del polinomio $x^{p^{ri}} - x \in F[x] \ \forall \ \alpha \in K$.
Dado que $|K| = p^{rn} \Rightarrow$ el polinomio $x^{p^{ri}} - x \in F[x]$ debe tener al menos $|K| = p^{rn}$ ceros distintos $\Rightarrow$ el grado de $x^{p^{ri}} - x$ debe ser al menos $p^{rn} \Rightarrow i \geqslant n$.
$\Rightarrow |\langle \sigma_{p^r} \rangle| \geqslant n$ para $\sigma_{p^r} \in G(K/F)$. Dado que $|G(K/F)| = n \Rightarrow G(K/F) = \langle \sigma_{p^r} \rangle \therefore G(K/F)$ es un grupo cíclico de orden n con generador el elemento $\sigma_{p^r} \in G(K/F)$ ■

Usaremos el teorema 3.2.1 para dar otra ilustración del teorema principal de la teoría de Galois.

Ejemplo 3.2.2 *Sea $F = \mathbb{Z}_p$ y sea $K = CG(p^{12})$.*
Así, tenemos que $|K| = p^{12} < \infty \Rightarrow [K : \mathbb{Z}_p] < \infty \Rightarrow [K : \mathbb{Z}_p] = m$ para algún $m > 0$ y dado que $|F| = |\mathbb{Z}_p| = p$, por el teorema 2.14.1 tenemos $|K| = p^m \Rightarrow |K| = p^{12} = p^m \Rightarrow m = 12 \therefore [K : F] = 12$. Usando el teorema 3.2.1 se tiene que $G(K/F)$ es cíclico de orden $n = 12$, es decir,

$$G(K/F) \cong \langle \mathbb{Z}_{12}, + \rangle$$

y $G(K/F)$ está generado por σ_{p^1} ($r = 1$ en este caso), donde

$$\sigma_{p^1} : CG(p^{12}) \longrightarrow CG(p^{12})$$

$$a \longmapsto a^p$$

Utilizando el teorema de grupos cíclicos enunciado en el ejemplo 2.14.11, podemos describir todos los subgrupos cíclicos (o sea todos los subgrupos) de $G(K/F) = \langle \sigma_p \rangle$.
Calculemos todos los divisores d, de $n = 12$ que son: $d = 1, 2, 3, 4, 6$ y 12, así $b = a^s$ genera un subgrupo cíclico H de G con $\frac{n}{d}$ elementos donde $(n, s) = d$, es decir, $(12, s) = d$.

Calculamos cada caso

$$\begin{array}{llll} (12,s) & = 1 & \Rightarrow s = 1,5,7,11 & \Rightarrow (\sigma_p)^1 \text{ genera } G(K/F) \\ (12,s) & = 2 & \Rightarrow s = 2,10 & \Rightarrow (\sigma_p)^2 \\ (12,s) & = 3 & \Rightarrow s = 3,9 & \Rightarrow (\sigma_p)^3 \\ (12,s) & = 4 & \Rightarrow s = 4,8 & \Rightarrow (\sigma_p)^4 \\ (12,s) & = 6 & \Rightarrow s = 6 & \Rightarrow (\sigma_p)^6 \\ (12,s) & = 12 & \Rightarrow s = 12 & \Rightarrow (\sigma_p)^{12} = Id \end{array}$$

Por tanto, los subgrupos de $G(K/F) \equiv \langle \sigma_p \rangle$ *son*

$$\langle \sigma_p \rangle, \quad \langle \sigma_p^2 \rangle, \quad \langle \sigma_p^3 \rangle, \quad \langle \sigma_p^4 \rangle, \quad \langle \sigma_p^6 \rangle, \quad \{Id\}.$$

■

Demostraremos las propiedades 3 y 5 del teorema principal de la teoría de Galois que quedaron pendientes.

Demostración.
3.– Demostraremos que si H es subgrupo de $G(K/F)$ entonces $\lambda(K_H) = H$. Sea H subgrupo de $G(K/F)$ debemos demostrar que

$$G(K/K_H) \equiv \lambda(K_H) = H.$$

Tenemos que $F \leqslant K_H \leqslant K$ (F es subcampo de K_H pues tomando $f \in F$ fijo, sea $\sigma \in H \leqslant G(K/F)$ arbitrario $\Rightarrow \sigma \in G(K/F)$ y por definición de $G(K/F)$ $\sigma(f) = f$ y como σ fue tomado arbitrario entonces $\sigma(f) = f \; \forall \; \sigma \in H$, así se tiene por definición de K_H que $f \in K_H$).

Notemos también que $H \leqslant G(K/K_H) \equiv \{\sigma \in Aut(K) | \sigma(a) = a \; \forall \; a \in K_H\}$. En efecto; sea $\sigma \notin G(K/K_H) \Rightarrow \sigma(a) \neq a$ para algún $a \in K_H \equiv \{a \in K | \sigma(a) = a \; \forall \; \sigma \in H\} \Rightarrow \sigma \notin H$.

Hemos probado que $G(K/F) - G(K/K_H) \subseteq G(K/F) - H \Rightarrow H \subseteq G(K/K_H) \therefore$ $H \leqslant G(K/K_H)$. Hasta ahora sólo hemos probado que

$$F \leqslant K_H \leqslant K \qquad \textbf{(I)}$$

y que $H \leqslant G(K/K_H)$, debemos demostrar que $H = G(K/K_H)$. Lo haremos por contradicción. Supongamos que $H \subsetneq \lambda(K_H)$ (esto es, supongamos que H es un subgrupo propio de $\lambda(K_H)$) demostraremos que ésto es imposible.

Primero demostraremos que K es una extensión simple de K_H

CASO 1: K_H es un campo infinito.
Vimos en **(I)** que $F \leqslant K_H \leqslant K \leqslant \overline{F}$. Además por hipótesis K es una extensión normal finita del campo F, entonces por definición tenemos que K es una extensión separable finita de F. Por el teorema 2.11.5 K es una extensión separable finita sobre K_H y K_H es una extensión separable finita sobre F.
Así tenemos que $[K : K_H] < \infty$ con K extensión separable sobre K_H $\therefore$ K es una extensión separable finita de un campo infinito y por el teorema 2.13.1 (teorema del elemento primitivo) tenemos que K es una extensión simple sobre K_H, esto es, $\exists\ \alpha \in K$ tal que $K = K_H(\alpha)$.

CASO 2: K_H es un campo finito. Entonces por hipótesis K es una extensión finita del campo finito K_H, por el corolario 2.14.9 K_H es una extensión simple de F.
Así tanto en el CASO 1 como en el CASO 2 tenemos que

$$K = K_H(\alpha) \text{ para algún } \alpha \in K \qquad \textbf{(II)}$$

Por otra parte tenemos que por hipótesis K es una extensión normal finita de F y por **(I)** tenemos que $F \leqslant K_H \leqslant K \leqslant \overline{F}$, entonces por el teorema 3.1.2 K es una extensión normal finita de K_H

$$\Rightarrow [K : K_H] = \{K : K_H\} = |G(K/K_H)|.$$

Sea

$$n = [K : K_H] = |G(K/K_H)| \qquad \textbf{(III)}$$

Dado que estamos suponiendo que $H \subsetneq G(K/K_H)$ entonces tenemos que $|H| < |G(K/K_H)| = n$ y por **(III)** $\Rightarrow |H| < [K : K_H] = n$.
Sean $\sigma_1, \cdots, \sigma_{|H|}$ los elementos de H.
Consideremos el polinomio

$$f(x) = \Pi_{i=1}^{|H|}(x - \sigma_i(\alpha)) \in K[x] \qquad (pues\ \ \sigma_i(\alpha) \in K).$$

Entonces $f(x)$ es de grado $|H| < n$.
Veamos que los coeficientes de cada potencia de x en $f(x)$ son " expresiones simétricas en los $\sigma_i(\alpha)$ ", es decir, si

$$f(x) = a_0 + a_1x + \cdots + a_{|H|}x^{|H|} \in K[x],$$

entonces para cualquier $\sigma \in H$ tendremos que:

$$\sigma(a_0) = a_0,\ \sigma(a_1) = a_1, \cdots, \sigma(a_{|H|}) = a_{|H|}.$$

En efecto, sea $\sigma \in H$ cualquiera. Dado que $H \subsetneq G(K/K_H) \Rightarrow \sigma \in Aut(K) \Rightarrow \sigma : K \longrightarrow K$ es isomorfismo $\Rightarrow \sigma$ induce un isomorfismo:

$$\overline{\sigma} : K[x] \longrightarrow K[x].$$

$$\Rightarrow \overline{\sigma}(f(x)) = \overline{\sigma}(\Pi_{i=1}^{|H|}(x - \sigma_i(\alpha))) = \Pi_{i=1}^{|H|}(x - \sigma\sigma_i(\alpha)) = f(x),$$

donde la última igualdad se tiene porque H es grupo finito y así, la colección $\sigma(\sigma_1), \cdots, \sigma(\sigma_{|H|})$ es igual a la colección $\sigma_1, \cdots, \sigma_{|H|}$ de todos los elementos de H excepto quizás por el orden, por tanto,

$$\sigma(a_0) = a_0,\ \sigma(a_1) = a_1, \cdots, \sigma(a_{|H|}) = a_{|H|}\ \forall\ \sigma \in H,$$

$\Rightarrow f(x)$ tiene todos sus coeficientes en K_H (es decir, $a_i \in K_H\ \forall\ i = 0, \cdots, |H|$).
Dado que algún σ_i tiene que ser la identidad (Id) en H,

$$\text{tenemos que en } f(x) = \Pi_{i=1}^{|H|}(x - \sigma_i(\alpha)) \in K_H[x]$$

aparece el factor $(x - \alpha)$. $\Rightarrow f(\alpha) = 0$,

$$\Rightarrow irr(\alpha, K_H) | f(x) \Rightarrow grad(irr(\alpha, K_H)) \leqslant grad(f(x)) = |H|$$

$$\Rightarrow grad(irr(\alpha, K_H)) \leqslant |H| < n = [K_H(\alpha) : K_H]$$

$\Rightarrow grad(irr(\alpha, K_H)) < [K_H(\alpha) : K_H]$ lo cual es una contradicción

pues por el corolario 2.1.4 siempre tenemos que $grad(\alpha, K_H) = [K_H(\alpha) : K_H]$), por tanto, se cumple **3.** ■

5.- Demostraremos que si E una extensión normal de $F \Leftrightarrow \lambda(E) \equiv G(K/E)$ es un subgrupo normal de $G(K/F)$ $(G(K/E) \triangleleft (K/F))$.

Demostración.
Por el Teorema 2.11.5, toda extensión E de F, $F \leq E \leq K$ es separable sobre F. Así, E es normal sobre F, si sólo si E es un campo de descomposición sobre F.
Por otra parte, por el teorema de extensión de isomorfismos, cualquier monomorfismo

$$\sigma : E \longrightarrow \overline{F} \quad \text{tal que} \quad \sigma|_F = \text{inclusión}$$

se extiende a un monomorfismo $\overline{\sigma}$ tal que el diagrama siguiente conmuta

$$\begin{array}{ccc} K & \overset{\overline{\sigma}}{\rightarrowtail} & \overline{\sigma(E)} \equiv \overline{F} \\ \uparrow & & \uparrow \\ E & \underset{\sigma}{\longrightarrow} & \sigma(E) \subseteq \overline{F} \end{array}$$

Dado que K es normal sobre $F \Rightarrow K$ es campo de descomposición sobre F, ésto por definición de campo normal. Por el corolario 2.9.5

$$\overline{\sigma}(K) \subseteq K.$$

Por lo que tenemos el siguiente diagrama conmutable

$$\begin{array}{ccc} K & \overset{\overline{\sigma}}{\longrightarrow} & K \\ \uparrow & & \uparrow \\ E & \underset{\sigma}{\longrightarrow} & \sigma(E) \end{array}$$

con $\overline{\sigma} : K \longrightarrow K$ automorfismo.Tal que $\overline{\sigma}|_E = \sigma$ y $\overline{\sigma}|_F = Id$, esto es, $\overline{\sigma} \in G(K/F) = \{\overline{\sigma} : K \longrightarrow K |\ \overline{\sigma}|_F = \text{inclusión}\}$. Así si σ es cualquier monomorfismo tal que el diagrama siguiente conmuta

$$\begin{array}{ccc} E & \overset{\sigma}{\rightarrowtail} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \end{array}$$

Por la observación anterior se tiene que σ es restricción de algún elemento $\overline{\sigma} \in G(K/F)$. Por tanto $G(K/F)$ induce todos los posibles monomorfismos $\sigma : E \longrightarrow \overline{F}$ que fijan F. **(I)**

Por otra parte, por el teorema 2.9.3 E es campo de descomposición sobre $F \Leftrightarrow \forall\ \sigma$ monomorfismo tal que el diagrama siguiente conmuta

$$\begin{array}{ccc} E & \overset{\sigma}{\rightarrowtail} & \overline{F} \\ \uparrow & & \uparrow \\ F & = & F \subseteq E \end{array}$$

se tiene que $\sigma(E) \subseteq E$. Por tanto E es campo de descomposición de $F \Leftrightarrow \sigma(E) \subseteq E\ \ \forall\ \sigma \in G(K/F)$ por **(I)**.

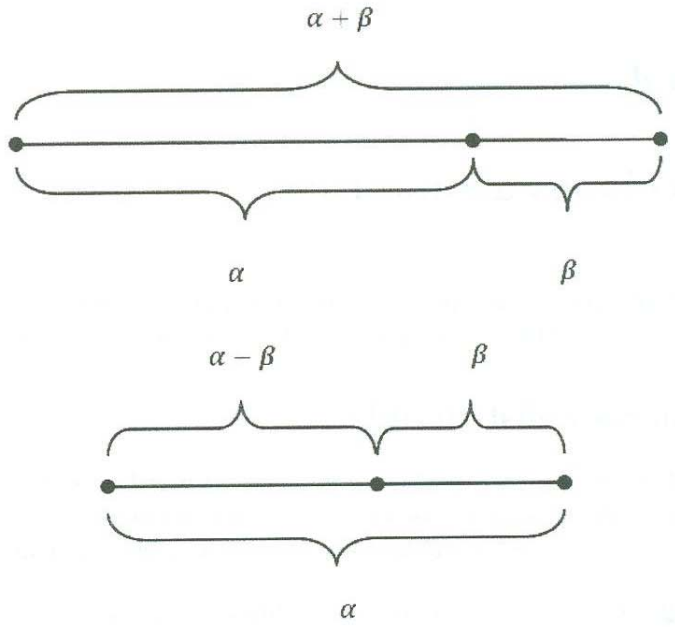


Figura 4.1: $\alpha + \beta$

En la figura 4.3 se muestra la construcción de $\alpha\beta$.
Sea $\overline{OA}$ el segmento de recta del punto O al punto A y sea $|\overline{OA}|$ la longitud de este segmento de recta.
Si $\overline{OA}$ es de longitud $|\alpha|$, encontramos la recta l que pase por O y no contenga a $\overline{OA}$. Después, localizamos los puntos P y B en l, tales que $\overline{OP}$ es de longitud 1 y $\overline{OB}$ es de longitud $|\beta|$. Por último basta trazar $\overline{PA}$ y construir l' que pase por B y sea paralela a $\overline{PA}$ e interseque la extensión de $\overline{OA}$ en Q. Por triángulos semejantes se tiene que

$$\frac{1}{|\alpha|} = \frac{|\beta|}{|\overline{OQ}|}$$

De donde:

$$|\overline{OQ}| = |\alpha\beta|.$$

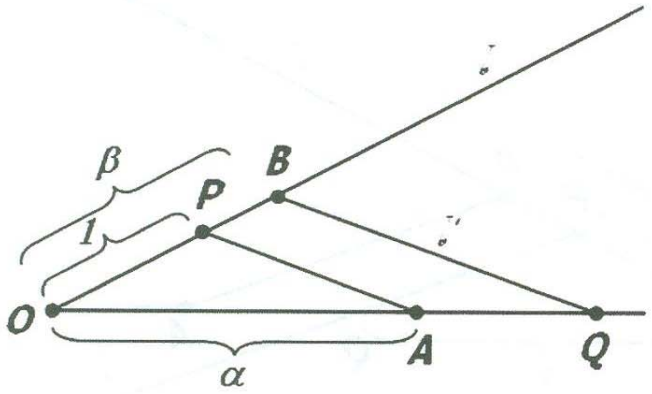


Figura 4.2: $\alpha\beta$

Se muestra en la figura 4.4 que $\frac{\alpha}{\beta}$ es constructible si $\beta \neq 0$. Sea $\overline{OA}$ de longitud $|\alpha|$ y encontramos el segmento de recta l que pase por O y no contesnga a $\overline{OA}$. Después, hallamos B y P en l, tal que, $\overline{OB}$ sea de longitud $|\beta|$ y $\overline{OP}$ sea de longitud 1. Construirmos l', una recta paralela a $\overline{BA}$ y que además pase por P e interseque $\overline{OA}$ en Q. De nuevo por triángulos semejantes tenemos:

$$\frac{|\overline{OQ}|}{1} = \frac{|\alpha|}{|\beta|},$$

de tal forma que

$$|\overline{OQ}| = \frac{|\alpha|}{|\beta|}.$$

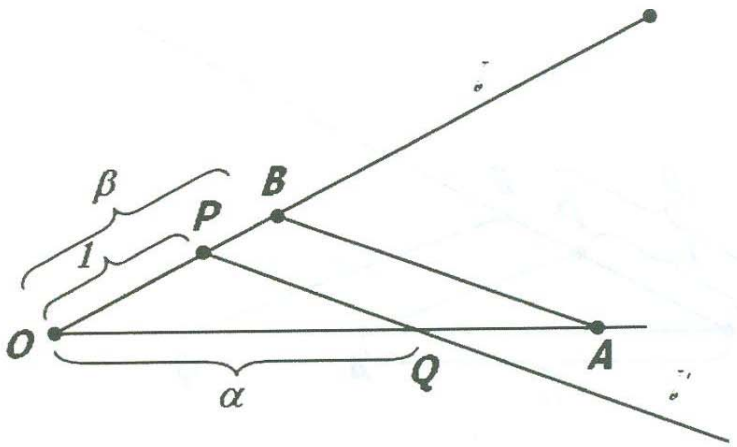


Figura 4.3: $\frac{\alpha}{\beta}$

Por último mostraremos que $\sqrt{\alpha}$ es construible. Sea $\overline{OA}$ de longitud $|\alpha|$ en la figura 4.5. Localizamos el punto P en la extensión de $\overline{OA}$ de modo que $|\overline{OP}| = 1$. Procedemos encontreando el punto medio de $\overline{PA}$ para trazar un semicírculo de diámetro $\overline{PA}$. Levantamos una perpendicular a $\overline{PA}$ en O, tal que interseque al semicírculo en Q. Entonces, los triángulos OPQ y OQA son semejantes, de modo que

$$\frac{|\overline{OQ}|}{|\overline{OA}|} = \frac{|\overline{OP}|}{|\overline{OQ}|}$$

y

$$|\overline{OQ}|^2 = 1\alpha = \alpha$$

Así, $\overline{OQ}$ es de longitud $\sqrt{\alpha}$. Por lo que las raíces cuadradas de números constructibles son constructibles.

■

Corolario 4.1.3 *El conjunto de todos los números reales constructibles forma un subcampo F del campo de los números reales.*

Demostración. La demostración de este corolario es inmediata del Teorema 4.1.2 ■

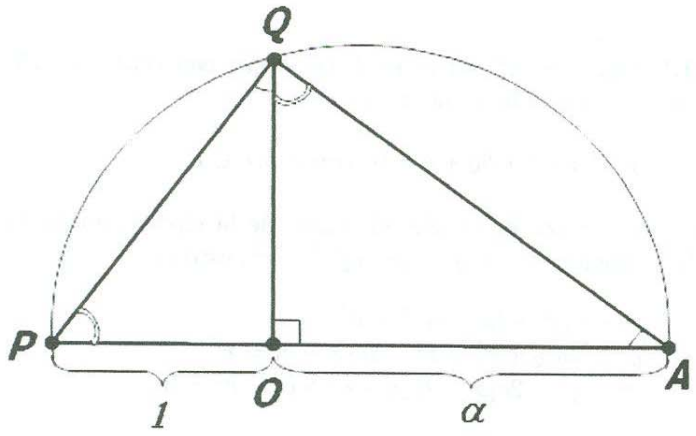


Figura 4.4: $\sqrt{\alpha}$

El campo F de los números reales constructibles contiene a $\mathbb{Q}$, el campo de los números racionales, pues $\mathbb{Q}$ es el menor subcampo de $\mathbb{R}$, es decir,

$$\mathbb{Q} \subseteq F \subseteq \mathbb{R}.$$

Para la demostración del siguiente teorema, es necesario probar algunas afirmaciones;

Sea F subcampo de $\mathbb{R}$. Definimos como $PF = \{(x, y) \in \mathbb{R}^2 | x, y \in F\}$, el plano de F.

Afirmación 4.1.4 *Una recta que une dos puntos en F tiene una ecuación de la forma*

$$ax + by + c = 0 \quad con \quad a, b \; y \; c \; en \; F.$$

Demostración. Sean $(x, y), (x_1, y_1) \in PF$, la ecuación de la recta es,

$$m = \frac{y - y_1}{x - x_1} \; con \; x \neq x_1, \quad y - x_1 = 0 \; si \; x = x_1$$

con $a = 0, b = 1, c = -x_1 \in F$

$\Rightarrow m(x - x_1) = y - y_1 \; con \; m \in F$
$\Rightarrow mx - mx_1 = y - y_1$
$\Rightarrow mx - y - (mx_1 - y_1) = 0 \; con \; a = m, \; b = -1, \; c = -(mx_1 - y_1) \in F$

$\therefore a, b, c \in F$. ■

Afirmación 4.1.5 *Una circunferencia en F (es decir, con centro en PF y radio $r \in F$) tiene una ecuación de la forma*

$$x^2 + y^2 + ax + by + c = 0 \quad con\ a, b, c \in F$$

Demostración. Sea $c = (c_1, c_2) \in PF$ el centro de la circunferencia C y $r \in F$ el radio. La ecuación es $|(x, y) - (c_1, c_2)|^2 = r^2$, esto es

$$\begin{aligned} & (y - c_2)^2 + (x - c_1)^2 = r^2 \\ \Rightarrow\ & y^2 - 2yc_2 + c_2^2 + x^2 - 2c_1x + c_1^2 = r^2 \\ \Rightarrow\ & x^2 + y^2 - 2c_1x - 2c_2y + c_1^2 + c_2^2 - r^2 = 0 \end{aligned}$$

entonces, $a = -2c_1, b = -2c_2, c = c_1^2 + c_2^2 - r^2 \in F \therefore a, b, c \in F$. ■

Afirmación 4.1.6 *Dos rectas en F que se intersectan en el plano real, se intersectan en un punto del plano F.*

Demostración. Sean

$$a_1x + b_1y + c_1 = 0 \qquad \textbf{(I)}$$

$$a_2x + b_2y + c_2 = 0 \qquad \textbf{(II)}$$

dos rectas que están en F (es decir, $a_i, b_i, c_i \in F$ para $i = 1, 2$). Entonces despejamos el valor de una una variable en **(I)** y sustituyendo en **(II)** obtenemos el punto de intersección. Dado que solo hacemos sumas, restas, productos y cocientes, los puntos que obtenemos están en F. ■

Afirmación 4.1.7 *Una recta en F que se intersecta en el plano real con una circunferencia en F lo hace en un punto que está en el plano F o en el plano de $F(\sqrt{\gamma})$ para algún $\gamma > 0$ en F ($F \subseteq \mathbb{R}$).*

Demostración. Sean

$$ax + by + c = 0\ con\ \ a, b, c\ \ en\ F \qquad \textbf{(I)}$$

$$x^2 + y^2 + dx + ey + f = 0\ con\ d, e, f\ en\ F \qquad \textbf{(II)}$$

Si $b \neq 0$

$$y = \frac{-c - ax}{b} \qquad \textbf{(III)}$$

Sustituyendo **(III)** en **(II)**

$$\Rightarrow x^2 + (\frac{-c - ax}{b})^2 + dx + e(\frac{-c - ax}{b}) + f = 0.$$

Entonces al simplificar obtenemos una ecuación cuadrática

$$Ax^2 + Bx + C = 0 \; con \; A, B, C \in F.$$

Si $B^2 - 4AC < 0$ sabemos por geometría analítica que la recta no intersecta a la circunferencia, por tanto

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A} \qquad \textbf{(IV)}$$

$$x = \frac{-B}{2A} \pm \sqrt{\frac{B^2 - 4AC}{4A^2}}$$

con $B^2 - 4A > 0$ es decir, $x = s \pm \sqrt{\gamma}$ con $\gamma > 0 \in F$.
Sustituyendo **(IV)** en **(III)** se tiene que:

$$y = -c - a\frac{(-s \pm \sqrt{\gamma})}{b}.$$

Sea $p(x) = x^2 - \gamma$, si existe $a \in F$ tal que $p(a) = 0$, entonces $x, y \in F$, si no, entonces $x, y \in F(\sqrt{\gamma})$ donde $F(\sqrt{\gamma})$ significa la mínima extensión de F que contiene a F y a $\sqrt{\gamma}$.
Si $b = 0$ se tiene que

$$ax + c = 0 \Rightarrow x = \frac{-c}{a}$$

por lo que

$$y^2 + (-\frac{c}{a})^2 + d(-\frac{c}{a}) + ey + f = 0$$

la ecuación se simplifica tal que

$$Ay^2 + By + C = 0 \Rightarrow y = s \pm a\sqrt{\gamma} \; con \; \gamma > 0$$

de donde se obtiene que $x = \frac{a}{c} \Rightarrow x, y \in F$ ó $x, y \in F(\gamma)$ para algún $\gamma > 0 \in F$. ■

Observación 4.1.8 *La intersección de dos circunferencias en F puede realizarse como la de una recta en F y la de una circunferencia en F. Pues si*

$$c_1 \; es \; x^2 + y^2 + a_1x + b_1y + c_1 = 0 \;\; y$$

$$c_2 \text{ es } x^2 + y^2 + a_2x + b_2y + c_2 = 0$$

entonces su intersección es la recta

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$$

un punto que está en F, por lo que podemos considerar la intersección de dos circunferencias en F, como la intersección de una recta en F con una circunferencia en F.

Teorema 4.1.9 *Un número $\alpha \in \mathbb{R}$ es constructible si existe una sucesión $\alpha_1, \cdots, \alpha_n \in \mathbb{R}$ tal que $\sqrt{\alpha_i} \in \mathbb{Q}(\alpha_1, \cdots, \alpha_i)$ $\forall$ i y $\alpha \in \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$.*

Demostración. Podemos construir cualquier número racional. si consideramos nuestro segmento unidad dado, de longitud 1 como la unidad básica sobre el eje x, podemos localizar cualquier punto (q_1, q_2) en el plano $\mathbb{R}^2$, con ambas coordenadas racionales. Cualquier otro punto en el plano que podamos localizar con regla y compás, puede hallarse de alguna de las tres formas siguientes:

1. como intersección de dos rectas, cada una de las cuales pasa por dos puntos conocidos con coordenadas racionales, por la afirmación 4.1.6.

2. como intersección de una recta que pasa por coordenadas racionales y un círculo tiene coordenadas racionales y el cuadrado de su radio es racional, por la afirmación 4.1.7.

3. como intersección de dos círculos cuyos centros tienen coordenadas racionales y los cuadrados de sus radios son racionales, por la observación 4.1.8.

Las ecuaciones de las rectas y los círculos anteriormente mencionados por las afirmaciones 4.1.4 y 4.1.5, son de la forma:

$$ax + by + c = 0$$

$$x^2 + y^2 + dx + ey + f = 0$$

donde a, b, c, d, e y f están en $\mathbb{Q}$.

Para el CASO 1, tenemos la intersección de dos rectas y por la afirmación 4.1.6, las soluciones para x y y son todas números racionales.

En el caso 2 tenemos la interseccion de la forma siguente:

$$x^2 + y^2 + dx + ey + f = ax + by + c$$
$$x^2 + y^2 + (d-a)x + (e-b)y + f - c = 0$$

Aplicando la afirmación 4.1.7, se obtiene que las soluciones para x y y son números racionales, o bien números en una extensión de la forma $\mathbb{Q}(\sqrt{\alpha_1})$ con $\alpha_1 \in \mathbb{Q}$.

Partiedo del nuevo campo $\mathbb{Q}(\sqrt{\alpha_1})$ trazando rectas y circunferencias tenemos que los nuevos números constructibles se encuentran o en $\mathbb{Q}(\sqrt{\alpha_1})$ o en la extensión $\mathbb{Q}(\sqrt{\alpha_1}, \sqrt{\alpha_2})$ de grado dos, donde $\alpha_2 \in \mathbb{Q}(\sqrt{\alpha_1})$, siguiendo este procedimiento para un número finito de veces encontraremos $\mathbb{Q}(\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_n})$ el campo donde se encuentra α. Por tanto, para cualquier $\alpha \in$ F tal que $\alpha \notin \mathbb{Q}$, se tiene que α esta en un campo de extension de $\mathbb{Q}$.

El caso 3 se reduce al caso 2 por la afirmación 4.1.8 ■

Corolario 4.1.10 *Si γ es constructible y $\gamma \notin \mathbb{Q}$, entonces $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$ para algún entero $r \geqslant 0$.*

Demostración. Por el Teorema 4.1.9 tenemos que existen $\alpha_1, \cdots, \alpha_n = \gamma$ tal que $\mathbb{Q}(\alpha_1, \cdots, \alpha_i)$ es una extensión de $\mathbb{Q}(\alpha_1, \cdots, \alpha_{i-1})$ de grado 2.
Por el Teorema 2.3.5

$$\begin{aligned}[\mathbb{Q}(\gamma) : \mathbb{Q}] &= [\mathbb{Q}(\alpha_1, \cdots, \alpha_n) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha_1, \cdots, \alpha_n) : \mathbb{Q}(\alpha_1, \cdots, \alpha_{n-1})] \cdots [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \\ &= 2^r\end{aligned}$$

Para algún r positivo. ■

4.2. Imposibilidad de ciertas construcciones.

Ahora podemos demostrar la imposibilidad de ciertas construcciones geométricas.

Teorema 4.2.1 ***.-*Es imposible duplicar el cubo*.***
Dado el lado de un cubo, no siempre es posible construir con regla y compás el lado de un cubo que tenga el doble del volumen del cubo original.

Demostración. Sea el cubo de lado 1 y en consecuencia, de volumen 1. El cubo buscado debe tener volumen 2 y, por tanto, lado de longitud $\sqrt[3]{2}$. Pero $\sqrt[3]{2}$ es un cero del polinomio $x^3 - 2$ sobre $\mathbb{Q}$, de modo que

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

El corolario 4.1.10 muestra que para doblar el cubo de volumen 1 se necesita un entero r tal que,

$$3 = 2^r,$$

es claro que no existe dicha r. ■

Teorema 4.2.2 ***.-*Es imposible cuadrar el círculo*.***
Dado un círculo, no siempre es posible construir con regla y compás un cuadrado que tenga área igual al área del círculo dado.

Demostración. Sea el círculo dado de radio 1 y, por tanto, de área π. Necesitaríamos contruir un cuadrado de lado $\sqrt{\pi}$. Pero π es trascendente sobre $\mathbb{Q}$, de modo que también $\sqrt{\pi}$ es trascendente sobre $\mathbb{Q}$. ■

Teorema 4.2.3 ***.-*Es imposible trisecar el ángulo*.***
Existe algún ángulo que no puede trisecarse con regla y compás.

Demostración. Un ángulo Θ puede construirse si y sólo si puede construirse un segmento de recta de longitud $|cos\Theta|$. Ahora bien, el ángulo de $60°$ puede construirse y mostraremos que no puede trisecarse.
Digamos

$$\begin{aligned} cos3\Theta &= cos(2\Theta + \Theta) \\ &= cos2\Theta cos\Theta - sen2\Theta sen\Theta \\ &= (2cos^2 - 1)cos\Theta - 2sen\Theta cos\Theta sen\Theta \\ &= (2cos^2 - 1)cos\Theta - 2cos\Theta(1 - cos^2\Theta) \\ &= 4cos^3\Theta - 3cos\Theta. \end{aligned}$$

Sea $\Theta = 20°$, de modo que el $cos3\Theta = \frac{1}{2}$ y sea $\alpha = cos20°$. De nuestra identidad $4cos^3\Theta - 3cos\Theta = cos3\Theta$ vemos que

$$4\alpha^3 - 3\alpha = \frac{1}{2}.$$

Así, α es cero de $8x^3 - 6x - 1$. Este polinomio es irreducible en $\mathbb{Q}[x]$, pues por el teorema 1.5.2 basta probar que no se factoriza en $\mathbb{Z}[x]$. Si el polinomio se factoriza en $\mathbb{Z}[x]$ entonces tendría factores de la forma

$$(8x \pm 1), (4x \pm 1), (2x \pm 1), (x \pm 1).$$

Pero claramente tenemos que ninguno de los siguientes números son ceros del polinomio.

$$\pm\frac{1}{8}, \pm\frac{1}{4}, \pm\frac{1}{2}, \pm 1.$$

Así

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3,$$

de modo que por el corolario 4.1.10, α no es constructible y por tanto, el ángulo de 60° no se puede trisecar. ■

Observación 4.2.4 *Del teorema anterior podemos concluir que* ***no todos los n-gonos regulares se pueden construir con regla y compás,*** *pues tenemos que un n-gono regular para $n \geqslant 3$ se puede construir si y sólo si, el ángulo $\frac{2\pi}{n}$ es constructible, lo cual es el caso si y sólo si, es constructible el segmento de recta de longitud $cos(\frac{2\pi}{n})$.*

4.3. Extensiones ciclotómicas

Definición 4.3.1 *El campo de descomposición de $x^n - 1$ sobre F es la* ***n-ésima extensión ciclotómica de F.***

Supongamos que F es cualquier campo y considérese $(x^n - 1) \in F[x]$. Como en la demostración del lema 2.15.1, vemos, por división, que si α es cero de $x^n - 1$ y $g(x) = \frac{x^n - 1}{x - \alpha}$, entonces

$$g(\alpha) = \frac{(n \cdot 1)\alpha^n}{\alpha} = n \cdot \frac{1}{\alpha} \neq 0$$

siempre que la característica de F no divida a n. Por tanto , bajo esta condición, el campo de descomposición de $x^n - 1$ es separable y, en consecuencia, es una extensión normal de F.

Supóngase,de ahora en adelante, que así sucede, y sea K el campo de descomposición de $x^n - 1$ sobre F. Entonces $x^n - 1$ tiene n ceros distintos en K y, por el teorema 2.14.7 forman un grupo ciclico de orden n bajo la multiplicación de campo. Un grupo cíclico de orden n tiene $\varphi(n)$ generadores, donde φ es la función de Euler (ver el teorema 24.8 [1] pp. 221). Así, se obtiene que el grupo tiene $\varphi(n)$ generadores, en esta ocasión esos $\varphi(n)$ generadores son exactamente las raíces n-ésimas primitivas del unitario.

Definición 4.3.2 *El polinomio*

$$\Phi_n(x) = \Pi_{i=1}^{\varphi(n)}(x - \alpha_i),$$

donde las α_i son la raíces n-ésimas primitivas del unitario en $\overline{F}$, es el ***n-ésimo polinomio ciclotómico sobre F.***

Como un automorfismo del grupo de Galois $G(K/F)$ debe permutar las raíces n-ésimas primitivas del unitario, veamos que $\Phi_n(x)$ queda fijo bajo todo elemento de $G(K/F)$, es decir, sea $\sigma \in G(K/F)$ entonces

$$\sigma(\Phi_n(x)) = \sigma(\Pi_{i=1}^{\varphi(n)}(x - \alpha_i)) = \Pi_{i=1}^{\varphi(n)}(x - \sigma\alpha_i) = \Pi_{i=1}^{\varphi(n)}(x - \alpha_i) = \Phi_n(x).$$

Tenemos K una extensión normal finita de un campo F con Grupo de Galois $G(K/F)$. Entonces podemos aplicar el Teorema de Galois obteniendo así que el campo fijo $K_{G(K/F)}$ resulta ser precisamente F. Así, $\Phi_n(x) \in \mathbb{F}[x]$. En particular, para $F = \mathbb{Q}$, $\Phi_n(x) \in \mathbb{Q}[x]$ y $\Phi_n(x)$ es cero de $x^n - 1$. Así sobre $\mathbb{Q}$ debemos tener en realidad, por el teorema 1.5.2 que $\Phi_n(x) \in \mathbb{Z}[x]$.

Hemos visto en el corolario 1.5.8 que $\Phi_p(x)$ es irreducible sobre $\mathbb{Q}$. pero $\Phi_n(x)$ no necesariamente es irreducible.

Limitemos ahora nuestro análisis a la característica 0, en particular, a subcampos de los números complejos.

Teorema 4.3.3 *El grupo de Galois de la n-ésima extensión ciclotómica de $\mathbb{Q}$ tiene $\varphi(n)$ elementos y es isomorfo al grupo formado por los enteros positivos menores que n y primos relativos con n bajo la multiplicación módulo n.*

Demostración. Supongamos $\Phi_n(x) \in \mathbb{Q}[x]$ irreducible sobre $\mathbb{Q}$.
Sea

$$\zeta = cos\frac{2\phi}{n} + isen\frac{2\pi}{n}$$

De modo que ζ es una raíz n-ésima del unitario, pues tenemos que:

$$(cos\theta + isen\theta)(cos\theta_1 + isen\theta_1) = cos(\theta + \theta_1) + isen(\theta + \theta_1).$$

Haciendo $\theta = \theta_1$ tenemos que lo anterior se puede escribir:

$$(cos\theta + isen\theta)^2 = cos2\theta + isen2\theta,$$

el paso de inducción para $k = n - 1$ se escribe de la sigueinte forma:

$$(cos\theta + isen\theta)^{n-1} = cos(n-1)\theta + isen(n-1)\theta$$

Para $k = n$

$$\begin{aligned}
(cos\theta + isen\theta)^n &= (cos\theta + isen\theta)^{n-1}(cos\theta + isen\theta) \\
&= (cos(n-1)\theta + isen(n-1)\theta)(cos\theta + isen\theta) \\
&= cos(n-1)\theta cos\theta + i^2 sen(n-1)\theta sen\theta + i(cos(n-1)\theta sen\theta + sen(n-1)\theta cos\theta) \\
&= cos(n-1)\theta cos\theta - sen(n-1)\theta sen\theta_1 + i(cos(n-1)\theta sen\theta + sen(n-1)\theta cos\theta) \\
&= cos((n-1)\theta + \theta)) + i(sen((n-1)\theta + \theta)) \\
&= cos(n\theta) + isen(n\theta)
\end{aligned}$$

Haciando $\theta = \frac{2\phi}{n}$ tenemos que:

$$\zeta = cos\frac{2\phi}{n} + isen2\phi n$$

ζ es una raíz n-ésima del unitario, pues el menor m tal que

$$\zeta^m = (cos\frac{2\phi}{n} + isen\frac{2\phi}{n})^m = 1$$

es precisamente $m = n$.

$$(\zeta^n = cos\frac{2\phi}{n} + isen2\phi n)^n = cos2\phi + isen2\phi = 1.$$

Tal que ζ además es generador del grupo formado por todas las raíces n-ésimas del unitario por ser ζ primitiva, es decir, $\zeta^m \neq 1 \ \forall \ m < n$.
Todos los generadores del grupo son de la forma ζ^m para $1 \leq m \leq n$ y m primo relativo con n.
Como ζ es primitiva entonces todas las raíces de $\Phi_n(x)$ son potencians de

ζ, el campo de descomposición K del polinomio se obtiene adjuntando a F las raíces de $\Phi_n(x)$, como K es un campo que contiene a $\mathbb{Q}$ y a todas las ζ^m para $1 \leq m \leq n$, Entonces $K = \mathbb{Q}(\zeta)$.

Las raíces primitivas de $\Phi_n(x)$ son de la forma ζ^m con $1 \leq m \leq n$ (m primo relativo con n).

Si ζ^m es primitiva entonces existe $\sigma_m \in G(K/\mathbb{Q})$ tal que $\sigma_m(\zeta) = \zeta^m$, por ser ζ y ζ^m conjugados sobre $\mathbb{Q}$, pues el grupo de Galois es precisamente las permutaciones de las raíces, por lo que va a existir el automorfismo σ_m que tranforme ζ en ζ^m. Digamos ζ^r otra raź primitiva del unitario, para la cual también va a existir $\sigma_r \in G(K/\mathbb{Q})$ análogo al anterior. Entonces

$$\sigma_r\sigma_m(\zeta) = \sigma_r(\zeta^m) = (\zeta^m)^r = \zeta^{mr} = \sigma_m r(\zeta)$$

Entonces las σ forman un subgrupo de $G(K/\mathbb{Q})$ de orden $\varphi(n)$ que es el número de raíces primitivas de la unidad.
Por otra parte tenemos que como K es un campo de descomposición sobre $\mathbb{Q}$ se tiene que $|G(K/\mathbb{Q})| = \{K : \mathbb{Q}\} = \varphi(n)$. Por tanto, tenemos que $G(K/\mathbb{Q}) = \{\sigma_m\}$ con m primo relativo con n. Así se puede definir un isomorfismo natural con el grupo abeliano G_n formado por los elementos de $\mathbb{Z}_n$ primos relativos con n bajo la multiplicación módulo n, el cual es de orden $\varphi(n)$.

Sea $\tau : G(K/\mathbb{Q}) \longrightarrow G_n$, tal que $\tau(\sigma_m) \longmapsto a^m$, donde a es el generador de G_n. ■

Ejemplo 4.3.4 *Una raíz octava primitiva del unitario en $\mathbb{C}$ es*

$$\begin{aligned} \zeta &= cos\tfrac{2\phi}{8} + isen\tfrac{2\phi}{8} \\ &= cos\tfrac{\phi}{4} + isen\tfrac{\phi}{4} \\ &= \tfrac{1}{\sqrt{2}} + i\tfrac{1}{\sqrt{2}} \\ &= \tfrac{1+i}{\sqrt{2}} \end{aligned}$$

Entonces tendremos que por la demostración del teorema 4.3.3 que todas las raíces octavas primitivas en $\mathbb{Q}$ son $\zeta, \zeta^3, \zeta^5, \zeta^7$, de modo que

$$\Phi_8(x) = (x-\zeta)(x-\zeta^3)(x-\zeta^5)(x-\zeta^7) = x^4 + 1$$

Considérese el campo de descomposición de x^4+1 sobre $\mathbb{Q}$ por el teorema 1.5.2 es irreducible sobre $\mathbb{Q}$, argumentando que no se factoriza en $\mathbb{Z}[x]$. Pues los ceros del polinomio son

$$\frac{1 \pm i}{\sqrt{2}} \; y \; \frac{-1 \pm i}{\sqrt{2}}$$

Si $\alpha = \frac{1+i}{\sqrt{2}}$, *entonces se obtienen* $\alpha^3 = \frac{-1+i}{\sqrt{2}}$, $\alpha^5 = \frac{-1-i}{\sqrt{2}}$, $\alpha^7 = \frac{1-i}{\sqrt{2}}$, *así el campo de descomposición de* x^4+1 *sobre* $\mathbb{Q}$ *es* $\mathbb{Q}(\alpha)$ *y* $[K:\mathbb{Q}] = 4$.
Como existen automorfismos en K *que transforman a cada* α *en uno de sus conjugados y como un automorfismo* σ *en* $G(K/\mathbb{Q})$ *esta completamente determinado por* $\sigma(\alpha)$, *vemos que los elementos de* $G(K/\mathbb{Q})$ *son:* $\sigma_1(\alpha) = \alpha, \sigma_3(\alpha) = \alpha^3, \sigma_5(\alpha) = \alpha^5$ *y* $\sigma_7(\alpha) = \alpha^7$. *Y con* $\alpha^8 = 1$, *vemos que* $G(K/\mathbb{Q})$ *es isomorfo a* $\{1,3,5,7\}$ *bajo la multiplicación módulo* 8 (G_8).

Corolario 4.3.5 *El grupo de Galois de la p-ésima extensión ciclotómica de* $\mathbb{Q}$ *para un primo p es cíclico de orden* $p-1$.

Demostración. Por el teorema 4.3.3 el Grupo de Galois de la p-ésima extensión ciclotómica de $\mathbb{Q}$ tiene $\varphi(p) = p-1$ elementos y es isomorfo al grupo de eneteros positivos menores que p y primos relativos con p bajo la multiplicación módulo p. Esto es exactamente el grupo $\langle \mathbb{Z}_p^*, \cdot \rangle$ de elementos distintos de cero del campo $\mathbb{Z}_p$ bajo la multiplicación del campo. por el corolario 2.14.8, este grupo es cíclico.
■

4.4. Polígonos constructibles.

Ahora determinaremos cuales n-gonos regulares son constructibles con regla y compás. Recordaremos que en la observación 4.2.4 veíamos que los n-gonos regulares que son constructibles si y sólo si,

$$cos(\frac{2\pi}{n})$$

es un número real constructible. Sea ahora

$$\zeta = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$$

entonces,

$$\frac{1}{\zeta} = cos\frac{2\pi}{n} - isen\frac{2\pi}{n}$$

para

$$\left(\zeta = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}\right)\left(\frac{1}{\zeta} = cos\frac{2\pi}{n} - isen\frac{2\pi}{n}\right) = cos^2\frac{2\pi}{n} + sen^2\frac{2\pi}{n} = 1$$

pero entonces,

$$\zeta + \frac{1}{\zeta} = 2cos\frac{2\pi}{n}.$$

Así el corolario 4.1.10 muestra que el n-gono regular es construible sólo si $\zeta + \frac{1}{\zeta}$ genera una extensión de $\mathbb{Q}$ de grado una potencia de 2.
Si K es el campo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$, entonces

$$[K : \mathbb{Q}] = \varphi(n).$$

Por el teorema 4.3.3. Si $\sigma \in G(K/\mathbb{Q})$ y $\zeta\sigma = \zeta^r$, entonces

$$\begin{aligned}\left(\zeta + \tfrac{1}{\zeta}\right)\sigma &= \zeta^r + \tfrac{1}{\zeta^r} \\ &= \left(cos\tfrac{2\pi r}{n} + isen\tfrac{2\pi r}{n}\right) + \left(cos\tfrac{2\pi r}{n} - isen\tfrac{2\pi r}{n}\right) \\ &= 2cos\tfrac{2\pi r}{n}\end{aligned}$$

Pero para $1 < r < n$ tenemos que $2cos(2\pi r/n) = 2cos(2\pi/n)$ sólo en el caso de que $r = n - 1$. Así, los únicos elementos de $G(K/\mathbb{Q})$ que llevan a $\zeta + \frac{1}{\zeta}$ sobre si mismo son el automorfismo identidad y el autorfismo τ. con $\zeta\tau = \zeta^{n-1} = \frac{1}{\zeta}$. Esto muestra que el subgrupo de $G(K/\mathbb{Q})$ que deja fijo a $\mathbb{Q}(\zeta + \frac{1}{\zeta})$, es de orden 2, de modo que, por la teoría de Galois,

$$\left[\mathbb{Q}\left(\zeta + \frac{1}{\zeta}\right) : \mathbb{Q}\right] = \frac{\varphi(n)}{2}$$

De aquí se tiene que el n-gono regular es constructible sólo si $\frac{\varphi(n)}{2}$, y por lo tanto también $\varphi(n)$, es una potencia de 2.
Tenemos que el **Teorema fundamental de la aritmética o teorema de factorización única** afirma que todo entero positivo se puede representar de forma única como producto de factores primos. Por lo que aplicandolo tenemos que:

$$n = 2^{\nu} p_1^{s_1} \cdots p_t^{s_t},$$

donde las p_i son primos impares distintos que dividen a n, entonces

$$\varphi(n) = 2^{\nu-1} p_1^{s_1-1} \cdots p_t^{s_t-1}(p_1 - 1) \cdots (p_t - 1).$$

Si $\varphi(n)$ es una potencia de 2, entonces todo primo impar que divide a n debe aparecer sólo a la primera potencia y debe ser uno más que una potencia de 2. Así, debemos tener que cada

$$p_t = 2^m + 1$$

para alguna m. Como -1 es un cero de $x^q + 1$ para q un primo impar, $x + 1$ divide $x^q + 1$ para q un primo impar. Así, si $m = q\nu$, donde q es un primo

impar, entonces $2^m + 1 = (2^\nu)^q + 1$ es divisible entre $2^\nu + 1$, por tanto, para que $p_i = 2^m + 1$ sea primo debe tenerse que m sea divisible sólo entre 2 de modo que p_i tiene que ser de la siguiente forma:

$$p_i = 2^{(2^k)} + 1,$$

Un **primo de Fermat**. Hemos demostrado que los únicos n-gonos regulares construibles son aquéllos en que los primos impares que dividen n son primos de Fermat cuyo cuadrado no divide n. En particular, los únicos p-gonos regulares que pueden ser construibles para p primo mayor que 2, son aquellos donde p es un primo de Fermat. ■

Ejemplo 4.4.1 *El 7-gono regular no es construible, pues 7 no es un primo de Fermat. Análogamente, el 18−gono regular no es costruible, pues aunque 3 es un primo de Fermat, su cuadrado divide al 18.* ■

Teorema 4.4.2 *El n-gono regular es construible con regla y compás si y sólo si todos los primos impares que dividen n son primos de Fermat cuyo cuadrado no divide n.*

Demostración. Sea ζ la raíz n-ésima primitiva del unitario $\cos(2\pi/n) + i sen(2\pi/n)$. Vimos antes que

$$2\cos\frac{2\pi}{n} = \zeta + \frac{1}{\zeta},$$

y que

$$\left[\mathbb{Q}\left(\zeta + \frac{1}{\zeta}\right) : \mathbb{Q}\right] = \frac{\varphi(n)}{2}.$$

Supongamos que $\varphi(n)$ es una potencia de 2^s de 2. Sea $E = \mathbb{Q}(\zeta + 1/\zeta)$. Tenemos que $\mathbb{Q}(\zeta + 1/\zeta)$ es el subcampo de $K = \mathbb{Q}(\zeta)$ que queda fijo bajo $H_1 = \{\iota, \tau\}$ donde ι es el elemento identidad de $G(K/\mathbb{Q})$ y $\zeta\tau = 1/\zeta$. Por el primer teorema de Sylow (ver el teorema 18.3 [1] pp. 170), existen subgrupos adicionales H_j de orden 2^j de $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ para $j = 0, 2, 3 \cdots, s$ tales que

$$\{\iota\} = H_0 < H_1 < \cdots < H_s = G(\mathbb{Q}(\zeta)/\mathbb{Q}).$$

Por la teoría de Galois,

$$\mathbb{Q} = K_{H_s} < K_{H_{s-1}} < \cdots < K_{H_1} = \mathbb{Q}\left(\zeta + \frac{1}{\zeta}\right),$$

Y $[K_{H_{j-1}} : K_{H_j}] = 2$. Nótese que $(\zeta + \frac{1}{\zeta}) \in \mathbb{R}$, de modo que $\mathbb{Q}(\zeta + \frac{1}{\zeta}) < \mathbb{R}$. Si $K_{H_{j-1}} = K_{H_j}(\alpha_j)$, entonces α_j es un cero del algún $(a_j x^2 + b_j x + c_j) \in K_{H_j}[x]$. Por la *fórmula cuadrática*, tenemos

$$K_{H_{j-1}} = K_{H_j}(\sqrt{b_j^2 - 4a_{jc_j}}).$$

En el teorema 4.1.2 vimos que las raíces cuadradas de un número constructible, son constructibles con regla y compás, por lo que, todo elemento en $\mathbb{Q}(\zeta + \frac{1}{\zeta})$, en particular, $cos(2\pi/n)$, es construible. De aquí que los n-gonos regulares donde $\varphi(n)$ es una potencia de 2, son construibles. ■

Ejemplo 4.4.3 *El 60-gono regular es construible, ya que*

$$60 = (2^2)(3)(5)$$

Y 3 y 5 son ambos primos de Fermat. ■

Bibliografía

[1] FRALEIGH, John B., *Álgebra abtracta: primer curso*, México: Sistemas Técnicos de Edición, 3a ed. (1988) 485 p.

[2] HERSTEIN, I. N., *Álgebra moderna: grupos, anillos, campos, teoría de Galois*, México: Trillas, 2a ed. (1990) 392 p.

[3] JACOBSON, N., *Basic Algebra I, II*, San Francisco: W,H. Freeman, (1974), (1980).

[4] KAPLANSKY, I., *Fields and Rings*, Chicago: Chicago ectures in mathematics, (1969)

[5] Mc CARTHY, P.J., *Algebraic extensions of Fields*, Waltham Mass: Blaisdell, (1966)