UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Extensiones Cíclicas de Campos

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemático

P R E S E N T A :

Benjamín Iván Juárez Santos

DIRECTOR DE TESIS:
Dra. Eugenia O´Reilly Regueiro

2015

Ciudad Universitaria, D. F.

ÍNDICE

CAPÍTULO 1. Grupos.....4

1.1 Grupos y subgrupos.....3
1.2 Clases laterales y subgrupos normales.....6
1.3 Homomorfismos.....11

CAPÍTULO 2. Anillos.....19

2.1 Anillos.....19
2.2 Homomorfismos y anillos cociente.....26
2.3 Extensiones de campos.....33

CAPÍTULO 3. Polinomios.....36

3.1 Dominios euclidianos.....36
3.2 Factorización única.....37
3.3 Anillos de polinomios.....39
3.4 Polinomios irreducibles.....44
3.5 Extensiones de campos y raíces de polinomios.....47

CAPÍTULO 4. El grupo de Galois.....56

4.1 Definiciones básicas.....56
4.2 Extensiones normales.....65
4.3 La correspondencia de Galois.....67
4.4 El teorema fundamental.....70

CAPÍTULO 5. Ecuaciones y Grupos.....73

5.1 Polinomios ciclotómicos.....73
5.2 Extensiones cíclicas.....76

APÉNDICE.....83

A. Grupos.....83
B. Campos.....85

INTRODUCCIÓN

El álgebra es una de las ramas más importantes en el estudio de las matemáticas, pues es la base sobre la que se apoyan éstas últimas. No hay ramas de las matemáticas, o son muy pocas, en las que no intervenga.

Es por ello que este trabajo está dedicado a su estudio. Sin embargo, no es un estudio general de álgebra, sino, más bien, un estudio de lo que se conoce como álgebra abstracta y, más en particular, de la teoría de grupos y de la teoría de anillos.

Hemos tratado de ser lo más claros posible, sobre todo al principio, en las demostraciones de los teoremas, incluyendo ejemplos tanto de cálculos como de demostración, de manera que facilitemos a los lectores su comprensión.

Algunos de los resultados presentados, conforme se va avanzando, dependen de otros anteriores, como se podrá apreciar en la prueba del teorema fundamental de la teoría de Galois, justificando el por qué de esta elección.

En el capítulo 1, se desarrolla, brevemente, la teoría de grupos, ya que es el fundamento para el estudio de los anillos, en particular, de la teoría de Galois. Se presentan conceptos y resultados básicos. En la parte de homomorfismo sólo se ha incluido el primer teorema de isomorfismos, porque consideramos que es el de mayor uso.

En el capítulo 2, se estudian estructuras con dos operaciones, llamadas anillos. Se definen conceptos y se dan resultados, básicos ambos. Conforme avancemos, podremos observar que dichos resultados son análogos a los de grupos, sobre todo la parte de homomorfismos, ideales y anillos cociente. Ya que el estudio de las extensiones de campos, también incluido en este capítulo, usa nociones de álgebra lineal, hemos mencionado el concepto de espacio vectorial, aunque no se han demostrado ciertos resultados que usaremos. Sin embargo, puede referirse el lector a la bibliografía.

En el capítulo 3, aparecen los polinomios, importantes para el desarrollo del capítulo 4. Muchos resultados de estos objetos, polinomios, son similares a los de los números enteros, que también constituyen un anillo. De esta manera, resulta que ya desde hace muchos años hemos trabajado con estructuras abstractas, ¡¡sin darnos cuenta!! Se estudian los campos, que serán el camino hacia la Teoría de Galois, y su relación con los polinomios, en la última sección.

El capítulo 4 resulta de relacionar la teoría de grupos y la teoría de campos: la teoría de Galois. Desde luego, aquí no puede faltar el clásico teorema fundamental de la teoría de Galois.

Finalmente, en el capítulo 5, el objeto de este trabajo, nos interesaremos en extensiones cuyos grupos de Galois son "manejables". Mostraremos que, en condiciones adecuadas, las extensiones cíclicas son extensiones radicales. Terminaremos con un resultado debido a Abel, el cual nos dice bajo qué condiciones el polinomio $x^m - a$ es irreducible sobre $\mathbb{Q}(\omega)$, donde ω es raíz de dicho polinomio en alguna extensión de campo.

CAPÍTULO 1

GRUPOS

1.1 Grupos y Subgrupos.

En este capítulo desarrollamos brevemente la teoría de grupos. Existen muchos temas interesantes acerca de ellos, sin embargo, nos limitaremos a incluir sólo lo necesario para el desarrollo de este trabajo, pues la relación fundamental de los grupos es con la teoría de Galois, de manera que también estamos interesados sólo en los grupos finitos.

En la primera sección damos los conceptos de grupos y subgrupos e incluimos algunos ejemplos y propiedades elementales.

DEFINICIÓN 1.1 Sea G un conjunto, $G \neq \varnothing$. Una ***operación binaria*** $*$, sobre G, es una función:

$$* : G \times G \longrightarrow G$$

Si $g, h \in G$, entonces denotamos por $g * h$ a la imagen de (g, h) bajo $*$.

EJEMPLO 1.2 En $\mathbb{Z}$, tenemos las operaciones binarias de $+$ (suma) y $\cdot$ (producto):

$$+, \cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(n, m) \mapsto n + m$$
$$(n, m) \mapsto n \cdot m$$

EJEMPLO 1.3 Sean $A = \{a, b, c\}$, $S_3 = \{f : A \longrightarrow A | f \text{ es biyectiva}\}$. Tenemos la operación de composición:

$$\circ : S_3 \times S_3 \longrightarrow S_3$$

Hay seis biyecciones en el conjunto A:

$$\begin{array}{cccccc} I : A \longrightarrow A, & \varphi : A \longrightarrow A, & \psi : A \longrightarrow A, & \gamma : A \longrightarrow A, & \sigma : A \longrightarrow A, & \xi : A \longrightarrow A \\ a \mapsto a & a \mapsto b & a \mapsto b & a \mapsto c & a \mapsto c & a \mapsto a \\ b \mapsto b & b \mapsto a & b \mapsto c & b \mapsto a & b \mapsto b & b \mapsto c \\ c \mapsto c & c \mapsto c & c \mapsto a & c \mapsto b & c \mapsto a & c \mapsto b \end{array}$$

Las funciones biyectivas sobre A se llaman ***permutaciones***, y frecuentemente las denotamos por:

$$f = \begin{pmatrix} a & b & c \\ f(a) & f(b) & f(c) \end{pmatrix}$$

De este modo:

$$S_3 = \left\{ I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \varphi = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, \psi = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \gamma = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \sigma = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, \xi = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \right\}$$

Aclaramos que la composición se toma como es usual: de derecha a izquierda. Por ejemplo, en $\psi \circ \varphi$ se aplica primero φ y luego ψ. (Ver ejemplo 1.17.)

DEFINICIÓN 1.4 Decimos que la operación binaria $* : G \times G \longrightarrow G$, es ***asociativa*** si:

$$(x * y) * z = x * (y * z), \ \forall x, y, z \in G$$

En este caso a la pareja $(G, *)$ se le llama ***semigrupo***.

EJEMPLO 1.5 Son semigrupos $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$.

DEFINICIÓN 1.6 Una terna $(M, *, e)$ es un ***monoide*** si $(M, *)$ es un semigrupo y e es un neutro para $*$, es decir:

$$e * a = a * e = a, \ \forall a \in M$$

EJEMPLO 1.7 Son monoides $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, \cdot, 1)$.

DEFINICIÓN 1.8 Un ***grupo*** es un monoide $(M, *, e)$ en el que cada elemento tiene inverso. Esto es:

$$\forall m \in M, \ \exists n \in M \ \ni \ m * n = e = n * m.$$

EJEMPLO 1.9 $(\mathbb{Z}, +, 0)$ es un grupo.

EJEMPLO 1.10 $(S_3, \circ, I)$ es un grupo.

Observación 1.11 En un grupo G hay un único elemento $e \in G$ tal que $e * a = a * e = a$, $\forall a \in G$.

Demostración. Supongamos que existe $f \in G$ tal que:

$$f * a = a * f = a, \ \forall a \in G$$

entonces, en particular para $a = e$, tenemos:

$$e = e * f = f. \ \blacksquare$$

Observación 1.12 En un grupo G cada elemento tiene un único inverso.

Demostración. Sea $g \in G$ y supongamos que existen $h, k \in G$ con la propiedad de que:

$$g * h = h * g = e \ \ y \ \ g * k = k * g = e$$

entonces:

$$h = e * h = (k * g) * h = k * (g * h) = k * e = k$$

$$\therefore h = k. \blacksquare$$

DEFINICIÓN 1.13 Al elemento e de G se le llama ***elemento identidad*** o ***neutro*** de G; y, si $b * a = e = a * b$, entonces b se llama ***inverso de a*** y se denota por a^{-1}.

DEFINICIÓN 1.14 El ***orden*** de un grupo G, denotado por $o(G)$ ó $|G|$, es la cardinalidad del conjunto G. Si $o(G)$ es finito, entonces G se llama ***grupo finito***.

DEFINICIÓN 1.15 Si la operación de un grupo G cumple con:

$$g * h = h * g, \ \forall g, h \in G$$

entonces llamamos a G un ***grupo conmutativo*** o ***abeliano***.

EJEMPLO 1.16 $(\mathbb{Z}, +, 0)$ y $(\mathbb{Z}_5 \backslash \{\overline{0}\}, \cdot, \overline{1})$ son grupos abelianos.

EJEMPLO 1.17 $(S_3, \circ, I)$ no es un grupo abeliano. Por ejemplo, tómense ψ y φ, entonces:

$$\psi \circ \varphi = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \circ \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} = \sigma,$$

por otro lado:

$$\varphi \circ \psi = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \circ \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = \xi.$$

$$\therefore \varphi \circ \psi \neq \psi \circ \varphi.$$

DEFINICIÓN 1.18 Sea G un grupo. Un subconjunto $H \neq \varnothing$ de G es un ***subgrupo***, de G, si H, con la operación de G, es en sí mismo un grupo. Escribimos $H \leq G$ para indicar que H es un subgrupo de G, y $H \not\leq G$ si no lo es.

Observación 1.19 Para cualquier grupo G, el conjunto G y el subconjunto $\{e\}$, de G, son subgrupos de G, los cuales se llaman ***subgrupos triviales***.

EJEMPLO 1.20 $(2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}, +, 0) < (\mathbb{Z}, +, 0)$.

EJEMPLO 1.21 $(\{I, \varphi\}, \circ, I) < (S_3, \circ, I)$.

EJEMPLO 1.22 $H = (\{I, \psi\}, \circ, I) \not\leq (S_3, \circ, I)$, ya que $\psi^{-1} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \gamma \notin H$.

Cuando sea claro quién es el neutro simplemente usaremos parejas, en vez de ternas, tanto para grupos como para subgrupos. A veces simplemente ponemos G, H, etc., para denotar grupos y subgrupos, sin poner la operación ni el neutro.

PROPOSICIÓN 1.23 Sea $H \neq \varnothing$, $H \subseteq G$. Entonces $H \leq G$ si y sólo si $a, b \in H$ implica $a * b^{-1} \in H$.

Demostración. $\Longrightarrow$) Si H es un subgrupo de G, entonces H es en sí mismo un grupo. De aquí, que:

$$a * b \in H \quad y \quad b^{-1} \in H, \ \forall a, b \in H$$

de donde:

$$a * b^{-1} \in H.$$

$\Longleftarrow$) Supongamos que $a * b^{-1} \in H$, $\forall a, b \in H$.

$H \neq \varnothing$, por hipótesis, así existe una $h \in H$. Entonces:

$$e = h * h^{-1} \in H.$$

Pero, entonces:

$$h^{-1} = e * h^{-1} \in H, \ \forall h \in H.$$

Y, por lo tanto:

$$a * (h^{-1})^{-1} = a * h \in H, \ \forall a, h \in H$$

Finalmente, la asociatividad de $*$ en H se sigue de la asociativiad en G.

$$\therefore H \leq G. \ \blacksquare$$

Observación 1.24 Si G es un grupo, entonces $(h^{-1})^{-1} = h$, $\forall h \in G$.

Demostración. Es fácil, ya que:

$$h^{-1} * h = e \text{ implica que } (h^{-1})^{-1} = h. \ \blacksquare$$

Ahora que hemos definido a los subgrupos construimos una clase especial de ellos, los llamados subgrupos normales, que serán importantes para definir a los grupos cociente.

1.2 Clases Laterales y Subgrupos Normales.

DEFINICIÓN 1.25 Para H y K subconjuntos no vacíos de un grupo G, definimos el conjunto HK como:

$$HK = \{h * k | h \in H, k \in K\}.$$

DEFINICIÓN 1.26 Sea G un grupo. Si $g \in G$ y H es un subgrupo de G, llamamos al conjunto:

$$gH = \{g * h | h \in H\}$$

una ***clase lateral izquierda de*** G ***con respecto a*** H, y al conjunto:

$$Hg = \{h * g | h \in H\}$$

una ***clase lateral derecha de*** G ***con respecto a*** H. En cualquier caso, al elemento g se le llama ***representante*** de la clase.

EJEMPLO 1.27 Sean $G = (S_3, \circ),\ H = \{I, \varphi\}\ y\ g = \psi$. Entonces:

$$Hg = H\psi = \{I \circ \psi, \varphi \circ \psi\} = \{\psi, \sigma\}$$

y,

$$gH = \psi H = \{\psi \circ I, \psi \circ \varphi\} = \{\psi, \xi\}$$

Nótese que, en este ejemplo, $Hg \neq gH$.

PROPOSICIÓN 1.28 Sean $H \leq G$ y $g, k \in G$. Entonces $Hg = Hk$ si y sólo si $gk^{-1} \in H$.

Demostración. $\Longrightarrow$) Supongamos que $Hg = Hk$, entonces, si $x \in Hg = Hk$, tenemos que:

$$x = hg = h_1 k,\ h, h_1 \in H \implies hgk^{-1} = h_1$$

$$\implies gk^{-1} = h^{-1}h_1 \in H$$

$$\therefore\ gk^{-1} \in H.$$

$\Longleftarrow$) Supongamos ahora que $gk^{-1} \in H$, entonces $gk^{-1} = h$, para alguna $h \in H$, entonces $g = hk$, y $k = h^{-1}g$. Veamos que $Hg = Hk$.

$\subseteq$) Sea $x \in Hg$, entonces:

$$x = h_1 g = h_1 hk \in Hk,\ h_1, h \in H \implies Hg \subseteq Hk$$

$\supseteq$) Sea $y \in Hk$, entonces:

$$y = h_1 k = h_1 h^{-1} g \in Hg,\ h_1 \in H \implies Hk \subseteq Hg$$

$$\therefore Hk = Hg.\ \blacksquare$$

De la misma manera, tenemos que:

PROPOSICIÓN 1.29 Bajo las mismas condiciones que en 1.28, tenemos que $gH = kH$ si y sólo si $g^{-1}k \in H$.

Demostración. $\Longrightarrow$) Supongamos que $gH = kH$ y sea $x \in gH$, entonces:

$$x = gh = kh_1,\ h, h_1 \in H$$

$$\implies gh = kh_1 \implies h = g^{-1}kh_1 \implies hh_1^{-1} = g^{-1}k, \text{ pero } hh_1^{-1} \in H$$

$$\therefore g^{-1}k \in H$$

$\Longleftarrow$) Si $g^{-1}k \in H$, entonces $g^{-1}k = h,\ h \in H$.

$\subseteq$) Sea $x \in gH$, entonces $x = gh_1,\ h_1 \in H$, pero $g = kh^{-1}$, así:

$$x = kh^{-1}h_1 \in kH$$

$$\therefore gH \subseteq kH$$

$\supseteq$) Sea $y \in kH$, entonces $y = kh_1,\ h_1 \in H$, pero $k = gh$, luego:

$$y = ghh_1 \in gH \Longrightarrow kH \subseteq gH$$

$$\therefore kH = gH. \blacksquare$$

TEOREMA 1.30 Si $H \leq G$, entonces la cardinalidad del conjunto de clases laterales derechas de H en G es igual a la cardinalidad del conjunto de clases laterales izquierdas de H en G.

Demostración. Sean $D = \{Hg | g \in G\}$ e $I = \{gH | g \in G\}$. Queremos ver que existe una función biyectiva:

$$f : D \longrightarrow I$$

Definimos $f : D \longrightarrow I$ mediante $f(Hg) = g^{-1}H$.

i) Supongamos que $f(Hg) = f(Hg_1),\ Hg, Hg_1 \in D$.

$$\Longrightarrow g^{-1}H = g_1^{-1}H$$

$$\Longrightarrow (g^{-1})^{-1}g_1^{-1} = gg_1^{-1} \in H, \text{ por la Proposición 1.29.}$$

$$\Longrightarrow Hg = Hg_1, \text{ por la Proposición 1.28.}$$

$$\therefore\ f \text{ es inyectiva.}$$

ii) Sea $gH \in I$ y veamos que $\exists d \in D$ tal que $f(d) = gH$. Sea $d = Hg^{-1}$, entonces:

$$f(d) = f(Hg^{-1}) = (g^{-1})^{-1}H = gH$$

$$\therefore\ f \text{ es suprayectiva.}$$

$$\therefore\ f \text{ es biyectiva.}$$

$$\therefore\ D \text{ e } I \text{ tienen la misma cardinalidad. } \blacksquare$$

DEFINICIÓN 1.31 Sea $H \leq G$. El ***índice*** de H en G, denotado por $[G : H]$, es la cardinalidad del conjunto de clases laterales derechas (o izquierdas) de H en G.

DEFINICIÓN 1.32 Sea $H \leq G$. Decimos que H es ***normal*** en G si $g^{-1}Hg = H,\ \forall\ g \in G$, y lo denotamos por $H \trianglelefteq G$.

Observación 1.33 Todo subgrupo de un grupo abeliano es un subgrupo normal.

Demostración. Sea $H \leq G$, G abeliano. Entonces para toda $g \in G$, $h \in H$, tenemos que:

$$g^{-1}hg = g^{-1}gh = eh = h. \blacksquare$$

TEOREMA 1.34 $H \trianglelefteq G$ si y sólo si $Hg = gH$, $\forall g \in G$.

Demostración. $\Longrightarrow$) Supongamos que $H \trianglelefteq G$ $g \in G$, entonces:

$$g^{-1}Hg = \{g^{-1}hg | h \in H\} = H$$

Es decir:

$$\forall k \in H,\ k = g^{-1}hg,\ h \in H.$$

Entonces:

$$gk = hg \in Hg$$

pero:

$$gk \in gH,$$

entonces:

$$gH \subseteq Hg \text{ y, análogamente, } Hg \subseteq gH$$

$$\therefore\ Hg = gH.$$

$\Longleftarrow$) Supongamos ahora que:

$$Hg = \{hg | h \in H\} = \{gh_1 | h_1 \in H\} = gH,\ g \in G$$

Veamos que $g^{-1}Hg = H$.

$\subseteq$) Sea $x \in g^{-1}Hg$, entonces:

$$x = g^{-1}h_2g,\ h_2 \in H$$
$$\Longrightarrow gx = h_2g \in Hg = gH$$
$$\Longrightarrow gx = gh_1,\ h_1 \in H$$
$$\Longrightarrow x = g^{-1}gh_1 = h_1 \in H$$
$$\therefore\ g^{-1}Hg \subseteq H.$$

$\supseteq$) Supongamos ahora que $h \in H$, tenemos que:

$$h = g^{-1}ghg^{-1}g$$
$$\Longrightarrow\ gh = ghg^{-1}g$$

pero sabemos que $Hg = gH$, y así:

$$gh = h_1g,\ h_1 \in H$$
$$\Longrightarrow ghg^{-1}g = h_1g$$
$$\Longrightarrow g^{-1}ghg^{-1}g = h = g^{-1}h_1g \in g^{-1}Hg$$
$$\therefore\ H \subseteq g^{-1}Hg$$
$$\therefore\ H = g^{-1}Hg$$
$$\therefore\ H \trianglelefteq G.\ \blacksquare$$

EJEMPLO 1.35 Sea $G = (S_3, \circ)$, $H = \{I, \psi, \psi^2\}$, entonces:

$$HI = \{I, \psi, \psi^2\}$$

$$H\varphi = \{\varphi, \xi, \sigma\}$$

$$IH = \{I, \psi, \psi^2\}$$

$$\varphi H = \{\varphi, \xi, \sigma\}$$

No es difícil verficar que $H\psi = \psi H = H\gamma = \gamma H = HI$ y también que $H\sigma = \sigma H = H\xi = \xi H = \varphi H$, y entonces tenemos que $Hg = gH, \forall g \in G$. De donde $H \lhd G$.

TEOREMA 1.36 Sea $H \trianglelefteq G$. Entonces el conjunto:

$$G/H = \{Hg | g \in G\}$$

es decir, el conjunto de todas las clases laterales derechas (o izquierdas) de H en G, forma un grupo, con la operación de G.

Demostración. Como:

$$He = \{he | h \in H\} = \{h | h \in H\} = H \in G/H$$

entonces $G/H \neq \varnothing$.

Ahora definimos:

$$* : G/H \times G/H \longrightarrow G/H$$

mediante: $(Hg_1) * (Hg_2) = H(g_1 g_2)$.

i) $*$ es binaria, por definición.

ii) Sean $g_1, g_2, g_3 \in G$, entonces:

$$((Hg_1)*(Hg_2))*(Hg_3) = (H(g_1g_2))*Hg_3 = H(g_1g_2)g_3 = Hg_1(g_2g_3) = Hg_1*(Hg_2g_3) = Hg_1*((Hg_2)*(Hg_3))$$

$$\therefore * \text{ es asociativa.}$$

iii) Si $g \in G$, entonces:

$$(Hg) * (He) = H(ge) = Hg$$

y,

$$(He) * (Hg) = H(eg) = Hg$$

$$\therefore He = H \text{ es el neutro.}$$

iv) Finalmente:

$$(Hg) * (Hg^{-1}) = H(gg^{-1}) = He$$

y,

$$(Hg^{-1}) * (Hg) = H(g^{-1}g) = He$$

$$\therefore\ Hg^{-1} \text{ es el inverso de } Hg.$$

$$\therefore\ G/H \text{ es un grupo } \blacksquare$$

Observación 1.37 Nótese que si G es abeliano, entonces:

$$HaHb = Hab = Hba = HbHa,\ \forall a, b \in G$$

de donde, G/H resulta ser abeliano.

DEFINICIÓN 1.38 Al grupo G/H se le llama el ***grupo cociente*** o ***grupo factor*** de G entre H, y su cardinalidad es $[G : H]$.

En esta última sección trabajamos el concepto, esencial para las estructuras que estudiaremos posteriormente, de homomorfismos de grupos, los cuales están estrechamente relacionados con los grupos cociente. Se trata de identificar a dos grupos como "el mismo", en cuyo caso decimos que son isomorfos, en el sentido de que poseen la misma estructura y propiedades. Terminamos con el primer teorema de isomorfismo, hay otros tres, pero éste es el que más aplicaciones tiene.

1.3 Homomorfismos.

DEFINICIÓN 1.39 Sean $(G, *)$ y $(G', *')$ grupos. Una función $f : G \longrightarrow G'$ tal que:

$$f(g * h) = f(g) *' f(h)\ \ \forall g, h \in G$$

se llama ***homomorfismo de grupos.***

Observación 1.40 Observemos que $g * h \in G$ y $f(g) *' f(h) \in G'$.

EJEMPLO 1.41 Sean $G_1 = (\mathbb{R}, +)$, $G_2 = (\mathbb{R} \setminus \{0\}, \cdot)$ y $f : G_1 \longrightarrow G_2$ dada por $f(a) = 2^a$. Entonces:

$$f(a + b) = 2^{a+b} = 2^a \cdot 2^b$$

por otro lado:

$$f(a) \cdot f(b) = 2^a \cdot 2^b$$

de esta manera, vemos que f es un homomorfismo.

EJEMPLO 1.42 Sean $f : G \longrightarrow G_1$ y $h : G_1 \longrightarrow G_2$ homomorfismos de grupos. Entonces $h \circ f : G \longrightarrow G_2$ también es un homomorfismo de grupos.

Prueba. Sean $g_1, g_2 \in G$, entonces:

$$\begin{aligned}(h \circ f)(g_1 * g_2) &= h(f(g_1 * g_2)) \\ &= h(f(g_1) *^1 f(g_2)), \quad \textit{pues } f \textit{ es homomorfismo} \\ &= h(f(g_1)) *^2 h(f(g_2)), \quad h \textit{ es homomorfismo} \\ &= (h \circ f)(g_1) *^2 (h \circ f)(g_2).\end{aligned}$$

$$\therefore\ h \circ f \text{ es un homomorfismo de grupos. } \blacksquare$$

Nota. $*, *^1, *^2$ denotan la operación en G, G_1 y G_2, respectivamente.

DEFINICIÓN 1.43 Sea f un homomorfismo de grupos. Si f es inyectiva, como función, la llamaremos ***monomorfismo de grupos***; si es suprayectiva, la llamaremos ***epimorfismo***; y, si es biyectiva, entonces la llamaremos ***isomorfismo.***

DEFINICIÓN 1.44 Si $f : G \longrightarrow G'$ es un isomorfismo de grupos, entonces decimos que G y G' son ***isomorfos*** y lo denotamos por $G \cong G'$. De esta definición, tenemos que para todo grupo G, $G \cong G$ con $Id : G \longrightarrow G$, la función identidad.

EJEMPLO 1.45 Si uno de dos grupos isomorfos es abeliano, entonces el otro también lo es.

Prueba. Sea $f : G \longrightarrow G'$ un isomorfismo, y supongamos que G es abeliano. Sabemos que, por ser f un homomorfismo, $f(xy) = f(x)f(y)$.

Sean $x',\ y' \in G'$. Como f es suprayectiva, existen $x,\ y \in G$ tales que $f(x) = x'$, y $f(y) = y'$. Pero, entonces:

$$f(xy) = f(x)f(y) = x'y',$$

y

$$f(yx) = f(y)f(x) = y'x'.$$

Como G es abeliano, tenemos que $xy = yx$. Entonces:

$$f(xy) = x'y' = f(yx) = y'x',$$

$$\implies \quad x'y' = y'x'.$$

$$\therefore \quad G' \text{ es abeliano. } \blacksquare$$

EJEMPLO 1.46 Si $G,\ H$ son grupos y $|G| \neq |H|$, entonces G no puede ser isomorfo a H.

Prueba. Supongamos que $f : G \longrightarrow H$ es un isomorfismo. Entonces dicho isomorfismo es, en particular, una función biyectiva, y así ambos conjuntos tienen la misma cardinalidad. Luego G y H no pueden ser isomorfos. $\blacksquare$

DEFINICIÓN 1.47 Un homomorfismo $f : G \longrightarrow G$ se llama ***endomorfismo de G***; y, un isomorfismo $f : G \longrightarrow G$ se llama ***automorfismo de G.***

DEFINICIÓN 1.48 Sea G un grupo y sea $a \in G$, definimos $a^0 = e,\ a^1 = a$; y si $n \geq 1$, $a^n = a^{n-1} * a$; y, también $a^{-n} = (a^{-1})^n$, para $n \geq 1$.

PROPOSICIÓN 1.49 Sea $f : G \longrightarrow H$ un homomorfismo y sea $a \in G$. Entonces:

$$f(a^n) = f(a)^n \quad \forall n \in \mathbb{Z}.$$

En particular, si $n = 0$, entonces $f(a^0) = f(e_G) = e_H$, y si $n = -1$, entonces $f(a^{-1}) = (f(a))^{-1}$.

Demostración. Por inducción sobre n.

CASO 1) $n \geq 0$. Si $n = 0$, veamos que $f(a^0) = f(e_G) = (f(a))^0 = e_H$. Pero:

$$f(a^0) = f(e_G) = f(e_G * e_G) = f(e_G) * f(e_G).$$

Por otro lado:

$$f(e_G) = f(e_G) * e_H.$$

Así:

$$\begin{aligned} f(e_G) * e_H &= f(e_G) * f(e_G) \\ \implies (f(e_G))^{-1} * (f(e_G) * e_H) &= (f(e_G))^{-1} * (f(e_G) * f(e_G)) \\ \implies ((f(e_G))^{-1} * f(e_G)) * e_H &= ((f(e_G))^{-1} * f(e_G)) * f(e_G) \\ \implies e_H * e_H &= e_H * f(e_G). \\ \therefore \quad e_H &= f(e_G). \end{aligned}$$

Supongamos ahora que:

$$f(a^n) = (f(a))^n, \ n \geq 0.$$

Entonces:

$$\begin{aligned} f(a^{n+1}) &= f(a^n * a) \\ &= f(a^n) * f(a) \\ &= f(a)^n * f(a) \\ &= f(a)^{n+1}. \end{aligned}$$

CASO 2) $n < 0$. Si $n = -1$, veamos que $f(a^{-1}) = f(a)^{-1}$. Ya que $f(a^{-1} * a) = f(e_G) = e_H$.

Pero:

$$\begin{aligned} f(a^{-1} * a) &= f(a^{-1}) * f(a) \\ \implies f(a^{-1}) * f(a) &= e_H \\ \implies (f(a^{-1}) * f(a)) * f(a)^{-1} &= e_H * f(a)^{-1} \\ \implies f(a^{-1}) * (f(a) * f(a)^{-1}) &= f(a)^{-1} \\ \implies f(a^{-1}) * e_H &= f(a)^{-1} \\ \therefore \quad f(a^{-1}) &= f(a)^{-1}. \end{aligned}$$

Supongamos que:

$$f(a^n) = f(a)^n, \ n < 0.$$

Entonces:

$$\begin{aligned} f(a^{n-1}) &= f(a^n * a^{-1}) \\ &= f(a^n) * f(a^{-1}) \\ &= f(a)^n * f(a)^{-1} \\ &= f(a)^{n-1}. \ \blacksquare \end{aligned}$$

DEFINICIÓN 1.50 Sean G y G' grupos y $f : G \longrightarrow G'$ un homomorfismo. Definimos el ***núcleo de f*** como:

$$\textbf{Núc(f)}= \{g \in G | f(g) = e'\},$$

donde e' es la identidad de G'. Y la ***imagen de f*** como:

$$\textbf{Imf} = \{g' \in G' | g' = f(g),\ g \in G\}.$$

EJEMPLO 1.51 Sea $f : G_1 \longrightarrow G_2$ el homomorfismo del ejemplo 1.41. Tenemos que:

$$Núc(f) = \{g \in G_1 | f(g) = e_2\} = \{g \in \mathbb{R} | f(g) = 1\} = \{g \in \mathbb{R} | 2^g = 1\} = \{0\}.$$

Antes de probar que el núcleo de un homomorfismo es un subgrupo normal del dominio, veamos el siguiente resultado que nos permitirá mostrar de manera un poco más rápida cuando un subgrupo es normal.

LEMA 1.52 Un subgrupo H de G es normal si y sólo si $g^{-1}Hg \subset H$, para cada $g \in G$.

Demostración. $\Longrightarrow$) Si $H \trianglelefteq G$, entonces $g^{-1}Hg = H$, para cada $g \in G$, en particular, $g^{-1}Hg \subset H$, para cada $g \in G$.

$\Longleftarrow$) Si $g^{-1}Hg \subset H$, veamos que $H \subset g^{-1}Hg$. Pero:

$$H = (gg^{-1})H(gg^{-1}) = g(g^{-1}Hg)g^{-1} \subset g^{-1}Hg,$$

la contención se da por el hecho de que $g^{-1}Hg \subset H$.

$$\Longrightarrow \quad H \subset g^{-1}Hg.$$

$$\therefore \quad g^{-1}Hg = H, \text{ y } H \trianglelefteq G. \ \blacksquare$$

TEOREMA 1.53 Si $f : G \longrightarrow H$ es un homomorfismo de grupos, entonces $\textbf{Núc(f)} \trianglelefteq G$.

Demostración. Notemos primero que Núc$(f) \neq \varnothing$, pues por la proposición 1.49, tenemos que $f(e_G) = e_H$, y así $e_G \in$Núc(f).

i) Veamos ahora que $\textbf{Núc(f)} \leq G$. Sean $a, b \in \textbf{Núc}(f)$ y mostremos que $a * b^{-1} \in \textbf{Núc}(f)$.
Como $a, b \in$Núc(f), entonces: $f(a) = e_H = f(b)$. Así:

$$\begin{aligned} f(a * b^{-1}) &= f(a) * f(b^{-1}) \\ &= f(a) * f(b)^{-1} \\ &= e_H * e_H^{-1} \\ &= e_H * e_H \\ &= e_H. \end{aligned}$$

La segunda igualdad se da por la proposición 1.49.

$$\therefore \quad a * b^{-1} \in \text{Núc}(f).$$

ii) Veamos ahora que Núc$(f) \trianglelefteq G$, es decir, de acuerdo con el Lema 1.52, que g^{-1}Núc$(f)g \subset$Núc$(f)\ \forall g \in G$.
Sea entonces $x \in$Núc(f), y mostremos que $g^{-1}xg \in$Núc(f). Pero:

$$\begin{aligned} f(g^{-1}xg) &= f(g^{-1})f(x)f(g) \\ &= f(g^{-1})e_H f(g) \\ &= f(g^{-1})f(g) \\ &= f(g^{-1}g) \\ &= f(e_G) \\ &= e_H, \end{aligned}$$

$$\implies \quad g^{-1}xg \in \text{Núc}(f).$$

$$\therefore \ \text{Núc}(f) \trianglelefteq G. \ \blacksquare$$

TEOREMA 1.54 Sea $N \trianglelefteq G$. Entonces la función $\pi : G \longrightarrow G/N$ definida por $\pi(a) = Na$, es un epimorfismo con núcleo N.

Demostración. Sean $a, b \in G$, entonces:

$$\pi(ab) = Nab = NaNb = \pi(a)\pi(b),$$

$$\therefore \ \pi \text{ es un homomorfismo.}$$

Sea $x = Na \in G/N$, se tiene que $Na = \pi(a), \ \ a \in G$ y así π es un epimorfismo. Finalmente:

$$\begin{aligned} Núc(\pi) &= \{g \in G | \pi(g) = e_{G/N}\} \\ &= \{g \in G | \pi(g) = N\} \\ &= \{g \in G | Ng = N\} \\ &= \{g \in G | g \in N\} \\ &= N. \blacksquare \end{aligned}$$

DEFINICIÓN 1.55 El epimorfismo π, del teorema anterior, se llama ***epimorfismo canónico*** ó ***proyección.***

COROLARIO 1.56 Si $f : G \longrightarrow H$ es un homomorfismo de grupos, entonces f es un monomorfismo si y sólo si Núc$(f) = \{e_G\}$.

Demostración. $\Longrightarrow$) Supongamos que f es inyectiva, es decir, un monomorfismo. Si $a \in$Núc(f), entonces: $f(a) = e_H$. Debemos mostrar que $a = e_G$.
Como f es un homomorfismo, entonces, por la Proposición 1.49:

$$f(e_G) = e_H.$$

Luego:

$$f(a) = f(e_G).$$

$$\implies \quad a = e_G, \text{ pues } f \text{ es monomorfismo.}$$

$$\therefore \quad Núc(f) = \{e_G\}.$$

$\Longleftarrow$) Supongamos ahora que Núc$(f) = \{e_G\}$, y sean $a, b \in G$ tales que $f(a) = f(b)$. Entonces:

$$f(a)f(b)^{-1} = e_H.$$

$$\implies \quad f(a)f(b^{-1}) = e_H,$$

$$\implies \quad f(ab^{-1}) = e_H,$$

$$\implies \quad a * b^{-1} \in Núc(f) = \{e_G\},$$

$$\implies \quad a * b^{-1} = e_G,$$

$$\implies \quad a = b.$$

$$\therefore \quad f \text{ es un monomorfismo. } \blacksquare$$

El Teorema siguiente es uno de los más importantes acerca de isomorfismos y es conocido como el ***Primer Teorema de Isomorfismos.***

TEOREMA 1.57 Sea $f : G \longrightarrow H$ un homomorfismo con núcleo N. Entonces $N \trianglelefteq G$ y $G/N \cong Imf$.

Demostración. Para que tenga sentido hablar de G/N, N debe ser normal en G, pero lo es, debido al teorema 1.53. Demostremos primero que $Imf = \{h \in H | h = f(g),\ g \in G\} \leq H$.

Como $e_H = f(e_G)$, entonces $e_H \in Imf$. Así $Imf \neq \varnothing$.
Sean $x, y \in Imf$, es decir $x = f(g_1),\ y = f(g_2),\ g_1, g_2 \in G$. Entonces:

$$f(g_1) * f(g_2)^{-1} = f(g_1 * g_2^{-1}).$$

Como $g_1 * g_2^{-1} \in G$, entonces:

$$f(g_1 * g_2^{-1}) \in Imf.$$

$$\therefore \quad Imf \leq H.$$

A continuación, definimos: $\overline{f} : G/N \longrightarrow Imf$, por $\overline{f}(Ng) = f(g)$.

Si $Na = Nb$, entonces $a * b^{-1} \in N$, es decir, $f(a * b^{-1}) = e_H$. Entonces:

$$\begin{aligned} e_H &= f(a * b^{-1}) \\ &= f(a) * f(b^{-1}) \\ &= f(a) * f(b)^{-1}, \end{aligned}$$

$$\therefore \quad f(a) = f(b), \text{ y así } \overline{f} \text{ está bien definida.}$$

Sean $Na,\ Nb \in G/N$. Entonces:

$$\begin{aligned} \overline{f}(Na * Nb) &= \overline{f}(N(a * b)) \\ &= f(a * b) \\ &= f(a) * f(b) \\ &= \overline{f}(Na) * \overline{f}(Nb) \end{aligned}$$

$$\therefore \quad \overline{f} \text{ es un homomorfismo.}$$

Si se tiene: $\overline{f}(Na) = \overline{f}(Nb)$, entonces:

$$\begin{aligned} f(a) = f(b) &\Longrightarrow \quad f(a) * f(b)^{-1} = e_H \\ &\Longrightarrow \quad f(a * b^{-1}) = e_H \\ &\Longrightarrow \quad a * b^{-1} \in N \\ &\Longrightarrow Na = Nb \end{aligned}$$

$$\therefore \quad \overline{f} \text{ es un monomorfismo.}$$

Finalmente, sea $f(a) \in Imf$, entonces existe $Na \in G/N$, tal que $\overline{f}(Na) = f(a)$, con lo que $\overline{f}$ es un epimorfismo y, en consecuencia es un isomorfismo, lo que completa la demostración. ■

Supongamos que queremos encontrar todos los grupos que son imágenes homomorfas de un grupo dado G. Es decir, los grupos H tales que existe un epimorfismo $f : G \longrightarrow H$.

Supongamos que H es una imagen homomorfa de G, entonces existe $f : G \longrightarrow H$ suprayectivo, y, por el Primer Teorema de Isomorfismo, sabemos que $G/N\acute{u}c(f) \cong H = Imf$. Es decir, tenemos que encontrar los subgrupos normales de G

EJEMPLO 1.58 Sea $G = (S_3, \circ)$. Tenemos que:

$$\{I\} \lhd S_3,$$

$$\{I, \psi, \psi^2\} \lhd S_3,$$

$$S_3 \lhd S_3$$

¿Cuántas imágenes homomorfas de S_3 hay?

Si H es una imagen homomorfa, entonces existe $f : S_3 \longrightarrow H$, suprayectivo; entonces por el Primer Teorema: $S_3/N\acute{u}c(f) \cong H$, y, además, $N\acute{u}c(f) \lhd S_3$.

De esta manera: $N\acute{u}c(f) = \{I\}$, ó $N\acute{u}c(f) = \{I, \psi, \psi^2\}$, ó $N\acute{u}c(f) = S_3$.

i) Si $N\acute{u}c(f) = \{I\}$, entonces $S_3 = S_3/\{I\} \cong H$.

ii) Si $N\acute{u}c(f) = \{I, \psi, \psi^2\}$, entonces $C_2 = S_3/\{I, \psi, \psi^2\} \cong H$,

en este caso, a C_2 se le llama ***grupo cíclico de orden 2.***

iii) Si $N\acute{u}c(f) = S_3$, entonces $\{e\} = S_3/S_3 \cong H$. ■

CAPÍTULO 2

ANILLOS

2.1 Anillos.

Ahora que hemos estudiado a los grupos, que son estructuras con una operación binaria, emprendemos nuestro estudio de conjuntos que tienen dos operaciones, los anillos, y, de los cuales, parte de su estructura resulta ser un grupo abeliano (aditivo.)

Ya desde la primaria trabajamos con los números enteros y sabemos cómo operar con ellos y también que hay tanto positivos como negativos.

Nos enseñan, además, a dividirlos (es decir que existe un algoritmo de la división en ellos), y que no siempre dado un entero existe otro tal que al multiplicarlos nos dé como resultado 1 (a estas alturas sabemos que dicho 1 se llama neutro multiplicativo; como veremos más adelante, no todos los anillos poseen dicho elemento).

¡Qué sorprendente puede parecernos hoy que en realidad hemos trabajado con un anillo desde entonces! Así pues, gracias a los enteros, algunos conceptos de anillos en general no resultarán difíciles de entender.

Empezamos este capítulo, al igual que con los grupos, con definiciones y propiedades básicas de anillos y subanillos, dando siempre ejemplos de dichos conceptos.

DEFINICIÓN 2.1 Un ***anillo*** es un conjunto no vacío equipado con dos operaciones binarias, suma $(+)$ y producto $(\cdot)$, tales que:

i) $(R, +, 0)$ es un grupo abeliano;
ii) $(R, \cdot)$ es un semigrupo;
iii) Se cumplen las leyes distributivas: para toda a, b, c en R:

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Escribiremos ab en lugar de $a \cdot b$.

DEFINICIÓN 2.2 Si en un anillo R se cumple que:

$$ab = ba, \quad \forall a, b \in R,$$

entonces decimos que R es un ***anillo conmutativo.***

DEFINICIÓN 2.3 Si en un anillo R existe un elemento $1 \in R$, tal que:

$$1a = a = a1, \quad \forall a \in R,$$

entonces llamamos a R ***anillo con unitario***. Al elemento 1 de R lo denotamos por 1_R.

PROPOSICIÓN 2.4 Sea R un anillo, entonces, para toda $a, b, c \in R$:

i) $0a = 0 = a0$;
ii) $a(-b) = (-a)b = -(ab)$;
iii) $(-a)(-b) = (ab)$;

si, además R tiene unitario, entonces:

iv) $(-1)a = -(1a) = -a, \ \forall a \in R$; y
v) $(-1)(-1) = 1$.

Demostración. Ver ([1]).■

Observemos que si R es un anillo con unitario 1 y no es el anillo trivial , entonces los elementos 0 y 1 son distintos, pues como $R \neq \{0\}$, existe un elemento $a \in R, \ a \neq 0$. Si 1 fuera igual a 0, entonces:

$$a = 1a = 0a = 0, \text{ y } a = 0, \text{ una contradicción. } \blacksquare$$

Así pues, si R es un anillo con unitario 1, supondremos que $1 \neq 0$, es decir no consideraremos el anillo trivial.

En lo que sigue, todos los anillos considerados serán conmutativos y con unitario.

EJEMPLO 2.5 $(\mathbb{Z}, +, \cdot), \ (\mathbb{R}, +, \cdot), \ (\mathbb{Q}, +, \cdot), \ (\mathbb{C}, +, \cdot)$, son anillos conmutativos con unitario. Aquí + y $\cdot$ denotan a la suma y producto usuales en los cuatro conjuntos.

EJEMPLO 2.6 El conjunto $M_{n\times n}(\mathbb{R})$ de matrices de $n \times n$ con coeficientes en $\mathbb{R}$, con la adición y multiplicación usuales, es un anillo con unitario que no es conmutativo.

EJEMPLO 2.7 El ***anillo trivial*** es el anillo que solamente tiene un elemento: $\{0\}$, y $0 + 0 = 0$, $0 \cdot 0 = 0$

DEFINICIÓN 2.8 Sea R un anillo conmutativo con unitario. Si para toda a, b, c en R, con $c \neq 0$, se tiene que:

$$ac = bc \implies a = b,$$

entonces, decimos que R es un ***dominio entero***.

EJEMPLO 2.9 $(\mathbb{Z}, +, \cdot)$ es un dominio entero.

DEFINICIÓN 2.10 Si en un anillo R conmutativo con unitario se tiene que para toda $a \neq 0$ existe un elemento $a^{-1} \in R$, tal que:

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

entonces, decimos que R es un ***campo***. Al elemento a^{-1} se le llama ***inverso multiplicativo*** de a.

EJEMPLO 2.11 $(\mathbb{C}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ son campos.

DEFINICIÓN 2.12 Dado un anillo conmutativo con unitario R, a los elementos de R que tienen un inverso multiplicativo se les llama ***unidades***.

PROPOSICIÓN 2.13 Sea R un anillo conmutativo con unitario. El conjunto:

$$U = \{a \in R | \exists b \in R(ab = 1)\}$$

de todas las unidades de R, forma un grupo abeliano bajo la multiplicación en R. A tal conjunto le llamaremos el ***grupo de unidades de*** R.

Demostración. Como R tiene unitario y $1 \cdot 1 = 1$, entonces $1 \in U$, y así $U \neq \varnothing$.
Ahora, sean $a, b \in U$, entonces existen $u, v \in R$ tales que:

$$au = 1 \text{ y } bv = 1,$$

de donde, como R es conmutativo:

$$1 = (ab)(uv) = a(bu)v = a(ub)v = (au)(bv)$$

$$\therefore \ ab \in U.$$

La asociatividad en U se sigue de la asociatividad en R. El neutro de U es el 1; y, como U consta de unidades, entonces cada elemento de U tiene un inverso multiplicativo.

Que U es abeliano también se sigue de R, ya que la operación de U es el producto de R y R es conmutativo.

$$\therefore \ U \text{ es un grupo abeliano. } \blacksquare$$

DEFINICIÓN 2.14 Sea R un anillo y sean $a, b \in R$ con $a, b \neq 0$. Si:

$$ab = 0,$$

entonces decimos que a y b son ***divisores de cero***. En este caso, a es un ***divisor izquierdo de cero*** y b es un ***divisor derecho de cero.***

EJEMPLO 2.15 En $\mathbb{Z}_6$ tenemos que 2, 3 y 4 son divisores de cero, ya que:

$$(2)(3) = (3)(2) = (4)(3) = (3)(4) = 0.$$

Observación 2.16 En un anillo R, $ab = ac$ o $ba = ca$, $a \neq 0$, implican que $b = c$ si y sólo si R no tiene divisores de cero.

Demostración. $\Longrightarrow$) Sea R un anillo en el cual:

$$ab = ac \implies b = c \ \ \forall a, b, c \in R, \ a \neq 0.$$

y supongamos que $ab = 0$ para algunas $a, b \in R$ y $a \neq 0$. Entonces:

$$ab = 0 = a0 \implies b = 0.$$

Análogamente, $b \neq 0$ implica $a = 0$, lo que significa que R no tiene divisores de cero.

De igual forma, al suponer que $ba = ca$ implica $b = c$ llegaremos a que R no tiene divisores de cero.

$\Longleftarrow$) Supongamos ahora que $ab = 0$ implica $a = 0$ o $b = 0$. Sea $a \neq 0$, así:

$$ab = ac \implies ab - ac = 0$$
$$\implies a(b - c) = 0$$
$$\implies b - c = 0 \text{ pues } a \neq 0$$
$$\implies b = c.$$

De la misma forma $ba = ca$ implica que $b = c$.
De aquí que en R se cumplen las leyes de cancelación. ■

Observación 2.17 Notemos que un divisor de cero nunca puede ser una unidad. Pues, supongamos, por ejemplo, que $a \in R$ es una unidad, y que $ab = 0$ para alguna $b \in R,\ b \neq 0$. Entonces $va = 1$ para alguna $v \in R$, y así:

$$b = 1b = (va)b = v(ab) = v0 = 0,$$

lo cual es una contradicción. Similarmente, si $ba = 0$ para alguna $b \neq 0$. De esta manera, a no puede ser una unidad.

Esto muestra, en particular, que los campos no tienen divisores de cero.

TEOREMA 2.18 Si K es un campo, entonces K es un dominio entero.

Demostración. Sea K un campo y veamos que K no admite divisores de cero; es decir, veamos que $ab = 0$ implica $a = 0$ o $b = 0$, para algunas $a, b \in K$.

Supongamos entonces que $ab = 0$ con $a \neq 0$. Entonces:

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

$\therefore$ K no admite divisores de cero, y como es campo entonces es conmutativo y tiene unitario.

$\therefore$ K es un dominio entero. ■

TEOREMA 2.19 Cualquier dominio entero finito es un campo.

Demostración. Ver ([2]). ■

PROPOSICIÓN 2.20 Sea R un anillo. Entonces, para todas $a, b \in R$ y para todos $m, n \in \mathbb{Z}$, tenemos que:

$$(na)b = n(ab) = a(nb),$$

y

$$(na)(mb) = (nm)(ab),$$

donde na significa $a + a + \cdots + a$, n veces.

Demostración. Tenemos que:

$$(na)b = (\underbrace{a + a + \cdots + a}_{n})b = \underbrace{ab + ab + \cdots + ab}_{n} = n(ab)$$

Por otro lado, tenemos que:

$$a(nb) = a(\underbrace{b + b + \cdots + b}_{n}) = \underbrace{ab + ab + \cdots + ab}_{n} = n(ab)$$

$$\therefore\ (na)b = n(ab) = a(nb).$$

De la misma manera:

$$\begin{aligned}
(na)(mb) &= (\underbrace{a + a + \cdots + a}_{n})(\underbrace{b + b + \cdots + b}_{m}) \\
&= \underbrace{(a + a + \cdots + a)b + (a + a + \cdots + a)b + \cdots + (a + a + \cdots + a)b}_{m} \\
&= \underbrace{(ab + \cdots + ab)}_{n} + \underbrace{(ab + \cdots + ab)}_{n} + \cdots + \underbrace{(ab + \cdots + ab)}_{n} \\
&= \underbrace{n(ab) + n(ab) + \cdots + n(ab)}_{m} \\
&= (nm)(ab).
\end{aligned}$$

$$\therefore\ (na)(mb) = (nm)(ab).\ \blacksquare$$

DEFINICIÓN 2.21 Sea K un campo. La ***característica de K***, $carK$, se define como el menor entero positivo n tal que $n1_K = 0$, si existe tal n; si no existe, entonces la característica se define como 0.

TEOREMA 2.22 Sea K un campo, entonces:

$$carK = 0,$$

$$\text{o } carK = p,\ p \text{ primo.}$$

Demostración. Supongamos que $carK \neq 0$. Entonces $carK = n$. Supongamos que $n = rs$, donde $1 < r < n,\ 1 < s < n$. Por la propiedad de n, tenemos que $r1_K \neq 0,\ s1_K \neq 0$. Por otro lado, por el teorema 2.20 tenemos que:

$$(r1_K)(s1_K) = (rs)1_K = n1_K = 0,$$

lo cual no puede ser posible, pues K no tiene divisores de cero. $\blacksquare$

EJEMPLO 2.23 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ tienen característica cero.

EJEMPLO 2.24 $(\mathbb{Z}_5, +, \cdot)$ es un campo de característica 5:

$$\overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{5} = \overline{0}.$$

EJEMPLO 2.25 Si K es un campo de característica p, entonces tenemos que para toda $x, y \in K$:

$$(x + y)^p = x^p + y^p$$

ya que, por el teorema del binomio:

(1)

$$(x + y)^p = \sum_{r=0}^{p} \binom{p}{r} x^{p-r} y^r$$

Para $r = 1, ..., p - 1$, el coeficiente binomial:

$$\binom{p}{r} = \frac{p(p-1) \cdots (p-r+1)}{r!}$$

es un entero, y así $r!$ divide a $p(p-1) \cdots (p-r+1)$. Como p es primo y $r < p$, ningún factor de $r!$ puede ser divisible por p. De donde $r!$ divide a $(p-1) \cdots (p-r+1)$ y así $\binom{p}{r}$ es un entero divisible por p. Entonces, para $r = 1, ..., p - 1$:

$$\binom{p}{r} x^{p-r} y^r \equiv 0 \ (mod p)$$

y, por lo tanto, en (1), sólo el primer y el último términos sobreviven, lo que da el resultado.

DEFINICIÓN 2.26 Un subconjunto $S \neq \varnothing$ de un anillo R es un ***subanillo de R*** si S con las operaciones de R es, en sí mismo, un anillo.

PROPOSICIÓN 2.27 Un subconjunto $S \neq \varnothing$ de un anillo R es un subanillo de R si y sólo si $\forall a, b \in S$ se tiene que $a - b \in S$ y $ab \in S$.

Demostración. $\Longrightarrow$) Supongamos que S es un subanillo de R. Entonces S es un anillo y así $ab \in S, \quad \forall a, b \in S$.

Como S es también un grupo abeliano bajo la adición, tenemos entonces que todo elemento $b \in S$ tiene un inverso aditivo $-b \in S$ y S es cerrado bajo la adición, así $a + b \in S, \ \forall a, b \in S$, luego, $a + (-b) = a - b \in S$.

$\Longleftarrow$) Supongamos ahora que $\forall a, b \in S$ se tiene que $a - b \in S$ y $ab \in S$.

Entonces, por la Proposición 1.23, en notación aditiva, se tiene que S es un grupo abeliano bajo la adición.

Por otro lado, como $S \subseteq R$, entonces su asociatividad y las leyes distributivas las hereda de R. Por lo tanto S es un subanillo de R. ■

Observación 2.28 Para cualquier anillo $R \neq \{0\}$, R y $\{0\}$ son subanillos de R, los ***subanillos triviales.***

EJEMPLO 2.29 $(2\mathbb{Z}, +, \cdot)$ es un subanillo de $(\mathbb{Z}, +, \cdot)$.

EJEMPLO 2.30 Sea R un anillo, el conjunto:

$$Z(R) = \{a \in R | ar = ra, \ \forall r \in R\}$$

es un subanillo de R. A este conjunto se le conoce como el ***centro de R***.

Demostración. Notemos primero que $Z(R) \neq \varnothing$ pues $0 \in Z(R)$.
Ahora, sean $a, b \in Z(R)$ y $r \in R$, entonces:

$$r(a-b) = ra - rb = ar - br = (a-b)r.$$

$$\therefore \ a - b \in Z(R).$$

Y también:

$$r(ab) = (ra)b = (ar)b = a(rb) = a(br) = (ab)r.$$

$$\therefore \ ab \in Z(R)$$

$\therefore$ $Z(R)$ es un subanillo de R, por la Proposición 2.27. ■

2.2 Homomorfismos y Anillos cociente.

DEFINICIÓN 2.31 Sean R y S anillos. Un ***homomorfismo de anillos*** es una función $f : R \longrightarrow S$ tal que:

i) $f(a+b) = f(a) + f(b), \ \forall a, b \in R$,
ii) $f(ab) = f(a)f(b), \forall a, b \in R$.

DEFINICIÓN 2.32 Sea $f : R \longrightarrow S$ un homomorfismo. Entonces el ***núcleo de f*** es el conjunto:

$$K = \{r \in R | f(r) = 0_S\}.$$

DEFINICIÓN 2.33 Un homomorfismo biyectivo se llama ***isomorfismo.*** Decimos que R y S son ***isomorfos*** y escribimos $R \cong S$.

EJEMPLO 2.34 La función $f : \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$, definida al enviar un entero par a 0 y un entero impar a 1 es un homomorfismo de anillos. La función es aditiva, ya que la suma de dos enteros pares o impares es par, y la suma de un entero par y un impar es impar. La función es multiplicativa, pues el producto de dos enteros impares es impar y el producto de un entero par con cualquier entero es par. El núcleo de f es el conjunto de enteros pares.

PROPOSICIÓN 2.35 Sean R y S anillos y sea $f : R \longrightarrow S$ un homomorfismo. Entonces:

i) $f(0_R) = 0_S$;
ii) $f(-r) = -f(r), \ \forall r \in R$;
iii) La imagen de f es un subanillo de S; y,

iv) El núcleo, K, de f es un subanillo de R. Además, si $\alpha \in K$, entonces $r\alpha, \alpha r \in K,\ \forall r \in R$; es decir, K es cerrado bajo la multiplicación con elementos de R.

Demostración. *i*) Como:

$$f(r) + f(0_R) = f(r + 0_R) = f(r),$$

tenemos que:

$$f(0_R) = 0_S + f(0_R) = -f(r) + f(r) + f(0_R) = -f(r) + f(r) = 0_S,$$

de donde:

$$f(0_R) = 0_S.$$

ii) Para toda r in R se tiene:

$$f(r) + f(-r) = f(r + (-r)) = f(0_R) = 0_S = f(r) + (-f(r)),$$

así:

$$f(-r) = -f(r).$$

iii) De:

$$f(r_1 - r_2) = f(r_1) + f(-r_2) = f(r_1) - f(r_2) \in Imf,$$

y,

$$f(r_1 r_2) = f(r_1)f(r_2) \in Imf,$$

concluimos que la imagen de f es un subanillo de S.

iv) Sean $\alpha, \beta \in K$. Entonces:

$$f(\alpha) = f(\beta) = 0.$$

$$\Longrightarrow\ f(\alpha - \beta) = 0, \text{ y } f(\alpha\beta) = 0.$$

$$\therefore\ \ K \text{ es un subanillo de } R.$$

Similarmente, para cualquier $r \in R$:

$$f(r\alpha) = f(r)f(\alpha) = f(r)0 = 0,$$

$$f(\alpha r) = f(\alpha)f(r) = 0f(r) = 0.$$

$$\therefore\ \ r\alpha, \alpha r \in K. \ \blacksquare$$

De la misma manera que se hizo en grupos, los homomorfismos que son inyectivos y suprayectivos reciben nombres específicos.

DEFINICIÓN 2.36 Sea $f : R \longrightarrow S$ un homomorfismo. Si f es inyectivo, lo llamaremos ***monomorfismo***; si f es suprayectivo, lo llamaremos ***epimorfismo***; y, si $f : R \longrightarrow R$ es un isomorfismo, entonces se llamará ***automorfismo.***

DEFINICIÓN 2.37 Un subanillo J de un anillo R se llama ***ideal bilateral***, o simplemente ***ideal***, si:

i) $0_R \in J$, donde 0_R denota el neutro aditivo de R;
ii) $a, b \in J$ implica $a - b \in J$; y
iii) $r \in R,\ j \in J$ implica $rj \in J$ y $jr \in J$.

EJEMPLO 2.38 Sea R un anillo conmutativo y sea a un elemento fijo de R. Entonces el conjunto:

$$I_a = \{x \in R | ax = 0_R\}$$

es un ideal de R.

Demostración. *i*) Como $a0_R = 0_R$, entonces $0_R \in I_a$.

ii) Supongamos que $x, y \in I_a$. Queremos ver que $x - y \in I_a$. Tenemos que:

$$a(x - y) = ax - ay = 0_R - 0_R = 0_R \implies x - y \in I_a.$$

iii) Finalmente, sea $r \in R$ y $x \in I_a$, y veamos que rx y xr pertenecen a I_a. Como R es un anillo conmutativo, es suficiente mostrar que $rx \in I_a$. Tenemos que:

$$a(rx) = (ar)x = (ra)x = r(ax) = r0_R = 0_R \implies rx \in I_a.$$

$$\therefore\ I_a \text{ es un ideal de } R. \blacksquare$$

Recordemos que en un anillo R, $(R, +)$ es un grupo abeliano, así, de acuerdo con la observación 1.33, todo subgrupo de él es normal. Por lo tanto, si $I \lhd R$ podemos entonces construir el grupo R/I. Quisiéramos que R/I no sólo tuviera estructura de grupo sino, además, de anillo, lo cual haremos a continuación.

TEOREMA 2.39 Sea I un ideal de un anillo R. Entonces R/I resulta un anillo al definir la suma por $(a + I) + (b + I) = (a + b) + I$, y producto dado por $(a + I)(b + I) = ab + I$.

Demostración. Como I es un ideal de R, entonces $(I, +)$ es un subgrupo de $(R, +)$. Así, tenemos un grupo cociente bien definido R/I, donde los elementos son las clases de I en R, esto es:

$$R/I = \{r + I | r \in R\},$$

y la operación binaria de adición es dada por $(a + I) + (b + I) = (a + b) + I,\ \ \forall a, b \in R$. Veamos ahora que el producto está bien definido, es decir, si $a + I = a' + I$, y $b + I = b' + I$, entonces $ab + I = a'b' + I$.

Si $a + I = a' + I$, entonces:

$$a + I = \{a + i | i \in I\} = \{a' + i | i \in I\} = a' + I,$$

y, análogamente para $b + I$. De estas igualdades surgen las contenciones:

$$a' + I \subset a + I, \text{ y } b' + I \subset b + I,$$

lo cual significa que existen $x, y \in I$ tales que $a' = a + x$, y $b' = b + y$. De donde:

$$a'b' = (a + x)(b + y) = ab + ay + xb + xy.$$

Como I es un ideal, entonces:

$$a'b' - ab = ay + xb + xy \in I,$$

$$\implies a'b' - ab \in I.$$

$$\therefore \quad a'b' + I = ab + I, \text{ por Proposición 1.29, en notación aditiva.}$$

$$\therefore \text{ la multiplicación en } R/I \text{ está bien definida.}$$

Para ver que R/I es un anillo, sólo hay que verificar los axiomas restantes de anillo, lo cual se puede consultar en ([3]). ■

Observación 2.40 Si R es conmutativo, entonces:

$$(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I),$$

y así, R/I es conmutativo.

Observación 2.41 Si R tiene unitario, entonces:

$$(a + I)(1 + I) = a \cdot 1 + I = a + I,$$

luego, R/I tiene unitario, también: $1 + I$. Notemos que si $1 \in I$, entonces $I = R$.

DEFINICIÓN 2.42 El anillo R/I se llama ***anillo cociente de*** R ***relativo a*** I**.**

TEOREMA 2.43 PRIMER TEOREMA DE ISOMORFISMO PARA ANILLOS. Sea $f : R \longrightarrow S$ un homomorfismo de anillos, entonces:

i) El núcleo K de f es un ideal de R;
ii) la imagen de f es un subanillo de S; y,
iii) $R/K \cong Imf$.

Demostración *i*) y *ii*) son *iv*) y *iii*) de la Proposición 2.35.
iii) Definimos $\overline{f} : R/K \longrightarrow S$ por $\overline{f}(r + K) = f(r)$. $\overline{f}$ es función, pues, si $r + K = r' + K$, entonces $r - r' \in K$,

$$\begin{aligned} &\implies f(r - r') = 0, \\ &\implies f(r) = f(r'), \\ &\implies \overline{f}(r + K) = \overline{f}(r' + K.) \end{aligned}$$

Por el Primer Teorema de Isomorfismo para grupos, $\overline{f}$ es homomorfismo de grupos. Ahora, sean $r + K, r' + K \in R/K$. Entonces:

$$\begin{aligned} \overline{f}((r + K)(r' + K)) &= \overline{f}((rr') + K) \\ &= f(rr') \\ &= f(r)f(r') \\ &= \overline{f}(r + K)\overline{f}(r' + K), \end{aligned}$$

$$\therefore \ \overline{f} \text{ es homomorfismo de anillos.}$$

Ahora, si $s \in Imf$, entonces existe $r \in R$ tal que $f(r) = s$. Esto significa que $\overline{f}(r + K) = s$, y, de esta manera, $\overline{f}$ es suprayectiva. Finalmente, si $\overline{f}(r + K) = \overline{f}(r' + K)$, entonces:

$$f(r) = f(r'),$$

$$\Longrightarrow\ f(r - r') = 0,$$

$$\Longrightarrow\ r - r' \in K,$$

$$\Longrightarrow\ r + K = r' + K,$$

$$\therefore\ \overline{f} \text{ es inyectiva y, en consecuencia, es biyectiva.}$$

$$\therefore\ R/K \cong Imf. \blacksquare$$

TEOREMA 2.44 Si I es cualquier ideal de R, entonces la función $f : R \longrightarrow R/I$ definida por $r \mapsto r + I$ es un epimorfismo con núcleo I.

Demostración. Si I es cualquier ideal, entonces R/I es un anillo (en particular, es un grupo abeliano) y la función $f : r \mapsto r + I$ es un homomorfismo de grupos de núcleo I. Sólo hay que ver que f es un homomorfismo de anillos, pero como:

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

entonces, hemos terminado. ■

DEFINICIÓN 2.45 El epimorfismo del teorema anterior se llama ***proyección natural de*** R ***sobre*** R/I.

EJEMPLO 2.46 **a)** Sea R un anillo con unitario 1_R, veamos que si I es un ideal de R que posee una unidad a de R, entonces $I = R$.

Pues sea entonces a una unidad de R y supongamos que $a \in I$. Como I es cerrado bajo multiplicación por elementos de R, tenemos que:

$$1_R = a^{-1}a \in I,$$

y así, para cualquier $r \in R$:

$$r = r \cdot 1_R \in I,$$

lo cual muestra que $R \subseteq I$; y, como $I \subseteq R$, entonces $I = R$, como queríamos.

b) Ahora, usando lo anterior probemos que un campo no contiene ideales propios.

Prueba. Sea I un ideal de un campo R, $I \neq \{0_R\}$. Sea $a \in I,\ a \neq 0_R$. Como R es un campo, a es una unidad de R y, por a), $I = R$. De donde los únicos posibles ideales son $\{0\}$ y R, y no existen ideales propios. ■

c) Finalmente, usando lo anterior y el primer teorema de isomorfismo para anillos, mostremos que si f es un homomorfismo de un campo F a un anillo R, entonces la imagen de f o es isomorfa a F o es

$\{0_R\}$.

Demostración. Por el teorema 2.43, la imagen $f(F)$ es isomorfa al anillo cocienteF/I, donde I es un ideal de F. Por b), los únicos ideales de F son $\{0\}$ y F. Si $I = \{0\}$, entonces $F/I = \{a + \{0\}|a \in F\}$, y así $f(F)$ es isomorfo a F. Si $I = F$, entonces F es el núcleo de f, y $f(F) = \{0_R\}$. ■

DEFINICIÓN 2.47 Un ideal M en un anillo arbitrario S se llama ***ideal máximo*** si $M \neq S$ y los únicos ideales que contienen a M son M y S. En otras palabras, para cada ideal N tal que $M \subset N \subset S$, se tiene que ó $N = M$, ó $N = S$.

EJEMPLO 2.48 El ideal $3\mathbb{Z}$ es máximo en $\mathbb{Z}$, pero el ideal $4\mathbb{Z}$ no lo es, pues $4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Sea J un ideal de un anillo conmutativo con unitario R, y sea $a \in R$. Consideremos el conjunto:

$$I = \{ra + t|r \in R, t \in J\}.$$

¿Qué propiedades tiene este conjunto? En primer lugar, notemos que como:

$$0_R = a \cdot 0_R + 0_R \in I,$$

entonces $I \neq \varnothing$. Ahora, si $r_1a + t_1, r_2a + t_2 \in I$, entonces:

$$(r_1a + t_1) - (r_2a + t_2) = (r_1 - r_2)a + (t_1 - t_2) \in I.$$

Además, si $r_1 \in R,\ ra + t \in I$, se tiene que:

$$r_1(ra + t) = (r_1r)a + (r_1t \in I),$$

y como R es conmutativo, también $(ra + t)r_1 \in I$. Todo esto significa que el subanillo I es un ideal de R. Con esto, estamos ahora en disposición de probar nuestro siguiente resultado.

TEOREMA 2.49 Sea R un anillo conmutativo con unitario y J un ideal de R. Entonces R/J es campo si y sólo si J es un ideal máximo.

Demostración. $\Longrightarrow$) Supongamos que R/J es campo y que $J \subseteq I$, I ideal de R. Consideremos la proyección natural $f : R \longrightarrow R/J$. Como f es un epimorfismo, sucede que $f(I)$ es ideal de R/J, y como este último es campo, entonces sus únicos ideales son R/J y $\{J\}$, es decir $f(I) = R/J$ ó $f(I) = J$. Pero entonces $I = R$ ó $I = J$. Así I es máximo.

$\Longleftarrow$) Supongamos que J es máximo, y sea $a + J \in R/J,\ a \notin J$. Sea:

$$I = \{ra + t|r \in R, t \in J\},$$

que, como ya hemos visto, es un ideal de R. Por otro lado:

$$a = 1 \cdot a + 0 \text{ implica que } a \in I,$$

y, para cada $t \in J$ se tiene que:

$$t = 0a + t \text{ implica } t \in I, \text{ que a su vez implica que } J \subsetneq I.$$

Como J es máximo, entonces $I = R$, y , con esto $1 \in I$. Así 1 se puede escribir como $1 = ra+t,\ r \in R, t \in J$. Pero entonces:

$$\begin{aligned} 1 + J &= ra + t + J \\ &= ra + J \\ &= (r + J)(a + J) \end{aligned}$$

la segunda igualdad se da porque $t \in J$. En consecuencia $(r + J)$ es inverso de $a + J$. Por lo tanto R/J es campo. ■

PROPOSICIÓN 2.50 Sea $A = \{t_1, ..., t_n\}$ un subconjunto finito de un anillo conmutativo R. Entonces el conjunto:

$$Rt_1 + Rt_2 + \cdots + Rt_n = \{x_1t_1 + x_2t_2 + \cdots + x_nt_n | x_1, ..., x_n \in R\}$$

es el ideal más pequeño de R que contiene a A.

Demostración. Sean $x_1, ..., x_n, y_1, ..., y_n \in R$, entonces:

$$\begin{aligned} (x_1t_1 + \cdots + x_nt_n) - (y_1t_1 + \cdots + y_nt_n) &= x_1t_1 + \cdots + x_nt_n + (-y_1t_1) + \cdots + (-y_nt_n) \\ &= x_1t_1 + (-y_1t_1) + \cdots + x_nt_n + (-y_nt_n) \\ &= (x_1 - y_1)t_1 + \cdots + (x_n - y_n)t_n \in Rt_1 + \cdots + Rt_n \end{aligned}$$

y, si $r \in R$, entonces:

$$\begin{aligned} r(x_1t_1 + \cdots + x_nt_n) &= r(x_1t_1) + \cdots + r(x_nt_n) \\ &= (rx_1)t_1 + \cdots + (rx_n)t_n \in Rt_1 + \cdots + Rt_n \end{aligned}$$

de igual forma:

$$\begin{aligned} (x_1t_1 + \cdots + x_nt_n)r &= (x_1t_1)r + \cdots + (x_nt_n)r \\ &= (rx_1)t_1 + \cdots + (rx_n)t_n \in Rt_1 + \cdots + Rt_n \end{aligned}$$

$$\therefore\ Rt_1 + \cdots + Rt_n \text{ es un ideal de } R.$$

Sea J un ideal tal que $A \subseteq J$. Entonces:

$$x_1t_1, ..., x_nt_n \in J,$$

y, por ser J subanillo:

$$x_1t_1 + \cdots + x_nt_n \in J,$$

así $Rt_1 + \cdots + Rt_n \subset J$

$$\therefore Rt_1 + \cdots + Rt_n \text{ es el ideal más pequeño que contiene a } A. \blacksquare$$

DEFINICIÓN 2.51 Al ideal $Rt_1 + \cdots + Rt_n$ se le llama ***ideal generado por*** $t_1, ..., t_n$, y se denota por $\langle t_1, ..., t_n \rangle$. Si este ideal es generado por un solo elemento $t \in R$, entonces decimos que $Rt = \langle t \rangle$ es un ***ideal principal.***

DEFINICIÓN 2.52 Un ideal generado por un conjunto finito se llama ***ideal finitamente generado.***

DEFINICIÓN 2.53 Un ***anillo de ideales principales*** es un anillo en el cual cada ideal es principal. Si en un dominio entero cada ideal es principal, entonces lo llamaremos ***dominio de ideales principales.***

2.3 Extensiones de Campos.

DEFINICIÓN 2.54 Un ***espacio vectorial*** es una quinteta ordenada $(V, +, 0, F, \cdot)$ tal que:

i) $(V, +, 0)$ es un grupo abeliano;
ii) F es un campo;
iii) $\cdot$ es una función $\cdot : F \times V \longrightarrow V$, llamada ***multiplicación escalar***, que cumple con lo siguiente, para toda v, w en V y para toda α, β en F:

a) $1v = v$;
b) $(\alpha\beta)v = \alpha(\beta v)$;
c) $(\alpha + \beta)v = \alpha v + \beta v$;
d) $\alpha(v + w) = \alpha v + \alpha w$.

A los elementos de V los llamaremos ***vectores*** y a los de F ***escalares.***

DEFINICIÓN 2.55 Un ***subcampo*** E de un campo K es un subanillo, el cual es un campo. Si $E \subset K$ entonces decimos que E es un ***subcampo propio de K.***

EJEMPLO 2.56 Todo campo es un espacio vectorial sobre cualquiera de sus subcampos, incluido él mismo.

DEFINICIÓN 2.57 Si K es un campo que contiene al campo F, entonces decimos que K es una ***extensión de F*** y lo denotaremos por K/F.

Así pues, K es una extensión de F si F es un subcampo de K.

EJEMPLO 2.58 Como $\mathbb{R} \subset \mathbb{C}$ y ambos son campos, entonces $\mathbb{C}$ es una extensión de $\mathbb{R}$.

Si K/F es cualquier extensión de campos, entonces la multiplicación definida en K hace de K un espacio vectorial sobre F.

DEFINICIÓN 2.59 El ***grado*** ó ***índice*** de una extensión de campos K/F, denotado por $[K : F]$, es la dimensión de K como espacio vectorial sobre F. Decimos que la extensión es ***finita*** si $[K : F]$ lo es, e ***infinita*** en caso contrario.

TEOREMA 2.60 Sea K/F una extensión de campos. Entonces $K = F$ si y sólo si $[K : F] = 1$.

Demostración. $\Longrightarrow$) Supongamos que $K = F$. Debemos encontrar una base para K sobre F que tenga un sólo elemento. Pero como $1 \in K$ y cada elemento $x \in K$ se puede expresar como $x1$ con $x \in F$,

entonces $\{1\}$ es un conjunto generador para K sobre F. Además si $a \cdot 1 = 0$, para $a \in F$, se tiene que $a = 0$, de donde $\{1\}$ es linealmente independiente, y, por lo tanto es una base para K sobre F.

$$\therefore\ [K : F] = 1.$$

$\Longleftarrow$) Supongamos ahora que $[K : F] = 1$, y sea $\{x\}$ una base para K sobre F. Entonces, en particular, existe $a \in F$ tal que:

$$1 = ax$$

$$\therefore\ x = a^{-1} \in F.$$

Ahora, para cada $y \in K$, existe $b \in F$ tal que:

$$y = bx = ba^{-1}.$$

Así $y \in F$ y, por lo tanto $K = F$. ■

TEOREMA 2.61 Sean L/K y M/L extensiones de campos. Entonces:

$$[M : L][L : K] = [M : K].$$

Demostración. Sean $\{\alpha_1, ..., \alpha_r\}, \{\beta_1, ..., \beta_s\}$ bases de L sobre K y de M sobre L, respectivamente. Consideremos el conjunto:

$$\{\alpha_i\beta_j | i = 1, ..., r; j = 1, ..., s\},$$

y veamos que los sr vectores forman una base para M sobre K.

Sea $\gamma \in M$ cualquiera. Entonces:

$$\gamma = \textstyle\sum_{j=1}^{s} b_j\beta_j, \text{ con } b_j \in L.$$

Como las α_i forman base para L sobre K, tenemos que:

$$b_j = \sum_{i=1}^{r} a_{ij}\alpha_i, \quad a_{ij} \in K.$$

Entonces:

$$\gamma = \sum_{j=1}^{s}(\sum_{i=1}^{r} a_{ij}\alpha_i)\beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j)$$

$$\therefore\ \{\alpha_i\beta_j | i = 1, ..., r; j = 1, ..., s\} \text{ genera a } M \text{ sobre } K.$$

Mostremos ahora que el conjunto es independiente sobre K. Supongamos que:

$$\sum_{i,j} c_{ij}(\alpha_i\beta_j) = 0, \quad c_{ij} \in K.$$

Entonces:

$$\textstyle\sum_{j=1}^{s}(\sum_{i=1}^{r} c_{ij}\alpha_i)\beta_j = 0, \text{ y } \sum_{i=1}^{r} c_{ij}\alpha_i \in L.$$

Como las β_j son independientes sobre L, entonces:

$$\sum_{i=1}^{r} c_{ij}\alpha_i = 0,$$

para toda j. Pero las α_i son independientes sobre K y así la ecuación anterior implica que $c_{ij} = 0$, para todas las i, j. De este modo $\{\alpha_i\beta_j | i = 1, ..., r; j = 1, ..., s\}$ es independiente sobre K y, por lo tanto, forma una base para M sobre K.

Si $[L : K]$ es infinito, entonces existe una cantidad infinita de elementos de L (por consiguiente de M) que son linealmente independientes sobre K, y así $[M : K]$ también es infinito. Similarmente, si $[M : L]$ es infinito.

Ahora, si $[M : L]$ y $[L : K]$ son finitos, entonces la prueba muestra que $[M : K]$ es finito, de donde $[M : K]$ infinito implica que al menos uno de $[M : L]$ ó $[L : K]$ es infinito, con lo que la prueba queda completa. ■

EJEMPLO 2.62 Sea L/K una extensión tal que $[L : K]$ es un número primo. Probemos que no existe subcampo E de L tal que $K \subset E \subset L$.

En efecto, como:

$$[L : K] = [L : E][E : K],$$

entonces:

$$[L : E] = 1 \text{ ó } [E : K] = 1,$$

$$\Longrightarrow E = L \text{ ó } E = K. \blacksquare$$

EJEMPLO 2.63 Si L es una extensión de K y M es una extensión de L con $[M : K]$ finita, y si $[M : K] = [L : K]$, entonces por teorema 2.61, sabemos que:

$$[M : K] = [M : L][L : K].$$

$$\Longrightarrow 1 = [M : L], \text{ y, por teorema 2.60, } M = L.$$

Análogamente si $[M : L] = [M : K]$, entonces $L = K$.

CAPÍTULO 3

POLINOMIOS

3.1 Dominios Euclidianos.

DEFINICIÓN 3.1 Sea R un dominio entero. Cualquier función $N : R \longrightarrow \mathbb{Z}^+ \cup \{0\}$, con $N(0) = 0$, se llama una ***función euclidiana sobre R.***

DEFINICIÓN 3.2 El dominio entero R se dice que es un ***dominio euclidiano*** (o que posee un ***algoritmo de la división***) si existe una función euclidiana N sobre R tal que para cualesquiera dos elementos $a, b \in R$ con $b \neq 0$ existen elementos $q, r \in R$ con:

i) $a = qb + r$ con $r = 0$ ó $N(r) < N(b)$.
ii) Para todo $a, b \in R,\ a, b$ ambos distintos de cero, se tiene que $N(a) \leq N(ab)$.

Al elemento q se le llama ***cociente*** y a r ***residuo*** de la división.

EJEMPLO 3.3 Los enteros $\mathbb{Z}$ son un dominio euclidiano con función euclidiana dada por $N(a) = |a|,\ a \neq 0$, el valor absoluto usual.

La propiedad *i*) se cumple por el algoritmo de la división en $\mathbb{Z}$ y la propiedad *ii*) es obvia.

TEOREMA 3.4 Todo dominio euclidiano R es un dominio de ideales principales.

Demostración. Si $I \neq 0$ es un ideal de R, sea $a \in I$ tal que $N(a)$ es el menor entero en el conjunto de enteros no negativos:

$$\{N(x) | x \neq 0,\ x \in I\}.$$

Si $b \in I$, entonces:

$$b = qa + r, \text{ con } r = 0 \text{ ó } r \neq 0 \text{ y } N(r) < N(a).$$

Como $b \in I$ y $qa \in I$, entonces se sigue que $r \in I$, ya que I es un ideal, y como $N(r) < N(a)$ esto daría una contradicción a la elección de a. Luego $r = 0$ y así $b = qa \in \langle a \rangle$. Entonces:

$$I \subset \langle a \rangle \subset I \text{ y, en consecuencia } I = Ra = \langle a \rangle.$$

La segunda contención se da porque $a \in I$. Por lo tanto R es un dominio de ideales principales. ■

DEFINICIÓN 3.5 Sea R un anillo conmutativo y sean $a, b \in R$ con $b \neq 0$. Decimos que ***a es un múltiplo de b*** si existe un elemento $x \in R$ con $a = bx$. En este caso decimos que ***b divide a a*** ó que ***es un divisor de a***, y escribimos $b|a$.

DEFINICIÓN 3.6 Un ***máximo común divisor de a y b*** es un elemento $d \neq 0$ tal que:

i) $d|a$ y $d|b$; y,
ii) si $d'|a$ y $d'|b$, entonces $d'|d$.

Denotaremos a un máximo común divisor de a y b por $MCD(a, b)$.

Observación 3.7 $b|a$ en R si y sólo si $a \in \langle b\rangle$ si y sólo si $\langle a\rangle \subseteq \langle b\rangle$. En particular, si d es cualquier divisor tanto de a como de b, entonces $\langle d\rangle$ debe contener tanto a a como a b y así debe contener al ideal generado por a y b.

Podemos así trasladar la definición 3.6 a ideales de la siguiente manera:

PROPOSICIÓN 3.8 Si I es el ideal de R generado por a y b, entonces d es un ***máximo común divisor de a y b*** si :

i) $I \subseteq \langle d\rangle$, y
ii) si $\langle d'\rangle$ es cualquier ideal principal con $I \subseteq \langle d'\rangle$ entonces $\langle d\rangle \subseteq \langle d'\rangle$.

Demostración. Supongamos que las condiciones $i), ii)$ se cumplen y veamos que d satisface las condiciones de la definicón 3.6. Si $\langle a, b\rangle \subseteq \langle d\rangle$, entonces $ax + by = dc,\ c \in R$. Como $a, b \in I$, entonces, en particular $a = de$ y $b = df$ para algunas $e, f \in R$. De donde $d|a$ y $d|b$.

Por otro lado, por $ii)$ y por la observación 3.7, se sigue que $d'|d$.■

DEFINICIÓN 3.9 Sea R un anillo conmutativo con unitario, con grupo de unidades U. Si $a, b \in R$ son tales que $a = ub$ para alguna $u \in U$ decimos que a y b son ***asociados.***

PROPOSICIÓN 3.10 Sea D un dominio entero con grupo de unidades U, y sean $a, b \in D \setminus \{0\}$. Entonces $\langle a\rangle = \langle b\rangle$ si y sólo si a y b son asociados.

Demostración. $\Longrightarrow$) Supongamos que $\langle a\rangle = \langle b\rangle$. Entonces existen $u, v \in D$ tales que $a = ub,\ b = va$. De donde:

$$(uv)a = u(va) = ub = a = 1a,$$

y así, por cancelación, $uv = 1$. Luego $u, v \in U$, y entonces a, b son asociados.

$\Longleftarrow$) Si a es asociado de b, entonces existe $u \in U$ tal que $a = ub$, de esta manera $b = u^{-1}a$. Como consecuencia $b|a$ y $a|b$. Por la observación 3.7 tenemos $\langle a\rangle = \langle b\rangle$. ■

3.2 Factorización Única.

Sea R un dominio entero.

DEFINICIÓN 3.11 Supongamos que $r \in R$ es distinto de cero y no es una unidad. Entonces r se llama ***irreducible en*** R si siempre que $r = ab$ con $a, b \in R$ al menos uno de a ó b debe ser una unidad en R. De lo contrario, llamamos a r ***reducible.***

DEFINICIÓN 3.12 Un elemento $p \in R$ distinto de cero, se llama ***primo*** si no es una unidad y siempre que $p|ab$ para cualquier $a, b \in R$, entonces ó $p|a$ ó $p|b$.

TEOREMA 3.13 Sea p un elemento de un dominio de ideales principales D. Entonces son equivalentes:

i) p es irreducible;
ii) $\langle p\rangle$ es un ideal máximo de D; y;
iii) $D/\langle p\rangle$ es un campo.

Demostración. *i*) $\Longrightarrow$ *ii*). Supongamos que p es irreducible en D. Entonces si $\langle p\rangle \subseteq \langle a\rangle$, $a \in D$, se tiene $p = ab$, para alguna $b \in D$. Si a es unidad, entonces:

$$\langle a\rangle = \langle 1\rangle = D.$$

Si a no es unidad, entonces b debe ser unidad, así existe $u \in D$ tal que $bu = 1$. Luego:

$$pu = abu = a,$$

con lo que $\langle a\rangle \subseteq \langle p\rangle$.

$$\therefore\ \langle a\rangle = \langle p\rangle.$$

Luego $\langle p\rangle \subseteq \langle a\rangle$ implica $\langle a\rangle = D$ ó $\langle a\rangle = \langle p\rangle$ y $\langle p\rangle = D$ ó p sería unidad. Por lo tanto $\langle p\rangle$ es máximo.

ii) $\Longrightarrow$ *iii*) Esto es una consecuencia de que $\langle p\rangle$ es máximo.

iii) $\Longrightarrow$ *i*) Supongamos que $D/\langle p\rangle$ es un campo. Entonces $\langle p\rangle$ es máximo en D, que es un DIP. Supongamos que $p = ab$ en D. Entonces, es claro que $\langle p\rangle \subseteq \langle a\rangle$.

Si $\langle p\rangle = \langle a\rangle$ se tiene que a y p serían asociados y así b debe ser una unidad.

Si $\langle p\rangle \neq \langle a\rangle$, entonces debemos tener $\langle a\rangle = \langle 1\rangle = D$ ya que $\langle p\rangle$ es máximo. Pero entonces a y 1 son asociados, de donde a es unidad.

Luego $p = ab$ implica que alguno de a ó b es unidad y, por lo tanto, p es irreducible en D. ■

DEFINICIÓN 3.14 Un ***dominio de factorización única*** (DFU) es un dominio entero R en el cual cada elemento no cero $r \in R$ que no es una unidad, tiene las siguientes propiedades:

i) r puede escribirse como un producto finito de elementos irreducibles p de R (no necesariamente distintos):

$$r = p_1 p_2 \cdots p_n;$$

ii) la descomposición en *i*) es "única salvo asociados": a saber, si $r = q_1 q_2 \cdots q_m$ es otra factorización de r en irreducibles, entonces $m = n$ y hay alguna reordenación de los factores para que p_i sea un asociado de q_i, para $i = 1, 2, ..., n$.

EJEMPLO 3.15 Un campo F es un DFU pues cada elemento distinto de cero es una unidad, luego, no hay elementos para los cuales las propiedades *i*) y *ii*) se deban verificar.

TEOREMA 3.16 Cada DIP es un DFU. En particular, cada dominio euclidiano es un DFU.

Demostración. Ver [4]. ■

3.3 Anillos de Polinomios.

Sea R un anillo conmutativo con unitario.

DEFINICIÓN 3.17 Un ***polinomio f con coeficientes*** $a_i \in R,\ \forall i \geq 0$, es una sucesión:

$$(a_0, a_1, ...),$$

donde sólo una cantidad finita de $\{a_0, a_1, ...\}$ son distintos de cero.

DEFINICIÓN 3.18 Si existe un último elemento $a_n \neq 0$ en la sucesión anterior decimos que f tiene ***grado n, gdo(f),*** y a_n se llama el ***coeficiente principal de f.*** Si $a_n = 1$, decimos que el polinomio es ***mónico.***

En caso de que todos los coeficientes sean 0, convenimos en que el grado del polinomio $(0, 0, 0, ...)$ es $-\infty$, y también que, para cada $n \in \mathbb{Z}$:

$$-\infty < n,\ -\infty + (-\infty) = -\infty,\ -\infty + n = -\infty.$$

A los polinomios $(a, 0, 0, ...)$ de grado cero ó $-\infty$ les llamaremos ***constantes.***

La adición de polinomios se define de la siguiente manera:

$$(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$$

Y la multiplicación como:

$$(a_0, a_1, ...)(b_0, b_1, ...) = (c_0, c_1, ...),$$

donde, para $k = 0, 1, 2, ...$,

$$c_k = \sum_{\{(i,j)|i+j=k\}} a_i b_j.$$

De esta manera:

$$c_0 = a_0 b_0,\ c_1 = a_0 b_1 + a_1 b_0,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, ...$$

Con respecto a estas dos operaciones, el conjunto P de todos los polinomios con coeficientes en R resulta un anillo conmutativo con unitario.

Existe un monomorfismo $\theta : R \longrightarrow P$ dado por:

$$\theta(a) = (a, 0, 0, ...),\ a \in R.$$

Identificamos al polinomio constante $\theta(a) = (a, 0, 0, ...)$ con el elemento a de R.

Sea x el polinomio $(0, 1, 0, 0, ...)$. Por la definición de multiplicación tenemos:

$$x^2 = (0, 0, 1, 0, ...),$$

$$x^3 = (0, 0, 0, 1, 0, ...)$$

y, en general:

$$x^n = (\alpha_0, \alpha_1, ...),$$

donde α_m es 1 si $m = n$ y es 0 en otro caso. Entonces un polinomio:

$$(a_0, a_1, ..., a_n, 0, 0, ...)$$

de grado n se puede escribir como:

$$\theta(a_0) + \theta(a_1)x + \theta(a_2)x^2 + \cdots + \theta(a_n)x^n,$$

o bien, como:

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

si identificamos $\theta(a_i)$ con a_i.

Esta última expresión es la conocida definición de polinomio, en la cual x se considera como una "indeterminada". Algunas veces escribimos $f = f(x)$ y se dice que es un ***polinomio sobre*** R ***en la indeterminada*** x**.** El anillo P de todos estos polinomios se escribe como $R[x]$.

EJEMPLO 3.19 Los anillos de polinomios con coeficientes enteros y racionales son los familiares: $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$, respectivamente.

EJEMPLO 3.20 El anillo de polinomios $(\mathbb{Z}/3\mathbb{Z})[x]$, en x con coeficientes en $\mathbb{Z}/3\mathbb{Z}$, consiste de potencias no negativas de x con coeficientes $0, 1, 2$, operando sobre los coeficientes tomados módulo 3.

Por ejemplo, si $p(x) = x^2 + 2x + 1$ y $q(x) = x^3 + x + 2$, entonces:

$$p(x) + q(x) = x^3 + x^2,$$

y,

$$p(x) \cdot q(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2.$$

OBSERVACIÓN 3.21 Sea R un dominio entero y sean $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, q(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \in R[x]$, entonces $p(x) = q(x)$ si y sólo si $a_i = b_i,\ \forall i \geq 0$.

PROPOSICIÓN 3.22 Sea R un dominio entero y sean $p(x), q(x) \in R[x]$. Entonces:

i) $R[x]$ es un dominio entero;
ii) gdo$(p(x) + q(x))$ $\leq$máx(gdo$(p(x))$,gdo$(q(x))$), donde gdo$(p(x))$ denota el grado de $p(x)$, etc.;
iii) gdo$(p(x)q(x))$ =gdo$(p(x))$+gdo$(q(x))$;
iv) las unidades de $R[x]$ son exactamente las unidades de R.

Demostración. *i*) Sean $p(x), q(x) \in R[x]$ y veamos que no existen divisores de cero. Supongamos que $p(x), q(x) \neq 0$ con términos principales a_n, b_m respectivamente. Entonces $p(x)q(x)$ tiene término principal a_nb_m. Como D no tiene divisores de cero, entonces $a_nb_m \neq 0$ y así $p(x)q(x) \neq 0$.

ii) Sean $p(x), q(x) \neq 0$, y sean gdo$(p(x)) = n$ y gdo$(q(x)) = m$. Supongamos sin pérdida de generalidad que $n \geq m$.

Si $n > m$, entonces es claro que el término principal de $p(x) + q(x) = a_nx^n$ y así:

$$\text{gdo}(p(x)+q(x)) = \text{máx}\{\text{gdo}(p(x)),\text{gdo}(q(x))\}$$

Si $n = m$, entonces podemos tener:

$$a_n + b_m = 0$$

y así, todo lo que podemos decir es que:

$$\text{gdo}(p(x)+q(x)) \leq \text{máx}\{\text{gdo}(p(x)),\text{gdo}(q(x))\}.$$

iii). Por *i*), si $p(x), q(x) \neq 0$, entonces $\text{gdo}(p(x)q(x)) = n + m = \text{gdo}(p(x)) + \text{gdo}(q(x))$.

Si alguno de $p(x)$ ó $q(x)$ es cero, entonces el resultado se cumple por las convenciones hechas después de la definición 3.18.

iv) Sean $p(x), q(x) \in R[x]$ y supongamos que:

$$p(x)q(x) = 1.$$

Entonces, de *iii*):

$$\text{gdo}(p(x)) = \text{gdo}(q(x)) = 0$$

$$\Longrightarrow \; p(x), q(x) \in R, \text{ y } p(x)q(x) = 1,$$

de aquí que ambos son de grado 0 y, por lo tanto son constantes distintas de cero en R que, además, multiplicadas dan 1, con lo que son unidades. ■

De acuerdo con la definición 3.2, podemos definir en $F[x]$ una norma para que sea un dominio euclidiano:

EJEMPLO 3.23 Si F es un campo, entonces el anillo de polinomios $F[x]$ es un dominio euclidiano con norma dada por:

$$N(p(x)) = \text{gdo}(p(x)).$$

El algoritmo de la división para polinomios es simplemente la división larga de polinomios, la cual puede ser familiar para polinomios con coeficientes reales. La prueba es muy similar a la de $\mathbb{Z}$ y la daremos a continuación.

TEOREMA 3.24 Sea F un campo. El anillo de polinomios $F[x]$ es un dominio euclidiano; es decir, si $a(x)$ y $b(x)$ son dos polinomios en $F[x]$ con $b(x) \neq 0$, entonces existen polinomios únicos $q(x)$ y $r(x)$ en $F[x]$ tales que:

$$a(x) = q(x)b(x) + r(x) \;\; \text{con } r(x) = 0 \text{ ó } \text{gdo}(r(x)) < \text{gdo}(b(x)).$$

Demostración. Si $a(x)$ es el polinomio cero entonces tomamos $q(x) = r(x) = 0$, y listo.

Supongamos entonces que $a(x) \neq 0$ y probemos la existencia de $q(x)$ y $r(x)$ por inducción sobre $n = \text{gdo}(a(x))$. Sea $m = \text{gdo}(b(x))$.

i) Si $n < m$ tomamos $q(x) = 0$ y $r(x) = a(x)$.

ii) Si $n \geq m$, escribimos:

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

y

$$b(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

Entonces el polinomio:

$$a_1(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$$

es de grado menor que n. Notemos que este polinomio está bien definido, pues los coeficientes se toman de un campo y $b_m \neq 0$. Entonces, por inducción, existen polinomios $q_1(x)$ y $r(x)$ con:

$$a_1(x) = q_1(x)b(x) + r(x) \text{ y } r(x) = 0 \text{ ó } \text{gdo}(r(x)) < \text{gdo}(b(x)).$$

Entonces poniendo:

$$q(x) = q_1(x) + \frac{a_n}{b_m} x^{n-m},$$

tenemos:

$$a(x) = q(x)b(x) + r(x), \text{ con } r(x) = 0 \text{ ó } \text{gdo}(r(x)) < \text{gdo}(b(x)),$$

con lo cual se completa el paso inductivo.

Ahora para la unicidad, supongamos que $q_2(x)$ y $r_1(x)$ también satisfacen las condiciones del teorema. Entonces los polinomios:

$$a(x) - q(x)b(x), \quad a(x) - q_2(x)b(x),$$

son de grado menor que $m = \text{gdo}(b(x))$. La diferencia de estos dos polinomios, es decir:

$$b(x)(q(x) - q_2(x))$$

también es de grado menor que m. Pero el grado del producto de dos polinomios distintos de cero, es la suma de sus grados (ya que F es un dominio entero), de donde:

$$q(x) - q_2(x) = 0,$$

esto es:

$$q(x) = q_2(x).$$

Esto implica que $r(x) = r_1(x)$, completando la demostración. ■

Observación. Dada $\alpha \in F$ existe una única función $Ev(\alpha) : F[x] \to F$, a la que llamaremos ***evaluación en*** α, tal que:

i)$Ev(\alpha)(r) = r, \ \forall r \in F$.
ii)$Ev(\alpha)(x) = \alpha$.
iii)$Ev(\alpha)$ respeta la suma, el producto y el uno.

De esta manera, si el polinomio $p(x) \in F[x]$ y si:

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

entonces, si $\alpha \in F$, por $p(\alpha)$ entenderemos el elemento:

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

de F. Decimos que $p(\alpha)$ ***es el valor*** del polinomio $p(x)$ obtenido al sustituir la x por la α.

COROLARIO 3.25 (TEOREMA DEL RESIDUO.) Sea R un anillo con unitario y sea:

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x].$$

Para cualquier $c \in R$ existe un único $q(x) \in R[x]$ tal que:

$$f(x) = q(x)(x - c) + f(c).$$

Demostración. Si $f(x) = 0$, simplemente ponemos $q(x) = 0$ y ya. Supongamos entonces que $f(x) \neq 0$. Por el teorema anterior, existen únicos $q(x), r(x) \in R[x]$ tales que:

$$f(x) = q(x)(x - c) + r(x) \text{ con } \text{gdo}(r(x)) < \text{gdo}((x - c)) = 1.$$

Entonces $r(x) = r$ es un polinomio constante, posiblemente cero. Si:

$$q(x) = \sum_{j=0}^{n-1} b_j x^j,$$

entonces:

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

de donde:

$$f(c) = q(c)(c - c) + r = 0 + r = r.\blacksquare$$

DEFINICIÓN 3.26 Sean $f(x), g(x) \in R[x]$, diremos que ***f(x) divide a g(x)***, $(f(x)|g(x))$ si existe $h(x) \in R[x]$ tal que $f(x)h(x) = g(x)$.

DEFINICIÓN 3.27 $h(x) \in R[x]$ es el ***máximo común divisor*** de $f(x)$ y $g(x)$ si:

i) $h(x)|f(x), h(x)|g(x)$. (Es decir, $h(x)$ es un divisor común).
ii) $k(x)|f(x), k(x)|g(x)$ implican $k(x)|h(x)$. (Cualquier otro divisor común divide a $h(x)$).
iii) $h(x)$ es mónico. (Es decir, que el coeficiente principal de $h(x)$ es 1).

DEFINICIÓN 3.28 Un polinomio $p(x) \in F[x]$ se dice que es ***irreducible sobre*** F si siempre que $p(x) = a(x)b(x) \in F[x]$, entonces ó $a(x)$ ó $b(x)$ tiene grado cero, es decir, es una constante.

Como una consecuencia de los teoremas 3.4, 3.16 y 3.24 podemos resumir las propiedades importantes de $F[x]$ de la siguiente manera:

TEOREMA 3.29 Sea F un campo. Entonces:

i) cada pareja $(f(x), g(x))$ de polinomios en $F[x]$ tiene un máximo común divisor $d(x)$, el cual se puede expresar como $a(x)f(x) + b(x)g(x)$, con $a(x), b(x) \in F[x]$;
ii) $F[x]$ es un dominio de ideales principales;
iii) $F[x]$ es un dominio de factorización única;
iv) si $f(x) \in F[x]$, entonces $F[x]/\langle f(x)\rangle$ es un campo si y sólo si $f(x)$ es irreducible. ■

EJEMPLO 3.30 En $\mathbb{Z}[x]$ consideremos el ideal:

$$I = \langle 2, x\rangle = \{2f(x) + xg(x) | f(x), g(x) \in \mathbb{Z}[x]\},$$

que consiste en todos los polinomios cuyo término constante es par. Supongamos que $I = \langle p(x)\rangle$ para algún polinomio $p(x)$. Entonces:

$$p(x)|2, \text{ y } p(x)|x \text{ de donde } p(x) \text{ es un asociado de 1.}$$

Pero entonces:

$$\langle p(x)\rangle = \mathbb{Z}[x] \neq I,$$

lo cual muestra que $\mathbb{Z}[x]$ no es un dominio de ideales principales.

3.4 Polinomios Irreducibles.

PROPOSICIÓN 3.31 Sea F un campo y sea $p(x) \in F[x]$. Entonces $p(x)$ tiene un factor de grado uno si y sólo si $p(x)$ tiene una raíz en F, es decir, existe $\alpha \in F$ con $p(\alpha) = 0$.

Demostración. $\Longrightarrow$) Si $p(x)$ tiene un factor de grado uno, entonces, como F es un campo, podemos suponer que el factor es mónico, esto es, que es de la forma $(x - \alpha)$ para alguna $\alpha \in F$. Pero entonces:

$$p(\alpha) = \alpha - \alpha = 0.$$

$\Longleftarrow$) Supongamos que $p(\alpha) = 0$. Por el algoritmo de la división en $F[x]$ podemos escribir:

$$p(x) = q(x)(x - \alpha) + r(x),$$

donde $r(x)$ es una constante. Como $p(\alpha) = 0$, $r(x)$ debe ser 0, luego $p(x)$ tiene a $(x - \alpha)$ como factor. ■

PROPOSICIÓN 3.32 Un polinomio de grado 2 ó 3 sobre un campo F es reducible si y sólo si tiene una raíz en F.

Demostración. Esto es una consecuencia del resultado previo, ya que un polinomio de grado 2 ó 3 es reducible si y sólo si tiene al menos un factor lineal. ■

TEOREMA 3.33 Sea $g(x) = x^2 + a_1x + a_0$ un polinomio con coeficientes en $\mathbb{Q}$. Entonces:

i) si $g(x)$ es irreducible sobre $\mathbb{R}$, también lo es sobre $\mathbb{Q}$;

ii) si $g(x) = (x - \beta_1)(x - \beta_2)$, con $\beta_1, \beta_2 \in \mathbb{R}$, entonces $g(x)$ es irreducible sobre $\mathbb{Q}[x]$ si y sólo si β_1 y β_2 son irracionales.

Demostración. *i*) Sea $g(x)$ irreducible sobre $\mathbb{R}$. Si:

$$g(x) = (x - q_1)(x - q_2)$$

fuera una factorización en $\mathbb{Q}[x]$, también sería una factorización en $\mathbb{R}[x]$, y tendríamos una contradicción.

ii) Si β_1, β_2 fueran racionales tendríamos una factorización en $\mathbb{Q}[x]$, y $g(x)$ no sería irreducible.

Si β_1, β_2 son irracionales, entonces:

$$(x - \beta_1)(x - \beta_2)$$

es la única factorización en $\mathbb{R}[x]$, y así no es posible una factorización en $\mathbb{Q}[x]$ en factores lineales. ■

Podemos, desde luego, determinar cuando un polinomio cuadrático $ax^2 + bx + c$ en $\mathbb{R}[x]$ es irreducible: es irreducible si y sólo si el discriminante $b^2 - 4ac < 0$.

EJEMPLO 3.34. Examinemos la irreducibilidad de los siguientes polinomios en $\mathbb{R}[x]$ y en $\mathbb{Q}[x]$:

$$x^2 + x + 1,\ x^2 + x - 1,\ x^2 + x - 2.$$

Solución. El primer polinomio es irreducible sobre $\mathbb{R}$, pues el discriminante es -3. Se sigue que es irreducible sobre $\mathbb{Q}$.

El segundo polinomio se factoriza sobre $\mathbb{R}$ como $(x - \beta_1)(x - \beta_2)$, donde:

$$\beta_1 = \tfrac{-1+\sqrt{5}}{2},\ \beta_2 = \tfrac{-1-\sqrt{5}}{2}.$$

Es irreducible sobre $\mathbb{Q}$.

El tercer polinomio se factoriza sobre $\mathbb{Q}$ como $(x - 1)(x + 2)$ y entonces no es irreducible.

TEOREMA 3.35 (LEMA DE GAUSS). Sea $f(x)$ un polinomio en $\mathbb{Z}[x]$, irreducible sobre $\mathbb{Z}$. Entonces $f(x)$, considerado como un polinomio en $\mathbb{Q}[x]$, es irreducible sobre $\mathbb{Q}$.

Demostración. Supongamos, por contradicción, que $f(x) = g(x)h(x)$, con $g(x), h(x) \in \mathbb{Q}[x]$ y gdo($g(x)$),gdo($h(x)$) <gdo($f(x)$). Entonces existe un entero positivo n tal que:

$$nf(x) = g_1(x)h_1(x),$$

donde $g_1(x), h_1(x) \in \mathbb{Z}[x]$. Supongamos que n es el menor entero positivo con esta propiedad y sean:

$$g_1(x) = a_0 + a_1x + \cdots + a_kx^k,$$

$$h_1(x) = b_0 + b_1x + \cdots + b_\ell x^\ell.$$

Si $n = 1$, entonces $g_1(x) = g(x),\ h_1(x) = h(x)$, y tenemos una contradicción. Caso contrario, sea p un factor primo de n.

Veamos que, entonces, ó p divide a todos los coeficientes de $g_1(x)$, ó p divide a todos los coeficientes de $h_1(x)$.

Supongamos que p no divide a todos los coeficientes de $g_1(x)$, y que p no divide a todos los coeficientes de $h_1(x)$. Supongamos también que p divide a $a_0, ..., a_{i-1}$, pero no a a_i, y que p divide a $b_0, ..., b_{j-1}$, pero no a b_j. El coeficiente de x^{i+j} en $nf(x)$ es:

$$a_0 b_{i+j} + \cdots + a_i b_j + \cdots + a_{i+j} b_0.$$

En esta suma, todos los términos antes de $a_i b_j$ son divisibles por p, ya que p divide a $a_0, ..., a_{i-1}$; y todos los términos siguientes son divisibles por p, pues p divide a $b_0, ..., b_{j-1}$. De donde sólo el término $a_i b_j$ no es divisible por p y entonces el coeficiente de x^{i+j} en $nf(x)$ no es divisible por p, lo cual es una contradicción, debido a que los coeficientes de $f(x)$ son enteros, y así ciertamente todos los coeficientes de $nf(x)$ son divisibles por p.

Volviendo al teorema. Podemos suponer, sin pérdida de generalidad, que:

$$g_1(x) = p g_2(x),$$

donde $g_2(x) \in \mathbb{Z}[x]$. Se sigue que:

$$(n/p) f(x) = g_2(x) h_1(x),$$

y esto contradice la elección de n como el menor entero positivo con esta propiedad. Esto significa que no es posible una factorización en $\mathbb{Q}$, y como consecuencia, $f(x)$ es irreducible sobre $\mathbb{Q}$. ■

TEOREMA 3.36 (CRITERIO DE EISENSTEIN.) Sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio en $\mathbb{Z}[x]$. Supongamos que existe un número primo p tal que:

i) $p \nmid a_n$,
ii) $p | a_i,\ i = 0, ..., n-1$,
iii) $p^2 \nmid a_0$.

Entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

Demostración. Por el lema de Gauss, es suficiente probar que $f(x)$ es irreducible sobre $\mathbb{Z}$. Supongamos, por contradicción, que $f(x) = g(x)h(x)$, donde:

$$g(x) = b_0 + b_1 x + \cdots + b_r x^r,$$

$$h(x) = c_0 + c_1 x + \cdots + c_s x^s,$$

con $r, s < n$ y $r + s = n$. Como $a_0 = b_0 c_0$, se sigue de *ii)* que:

$$p | b_0 \text{ ó } p | c_0.$$

Como $p^2 \nmid a_0$, los coeficientes b_0 y c_0 no pueden ser ambos divisibles por p, y podemos suponer, sin pérdida de generalidad, que:

(2)
$$p | b_0,\ p \nmid c_0.$$

Supongamos inductivamente que p divide a $b_0, b_1, ..., b_{k-1}$ donde $1 \leq k \leq r$. Entonces:

$$a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0.$$

Como p divide a cada uno de $a_k, b_0c_k, b_1c_{k-1}, ..., b_{k-1}c_1$, se sigue que p divide a b_kc_0, y de aquí, de (2), $p|b_k$.

Concluimos que $p|b_r$, y entonces, como $a_n = b_rc_s$, tenemos que $p|a_n$, contradicción, por i). De esta manera $f(x)$ es irreducible. ■

3.5 Extensiones de Campos y Raíces de Polinomios.

Sea F un campo y sea K una extensión de F.

DEFINICIÓN 3.37 El elemento $\alpha \in K$ se dice que es ***algebraico sobre F*** si α es una raíz de algún polinomio no cero $f(x) \in F[x]$. Si α no es algebraico sobre F (es decir, no es la raíz de todo polinomio distinto de cero con coeficientes en F), entonces α se llama ***trascendental sobre F.*** La extensión K/F se dice que es ***algebraica*** si cada elemento de K es algebraico sobre F.

DEFINICIÓN 3.38 Sea K una extensión del campo F y sean $\alpha, \beta, ...$ una colección de elementos de K. Entonces el subcampo más pequeño de K que contiene tanto a F como a los elementos $\alpha, \beta, ...$, denotado $F(\alpha, \beta, ...)$, se llama el ***campo generado por*** $\alpha, \beta, ...$ ***sobre F.***

DEFINICIÓN 3.39 Si el campo K se genera por un sólo elemento α sobre K, $K = F(\alpha)$, entonces K se llama una ***extensión simple de*** F y a α se le llama un ***elemento primitivo*** para la extensión.

Consideremos todos los elementos de K que pueden expresarse en la forma $a_0 + a_1\alpha + \cdots + a_r\alpha^r$ donde las a_i pueden tomar valores cualesquiera sobre F y r puede ser cualquier entero no negativo. Como esta suma está en K, entonces podemos dividir dicho elemento por otro distinto de cero. $F(\alpha)$ es precisamente el conjunto de todos estos cocientes, y es un subcampo de K que contiene tanto a F como a α. Así $F(\alpha)$ contiene a los inversos multiplicativos de dichos elementos.

PROPOSICIÓN 3.40 Sea K una extensión de F y sea $\alpha \in K$ algebraico sobre F. Entonces existe un único polinomio mónico irreducible $m(x) \in F[x]$ el cual tiene a α como una raíz. Un polinomio $f(x) \in F[x]$ tiene a α como raíz si y sólo si $m(x)$ divide a $f(x)$ en $F[x]$. Además $[F(\alpha) : F] = \text{gdo}(m(x))$.

Demostración. Sea $g(x) \in F[x]$ un polinomio de grado mínimo que tiene a α como una raíz. Multiplicando a $g(x)$ por una constante, podemos suponer que $g(x)$ es mónico. Suponiendo que $g(x)$ fuera reducible en $F[x]$, digamos:

$$g(x) = a(x)b(x),$$

con $a(x), b(x) \in F[x]$ ambos de grado menor que el grado de $g(x)$. Entonces:

$$g(\alpha) = a(\alpha)b(\alpha) = 0$$

en F, y como F es un campo:

$$a(\alpha) = 0 \text{ ó } b(\alpha) = 0,$$

contradiciendo la minimalidad del grado de $g(x)$.

$\therefore$ $g(x)$ es un polinomio mónico irreducible que tiene a α como una raíz.

Supongamos ahora que $f(x) \in F[x]$ es cualquier polinomio que tiene a α como una raíz. Por el Algoritmo de la División en $F[x]$ existen polinomios $q(x), r(x) \in F[x]$ tales que:

$$f(x) = q(x)g(x) + r(x), \text{ con gdo}(r(x)) < \text{gdo}(g(x)),$$

de donde:

$$f(\alpha) = q(\alpha)g(\alpha) + r(\alpha)$$

en F, y como α es una raíz tanto de $f(x)$ como de $g(x)$, obtenemos $r(\alpha) = 0$, lo cual contradice la minimalidad de $g(x)$ a menos de que $r(x) = 0$. Se concluye que $g(x)$ divide a cualquier polinomio $f(x)$ en $F[x]$ que tiene a α como una raíz y, en particular, dividiría a cualquier otro polinomio mónico irreducible en $F[x]$ que tiene a α como una raíz. Esto prueba que $m(x) = g(x)$ es único.

Finalmente, supongamos que $\text{gdo}(m(x)) = n$, y sea $f(\alpha) \in F[\alpha]$, donde $f(x)$ es un polinomio. Entonces:

$$f(\alpha) = q(\alpha)m(\alpha) + r(\alpha), \text{ donde gdo}(r(x)) < \text{gdo}(m(x)) = n.$$

$$\Longrightarrow \ f(\alpha) = r(\alpha),$$

y así existen $c_0, c_1, ..., c_{n-1}$, (los coeficientes de $r(x)$, algunos de los cuales pueden ser cero) en F tales que:

$$f(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}.$$

$$\therefore \ \{1, \alpha, ..., \alpha^{n-1}\}$$

es un conjunto generador para $F[\alpha]$. Además, el conjunto $\{1, \alpha, ..., \alpha^{n-1}\}$ es linealmente independiente sobre F, pues si los elementos $a_0, a_1, ..., a_{n-1}$ de F son tales que:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0,$$

entonces:

$$a_0 = a_1 = \cdots = a_{n-1} = 0,$$

pues de lo contrario, tendríamos un polinomio distinto de cero:

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

de grado a lo más $n - 1$ tal que $f(\alpha) = 0$.

$$\Longrightarrow \ \{1, \alpha, ..., \alpha^{n-1}\}$$

es una base de $F(\alpha)$ sobre F, y así:

$$[F(\alpha) : F] = n. \ \blacksquare$$

DEFINICIÓN 3.41 El polinomio $m(x)$ de la proposición anterior se llama ***polinomio mínimo para*** α ***sobre F.*** El grado de $m(x)$ se llama ***grado de*** α.

TEOREMA 3.42 Cada extensión finita es algebraica.

Demostración. Sea L una extensión finita de K, y supongamos, por contradicción, que L contiene un elemento α que es trascendental sobre K. Entonces los elementos:

$$1, \alpha, \alpha^2, ...$$

son linealmente independientes sobre K, y así $[L : K]$ no puede ser finita. ■

TEOREMA 3.43 Sean L/K y M/L extensiones de campos, y sea $\alpha \in M$. Si α es algebraico sobre K, entonces también es algebraico sobre L.

Demostración. Como α es algebraico sobre K, entonces existe un polinomio distinto de cero $f(x) \in K[x]$ tal que:

$$f(\alpha) = 0.$$

Como $f(x) \in L[x]$, entonces α es algebraico sobre L. ■

TEOREMA 3.44 Sea K un campo y sea $g(x)$ un polinomio irreducible en $K[x]$. Entonces $K[x]/\langle g(x)\rangle$ es un campo que contiene a K salvo isomorfismo.

Demostración. Sabemos del teorema 3.28 que $K[x]/\langle g(x)\rangle$ es un campo. La función $\varphi : K \longrightarrow K[x]/\langle g(x)\rangle$ dada por:

$$\varphi(a) = a + \langle g(x)\rangle,\ a \in K$$

es un homomorfismo: Si $a, b \in K$, entonces:

$$\begin{aligned}\varphi(ab) &= (ab) + \langle g(x)\rangle \\ &= (a + \langle g(x)\rangle)(b + \langle g(x)\rangle) \\ &= \varphi(a)\varphi(b).\end{aligned}$$

Por otra parte, como:

$$a + \langle g(x)\rangle = b + \langle g(x)\rangle$$

implica:

$$a - b \in \langle g(x)\rangle,$$

entonces $a = b$. Así φ es un monomorfismo. ■

Sea K un campo, y sea $m(x) \in K[x]$ irreducible y mónico. Sea $L = K[x]/\langle m(x)\rangle$. Entonces L es un campo. Por el teorema anterior, la función:

$$a \mapsto a + \langle m(x)\rangle$$

es un monomorfismo de K en L. Así L es una extensión de K.

Sea $\alpha = x + \langle m(x)\rangle$. Entonces, para cada polinomio:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x],$$

tenemos:

$$\begin{aligned}f(\alpha) &= a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n \\ &= a_0 + a_1(x + \langle m(x)\rangle) + a_2(x + \langle m(x)\rangle)^2 + \cdots + a_n(x + \langle m(x)\rangle)^n \\ &= a_0 + a_1(x + \langle m(x)\rangle) + a_2(x^2 + \langle m(x)\rangle) + \cdots + a_n(x^n + \langle m(x)\rangle) \\ &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) + \langle m(x)\rangle \\ &= f(x) + \langle m(x)\rangle,\end{aligned}$$

$$\implies f(\alpha) = 0 + \langle m(x)\rangle \iff m(x)|f(x)$$

Por lo tanto, $m(x)$ es el polinomio mínimo de α. De esta manera:

TEOREMA 3.45 Sea K un campo y sea $m(x)$ un polinomio mónico irreducible con coeficientes en K. Entonces $L = K[x]/\langle m(x)\rangle$ es una extensión algebraica simple $K(\alpha)$ de K, y $\alpha = x + \langle m(x)\rangle$ tiene polinomio mínimo $m(x)$ sobre K. ■

El campo L en el teorema es, de hecho, único:

TEOREMA 3.46 Sean K, K' campos y $\varphi : K \longrightarrow K'$ un isomorfismo con extensión canónica (definición B.2) $\widehat{\varphi} : K[x] \longrightarrow K'[x]$. Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ un polinomio irreducible de grado n con coeficientes en K, y sea $f_1(x) = \widehat{\varphi}(f(x)) = \varphi(a_n)x^n + \varphi(a_{n-1})x^{n-1} + \cdots + \varphi(a_0)$. Sea L una extensión de K que contiene una raíz α de f, y sea L' una extensión de K' que contiene una raíz α_1 de f_1. Entonces existe un isomorfismo ψ de $K(\alpha)$ sobre $K'(\alpha)$, una extensión de φ.

Demostración. El campo $K(\alpha)$ consiste de expresiones de la forma $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, con la adición usual, y donde la multiplicación se efectúa usando la ecuación:

$$\alpha^n = -\frac{1}{a_n}(a_{n-1}\alpha^{n-1} + \cdots + a_0).$$

La función ψ se define por:

$$\psi(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}) = \varphi(b_0) + \varphi(b_1)\alpha_1 + \cdots + \varphi(b_{n-1})(\alpha_1)^{n-1}.$$

Dicho de otra manera, tenemos que, para cada polinomio $u(x) \in K[x]$ con $\text{gdo}(u(x)) < n$:

$$\psi(u(\alpha)) = (\widehat{\varphi}(u))(\alpha_1).$$

Es claro que ψ es inyectiva, sobreyectiva y extiende al isomorfismo $\varphi : K \longrightarrow K'$.

Sean $u(x), v(x) \in K[x]$, donde $\text{gdo}(u(x))$,$\text{gdo}(v(x)) \leq n-1$. Entonces claramente:

$$\psi(u(\alpha) + v(\alpha)) = \psi(u(\alpha)) + \psi(v(\alpha)).$$

La igualdad correspondiente para la multiplicación es menos clara. Multiplicamos $u(\alpha)$ y $v(\alpha)$ y usamos el polinomio mínimo para reducir el resultado a $w(\alpha)$, digamos, donde $\text{gdo}(w(x)) \leq n-1$. Precisamente, usando el algoritmo de la división para escribir:

$$u(x)v(x) = q(x)m(x) + w(x), \text{ donde } \text{gdo}(w(x)) < n.$$

De aquí:

$$\begin{aligned} \psi(u(\alpha)v(\alpha)) &= \psi(w(\alpha)) \\ &= (\widehat{\varphi}(w)(\alpha_1) \end{aligned} \tag{3}$$

El isomorfismo $\widehat{\varphi}$ nos asegura que el algoritmo de la división en $K'[x]$ da:

$$\widehat{\varphi}(u)\widehat{\varphi}(v) = \widehat{\varphi}(q)\widehat{\varphi}(m) + \widehat{\varphi}(w) \tag{4}$$

Y entonces:

$$\begin{aligned}
\psi(u(\alpha))\psi(v(\alpha)) &= (\widehat{\varphi}(u))(\alpha_1)(\widehat{\varphi}(v))(\alpha_1) \\
&= (\widehat{\varphi}(u)\widehat{\varphi}(v))(\alpha_1) \\
&= (\widehat{\varphi}(q)\widehat{\varphi}(m) + \widehat{\varphi}(w))(\alpha_1), && \text{(de 4)} \\
&= (\widehat{\varphi}(q))(\alpha_1)(\widehat{\varphi}(m))(\alpha_1) + (\widehat{\varphi}(w))(\alpha_1) \\
&= (\widehat{\varphi}(w))(\alpha_1) && \text{(pues } (\widehat{\varphi}(m))(\alpha_1) = 0)
\end{aligned}$$

Comparando esto con (3) obtenemos el resultado requerido. ■

COROLARIO 3.47 Sea K un campo, y sea $f(x)$ un polinomio irreducible con coeficientes en K. Si L, L' son extensiones de K que contienen raíces α, α_1 de $f(x)$, respectivamente, entonces existe un isomorfismo de $K(\alpha)$ sobre $K(\alpha_1)$ el cual fija a cada elemento de K. ■

Como la idea ocurrirá muy a menudo, aplicaremos el término ***K-isomorfismo*** a un isomorfismo α de L sobre L' con la propiedad de que $\alpha(x) = x$ para cada elemento de K.

EJEMPLO 3.48 Si $K = \mathbb{R}$ y $m(x) = x^2 + 1$, el campo $L = K[x]/\langle x^2 + 1\rangle$ contiene un elemento $\delta = x + \langle x^2 + 1\rangle$ tal que $\delta^2 = -1$. El polinomio $x^2 + 1$, irreducible sobre $\mathbb{R}$, se factoriza como $(x + \delta)(x - \delta)$ en el campo L. Cada elemento de L se escribe de forma única como $a + b\delta$, con a, b reales, y así L resulta ser el campo $\mathbb{C}$ de números complejos.

DEFINICIÓN 3.49 La extensión de campo K de F se llama un ***campo de descomposición*** para el polinomio $f(x) \in F[x]$ si $f(x)$ se factoriza completamente en factores lineales en $K[x]$ y $f(x)$ no se factoriza completamente en factores lineales sobre cualquier subcampo propio de K que contiene a F.

DEFINICIÓN 3.50 Si K es una extensión algebraica de F la cual es el campo de descomposición sobre F para una colección de polinomios $\{f_i(x)\}_{i\in I} \in F[x]$, entonces K se llama una ***extensión normal*** de F.

Generalmente usaremos el término "campo de descomposición", en lugar de "extensión normal".

EJEMPLO 3.51 El campo de descomposición para $x^2 - 2$ sobre $\mathbb{Q}$ es justo $\mathbb{Q}(\sqrt{2})$, pues las dos raíces son $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, y no están en $\mathbb{Q}$

EJEMPLO 3.52 El polinomio $x^4 + 4$ se factoriza sobre $\mathbb{Q}$ como:

$$\begin{aligned}
x^4 + 4 &= x^4 + 4x^2 + 4 - 4x^2 \\
&= (x^2 + 2)^2 - 4x^2 \\
&= (x^2 + 2x + 2)(x^2 - 2x + 2)
\end{aligned}$$

donde estos dos factores son irreducibles (Eisenstein). Resolviendo para las raíces de los dos factores por la fórmula cuadrática, encontramos las 4 raíces $\pm 1 \pm i$, así el campo de descomposición de este polinomio es precisamente el campo $\mathbb{Q}(i)$, una extensión de grado 2 de $\mathbb{Q}$.

En general, si $f(x) \in F[x]$ es un polinomio de grado n, entonces adjuntando una raíz de $f(x)$ a F se genera una extensión F_1, de grado a lo más n (e igual a n si y sólo si $f(x)$ es irreducible).

Sobre F_1, el polinomio $f(x)$ ahora tiene al menos un factor lineal, así que cualquier otra raíz de $f(x)$ satisface una ecuación de grado a lo más $n-1$ sobre F_1. Adjuntando una tal raíz a F_1, obtenemos por lo tanto una extensión de grado a lo más $n-1$ de F_1, etcétera. Esto prueba:

PROPOSICIÓN 3.53 Un campo de descomposición de un polinomio de grado n sobre F es de grado a lo más $n!$ sobre F ■.

TEOREMA 3.54 Sean K y K' campos, y sea $\varphi : K \longrightarrow K'$, un isomorfismo que se extiende a un isomorfismo $\widehat{\varphi} : K[x] \longrightarrow K'[x]$. Sea $f(x) \in K[x]$ y sean L, L', respectivamente, campos de descomposición de $f(x)$ sobre K y de $\widehat{\varphi}(f(x))$ sobre K'. Entonces existe un isomorfismo $\varphi^* : L \longrightarrow L'$ tal que extiende a φ.

Demostración. Supongamos que $\text{gdo}(f(x)) = n$ y que en $L[x]$ tenemos la factorización:

$$f(x) = \alpha(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

donde α, el coeficiente principal de $f(x)$, está en K, y $\alpha_1, \alpha_2, ..., \alpha_n \in L$. Podemos suponer que, para alguna $m \in \{0, 1, ..., n\}$, las raíces $\alpha_1, \alpha_2, ..., \alpha_m$ no están en K, y que $\alpha_{m+1}, ..., \alpha_n \in K$. Probaremos el teorema por inducción sobre m.

Si $m = 0$, entonces todas las raíces están en K, y así K es en sí mismo un campo de descomposición para $f(x)$. De donde, en $K'[x]$, tenemos:

$$\widehat{\varphi}(f(x)) = \varphi(\alpha)(x-\varphi(\alpha_1))(x-\varphi(\alpha_2))\cdots(x-\varphi(\alpha_n));$$

Por lo tanto, K' es un campo de descomposición para $\widehat{\varphi}(f(x))$ y $\varphi* = \varphi$.

Supongamos ahora que $m > 0$. Hacemos la hipótesis inductiva de que, para cada campo E y cada polinomio $g(x) \in E[x]$ que tiene menos que m raíces fuera de E en un campo de descomposición L de $g(x)$, cada isomorfismo de E se puede extender a un isomorfismo de L.

Nuestra hipótesis de que $m > 0$ implica que los factores irreducibles de $f(x)$ en $K[x]$ no son todos lineales. Sea $f_1(x)$ un factor irreducible no lineal de $f(x)$.

$$\Longrightarrow \ \widehat{\varphi}(f_1(x)) \text{ es un factor irreducible de } \varphi(f(x)) \text{ en } K'.$$

Las raíces de $f_1(x)$ en el campo de descomposición L están incluidas entre las raíces:

$$\alpha_1, \alpha_2, ..., \alpha_n,$$

y podemos suponer, sin pérdida de generalidad, que α_1 es una raíz de $f_1(x)$. Similarmente, la lista de raíces de $\widehat{\varphi}(f(x))$:

$$\varphi(\alpha_1), \varphi(\alpha_2), ..., \varphi(\alpha_n)$$

incluyen una raíz $\beta_1 = \varphi(\alpha_i)$ de $\widehat{\varphi}(f_1(x))$.(No podemos suponer que $i = 1$.) Por el teorema 3.46, existe un isomorfismo:

$$\varphi' : K(\alpha_1) \longrightarrow K'(\beta_1)$$

que extiende a φ.

Como $f(x)$ tiene ahora menos que m raíces fuera de $K(\alpha_1)$, podemos usar la hipótesis de inducción para asegurar la existencia de un isomorfismo $\varphi^* : L \longrightarrow L'$ que extiende a $\varphi' : K(\alpha_1) \longrightarrow K'(\beta_1)$, y de donde extiende a $\varphi : K \longrightarrow K'$. ■

EJEMPLO 3.55 Mostrar que si α es una raíz de $x^3 - 3x + 1 = 0$, entonces $\alpha^2 - 2$ y $2 - \alpha - \alpha^2$ son las otras raíces.

Sea $f(x) = x^3 - 3x + 1$. Demostrar que $\mathbb{Q}(\alpha)$ es un campo de descomposición para $f(x)$ sobre $\mathbb{Q}$ y encontrar $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Demostración. Primero notemos que, como α es un cero de $f(x)$, tenemos $\alpha^3 = 3\alpha - 1$. Ahora:

$$\begin{aligned}(x-\alpha)(x-\alpha^2+2)(x+\alpha^2+\alpha-2) &= (x^2+(-\alpha^2-\alpha+2)x+\alpha^3-2\alpha)(x+\alpha^2+\alpha-2)\\ &= (x^2+(-\alpha^2-\alpha+2)x+\alpha-1)(x+\alpha^2+\alpha-2)\\ &= x^3+(-\alpha^2-\alpha+2+\alpha^2+\alpha-2)x^2+\\ &+ [(-\alpha^2-\alpha+2)(\alpha^2+\alpha-2)+\alpha-1]x+(\alpha-1)(\alpha^2+\alpha-2)\end{aligned}$$

pero claramente, el coeficiente de x^2 es 0, mientras que el de x es:

$$\begin{aligned}-\alpha^4-\alpha^3+2\alpha^2-\alpha^3-\alpha^2+2\alpha+2\alpha^2+2\alpha-4+\alpha-1 &= -\alpha(3\alpha-1)\\ &\quad -2(3\alpha-1)+3\alpha^2+5\alpha-5=-3\end{aligned}$$

y el término constante es:

$$\alpha^3+\alpha^2-2\alpha-\alpha^2-\alpha+2=1.$$

Como:

$$f(x)=(x-\alpha)(x-\alpha^2+2)(x+\alpha^2+\alpha-2),$$

vemos que $\mathbb{Q}(\alpha)$ es un campo de descomposición para f sobre $\mathbb{Q}$ y que:

$$\{1, \alpha, \alpha^2\}$$

es una base.

$$\therefore\ [\mathbb{Q}(\alpha):\mathbb{Q}]=3.\ \blacksquare$$

Sea F un campo y sea $f(x) \in F[x]$ un polinomio. Sobre un campo de descomposición para $f(x)$ tenemos la factorización:

$$f(x)=(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_k)^{n_k},$$

donde $\alpha_1, \alpha_2, ..., \alpha_k$ son elementos distintos del campo de descomposición y $n_i \geq 1$ para $i = 1, 2, ..., k$.

DEFINICIÓN 3.56 α_i se llama ***raíz múltiple*** si $n_i > 1$ y se llama ***raíz simple*** si $n_i = 1$. El entero n_i se llama la ***multiplicidad*** de la raíz α_i.

DEFINICIÓN 3.57 Un polinomio sobre F se llama ***separable*** si no tiene raíces múltiples (es decir, todas sus raíces son distintas). Un polinomio que no es separable, se llama ***inseparable.***

EJEMPLO 3.58 El polinomio $x^2 - 2$ es separable sobre $\mathbb{Q}$ pues sus dos raíces $\pm\sqrt{2}$ son distintas. El polinomio $(x^2 - 2)^n$ para cualquier $n \geq 2$ es inseparable, pues tiene a las raíces múltiples $\pm\sqrt{2}$, cada una de multiplicidad n.

DEFINICIÓN 3.59 La ***derivada*** del polinomio:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

se define como el polinomio:

$$D_x f(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in F[x].$$

Esta fórmula no es otra más que la usual de cálculo. Las reglas familiares de derivación, de cálculo, también se cumplen para derivadas en esta situación.

EJEMPLO 3.60 Sean $f(x), g(x)$ polinomios sobre un campo K, con $\text{gdo}(f(x)) = m$, $\text{gdo}(g(x)) = n$. Entonces:

i) $D_x(f(x) + g(x)) = D_x f(x) + D_x g(x)$.
ii) $D_x(f(x)g(x)) = f(x)D_x g(x) + (D_x f(x))g(x)$.

Demostración. Por inducción sobre $m + n$.
Es fácil verificar la identidad para valores pequeños de $m + n$. Supongamos que:

$$D_x(f(x)g(x)) = (D_x f(x))g(x) + f(x)(D_x g(x))$$

para todos los polinomios tales que $\text{gdo}(f(x))+\text{gdo}(g(x)) < k$. Sean:

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m,$$

donde $m > 1$, y:

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n,$$

y sea $m + n = k$. Escribimos:

$$f(x) = f_1(x) + f_2(x), \text{ donde } f_2(x) = a_m x^m$$

Entonces:

$$\begin{aligned} D_x(f(x)g(x)) &= D_x(f_1(x)g(x) + f_2(x)g(x)) \\ &= D_x(f_1(x)g(x)) + D_x(f_2(x)g(x)) \end{aligned}$$

Ahora:

$$D_x(f_1(x)g(x)) = (D_x f_1(x))g(x) + f_1(x)D_x g(x),$$

por hipótesis de inducción. También:

$$\begin{aligned} D_x(f_2(x)g(x)) &= D_x(a_m b_0 x^m + a_m b_1 x^{m+1} + \cdots + a_m b_n x^{m+n}) \\ &= a_m(mb_0 x^{m-1} + (m+1)b_1 x^m + (m+2)b_2 x^{m+1} + \cdots + (m+n)b_n x^{m+n-1}) \\ &= ma_m x^{m-1}(b_0 + b_1 x + \cdots + b_n x^n) + a_m x^m(b_1 + 2b_2 x + \cdots + nb_n x^{n-1}) \\ &= (D_x f_2(x))g(x) + f_2(x)D_x g(x) \end{aligned}$$

Entonces:

$$\begin{aligned} D_x(f(x)g(x)) &= D_x(f_1(x)g(x)) + D_x(f_2(x)g(x)) \\ &= (D_x(f_1(x)))g(x) + f_1(x)(D_x g(x)) + (D_x(f_2(x)))g(x) + f_2(x)(D_x(g(x))) \\ &= (D_x(f_1(x) + f_2(x)))g(x) + (f_1(x) + f_2(x))(D_x g(x)) \\ &= (D_x f(x))g(x) + f(x)(D_x g(x)). \blacksquare \end{aligned}$$

Existe un criterio simple para determinar cuándo un polinomio tiene raíces múltiples:

PROPOSICIÓN 3.61 Un polinomio $f(x)$ tiene una raíz múltiple α si y sólo si α es también una raíz de $D_x f(x)$, es decir, $f(x)$ y $D_x f(x)$ son ambos divisibles por el polinomio mínimo para α. En particular, $f(x)$ es separable si y sólo si es primo relativo a su derivada.

Demostración. $\Longrightarrow$) Supongamos que α es una raíz múltiple de $f(x)$. Entonces:

$$f(x) = (x - \alpha)^n g(x),$$

para algún entero $n \geq 2$ y algún polinomio $g(x)$. Tomando derivadas, obtenemos:

$$D_x f(x) = n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n D_x g(x),$$

lo cual muestra que $(n \geq 2),\ D_x f(x)$ tiene a α como una raíz.

$\Longleftarrow$) Supongamos que α es una raíz tanto de $f(x)$ como de $D_x f(x)$. Entonces escribimos:

$$f(x) = (x - \alpha)h(x),$$

para algún polinomio $h(x)$, y tomamos la derivada:

$$D_x f(x) = h(x) + (x - \alpha)D_x h(x).$$

Como $D_x f(\alpha) = 0$ por hipótesis, sustituyendo α en la ecuación anterior tenemos que $0 = h(\alpha)$ y así:

$$h(x) = (x - \alpha)h_1(x),$$

para algún polinomio $h_1(x)$ y:

$$f(x) = (x - \alpha)^2 h_1(x),$$

con lo que α es una raíz múltiple de $f(x)$.

La equivalencia con divisibilidad por el polinomio mínimo para α se sigue de la proposición 3.38. El último enunciado es entonces claro: Sea α cualquier raíz de un factor común de $f(x)$ y $D_x f(x)$. $\blacksquare$

EJEMPLO 3.62 Sea F un campo de característica p. El polinomio $x^{p^n} - x$ sobre F tiene derivada:

$$p^n x^{p^n - 1} - 1 = -1.$$

Como en este caso la derivada no tiene raíces, pues es una constante, se sigue que el polinomio no tiene raíces múltiples, de donde, es separable.

COROLARIO 3.63 Cada polinomio irreducible sobre un campo de característica 0 es separable. Un polinomio sobre un tal campo es separable si y sólo si es el producto de polinomios irreducibles distintos.

Demostración. Supongamos que F es un campo de característica 0 y $p(x) \in F[x]$ es irreducible de grado n. Entonces la derivada $D_x p(x)$ es un polinomio de grado $n-1$. Salvo factores constantes, los únicos factores de $p(x)$ en $F[x]$ son 1 y $p(x)$, así $D_x p(x)$ debe ser primo relativo a $p(x)$. Esto muestra que cualquier polinomio irreducible sobre un campo de característica 0 es separable. El segundo enunciado es fácil ya que distintos irreducibles nunca tienen ceros en común. (Proposición 3.38). ■

DEFINICIÓN 3.64 Un campo K se llama ***perfecto*** si cada polinomio en $K[x]$ es separable sobre K.

Así, de lo anterior, tenemos de inmediato:

COROLARIO 3.65 Cada campo de característica 0 es perfecto. ■

DEFINICIÓN 3.66 El campo K se dice que es ***separable*** sobre F si cada elemento de K, que es algebraico sobre F, es la raíz de un polinomio separable sobre F. (Equivalentemente, el polinomio mínimo sobre F de cada elemento de K es separable). Un campo que no es separable se llama ***inseparable.*** Por ejemplo $\mathbb{Q}(\pi)$ es inseparable sobre $\mathbb{Q}$, pues π no es algebraico sobre $\mathbb{Q}$. Sin embargo, π es algebraico sobre $\mathbb{Q}(\pi)$.

CAPÍTULO 4

EL GRUPO DE GALOIS

4.1 Definiciones Básicas.

Sea K un campo.

DEFINICIÓN 4.1 Un isomorfismo α de K consigo mismo se llama un ***automorfismo de*** K. La colección de automorfismos de K se denotará por $Aut(K)$.

DEFINICIÓN 4.2 Un automorfismo $\alpha \in Aut(K)$ se dice que ***fija*** a un elemento $x \in K$ si $\alpha(x) = x$. Si F es un subconjunto de K (por ejemplo, un subcampo), entonces un automorfismo α se dice que ***fija a*** F si fija a todos los elementos de F, es decir, $\alpha(x) = x,\ \forall x \in F$.

Notemos que cualquier campo tiene al menos un automorfismo, la función identidad, denotado por ι y algunas veces llamado el ***automorfismo trivial.***

DEFINICIÓN 4.3 Sea K/F una extensión de campos. $Aut(K/F)$ denotará la colección de automorfismos de K que fijan a F. Si $\alpha \in Aut(K/F)$ entonces α se llama F***-automorfismo.***

PROPOSICIÓN 4.4 $Aut(K)$ es un grupo bajo la composición de funciones, y $Aut(K/F)$ es un subgrupo de $Aut(K)$.

Demostración. La composición de funciones siempre es asociativa, pues para toda $x \in K$ y todo $\alpha, \beta, \gamma \in Aut(K)$ tenemos:

$$[(\alpha \circ \beta) \circ \gamma](x) = (\alpha \circ \beta)[\gamma(x)] = \alpha(\beta(\gamma(x))),$$

y,

$$[\alpha \circ (\beta \circ \gamma)](x) = \alpha([\beta \circ \gamma](x)) = \alpha(\beta(\gamma(x))).$$

Existe un automorfismo identidad $\iota \in Aut(K)$, definido por $\iota(x) = x$ para toda $x \in K$, y claramente:

$$\iota \circ \alpha = \alpha \circ \iota = \alpha,\ \forall \alpha \in Aut(K).$$

Finalmente, para cada automorfismo $\alpha \in Aut(K)$, existe una función inversa, α^{-1} definida por la propiedad de que $\alpha^{-1}(x)$ es el único $z \in K$ tal que $\alpha(z) = x$. Esta función también es un automorfismo, pues si $x, y \in K,\ \alpha^{-1}(x) = z,\ \alpha^{-1}(y) = t$, entonces $\alpha(z) = x,\ \alpha(t) = y$, y así $\alpha(z + t) = x + y$. De donde:

$$\begin{aligned} \alpha^{-1}(x) + \alpha^{-1}(y) &= z + t \\ &= \alpha^{-1}(\alpha(z + t)) \\ &= \alpha^{-1}(x + y), \end{aligned}$$

y similarmente, podemos ver que:

$$(\alpha^{-1}(x))(\alpha^{-1}(y)) = \alpha^{-1}(xy).$$

Así, $\alpha^{-1} \in Aut(K)$, y tiene la propiedad de que $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = \iota$.

$$\therefore \ Aut(K) \text{ es un grupo.}$$

Ahora veamos que $Aut(K/F)$ es un subgrupo. Ciertamente $\iota \in Aut(K/F)$. Sean $\alpha, \beta \in Aut(K/F)$. Entonces para toda $x \in F$:

$$x = \beta^{-1}(\beta(x)) = \beta^{-1}(x),$$

y así:

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

Luego $\alpha\beta^{-1} \in Aut(K/F)$ y, por el criterio de subgrupo, $Aut(K/F)$ es un subgrupo de $Aut(K)$. ■

Nos referiremos a $Aut(K)$ como el ***grupo de automorfismos de*** K y $Aut(K/F)$ como el ***grupo de Galois de*** K ***sobre*** F**,** y será denotado por $Gal(K/F)$. El ***grupo de Galois,*** $Gal(f(x))$***, de un polinomio*** $f(x)$ en $F[x]$ se define como $Gal(K/F)$, donde K es un campo de descomposición de $f(x)$ sobre F.

PROPOSICIÓN 4.5 Sea K/F una extensión de campos y sea $z \in K$ algebraico sobre F. Entonces para cualquier $\alpha \in Gal(K/F)$, $\alpha(z)$ es una raíz del polinomio mínimo para z sobre F, es decir, $Gal(K/F)$ permuta las raíces de polinomios irreducibles. Equivalentemente, cualquier polinomio con coeficientes en F que tiene a z como una raíz también tiene a $\alpha(z)$ como una raíz.

Demostración. Sea:

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

el polinomio mínimo para z, donde $a_0, a_1, ..., a_n \in F$, y supongamos que $f(z) = 0$. Entonces:

$$\begin{aligned} f(\alpha(z)) &= a_0 + a_1\alpha(z) + \cdots + a_n(\alpha(z))^n \\ &= \alpha(a_0) + \alpha(a_1)\alpha(z) + \cdots + \alpha(a_n)\alpha(z^n) \\ &= \alpha(a_0 + a_1z + \cdots + a_nz^n) \\ &= \alpha(0) = 0. \blacksquare \end{aligned}$$

Ahora introducimos una idea importante que conecta a los subcampos E de K que contienen a F y los subgrupos H de $Gal(K/F)$. Para cada E definimos:

$$\Gamma(E) = \{\alpha \in Aut(K) | \alpha(z) = z, \ \forall z \in E\}, \tag{1}$$

y, para cada H definimos:

$$\Phi(H) = \{x \in K | \alpha(x) = x, \forall \alpha \in H\}. \tag{2}$$

Notemos que Γ es la función que asocia al subcampo E, el subgrupo $Gal(K/E)$, y Φ es la función que asocia al subgrupo H el conjunto $\Phi(H)$, a veces denotado K_H, el cual recibe el nombre de campo fijo. ($\Phi(H)$ es de hecho un subcampo de K como lo muestra el teorema siguiente.) La esencia de la teoría de Galois está contenida en estas dos funciones, y el objetivo principal de esta sección es encontrar condiciones bajo las cuales éstas son mutuamente inversas.

TEOREMA 4.6 Sea K/F una extensión.

i) Para cada subcampo E de K que contiene a F, el conjunto $\Gamma(E)$ es un subgrupo de $Gal(K/F)$.
ii) Para cada subgrupo H de $Gal(K/F)$, el conjunto $\Phi(H)$ es un subcampo de K que contiene a F.

Demostración. *i*) $\Gamma(E) \neq \varnothing$, pues $\iota \in \Gamma(E)$, (el automorfismo identidad).

Ahora, como cada automorfismo que fija a todos los elementos de E automáticamente fija a todos los elementos de F, tenemos:

$$\Gamma(E) \subseteq Gal(K/F).$$

$$\therefore\ \Gamma(E) \leq Gal(K/F).$$

Notemos, además que $\Gamma(E) = Gal(K/E)$, pues si $\alpha \in \Gamma(E)$, entonces para toda $z \in E$ se tiene $\alpha(z) = z$ y así $\alpha \in Gal(K/E)$. Análogamente $Gal(K/E) \subseteq \Gamma(E)$.

ii) Como cada automorfismo en $Gal(K/F)$ fija a los elementos de F, entonces $F \subseteq \Phi(H)$. Sean $x, y \in \Phi(H)$. Entonces, para toda $\alpha \in H$:

$$\alpha(x-y) = \alpha(x) - \alpha(y) = x - y,$$

y así $x - y \in \Phi(H)$. Si $y \neq 0$, entonces, para toda $\alpha \in H$:

$$\begin{aligned} \alpha(xy^{-1}) &= \alpha(x)\alpha(y^{-1}) \\ &= \alpha(x)(\alpha(y))^{-1} \\ &= xy^{-1}, \end{aligned}$$

De donde $xy^{-1} \in \Phi(H)$. Por lo tanto $\Phi(H)$ es un subcampo de K. ■

TEOREMA 4.7 Sea K/F una extensión.

i) Si E_1, E_2 son subcampos de K que contienen a F, entonces:

$$E_1 \subseteq E_2 \implies \Gamma(E_1) \supseteq \Gamma(E_2).$$

ii) Si H_1, H_2 son subgrupos de $Gal(K/F)$, entonces:

$$H_1 \subseteq H_2 \implies \Phi(H_1) \supseteq \Phi(H_2).$$

Demostración. *i*) Supongamos que $E_1 \subseteq E_2$, y sea $\alpha \in \Gamma(E_2)$. Entonces α fija a cada elemento de E_2 y así fija a cada elemento de E_1.

$$\therefore\ \ \alpha \in \Gamma(E_1).$$

ii) Supongamos que $H_1 \subseteq H_2$, y sea $z \in \Phi(H_2)$. Entonces:

$$\alpha(z) = z, \text{ para cada } \alpha \in H_2,$$

en particular, para cada $\alpha \in H_1$

$$\therefore \quad z \in \Phi(H_1). \blacksquare$$

EJEMPLO 4.8 Describir el grupo $Gal(\mathbb{C}/\mathbb{R})$.

Solución. Si $\alpha \in Gal(\mathbb{C}/\mathbb{R})$, entonces $\alpha(x) = x, \ \forall x \in \mathbb{R}$. Sea $\alpha(i) = j$. Entonces:

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

y así $j = \pm i$. Si $j = i$ entonces, para todo $x + yi \in \mathbb{C}$, con $x, y \in \mathbb{R}$, tenemos:

$$\alpha(x + yi) = \alpha(x) + \alpha(y)\alpha(i) = x + yi.$$

$$\therefore \ \alpha = \iota, \text{ el automorfismo identidad.}$$

Si $j = -i$, entonces:

$$\alpha(x + yi) = x - yi.$$

Claramente esta función fija a los elementos de $\mathbb{R}$. Para verificar que es un automorfismo, notemos que:

$$\begin{aligned} \alpha((x + yi) + (u + vi)) &= \alpha((x + u) + (y + v)i) \\ &= (x + u) - (y + v)i \\ &= (x - yi) + (u - vi) \\ &= \alpha(x + yi) + \alpha(u + vi), \end{aligned}$$

y:

$$\begin{aligned} \alpha((x + yi)(u + vi)) &= \alpha((xu - yv) + (xv + yu)i) \\ &= (xu - yv) - (xv + yu)i \\ &= (x - yi)(u - vi) \\ &= \alpha(x + yi)\alpha(u + vi). \end{aligned}$$

$$\therefore \ Gal(\mathbb{C}/\mathbb{R}) \text{ es el grupo } \{\iota, \kappa\} \text{ de orden 2,}$$

donde κ es la función ***conjugación compleja*** que manda $x + yi$ a $x - yi$.

Como $[\mathbb{C} : \mathbb{R}] = 2$, un número primo, no puede haber subcampos entre $\mathbb{C}$ y $\mathbb{R}$. Tenemos:

$$\Phi(\{\iota\}) = \mathbb{C}, \quad \Phi(\{\iota, \kappa\}) = \mathbb{R}. \blacksquare$$

TEOREMA 4.9 Sean K/F una extensión, E un subcampo de K que contiene a F, y $H \leq Gal(K/F)$. Entonces:

$$E \subseteq \Phi(\Gamma(E)), \quad H \subseteq \Gamma(\Phi(H)).$$

Demostración. Sea $z \in E$. El grupo $\Gamma(E)$ es el conjunto de todos los automorfismos que fijan a cada elemento de E, y así z queda fijo por todos los automorfismos en $\Gamma(E)$. Esto es, $z \in \Phi(\Gamma(E))$.

$$\therefore \ E \subseteq \Phi(\Gamma(E)).$$

Sea $\alpha \in H$. Entonces el campo $\Phi(H)$ es el conjunto de elementos de K que quedan fijos por cada elemento de H, y así α fija a cada elemento de $\Phi(H)$. Es decir $\alpha \in \Gamma(\Phi(H))$.

$$\therefore\ H \subseteq \Gamma(\Phi(H)).\ \blacksquare$$

EJEMPLO 4.10 Demostrar que $\Gamma\Phi\Gamma = \Gamma$, y $\Phi\Gamma\Phi = \Phi$.

Demostración. Sea E un subcampo de K que contiene a F y sea H un subgrupo de $Gal(K/F)$. Del teorema 4.9 sabemos que:

$$E \subseteq \Phi(\Gamma(E)),$$

y, por la propiedad de revertir orden, tenemos:

$$\Gamma(E) \supseteq (\Gamma\Phi\Gamma)(E).$$

Por otro lado, sabemos que

$$H \subseteq \Gamma(\Phi(H)),$$

y así, sustituyendo $\Gamma(E)$ por H:

$$\Gamma(E) \subseteq (\Gamma\Phi\Gamma)(E).$$

$$\therefore\ \Gamma\Phi\Gamma = \Gamma.$$

Similarmente, de $H \subseteq \Gamma(\Phi(H))$ tenemos, por la propiedad de revertir el orden, que:

$$\Phi(H) \supseteq (\Phi\Gamma\Phi)(H).$$

Por otra parte, sustituyendo $\Phi(H)$ por E en $E \subseteq \Phi(\Gamma(E))$, tenemos:

$$\Phi(H) \subseteq (\Phi\Gamma\Phi)(H).$$

$$\therefore\ \Phi\Gamma\Phi = \Phi.\ \blacksquare$$

Así, por ejemplo si $\alpha \in Gal(\mathbb{Q}(u)/\mathbb{Q})$, donde $u = \sqrt[3]{2}$, entonces:

$$(\alpha(u))^3 = \alpha(u^3) = \alpha(2) = 2,$$

luego, siendo real, $\alpha(u)$ debe ser igual a u. Se sigue que $Gal(\mathbb{Q}(u)/\mathbb{Q}) = \{\iota\}$, el grupo trivial.

Ahora, dos funciones pueden ser mutuamente inversas sólo si son biyecciones, y aquí tenemos:

$$\Gamma(\mathbb{Q}(u)) = \Gamma(\mathbb{Q}) = \{\iota\}.$$

También:

$$\Phi(\Gamma(\mathbb{Q})) = \Phi(\{\iota\}) = \mathbb{Q}(u).\ \blacksquare$$

Sea K un campo, y sea S un conjunto no vacío. Sea $\mathcal{M}$ el conjunto de funciones de S en K. Si $\theta, \varphi \in \mathcal{M}$, entonces, $\theta + \varphi$, definida por:

$$(\theta + \varphi)(s) = \theta(s) + \varphi(s), \quad \forall s \in S \tag{3}$$

es una función de S en K, y así $\theta + \varphi \in \mathcal{M}$. Similarmente, si $\theta \in \mathcal{M}$ y $a \in K$, entonces $a\theta$, definida por :

$$(a\theta)(s) = a\theta(s), \quad \forall s \in S \tag{4}$$

pertenece a $\mathcal{M}$. Es fácil verificar que $\mathcal{M}$ es un espacio vectorial con respecto a estas dos operaciones. El vector cero en $\mathcal{M}$ es la función ζ dada por:

$$\zeta(s) = 0, \quad s \in S. \tag{5}$$

Normalmente la denotamos simplemente por 0, pues el contexto usualmente hará claro cuándo entenderemos el elemento cero de K o la función ζ.

DEFINICIÓN 4.11 Un conjunto $\{\theta_1, \theta_2, ..., \theta_n\}$ de elementos de $\mathcal{M}$ es ***linealmente independiente*** si, para $a_1, a_2, ..., a_n$ en K:

$$a_1\theta_1(s) + a_2\theta_2(s) + \cdots + a_n\theta_n(s) = 0,$$

para toda $s \in S$ si y sólo si $a_1 = a_2 = \cdots = a_n = 0$. En otras palabras, podemos escribir la condición como:

$$a_1\theta_1 + a_2\theta_2 + \cdots + a_n\theta_n = 0 \iff a_1 = a_2 = \cdots = a_n = 0.$$

TEOREMA 4.12 Sean K y L campos, y sean $\theta_1, \theta_2, ..., \theta_n$ monomorfismos distintos de K en L. Entonces $\{\theta_1, \theta_2, ..., \theta_n\}$ es un conjunto linealmente independiente en el espacio vectorial $\mathcal{M}$ de todas las funciones de K en L.

Demostración. Por inducción sobre n.

Si $n = 1$, el enunciado es verdadero, ya que θ_1, siendo un monomorfismo, manda a 1_K a 1_L, y entonces no es la función cero definida por (5).

Supongamos ahora que se ha establecido que cada conjunto de menos de n distintos monomorfismos de K en L es linealmente independiente. Y supongamos, por contradicción, que existen $a_1, a_2, ..., a_n$ en L, no todos cero, tales que:

$$a_1\theta_1 + a_2\theta_2 + \cdots + a_n\theta_n = 0. \tag{6}$$

De hecho, podemos suponer que todos los a_i son distintos de cero: si, por ejemplo, $a_n = 0$, entonces:

$$\{\theta_1, \theta_2, ..., \theta_{n-1}\}$$

es linealmente independiente, en contradicción con la hipótesis de inducción. Dividiendo (6) con a_n obtenemos:

$$b_1\theta_1 + \cdots + b_{n-1}\theta_{n-1} + \theta_n = 0, \tag{7}$$

donde $b_i = a_i/a_n, \ i = 1, 2, ..., n-1$.

Los monomorfismos, θ_1 y θ_n son distintos por hipótesis, luego existe $u \in K$ tal que:

$$\theta_1(u) \neq \theta_n(u);$$

ciertamente, el elemento u no es cero, así como tampoco $\theta_1(u)$ y $\theta_n(u)$. Para cada $z \in K$:

$$b_1\theta_1(uz) + \cdots + b_{n-1}\theta_{n-1}(uz) + \theta_n(uz) = 0, \tag{8}$$

y como $\theta_1, \theta_2, ..., \theta_n$ son monomorfismos tenemos que:

$$b_1\theta_1(u)\theta_1(z) + \cdots + b_{n-1}\theta_{n-1}(u)\theta_{n-1}(z) + \theta_n(u)\theta_n(z) = 0. \tag{9}$$

Dividiendo esto con $\theta_n(u)$, tenemos que, para toda $z \in K$:

$$b_1 \frac{\theta_1(u)}{\theta_n(u)}\theta_1(z) + \cdots + b_{n-1}\frac{\theta_{n-1}(u)}{\theta_n(u)}\theta_{n-1}(z) + \theta_n(z) = 0, \tag{10}$$

la cual podemos reescribir como:

$$b_1 \frac{\theta_1(u)}{\theta_n(u)}\theta_1 + \cdots + b_{n-1}\frac{\theta_{n-1}(u)}{\theta_n(u)}\theta_{n-1} + \theta_n = 0, \tag{11}$$

donde el 0 de la derecha sabemos que significa la función cero definida por (5). Restando (11) de (7) :

$$b_1\Big(1 - \frac{\theta_1(u)}{\theta_n(u)}\Big)\theta_1 + \cdots + b_{n-1}\Big(1 - \frac{\theta_{n-1}(u)}{\theta_n(u)}\Big)\theta_{n-1} = 0. \tag{12}$$

La elección de u como un elemento tal que $\theta_1(u) \neq \theta_n(u)$ significa que el coeficiente de θ_1 es distinto de 0. Así (12) implica que el conjunto $\{\theta_1, \theta_2, ..., \theta_{n-1}\}$ es linealmente dependiente, en contradicción con la hipótesis de inducción. ■

Sean V y W espacios vectoriales de dimensión finita sobre un campo K, con dimensiones m, n, respectivamente, y sea $T : V \longrightarrow W$ una transformación lineal. La ***imagen de T*** es el conjunto:

$$\mathbf{im}T = \{T(v) | v \in V\},$$

la cual es un subespacio de W, y su dimensión, **dim(imT)**, se llama ***rango de T***, $\rho(T)$. El ***núcleo de T*** es el conjunto:

$$\mathbf{Núc}T = \{v \in V | T(v) = 0\},$$

y es un subespacio de V, y su dimensión, **dim(NúcT)**, se llama la ***nulidad de T***, $\nu(T)$. Un resulatdo estándar en álgebra lineal enuncia que:

$$\rho(T) + \nu(T) = dimV = m. \tag{13}$$

Si $n < m$, entonces ciertamente, $\rho(T) \leq n < m$, y así $\nu(T) > 0$. Por lo tanto existe un vector distinto de cero v en V tal que $T(v) = 0$.

En términos más concretos, si tenemos una matriz de $n \times m$, $A = [a_{ij}]_{n\times m}$ con entradas en K, y un vector columna de $m \times 1$, v, la función $v \mapsto Av$ es una función lineal del espacio vectorial K^m en el espacio vectorial K^n. Del enunciado final del último párrafo, deducimos que , si $n < m$, entonces existe un vector $v \neq 0$ tal que $Av = 0$. Esto es, existen $v_1, v_2, ..., v_m \in K$, no todos cero, tales que:

$$a_{j1}v_1 + a_{j2}v_2 + \cdots + a_{jm}v_m = 0, \ j = 1, 2, ..., n. \tag{14}$$

TEOREMA 4.13 Sea K una extensión finita de un campo F, y sea G un subgrupo finito de $Gal(K/F)$. Entonces:

$$[K : \Phi(G)] = |G|.$$

Demostracíón. Sean $|G| = m$ y $[K : \Phi(G)] = n$.
Supongamos que $m > n$, y escribimos:

$$G = \{\alpha_1 = \iota, \alpha_2, ..., \alpha_m\},$$

donde ι es la función identidad, y supongamos que $\{z_1, z_2, ..., z_n\}$ es una base para K sobre $\Phi(G)$. Consideremos la matriz de $n \times m$:

$$\begin{bmatrix} \alpha_1(z_1) & \alpha_2(z_1) & \cdots & \alpha_m(z_1) \\ \alpha_1(z_2) & \alpha_2(z_2) & \cdots & \alpha_m(z_2) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1(z_n) & \alpha_2(z_n) & \cdots & \alpha_m(z_n) \end{bmatrix}$$

De (14) deducimos que existen $v_1, v_2, ..., v_m \in K$, no todos cero, tales que:

$$\alpha_1(z_j)v_1 + \alpha_2(z_j)v_2 + \cdots + \alpha_m(z_j)v_m = 0,\ j = 1, 2, ..., n \tag{15}$$

Sea $b \in K$. Como $\{z_1, z_2, ..., z_n\}$ es una base para K sobre $\Phi(G)$, existen $b_1, b_2, ..., b_n$ en $\Phi(G)$ con:

$$b = b_1 z_1 + b_2 z_2 + \cdots + b_n z_n. \tag{16}$$

Multiplicando las n ecuaciones (15) con $b_1, b_2, ..., b_n$, respectivamente, vemos que:

$$b_j\alpha_1(z_j)v_1 + b_j\alpha_2(z_j)v_2 + \cdots + b_j\alpha_m(z_j)v_m = 0,\ j = 0, 1, ..., n. \tag{17}$$

Pero todas las b_j están en $\Phi(G)$ y todas las α_i están en G, luego:

$$b_j = \alpha_i(b_j) \text{ para toda } i, j.$$

Así, podemos reescribir las ecuaciones (17) como:

$$\alpha_1(b_j z_j)v_1 + \alpha_2(b_j z_j)v_2 + \cdots + \alpha_m(b_j z_j)v_m = 0,\ j = 1, 2, ..., n. \tag{18}$$

Sumando estas n ecuaciones y usando (16), obtenemos:

$$v_1\alpha_1(b) + v_2\alpha_2(b) + \cdots + v_m\alpha_m(b) = 0.$$

Esto se cumple para toda $b \in K$, y así, los automorfismos $\alpha_1, \alpha_2, ..., \alpha_m$ son linealmente dependientes. Por el teorema 4.12, esto es imposible. En consecuencia $n \geq m$.

Ahora supongamos que $n = [K : \Phi(G)] > m$. Esta vez, tenemos el subconjunto $\{z_1, z_2, ..., z_{m+1}\}$ de K, el cual es linealmente independiente sobre $\Phi(G)$, y consideremos la matriz de $m \times (m + 1)$:

$$\begin{bmatrix} \alpha_1(z_1) & \alpha_1(z_2) & \cdots & \alpha_1(z_{m+1}) \\ \alpha_2(z_1) & \alpha_2(z_2) & \cdots & \alpha_2(z_{m+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_m(z_1) & \alpha_m(z_2) & \cdots & \alpha_m(z_{m+1}) \end{bmatrix}.$$

Por (14), existen $u_1, u_2, ..., u_{m+1} \in K$, no todos cero, tales que:

$$\alpha_j(z_1)u_1 + \alpha_j(z_2)u_2 + \cdots + \alpha_j(z_{m+1})u_{m+1} = 0,\ j = 1, 2, ..., m.$$

Supongamos que los elementos $u_1, u_2, ..., u_{m+1}$ se eligen de tal forma que el número de elementos no nulos sea mínimo. Podemos, entonces, reetiquetarlos de modo que $u_1, u_2, ..., u_r$ son distintos de cero y $u_{r+1} = \cdots = u_{m+1} = 0$. Entonces tenemos:

$$\alpha_j(z_1)u_1 + \alpha_j(z_2)u_2 + \cdots + \alpha_j(z_r)u_r = 0,\ j = 1, 2, ..., m. \tag{19}$$

Dividiendo (19) con u_r:

$$\alpha_j(z_1)u'_1 + \cdots + \alpha_j(z_{r-1})u'_{r-1} + \alpha_j(z_r) = 0,\ j = 1, 2, ..., m, \tag{20}$$

donde $u'_i = u_i/u_r,\ i = 1, 2, ..., r-1$. Como $\alpha_1 = \iota$, en G, la primera de estas ecuaciones es:

$$z_1u'_1 + \cdots + z_{r-1}u'_{r-1} + z_r = 0. \tag{21}$$

Si todos los elementos $u'_1, \ldots, u'_{r-1}$ pertenecieran a $\Phi(G)$, entonces $\{z_1, z_2, ..., z_r\}$ sería linealmente dependiente sobre $\Phi(G)$, y sabemos que no es así. De aquí que al menos una de las $u'_1, \ldots, u'_{r-1}$ no está en $\Phi(G)$: sin pérdida de generalidad, podemos suponer que $u'_1 \notin \Phi(G)$. Esto es, existe un automorfismo en G, que podemos tomar como α_2 tal que:

$$\alpha_2(u'_1) \neq u'_1. \tag{22}$$

Aplicamos α_2 a las ecuaciones de (20) para $j = 1, 2, .., m$:

$$(\alpha_2\alpha_j)(z_1)\alpha_2(u'_1) + \cdots + (\alpha_2\alpha_j)(z_{r-1})\alpha_2(u'_{r-1}) + (\alpha_2\alpha_j)(z_r) = 0. \tag{23}$$

Como G es un grupo, el conjunto $\{\alpha_2\alpha_1, \alpha_2\alpha_2, ..., \alpha_2\alpha_m\}$ es el mismo que $\{\alpha_1, \alpha_2, ..., \alpha_m\}$: sólo el orden de los elementos es diferente. De aquí que podemos cambiar el orden de las ecuaciones enlistadas en (23) y obtener:

$$\alpha_j(z_1)\alpha_2(u'_1) + \cdots + \alpha_j(z_{r-1})\alpha_2(u'_{r-1}) + \alpha_j(z_r) = 0,\ j = 1, 2, .., m. \tag{24}$$

Restando (24) de (20) tenemos, para $j = 1, 2, .., m$:

$$\alpha_j(z_1)(u'_1 - \alpha_2(u'_1)) + \cdots + \alpha_j(z_{r-1})(u'_{r-1} - \alpha_2(u'_{r-1})) = 0. \tag{25}$$

Sean $v_i = u'_i - \alpha_2(u'_i)$ para $i = 1, 2, ..., r-1$ y $v_i = 0$ para $i = r, r+1, ..., m+1$. Entonces (25) se vuelve:

$$\alpha_j(z_1)v_1 + \cdots + \alpha_j(z_2)v_2 + \cdots + \alpha_j(z_{m+1})v_{m+1} = 0,\ j = 1, 2, ..., m.$$

De (22) sabemos que no todas las v_i son cero, y también hemos supuesto que no más de $r-1$ de las v_i son no cero. Esto es una contradicción a la propiedad enunciada de los elementos $u_1, u_2, ..., u_{m+1}$, y así concluimos que no es posible tener $[K : \Phi(G)] > m$.

$$\therefore\ [K : \Phi(G)] = m.\ \blacksquare$$

4.2 Extensiones Normales.

TEOREMA 4.14 Sea K una extensión normal de grado finito sobre un campo F, y sea E un subcampo de K que contiene a F. Entonces cada $F-$automorfismo de E se puede extender a un $F-$automorfismo de K.

Demostración. Sea φ un $F-$automorfismo de E. Como K es normal, existe un polinomio $f(x)$ tal que K es un campo de descomposición para $f(x)$ sobre F. También es un campo de descomposición para $f(x)$ sobre E y sobre $\varphi(E)$. Por el teorema 3.54 (con $L' = K$), deducimos que existe un $F-$automorfismo φ^* de K que extiende a φ. $\blacksquare$

TEOREMA 4.15 Sea K una extensión normal de grado finito sobre un campo F. Si z_1 y z_2 son

raíces en K de un polinomio irreducible en $F[x]$, entonces existe un $F-$automorfismo θ de K tal que $\theta(z_1) = z_2$.

Demostración. Por el corolario 3.47, existe un $F-$automorfismo de $F(z_1)$ sobre $F(z_2)$. Por el teorema 4.14, éste se puede extender a un $F-$automorfismo θ de K. ■

EJEMPLO 4.16 Sea K una extensión normal de un campo F, y sea E un subcampo de K que contiene a F. Entonces K es un campo de descomposición para algún polinomio $f(x) \in F[x]$. Como $f(x) \in E[x]$, entonces K es una extensión normal de E.

DEFINICIÓN 4.17 Sea K una extensión finita de un campo F. Un campo N que contiene a K se llama una ***cerradura normal de*** K ***sobre*** F si:

i) es una extensión normal de F; y,
ii) si E es un subcampo propio de N que contiene a K, entonces E no es una extensión normal de F.

TEOREMA 4.18 Sea K una extensión normal finita de un campo F, y sea E un subcampo de K que contiene a F. Entonces, E es una extensión normal de F si y sólo si cada $F-$monomorfismo de E en K es un $F-$automorfismo de E.

Demostración. $\Longrightarrow$) Supongamos primero que E es una extensión normal, entonces E es su propia cerradura normal. Sea φ un $F-$monomorfismo de E en K, y sea $z \in E$. Sea:

$$m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

el polinomio mínimo de z sobre F. Entonces:

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = 0,$$

y así, aplicando φ a esta igualdad, obtenemos:

$$(\varphi(z))^n + a_{n-1}(\varphi(z))^{n-1} + \cdots + a_1\varphi(z) + a_0 = 0.$$

Y, por lo tanto, $\varphi(z)$ también es una raíz de $m(x)$ en K.

Pero z, un elemento de E, es una raíz del polinomio irreducible $m(x)$, luego, como E es normal, $m(x)$ se descompone completamente sobre E. De esta manera $\varphi(z) \in E$. De donde, $\varphi(E)$ es un campo contenido en E. Se sigue del ejemplo 2.63 que:

$$[\varphi(E) : F] = [\varphi(E) : \varphi(F)] = [E : F] = [E : \varphi(E)][\varphi(E) : F].$$

$$\Longrightarrow \ \varphi(E) = E$$

$$\therefore \ \varphi \text{ es un } F-\text{automorfismo de } E.$$

$\Longleftarrow$) Supongamos ahora que cada $F-$monomorfismo de E en K es un $F-$automorfismo de E. Sea $f(x)$ un polinomio irreducible en $F[x]$ que tiene una raíz $z \in E$. Para establecer que E es una extensión normal de F, necesitamos mostrar que $f(x)$ se descompone completamente sobre E. Como K es normal,

ciertamente $f(x)$ se descompone completamente sobre sobre K. Sea z' otra raíz de $f(x)$ en K. Entonces, por el teorma 4.14, existe un $F-$automorfismo ψ de K tal que:

$$\psi(z) = z'.$$

Sea ψ^* la restricción de ψ a E. Entonces ψ^* es un $F-$monomorfismo de E en K, y así, por hipótesis, es un $F-$automorfismo de E.

$$\Longrightarrow\ z' = \psi(z) = \psi^*(z) \in E.$$

$$\therefore\ E \text{ es normal. } \blacksquare$$

4.3 La Correspondencia de Galois.

DEFINICIÓN 4.19 Un elemento algebraico en una extensión K de F se llama ***separable sobre*** F si su polinomio mínimo es separable sobre F.

TEOREMA 4.20 Sea K una extensión separable finita de un campo F, y sea E un subcampo de K que contiene a F. Entonces K es una extensión separable de E.

Demostración. Sea $a \in K$, y sean $m_F(x), m_E(x)$ los polinomios mínimos de a sobre F y E, respectivamente. Supongamos que $m_F(x)$ es separable. Dentro de $E[x]$ podemos usar el algoritmo de la división:

$$m_F(x) = qm_E(x) + r(x),\ \text{gdo}(r(x)) < \text{gdo}(m_E(x))$$

y, entonces:

$$r(a) = m_F(a) - q(a)m_E(a) = 0 - 0 = 0.$$

Este hecho contradice la minimalidad de m_E, a menos de que $r(x) = 0$.

$$\therefore\ m_F(x) = qm_E(x) \text{ en el anillo } E[x].$$

Si $m_E(x)$ no es separable, entonces existe un polinomio no constante $g(x)$ que divide a $m_E(x)$ y $D_x m_E(x)$. Como:

$$D_x m_F(x) = qD_x m_E(x) + m_E(x)D_x q,$$

entonces:

$$g(x)|m_F(x),\ \text{y}\ g(x)|D_x m_F(x).$$

Esto solamente puede suceder si $m_F(x)$ tiene al menos una raíz repetida en un campo de descomposición, y tenemos una contradicción. De esta manera, $m_E(x)$ es separable. $\blacksquare$

DEFICIÓN 4.21 Una extensión finita de un campo K que es tanto normal como separable se llama ***extensión de Galois.***

TEOREMA 4.22 Sea K una extensión de F separable de grado finito n. Entonces existen precisamente n diferentes F-monomorfismos de K en una cerradura normal N de K sobre F.

Demostración. Se hará por inducción sobre $[K : F]$.
Si $[K : F] = 1$, entonces $K = F = N$ y el único F-monomorfismo de F en N es la función identidad ι.

Supongamos ahora que el resultado se cumple para toda $n \leq k-1$, y supongamos que $[K : F] = k > 1$. Sea $z_1 \in K \setminus F$, y sea $m(x)$ (con $\text{gdo}(m(x)) = r \geq 2$) el polinomio mínimo de z_1 sobre F. Entonces:

$$F \subset F(z_1) \subseteq K \text{ y } [F(z_1) : F] = r.$$

Así, como $m(x)$ es irreducible y tiene una raíz z_1 en la extensión normal N, se descompone completamente sobre N. Como K es separable, las raíces de $m(x)$ son todas distintas. Supongamos que las raíces son $z_1, z_2, ..., z_r$. Sea $[K : F(z_1)] = s$; entonces $1 \leq s < k$ y $rs = k$.

El campo N es una cerradura normal de K sobre $F(z_1)$, y así, por hipótesis de inducción podemos suponer que el número de $F(z_1)-$monomorfismos de K en N es precisamente s: $\mu_1, \mu_2, ..., \mu_s$. Por el teorema 4.15, hay r distintos $F-$automorfismos $\lambda_1, \lambda_2, ..., \lambda_r$ de N, donde $\lambda_i(z_1) = z_i,\ i = 1, 2, ..., r$. Definimos las funciones $\varphi_{ij} : K \longrightarrow N$ por:

$$\varphi_{ij}(x) = \lambda_i(\mu_j(x)),\ x \in K,\ i = 1, 2, ..., r;\ j = 1, 2, ..., s. \tag{26}$$

Las definiciones hacen claro que las funciones son todas $F-$monomorfismos.

Veamos que todas son distintas. En primer lugar, notemos que:

$$\varphi_{ij}(z_1) = \lambda_i(\mu_j(z_1)) = \lambda_i(z_1) = z_i. \tag{27}$$

De donde, si $\varphi_{ij} = \varphi_{pq}$, se sigue que $i = p$. Supongamos ahora que $\varphi_{ij} = \varphi_{iq}$. Entonces, para toda $x \in L$:

$$\lambda_i(\mu_j(x)) = \lambda_i(\mu_q(x)).$$

Como λ_i es uno a uno, entonces $\mu_j(x) = \mu_q(x)$, para toda $x \in L$, y así $j = q$. Por lo tanto las funciones φ_{ij} son todas distintas, y de (26) deducimos que hay al menos $rs = k$ $F-$monomorfismos distintos de K en N.

Para mostrar que no hay más de k, debemos mostrar que cada $F-$monomorfismo ψ de K en N coincide con una de las funciones φ_{ij}. La función ψ debe mandar z_1 a otra raíz z_i de $m(x)$ en N. Sea $\chi : K \longrightarrow N$ definida por:

$$\chi(x) = \lambda_i^{-1}(\psi(x)).$$

Claramente, ésta es un $F-$monomorfismo; de hecho, como:

$$\chi(z_1) = \lambda_i^{-1}(\psi(z_1)) = \lambda_i^{-1}(z_i) = z_1,\ x \in L,$$

es un $F(z_1)-$monomorfismo, y entonces debe coincidir con alguna de $\mu_1, \mu_2, ..., \mu_s$, digamos con μ_j. Entonces:

$$\mu_j(x) = \lambda_i^{-1}(\psi(x)),\ \forall x \in K$$

y así, $\psi(x) = \lambda_i(\mu_j(x))$.

$$\therefore\quad \psi(x) = \varphi_{ij}(x). \blacksquare$$

Si en el enunciado del teorema suponemos que K es tanto normal como separable, entonces K es su propia cerradura normal, y obtenemos el siguiente corolario importante:

COROLARIO 4.23 Sea K una extensión de Galois de F, y sea G el grupo de Galois de K sobre F. Entonces:

$$|G| = [K : F]. \blacksquare$$

TEOREMA 4.24 Sea K una extensión finita de F. Entonces $\Phi(Gal(K/F)) = F$ si y sólo si K es una extensión normal y separable de F.

Demostración. Supongamos que K es una extensión normal y separable de F, y sea $[K : F] = n$. Por el corolario 4.23, $|Gal(K/F)| = n$. Denotemos $\Phi(Gal(K/F))$ por F'; entonces, del teorema 4.9, sabemos que $F \subseteq F'$. Por el teorema 4.13, tenemos que $[K : F'] = n$. De donde, como $F \subseteq F'$ y $[K : F] = [K : F']$, se sigue del ejemplo 2.63 que $F = F'$.

Ahora supongamos que $F = F'$. Sea:

$$Gal(K/F) = \{\varphi_1 = \iota, \varphi_2, ..., \varphi_n\}.$$

Sea $f(x) \in F[x]$ irreducible con una raíz $z \in K$. Para probar que K es normal, necesitamos establecer que $f(x)$ se descompone completamente sobre K.

Las imágenes de z bajo los $F-$automorfismos $\varphi_1, \varphi_2, ..., \varphi_n$ no necesitan ser todas distintas: sabemos que $\varphi_1(z) = z$, y podemos renombrar los elementos de Gal(K/F) para que $\varphi_2(z), ..., \varphi_r(z)$ sean las distintas imágenes renombradas de z bajo los automorfismos en Gal(K/F). Por simplicidad, escribimos $\varphi_i(z) = z_i,\ i = 1, 2, ..., r$. Notemos que $z_1 = z$.

LEMA 4.25 Para cada $\varphi_j(x)$ en Gal(K/F), tenemos:

$$\{z_1, z_2, ..., z_r\} = \{\varphi_j(z_1), \varphi_j(z_2), ..., \varphi_j(z_r)\}$$

Demostración. Notemos que:

$$\varphi_j(z_i) = (\varphi_j\varphi_i)(z) = z_k,$$

para alguna k, pues $\varphi_j\varphi_i \in Gal(K/F)$. Como φ_j es uno a uno, podemos concluir que permuta a los elementos $z_1, z_2, ..., z_r$. ■

Ahora sea $g(x)$ el polinomio:

$$(x - z_1)(x - z_2)\cdots(x - z_r) = x^r - e_1x^{r-1} + \cdots + (-1)^r e_r, \tag{28}$$

donde los coeficientes $e_1, e_2, ..., e_r$ son las funciones:

$$e_1 = \sum_{i=1}^{r} z_i,\ e_2 = \sum_{i \neq j} z_i z_j, ...,\ e_r = z_1 z_2 \cdots z_r.$$

Ninguna permutación de $z_1, z_2, ..., z_r$ modifica a estos coeficientes, y, por el lema 4.25, ninguna de las φ_j en Gal(K/F) los modifica. Así $g(x)$ es un polinomio con coeficientes en $\Phi(\text{Gal}(K/F))$, el cual, estamos suponiendo, coincide con F.

Recordemos ahora que z se definió como una raíz en K del polinomio irreducible $f(x) \in F[x]$.

LEMA 4.26 El polinomio $g(x)$ definido por (28) es el polinomio mínimo de z sobre F.

Demostración. Debemos mostrar que cada polinomio en $F[x]$ que tiene a z como una raíz es divisible por $g(x)$. Supongamos pues que:

$$h(x) = a_0 + a_1x + \cdots + a_mx^m,$$

con coeficientes en F, es tal que:

$$a_0 + a_1z + \cdots + a_mz^m = 0.$$

Podemos, entonces, aplicar cada una de las $\varphi_j(x)$ a esta relación: como $\varphi_j(x)$ deja fijos a los coeficientes a_i, obtenemos:

$$a_0 + a_1 z_j + \cdots + a_m z_j^m = 0,\ j = 1, 2, .., r,$$

y se sigue que $h(x)$ es divisible por cada uno de $x - z_1, x - z_2, ..., x - z_r$. Por lo tanto $g(x)$ divide a $h(x)$. ■

Ahora, entre los polinomios en $F[x]$ que tienen una raíz $z \in K$ está el polinomio $f(x)$ con el que empezamos. Por el lema 4.26, $g(x)|f(x)$, y así, como $f(x)$ es irreducible, es un múltiplo de $g(x)$. Como $g(x)$ se descompone completamente sobre K, también $f(x)$. Además, todas sus raíces son distintas, y en consecuencia es, como queríamos, una extensión normal y separable de F ■.

TEOREMA 4.27 Sea K una extensión de Galois de un campo F, y sea E un subcampo de K que contiene a F. Si $\delta \in$Gal(K/F), entonces $\Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}$.

Demostración. Escribimos $\delta(E) = E'$, $\Gamma(E) = H$ y $\Gamma(E') = H'$. Debemos mostrar que $H' = \delta H \delta^{-1}$. Entonces, sea $\theta \in H$; mostraremos que $\delta\theta\delta^{-1} \in H'$. Sea $z' \in E'$ y sea z el único elemento de E tal que $\delta(z) = z'$. Entonces, como θ fija a todos los elementos de E, tenemos que:

$$(\delta\theta\delta^{-1})(z') = (\delta\theta\delta^{-1}\delta)(z) = \delta(\theta(z)) = \delta(z) = z',$$

y así $\delta\theta\delta^{-1} \in H'$, con lo cual $\delta H \delta^{-1} \subseteq H'$.

Para mostrar la otra inclusión, sea θ' un elemento arbitrario de H', y sea $z \in E$. Entonces $\delta(z) \in E'$, y se tiene $\theta'(\delta(z)) = \delta(z)$. De donde:

$$(\delta^{-1}\theta'\delta)(z) = (\delta^{-1}\delta)(z) = z,$$

$$\Longrightarrow \quad \delta^{-1}\theta'\delta \in \Gamma(E) = H.$$

$$\Longrightarrow \quad \delta^{-1}H'\delta \subseteq H.$$

$$\therefore \quad H' \subseteq \delta H \delta^{-1}. \blacksquare$$

4.4 El Teorema Fundamental.

TEOREMA 4.28(El Teorema Fundamental de la Teoría de Galois.)

Sea K una extensión normal y separable de un campo F, con grado finito n.

i) Para todos los subcampos E de K que contienen a F, y para todos los subgrupos H de Gal(K/F):

$$\Phi(\Gamma(E)) = E, \quad \Gamma(\Phi(H)) = H.$$

También:

$$|\Gamma(E)| = [K : E], \quad |Gal(K/F)|/|\Gamma(E)| = [E : F].$$

ii) Un subcampo E es una extensión normal de F si y sólo si $\Gamma(E)$ es un subgrupo normal de Gal(K/F). Si E es una extensión normal, entonces Gal(E/F) es isomorfo al grupo cociente Gal$(K/F)/\Gamma(E)$.

Demostración. *i*) Sea E un subcampo de K que contiene a F. Del ejemplo 4.16 sabemos que K es una extensión normal de E. También, por el teorema 4.20, K es una extensión separable de E. De donde, según el corolario 4.23, $|\Gamma(E)| = [K : E]$. Del teorema 2.61 y del corolario 4.23 se sigue que:

$$[E : F] = [K : F]/[K : E] = |Gal(K/F)|/|\Gamma(E)|.$$

Como $\Gamma(E) =$Gal(K/E), por el teorema 4.24, tenemos que:

$$\Phi(\Gamma(E)) = E.$$

Ahora sea H cualquier subgrupo del grupo finito Gal(K/F). Del teorema 4.9 sabemos que:

$$H \subseteq \Gamma(\Phi(H)). \tag{29}$$

Denotemos $\Gamma(\Phi(H))$ por H'. Entonces, por el ejemplo 4.10 se sigue que:

$$\Phi(H) = \Phi(\Gamma(\Phi(H)) = \Phi(H').$$

Del teorema 4.13:

$$|H| = [K : \Phi(H)] = [K : \Phi(H')] = |H'|.$$

Esto, junto con (29) y la finitud de Gal(K/F), nos dice que $H' = H$. Es decir:

$$\Gamma(\Phi(H)) = H.$$

ii) Supongamos ahora que E es una extension normal. Sea $\delta \in$Gal(K/F) y sea δ' la restricción de δ a E. Entonces δ' es un monomorfismo de E en K y así, por el teorema 4.18, es un $F-$automorfismo de E. Como $\delta(E) = \delta'(E) = E$, por el teorema 4.27:

$$\Gamma(E) = \Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}.$$

$$\therefore \quad \Gamma(E) \trianglelefteq Gal(K/F).$$

Para la otra implicación, supongamos que $\Gamma(E) \trianglelefteq$Gal$(K/F)$. Sea δ_1 un $F-$monomorfismo de E en K. Por el corolario 4.14, éste se extiende a un $F-$automorfismo δ de K. La normalidad de $\Gamma(E)$ dentro de Gal(K/F) significa que $\delta\Gamma(E)\delta^{-1} = \Gamma(E)$, y de aquí, por el teorema 4.27:

$$\Gamma(\delta(E)) = \Gamma(E).$$

Como Γ es uno a uno, entonces $\delta(E) = \delta_1(E) = E$. Así δ_1 es un $F-$automorfismo de E. Con esto, hemos mostrado que cada $F-$monomorfismo de E en K es un $F-$automorfismo de E. Del teorema 4.18 se tiene que E es una extensión normal de F.

Falta mostrar que, si E es una extensión normal, entonces Gal$(E/F) \cong$Gal$(K/F)/\Gamma(E)$. Entonces, supongamos que E es normal y, como arriba, sea δ' la restricción a E del $F-$automorfismo δ de K. Ya vimos que $\delta' \in$Gal(E/F). Sea $\Theta :$Gal$(K/F) \longrightarrow$Gal(E/F) dada por:

$$\Theta(\delta) = \delta'.$$

Entonces Θ es un homomorfismo de grupos: para toda $\delta_1, \delta_2 \in \mathrm{Gal}(K/F)$, con $\Theta(\delta_1) = \delta_1'$, y $\Theta(\delta_2) = \delta_2'$, y, para toda $z \in E$:

$$\begin{aligned}([\Theta(\delta_1)][\Theta(\delta_2)])(z) &= (\delta_1'\delta_2')(z) \\ &= \delta_1'(\delta_2(z)) \\ &= \delta_1(\delta_2(z) \\ &= (\delta_1\delta_2)(z) \\ &= (\Theta(\delta_1\delta_2))(z).\end{aligned}$$

$$\implies \quad [\Theta(\delta_1)][\Theta(\delta_2)] = \Theta(\delta_1\delta_2).$$

El núcleo de este homomorfismo es el conjunto de toda δ en $\mathrm{Gal}(K/F)$ tal que δ' es la función identidad sobre E, y no es otro más que $\Gamma(E)$. Ahora el resultado se sigue del teorema de isomorfismo para grupos. ■

CAPÍTULO 5

ECUACIONES Y GRUPOS

5.1 Polinomios Ciclotómicos.

Los campos en este capítulo serán de característica cero.

DEFINICIÓN 5.1 Sea K un campo. Un campo L que contiene a K se llama una ***extensión por radicales***, o una ***extensión radical***, si existe una sucesión:

$$K = L_0, L_1, ..., L_m = L,$$

con la propiedad de que, para $j = 0, 1, ..., m-1,\ L_{j+1} = L_j(\alpha_j)$, donde α_j es una raíz de un polinomio irreducible en $L_j[x]$ de la forma $x^{n_j} - c_j$.

DEFINICIÓN 5.2 Un polinomio $f(x) \in K[x]$ es ***soluble por radicales*** si existe un campo de descomposición para $f(x)$ contenido en una extensión radical de K.

Una solución por radicales involucra polinomios del tipo $x^m - a$, así que empezaremos con polinomios $f(x) = x^m - 1$. Como trabajaremos con campos K de característica cero, podemos asegurar que el campo de descomposición L de $f(x)$ sobre K es tanto normal como separable. Se puede verificar que el conjunto R consistente de las raíces en L de $x^m - 1$ es un subgrupo multiplicativo (abeliano) en L.

LEMA 5.3 $(R, \cdot)$ es un grupo cíclico.

Demostración. Sea $e(R)$ el exponente de R (ver Apéndice A), entonces:

$$a^{e(R)} = e, \quad \forall a \in R.$$

Como $x^{e(R)} - 1$ tiene a lo más $e(R)$ raíces, debemos tener:

$$|R| \leq e(R).$$

Sin embargo, el exponente de un grupo nunca puede exceder al orden del grupo, y así $e(R) \leq |R|$.

$$\therefore \quad e(R) = |R| = m,$$

y por lo tanto, por Corolario A.6, R es cíclico. ■

Sea ω una raíz m-ésima ***primitiva*** de la unidad, es decir, un generador del grupo cíclico R. Entonces:

$$R = \{1, \omega, \omega^2, ..., \omega^{m-1}\},$$

y ω^j es una raíz m-ésima primitiva de la unidad si y sólo si j y m son primos relativos. Sea P_m el conjunto de raíces m-ésimas primitivas de la unidad.

DEFINICIÓN 5.4 El ***polinomio ciclotómico,*** $\Phi_m(x)$, se define por:

$$\Phi_m(x) = \prod_{e \in P_m} (x - e) \tag{5.1}$$

EJEMPLO 5.5 Sea K un campo de característica cero, y sea $L \subset \mathbb{C}$ el campo de descomposición para $x^p - 1$, donde p es primo. Entonces, con la excepción de la raíz 1, todas las raíces de $x^p - 1$ son primitivas y así:

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

EJEMPLO 5.6 Como el polinomio $x^{15} - 1$ tiene factores:

$$\Phi_1(x) = x - 1,$$

$$\Phi_3(x) = x^2 + x + 1,$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

tenemos:

$$x^{15} - 1 = (x-1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)\Phi_{15}(x).$$

Notemos también que:

$$\begin{aligned} x^{15} - 1 &= (x^5)^3 - 1 \\ &= (x^5 - 1)(x^{10} + x^5 + 1) \\ &= (x-1)(x^4 + x^3 + x^2 + x + 1)(x^{10} + x^5 + 1) \end{aligned}$$

Igualando estas dos factorizaciones, deducimos que:

$$\Phi_{15}(x) = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1. \blacksquare$$

LEMA 5.7 Sean K, L campos, con $K \subset L$. Sean $f(x), g(x) \in L[x]$ tales que $f(x), (fg)(x) \in K$. Entonces $g(x) \in K$.

Demostración. Sean:

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m,$$

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n,$$

donde $a_0, a_1, ..., a_m \in K,\ b_0, b_1, ..., b_n \in L,\ a_m \neq 0,\ b_n \neq 0$. Supongamos que:

$$(fg)(x) = c_0 + c_1 x + c_{m+n} x^{m+n} \in K[x].$$

Entonces $b_n = c_{m+n}/a_m \in K$. Supongamos inductivamente que $b_j \in K$ para toda $j > r$. Entonces:

$$c_{m+r} = a_m b_r + a_{m-1} b_{r+1} + \cdots + a_{m-n+r} b_n,$$

donde $a_i = 0$ si $i < 0$. De donde:

$$b_r = (a_{m+r} - a_{m-1} b_{r+1} - \cdots - a_{m-n+r} b_n)/a_m \in K.$$

Se sigue que $b_j \in K$ para toda j, y así $g(x) \in K[x]$. ■

OBSERVACIÓN 5.8 Sea K un campo con característca cero. Entonces los elementos $n1_k, n \in \mathbb{Z}$, donde $n1_k = 1_k + 1_k + \cdots + 1_k$, n sumandos, son todos distintos, y forman un subanillo de K isomorfo a $\mathbb{Z}$. De hecho, el conjunto:

$$P(K) = \{m1_k/n1_k | m, n \in \mathbb{Z},\ n \neq 0\}$$

es un subcampo de K isomorfo a $\mathbb{Q}$. Cualquier subcampo de K debe contener a 1 y a 0 y, por lo tanto, debe contener a $P(K)$, el cual recibe el nombre de ***subcampo primo de*** K**.**

TEOREMA 5.9 Sea K un campo de característica cero, que contiene a las raíces m-ésimas de la unidad para cada m, y sea $K_0(\cong \mathbb{Q})$ el subcampo primo de K. Entonces, para cada divisor d de m (incluyendo m mismo), el polinomio ciclotómico $\Phi_d(x)$ está en $K_0[x]$.

Demostración. Claramente $\Phi_1(x) = x - 1 \in K_0[x]$. Sea $d \neq 1$ un divisor de m, y supongamos por inducción que $\Phi_r(x) \in K_0[x]$ para todo divisor propio r de d. Entonces, si Δ_d es el conjunto de todos los divisores de d, tenemos:

$$x^d - 1 = (\prod_{r \in \Delta_d \setminus \{d\}} \Phi_r(x))\Phi_d(x).$$

Se sigue del lema 5.7 que $\Phi_d \in K_0[x]$. ■

TEOREMA 5.10 Sea K un campo de característica cero, y sea L un campo de descomposición sobre K del polinomio $x^m - 1$. Entonces $\mathrm{Gal}(L/K)$ es isomorfo a R_m, el grupo multiplicativo de clases de residuos $\overline{r}$ (mód m) tal que $(r, m) = 1$.

Demostración. Sea ω una raíz m-ésima primitiva de la unidad en L, y sea $\sigma \in \mathrm{Gal}(L/K)$. Entonces $L = K(\omega)$. Sabemos que $\sigma(\omega)$ también debe ser una raíz m-ésima primitiva de la unidad, y así:

$$\sigma \in Gal(L/K) \iff \sigma(\omega) = \omega^{r_\sigma}, \tag{5.2}$$

donde $(r_\sigma, m) = 1$. Como $\omega^r = \omega^s$ si y sólo si $r \equiv s$ (mód m), tenemos una función inyectiva de $\mathrm{Gal}(L/K)$ sobre R_m, el grupo multiplicativo de clases de residuos $\overline{r}$ módm tal que $(r, m) = 1$.

Sean $\sigma, \tau \in \mathrm{Gal}(L/K)$. Entonces:

$$\begin{aligned}(\sigma\tau)(\omega) &= \sigma(\omega^{r_\tau}) \\ &= (\omega^{r_\tau})^{r_\sigma} \\ &= \omega^{r_\sigma r_\tau} \\ &= (\omega^{r_\sigma})^{r_\tau} \\ &= (\tau\sigma)(\omega)\end{aligned} \tag{5.3}$$

y así $\mathrm{Gal}(L/K)$ es abeliano. La otra consecuencia de (5.3) es que la función $\sigma \to \overline{r}_\sigma$ es un homomorfismo, pues $\sigma\tau$ va a dar a $\overline{r}_\sigma \overline{r}_\tau$. Es claro que la función es inyectiva, y de (5.2) deducimos que también es sobreyectiva. ■

5.2 Extensiones Cíclicas.

Sea K un campo de característica cero, y sea L/K una extensión.

DEFINICIÓN 5.11 Decimos que L es una ***extensión cíclica*** de K si es una extensión normal (y separable) y si $\mathrm{Gal}(L/K)$ es un grupo cíclico.

Sea L una extensión, de grado finito n, de un campo K, con característica cero, y sea N una cerradura normal de L. Por teorema 4.22, hay exactamente n distintos $K-$monomorfismos $\tau_1, \tau_2, ..., \tau_n$ de L en N. Para cada elemento x de L, definimos la ***norma***, $N_{L/K}(x)$, y la ***traza***, $Tr_{L/K}(x)$, por:

$$N_{L/K}(x) = \prod_{i=1}^{n} \tau_i(x), \quad Tr_{L/K}(x) = \sum_{i=1}^{n} \tau_i(x). \tag{5.4}$$

TEOREMA 5.12 La función $N_{L/K}$ es un homomorfismo de grupos de $(L \setminus \{0\}, \cdot)$ en $(K \setminus \{0\}, \cdot)$. La función $Tr_{L/K}$ es un homomorfismo distinto de cero de grupos de $(L, +)$ en $(K, +)$.

Demostración. Es claro que, para toda $x, y \in L \setminus \{0\}$:

$$\begin{aligned} N_{L/K}(xy) &= \prod_{i=1}^{n} \tau_i(xy) = \prod_{i=1}^{n} \tau_i(x)\tau_i(y) \\ &= (\prod_{i=1}^{n} \tau_i(x))(\prod_{i=1}^{n} \tau_i(y)) \\ &= N_{L/K}(x)N_{L/K}(y), \end{aligned}$$

y similarmente:

$$Tr_{L/K}(x + y) = Tr_{L/K}(x) + Tr_{L/K}(y);$$

de este modo, $N_{L/K}$ y $Tr_{L/K}$ son monomorfismos en $(L\setminus\{0\}, \cdot)$ y $(L, +)$, respectivamente. Ahora probemos que las imágenes están contenidas en K.

Sea τ un $K-$automorfismo de L. Entonces:

$$\tau\tau_1, \tau\tau_2, ..., \tau\tau_n, \tag{5.5}$$

son n $K-$monomorfismos distintos de L en N, y, por lo tanto la lista (5.5) es simplemente la lista $\tau_1, \tau_2, ..., \tau_n$ en un orden distinto. De aquí que , para toda x en L y todo τ en $\mathrm{Gal}(L/K)$:

$$\begin{aligned} \tau(N_{L/K}(x)) &= \tau(\prod_{i=1}^{n} \tau_i(x)) = \prod_{i=1}^{n} \tau(\tau_i(x)) \\ &= \prod_{i=1}^{n} \tau_i(x) \qquad \text{(pues la multiplicación es conmutativa)} \\ &= N_{L/K}(x), \end{aligned}$$

y, del mismo modo:

$$\tau(Tr_{L/K}(x)) = Tr_{L/K}(x).$$

Luego, por teorema 4.28, tanto $N_{L/K}(x)$ como $Tr_{L/K}(x)$ están en $\Phi(\mathrm{Gal}(L/K)) = K$.

Ya sólo falta ver que $Tr_{L/K}$ no es el homomorfismo cero. Supongamos, por contradicción, que para toda x en L:

$$Tr_{L/K}(x) = \tau_1(x) + \tau_2(x) + \cdots + \tau_n(x) = 0.$$

Se sigue, entonces, que el conjunto $\{\tau_1, \tau_2, ..., \tau_n\}$ es linealmente dependiente sobre L, y esto contradice el teorema 4.12. ■

TEOREMA 5.13(Hilbert) Sea L una extensión cíclica de un campo K, y sea τ un generador del grupo $\mathrm{Gal}(L/K)$. Si $x \in L$, entonces $N_{L/K}(x) = 1$ si y sólo si existe un elemento $y \in L$ tal que $x = y/\tau(y)$, y $Tr_{L/K}(x) = 0$ si y sólo si existe un elemento $z \in L$ tal que $x = z - \tau(z)$.

Demostración. $\Longleftarrow$) Sea $[L : K] = n$; entonces $\tau^n = \iota$, el automorfismo identidad. Supongamos primero que $x = y/\tau(y)$; entonces:

$$\begin{aligned} N_{L/K}(x) &= \iota(x)\tau(x)\cdots\tau^{n-1}(x) \\ &= \frac{y}{\tau(y)}\frac{\tau(y)}{\tau^2(y)}\frac{\tau^2(y)}{\tau^3(y)}\cdots\frac{\tau^{n-1}(y)}{\tau^n(y)} = 1. \end{aligned}$$

$\Longrightarrow$) Supongamos que $N_{L/K}(x) = 1$. Entonces:

$$x^{-1} = \tau(x)\tau^2(x)\cdots\tau^{n-1}(x). \tag{5.7}$$

Por el teorema 4.12, el conjunto $\{\iota, \tau, \tau^2, ..., \tau^{n-1}\}$ es linealmente independiente sobre L, y así:

$$\iota + x\tau + x\tau(x)\tau^2 + \cdots + x\tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}$$

es distinto de cero; digamos que dicho elemento es, para alguna $t \in L$:

$$y = t + x\tau(t) + x\tau(x)\tau^2(t) + \cdots + x\tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t)$$

y es distinto de cero. Aplicando el automorfismo τ obtenemos:

$$\tau(y) = \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots + \tau(x)\tau^2(x)\tau^3(x)\cdots\tau^{n-1}(x)\tau^n(t). \tag{5.8}$$

Notemos también que:

$$\begin{aligned} x^{-1}y &= x^{-1}t + \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots \\ &\quad + \tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t) \\ &= \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots + \tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t) + x^{-1}\tau^n(t) \end{aligned} \tag{5.9}$$

Comparando (5.8) y (5.9) y usando (5.7) obtenemos $\tau(y) = x^{-1}y$, y así $x = y/\tau(y)$, como queríamos.

De la misma manera se prueba para $Tr_{L/K}$. ■

EJEMPLO 5.14 Sea L una extensión cíclica de un campo K, y sea τ un generador del grupo $\mathrm{Gal}(L/K)$.

i) Demostrar que, para cada $x \in L$, $Tr_{L/K}(x) = 0$ si y sólo si existe un elemento $z \in L$ tal que $x = z - \tau(z)$.
ii) Demostrar que $z - \tau(z) = z' - \tau(z')$ si y sólo si $z - z' \in K$.

Demostración. *i*) $\Longleftarrow$) Si $x = z - \tau(z)$, entonces:

$$\begin{aligned} Tr_{L/K}(x) &= (z - \tau(z)) + (\tau(z) - \tau^2(z)) + \cdots \\ &\quad + (\tau^{n-1}(z) - \tau^n(z)) = z - \tau^n(z) = 0. \end{aligned}$$

$\Longrightarrow$) Supongamos que $Tr_{L/K}(x) = 0$. Entonces:

$$-x = \tau(x) + \tau^2(x) + \cdots + \tau^{n-1}(x).$$

Como en la prueba del teorema 5.13, existe $t \in K$ tal que:

$$\begin{aligned} u &= x\tau(t) + (x + \tau(x))\tau^2(t) + \cdots \\ &\quad + (x + \tau(x) + \tau^2(x) + \cdots + \tau^{n-2}(x))\tau^{n-1}(t) \end{aligned}$$

es distinto de cero. De aquí que:

$$\begin{aligned} \tau(u) &= \tau(x)\tau^2(t) + (\tau(x) + \tau^2(x))\tau^3(t) + \cdots \\ &\quad + (\tau(x) + \tau^2(x) + \tau^3(x) + \cdots + \tau^{n-1}(x))\tau^n(t) \\ &= \tau(x)\tau^2(t) + (\tau(x) + \tau^2(x))\tau^3(t) + \cdots + (-xt), \end{aligned}$$

y:

$$\begin{aligned} u - \tau(u) &= xt + x\tau(t) + (x + \tau(x))\tau^2(t) + (x + \tau(x) + \tau^2(x))\tau^3(t) + \\ &\quad \cdots + (x + \tau(x) + \tau^2(x) + \cdots + \tau^{n-2}(x))\tau^{n-1}(t) \\ &\quad - \tau(x)\tau^2(t) - (\tau(x) + \tau^2(x))\tau^3(t) - \cdots \\ &\quad - (\tau(x) + \tau^2(x) + \tau^3(x) + \cdots + \tau^{n-2}(x))\tau^{n-1}(t) \\ &= x(t + \tau(t) + \tau^2(t) + \cdots + \tau^{n-1}(t)) = xTr_{L/K}(t). \end{aligned}$$

Como $Tr_{L/K}(t) \in K$, por el teorema 5.12, se queda fija por τ. Sea $z = u/Tr_{L/K}(t)$; entonces $z - \tau(z) = (u - \tau(u))/Tr_{L/K}(t) = x$.

ii) $z - \tau(z) = z' - \tau(z') \Leftrightarrow \tau(z - z') = z - z' \Leftrightarrow z - z' \in K$.■

Sea K un campo de característica cero y sea $x^m - a \in K[x]$, $a \neq 0$. Sea L un campo de descomposición para $f(x) = x^m - a$ sobre K. Entonces, por el teorema B.1, $f(x)$ tiene raíces distintas $\alpha_1, \alpha_2, ..., \alpha_m$ en L, y de esta manera, L contiene las raíces distintas:

$$\alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, ..., \alpha_m\alpha_1^{-1} \tag{5.10}$$

del polinomio $x^m - 1$. Supongamos, sin pérdida de generalidad, que $\alpha_2\alpha_1^{-1} = \omega$ es una raíz m-ésima primitiva de la unidad. Entonces, en algún orden, los elementos enlistados en (5.10) son los elementos $1, \omega, ..., \omega^{m-1}$, y así podemos reetiquetar las raíces de $x^m - a$ en L como:

$$\alpha_1, \omega\alpha_1, ..., \omega^{m-1}\alpha_1. \tag{5.11}$$

Así que, sobre L:

$$x^m - a = (x - \alpha_1)(x - \omega\alpha_1)\cdots(x - \omega^{m-1}\alpha_1).$$

Tenemos que $K \subseteq K(\omega) \subseteq L$, y el campo intermedio $K(\omega)$ contiene todas las raíces de la unidad.

Hemos establecido parte del siguiente teorema:

TEOREMA 5.15 Sea $f(x) = x^m - a \in K[x]$, donde K es un campo de característica cero, y sea L un campo de descomposición de $f(x)$ sobre K. Entonces L contiene un elemento ω, una raíz m-ésima primitiva de la unidad. El grupo $\text{Gal}(L/K(\omega))$ es cíclico, con orden d divisor de m. El orden es igual a m si y sólo si $f(x)$ es irreducible sobre $K(\omega)$.

Demostración. Hemos visto que, si α es una raíz de $f(x)$, entonces, sobre L:

$$f(x) = (x - \alpha)(x - \omega\alpha)\cdots(x - \omega^{m-1}\alpha),$$

donde ω es una raíz m-ésima primitiva de la unidad. Así $L = K(\omega, \alpha)$, y un automorfismo $\sigma \in \text{Gal}(L/K(\omega))$ está determinado por su acción sobre α. La imagen debe ser una raíz de $f(x)$, y, por lo tanto:

$$\sigma(\alpha) = \omega^{r_\sigma}\alpha$$

para algún r_σ en $\{0, 1, .., m-1\}$. Si τ es otro elemento en $\text{Gal}(L/K(\omega))$, entonces:

$$(\sigma\tau)(\alpha) = \sigma(\omega^{r_\tau}\alpha) = \omega^{r_\tau}\omega^{r_\sigma}\alpha = \omega^{r_\tau + r_\sigma}\alpha,$$

y así $\sigma \mapsto \overline{r}_\sigma$ es un homomorfismo sobre el grupo aditivo $\mathbb{Z}_m$ de enteros módulo m. Además $\overline{r}_\sigma = \overline{0}$ si y sólo si m divide a r_σ, esto es, si y sólo si $\sigma(\alpha) = \alpha$. El núcleo del homomorfismo $\sigma \mapsto \overline{r}_\sigma$ es la identidad en $\text{Gal}(L/K(\omega))$, y entonces $\text{Gal}(L/K(\omega))$ es isomorfo a un subgrupo del grupo aditivo $\mathbb{Z}_m$. De los ejemplos A.7 y A.8, deducimos que el grupo es cíclico.

Supongamos ahora que $f(x) = x^m - a$ es irreducible sobre $K(\omega)$. Entonces, por Corolario 4.23 y Teorema 3.38:

$$|Gal(L/K(\omega))| = [L : K(\omega)] = \text{gdo}(f(x)) = m,$$

y así $\text{Gal}(L/K(\omega)) \cong \mathbb{Z}_m$. Por otro lado, si $f(x)$ no es irreducible sobre $K(\omega)$, entonces tiene un factor propio mónico irreducible $g(x)$ tal que $\text{gdo}(g(x)) < m$. Si ρ es una raíz de $g(x)$ en L, entonces:

$$x^m - a = (x - \rho)(x - \omega\rho)\cdots(x - \omega^{m-1}\rho),$$

y con esto $L = K(\omega, \rho)$ es un campo de descomposición para $f(x)$ sobre $K(\omega)$. Luego:

$$|Gal(L/K(\omega))| = [L : K(\omega)] = \text{gdo}(g(x)) < m,$$

$$\therefore \text{ Gal}(L/K(\omega)) \text{ es isomorfo a un subgrupo propio de } \mathbb{Z}_m. \blacksquare$$

TEOREMA 5.16 Sea K un campo de característica cero, sea m un entero positivo, y supongamos que $x^m - 1$ se descompone completamente sobre K. Sea L una extensión cíclica de K tal que $[L : K] = m$. Entonces existe $a \in K$ tal que $x^m - a$ es irreduclible sobre K y L es un campo de descomposición para $x^m - a$. Además, L se genera sobre K por una sola raíz de $x^m - a$.

Demostración. Aquí (en la notación del teorema 5.15) $K(\omega) = K$. Sea τ un generador del grupo $G =$Gal(L/K). Ciertamente, cada raíz m-ésima de la unidad queda fija por todo automorfismo de G. De donde $N_{L/K}(\omega) = \omega^m = 1$. Del teorema 5.13 deducimos que existe un elemento z en L tal que $\omega = z/\tau(z)$. Entonces:

$$\tau(z) = \omega^{-1}z, \tag{5.12}$$

y se sigue fácilmente que:

$$\tau^k(z) = \omega^{-k}z \neq z, \ k = 1, 2, ..., m-1. \tag{5.13}$$

Así:

$$\Gamma[K(z)] = \{\iota\},$$

y, entonces, como L es una extensión cíclica, (y, en consecuencia, por definición, normal) podemos aplicar el Teorema Fundamental (teorema 4.28) para obtener:

$$K(z) = \Phi(\Gamma[K(z)]) = \Phi(\{\iota\}) = L.$$

De (5.12) concluimos que

$$\tau(z^m) = [\tau(z)]^m = \omega^{-m}z^m = z^m,$$

y se sigue que:

$$\tau^k(z^m) = z^m \text{ para } k = 0, 1, ..., m-1.$$

Luego $z^m \in \Phi(G) = K$. Denotemos por a a z^m. Entonces z es una raíz del polinomio $x^m - a$ en $K[x]$, y en consecuencia el polinomio mínimo $g(x)$ de z sobre K es un factor de $x^m - a$. Como:

$$[K(z) : K] = [L : K] = m,$$

el polinomio mínimo $g(x)$ debe ser $x^m - a$. De este modo $x^m - a$ es irreducible sobre K. Más aún, las raíces de $x^m - a$ son los elementos:

$$\omega^{-k}z, \quad k = 0, 1, ..., m-1,$$

todas pertenecientes a L, de aquí que L es un campo de descomposición para $x^m - a$ sobre K. ■

TEOREMA 5.17 (Abel) Sea K un campo de característica cero, sea p primo, y sea $a \in K$. Si $x^p - a$ es reducible sobre K, entonces tiene un factor lineal $x - c$ en $K[x]$.

Demostración. Supongamos que $f(x) = x^p - a$ es reducible sobre K, y sea $g(x)(\in K[x])$ un factor mónico irreducible de $f(x)$ de grado d. Si $d = 1$, no tenemos nada que probar; supongamos, pues, que $1 < d < p$. Sea L un campo de descomposición para $f(x)$ sobre K, y sea β una raíz de $f(x)$ en L. Entonces $g(x)$ se factoriza en $L[x]$ como:

$$g(x) = (x - \omega^{n_1}\beta)(x - \omega^{n_2}\beta)\cdots(x - \omega^{n_d}\beta), \tag{5.14}$$

donde ω es una raíz p-ésima primitiva de la unidad y $0 \leq n_1 < n_2 < ..., n_d < p$.

Supongamos que:

$$g(x) = x^d - b_{d-1}x^{d-1} + \cdots + (-1)^d b_0; \tag{5.15}$$

entonces, comparando (5.14) y (5.15), vemos que:

$$b_0 = \omega^{n_1+n_2+\cdots+n_d}\beta^d = \omega^n\beta^d. \text{ (digamos)}$$

De donde, como $\beta^p = a$:

$$b_0^p = \omega^{n_p}\beta^{dp} = \beta^{dp} = a^d.$$

Como p es primo, d y p tienen máximo común divisor 1, y así existen, entonces, s y t tales que:

$$sd + tp = 1.$$

Luego:

$$a = a^{sd}a^{tp} = b_0^{sp}a^{tp} = (b_0^s a^t)^p.$$

$$\therefore \quad x - c \text{ es un factor lineal de } f(x),$$

donde $c = b_0^s a^t \in K$.■

EJEMPLO 5.18 Sea ω una raíz sexta primitiva de la unidad. Mostrar que $x^6 - 3$ no es irreducible sobre $\mathbb{Q}(\omega)$. Describir el grupo de Galois de $x^6 - 3$ sobre $\mathbb{Q}$.

Solución. Las raíces sextas de la unidad son:

$$1, -1, e^{\pm\pi i/3} = 1/2(1 \pm i\sqrt{3}), e^{\pm 2\pi i/3} = 1/2(-1 \pm i\sqrt{3}),$$

y así, escribiendo $e^{\pi i/3}$ como ω, deducimos que:

$$\mathbb{Q}(\omega) = \mathbb{Q}(i\sqrt{3}).$$

Las raíces primitivas de la ecuación son ω y $\omega^5 = \overline{\omega}$. Es claro que, sobre $\mathbb{Q}(i\sqrt{3})$, el polinomio $x^6 + 3$ se descompone completamente como:

$$(x^3 + i\sqrt{3})(x^3 - i\sqrt{3}).$$

Pero supongamos que $x^3 - i\sqrt{3}$ no es irreducible sobre $\mathbb{Q}(i\sqrt{3})$. Entonces tiene un factor lineal, y así existe $a + bi\sqrt{3}$, con $a, b \in \mathbb{Q}$, tal que:

$$i\sqrt{3} = (a + bi\sqrt{3})^3 = a^3 + 3a^2bi\sqrt{3} - 9ab^2 - 3b^3i\sqrt{3}.$$

$$\Longrightarrow \quad a^3 - 9ab^2 = 0, \quad 3a^2b - 3b^2 = 1.$$

Si $a = 0$, entonces $-3b^2 = 1$, lo cual no es posible para un racional b. De lo contrario, $a^2 - 9b^2 = 0$, y así $a = \pm 3b$. Entonces:

$$27b^2 - 3b^2 = 1,$$

y de nuevo esto no es posible para un racional b.

Las raíces de $x^3 - i\sqrt{3}$ son:

$$r, r\omega^2, r\omega^4.$$

El grupo de Galois consiste en los elementos $\sigma_{s,t}$, donde $s \in \{0, 2, 4\}$ y $t \in \{1, -1\}$, definidos por:

$$\sigma_{s,t}(r) = r\omega^s, \quad \sigma_{s,t}(\omega) = \omega^t.$$

Entonces:

$$\begin{aligned}\sigma_{s,t}\sigma_{u,v}(r) &= \sigma_{s,t}(r\omega^4)\\ &= r\omega^s\omega^{tu} = r\omega^{s+tu},\end{aligned}$$

y:

$$\sigma_{s,t}\sigma_{u,v}(\omega) = \sigma_{s,t}(\omega^v) = \omega^{tv},$$

y así, módulo 6:

$$\sigma_{s,t}\sigma_{u,v} = \sigma_{s+tu,tv}.$$

Notemos que:

$$(\sigma_{2,1})^2 = \sigma_{4,1}, \quad (\sigma_{2,1})^3 = 1, \quad (\sigma_{0,-1})^2 = 1.$$

Notemos también que:

$$\sigma_{2,1}\sigma_{0,-1} = \sigma_{2,-1}, \quad \sigma_{0,-1}\sigma_{2,1} = \sigma_{4,-1} = \sigma_{4,1}\sigma_{0,-1}.$$

Escribiendo $\sigma_{2,1}$ como β y $\sigma_{0,-1}$ como α, obtenemos:

$$\alpha^2 = \beta^3 = 1, \quad \alpha\beta = \beta^2\alpha = \beta^{-1}\alpha.$$

El grupo así obtenido tiene 6 elementos, y suele representarse como:

$$\langle \alpha\beta | \alpha^2 = \beta^3 = \alpha\beta\alpha^{-1}\beta = 1 \rangle. \blacksquare$$

APÉNDICE

A. Grupos.

DEFINICIÓN A.1 Un grupo G se llama ***cíclico*** si existe un elemento $a \in G$ tal que:

$$G = \{a^n | n \in \mathbb{Z}\}.$$

Si las potencias a^n son todas distintas, G es el ***grupo cíclico infinito.*** Si no, entonces existe el menor $m > 0$ tal que $a^m = e$.

Observación A.2 En el último caso, el algoritmo de la división (para enteros) implica entonces que, para toda $n \in \mathbb{Z}$, existen enteros q, r tales que:

$$a^n = a^{qm+r} = (a^m)^{qr} a = a^r, \quad 0 \leq r \leq m-1.$$

Es decir, G consta de las potencias de $a : e, a, a^2, ..., a^{m-1}$, el ***grupo cíclico de orden m***. Tanto el grupo cíclico infinito como el grupo cíclico de orden m son abelianos.

Observación A.3 Dado G un grupo, para cada elemento $a \in G$, el conjunto:

$$\{a^n | n \in \mathbb{Z}\}$$

es un subgrupo, llamado el ***subgrupo cíclico generado por a***, y denotado por $\langle a \rangle$.

Sea G un grupo finito:

DEFINICIÓN A.4 El ***exponente de*** G es el menor entero positivo, $e(G)$, con la propiedad de que:

$$a^{e(G)} = e,$$

la identidad en G, para toda $a \in G$. El exponente siempre existe en un grupo finito: es el mínimo común múltiplo de los órdenes de los elementos de G. Como $o(a)||G|$ para cada a, podemos deducir que $e(G)||G|$.

TEOREMA A.5 Sea G un grupo abeliano finito con exponente $e(G)$. Entonces existe un elemento $a \in G$ tal que $o(a) = e(G)$.

Demostración. Supongamos que:

$$e(G) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

donde $p_1, p_2, ..., p_k$ son primos distintos y $\alpha_1, \alpha_2, ..., \alpha_k \geq 1$. Como $e(G)$ es el mínimo común múltiplo de los órdenes de los elementos de G, debe existir un elemento h_1 cuyo orden es divisible por $p_1^{\alpha_1}$, así:

$$o(h_1) = p_1^{\alpha_1} q_1, \text{ donde } q_1 | p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Sea $g_1 = h_1^{q_1}$. Entonces, para toda $m \geq 1$, tenemos:

$$g_1^m = h_1^{mq_1},$$

y esto es igual a e si y sólo si $p_1^{\alpha_1} q_1 | mq_1$, esto es, si y sólo si:

$$p_1^{\alpha_1} | m.$$

$$\therefore \quad o(g_1) = p_1^{\alpha_1}.$$

Similarmente, para $i = 2, .., k$, podemos encontrar un elemento g_i de orden $p_i^{\alpha_i}$. Sea :

$$a = g_1 g_2 \cdots g_k,$$

y sea $n = o(a)$. Entonces:

$$a^n = g_1^n g_2^n \cdots g_k^n = 1,$$

(aquí es donde estamos usando la propiedad abeliana) y, por lo tanto:

$$g_1^n = g_2^{-n} \cdots g_k^{-n}.$$

Sea $r = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Entonces, como $g_i^{-nr} = 1$ para $i = 2, ..., k$, se sigue que $g_1^{nr} = 1$. Luego:

$$p_1^{\alpha_1} | nr,$$

y de aquí que, como p_1 y r son primos relativos:

$$p_1^{\alpha_1} | n.$$

Del mismo modo, $p_i^{\alpha_i} | n$ para $i = 2, .., k$, y deducimos que $e(G)|n$. Como, de la definición de exponente, también tenemos $n|e(G)$, concluimos que:

$$o(a) = e(G). \blacksquare$$

COROLARIO A.6 Si G es un grupo abeliano finito tal que $e(G) = |G|$, entonces G es cíclico. ■

EJEMPLO A.7 Como el grupo $(\mathbb{Z}_n, +)$ consiste de los elementos $1, 1+1, 1+1+1, ...$, entonces, para cada $n \geq 2$, es cíclico, generado por 1.

EJEMPLO A.8 Cualquier subgrupo de un grupo cíclico es cíclico.

Pues si $G = \langle a \rangle$ y H cualquier subgrupo propio de G, entonces $a \notin H$, y existe el entero positivo más pequeño m con la propiedad de que $a^m \in H$. Si $a^n \in H$, entonces $m|n$, pero n se puede escribir como:

$$qm + r, \quad 0 \leq r \leq m - 1,$$

y:

$$a^r = a^n (a^m)^{-q} \in H,$$

así, como m es mínimo, se sigue que $r = 0$.

$\therefore$ H es cíclico, generado por a^m. ■

B. Campos.

TEOREMA B.1 Sea $f(x)$ un polinomio irreducible con coeficientes en un campo K.

i) Si K tiene caracterísitica cero, entonces $f(x)$ es separable sobre K.
ii) Si K tiene característica finita p, entonces $f(x)$ es separable en caso de que sea de la forma:

$$b_0 + b_1x^p + b_2x^{2p} + \cdots + b_mx^{mp}.$$

Demostración. Sea:

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

con gdo$(f(x)) = n \geq 1$, y supongamos que $f(x)$ no es separable. Entonces $f(x)$ y $D_xf(x)$ tienen un factor común d de grado al menos 1. Como $f(x)$ es irreducible, el factor d debe ser un múltiplo constante (un asociado) de $f(x)$ y éste sólo puede dividir a $D_xf(x)$ cuando:

$$D_xf(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

es el polinomio cero. De donde:

$$a_1 = 2a_2 = \cdots = na_n = 0.$$

Si K tiene característica cero, esto implica que $f(x)$ es el polinomio constante a_0 y tenemos una contradicción.

$\therefore$ $f(x)$ debe ser separable.

Supongamos ahora que la característica de K es p. Entonces:

$$ra_r = 0$$

implica que $a_r = 0$ si y sólo si $p \nmid r$. De donde los únicos términos no cero en $f(x)$ son de la forma:

$$a_{kp}x^{kp},$$

para $k = 0, 1, 2, ...$ Escribiendo a_{kp} como b_k obtenemos la conclusión. ■

DEFINICIÓN B.2 Sean D, D' dominios enteros, y sea $\varphi : D \to D'$ un isomorfismo. La ***extensión canónica de*** φ es el isomorfismo $\widehat{\varphi} : D[x] \to D'[x]$ definido por:

$$\widehat{\varphi}(a_0 + a_1x + \cdots + a_nx^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

BIBLIOGRAFÍA.

[1] Herstein, I. N., *Álgebra Moderna*, Trillas, 1990.
[2] Dummit, David and Foote, Richard, *Abstract Algebra*, John Wiley and Sons, Inc., 2004.
[3] Moore, J. T., *Introduction to Abstract Algebra*, Academic Press, 1975.
[4] Hungerford, T. W., *Algebra*, Nueva York, Holt, Rinehart and Winston, 1974.