UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

ALGUNOS ASPECTOS DE LA TEORÍA DE GALOIS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A :

SEBASTIÁN PARDO GUERRA

DIRECTOR DE TESIS:
DR. HUGO ALBERTO RINCÓN MEJÍA

2010

Índice general

0.1. Dedicatorias

Dedico este trabajo a todas las personas que han sido parte de mi vida antes y durante la carrera de matemáticas, así como en el tiempo que me he tardado escribiéndola. En especial, quiero primero agradecer a mis padres por haberme brindado una educación, desde el haberme llevado a la primaria, a pesar de mis quejas, hasta los principios morales que hoy día me definen. Muchas gracias por su apoyo y por sus recomendaciones, por su cariño y por ser parte de mi vida. Junto con ellos, dedico a mis dos hermanos este trabajo que, si no fuera por sus interminables bromas, no lo hubiera acabado. Gracias Gaby por tu apoyo y por las pláticas que tuvimos. A mis tíos, la Nena y Carlos que fueron parte de charlas y motivaciones.

En segundo lugar, agradesco a mi director de tesis Hugo, que me tuvo mucha calma y pasiencia para explicarme y guiarme durante este trabajo, pero sobre todo, por ayudarme a fomentar ese gusto por las matemáticas. También agradesco a mis sinodales, en especial a Ernesto y Violeta que con sus comentarios, han ayudado mucho a la corrección de este trabajo. No por último menos importante, agradesco a todos mis amigos y amigas, en especial a Daniel, Pedro, Pablo y Victor, que hemos crecido desde pequeños; a Mariana, Antonieta, Prisila, Laura, y Dalia, que soporaban mis quejas y mi desesperación, y que al mismo tiempo ayudaban a darme un nuevo empujón; a mis compañeros y compañeras de la Facultad de Ciencias que fueron parte de mi transcurso y proceso de matemático e individuo; y a todos los profesores que fueron parte de mi educación durante la Facultad. También agradesco a mi maestra Nancy que fue mi primer motivo para estudiar matemáticas.

Y bueno, la verdad es que también se la dedico a mi perro.

0.2. Introducción

En este trabajo se desarrollan las teorías de grupos y anillos, necesarias para la construcción de la teoría de Galois. Ésta consta del grupo de automorfismos de un campo que dejan invariante a un subcampo, y que bajo ciertas hipótesis, se tiene una biyección entre subcampos y subgrupos del grupo de automorfismos.

La teoría de Galois es una muestra de unificación de las matemáticas en diferentes ramas. Algunas de sus aplicaciones se dan en el estudio de problemas históricos y de gran importancia matemática. Tal es el caso de la cuadratura del círculo, la trisección de ángulos, la construcción de polígonos regulares y la imposibilidad de resolver la ecuación de quinto grado. Nosotros sólo veremos que la ecuación general de un polinomio no es soluble por radicales cuando éste tiene grado mayor o igual que cinco.

Además, la teoría de Galois es el inicio del álgebra moderna, pasando de construir teoremas para casos particulares a teorías más abstractas y amplias, dejando lo particular por lo general.

Por otra parte, en el capítulo de extensiones de campo, veremos la existencia de extensiones de campo que son algebráicamente cerrados, es decir, que con-

tienen una raíz para cualquier polinomio con coeficientes en dicho campo. Para esto, utilizaremos el Lema de Zorn, herramienta muy usada para demostraciones de existencia.

Finalizaremos este trabajo con el tema de campos real cerrados, que nos llevará a demostrar el teorema fundamental del álgebra, el cual menciona que el campo de los complejos es algebráicamente cerrado.

0.3. Biografía

Évariste Galois nació en Bourg la Reine, cerca de Paris, el 25 de Octubre de 1811. Su padre, Nicolas Gabriel Galois, era republicano y estaba encargado del partido liberal del pueblo. Su madre, Adelaide Marie, hija de un juez de la corte francesa, era experta en Latín y en la literatura clásica, debido a su sólida educación. Los primeros doce años de vida, Galois fue educado por su madre, quien lo encaminó hacia la literatura clásica.

En 1823 entró a la preparatoria, donde su gusto por las matemáticas se desarrollo hasta su segundo año escolar. A la edad de 15 años, se encontraba ya leyendo textos para matemáticos profesionales. A pesar de su temprano desarrollo mental para las matemáticas, su dedicación a éstas era de un tipo informal, guardándose todo en la mente o escribiéndolo en manuscritos de manera desordenada. Intentó entrar a la École Polytechnique, cuna de los grandes matemáticos franceses en su tiempo, pero le negaron la entrada.

En 1828, Galois tomó un curso en matemáticas avanzadas, impartido por Louis Paul Émile Richard, quien simpatizó con el y reconoció su gran habilidad. Su primer trabajo de investigación trató acerca de fracciones continuas. Mientras tanto, Galois había hecho descubrimientos fundamentales en la teoría de ecuaciones de polinomios, información que presentó a la Academia de Ciencias, cuyo juez en ese momento era Augustin Louis Cauchy.

Muchas fuentes mencionan que Cauchy perdió el manuscrito, o que hasta lo tiró a la basura. Otras afirman que Cauchy nunca dejó de tener el manuscrito. Al parecer, Cauchy se impresionó por el trabajo de Galois, por lo que le recomendó al joven preparar una nueva versión y presentarla para el Gran Premio de Matemáticas, que tenía fecha límite el 1ro de Marzo. Para febrero de 1830, Galois presentó su nueva versión a la Academia de Ciencias para la competencia del Gran Premio de Matemáticas. Este manuscrito fue recibido por Joseph Fourier, quien murió antes de leerlo, perdiéndose el documento entre sus papeles. Galois estaba convencido de que las repetidas pérdidas de sus trabajos no eran sólo mala suerte. Esto le cambió la mentalidad, viendo un inevitale efecto en la sociedad donde a los genios se les condenaba a un estado eterno de mediocridad, culpando así al régimen político opresivo Borbón.

Volvió a intentar ingresar a la Polytechnique, donde de nuevo fue rechazado. Aún así, terminó sus estudios en la École Normale con grado de licenciado en Ciencias y en letras en 1829.

En Enero de 1831, hizo un tercer intento de mandar sus resultados a la Academia; Çondiciones de Solubilidad de Ecuaciones por Radicales". Tras no recibir

respuesta, dos meses después mandó una carta al presidente de la Academia preguntando qué había pasado con su reporte. No obtuvo respuesta, hasta el 4 de Julio, donde el jurado lo dictaminó como "incomprensible". A partir de ahí, el comportamiento de Galois empezó a hacerse más extremo, llegando a los límites de la paranoia. El 14 de Julio, día de la Bastilla, Galois y su amigo Ernest Duch$\hat{a}$telet fueron aprisionados por cargar armas de fuego y usar el uniforme de la Artillería. Galois fue pasado a un hospital en 1832 por la epidemia de cólera, saliendo prontamente con libertad condicional. Durante su libertad, tuvo un amorío con la joven Mlle. Stéphanie D., hija del médico Jean Louis Auguste Poterin du Motel.

Después de que su amorío con la joven Stéphanie acabara, el joven Galois fue retado a duelo por los avances que tenía por la ésta mujer. El 29 de Mayo, en vísperas del duelo, escribió una carta a su amigo Auguste Chevalier, en donde hace un bosquejo de la conección entre grupos y ecuaciones de polinomios, afirmando que una ecuación es soluble por radicales si su grupo era soluble. Además, menciona ideas acerca de funciones elípticas y la integración de funciones algebráicas.

Galois murió el 31 de Mayo de peritonitis a causa de la herida de bala en el estomago por el duelo del día anterior. La muerte de Évariste Galois sigue siendo un misterio ya que se piensa que el duelo estuvo arreglado, pues cuando se anunció su muerte en la presna local, se narra que sólo una de las pistolas estaba cargada.

Parte I

Grupos

Empezaremos por la siguiente

Definición 1 *Un monoide M es una terna $(M, \bullet, e)$ tal que M es un conjunto no vacío, $\bullet$ es una operación binaria asociativa y e un elemento distinguido, que llamaremos neutro para la operación $\bullet$, tal que $a \bullet e = a = e \bullet a, \forall a \in M$.*

Al decir que $\bullet$ es una operación binaria asociativa nos referimos a que $(a \bullet b) \bullet c = a \bullet (b \bullet c), \forall a, b, c \in M$. Afirmamos que este neutro es único. Supongamos que $e' \in M$ es tal que $a \bullet e' = a = e' \bullet a, \forall a \in M$. Entonces, en particular, $e = e' \bullet e = e'$. Por lo tanto, e es único.

Ejemplos 1 *1.* $(\mathbb{N}, +, 0)$ *es un monoide, ya que la suma es binaria y asociativa y además, se tiene que* $a + 0 = a = 0 + a, \forall a \in \mathbb{N}$.

2. $(\mathbb{Z}, \cdot, 1)$ *es un monoide, ya que para cualesquiera* $x, y, z \in \mathbb{Z}$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *y* $x \cdot 1 = x = 1 \cdot x$.

3. Sea S un conjunto no vacío. Sea $\wp(S)$ el conjunto potencia de S. Sea $(\wp(s), \cup, \varnothing)$. Como $S \neq \varnothing$, entonces $\wp(S) \neq \varnothing$. Sabemos que $(A \cup B) \cup C = A \cup (B \cup C)$ para cualesquiera conjuntos A, B, C, por lo que la unión es una operación binaria y asociativa. Además, $\varnothing \in \wp(S)$ y es tal que $A \cup \varnothing = A = \varnothing \cup A$, por lo que $(\wp(S), \cup, \varnothing)$ es un monoide.

Definición 2 *Un grupo G es un monoide $(G, \bullet, e)$ tal que $\forall g \in G$ existe $h \in G$ tal que $g \bullet h = e = h \bullet g$.*

Veamos que de la definición anterior, se sigue que el inverso es único. Si k es un elemento en G tal que $g \bullet k = e = k \bullet g$, entonces $k = k \bullet e = k \bullet (g \bullet h) = (k \bullet g) \bullet h = e \bullet h = h$. En lo que sigue del texto, nos referiremos al inverso de $a \in G$ por $b := a^{-1}$, y a $a \bullet b$ simplemente por ab.

Más adelante, se demostrará que cualquier monoide (grupo) es isomorfo a un monoide (grupo) de transformaciones. Para esto, debemos definir lo que es un isomorfismo entre monoides o grupos.

Definición 3 *Una función $\eta : M \longrightarrow M'$ es un morfismo entre los monoides $(M, \bullet, e)$ y $(M', \bullet', e')$ si $\forall a, b \in M$, $\eta(ab) = \eta(a)\ \eta(b)$,.*

Cuando η es una biyección, decimos que M es isomorfo a M' y lo denotaremos como $M \cong M'$. Notemos también que, si η es un morfismo entre grupos, entonces $\eta(e) = e'$, es decir, manda el neutro de G al neutro de G'. Esto se sigue viendo que

$$e'\eta(e) = \eta(e) = \eta(ee) = \eta(e)\eta(e)$$

Como podemos cancelar por el lado derecho, se tiene que $e' = \eta(e)$, por lo que η manda neutros en neutros.

Cuando un morfismo f es inyectivo se le llama *monomorfismo* y si es suprayectivo lleva el nombre de *epimorfismo*.

Sea $(M, \bullet, e)$ un monoide y $a \in M$. Definimos la función $\eta_a : M \longrightarrow M$ por $\eta_a(x) = ax, \forall x \in M$, es decir, la función multiplicar por a por la izquierda. Definamos ahora al conjunto $M_\eta := \{\eta_a \mid a \in M\}$. Claramente $M_\eta \neq \varnothing$. Ahora,

si $\eta_a, \eta_b \in M_\eta$, podemos definir la función $\bullet : M_\eta \times M_\eta \longrightarrow M_\eta$ por $\eta_a \bullet \eta_b = \eta_{ab}$. De esta manera, se tiene que

$$\eta_a \bullet (\eta_b \bullet \eta_c) = \eta_a \bullet (\eta_{bc}) = \eta_{a(bc)} = \eta_{(ab)c} = \eta_{ab} \bullet \eta_c = (\eta_a \bullet \eta_b) \bullet \eta_c$$

es decir, $\bullet$ es una operación binaria asociativa. Además, $\forall \eta_a \in M_\eta$ se tiene que

$$\eta_a \bullet \eta_e = \eta_{ae} = \eta_a = \eta_{ea} = \eta_e \bullet \eta_a$$

por lo que η_e es el neutro multiplicativo de $\bullet$ en M_η. Por lo tanto, $(M_\eta, \bullet, \eta_e)$ es un monoide de transformaciones.

Notemos ahora que la función $\zeta : M \longrightarrow M_\eta$ con regla de correspondencia $a \longmapsto \eta_a$ es un isomorfismo. Es un morfismo ya que $\zeta(ab) = \eta_{ab} = \eta_a \eta_b = \zeta(a)\zeta(b)$. Por otra parte, para cualquier $\nu \in M_\eta$, se tiene que $\nu = \eta_a$, para alguna $a \in M$, es decir, $\nu(x) = ax$. Por lo tanto, $\zeta(a) = ax = v$, por lo que ζ es sobre. Ahora, si $\zeta(a) = \zeta(b)$, con $a, b \in M$, entonces $\eta_a = \eta_b$, es decir, $ax = bx$ para cualquier valor de $x \in M$. En particular, si $x = e$, se tiene que $a = ae = be = b$, por lo que ζ es inyectiva. Por lo tanto ζ es un isomorfismo y así $M \cong M_\eta$.

Sea $(G, \bullet, e)$ un grupo. Consideremos ahora las transformaciones definidas por la multiplicación en el grupo, es decir, a cada $g \in G$ le asociamos la transformación multiplicar por la izquierda $\mu_g := gx$. Esto nos induce una función $\mu : G \longrightarrow G_g$ donde $G_g = \{\mu_g \mid g \in G\}$, con regla de correspondencia $g \longmapsto \mu_g$. De manera análoga, $(G_g, \bullet, \mu_e)$ forma un monoide y se tiene que μ es un isomorfismo. Más aun, éste forma un grupo: si $\mu_g \in G_g$, entonces $g \in G$. Como G es grupo, $g^{-1} \in G$, por lo que $\nu := \mu_{g^{-1}}$ cumple que

$$\mu_g \bullet \nu = \mu_g \bullet \mu_{g^{-1}} = \mu_{gg^{-1}} = \mu_e = \mu_{g^{-1}g} = \mu_{g^{-1}} \bullet \mu_g = \nu \bullet \mu_g$$

es decir, $\nu = \left(\mu_g\right)^{-1}$. Por lo tanto, cada elemento en G_g tiene inverso, por lo que G_g es un grupo. De esta manera, hemos probado el siguiente

Teorema 1 *(Teorema de Cayley para monoides y grupos) Cualquier monoide (grupo) es isomorfo a un monoide (grupo) de transformaciones.*

En particular, si $|G| = n$, G es un subgrupo de S_n, el grupo simétrico del conjunto con n elementos. De esto último se tiene el siguiente

Corolario 1 *Cualquier grupo finito de orden n es isomorfo a un subgrupo del grupo simétrico S_n.*

0.4. Subgrupos generados por un conjunto

Dado un subconjunto S de un grupo G, nos preguntamos por el menor subgrupo de G que contenga a S. Lo que queremos es encontrar un subgrupo H de G que contenga a S y que además $H \subset K$, para cualquier subgrupo K tal que contenga a S. Por otro lado, si tal subgrupo existe, entonces es único.

Esto es claro ya que si H y H' son dos subgrupos de G tales que cumplen las condiciones anteriores entonces $H \subset H'$ y también $H' \subset H$, por lo que $H = H'$. Al subgrupo H lo denotaremos con $\langle S \rangle$. La existencia de $\langle S \rangle$ se establece de la siguiente manera:

Sea $\{G_S\}$ la familia de subgrupos de G tales que contienen a S. Este conjunto es distinto del vacío pues $G \in \{G_S\}$. Definimos ahora $\langle S \rangle = \cap\{G_S\}$. Afirmamos que $\langle S \rangle$ es un subgrupo;

1) como el neutro e está en cada subgrupo de G_S, entonces $e \in \langle S \rangle$,

2) si $a \in \langle S \rangle$, entonces $a \in \cap\{G_S\}$, por lo que está en cada subgrupo de G que contiene a S. Como estos son subgrupos, entonces también $a^{-1} \in \cap\{G_S\} = \langle S \rangle$, por lo que $\langle S \rangle$ es un subgrupo de G.

Por otra parte, si N es cualquier otro subgrupo de G que contiene a S entonces $N \in \{G_S\}$, por lo que $\langle S \rangle \subset N$. En el caso de que S sea un conjunto finito, $S = \{s_1, \ldots, s_n\}$, se tiene que $\langle S \rangle = \langle s_1, \ldots, s_n \rangle$. Un caso especial es cuando $G = \langle S \rangle$, para algún subconjunto S de G, donde decimos que G está generado por el conjunto S. Notemos que si $G = \langle S \rangle$, con $S = \{s_1, \ldots, s_n\}$, entonces

$$G = \left\{ s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} \mid s_i \in S, n \in \mathbb{N}, k_i \in \mathbb{Z} \right\}$$

ya que $\langle S \rangle$ tiene la forma de productos de potencias de los s_i. Cuando G es un grupo abeliano, es decir, que la operación es conmutativa, $\langle S \rangle$ tiene la fomra $\{k_1 s_1 + k_2 s_2 + \cdots + k_n s_n \mid s_i \in S, n \in \mathbb{N}, k_i \in \mathbb{Z}\}$.

Consideremos ahora el grupo más sencillo, esto es, que tenga sólo un generador. En este caso, $G = \langle a \rangle$ para alguna $a \in G$. A G lo llamaremos *el grupo cíclico con generador* a. Un ejemplo de grupo cíclico es el grupo aditivo de enteros $(\mathbb{Z}, +, 0)$ con generador 1, o -1. Por otra parte, se tiene una función $f : \mathbb{Z} \longrightarrow \langle a \rangle$ definida por $n \longmapsto a^n$. Como $\langle a \rangle = \{a^k\}_{k \in \mathbb{Z}}$ entonces esta función es claramente suprayectiva. Además, se cumple que $m + n \longmapsto a^{m+n} = a^m a^n$ y $0 \longmapsto 1$. Por lo tanto, si nuestra función es inyectiva, será un isomorfismo. Supongamos que no lo es. Entonces existen $m \neq n$ tales que $a^m = a^n$. Sin pérdida de generalidad, podemos suponer que $n > m$. De esta manera, se cumple que $1 = a^0 = a^{n-m}$, es decir, se tiene un natural, $n - m$, tal que $a^{n-m} = 1$. Por lo tanto, nos podemos fijar en el menor natural p tal que $a^p = 1$. Sea r el menor natural tal que $a^r = 1$. Afirmamos que $\langle a \rangle = \{1, a, a^2, \ldots, a^{r-1}\}$ donde cada $a^i \neq a^j$ para $i \neq j \in \{1, \ldots, r-1\}$. Sea $m > r$. Por el algoritmo de la division, se tiene que $m = pr + q$, donde $0 \leq q < r$. De esta manera, $a^m = a^{pr+q} = a^{pr} a^q = (a^r)^p a^q = 1^p a^q = a^q$. Por lo tanto, $a^m = a^q$ es un elemento de la lista. Ahora supongamos que $a^i = a^j$, con $i \neq j \in \{1, \ldots, r-1\}$. Sin pérdida de generalidad, supongamos que $i > j$. Entonces, $a^{i-j} = 1$, donde $0 < i - j < r$, lo que una contradice la elección de r. Por lo tanto, si $n \longmapsto a^n$ no es un isomorfismo, entonces $\langle a \rangle$ es un grupo cíclico finito. Notemos que en este caso, r es el menor natural tal que $a^r = 1$. En este caso, decimos que el *orden de* a es r. En caso contrario, cualquier grupo cíclico infinito es isomorfo a $(\mathbb{Z}, +, 0)$, por lo que cualesquiera dos grupos cíclicos infinitos son isomorfos.

Teorema 2 *Cualesquiera dos grupos cíclicos y finitos del mismo orden son isomorfos.*

Demostración. *Sea* $\langle a\rangle = \{1, a, a^2, \ldots, a^{r-1}\}$ *y* $\langle b\rangle = \{1, b, b^2, \ldots, b^{r-1}\}$ *donde* $a^r = 1$, *y* $b^r = 1$. *Notemos que si* h *es tal que* $a^h = 1$, *entonces* $r \mid h$; *si* $h = sr + q$, *entonces* $1 = a^h = a^{sr+q} = a^{sr}a^q = 1^s a^q = a^q$, *donde* $0 \leq q < r$. *Por la elección de* r *esto implica que* $q = 0$, *de donde* $r \mid h$. *Por otra parte, si* $a^m = a^n$ *entonces* $a^{m-n} = 1$, *con* $m > n$, *por lo que* $rk = m - n$. *De esta manera,* $b^{m-n} = b^{rk} = 1^k = 1$, *y así, se tiene que* $b^m = b^n$. *De manera análoga, si* $b^m = b^n$, *entonces* $a^m = a^n$.

Por lo tanto, $f : \langle a\rangle \longrightarrow \langle b\rangle$ *dada por* $a^n \longmapsto b^n$ *es sobre e inyectiva. Además,* $a^n a^m = a^{n+m} \longmapsto b^{n+m} = b^n b^m$ *y* $a^r = 1 \longmapsto b^r = 1$, *por lo que* f *es un isomorfismo de* $\langle a\rangle$ *en* $\langle b\rangle$. ■

El siguiente teorema determina a todos los posibles subgrupos de un grupo cíclico.

Teorema 3 *Cualquier subgrupo de un grupo cíclico* $\langle a\rangle$ *es cíclico. Si* $\langle a\rangle$ *es infinito, los subgrupos distintos al trivial son infinitos y además* $n \longmapsto a^n$ *es una biyección entre* $\mathbb{N}$ *y el conjunto de subgrupos de* $\langle a\rangle$. *Si* $\langle a\rangle$ *es finito y de orden* r, *entonces el orden de cualquier subgrupo es un divisor de* r, *y por cada divisor positivo* q *de* r, *hay un y sólo un subgrupo de orden* q.

Demostración. Sea H un subgrupo de $\langle a\rangle$. Si $H = \{e\}$ entonces $H = \langle e\rangle$. Supongamos que $H \neq e$. Entonces existe $n \in \mathbb{Z}$ tal que $a^n \in H$. Como H es subgrupo, entonces $a^{-n} = (a^n)^{-1} \in H$, por lo que podemos suponer que $n > 0$. Sea s el menor natural positivo tal que $a^s \in H$. Afirmamos que $H = \langle a^s\rangle$. Sea $a^m \in H$. Por el algoritmo de la división, $m = sk + n$, con $0 \leq n < s$. Entonces $a^n = a^{m-sk} = a^m(a^s)^{-k}$, y como H es subgrupo, entonces $a^n = a^m(a^s)^{-k} \in H$. Como por construcción, s es el menor natural tal que $a^s \in H$, entonces esto nos lleva a que $n = 0$, por lo que $m = sk$. Por lo tanto, $a^m = a^{sk} = (a^s)^k \in \langle a^s\rangle$. De esta manera se tiene que $H \subset \langle a^s\rangle$. Por otro lado, como $a^s \in H$, entonces todas sus potencias también se encuentran en H, es decir, $\langle a^s\rangle \subset H$. Por lo tanto, $H = \langle a^s\rangle$.

Ahora, si $\langle a\rangle$ es infinito entonces se vió que $a^m \neq a^n$ para cualesquiera $m \neq n \in \mathbb{Z}$. En particular, para cualquier natural positivo s, los elementos a^{sm}, con $m \in \mathbb{Z}$ son distintos, por lo que $\langle a^s\rangle$ también un grupo infinito. Además, s es el menor natural tal que $a^s \in \langle a^s\rangle$, por lo que cualquier subgrupo distinto del trivial es infinito y se tiene una correspondencia uno a uno entre los naturales y los subgrupos de $\langle a\rangle$, a saber, $n \longmapsto \langle a^n\rangle$.

Supongamos ahora que $\langle a\rangle$ es finito con orden r, por lo que

$$\langle a\rangle = \{1, a, a^2, \ldots, a^{r-1}\}.$$

Se demostró que si H es un subgrupo distinto de $\{e\}$ entonces $H = \langle a^k\rangle$, donde k es el menor natural tal que $a^k \in H$. Se afirma que $k \mid r$. Por el algoritmo de la división, se tiene que $r = ks + q, 0 \leq q < k$. Entonces $e = a^r = a^{ks+q} = (a^k)^s a^q$, por lo que $a^q = (a^k)^{-s} \in H$. Como k es el elemento mínimo tal que $a^k \in H$, esto implica que $q = 0$, por lo que $ks = r$, es decir, $k \mid r$. Ahora podemos ver a H como $\{1, a^k, a^{2k}, \ldots, a^{(s-1)k}\}$ donde $a^{ks} = a^r = 1$. De esta manera, tenemos

una correspondencia biyectiva $k \longmapsto \langle a^k \rangle$, del conjunto de divisores positivos del orden de G al conjunto de subgrupos de G, donde el orden del subgrupo $\langle a^k \rangle$ es $s = r/k$. Notemos que tanto k como s, se mueven en los posibles divisores de r. Por lo tanto, el orden de cada subgrupo de G, es un divisor de r, y por cada divisor positivo de r, se tiene un y solo un subgrupo de dicho orden. ■

Corolario 2 *Si $\langle a \rangle$ es de orden $r < \infty$, entonces el subgrupo H de orden $s \mid r$ se puede ver como el conjunto de elementos $b \in \langle a \rangle$ tales que $b^s = 1$.*

Demostración. Del teorema pasado, podemos ver a H como el conjunto $\{1, a^q, a^{2q}, \ldots, a^{(s-1)q}\}$, donde $qs = r$. Ahora, para cualquier elemento $b \in H$, $b = a^{kq}$ con $k \in \{0, \ldots, s-1\}$. Por lo tanto, $b^s = (a^{kq})^s = (a^{qs})^k = (a^r)^k = 1^k = 1$. Por otra parte, sea $b \in \langle a \rangle$ tal que $b = a^m$ y $b^s = 1$. Como r es el orden del grupo y $1 = b^s = a^{ms} = (a)^{ms}$, entonces $r \mid ms$, es decir, $rh = ms$, para alguna $h \in \mathbb{Z}$. Como $r = qs$ y $rh = ms$, se tiene que $qsh = ms$, por lo que $qh = m$, es decir, $b = a^m = a^{hq} \in H$. De esta manera, los elementos de H son aquellos tales que $b^s = 1$. ■

Terminaremos esta sección definiendo la función de Euler y demostraremos algunas propiedades de ésta con los grupos cíclicos finitos.

Definición 4 *La función de Euler φ se define como sigue: $\varphi(1) = 1$; y si $n > 1$, entonces $\varphi(n) = |\{k \mid 1 \leq k \leq n \ y \ (n,k) = 1\}|$.*

Proposición 1 *Si $G = \langle a \rangle$ es un grupo cíclico de orden n, entonces a^k también es un generador de G si y sólo si $(n,k) = 1$.*

Demostración. Notemos que a^k es generador de G si y sólo si existe $m \in \mathbb{N}$ tal que $\left(a^k\right)^m = a$. De esta manera, tenemos lo siguiente:

$$\begin{aligned} \left(a^k\right)^m &= a \iff a^{km} = a \iff a^{km}a^{-1} = e \\ &\iff a^{km-1} = e. \end{aligned}$$

Como $a^{km-1} = e$, entonces $n \mid km - 1$, por lo que existe $s \in \mathbb{N}$ tal que $ns = km - 1$, lo cual quiere decir que

$$1 = km + n(-s)$$

es decir, $(k,n) = 1$. De manera análoga, si $(k,n) = 1$, entonces existen $r, s \in \mathbb{Z}$ tales que $kr + ns = 1$. Ahora, como $ns = -kr + 1$, entonces $n(-s) = kr - 1$, por lo que

$$e = (a^n)^{-s} = a^{n(-s)} = a^{kr-1}$$

lo cual implica que $a^{kr-1} = e$. Multiplicando ambos lados por a, se tiene que $\left(a^k\right)^r = a^{kr} = a$, es decir, a está en el generado por a^k, por lo que a^k es un generador. ■

De la proposición anterior, se sigue que el número de generadores de un grupo cíclico finito $\langle a \rangle$ de orden n, es $\varphi(n)$.

Teorema 4 *Si n es un número natural, entonces $n = \Sigma_{d|n}\varphi(d)$, donde la suma se toma sobre todos los divisores d de n, con $1 \leq d \leq n$.*

Demostración. Si C es un subgrupo cíclico de un grupo G, denotaremos a $gen(C)$ como el conjunto de generadores del subgrupo C. Notemos que $G = \cup gen(C)$, donde C varía sobre todos los subgrupos cíclicos de G y la unión es disjunta. Claramente $\cup gen(C) \subset G$. Ahora, si $a \in G$, entonces $\langle a \rangle$ es un subgrupo cíclico de G con generador a, por lo que $a \in gen(\langle a \rangle) \subset \cup gen(C)$. Si $x \in gen(C) \cap gen(D)$, para C y D subgrupos cíclicos de G, entonces $C = \langle x \rangle = D$, por lo que cualquier generador de C también lo es de D. Por lo tanto, si $gen(C) \cap gen(D) \neq \varnothing$, entonces $gen(C) = gen(D)$, teniendo así que la unión $\cup gen(C)$ es disjunta.

Hemos visto que si G es un grupo cíclico de orden n, para cualquier divisor d de n, existe un subgrupo cíclico C_d de G, de orden d. De esta manera, se tiene que

$$n = |G| = \Sigma_{d|n} |gen(C_d)|.$$

Por la proposición anterior, $|gen(C_d)| = \varphi(d)$, donde d es el orden del subgrupo cíclico C_d. De esta manera, se tiene que

$$n = \Sigma_{d|n} |gen(C_d)| = \Sigma_{d|n}\varphi(d).$$

■

Para cerrar esta sección, veremos que G es un grupo cíclico de orden n si y sólo si para cada divisor d de n, existe a lo más un subgrupo cíclico de orden d. Hemos visto que si G es un grupo cíclico de orden n, entonces para cada divisor d de n, existe un y sólo un subgrupo cíclico de orden d. Usaremos la función de Euler para demostrar el regreso, pidiéndole todavía menos, es decir, que si G tiene orden n y es tal que, para cada divisor d de n existe a lo más un subgrupo de orden d, entonces G es cíclico. Para esto, notamos que $G = \cup gen(C)$, donde C varía sobre todos los subgrupos cíclicos de G y la unión es ajena. De esta manera se tiene lo siguiente:

$$n = |G| = \Sigma |gen(C)| \leq \Sigma_{d|n}\varphi(d) = n$$

donde la desigualdad se debe a que, por hipótesis, G tiene a lo más un subgrupo cíclico por cada divisor del orden. De esta manera,

$$\Sigma |gen(C)| = \Sigma_{d|n}\varphi(d)$$

y por lo tanto, podemos concluir que G contiene un subgrupo cíclico por cada divisor del orden. En particular, G contiene un subgrupo cíclico de orden $d = n$, teniendo así que G es cíclico.

Por lo tanto, hemos demostrado que un grupo finito G es cíclico si y sólo si, para cada divisor del orden existe a lo más un subgrupo cíclico de dicho orden.

0.5. Órbitas, clases laterales y subgrupos normales

Sea G un grupo de transformaciones de un conjunto S, es decir, $Id_S \in G$ y si $\mu, \eta \in G$ entonces $\mu^{-1} \in G$ y $\mu \circ \eta = \mu\eta \in G$. Notemos que G define una relación de equivalencia sobre S por la regla $x \sim_G y$ si $y = \mu(x)$ para algún $\mu \in G$: Es reflexiva porque $\forall x \in S$, $x = Id_S(x)$. Ahora, si $x \sim y$ entonces $y = \mu(x)$ para algún $\mu \in G$. Como G es un grupo de transformaciones, entonces $\mu^{-1}(y) = x$, por lo que $y \sim x$. Para ver la transitividad, supongamos que $x \sim y$ y $y \sim z$. Entonces se tiene que $y = \mu(x)$ y $z = \eta(y)$, por lo que al componer $\eta\mu(x) = \eta \circ \mu(x) = \eta(\mu(x)) = \eta(y) = z$, se tiene que $x \sim z$. Por otra parte, dado un elemento $x \in S$ se define la órbita de x bajo G, o $G - órbita$, como el conjunto $\{\eta(x) \mid \eta \in G\}$. Por ejemplo, si tomamos a G como el grupo de rotaciones alrededor del origen en $\mathbb{R}^2$ entonces la órbita bajo G de un punto $P \in \mathbb{R}^2$ es el círculo que pasa por P y centro en el origen.

Como se tiene una relación de equivalencia en S, ésta nos induce una partición del conjunto. Cuando sólo hay una $G - órbita$, es decir, $S = Gx$ para algún $x \in S$,(y por lo tanto para cualquier $y \in S$), se dice que G es un grupo transitivo de transformaciones del conjunto S. Notemos que cuando G es un grupo transitivo sobre S, entonces la relación $\sim_G$ induce una partición de S con un sólo elemento.

Definición 5 *Sea G un grupo y S un conjunto. Decimos que G actúa en el conjunto S si existe una función definida de $G \times S \longrightarrow S$ tal que*

i) $e \circ x = x, \forall x \in S$

ii) $(g_1 g_2) \circ x = g_1 (g_2 \circ x)$

Más adelante se desarrollará el tema de acción de un grupo sobre un conjunto, por ahora sólo mencionaremos un caso particular. Sea G un grupo y $H \leq G$. Como G es grupo, podemos definir la función $f : G \longrightarrow S_G$, con regla de correspondencia $g \longmapsto g \bullet \_$, es decir, la función multiplicar por g, para cada $g \in G$. Ahora, como H es un subrgupo de G, entonces $H \hookrightarrow G \longrightarrow S_G$, por lo que se tiene la restricción $f \mid_H : H \longrightarrow S_G$, dada por $h \longmapsto h \bullet \_$. De esta manera, H actúa en G por multiplicación, donde la órbita de $a \in G$ tiene la forma Ha. El conjunto de órbitas $\{Ha \mid a \in G\}$ se denota por el cociente G/H y su órden por $[G : H]$. Al conjunto Ha se le llama la *clase lateral derecha de a*. Análogamente, si ahora consideramos la función $g : G \longrightarrow S_G$ definida por $g \longmapsto \_ \bullet g$, es decir, la función multiplicar por la derecha, se tiene que H actúa en G, induciendo una partición de G en elementos de la forma aH, para cada $a \in G$. A los elementos de la forma aH, se le conoce como la *clase lateral izquierda de a*. De esta manera se tiene otra partición del grupo G definida por el conjunto $\{aH \mid a \in G\}$.

Algunos resultados sobre clases son los siguientes:

Lema 1 *Si $S \leq G$ entonces $Sa = Sb$ si y sólo si $ab^{-1} \in S$.*

Demostración. *Si $Sa = Sb$ entonces en particular, $a = sb$, para algún $s \in S$. Esto implica que $ab^{-1} = s \in S$. Supongamos ahora que $ab^{-1} \in S$. Entonces $ab^{-1} = s$ para alguna $s \in S$. Por otro lado, si $x \in Sa$ entonces $x = s_1 a$ con $s_1 \in S$. De esta manera se tiene que $x = s_1 a = s_1 sb = (s_1 s)b \in Sb$, por lo que $Sa \subset Sb$. La otra contención es análoga notando que $b = s^{-1}a$. Por lo tanto, $Sa = Sb$.* ■

Notemos ahora que si $S \leq G$ entonces cualesquiera dos clases derechas (o izquierdas) son ajenos o iguales ya que si $x \in Sa \cap Sb$ entonces $s_1 a = x = s_2 b$ para algún $s_1, s_2 \in S$, teniendo así que $ab^{-1} = s_1^{-1} s_2 \in S$. Por el lema anterior, $Sa = Sb$.

Teorema 5 *Si $S \leq G$ entonces el número de clases derechas de S en G es igual al número de clases izquierdas de S en G.*

Demostración. *Denotemos a D como el conjunto de clases derechas de S en G y a I como el de las izquierdas. Sea $f : D \longrightarrow I$ definida por $f(aS) \longmapsto Sa^{-1}$, con $a \in G$. Veamos primero que está bien definida. Si $aS = bS$ entonces $a = bs$, para alguna $s \in S$, por lo que $a^{-1} = s^{-1}b^{-1} \in Sb^{-1}$. De esta manera se tiene que $Sa^{-1} \subset Sb^{-1}$. La otra contención es totalmente análoga, notando que $b^{-1} = sa^{-1} \in Sa^{-1}$. Por lo tanto $Sa^{-1} = Sb^{-1}$ y así f esta bien definida.*

Supongamos que aS y bS son tales que $Sa^{-1} = Sb^{-1}$. Entonces $a^{-1} = sb^{-1}$, para alguna $s \in S$, lo que implica que $a = bs^{-1} \in bS$, por lo tanto, $aS \subset bS$. Análogamente, notando que $b = as \in aS$ se tiene que $bS \subset aS$, y así $aS = bS$. De esta manera, f es inyectiva. La suprayectividad se sigue de que si $Sa \in I$,con $a \in G$, entonces $a^{-1} \in G$ y $a^{-1}S \in D$ es tal que se tiene que dar un elemento en el dominio tal que al aplicarle f nos dé Sa. Como $a \in G$, entonces $a^{-1} \in G$, por lo que $a^{-1}S \in D$ es tal que $f\left(a^{-1}S\right) = S(a^{-1})^{-1} = Sa$. Por lo tanto, f es una biyección y $|D| = |I|$. ■

Teorema 6 *Sea G un grupo finito y $S \leq G$. Entonces $|S| \mid |G|$ y $[G : S] = |G| / |S|$.*

Demostración. *Como se vio anteriormente, dos clases laterales son la misma o son ajenas, por lo que G queda partido por S en clases laterales. Así, $G = Sx_1 \cup Sx_2 \cup \cdots \cup Sx_n$, donde las x_i son representantes de cada clase. Nótese también que es una partición finita porque G es finito. Además, como las clases son ajenas, se tiene que $|G| = \sum_{i=1}^{n} |Sx_i|$. Por otra parte, notemos que $|S| = |Sx_i|$. Esto se sigue considerando la función $f_i : S \longrightarrow Sx_i$ definida por $s \longmapsto sx_i$, la cual es una biyección: si $a \in Sx_i$ entonces $a = sx_i$ para algún $s \in S$, por lo que claramente f es sobre. Ahora, si $s_1, s_2 \in S$ son tales que $s_1 x_i = s_2 x_i$, entonces $s_1 = s_1(x_i x_i^{-1}) = (s_1 x_i)x_i^{-1} = (s_2 x_i)x_i^{-1} = s_2(x_i x_i^{-1}) = s_2$, por lo que f también es inyectiva. De esta manera $|S| = |Sx_i|, \forall i \in \{1, \ldots, n\}$ y para cualquier representante x_i. Se sigue entonces que $|G| = \sum_{i=1}^{n} |Sx_i| = n\,|S|$, donde $n = [G : S]$.* ■

De este gran teorema, se tiene el siguiente

Corolario 3 *Si G es un grupo finito de orden n, entonces $x^n = 1$, para toda $x \in G$.*

Demostración. Sea $x \in G$ y m el orden de $\langle x \rangle$. Como $\langle x \rangle \leq G$, entonces $|\langle x \rangle| = m \mid n = |G|$, es decir, $mk = n$, para alguna $k \in \mathbb{N}$. Por otra parte, como m es el orden de $\langle x \rangle$, $x^m = 1$, por lo que $x^n = x^{mk} = (x^m)^k = 1^k = 1$. ■

Definición 6 *Si S y T son subconjuntos de un grupo G entonces $ST = \{st \mid s \in S, t \in T\}$.*

En particular, de la definición anterior, si $T = \{t\}$ entonces ST es la $S-$*órbita* de t.

Teorema 7 *Si S y T son subgrupos de un grupo finito G, entonces $|ST|\,|S \cap T| = |S|\,|T|$.*

Demostración. *Sea $\varphi : S \times T \longrightarrow ST$ definida por $(s,t) \longmapsto st$. Notemos que φ es sobre, ya que para cualquier $st \in ST$, se tiene la pareja $(s,t) \in S \times T$ tal que $\varphi(s,t) = st$. Por lo tanto, como φ es sobre, $|S|\,|T| = |S \times T| = |ST| \times \{$numero de imágenes inversa para cada $st \in ST\}$. Basta entonces demostrar que para cualquier $x = st \in ST$, $\varphi(x)^{-1} = S \cap T$. Para esto probaremos que $\varphi(x)^{-1} = \{(sd, d^{-1}t) \mid d \in S \cap T\} := A$. Claramente, $A \subset \varphi(x)^{-1}$. Sean $(s,t),(r,q) \in \varphi(x)^{-1}$. Entonces $st = x = rq$, esto implica que $r^{-1}s = qt^{-1}$, donde $r^{-1}, s \in S$ y $q, t^{-1} \in T$, por lo que $d = r^{-1}s = qt^{-1} \in S \cap T$. Notemos entonces que $rd = r(r^{-1}s) = s$ y $d^{-1}q = (tq^{-1})q = t$ teniendo así que $(s,t) = (rd, d^{-1}q) \in A$, lo cual demuestra la otra contención. De esta manera $\varphi(x)^{-1} = \{(sd, d^{-1}t) \mid d \in S \cap T\}$ y así $\left|\varphi(x)^{-1}\right| = \left|\{(sd, d^{-1}t) \mid d \in S \cap T\}\right| = |S \cap T|$, con lo que $|ST|\,|S \cap T| = |S|\,|T|$.* ■

Definición 7 *Un subgrupo $K \leq G$ es normal, denotado por $K \lhd G$, si $gKg^{-1} = K$, $\forall g \in G$.*

Notemos que si $K \leq G$ es tal que $gKg^{-1} \leq K, \forall g \in K$ entonces $K \lhd G$, ya que como $gKg^{-1} \leq K, \forall g \in G$, entonces reemplazando g por g^{-1} se tiene $g^{-1}Kg \leq K, \forall g^{-1} \in G$. Esto nos da la otra inclusión $K \leq gKg^{-1}$, por lo que $gKg^{-1} = K$. Por otro lado, para cualquier homomorfismo $f : G \longrightarrow H$, el $\ker f = K$ es un subgrupo normal: Dado $k \in K$ se tiene que $f(k) = 1$, por lo que $\forall g \in G$ se tiene que $f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(g)^{-1} = 1$, por lo que $gkg^{-1} \in K, \forall g \in G, \forall k \in K$.

Otra observación es que $K \lhd G$ si y sólo si $Kg = gK, \forall g \in G$, es decir, las clases izquierdas y derechas en G inducidas por K son iguales. Para demostrar esto, notemos que si $gKg^{-1} = K$ entonces $Kg^{-1} = g^{-1}K, \forall g^{-1} \in G$ y por lo tanto $\forall g \in G$. Ahora, si $Kg = gK$, entonces $K = \left(Kg^{-1}\right)g = \left(g^{-1}K\right)g = g^{-1}Kg, \forall g \in G$, lo cual equivale a decir que $K \lhd G$.

Ahora veremos que cuando se tiene un subgrupo normal $K \lhd G$ entonces el cociente G/K forma un grupo:

Teorema 8 *Si $K \lhd G$ entonces las clases de K en G forman un grupo, denotado por G/K, de orden $[G : K]$.*

Demostración. *Para decir que G/K es un grupo, tenemos que definir una operación para los elementos de G/K, los cuales son las distintas clases inducidas por K en G. Nótese también que, como K es normal, entonces para cada $a \in G$, $aK = Ka$, es decir, sus clases laterales coinciden, por lo que basta definir la operación para cualquiera de ellas.*

Sean $Ka, Kb \in G/K$. Definimos el producto en G/K por

$$KaKb = Ka(a^{-1}Ka)b = K(aa^{-1})K(ab) = KKab = Kab$$

donde la primero igualdad se da porque $K \lhd G$, y la la última porque $K \leq G$. Veamos ahora que está bien definido: supongamos que $Ka = Ka'$ y que $Kb = Kb'$. Queremos ver que $KaKb = Ka'Kb'$. Por una parte, $KaKb = Kab$ y $Ka'Kb' = Ka'b'$. Como $Ka = Ka'$ entonces $a = a'k_1$ para algún $k_1 \in K$, análogamente, $b = k_2b'$. Por lo tanto, $Kab = K(a'k_1)b = Ka'(k_1b) = a'Kk_1b = a'Kb = Ka'b$, donde la tercera y quinta igualdad se deben a que K es normal en G y la cuarta ya que $kK = K, \forall k \in K$. Usando que $b = k_2b'$, se tiene que $Kab = Ka'b = Ka'(k_2b') = a'K(k_2b') = a'(Kk_2)b' = a'Kb' = Ka'b'$. Por lo tanto el producto está bien definido.

Veamos que $Ke = K$ es el neutro en G/K. Si $Ka \in G/K$, $KaK = KaKe = Kae = Ka$, así como $KKa = KeKa = Kea = Ka$. Por lo tanto, K es el elemento neutro en G/K. Por otra parte, si $Ka \in G/K$, entonces $Ka^{-1} \in G/K$ y se tiene que $KaKa^{-1} = Kaa^{-1} = Ke = K = Ke = Ka^{-1}a = Ka^{-1}Ka$, es decir, $(Ka)^{-1} = Ka^{-1}$. Como el producto no depende del representante, entonces tanto el neutro como el inverso son únicos. Por lo tanto, G/K es un grupo con tantos elementos como distintas clases laterales, es decir, $|G/K| = [G : K]$. ■

A continuación, se dan dos proposiciones que asocian al índice de un subgrupo con ser un subgrupo normal de un grupo G.

Proposición 2 *Si $H \leq G$ y $[G : H] = 2$, entonces $a^2 \in H$, para toda $a \in G$.*

Demostración. Sea $a \in G$. Si $a \in H \subset G$, el resultado es claro. Supongamos que $a \in G \setminus H$. Como $[G : H] = 2$ y $a \in G \setminus H$ entonces $aH \neq eH = H$. Análogamente, $a^{-1}H \neq H$. Como $[G : H] = 2$, y $aH \neq H \neq a^{-1}H$, entonces $aH = a^{-1}H$, lo cual implica que $a^2H = a(aH) = a(a^{-1}H) = eH = H$, teniendo así que $a^2 \in H$. ■

Proposición 3 *Si $H \leq G$ y $[G : H] = 2$, entonces $H \lhd G$.*

Demostración. Sea $a \in G$. Tenemos que probar que $aHa^{-1} = H$, o lo que es equivalente, $aH = Ha$. Ahora, como $[G : H] = 2$, entonces el conjunto

de clases laterales izquierdas tiene la forma $\{H, aH\}$ y el conjunto de clases laterales derechas la forma $\{H, Ha\}$. Como éstas son particiones de G, se tiene que

$$H \cup aH = G = H \cup Ha$$

donde la unión es ajena. Esto implica que $aH = Ha$, por lo que $aHa^{-1} = H$, $\forall a \in G$, es decir, $H \lhd G$. ■

0.6. Homomorfismos de grupos

Sean G y G' dos grupos y sea $f : G \longrightarrow G'$ tal que $f(e) = e'$ y $f(ab) = f(a)f(b)$, donde $e \in G$ y $e' \in G$ son los neutros de G y G', respectivamente. Notemos que f manda un producto en G al producto de las imágenes en G'. Por otra parte, para cualquier $a \in G$, $f(a^k) = f(a)^k$. Si $k = 0$ entonces el resultado es claro, pues $f(e) = e'$. Supongamos que vale para k y demostremos que vale para $k + 1$. Ahora, $f(a^{k+1}) = f(a^k a) = f(a^k)f(a) = f(a)^k f(a) = f(a)^{k+1}$.Además, si a es invertible, se tiene que $e = aa^{-1}$ por lo que

$$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$$

y como G' es grupo, entonces $(f(a))^{-1} = f\left(a^{-1}\right)$. De estas dos observaciones se tiene que $f(a^k) = f(a)^k, \forall k \in \mathbb{Z}$.

Teorema 9 *Sean η,$\mu : G \longrightarrow G'$ homomorfismos y sea S un conjunto de generadores de G. Supongamos que $\eta(s) = \mu(s), \forall s \in S$. Entonces $\eta = \mu$.*

Demostración. *Sean G, G' grupos y $\mu, \eta : G \longrightarrow G'$ homomorfismos tales que $\mu(s) = \eta(s)$, $\forall s \in S$, donde S es un conjunto generador de G. Sea $G_1 = \{g \in G \mid \eta(g) = \mu(g)\}$. Claramente $G_1 \subset G$ y $G_1 \neq \varnothing$, ya que $e \in G_1$.Además, si $g \in G_1$ entonces $\mu(g^{-1}) = \mu(g)^{-1} = \eta(g)^{-1} = \eta(g^{-1})$, por lo que $g^{-1} \in G_1$. Por otra parte, si $g, h \in G_1$ entonces $\eta(gh) = \eta(g)\eta(h) = \mu(g)\mu(h) = \mu(gh)$, teniendo así que $gh \in G_1$. Por lo tanto, $G_1 \leq G$. Finalmente, como $S \subset G_1$, con S el conjunto generador de G, se tiene que $G = G_1$ y por lo tanto, $\mu(g) = \eta(g), \forall g \in G$, es decir, $\eta = \mu$.* ■

Un homomorfismo de G en sí mismo se le llama *endomorfismo*, y cuando además éste es un isomorfismo, se le conoce como *automorfismo.* Del teorema anterior, se sigue que, si μ es un endomorfismo tal que $\mu(s) = s$, $\forall s \in S$, entonces $\mu = Id_G$. Veamos ahora que la composición de homomorfismos sigue siendo un homomorfismos. Si $\mu : G \longrightarrow H$, y $\eta : H \longrightarrow K$ son homomorfismos, entonces $\forall a, b \in G$, $\eta\mu(ab) = \eta(\mu(ab)) = \eta(\mu(a)\mu(b)) = \eta(\mu(a))\eta(\mu(b)) = \eta\mu(a)\eta\mu(b)$. Como μ y η mandan al neutro en el neutro respectivamente, entonces $\eta \circ \mu : G \longrightarrow K$ es un homomorfismo.

Sea μ un homomorfismo de G en G'. Notemos que la imagen de μ es un subgrupo de G'. Para esto, basta ver que la multiplicación es cerrada y la existencia de inversos. Si $x, y \in \operatorname{Im}\mu$, entonces existen $a, b \in G$ tales que $\mu(a) = x$ y $\mu(b) = y$, por lo que $xy = \mu(ab) \in \operatorname{Im}\mu$. Si $x \in \operatorname{Im}\mu$, entonces existe $a \in G$ tal que $\mu(a) = x$. Como G es grupo, $a^{-1} \in G$, por lo que $\mu(a^{-1}) \in \operatorname{Im}\mu$. Notando que $e' = \mu(e) = \mu(aa^{-1}) = \mu(a)\mu(a^{-1})$, se tiene que $(\mu(a))^{-1} = \mu(a^{-1})$, pues G' es un grupo y el inverso es único.

Por otra parte, observemos que μ es *monomorfismo* si y sólo si $\ker\mu = \{e\}$. Para la ida, supongamos que $\ker\mu \neq \{e\}$, entonces $\exists a \in \ker\mu$ con $a \neq e$ tal que $\mu(a) = e' = \mu(e)$, es decir, μ no es inyectiva. Por otra parte, si μ no es inyectiva, existen $a \neq b$ en G tales que $\mu(a) = \mu(b)$. Como $a \neq b$, $ab^{-1} \neq 1$ por lo que $\mu(ab^{-1}) = \mu(a)\mu(b^{-1}) = \mu(a)\mu(b)^{-1} = e'$, es decir, $\ker\mu \neq \{e\}$.

Sea L un subgrupo normal de G contenido en $K = \ker\mu$. Consideremos el grupo cociente $\overline{G} = G/L$, que consiste en elementos de la forma $aL = La, \forall a \in G$, donde la multiplicación de clases se define multiplicando a los representantes, es decir, $aLbL = abL$, y neutro $eL = L$. Definamos ahora la función $\nu : G \longrightarrow \overline{G}$ definida por $g \longmapsto gL$, para cada $g \in G$. Por la manera en que está definido el producto entre clases, se tiene que ν es un homomorfismo. Por otra parte, si $aL = bL$, para alguna $a, b \in G$, entonces $a = bl$, para alguna $l \in L$. Por lo tanto, $\mu(a) = \mu(bl) = \mu(b)\mu(l) = \mu(b)$, pues $l \in L \subset K$. De esta manera, la función $\overline{\mu} : \overline{G} :\longrightarrow G'$ con regla de correspondencia $aL \longmapsto \mu(a)$ está bien definida. Como también

$$\overline{\mu}((aL)(bL)) = \overline{\mu}(abL) = \mu(ab) = \mu(a)\mu(b) = \overline{\mu}(aL)\overline{\mu}(bL)$$

y

$$\overline{\mu}(L) = \overline{\mu}(eL) = \mu(e) = e'$$

entonces $\overline{\mu}$ también es un homomorfismo con $\operatorname{Im}\overline{\mu} = \operatorname{Im}\mu$. De esta manera, se tiene el siguiente diagrama conmutativo

$$\begin{array}{ccccc} & & & \overset{\mu}{\longrightarrow} & \\ & & G & & G' \\ & & \downarrow & \nearrow & \\ \overline{G} & = & G/L & & \end{array}$$

Además, el $\ker\overline{\mu}$ es el conjunto $\{aL \mid \overline{\mu}(aL) = e'\}$. Como $\overline{\mu}(aL) = \mu(a)$, esto equivale a la condición $\mu(a) = e'$. Por lo tanto, $\ker\overline{\mu} = \{aL \mid a \in \ker\mu\}$, es decir, $\ker\overline{\mu} = \ker\mu/L$, pues $L \lhd K$. Como un homomorfismo es inyectivo si y sólo si su kernel es trivial, entonces $\overline{\mu}$ es inyectiva si y sólo si $\ker\mu = L$. En particular, cuando $L = K$, se tiene el siguiente

Teorema 10 *Sea $\eta : G \longrightarrow G'$ un epimorfismo de grupos con kernel K. Entonces la función inducida $\overline{\eta} : \overline{G} = G/K \longrightarrow G'$ definida por $aK \longmapsto \eta(a)$ es un isomorfismo. Por lo tanto, cualquier imagen homomorfa a G es isomorfa a un grupo factor de G/K, con $K \lhd G$.*

0.7. Isomorfismos

En este capítulo veremos lo que son los tres teoremas de isomorfismos, los cuales los aplicaremos a grupos, cuando en realidad se pueden utilizar para una gran tipo de sistemas algebraicos, tales como semigrupos, anillos, módulos, entre otros.

Teorema 11 *Sean G y H grupos y $\eta : G \longrightarrow H$ un homomorfismo con kernel K. Entonces K es un subgrupo normal de G y $G/K \cong \operatorname{Im}\eta$.*

Demostración. *Se demostró anteriormente que $K \lhd G$ para cualquier $K = \ker\eta$, de algún homomorfismo η. Definamos ahora $\mu : G/K \longrightarrow H$ por $\mu(aK) \longmapsto \eta(a)$. Veamos que μ está bien definida. Si $aK = bK$ entonces $b^{-1}a \in K$. Por lo tanto, $e = \eta(b^{-1}a) = \eta(b^{-1})\eta(a)$. Como la imagen de η es un subgrupo, se tiene que $\eta(b)^{-1} = \eta(b^{-1}) = \eta(a)^{-1}$, es decir, $\eta(b) = \eta(a)$. Por lo tanto, $\mu(aK) = \mu(bK)$, por lo que η está bien definida. Notemos también que por la manera en que se definición η, es claro que $\operatorname{Im}\mu = \operatorname{Im}\eta$.*

Por otra parte, para cualquier $aK, bK \in G/K$, se tiene $\mu(aKbK) = \mu(abK) = \eta(ab) = \eta(a)\eta(b) = \mu(aK)\mu(bK)$, por lo que μ es un homomorfismo. Finalmente, basta ver que μ es inyectiva. Para esto supongamos que $\mu(aK) = \mu(bK)$. Entonces $\eta(a) = \eta(b)$, teniendo así que $\eta(ab^{-1}) = \eta(a)\eta(b^{-1}) = \eta(a)\eta(b)^{-1} = e$. Por lo tanto $ab^{-1} \in K$ y así $aK = bK$. Con esto se demuestra que μ es un isomorfismo y por lo tanto, $G/K \cong \operatorname{Im}\eta$. ■

Del teorema anterior se sigue que no hay diferencia entre un grupo cociente y la imagen de un homomorfismo. Si $\nu : G \longrightarrow G/K$, donde $K = \ker\eta$, es el morfismo natural, $\nu(g) = gK$, entonces, el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} & \overset{\eta}{} & \\ G & \longrightarrow & H \\ {\scriptstyle\nu}\searrow & & \nearrow{\scriptstyle\mu} \\ & G/K & \end{array}$$

De esta manera, podemos describir a $\mu^{-1} : \operatorname{Im}\eta \longrightarrow G/K$. Si $x \in \operatorname{Im}\eta$ entonces

$\exists a \in G$ tal que $\eta(a) = x$, por lo que $\mu^{-1}(x) = aK$. Veamos que está bien definida. Para esto, tomemos $b \in G$ tal que $\eta(b) = x$. Queremos ver que $bK = aK$, pero esto se sigue considerando $\eta(b^{-1}a) = \eta(b^{-1})\eta(a) = \eta(b)^{-1}\eta(a) = x^{-1}x = e$, por lo que $b^{-1}a \in K$, es decir, $aK = bK$. Notemos que al ser $K \lhd G$, también se pudo haber definido a μ^{-1} usando la clase Ka. El siguiente teorema se conoce como el **Teorema de la correspondencia**:

Teorema 12 *Sea $\eta : G \longrightarrow G'$ un epimorfismo y sea $\Delta = \{H \leq G \mid K \subset H\}$ donde $K = \ker\eta$. Entonces la función $H \longrightarrow \eta(H)$ es una biyección entre Δ y los subgrupos de G'. Además, $H \lhd G$ si y sólo si $\eta(H) \lhd G'$. En este caso, $\zeta : G/H \longrightarrow G/\eta(H)$ definido por $\zeta(gH) \longmapsto \eta(g)\eta(H)$ es un isomorfismo.*

Demostración. *Notemos primero que como η es epimorfismo entonces $G/K \cong G'$, por lo que si $\overline{H} \leq G'$ entonces lo podemos ver como un subgrupo de G/K, es decir, podemos identificar a $\overline{H}$ con $\xi\left(\overline{H}\right)^{-1} \leq G/K$, donde ξ es un isomorfismo entre G/K y G'. Además, si $H \leq G$ es tal que $K \subset H$ entonces $H/K \leq G/K$.*

Por otra parte, se demostró que para cualquier homomorfismo $\phi : A \longrightarrow B$, $\phi(A) \leq B$. En particular, si $H \leq G$, $\eta \mid_H : H \longrightarrow G'$ es un homomorfismo, por lo que $\eta(H) \leq G'$. De esta manera, nuestra función $H \longrightarrow \eta(H)$ está bien definida. Veamos ahora que es inyectiva. Supongamos que $H_1, H_2 \leq G$ son tales que $K \subset H_1, H_2$ y que $H_1/K = H_2/K, \leq G/K$. Entonces para cualquier $h_1 \in H_1$, $h_1K \in H_2/K$ por lo que $h_1K = h_2K$, para alguna $h_2 \in H_2$. Entonces $h_1 = h_2k$, para alguna $k \in K$. Como $K \subset H_2$, entonces $h_1 = h_2k \in H_2$. Como tomamos cualquier $h_1 \in H_1$, se concluye que $H_1 \subset H_2$. De manera análoga, para cualquier $h_2 \in H_2$ se tiene que $h_2 = h_1k^{-1}$, para alguna $h_1 \in H_1$ y para alguna $k \in K$. Como también $K \subset H_1$, $h_2 \in H_1$, por lo que $H_1 = H_2$. Por lo tanto, nuestra función es inyectiva.

Supongamos que $\overline{H} \leq G'$. Por la observación del principio, podemos ver a $\overline{H}$ como un subgrupo de G/K. De esta manera, $\overline{H}$ es una colección de clases laterales en G por K, por lo que basta demostrar que $\overline{H} = \{\eta(a)K \mid a \in H\}$, para algún $H \leq G$ que contenga a K. Sea $H = \cup aK$ donde $aK \in \overline{H}$. Afirmamos que $H \in \Delta$. Nótese que $K = eK \subset H$. Si $d_1, d_2 \in H$, entonces $d_1 = a_1k_1, d_2 = a_2k_2$.

De esta manera, como K es normal en G, se tienen las siguientes igualdades:

$$\begin{aligned}
d_1d_2 &= a_1k_1a_2k_2 = a_1k_1a_2k_2\left(a_2^{-1}a_2\right) = a_1k_1\left(a_2k_2a_2^{-1}\right)a_2 \\
&= a_1k_1\acute{k}a_2, \text{ donde } \acute{k} = a_2k_2a_2^{-1} \\
&= a_1k_1a_2a_2^{-1}\acute{k}a_2 = a_1k_1a_2\left(a_2^{-1}\acute{k}a_2\right) \\
&= a_1k_1a_2\acute{k}, \text{ donde } \acute{k} = a_2^{-1}\acute{k}a_2 \\
&= a_1a_2a_2^{-1}k_1a_2\acute{k} = a_1a_2\left(a_2^{-1}k_1a_2\right)\acute{k} \\
&= a_1a_2k\acute{k}, \text{ donde } k = a_2^{-1}k_1a_2
\end{aligned}$$

Por lo tanto, $d_1d_2 = a_1a_2k\acute{k} \in a_1a_2K$. Ahora, como $\overline{H} \leq G/K$ y $K \lhd G$, entonces $a_1a_2K = (a_1K)(a_2K) \in \overline{H}$, por lo que $d_1d_2 \in a_1a_2K \in H$. Como $K \lhd H$, se tiene que $(h_1h_2)K = h_1Kh_2K = d_1d_2 \in \overline{H}$, por lo que $h_1h_2 \in H$. Por otra parte, si $d \in H$, entonces $d = hK$. Ahora, la clase $h^{-1}K \in H$, ya que $hK \in \overline{H}$ y $\overline{H} \leq G/K$. Además, $K = hh^{-1}K = hKh^{-1}K = d(h^{-1}K)$, por lo que $h^{-1}K = d^{-1} \in H$. Por lo tanto, $H \leq G$, y así la función es biyectiva.

Supongamos ahora que $H \lhd G$. Sean $a \in G'$ y $h' \in \eta(H)$. Como η es un epimorfismo, existen $x \in G$ y $h \in H$ tales que $\eta(x) = a$ y $\eta(h) = h'$, por lo que $ah'a^{-1} = \eta(x)\eta(h)\eta(x^{-1}) = \eta(xhx^{-1}) \in \eta(H)$ pues $xhx^{-1} \in H$ al ser $H \lhd G$. Como esto fue para cualquier $a \in G'$ y cualquier $h' \in \eta(H)$ se tiene que $\eta(H) \lhd G'$. Ahora supongamos que $\eta(H) \lhd G'$ para algún $H \leq G$ tal que $K \subset H$. Sean $g \in G$ y $h \in H$. Entonces como $\eta(H) \lhd G'$, $\eta(ghg^{-1}) = \eta(g)\eta(h)\eta(g^{-1}) \in \eta(H)$, por lo que $ghg^{-1} \in H, \forall g \in G, h \in H$. Por lo tanto, $H \lhd G$.

Para finalizar, considerando esto último, se tiene la función $\rho : G/H \longrightarrow G'/\eta(H)$ *definida por* $gH \longmapsto \eta(g)\eta(H)$. *Afirmamos que* ρ *es un isomorfismo. Notemos que* ρ *es inyectiva pues* $\eta(g_1)\eta(H) = \eta(g_2)\eta(H)$ *si y sólo si* $\eta(g_2^{-1}g_1)\eta(H) = \eta(H)$, *si y sólo si* $\eta(g_2^{-1}g_1) \in \eta(H)$, *si y sólo si* $g_2^{-1}g_1 \in H$, *si y sólo si* $g_1H = g_2H$. *La suprayectividad de* ρ *se sigue de la suprayectividad de* η, *por lo que* ρ *es una biyección. Ahora, si* $\eta(H) \lhd G'$ *entonces, para* $aH, bH \in G/H$, $\rho(abH) = \eta(ab)\eta(H) = \eta(a)\,\eta(b)\,\eta(H) = \eta(a)\eta(H)\eta(b)\eta(H) = \rho(aH)\rho(bH)$, *por lo que* ρ *es un isomorfismo.* ■

Al isomorfismo ρ frecuentemente se le conoce como el primer teorema de isomorfismos para grupos. A continuación presentamos el segundo teorema de isomorfismos.

Teorema 13 *Sea* G *un grupo y* $H, K \leq G$ *con* $K \lhd G$. *Entonces* $HK = \{hk \mid h \in H, k \in K\}$ *es un subgrupo de* G *que contiene a* K. *Además* $H \cap K$ *es normal en* H *y* $HK/K \cong H/(H \cap K)$.

Demostración. *Como* $K \lhd G$ *entonces* $gK = Kg, \forall g \in G$. *En particular, se cumple que* $\forall h \in H$, *por lo que* $K \lhd H$. *Por lo tanto,* $hK = Kh$. *Notemos ahora que* $HK = \cup_{h\in H} hK = \cup_{h\in H} Kh = KH$. *Entonces para ver que* $HK \leq G$ *basta ver que es cerrado y que contiene inversos. Para lo primero, notemos que* $(HK)^2 = HKHK = HHKK = H^2K^2 = HK$, *pues* $H, K \leq G$, *por lo que* HK *es cerrado bajo producto. Es claro que* $e \in HK$, *pues* $e \in H \cap K$ *por ser subgrupos, por lo que* $e = ee \in HK$. *Por otro lado, si* $hk \in HK$, *entonces* $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, *por lo que también es cerrado bajo tomar inversos. Por lo tanto,* $HK \leq G$. *Además, se tiene que* $K = eK \subset HK$, *y como* $K \lhd H$, *se tiene que* $K \lhd HK$.

Consideremos ahora la función $\nu : G \longrightarrow G/K$ *dada por* $g \longrightarrow gK$, *y su restricción* $\nu' : H \longrightarrow H/K$. *Claramente,* ν' *es un homomorfismo y su imagen es el conjunto de clases* hK, *es decir,* H/K. *Notemos que para cualquier* $hk \in HK$, *su clase lateral* hkK *es simplemente* hK, *por lo que la imagen de* ν' *la podemos ver como* HK/K. *Por otro lado, el* $\ker \nu' = \{h \in H \mid hK = K\}$. *Como* $hK = K$ *si y sólo si* $h \in K$ *entonces el* $\ker \nu' = H \cap K$, *y por lo tanto,* $H \cap K \lhd H$. *Por el primer teorema de isomorfismos, se tiene que* $H/\ker \nu' \cong \operatorname{Im} \nu'$, *que es equivalente a* $H/(H \cap K) \cong HK/K$. ■

Por último, demostraremos el tercer teorema de isomorfismos:

Teorema 14 *Sean* $K \leq H \leq G$ *donde tanto* K *como* H *son normales en* G, *entonces* $H/K \lhd G/K$, *y* $(G/K)/(H/K) \cong G/H$.

Demostración. *Definamos la función* $\zeta : G/K \longrightarrow G/H$ *por* $\zeta(gK) = gH$. *Veamos primero que está bien definida. Si* $aK = bK$, *entonces* $b^{-1}a \in K$. *Como* $K \leq H$, *entonces* $b^{-1}a \in H$, *por lo que* $aH = bH$. *Por lo tanto,* ζ *está bien definida. Por otra parte,*

$$\forall aK, bK \in G/K, \zeta(aKbK) = \zeta(abK) = abH = aHbH = \zeta(aK)\zeta(bK)$$

esto último debido a que tanto K como H son normales en G. Como G/K y G/H son grupos, ζ es un homomorfismo de grupos. Por último, falta ver que ζ es sobre y encontrar el kernel de ζ. Lo primero es claro, ya que si $x \in G/H$ entonces $x = gH$, para alguna $g \in G$. Tomando la clase de g en G pero ahora inducida por K, se tiene que $x' = gK$ es tal que $\zeta(x') = \zeta(gK) = gH = x$, por lo que ζ es sobre. Por otra parte, por definición el $\ker\zeta = \{aK \in G/K \mid aH = H\}$, *pero esto equivale a decir que $a \in H$, es decir,* $\ker\zeta = \{aK \in G/K \mid a \in H\} = \{hK \mid h \in H\} = H/K$. *Como* $\ker\zeta$ *es un subgrupo normal, entonces $H/K \lhd G/K$. Por lo tanto, usando el primer teorema de isomorfismos, se tiene que $(G/K)/(H/K) \cong G/H$.* ■

0.8. Acción de un grupo

Sea G un grupo y S un conjunto. Sea $T : G \longrightarrow SymS$ un homomorfismo donde $SymS$ es el grupo de transformaciones biyectivas del conjunto S. Entonces, si $g \in G$, $T(g)$ es una biyección del conjunto S, y además

i) $T(e) = Id_S$

ii) $T(g_1g_2) = T(g_1) \circ T(g_2)$, donde $\circ$ es la operación de componer funciones.

Sea $x \in S$. Denotamos a $T(g)x$ por evaluar la función $T(g)$ en el punto $x \in S$. De esta manera se tiene una función de $G \times S \longrightarrow S$ definida por $(g, x) \longmapsto T(g)x$. Notemos que $(e, x) \longmapsto T(e)x = Id_S(x) = x$ y que $(g_1g_2, x) \longmapsto T(g_1g_2)x = T(g_1) \circ T(g_2)_{(x)} = T(g_1) \circ T(g_2)x$

Recordemos que si G es un grupo y S un conjunto, decimos que G actúa en S si existe una función definida de $G \times S \longrightarrow S$ tal que

$$i)\ e \circ x = x, \forall x \in S$$

$$ii)\ (g_1g_2) \circ x = g_1\,(g_2 \circ x)$$

Si sólo hay una órbita en la acción de G sobre S, es decir, $S = Gx$ para alguna $x \in S$, entonces también se cumple para toda $y \in S$, ya que $y = gx \Longrightarrow Gy = Ggx = Gx$. Cuando esto pasa decimos que G actúa transitivamente sobre S.

Sea $H \leq G$ y sea G/H. Veamos que G actúa transitivamente sobre G/H. Sea xH una clase lateral en G/H. Si yH es cualquier otra clase en G/H, entonces como $x, y \in G$ también $g = yx^{-1} \in G$. Así, $gxH = yx^{-1}xH = yH$, por lo que cualquier clase lateral en G/H está en la órbita de xH bajo G, es decir, $GxH = G/H$.

Definición 8 *Si $x \in S$ entonces definimos el conjunto $Est\ x = \{g \in G \mid gx = x\}$*

A este conjunto le llamaremos el *estabilizador de* x. Notemos que $Est\ x \leq G$, ya que si $g \in Est\ x$ entonces $gx = x$, lo cual implica que $x = g^{-1}x$, por lo que $g^{-1} \in Est\ x$. Además, si $g, h \in Est\ x$ entonces $ghx = g(hx) = gx = x$, por lo que $gh \in Est\ x$. Esto demuestra que $Estx$ es un subgrupo de G.

Sea G un grupo y consideremos la acción de conjugar, que va de G en sí misma. Para $x \in G$, se tiene que

$$Est\ x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = Cent\ x$$

Al conjunto $Centx$ se le conoce como el *centro de* x. Ahora, consideremos la acción de multiplicar por la izquierda, es decir, $I_x : G \times G \longrightarrow G$ con regla de correspondencia $(a, x) \longmapsto ax$, para cada $a, x \in G$. Si y está en la órbita de x, es decir, $y = ax\,, a \in G$, entonces $gy = y$ es equivalente a $gax = ax$, es decir, $(a^{-1}ga)x = x$, por lo que $a^{-1}(Est\ y)a \subset Est\ x$. Por otra parte, si $h \in Est\ x$, como $hx = x$ y $a^{-1}y = x$, entonces $h(a^{-1}y) = a^{-1}y$, lo cual se simplifica a $(aha^{-1})y = y$, es decir, $aha^{-1} \in Est\ y$. Como $aha^{-1} \in Est\ y$, entonces $h \in a^{-1}(Est\ y)a$, por lo que se tiene la otra contención y de esta manera $a^{-1}(Est\ y)a = Est\ x$. En particular, si G actúa transitivamente sobre S, todos los estabilizadores son conjugados, es decir, $Est\ y = a(Est\ x)a^{-1}$, $\forall x, y \in S$, donde $y = ax$.

Sea G un grupo. Decimos que dos acciones, $\mu : G \times S \longrightarrow S$ y $\nu : G \times S' \longrightarrow S'$ son equivalentes si existe una función biyectiva $\alpha : S \longrightarrow S'$ tal que

$$\alpha\,(gx) = g\alpha\,(x)\,, \forall g \in G, x \in S$$

Ahora, si $g \in G$, $x \in S$ y $\alpha\,(x) = x'$, al denotar a $\mu\,(g, x)$ por $T_g x$, se tiene que a $\nu\,(g, \alpha\,(x))$ lo denotamos por $T'_g\,(\alpha\,(x))$. De esta manera, la definición de equivalencia tiene la forma

$$\alpha \circ T_g x = T'_g\,(\alpha\,(x))\,, \forall g \in G, x \in S.$$

Notemos que decir que las acciones η y μ de G en S y de G en S', respectivamente, son equivalentes, es lo mismo que decir que el diagrama

$$\begin{array}{ccccc} & & \eta & & \\ & G \times S & \longrightarrow & S & \\ \rho & \downarrow & & \downarrow & \alpha \\ & G \times S' & \longrightarrow & S' & \\ & & \eta & & \end{array}$$

conmute, donde $\alpha : S \longrightarrow S'$ es una función biyectiva y $\rho : G \times S \longrightarrow G \times S'$ es tal que $(g, s) \longmapsto (g, \alpha\,(s))$, es decir, $\rho := Id_G \times \alpha$.

Sea G un grupo y S un conjunto tal que G actúa transitivamente sobre S. Sea $H = \cap_{x \in S} Est\ x$. Afirmamos que $H \lhd G$ y que G/H actúa sobre S de tal manera que el diagrama

$$\begin{array}{ccc} & \overset{\mu}{\longrightarrow} & \\ G \times S & & S \\ \overline{\rho}\downarrow & \nearrow_{\eta} & \\ G/H \times S & & \end{array}$$

conmuta, donde $\overline{\rho} : G \times S \longrightarrow G/H \times S$ está definida por $(g, s) \longmapsto (\overline{g}, s)$,

donde $\overline{g}$ es la clase de equivalencia de g en G/H. Ahora, por la observación anterior, como G actúa transitivamente sobre S, dado $x \in S$, se tiene que los estabilizadores son conjugados, es decir, si $ax = y$, entonces $Esty = a\,(Estx)\,a^{-1}$. Notemos ahora que

$$H = \cap_{x \in S} Estx = \cap_{g \in G} Estgx = \cap_{g \in G} g\,(Estx)\,g^{-1}$$

teniendo así que $\forall k \in G$

$$\begin{aligned} kHk^{-1} &= k\left(\cap_{g \in G} g\,(Estx)\,g^{-1}\right)k^{-1} = \cap_{g \in G} kg\,(Estx)\,g^{-1}k^{-1} \\ &= \cap_{g \in G}\,(kg)\,(Estx)\,(kg)^{-1} \end{aligned}$$

Ahora, como G es grupo, se tiene que la función $k : G \longrightarrow G$, dada por $g \longmapsto kg$ es una biyección, por lo que

$$\cap_{g \in G}\,(kg)\,(Estx)\,(kg)^{-1} = \cap_{g \in G} g\,(Estx)\,g^{-1}$$

es decir, H es normal en G. De esta manera tenemos que el espacio cociente G/H es un grupo y así podemos definir la siguiente función $\eta : G/H \times S \longrightarrow S$ con regla de correspondencia $(\overline{g}, x) \longmapsto gx$. Notemos que η está bien definida, ya que si $\overline{a} = \overline{b}$, entonces $aH = bH$, lo cual implica que $a = bh$, para alguna $h \in H$. Como $h \in H$, se tiene que para cualquier $x \in S$, $ax = (bh)\,x = b\,(hx) = bx$, por lo que η está bien definida. Ahora, como $H \lhd G$, entonces $\overline{a}\overline{b} = \overline{ab}$, por lo que $\left(\overline{ab}, x\right) \longmapsto (ab)\,x = a\,(bx) = a\left(\overline{b}, x\right)$. Claramente, $(\overline{e}, x) \longmapsto ex = x, \forall x \in S$, por lo que $\overline{G} := G/H$ actúa en S. Por último, si μ denota la acción de G en S, se tiene el siguiente diagrama

$$\begin{array}{lll} & \overset{\mu}{\longrightarrow} & \\ G \times S & & S \\ \overline{\rho}\,\downarrow & \nearrow_{\eta} & \\ G/H \times S & & \end{array}$$

donde $\overline{\rho} := \rho \times Id_S$, donde $\rho : G \longrightarrow G/H$ definida por $g \longmapsto \overline{g}$. Basta notar por último que

$$\mu\,(g, s) = gs = \eta\,(\overline{g}, s) = \eta\,(\overline{\rho}\,(g, s))$$

es decir, $\mu\,(g, s) = \eta \circ \overline{\rho}\,(g, s)\,, \forall\,(g, s) \in G \times S$, por lo que el diagrama conmuta.

Teorema 15 *Sea G un grupo y S un conjunto tal que G actúa transitivamente sobre S. Sea $H = Estx$, para cualquier $x \in S$. Entonces G actúa sobre G/H y la acción de G sobre S es equivalente a la acción de G sobre G/H.*

Demostración. Sea G un grupo y S un conjunto tal que G actúa transitivamente sobre S. Denotemos a dicha acción por μ. Consideremos ahora la función $\beta_x : G \longrightarrow S$ definida por $g \longmapsto gx$, donde $x \in S$. Como G actúa transitivamente sobre S, esta función es sobre, por lo que se tiene una biyección

$\alpha : \overline{G} \longrightarrow S$, donde $\overline{G}$ es el conjunto cociente de G inducido por β_x. Ahora, si $\overline{g} \in \overline{G}$, se tiene que

$$\overline{g} = \{a \in G \mid \beta(a) = \beta(g)\} = \{a \in G \mid ax = gx\}$$

De esta manera, $ax = gx$ es equivalente a decir $g^{-1}ax = x$, es decir, $g^{-1}a \in Estx$. Esto último equivale a decir que $a \in gEstx$, por lo que $\overline{g} = gEstx$, y así, $\overline{G} = G/H$, donde $H = Estx$. Por lo tanto, $\alpha : G/H \longrightarrow S$, definida por $\overline{g} = gEstx \longmapsto gx$, es una biyección inducida por la función β_x.

Por otra parte, consideremos ahora la función $\eta : G \times G/H \longrightarrow G/H$ definida por $(g', gEstx) \longmapsto g'g(Estx)$. Afirmamos que η es una acción. Notemos primero que $(e, gEstx) \longmapsto egEstx = Estx$. Ahora, si $g, g', k \in G$, entonces

$$(gg', kEstx) \longmapsto gg'k(Estx) = g(g'kEstx) = g(g'k(Estx)) = g\eta(g', kEstx)$$

por lo que η es una acción.

Para ver que las acciones η y μ son equivalentes, consideremos el siguiente diagrama:

$$\begin{array}{ccccc} & & \overset{\mu}{} & & \\ & G \times S & \longrightarrow & S & \\ \rho_x = Id_G \times \alpha & \uparrow & & \uparrow & \alpha \\ & G \times G/H & \longrightarrow & G/H & \\ & & \underset{\eta}{} & & \end{array}$$

Sea $(g, g'Estx) \in G \times G/H$. Por una parte,

$$\mu \circ \rho_x(g, g'Estx) = \mu(g, g'x) = gg'x$$

Por otra parte,

$$\alpha \circ \eta(g, g'Estx) = \alpha(gg'(Estx)) = gg'x$$

es decir, $\mu \circ \rho_x(g, g'Estx) = \alpha \circ \eta(g, g'Estx), \forall (g, g'Estx) \in G \times G/H$. De esta manera, el diagrama es conmutativo y por lo tanto $\mu \cong \eta$. ■

Supongamos ahora que G es un grupo finito tal que actúa transitivamente sobre un conjunto S. Por el teorema anterior, para cualquier $x \in S$, G actúa sobre $G/Est\ x$, y por lo tanto, S tiene tantos elementos como clases de equivalencia en G inducidas por $H = Est\ x$, es decir, $|S| = \sum[G : Est\ x]$. En general, podemos aplicar este argumento a cualquier grupo finito G que actúe en un conjunto finito S. En tal caso, S queda partido por las distintas órbitas de elementos de S bajo la acción de G, es decir, podemos ver a S como la unión de subconjuntos ajenos $S = O_1 \cup O_2 \cup \cdots \cup O_n$ donde $O_i \cap O_j = \varnothing, \forall i \neq j$, donde los $O_i's$ son las órbitas de elementos de S bajo la acción de G. En particular, G actúa transitivamente sobre $O_i, \forall i = 1, \ldots, n$, por lo que $|O_i| = [G : Est\ x_i]$. Por lo tanto, $|S| = \sum[G : Est\ x_i]$, donde la suma se toma sobre el conjunto $\{x_1, x_2, \ldots, x_n\}$ de representantes de las distintas órbitas. Notemos que cada $[G : Est\ x_i]$ es divisor de $|G|$.

Proposición 4 *Para cualquier grupo se tiene que* $Est\ axa^{-1} = a(Est\ x)a^{-1}$.

Demostración. *Sea* $z \in Est\ axa^{-1}$. *Entonces* $z(axa^{-1}) = axa^{-1}$. *Multiplicando por* a *y por* a^{-1} *por la derecha e izquierda respectivamente se obtiene* $a^{-1}zax = x$, *lo cual quiere decir que* $a^{-1}za \in Est\ x$. *Pero esto equivale a decir que* $z = a(a^{-1}za)a^{-1} \in a(Est\ x)a^{-1}$, *por lo que* $Est\ axa^{-1} \subset a(Est\ x)a^{-1}$. *Sea* $z \in a(Est\ x)a^{-1}$. *Entonces,* $z = awa^{-1}$ *para algún* $w \in Est\ x$. *Por lo tanto,* $z(axa^{-1}) = awa^{-1}(axa^{-1}) = awxa^{-1} = axa^{-1}$ *pues* $wx = x$. *Por lo tanto,* $z \in Est\ axa^{-1}$, *y entonces* $Est\ axa^{-1} \supset a(Est\ x)a^{-1}$, *obteniendo así la igualdad.* ■

Tomemos ahora la acción de conjugar de un grupo G en sí mismo. En este caso,

$$Estx := C(x) = \{g \in G \mid gxg^{-1} = x\}$$

Al conjunto $C(x)$ se le conoce como el *centralizador de* x, para cada $x \in G$. En general, dado un grupo G, el conjunto

$$C(G) := \{g \in G \mid gx = xg, \forall x \in G\} = \left\{g \in G \mid gxg^{-1} = x, \forall x \in G\right\}$$

se le conoce como el *centralizador de* G. Notemos que $C(G) \leq G$, ya que $e \in C(G)$ y si $g \in C(G)$ entonces $gx = xg$, multiplicando por g^{-1} tanto por la derecha como por la izquierda se tiene $xg^{-1} = g^{-1}x$, es decir, $g^{-1} \in C(G)$.

Regresando a lo anterior, si G actúa por conjugacion en sí mismo, se tiene que $|G| = \sum[G : C(x_i)]$ donde x_i es un representante de la clase de conjugación en G. A esta última ecuación se le conoce como la *ecuación de clases del grupo finito* G. Notemos que si $x_i \in C(G)$, entonces $ax_i = x_ia, \forall a \in G$, por lo que $ax_ia^{-1} = x_i, \forall a \in G$, es decir, $C(x_i) = G$. Para estos elementos, se tiene que $[G : C(x_i)] = [G : G] = 1$, por lo que su clase consta de sólo un elemento. Por lo tanto, la ecuación de clases la podemos modificar por $|G| = |C(G)| + \sum[G : C(y_i)]$, donde las y_i corren en un conjunto de representantes de las clases de conjugación tales que contienen más de un elemento, es decir, tales que $y_i \notin C(G)$ para cada i.

Teorema 16 *Para cualquier grupo finito* G *con orden una potencia de primo se tiene que* $C(G) \neq e$.

Demostración. Sea G un grupo finito tal que $|G| = p^k$, con p primo y $k > 0$.

Como G es finito entonces $|G| = |C(G)| + \sum[G : C(y_i)]$. Ahora, como G tiene orden potencia de p y $C(y_i)$ es un subgrupo de G, para toda y_i representante de la clase de conjugación, cada uno tiene orden una potencia de p. Por otra parte, como $C(y_i) \neq G$, entonces $[G : C(y_i)] > 1$. Como $|G| = |C(y_i)|\,[G : C(y_i)]$, y $[G : C(y_i)] > 1$ entonces también $[G : C(y_i)]$ es una potencia de p, por lo que $p \mid [G : C(y_i)]$. Por lo tanto, como p divide a $[G : C(y_i)]$ para toda y_i, $p \mid |G| - \sum[G : C(y_i)] = |C(G)|$. De esta manera se tiene que $p \mid |C(G)|$, concluyendo que $C(G) \neq e$. ■

0.9. Teoremas de Sylow

Hasta ahora, hemos visto que si $H \leq G$, entonces $|H| \mid |G|$, es decir, $|H|$ es un divisor de $|G|$. Por lo tanto, es natural preguntarnos si lo recíproco es cierto, es decir, si para cualquier k divisor de $|G|$, se tiene un subgrupo H de G con orden k. La respuesta general a esta pregunta es negativa, pero se verá que, para ciertos números sí se cumple dicha proposición.

Definición 9 *Si p es un primo, entonces un $p-$grupo es un grupo tal que todos sus elementos tienen orden potencia de p.*

Empezaremos con un resultado para el caso más sencillo, en donde sólo un primo divide al orden del grupo.

Lema 2 *Si $p \mid |G|$ y G es abeliano, entonces G contiene un elemento de orden p.*

Demostración. Sea $|G| = pk$. La prueba se hará por inducción sobre k. Supongamos que $|G| = p$. Sea $a \in G$, con $a \neq e$. Sabemos que $|\langle a \rangle| \mid |G| = p$, y como $a \neq e$, $|\langle a \rangle| > 1$, por lo que $\langle a \rangle = G$ teniendo así que el orden de a es p. Supongamos que se vale para todo $n < k$, con $pk = |G|$.

Tomemos $a \in G$, con $a \neq e$. Sea r el orden de a y supongamos primero que $p \mid r$. Entonces $pl = r$. Notemos que tanto p como l son menores que r. Consideremos a^l. Como $l < r$ y r es el orden de a, entonces $a^l \neq e$. Además, $(a^l)^p = a^{lp} = a^r = e$. Afirmamos que a^l tiene orden p, ya que si el orden de a^l fuese q, tendríamos que $(a^l)^q = a^{lq} = e$, por lo que $r \mid lq$. Como $pl = r$ y $r \mid lq$ entonces $p \mid q$. Por lo tanto, a^l tiene orden p.

Supongamos ahora que $(r, p) = 1$. Como G es abeliano, entonces $\langle a \rangle$ es un subgrupo normal de G. Consideremos entonces $G/\langle a \rangle$, donde el orden de $G/\langle a \rangle$ es $|G|/r$. Por una parte, $|G| = |\langle a \rangle| [G : \langle a \rangle]$ y como $p \mid |G|$ y $(r, p) = 1$, entonces $p \mid [G : \langle a \rangle]$, que es justamente el orden de $G/\langle a \rangle$. Como $|G/\langle a \rangle| < |G|$ entonces podemos usar la hipótesis de inducción. Por lo tanto, hay un elemento $b\langle a \rangle \in G/\langle a \rangle, b \in G$, tal que $(b\langle a \rangle)^p = \langle a \rangle$. Sea s el orden de b en G. Afirmamos que $p \mid s$, ya que $(b\langle a \rangle)^s = b^s\langle a \rangle = \langle a \rangle$. De esta manera, se tiene que p divide al orden de un elemento en G, encontrándonos en el caso anterior. ■

Ahora, utilizando este último resultado, demostraremos el caso general, es decir, sin pedir que G sea abeliano.

Teorema 17 *Si p es primo y G un grupo finito tal que $p \mid |G|$, entonces G contiene un elemento de orden p.*

Demostración. La prueba se hará por inducción sobre k donde, $|G| = kp$. La demostración para la base es totalmente análoga a la proposición anterior. Supongamos entonces que se vale para todo grupo con orden $k < n = |G|$.

Notemos que si $x \in G$, el número de clases conjugadas de x es justamente $[G : C_x]$, donde C_x es el centralizador de x en G. Si $x \notin C(G)$, entonces el número de clases conjugadas de x tiene más de un elemento, es decir, $[G : C_x] > 1$, por lo que $|C_x| < |G|$. Si $p \mid |C_x|$, entonces por inducción se tiene un elemento de orden p en C_x y por lo tanto también en G. Supongamos entonces que $p \nmid |C_x|$, para toda x en el conjunto de representantes de elementos de G que no están en el centro de G. Como $C_x \leq G$, entonces por Lagrange $|G| = |C_x|\,[G : C_x]$. Como $p \mid |G|$ y $p \nmid |C_x|$, entonces $p \mid [G : C_x]$.

Por otro lado, se tiene a G partido por sus clases conjugadas, teniendo así la ecuación de clases $|G| = |C(G)| + \sum[G : C_{y_i}]$, donde las C_{y_i} son las clases conjugadas con $y_i \notin C(G)$. Como $p \mid [G : C_{y_i}], \forall y_i \notin C(G)$, y p divide a $|G|$, entonces también divide a $C(G) = |G| - \sum[G : C_{y_i}]$. Como $C(G)$ es un subgrupo abeliano de G, por el lema anterior, se tiene un elemento en $C(G) \subset G$ con orden p. ■

Definición 10 *Sea p un primo. Decimos que un subgrupo de G es un $p-$ subgrupo de Sylow si es un $p-$ subgrupo máximo.*

El siguiente teorema nos asegura la existencia de los $p-$*subgrupos* de Sylow.

Teorema 18 *(Sylow I) Si p es primo y $p^k \mid |G|$ entonces existe un subgrupo $H \leq G$ de orden p^k.*

Demostración. La prueba se hará por inducción sobre $|G|$. Si $|G| = 1$ entonces es claro el resultado, pues $p^0 \mid 1$, y en tal caso $H = \{e\} = G$. Supongamos que se vale para todo grupo con orden menor que $n = |G|$. Por una parte, tenemos que $|G| = |C(G)| + \sum[G : C_{y_i}]$, donde $y_i \notin C(G)$ y C_{y_i} es el centralizador de y_i. Como $p^k \mid |G|$ entonces también lo divide p. Ahora, si $p \nmid C(G)$, entonces p no divide a algún sumando de $\sum[G : C_{y_i}]$, por lo que $p \nmid [G : C_{y_i}]$, para alguna i. Como C_{y_i} forma un subgrupo de G, entonces $|G| = |C_{y_i}|\,[G : C_{y_i}]$. Ahora, como $p^k \mid |G|$ y $p \nmid [G : C_{y_i}] = |G| / |C_{y_i}|$, entonces $p^k \mid |C_{y_i}|$. Notando que $|C_{y_i}| < |G|$, por hipótesis de inducción, se tiene que C_{y_i} tiene un subgrupo H de orden p^k. Como $H \leq C_{y_i} \leq G$ entonces $H \leq G$.

Supongamos ahora que $p \mid |C(G)|$. Como $C(G)$ es abeliano y p divide a su orden, entonces por la proposición anterior, $\exists b \in C(G)$ tal que $b^p = e$. Consideremos ahora $\langle b \rangle$. Como $b \in C(G)$, entonces $\langle b \rangle$ es un subgrupo normal de orden p, por lo que $G/\langle b \rangle$ es un grupo de orden $[G : \langle b \rangle]$, es decir, $|G|/p$. Como $p^k \mid |G|$, entonces $p^{k-1} \mid |G|/p = |G/\langle b \rangle|$. Por lo tanto, como $|G/\langle b \rangle| < |G|$, por hipótesis de inducción, $G/\langle b \rangle$ contiene un subgrupo $\overline{H}$ de orden p^{k-1}. Como $\overline{H} \leq G/\langle b \rangle$ entonces $\overline{H} = H/\langle b \rangle$, con $H \leq G$ tal que $|H| = [H : \langle b \rangle]\,|\langle b \rangle| = p^{k-1}p = p^k$. ■

Notemos que si G es un grupo y $H \leq G$ entonces $gHg^{-1} \leq G, \forall g \in G$, por lo que si Λ es el conjunto de subgrupos de G entonces G actúa en Λ bajo conjugación, ya que para todo $H \leq G$, $eHe^{-1} = H$ y $(g_1g_2)\,H\,(g_1g_2)^{-1} = g_1g_2Hg_2^{-1}g_1^{-1} = g_1\left(g_2Hg_2^{-1}\right)g_1^{-1}, \forall g_1g_2 \in G$. En particular, para cada subgrupo

H, $EstH = \left\{g \in G \mid gHg^{-1} = H\right\} := N(H)$ lo definiremos como el *subgrupo normalizador de* H en G, ya que por definición, $H \lhd N(H)$. Por otra parte, dado $H \leq G$ se tiene que $\left|\left\{gHg^{-1} \mid g \in G\right\}\right| = [G : N(H)]$. Esto se sigue viendo que, la función de las clases laterales izquierdas al conjunto de subgrupos de G definida por $f : G/N(G) \longrightarrow \Lambda$ tal que $aN(H) = \overline{a} \longmapsto aHa^{-1}$ es biyectiva. En primer lugar, notemos que

$$\begin{aligned} \overline{a} &= \overline{b} \Longleftrightarrow aN(H) = bN(H) \Longleftrightarrow b^{-1}aN(H) = N(H) \\ &\Longleftrightarrow b^{-1}a \in N(H) \Longleftrightarrow \left(b^{-1}a\right)(H)\left(b^{-1}a\right) = H \\ &\Longleftrightarrow aHa^{-1} = bHb^{-1} \end{aligned}$$

por lo que está bien definida y además es inyectiva. Claramente f es suprayectiva, por lo que f es una biyección.

Ahora, si G es finito y Π es el conjunto de $p-$subgrupos de Sylow, afirmamos que $gPg^{-1} \in \Pi, \forall g \in G$, con lo cual tendríamos que G actúa en Π bajo conjugación. Si $p \in P$, entonces gpg^{-1} sigue teniendo orden potencia de p, por lo que basta demostrar que gPg^{-1} es máximo. Supongamos que $gPg^{-1} \subset P'$, con $P' \in \Pi$. Entonces $P \subset g^{-1}P'g$, donde $g^{-1}P'g$ es un $p-$grupo. Como P es un $p-$grupo de Sylow, entonces es máximo, por lo que $P = g^{-1}P'g$, es decir, $P' = gPg^{-1}$ es un $p-$grupo de Sylow.

Lema 3 *Sea P un $p-$subgrupo de Sylow de G, $H \leq G$ tal que $|H| = p^k$ y $H \subset N(P)$. Entonces $H \subset P$.*

Demostración. Como $P \lhd N(P)$ y $H \leq N(P)$ entonces $HP \leq N(P)$. Además, $H, P \subset HP$. Notemos ahora que $|HP| = |H||P|/|P \cap H|$. Como $P \cap H \leq P$, y el orden de P es una potencia de p, entonces también lo es $|P \cap H|$, por lo que HP es un subgrupo de $N(P) \subset G$, de orden una potencia de p que además contiene a P. Como P es un $p-$subgrupo de Sylow, éste es máximo, por lo que $HP = P$, de lo cual, se tiene que $H \subset P$. ■

Del lema anterior se sigue que P es el único $p-$subgrupo de Sylow de $N(P)$, pues para cualquier $p-$subgrupo $H \subset N(P)$ se tiene que $H \subset P$.

Teorema 19 *(Sylow II) Sea p un primo y G grupo finito tal que p^m es la mayor potencia de p que divide al orden de G. Entonces*

a) Cualesquiera dos $p-$subgrupos de G son conjugados, es decir, si P,Q son $p-$subgrupos de Sylow, entonces existe $g \in G$ tal que $gPg^{-1} = Q$.

(b) El número de $p-$subgrupos de Sylow divide al índice de cualquier $p-$subgrupo de Sylow y es congruente con 1 módulo p.

(c) Si $H \leq G$ tal que $|H| = p^k$ entonces $H \subset P$, para algún $p-$subgrupo de Sylow.

Demostración. Sea Π el conjunto de todos los $p-$subgrupos de Sylow de G. Como gPg^{-1} es un $p-$subgrupo de Sylow, $\forall g \in G$ y $\forall P \in \Pi$, entonces se tiene la acción de conjugar $\gamma : G \times \Pi \longrightarrow \Pi$ definida por $(g, P) \longmapsto gPg^{-1}$ de G sobre Π. De esta manera Π queda partido por las distintas $G-$órbitas. Sea Σ una de ellas y $P \in \Sigma$. Como $\Sigma \subset \Pi$ y G actúa en Π, entonces se tiene

también la acción $\gamma\mid_{P,\Sigma}$: $P\times\Sigma\longrightarrow\Sigma$ definida por $(q,S)\longmapsto qSq^{-1}$, para $q\in P$ y $S\in\Sigma$. De esta manera, Σ queda partido en $P-$órbitas. Afirmamos que la única $P-$órbita de cardinalidad uno es la órbita de P: claramente, para cualquier $q\in P$, $qPq^{-1}=P$, por lo que $|[P]_P|=1$. Ahora, si P' es tal que $|[P']_P|=1$ entonces $\forall q\in P$ se tiene $qP'q^{-1}=P'$, por lo que $P\subset N(P')$. Como P' es el único $p-$subgrupo de Sylow en $N(P')$ y $P\subset N(P')$, entonces $P=P'$. Por otra parte, notemos que cualquier otra $P-$órbita en Σ tiene orden una potencia de p. Sea $S\in\Sigma$ con $S\neq P$ y sea $o(S)$ la órbita de S. Como P actúa sobre Σ, en particular, P actúa transitivamente sobre $o(S)$, por lo que $|o(S)|=[P:H]$, donde $H=Estx$, para cualquier $x\in o(S)$. Como P tiene cardinalidad una potencia de p y $[P:H]\mid|P|$, entonces $|o(S)|=[P:H]=p^r$, para algún $r\in\mathbb{N}$. Ahora, falta ver que $r\geq 1$. Si $r=0$, entonces $|o(S)|=1$, por lo que $pSp^{-1}=S,\forall p\in P$. De esta manera, se tiene que $P\subset N(S)$. Como S es el único $p-$subgrupo de Sylow en $N(S)$, entonces $P=S$, lo cual contradice la hipótesis $S\neq P$. Por lo tanto, $r\geq 1$ y así $o(S)$ tiene tantos elementos como una potencia de p. Ahora, como la cardinalidad de Σ es igual a la suma de cardinalidades de las distintas órbitas en Σ, entonces $|\Sigma|\equiv 1\,(\mathrm{mod}\,p)$, ya que todas excepto una, a saber la órbita de P, tienen como orden una potencia de p y $|[P]_P|=1$. Por lo tanto, se tiene la segunda parte de b). Ahora, si demostramos que G actúa transitivamente en Π, entonces demostraremos que cualesquiera dos $p-$subgrupos de Sylow son conjugados. Para esto, hay que demostrar que $\Sigma=\Pi$. Supongamos que no, es decir, que existe $R\in\Pi\setminus\Sigma$. De manera totalmente análoga, se tiene que R actúa en Σ por conjugación, sólo que esta vez todas las $R-$órbitas tienen cardinalidad una potencia de p, pues $R\notin\Sigma$, por lo que $|\Sigma|\equiv 0\,(\mathrm{mod}\,p)$, lo cual es una contradicción a lo antes notado. Por lo tanto, $\Sigma=\Pi$, y por lo tanto, G actúa transitivamente en Π por conjugación, teniendo así a).

Para la primera parte de b), basta notar que, como $\Sigma=\Pi$ y Σ queda partido por la órbita de P por la acción de conjugar, se tiene que $|\Sigma|=[G:H]$, donde $H=EstP$, para cualquier $P\in\Pi$. Por definición,

$$H=\left\{g\in G\mid gPg^{-1}=P\right\}:=N(P)$$

por lo que $|\Sigma|=[G:N(P)]$. Por otra parte, como G es finito y $P\subset N(P)\subset G$, entonces

$$[G:P]=[G:N(P)]\,[N(P):P]$$

por lo que $[G:N(P)]\mid[G:P]$. Por lo tanto, $|\Sigma|\mid[G:P]$, lo cual demuestra b).

Sea $H\leq G$ tal que $|H|=p^d$. Al restringir la acción de conjugar $\gamma\mid_{H\times\Pi}$: $H\times\Pi\longrightarrow\Pi$ se tiene que Π queda partido en $H-$órbitas. Notemos que las $H-$órbitas tienen cardinalidad una potencia de p, ya que cada una de ellas divide al orden de $H=p^d$. Ahora, como cada $H-$órbita tiene cardinalidad una potencia de p y $|\Pi|\equiv 1\,(\mathrm{mod}\,p)$, entonces existe una $H-$órbita con cardinalidad 1. Si $P\in\Pi$ es tal que $|[P]_H|=1$, entonces $hPh^{-1}=P,\forall h\in H$, por lo que $H\subset N(P)$. Como P es un $p-$subgrupo de Sylow, por el lema anterior, $H\subset P$.
■

Notemos que del teorema anterior, si p es un primo que divide al orden del grupo, entonces el $p-$subgrupo de Sylow asociado al primo p, tiene orden p^m, donde m es la máxima potencia de p que divide al orden del grupo.

Parte II

Anillos

0.10. Tipos de anillos.

En esta sección daremos la definición de la estructura algebraica llamada anillo. Daremos también algunos ejemplos de éstos que nos llevarán a definir lo que es un campo.

Definición 11 *Sea R un conjunto no vacío. Decimos que R es un anillo si existen dos operaciones, $+ : R\times R \longrightarrow R$ y $* : R\times R \longrightarrow R$ tales que $\forall a, b, c \in R$ se cumple que*

1. $a + (b + c) = (a + b) + c$.
2. $a + b = b + a$.
3. *Existe un elemento* $0 \in R$ *tal que* $a + 0 = a, \forall a \in R$.
4. *Dado* $a \in R$, *existe* $b \in R$ *tal que* $a + b = 0$
5. $a * (b * c) = (a * b) * c$.
6. $a * (b + c) = a * b + a * c$, *así como* $(a + b) * c = a * b + a * c$.

Notemos que de la definición, estamos pidiendo que R y la operación suma, $(R, +, 0)$, sea un grupo abeliano, es decir, que la operación $+$ sea asociativa y conmutativa. Por otro lado, se tiene que las dos operaciones están relacionadas por el inciso 6, la cual se conoce como la *ley distributiva.* Al elemento del inciso 3, se le conoce como *neutro aditivo.* Observemos también que en la definición, nunca se menciona a un elemento neutro para la operación $+$. Esto se debe a que existen anillos que no contienen elemento neutro para $*$. A los anillos que sí lo tienen, le llamaremos *anillos con unidad* y denotaremos a este elemento por 1.

Proposición 5 *Para cualquier anillo R, $0 * a = 0, \forall a \in R$.*

Demostración. Como 0 es el neutro aditivo, entonces $0 + 0 = 0$ y también

$0 + a = a, \forall a \in R$. Por lo tanto, se tiene que

$$0 + 0 * a = 0 * a = (0 + 0) * a = 0 * a + 0 * a$$

Como $(R, +, 0)$ es un grupo abeliano, entonces $a*0$ tiene un inverso aditivo. De las igualdades anteriores, se tiene que

$$0 = 0 * a$$

■

Notemos también que, si $1 = 0$, entonces $R = \{0\}$, ya que

$$\forall a \in R,\ 0 = a * 0 = a * 1 = a$$

por lo que $R = \{0\}$. Por otra parte, en algunos anillos, no siempre se cumple que si $a * b = 0$, esto implique que $a = 0$ ó $b = 0$. Cuando esto último sí se cumpla, diremos que el anillo es un *dominio.* De manera análoga, en la definición no se menciona que la operación $*$ sea conmutativa. Para esos tipos de anillos, donde $*$ sea una operación conmutativa, los llamaremos *anillos conmutativos.*

Definición 12 *Un anillo conmutativo R es un dominio integral o dominio entero, si $a * b = 0 \Longrightarrow a = 0$ ó $b = 0$.*

El ejemplo clásico de un dominio integral son los enteros $\mathbb{Z}$. En cambio, no siempre los $\mathbb{Z}_n$, que son las clases de los residuos en $\mathbb{Z}$ después de dividir por n, son dominios enteros. Por ejemplo, si consideramos a $\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{7}\}$ se tiene que $\overline{2}, \overline{4} \neq \overline{0}$ pero $\overline{2} * \overline{4} = \overline{8} = \overline{0}$. Pero si consideramos a los $\mathbb{Z}_p$, con p primo, estos sí son dominios enteros, pues como se verá, estos son más que dominios enteros, son campos.

Notemos que de la definición anterior, decir que R sea un dominio entero es equivalente a decir que $R^* := R \setminus \{0\}$ es un submonoide de $(R, *, 1)$, ya que de esta manera se asegura del hecho de que $a * b \neq 0$, para toda $a, b \in R^*$, la cual es la contrapuesta de la definición de dominio integral.

De ahora en adelante, denotaremos al producto $a * b$ simplemente por ab. Si a es un elemento de R un anillo para el cual existe un elemento $b \neq 0$ tal que $ab = 0$ ($ba = 0$), decimos que a es un divisor izquierdo (derecho) de cero. Claramente, cero es un divisor tanto izquierdo como derecho. También, si $a \neq 0$, es un divisor izquierdo tal que $ab = 0$ con $b \neq 0$, entonces b es un divisor derecho de cero. Por lo tanto, podemos decir que un anillo R es un dominio, si y sólo si, no tiene divisores derechos ni izquierdos a parte del elemento 0. Por otra parte, veamos ahora que R es un dominio si y sólo si $R \neq 0$, y las *leyes de cancelación* se cumplen, es decir, $\forall a \neq 0$, si $ab = ac \Longrightarrow b = c$, y $ba = ca \Longrightarrow b = c$. Si R es un dominio entonces vimos que $R \neq \{0\}$, y si $ab = ac$, entonces $a(b - c) = ab - ac = 0$. Ahora, si $a \neq 0$ entonces $b - c = 0$, lo cual implica que $b = c$. La otra implicación es totalmente análoga. Si $R \neq 0$ es un anillo para el cual las leyes de cancelación son válidas, se tiene que, si $a \neq 0$ es tal que existe $b \in R$ con $ab = 0 = a0$, entonces $b = 0$. Por lo tanto, R es un dominio.

Definición 13 *Un anillo R es un anillo con división si para cualquier $0 \neq a \in R$, existe $b \in R$, tal que $a * b = 1 = b * a$.*

Notemos que no hay ambigüedad en denotar a este elemento b por a^{-1}, ya que si $c \in R$ es otro elemento tal que $ac = 1 = ca$, entonces se tiene que

$$b = 1b = cab = c1 = c$$

Ahora, si R es un anillo con división, entonces $R \neq 0$ y además, si $ab = ac$, entonces, como R es anillo con división, existe $a^{-1} \in R$, por lo que $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = c$, análogamente, $ba = ca \Longrightarrow b = c$. Por lo tanto, R también es un dominio. Por otra parte, en un anillo con división, la ecuación $ax = b$ tiene la solución $x = a^{-1}b$. Como un anillo con división es un dominio y en éste las leyes de cancelación son válidas, entonces esta solución es única. Análogamente para la ecuación $ya = b$, a saber, $y = ba^{-1}$.

Al conjunto U de elementos invertibles de un monoide le llamaremos unidades. Estos claramente forma un subgrupo del monoide, por lo que U es un subgrupo de $(R, *, 1)$. Por ejemplo, el conjunto de unidades en $\mathbb{Z}$ es el conjunto $\{-1, 1\}$.

Definición 14 *Decimos que un anillo R es un campo si R es un anillo con división conmutativo.*

De esta definición se sigue que R es un campo si y sólo si R^* es un grupo. Ahora, para ver que $\mathbb{Z}_p$ es un campo, basta notar que es un anillo con división. Para esto, sea $\overline{a} \in \mathbb{Z}_p$ con $\overline{a} \neq \overline{0}$. Podemos suponer que $0 < a < p$. Entonces $(a, p) = 1$, por lo que existen enteros tales que $an + pk = 1$. Por lo tanto, $\overline{1} = \overline{an + pk} = \overline{an} + \overline{pk} = \overline{an} + \overline{p}\overline{k} = \overline{an} + \overline{0} = \overline{an}$, por lo que $(\overline{a})^{-1} = \overline{n} \neq 0$. Otros ejemplos de campos son los números racionales $\mathbb{Q}$ y los números reales $\mathbb{R}$. Notemos que los $\mathbb{Z}_p$ tienen cardinalidad finita para cualquier primo p, $\mathbb{Q}$ tiene cardinalidad infinita y numerable, y $\mathbb{R}$ también tiene cardinalidad infinita pero no numerable.

Proposición 6 *Cualquier dominio finito es un anillo con división.*

Demostración. Sea R un dominio. Sea $0 \neq a \in R$. Consideremos ahora la función multiplicar por la izquierda por a: $R \longrightarrow R$ definida por $x \longmapsto ax$. Esta función es inyectiva, ya que como R es dominio, por la ley de cancelación, si $ax = ay \Longrightarrow x = y$. Como además R es finito, entonces también es sobre, por lo que existe un $b \in R$ tal que $ab = 1$. Análogamente, para la la función multiplicar por la derecha por a se tiene una $c \in R$ tal que $ca = 1$. Basta ver que $c = b$. Para esto, se tiene que $b = 1b = (ca)b = c(ab) = c1 = c$. ■

0.11. Ideales y anillos cocientes.

Se define una congruencia $\cong$, en un anillo R, como una relación de equivalencia tanto en el grupo aditivo $(R, +, 0)$ como en la parte multiplicativa del monoide $(R, *, 1)$, es decir, una relación de equivalencia tal que si $a \cong a'$ y $b \cong b'$ entonces $a + b \cong a' + b'$ así como $ab \cong a'b'$. Sea $\overline{a}$ la clase de equivalencia de $a \in R$ y $\overline{R}$ el conjunto cociente, es decir, el conjunto de clases de equivalencia dada por la relación $\cong$. Como $\overline{a} + \overline{b} = \overline{a + b}$ y $\overline{a}\overline{b} = \overline{ab}$ entonces las operaciones no dependen de los representantes, por lo que estas definen el grupo $(\overline{R}, +, \overline{0})$ y el monoide $(\overline{R}, *, \overline{1})$ respectivamente. Además, $\overline{a}(\overline{b} + \overline{c}) = \overline{a}(\overline{b + c}) = \overline{a(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a}\overline{b} + \overline{a}\overline{c}$, análogamente, $(\overline{b} + \overline{c})\overline{a} = \overline{b}\overline{a} + \overline{c}\overline{a}$. Por lo tanto, $(\overline{R}, +, *, \overline{0}, \overline{1})$ es un anillo. A este último se le conoce como *anillo cociente*.

Por otra parte, las congruencias en $(R, +, 0)$ son obtenidas por subgrupos I, necesariamente normales pues $(R, +)$ es abeliano, definiendo $a \cong b$ si $a - b \in I$. Si además, la relación $\cong$ es también una congruencia para el monoide multiplicativo, entonces $\forall a \in R$ y $b \in I$ se tiene que $a \cong a$ y $b \cong 0$, por lo que $ab \cong a0 = 0$, análogamente, $ba \cong 0$. Esto quiere decir que para cualquier $a \in R$ se tiene que $ab \in I, \forall b \in I$.

Definición 15 *Si R es un anillo, entonces I es un ideal si es un subgrupo del grupo aditivo de R tal que $\forall a \in R$ y $\forall b \in I$, $ab, ba \in I$.*

Como ejemplo, consideremos al anillo $R = \mathbb{Z}$ y sea $I = n\mathbb{Z}$, es decir, los múltiplos enteros de n. Claramente $n\mathbb{Z}$ es un subgrupo aditivo de $\mathbb{Z}$, ya que $0 = 0n \in n\mathbb{Z}$ y si $a \in n\mathbb{Z}$, entonces $a = nk$, para alguna $k \in \mathbb{Z}$, por lo que $-a = n(-k) \in n\mathbb{Z}$. Falta ver entonces que $\forall a \in \mathbb{Z}$ y $\forall b \in n\mathbb{Z}$ se tiene que $ab, ba \in n\mathbb{Z}$. Si $k \in \mathbb{Z}$ y $l \in n\mathbb{Z}$, entonces $l = nm$, para alguna $m \in \mathbb{Z}$, por lo que $kl = k(nm) = knm = nkm \in n\mathbb{Z}$. Análogamente, $lk \in n\mathbb{Z}$, por lo que $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$.

Supongamos ahora que I es un ideal de R. Si $\cong$ es la congruencia inducida por I, es decir, $x \cong y$ si y sólo si $x - y \in I$, si $a \cong a'$ y $b \cong b'$, entonces $a - a' \in I$, por lo que $(a - a')b \in I$. Análogamente, $b - b' \in I$, por lo que $a'(b - b') \in I$. Como I es un subgrupo aditivo, se tiene que $ab - a'b' = ab - ab + ab' - a'b' = (ab - ab) + (ab' - a'b') \in I$, por lo que $ab \cong a'b'$.

Al anillo cociente $\overline{R}$ de las clases de equivalencia inducidas por I, lo denotaremos por R/I, y lo llamaremos el anillo cociente de R formado por el ideal I. Los elementos de R/I son las clases laterales $a + I$ donde la suma y multiplicación están definidas por $(a+I)+(b+I) = (a+b)+I$ y $(a+I)(b+I) = (ab+I)$, donde el $0+I$, $1+I$ son los neutros para la suma y la multiplicación, respectivamente.

Notemos que la intersección de ideales sigue siendo un ideal. Para esto, primero hay que notar que la intersección arbitraria de subgrupos sigue siendo un subrgupo. Sea $\{G_i\}_{i\in J}$ una familia de subgrupos y $G = \cap\{G_i\}_{i\in J}$. Como $e \in G_i$ para toda $i \in J$, entonces $e \in G$. Ahora, si $a \in G$, entonces $a \in G_i, \forall i \in J$, por lo que $a^{-1} \in G_i, \forall i \in J$. De esta manera, $a^{-1} \in G$ y por lo tanto G es un subgrupo. Sea $J = \cap\{I_k\}_{k\in H}$, con I_k un ideal y H un conjunto de índices. Entonces si $a \in R$ y $b \in J$ se tiene que $b \in I_k . \forall k \in H$ entonces $ab \in I_k \forall k \in H$, por lo que también $ab \in J$. El razonamiento es totalmente análogo para ba, por lo que J es un ideal.

Consideremos ahora un subconjunto $S \subset R$, con R un anillo. Entonces $(S) = \cap I_S$, donde I_S es un ideal que contiene a S, es el ideal más pequeño que contiene a S, es decir, cualquier otro ideal que contiene a S, contiene también a (S). A (S) lo llamaremos el ideal generado por S. Analicemos el caso cuando este conjunto es finito. Si $S = \{a_1, \ldots, a_n\}$ entonces es claro que los elementos de la forma $xa_iy \in (S)$, para cualesquiera $x, y \in R$. Además, se tiene que $x_ia_iy_i + x_ja_jy_j \in (S)$ y no hay manera en ponerlos en un sólo término. Consideremos ahora el conjunto I formado por elementos de la forma $\sum x_{i_1}a_1y_{i_1} + \sum x_{i_2}a_2y_{i_2} + \cdots \sum x_{i_n}a_ny_{i_n}$. Por una parte, se tiene que $I \subset (S)$. Además, por la manera en que se construyó, claramente I es un ideal que además contiene a S, viendo que $1a_i1 = a_i$. Por lo tanto, $I = (S)$.

Sean I, J ideales en un anillo R. Entonces el ideal generado por $I \cup J$ lo denotaremos por $I + J$. Afirmamos que este conjunto está formado por lo elementos de la forma $a+b$ tales que $a \in I$ y $b \in J$. Sea $K = \{a + b \mid a \in I, b \in J\}$. claramente $I \subset K$ y $J \subset K$, tomando $b = 0$ y $a = 0$ respectivamente. Además, K es un ideal, ya que para cualquier $r, s \in R$, $ras \in I, rbs \in J$, por lo que $r(a+b)s = (ra+rb)s = ras+rbs \in K$. Por lo tanto, K es un ideal que contiene

a I y J y que además, por la manera en que se construyó, está contenido en cualquier ideal que contenga a I, J, por lo que $K = I + J$.

De manera análoga, consideremos ahora el producto IJ. En primer lugar, $IJ = \{ab \mid a \in I, b \in J\}$, por lo que sumas de la forma $a_1b_1 + \cdots + a_mb_m$ están en el ideal generado por IJ. Si $K = \{a_1b_1 + \cdots + a_mb_m \mid a_i \in I, b_i \in J\}$ entonces si $r, s \in R$, $r(a_1b_1 + \cdots + a_mb_m)s = ra_1b_1s + \cdots + ra_mb_ms$. Como $ra_i \in I$ y $b_is \in J$, entonces $ra_ib_is \in IJ$, por lo que K es un ideal. Notemos también que K contiene a IJ. Por la manera en que se construyó K, se tiene que está contenido en cualquier ideal que contenga a IJ. Por lo tanto, $K = (IJ)$.

Teorema 20 *Sea R un anillo conmutativo distinto a 0. Entonces R es un campo si y sólo si sus únicos ideales son $I = R$ o $I = 0$.*

Demostración. Sea R un anillo con división e I un ideal de R. Claramente el ideal $I = 0$ está contenido en R, por lo que podemos supongamos que $I \neq 0$. Sea $0 \neq a \in I$. Entonces $1 = a^{-1}a \in I$, por lo que cualquier $r \in R$ también está en I, ya que $r = r1 \in I$. Por lo tanto, los únicos ideales son $I = 0$ o $I = R$. Como este argumento se tomó para R, un anillo con división, en particular se cumple si R es un campo.

Supongamos ahora que $R \neq 0$ es un anillo conmutativo tal que sus únicos ideales son $I = 0, R$. Sea $0 \neq a \in R$. Entonces $(a) = R$, por lo que $1 \in (a)$. Esto quiere decir que existe $b \in R$ tal que $ab = ba = 1$, ya que R es un anillo conmutativo. Notemos que $b \neq 0$, por lo que cualquier elemento tiene un inverso multiplicativo. Por lo tanto, R es un campo. ■

Definición 16 *Decimos que I es un ideal máximo de un anillo R si $I \neq R$, y no existe un ideal propio J de R que contenga propiamente a I.*

Del teorema anterior, se tiene que, si R es un campo entonces $I = \{0\}$ es su único ideal máximo. Para el próximo teorema, necesitaremos de la siguiente

Definición 17 *Un homomorfismo $\eta : R \longrightarrow R'$, entre los anillos R y R', es una función que cumple ser un homomorfismo entre el grupo aditivo y monoide multiplicativo de R al correspondiente grupo aditivo y monoide multiplicativo de R'.*

Recordemos que μ es un homomorfismo entre los grupos G y G' si $\mu(ab) = \mu(a)\mu(b)$ y μ manda al neutro de G en el neutro de G'. En el siguiente capítulo daremos las propiedades básicas de los homomorfismos entre anillos. Por ahora, daremos el siguiente

Ejemplo 2 *Sea R un anillo y M un ideal máximo. Consideremos la función $\Pi : R \longrightarrow R/M$ definida por $a \longmapsto \overline{a}$, donde $\overline{a} = a + M \in R/M$. Notemos primero que $0 \longmapsto \overline{0} = 0 + M = M$, el cual es el neutro de $(R/M, +)$. Si $a, b \in R$, entonces*

$$a + b \longmapsto \overline{a + b} = (a + b) + M = (a + M) + (b + M) = \overline{a} + \overline{b}$$

Por otra parte, como la multiplicación en R/M no depende de los representantes, se tiene que

$$ab \longmapsto \overline{ab} = ab + M = (a + M)(b + M) = \overline{a}\overline{b}$$

Claramente, $e \longmapsto \overline{e} = e + M$, el cual es el neutro multiplicativo en R/M. Por lo tanto, Π es un homomorfismo de anillos.

Al homomorfismo Π lo llamaremos *homomorfismo canónico.*

Teorema 21 *Sea R es un anillo conmutativo. Entonces M es un ideal máximo de R si y sólo si R/M es un campo.*

Demostración. Sea M un ideal máximo de R. Como R es un anillo conmutativo, R/M también es un anillo conmutativo con unidad $M \neq R$, pues M es máximo. Para ver que R/M es un campo, basta demostrar que para cualquier elemento existe un inverso. Sea $a + M \in R/M$ tal que $a \notin M$. Consideremos el conjunto $N = \{ra + m \mid r \in R \text{ y } m \in M\}$. Claramente $(N, +, 0)$ es un grupo pues $(ra + m) + (sa + n) = ((r + s)a + (m + n)) \in N$, $0a + 0 = 0 \in N$ y las operaciones son heredadas por el grupo $(R, +, 0)$. Ahora, como $r_1(ra + m) = (r_1 r)a + r_1 m \in N$, pues $r_1 m \in M$, se tiene que N es un ideal de R. Como además $a = 1a + 0 \in N$ y para cualquier $m \in M$, $m = 0a + m \in N$ se tiene que $M \subsetneq N$. Como M es máximo, $N = R$. En particular $1 \in N$, es decir, $1 = ba + m$, para alguna $b \in R$. Por lo tanto, $1 + M = ba + M = (b + M)(a + M)$, es decir, $(b + M)$ es el inverso multiplicativo de $a + M$.

Supongamos ahora que R/M es un campo. Si N un ideal de R tal que $M \subsetneq N \neq R$ y $\gamma : R \longrightarrow R/M$ es el homomorfismo canónico se tiene que $\gamma(N)$ es un ideal de R/M tal que $\{(0 + M)\} \subset \gamma(N)$. Esto se sigue notando que si $a + M \in \gamma(N)$ y $b + M \in R/M$ entonces $a \in N$ y $b \in R$, por lo que $ab \in N$. Por lo tanto, $(a + M)(b + M) = ab + M \in \gamma(N)$. De manera análoga, $ba + M \in \gamma(N)$. Como R/M es un campo, por el resultado anterior, los únicos ideales de R/M son el total y el trivial. Como $N \neq R$, $\gamma(N)$ tiene que ser el ideal trivial, es decir, $\gamma(N) = \{0 + M\} = M$. Pero esto quiere decir que $N \subset M$, lo cual contradice la hipótesis de $M \subsetneq N$. Por lo tanto, M es máximo en R. ■

Corolario 4 *Un anillo conmutativo R es un campo si y sólo si no tiene ideales propios no triviales.*

Demostración. Como notamos anteriormente, si R es un campo, entonces $I = \{0\}$ el único ideal máximo, por lo que R no puede contener un ideal $N \subsetneq R$.

Ahora, si R es un anillo conmutativo tal que no contiene ideales propios no triviales, se tiene que el conjunto $I = \{0\}$ es un ideal y además es máximo. Por lo tanto, $R/I = R/\{0\} \cong R$ es un campo por el teorema anterior. ■

Como hemos visto, R/M es un campo si y sólo si M es máximo en R. Si ahora queremos que el cociente R/M sea un dominio entero, surge la pregunta de qué es lo que se necesita pedirle a M. Notemos que R/M es un dominio si $(a + M)(b + M) = M$ si y sólo si $a+M = M$ o $b+M = M$, es decir, que R/M no tenga divisores de cero. Si consideramos al producto $(a + M)(b + M) = ab+M$, se tiene que $M = ab + M$ si $ab \in M$. Esto nos conduce a la siguiente

Definición 18 *Un ideal $N \neq R$ de un anillo conmutativo se llama ideal primo si $ab \in N$ implica que $a \in N$ o $b \in N$.*

De esta definición, se tiene el siguiente

Teorema 22 *Sea R un anillo conmutativo y $N \neq R$ un ideal. Entonces R/N es un dominio entero si y sólo si N es un ideal primo.*

Demostración. Como vimos anteriormente, si R/N es un dominio entonces $(a+N)(b+N) = N \Longleftrightarrow a+N = N$ o $b+N = N$. Si tomamos a representantes de las clases, esto equivale a decir que $ab \in N \Longleftrightarrow a \in N$ o $b \in N$, lo cual es la propiedad de que N sea un ideal primo.

Como N es un ideal, el cociente R/N es un anillo que también es conmutativo. De manera análoga, para cualquier $(a+N), (b+N) \in R/N$ se tiene que si $(a+N)(b+N) = ab+N = N$, entonces $ab \in N$, por lo que $a \in N$ o $b \in N$. Por lo tanto, $a+N = N$ o $b+N = N$, lo cual demuestra que R/N es un dominio. ■

Corolario 5 *Cualquier ideal máximo M en un anillo conmutativo R es un ideal primo.*

Demostración. Esto se sigue de que si M es ideal máximo entonces R/M es un campo, en particular es un dominio, por lo que M también es ideal primo. ■

Cerraremos esta sección demostrando que cualquier ideal propio I de un anillo R está contenido en un ideal máximo M de R. Si I es máximo, entonces no hay nada que demostrar. Supongamos entonces que I no es máximo. Definamos al conjunto $S = \{J \mid J \text{ es un ideal tal que } I \subsetneq J \subsetneq R\}$. Notemos que $S \neq \varnothing$ ya que I no es máximo. Ordenemos a S con la relación $\leq$ definida por $F \leq J$, si $F \subset J$. Como $J \subset J$ entonces $J \leq J$, por lo que es reflexiva. Si $F \leq J$ y $J \leq F$ entonces $F \subset J$ y $J \subset F$, por lo que $F = J$, es decir, $\leq$ es antisimétrica. Por último, si $F \leq J$ y $J \leq G$ entonces $F \subset J$ y $J \subset G$, por lo que $F \subset G$, es decir, $F \leq G$. Como $\leq$ es una relación de orden, tenemos que S queda parcialmente ordenado por $\leq$. Sea $C = \{J_i\}_{i \in I}$ una cadena de elementos en S. Sea $J = \cup_{i \in I} J_i$. Claramente $J \subset R$. Si $r \in R$ y $j \in J$, entonces $j \in J_i$ para alguna $i \in I$, por lo que $rj \in J_i \subset \cup_{i \in I} J_i = J$. Análogamente, $jr \in J$. Como esto se cumple para cualquier $r \in R$ y $j \in J$, se tiene que J es un ideal de R. Además, $I \subset J_i \subset \cup_{i \in I} J_i = J$ para cualquier J_i, por lo que $I \subset J$. Notemos que esta contención es propia, ya que si $I = J$, entonces se tendría que $I \subsetneq J_i \subset J = I$, lo cual implica que $I \subsetneq I$, lo cual es una contradicción. Afirmamos ahora que $J \subsetneq R$. En caso contrario, tendríamos que $1 \in J$. Como $J = \cup_{i \in I} J_i$, entonces $1 \in J_i$ para algún ideal $J_i \in S$, pero esto equivale a decir que $J_i = R$, lo cual contradice la hipótesis de que $J_i \subsetneq R$. Por lo tanto, cualquier cadena en S tiene una cota superior. Como el conjunto S está parcialmente ordenado por $\leq$ y cada cadena tiene un elemento máximo, por el lema de Zorn, S tiene un elemento

máximo M, es decir, existe un ideal M de R tal que $I \subset M \subsetneq R$ y para el cual no existe algún ideal $N \subsetneq R$ que contenga propiamente a M. Esto da por finalizada la demostración.

0.12. Homomorfismos de anillos.

Sea $\eta : R \longrightarrow R'$ un homomorfismo entre los anillos R y R'. Entonces $\eta(ab) = \mu(a)\mu(b)$, $\eta(a+b) = \eta(a) + \eta(b)$ y $\eta(1) = 1'$, donde $1'$ es la unidad de R'. En particular, si I es un ideal en R, podemos formar el anillo cociente $\overline{R} = R/I$, en donde se tiene el homomorfismo canónico $\mu : R \longrightarrow \overline{R}$ con regla de correspondencia $a \longmapsto \overline{a}$, es decir, a cada elemento en R lo mandamos a su clase de equivalencia en $\overline{R}$. Claramente esta función es sobre, por lo que μ es un epimorfismo de R a $\overline{R}$. Como en el caso de grupos, definimos a $K = \mu^{-1}(0)$ como el *kernel* de μ. Entonces se tiene una congruencia módulo K, a saber, $a \cong b$ si $a - b \in K$. Veamos que en efecto, K forma un ideal en R. Si $a, b \in K$, entonces $\mu(a+b) = 0 + 0 = 0$, por lo que $a + b \in K$. Claramente $-a \in K$, $\forall a \in K$, por lo que K es un subgrupo de la parte aditiva de R. Ahora, si $a \in K$ y $r \in R$, entonces $\mu(ar) = \mu(a)\mu(r) = 0\mu(r) = 0$, por lo que $ar \in K$. Análogamente $ra \in K$, por lo que K es un ideal de R. Por otra parte, μ es monomorfismo si y sólo si $\ker \mu = \{0\}$ y la imagen de cualquier homomorfismo de un anillo R a R', es un subanillo de R' puesto que éste es un subgrupo y submonoide de la parte aditiva y multiplicativa de R' respectivamente.

Sea $\mu : R \longrightarrow R'$ un homomorfismo e I un ideal contenido en $K = \ker \mu$. Como I es un ideal, se tiene el anillo cociente R/I, en donde podemos definir la función $\overline{\mu} : R/I \longrightarrow R'$ por $a + I \longmapsto \mu(a)$. Veamos que está bien definida: si $a \cong b (\mathrm{mod}\, I)$, entonces $a - b \in I \subset K$, por lo que $\mu(a) - \mu(b) = \mu(a - b) = 0$, por lo que $\mu(a) = \mu(b)$. Por otra parte, como I es un ideal, entonces la suma y multiplicación de elementos está bien definida, por lo que $\overline{\mu}$ es un homomorfismo de grupo y monoide, es decir, es un homomorfismo de anillos. A $\overline{\mu}$ le llamaremos el homomorfismo inducido por μ del anillo R/I a R'. De las observaciones anteriores, se tiene que el siguiente diagrama es conmutativo

$$\begin{array}{ccc} & \overset{\mu}{} & \\ R & \longrightarrow & R' \\ {\scriptstyle \nu}\downarrow & \nearrow_{\overline{\mu}} & \\ R/I & & \end{array}$$

donde $\overline{\mu}$ es el único homomorfismo de R/I a R' que hace conmutativo el diagrama. Notemos también que $\overline{\mu}$ es monomorfismo si y sólo si I coincide con el $\ker \mu$: Si $I \subsetneq K$, entonces existe un $a \in K$ tal que $a \notin I$. Como $a \notin I$, entonces $a + I \neq 0 + I$, pero como $a \in K$, $\mu(a) = \mu(0)$, por lo que μ no es inyectiva; supongamos ahora que $I = K = \ker \mu$. Si $\mu(a) = \mu(b)$, entonces $\mu(a - b) = \mu(a) - \mu(b) = 0$, por lo que $a - b \in K = I$, es decir, $a \cong b (\mathrm{mod}\, I)$, por lo que μ es inyectiva. En este caso, se tiene el siguiente

Teorema 23 *(Teorema fundamental de homomorfismos de anillos) Sea η un homomorfismo entre los anillos R y R' con $K = \eta^{-1}(0)$. Entonces K es un ideal*

de R y se tiene un único homomorfismo $\overline{\eta}$ de R/K a R' tal que $\mu = \nu\overline{\mu}$, donde ν es el homomorfismo natural de R a R/K. Además, ν es un epimorfismo y $\overline{\mu}$ monomorfismo.

Como resultado inmediato, se tiene el siguiente

Corolario 6 *Cualquier imagen homomórfica de un anillo R, es isomorfo a un anillo cociente R/K de R, con K un ideal.*

El siguiente teorema se conoce como el primer teorema de isomorfismos para anillos:

Teorema 24 *Sea η un epimorfismo entre los anillos R y R' con kernel K. Entonces, en la correspondencia uno a uno entre el conjunto de subgrupos H de $(R, +, 0)$ que contienen a K con el conjunto de subgrupos de R', que manda a H a $\eta(H)$; se tiene que H es un anillo(ideal) si y sólo si, $\eta(H)$ es un anillo(ideal). Más aún, si I es un ideal de R que contiene a K, entonces la función $\mu : R/I \longrightarrow R'/I'$ dada por $a + I \longmapsto \eta(a) + I'$ es un isomorfismo, donde $I' = \eta(I)$.*

Demostración. Sea $\eta : R \longrightarrow R'$ un epimorfismo con kernel K. Ya vimos que la imagen de un anillo bajo cualquier homomorfismo es un subanillo del contradominio, por lo que si restringimos η a un subanillo H de R, se tiene que su imagen, $\eta(H)$, es un subanillo de R'. Sea H un ideal que contiene a K. Como H es un subgrupo de la parte aditiva de R, $\eta(H)$ es también un subgrupo de $(R', +, 0')$. Si $h' \in \eta(H)$ y $x' \in R'$ entonces existen $h \in H$ y $x \in R$ tales que $\eta(x) = x'$ y $\eta(h) = h'$, por lo que $h'x' = \eta(h)\eta(x) = \eta(hx) \in \eta(H)$, ya que η es sobre y $hx \in H$. Análogamente, $x'h' \in \eta(H)$, por lo que $\eta(H)$ es un ideal en R'.

Supongamos ahora que H' es un subanillo de R'. Veamos que $\eta^{-1}(H')$ también es un subanillo: Si $a, b \in \eta^{-1}(H')$ entonces $\eta(a), \eta(b) \in H'$, por lo que $\eta(a+b) \in H'$, es decir, $a + b \in \eta^{-1}(H')$. Si $a \in \eta^{-1}(H')$, entonces $\eta(a) \in H'$. Como H' es un subanillo, y $\eta(a) \in H'$, entonces $-\eta(a) \in H'$, pero $\eta(-a) = -\eta(a)$, por lo que $-a \in \eta^{-1}(H')$. Por lo tanto, $\eta^{-1}(H')$ es un subgrupo de la parte aditiva de R. Por otra parte, como η es epimorfismo y $1' \in H'$, entonces $1 \in \eta^{-1}(H')$ y si, $a, b \in \eta^{-1}(H')$, entonces $\eta(a), \eta(b) \in H'$, por lo que $\eta(ab) = \eta(a)\eta(b) \in H'$, es decir, $ab \in \eta^{-1}(H')$. Por lo tanto $\eta^{-1}(H')$ es un subanillo. Sean $x \in R$ y $y \in \eta^{-1}(H')$. Como H' es un ideal, entonces $\eta(xy) = \eta(x)\eta(y) \in H'$, por lo que $xy \in \eta^{-1}(H')$. Análogamente, $yx \in \eta^{-1}(H')$, teniendo así que $\eta^{-1}(H')$ es un ideal en R.

Por lo tanto, se tiene una correspondencia biunívoca entre los subgrupos que contienen a K de la parte aditiva de R con los subgrupos de la parte aditiva de R', la cual induce una correspondencia biyectiva entre los ideales de R que contienen a K con los ideales de R'.

Sea I un ideal de R tal que $K \subset I$. Consideremos el siguiente diagrama:

$$\begin{array}{ccc} & \eta & \\ R & \longrightarrow & R' \\ \nu \downarrow & & \downarrow \nu' \\ R/I & \longrightarrow & R'/I' \end{array}$$

donde $\nu(a) = a + I$, $\nu'(a') = a' + I'$, e $I' = \eta(I)$.

Sea $\mu : R/I \longrightarrow R'/I'$ definida por $a + I \longmapsto \eta(a) + I'$. De la teoría de grupos, se tiene que μ es un isomorfismo entre los grupos aditivos de R/I y R'/I' si y sólo si, I es un subgrupo normal que contiene a K, del grupo aditivo de R, e $I' = \eta(I)$. Como I es un ideal de R, entonces μ es un isomorfismo entre los grupos aditivos de R/I y R'/I'. Por último, como I e I' son ideales, se tiene que $(a + I)(b + I) = (ab + I) \longmapsto \eta(ab) + I' = \eta(a)\eta(b) + I' = (\eta(a) + I')(\eta(b) + I')$, donde además, $1 + I \longmapsto \eta(1) + I' = 1' + I'$, teniendo así que μ es un isomorfismo de anillos. ■

Teorema 25 *(Segundo Teorema de Isomorfismos para anillos). Sea R un anillo, S un subanillo e I un ideal de R. Entonces $S + I := \{s + i \mid s \in S,\ i \in I\}$ es un subanillo de R que contiene a I como ideal, $S \cap I$ es un ideal de S. Además, la función $\zeta : S + I \longrightarrow S/S \cap I$, definida por $s + I \longmapsto s + S \cap I$ es un homomorfismo tal que define un isomorfismo entre $S + I/I$ y $S/S \cap I$.*

Demostración. Veamos primero que $S + I$ es un anillo. Para esto, hay que ver que $(S + I, +, 0)$ es un subgrupo abeliano y que $(S + I, *, 1)$ es un submonoide, ya que la ley distributiva se sigue de que $S + I \subset R$ y que el producto y suma son operaciones cerradas. Sean $s + i \in S + I$. Como $s \in S$ e $i \in I$ entonces $-s \in S, -i \in I$, por lo que $(s + i) + ((-s) + (-i)) = 0$, por lo que cualquier elemento tiene inverso. Además, es claro que las suma de elementos de $S + I$ es cerrada, por lo que $(S + I, +, 0)$ es un subgrupo de $(R, +, 0)$. Ahora, si $r + j \in S + I$, como I es un ideal, se tiene que $(s + i) * (r + j) = sr + sj + ir + ij = sr + (sj + ir + ij) \in S + I$, teniendo así que el producto es cerrado. Claramente, el elemento $1 + 0 = 1 \in S + I$ es el neutro y además, para cualquier $i \in I$, se tiene que $0 + i = i \in S + I$. Por lo tanto, $S + I$ es un subanillo que contiene a I. Como I es un ideal de R, entonces también es un ideal de cualquier subconjunto de R que lo contenga, por lo que también es un ideal de $S + I$.

Sea $\phi : R \longrightarrow R/I$ el homomorfismo que manda a cada $r \in R$ en su clase módulo I, es decir, $r \longmapsto r + I$. Sea η la restricción de ϕ a S. Entonces $\eta : S \longrightarrow (S + I)/I$. El kernel de η está formado por elementos de S tales que van a dar a I, es decir, las $s \in S$ tales que $s + I = I$, en otras palabras, tales que $s \in I$. Por lo tanto, $\ker \eta = S \cap I$. De esta manera, se tiene que $S/S \cap I \cong (S + I)/I$, por lo que $\overline{\eta} : S/S \cap I \longrightarrow (S + I)/I$ definida por $s + (S \cap I) \longmapsto s + I$ es un isomorfismo. Notemos por último que $\zeta = \overline{\eta}^{-1}$. ■

Ahora aplicaremos el teorema fundamental de homomorfismos de anillos para encontrar el anillo más pequeño de un anillo R, es decir, el anillo generado por el elemento 1. A este anillo le llamaremos el *anillo primo* de R. Por el momento, usaremos al anillo $\mathbb{Z}$ con unidad 1 y denotaremos al elemento e como el neutro de R. Consideremos la siguiente función de $\mathbb{Z}$ a R definida por la regla $n \longmapsto ne$, es decir, sumar n veces el neutro e de R. Como $(n + m)e = ne + me$, $(nm)e = (ne)(me)$ y $1 \longmapsto e$ se tiene que esta función es un homomorfismo entre los anillos $\mathbb{Z}$ y R, por lo que la imagen $\mathbb{Z}e = \{ne \mid n \in \mathbb{Z}\}$ es un subanillo de R.

Notemos que si S es un subanillo de R entonces $e \in S$, por lo que $\mathbb{Z}e \subset S$. Por lo tanto, $\mathbb{Z}e$ es nuestro anillo primo. Por otra parte, este último homomorfismo lo podemos considerar como uno a $\mathbb{Z}e$, por lo que éste sería un epimorfismo, teniendo así que $\mathbb{Z}e \cong \mathbb{Z}/K$, con K un ideal de $\mathbb{Z}$. Como los únicos ideales en $\mathbb{Z}$ son los generados por $\langle k \rangle = \{kn \mid n \in \mathbb{Z}\}$, con $k \geq 0$, se tiene que si $k = 0$, entonces $\mathbb{Z}e \cong \mathbb{Z}/0 \cong \mathbb{Z}$, y si $k > 0$ entonces $\mathbb{Z}e \cong \mathbb{Z}/\langle k \rangle$, es decir, al anillo de residuos módulo k.

Regresaremos ahora a la notación usual, donde 1 es el neutro para el anillo R, e identificaremos a los anillos primos con $\mathbb{Z}$ o $\mathbb{Z}/k$, cuando sea el caso. Por lo observado anteriormente, se tiene el siguiente

Teorema 26 *Para cualquier anillo R, su anillo primo es $\mathbb{Z}$ o $\mathbb{Z}/\langle k \rangle$, para algún $0 < k \in \mathbb{N}$.*

Recordemos que si k es un número compuesto, es decir, $k = lm$, entonces $\mathbb{Z}/\langle k \rangle$ tiene divisores de cero. Si R es un dominio, se sigue entonces que los únicos anillos primos posibles son $\mathbb{Z}$ o $\mathbb{Z}/\langle p \rangle$, con p primo. Decimos que R tiene **característica** k cuando su anillo primo es $\mathbb{Z}/\langle k \rangle$, para $k \geq 0$. Por lo tanto, R es dominio si y sólo si es de característica 0 o p, con p primo.

Proposición 7 *Sea R un anillo con división y η un homomorfismo de R . Entonces η también es un monomorfismo.*

Demostración. Para demostrar la proposición, notemos lo siguiente: Sea φ un homomorfismo de R tal que $\ker \varphi \neq \{0\}$. Sea $0 \neq a \in \ker \varphi$. Como R es un anillo con división, se tiene que $a^{-1} \in R$. Por lo tanto, como $1 = aa^{-1}$ y φ es un homomorfismo, se tiene que $\varphi(1) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) = 0\varphi(a^{-1}) = 0$. Por otra parte, como $b = b1, \forall b \in R$, se tiene que $\varphi(b) = \varphi(b1) = \varphi(b)\varphi(1) = \varphi(b)0 = 0$, por lo que $\varphi \equiv 0$. Por lo tanto, hemos probado que si φ es un homomorfismo de R tal que $\ker \varphi \neq \{0\}$, entonces $\varphi \equiv 0$. La contrapuesta de esta proposición, es que si η es un homomorfismo no trivial del anillo con división R, entonces $\ker \eta = \{0\}$, que es lo que queríamos demostrar. ■

0.13. El campo cociente de un dominio conmutativo.

Hemos visto que cualquier anillo con división es también un domino, por lo que cualquier subanillo de un anillo con división, es también un dominio. Nos preguntamos si lo recíproco también es cierto, es decir, si cualquier dominio puede ser insertado en un anillo con división, o lo que es equivale, dado un dominio D, exista un monomorfismo de D a un anillo con división F, ya que de esta manera, se tendría una copia D' en F de D, la cual puede ser pensada como nuestro dominio inicial D. En la sección, veremos que la respuesta es afirmativa si se toma la condición que D sea un dominio conmutativo. Durante muchos

años, este fue un problema abierto hasta que A. Malcev dió el primer ejemplo de un dominio que no puede ser insertado en algún anillo con división.

Empezaremos suponiendo que D es un subanillo de un campo K. Sea F el subcampo generado por D, es decir,

$$D = \cap\{E \mid D \subset E \text{ y } E \text{ es un subcampo de } K\}$$

Veamos que forma tiene F. Si $b \in D$ y $b \neq 0$ entonces $ab^{-1} \in F$ para toda $a \in D$. Demostraremos que, en efecto, F es el conjunto de elementos de la forma ab^{-1}, con $b \neq 0$. Notemos primero que el conjunto $\left\{ab^{-1} \mid a, b \in D \text{ y } b \neq 0\right\}$ es un subcampo de F:

$ab^{-1} + cd^{-1} = adb^{-1}d^{-1} + cbb^{-1}d^{-1} = (ad + cb)b^{-1}d^{-1} = (ad + bc)(db)^{-1}$, ya que $b, d \neq 0 \Longrightarrow bd \neq 0$,

$0b^{-1} = 0, \forall b \in D,\ b \neq 0$,

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

$(ab^{-1})(cd^{-1}) = acb^{-1}d^{-1} = ac(b^{-1}d^{-1}) = ac(db)^{-1}$

$aa^{-1} = 1$

Si $a \neq 0$, $(ab^{-1})^{-1} = (ba^{-1})$.

Nótese que en los pasos anteriores se usa la conmutatividad en el producto. Como F está generado por D, y $D \subset \left\{ab^{-1} \mid a, b \in D \text{ y } b \neq 0\right\}$, pues $a = a1 = a1^{-1}$, se tiene que $F = \left\{ab^{-1} \mid a, b \in D \text{ y } b \neq 0\right\}$. De esta manera, se tiene que los elementos de F tienen la forma ab^{-1}, con $b \neq 0$, pero no sabemos si están representados de una o más maneras, es decir, si $ab^{-1} = cd^{-1}$, con $a, b, c, d \in D$ y $b, d \neq 0$. Notemos que $ab^{-1} = cd^{-1}$ si y sólo si $ad = cb$, ya que la primera implicación se obtiene al multiplicar $ab^{-1} = cd^{-1}$ por bd y la segunda multiplicando $ad = cb$ por $(bd)^{-1} = d^{-1}b^{-1}$. Esto nos definirá más adelante una relación de equivalencia en el conjunto $D \times D^*$.

Sea D un dominio conmutativo. Por las observaciones anteriores, si D puede ser incrustado en algún campo, los elementos del campo F, generado por D, los podemos pensar como parejas ordenadas (a, b) con $b \neq 0$, ya que estos tienen la forma ab^{-1}, con $a, b \in D$ y $b \neq 0$.

Sea D^* el conjunto de elementos distintos de cero de D. Como $D \neq 0$ entonces $D^* \neq 0$. Consideremos ahora las parejas ordenadas (a, b) del producto $D \times D^*$, y definamos la relación $\backsim$ por $(a, b) \backsim (c, d)$ si y sólo si $ad = bc$. Afirmamos que $\backsim$ es una relación de equivalencia: claramente es reflexiva, pues $ab = ba$, ya que D es un dominio conmutativo, por lo que $(a, b) \backsim (a, b)$; si $(a, b) \backsim (c, d)$ entonces $ad = bc$, lo cual implica que $cb = da$, es decir, $(c, d) \backsim (a, b)$, por lo que es simétrica; si $(a, b) \backsim (c, d)$ y $(c, d) \backsim (e, f)$, con $b, d, f \neq 0$, se tiene que $ad = bc$ y $cf = de$. Multiplicando la primera igualdad por f, el cual por hipótesis es distinto a 0, se tiene que $afd = adf = bcf = bde = bed$. Como D es un dominio, entonces se valen las leyes de cancelación para elementos distintos de cero, por lo que $afd = bed \Longrightarrow af = be$, lo cual equivale a decir que $(a, b) \backsim (e, f)$, teniendo así que $\backsim$ es transitiva.

A la clase de equivalencia determinada por la pareja (a, b) la llamaremos la fracción $\frac{a}{b}$. Por lo tanto, tenemos que $\frac{a}{b} = \frac{c}{d}$ si y sólo si $ad = bc$. Sea $F = \left\{\frac{a}{b}\right\}$, el conjunto de fracciones definidas por la relación de equivalencia $\backsim$ en

$D \times D^*$. Introduciremos ahora dos operaciones en F, correspondientes a suma y producto, con elementos distinguidos cada uno, para hacerlo un campo. Notemos primero que si $\frac{a}{b}, \frac{c}{d} \in F$ entonces $bd \neq 0$, ya que $b, d \neq 0$. De esta manera, podemos definir el elemento $\frac{(ad+bc)}{bd}$. Supongamos que $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$. Entonces $ab' = ba'$ y $cd' = dc'$. Multiplicando la primera igualdad por dd' y la segunda por bb' se tiene $ab'dd' = ba'dd'$ y $cd'bb' = dc'bb'$, por lo que $ab'dd' + cd'bb' = ba'dd' + dc'bb'$, es decir, $(ad + cb)d'b' = (a'd' + c'b')bd$, lo cual implica que $\frac{(ad+cb)}{bd} = \frac{(a'd'+c'b')}{b'd'}$. De esta manera, queda claro que la operación $+ : F \longrightarrow F$, definida por $\frac{a}{b} + \frac{c}{d} \longmapsto \frac{ad+bc}{bd}$ está bien definida y no depende de los representantes. Por otra parte, si $\frac{a}{b}, \frac{c}{d}$ son fracciones entonces también lo es $\frac{ac}{bd}$, pues $b, d \neq 0$. Para ver que el producto de fracciones también está bien definido, supongamos que $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$. Entonces, $\frac{ac}{bd} = \frac{a'c'}{b'd'} \iff acb'd' = a'c'bd$. Como $ab' = ba'$ y $cd' = dc'$ entonces multiplicando la primera ecuación por cd' y usando la segunda ecuación se tiene que $acb'd' = (ab')cd' = (ba')cd' = (ba')dc' = a'c'bd$, por lo que $\frac{ac}{bd} = \frac{a'c'}{b'd'}$, es decir, está bien definido el producto. Por lo tanto, se tiene la operación $\bullet : F \longrightarrow F$ definida por $\frac{a}{b} \bullet \frac{c}{d} \longmapsto \frac{ac}{bd}$. Si denotamos a $\frac{0}{1} = 0 \in F$ y $\frac{1}{1} = 1 \in F$ se tiene que para cualquier $\frac{a}{b} \in F$, $\frac{a}{b} + 0 = \frac{a}{b} + \frac{0}{1} = \frac{a1+b0}{b1} = \frac{a}{b}$, y $\frac{a}{b} \bullet 1 = \frac{a}{b} \bullet \frac{1}{1} = \frac{a1}{b1} = \frac{a}{b}$. De manera análoga se tiene que $0 + \frac{a}{b} = \frac{a}{b}$ y $1 \bullet \frac{a}{b} = \frac{a}{b}$. Por lo tanto, $0, 1 \in F$ son los neutros aditivos y multiplicativos, respectivamente.

Notemos que, con la manera en que se definió la suma y el producto en F, y que, tanto la suma como el producto en D son conmutativos, se tiene que $\forall \frac{a}{b}, \frac{c}{d} \in F$,

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} = \frac{bc + ad}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b}$$

y

$$\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} * \frac{a}{b}$$

es decir, la suma como el producto en F son conmutativos. Por lo tanto, para afirmar que $(F, +, \bullet, 0, 1)$ es un anillo, falta demostrar que la ley distributiva se cumple en F. Si $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$, con $b, d, f \neq 0$, entonces $\frac{a}{b}(\frac{c}{d} + \frac{e}{f}) = \frac{a}{b}(\frac{cf+de}{df}) = \frac{a(cf+de)}{b(df)}$. Como D es un dominio conmutativo, entonces se vale la ley distributiva, por lo que $\frac{a(cf+de)}{b(df)} = \frac{acf+ade}{bdf}$. Por otra parte, $\frac{a}{b} \bullet \frac{c}{d} + \frac{a}{b} \bullet \frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{acbf+aebd}{bdbf} = \frac{b(acf+ade)}{b(bdf)}$. Notemos que como $b \neq 0$, entonces $\frac{b}{b} = \frac{1}{1}$, ya que $b = b1 = 1b = b.$, por lo que $\frac{b(acf+ade)}{b(bdf)} = \frac{b}{b} \bullet \frac{acf+ade}{bdf} = \frac{1}{1} \bullet \frac{acf+ade}{bdf} = \frac{acf+ade}{bdf}$, demostrando así que $\frac{a}{b} \bullet \frac{c}{d} + \frac{a}{b} \bullet \frac{e}{f} = \frac{a}{b}(\frac{c}{d} + \frac{e}{f})$. La demostración de la distributividad por la izquierda es totalmente análoga.

Supongamos ahora que $\frac{a}{b} \in F$ es tal que $\frac{a}{b} \neq 0$. Entonces $a \neq 0 \in D$, ya que de lo contrario, $\frac{0}{b} = \frac{0}{1} = 0$ pues $01 = 0 = 0b$. Por lo tanto, $\frac{b}{a} \in F$ y además, es tal que $\frac{a}{b} \bullet \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{1}{1} = 1 \in F$. Análogamente, $\frac{b}{a} \bullet \frac{a}{b} = \frac{1}{1} \in F$. Por lo tanto, $(\frac{a}{b})^{-1} = \frac{b}{a}$. Consideremos ahora la función $\kappa : D \longrightarrow F$ definida por $a \longmapsto \frac{a}{1}$. Claramente, $1 \longmapsto \frac{1}{1} = 1 \in F$ y $0 \longmapsto \frac{0}{1} = 0 \in F$. Además, $(a + b) \longmapsto \frac{a+b}{1} = \frac{a1+1b}{1*1} = \frac{a}{1} + \frac{b}{1}$, donde $*$ es el producto en D, y $ab \longmapsto \frac{ab}{1} = \frac{ab}{1*1} = \frac{a}{1} \bullet \frac{b}{1}$,

por lo que κ es un homomorfismo. Notemos que κ es inyectiva, ya que si $a \in D$ es tal que $\frac{a}{1} = 0 \in F$ entonces $\frac{a}{1} = \frac{0}{1}$ se tiene que $a = a1 = 01 = 0$, por lo que $\ker \kappa = \{0\}$. De esta manera, hemos demostrado el siguiente

Teorema 27 *Cualquier dominio conmutativo D puede ser incrustado en un campo F.*

De esta manera, identificaremos a cada elemento $a \in D$ con $\frac{a}{1} \in F$, teniendo así un subanillo de F que es isomorfo a D. Más aún, si $\frac{a}{b} \in F$, entonces $\frac{a}{b} = \frac{a}{1} \bullet \frac{1}{b} = \frac{a}{1} \bullet (\frac{b}{1})^{-1}$, el cual corresponde al elemento ab^{-1}, ya que por la manera en que se identificó, si $0 \neq b \longmapsto \frac{b}{1}$ entonces $b^{-1} \longmapsto (\frac{b}{1})^{-1} = (\frac{1}{b})$. Por lo tanto, D genera al campo F. Al campo F lo llamaremos *el campo cociente o campo de fracciones de D.*

Teorema 28 *Sea D un dominio conmutativo y F su campo cociente. Si $\eta : D \longrightarrow F'$ es un monomorfismo a cualquier campo F', entonces η tiene una única extensión a un monomorfismo $\mu : F \longrightarrow F'$.*

Demostración. Sea $\eta : D \longrightarrow F'$ un monomorfismo tal que a cada $D \ni a \longmapsto a'$. Veremos primero que si η puede ser extendida a un homomorfismo de F a F', ésta se hace de sólo una manera, es decir, si se puede hacer, ésta es de manera única. Supongamos que η_F es una extensión de η. Notemos que si $b \neq 0$ y η manda a $b \longmapsto b'$, entonces $b^{-1} \longmapsto (b')^{-1}$ bajo η_F, por lo que $ab^{-1} \longmapsto a'(b')^{-1}$ bajo η_F. Como cada elemento de F lo podemos escribir como ab^{-1}, se sigue que η_F está determinada por los valores que toma en ab^{-1}, es decir, tiene la regla de correspondencia $ab^{-1} \longmapsto a'(b')^{-1}$. Por lo tanto, sólo falta ver que $ab^{-1} \longmapsto a'(b')^{-1}$ está bien definido y que es un monomorfismo que extiende a η.

Supongamos que $a(b)^{-1} = c(d)^{-1}$. Esto quiere decir que $ad = bc$, con $a, b, c, d \in D$. Como η es homomorfismo, $a'd' = b'c'$, lo cual implica que $a'(b')^{-1} = c'(d')^{-1}$, lo cual demuestra que la correspondencia está bien definida. Para ver que es un homomorfismo, sean $a, b, c, d \in D$ con $b, d \neq 0$. Entonces, como D es un dominio conmutativo, se tiene que:

$$ab^{-1} + cd^{-1} = (ad + cb)(db)^{-1} \longmapsto (a'd' + c'b')(d'b')^{-1} = (a'd' + c'b')(d')^{-1}(b')^{-1}$$
$$= a'd'(d')^{-1}(b')^{-1} + c'b'(d')^{-1}(b')^{-1} = a'(b')^{-1} + c'(d')^{-1} = \eta_F(ab^{-1}) + \eta_F(cd^{-1})$$

y

$$(ab^{-1})(cd^{-1}) = ac(b^{-1}d^{-1}) = ac(bd)^{-1} \longmapsto a'c'(b'd')^{-1} = a'c'(b')^{-1}(d')^{-1}$$
$$= a'(b')^{-1}c'(d')^{-1} = \eta_F(ab^{-1})\eta_F(cd^{-1})$$

Como D y F tienen el mismo elemento 1 como unidad, y η es un monomorfismo de D a F', se sigue que $\eta_F(1) \longmapsto 1'$, la unidad de F'. Además, como cada $a \in D$ lo podemos ver como $a1^{-1}$, entonces se tiene que $a = a1^{-1} \longmapsto a'1' = a'$, por lo que η_F extiende a η. Por un resultado anterior que afirma que, cualquier homomorfismo de un campo F es también un monomorfismo, se tiene que $\mu = \eta_F$ es el único monomorfismo de $F \longrightarrow F'$ que extiende a η. ■

0.14. Anillos de Polinomios

A lo largo de esta sección supondremos siempre que R es un anillo conmutativo. Sean R' un anillo y R un subanillo. Si U es un subconjunto de R', consideraremos al subanillo de R' generado por R y por el conjunto U, es decir,

$$R[U] := \cap\{S \mid S \text{ es un subanillo de } R' \text{ tal que } R \subset S \text{ y } U \subset S\}$$

Notemos que esta intersección es distinta del vacío ya que $R' \in \{S \mid S$ es un subanillo de R' tal que $R \subset S$ y $U \subset S\}$. A este subanillo lo llamaremos el anillo que se obtiene adjuntando U al subanillo R. Si $V \subset R'$, entonces $R[U][V]$ es el subanillo que se obtiene del subanillo $R[U]$ al adherirle V. Afirmamos que $R[U][V] = R[U \cup V]$. Por una parte, como $R[U]$ contiene tanto a R como a U, entonces $R[U][V]$ contiene a R y a $U \cup V$, por lo que $R[U \cup V] \subset R[U][V]$. Por otra parte, $R[U][V]$ es el subanillo generado por $R[U]$ y V. Como $R[U][V]$ está contenido en cualquier subanillo que contenga tanto a $R[U]$ como a V, se tiene que $R[U][V] \subset R[U \cup V]$, por lo que $R[U][V] = R[U \cup V]$.

Nos interesaremos por ahora en subanillos obtenidos del anillo base R adheriéndole un conjunto finito U. En este caso, $R[U] = R[u_1, \ldots, u_n]$, donde $U = \{u_1, \ldots, u_n\}$. Por lo visto anteriormente, $R[u_1, \ldots, u_n] = R[u_1][u_2] \cdots [u_n]$, es decir, $R[u_1, \ldots, u_n]$ se obtiene de R por una sucesión de adiciones de un sólo elemento al subanillo previamente construído. Por lo tanto, veremos primero la forma que tiene R al adherirle un sólo elemento u. Como $R[u]$ es un subanillo que contiene a u, entonces también contiene a cualquier potencia de éste, así como el producto de un elemento de R por alguna potencia de u, es decir, $R[u]$ contiene cualquier elemento de la forma $a_i u^k$, donde $a_i \in R$ y $k \in \mathbb{N}$. Como además $R[u]$ es cerrado bajo la operación suma, se tiene que los polinomios en u con coeficientes en R, es decir, los elementos de la forma $a_n u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0$ donde $a_i \in R, \forall i$ y $n \in \mathbb{N}$, están en $R[u]$. Por otra parte, si $\sum_{i=1}^{n} a_i u^i$ y $\sum_{j=1}^{m} b_j u^j$ son dos polinomios en u con coeficientes en R, con $n \leq m$, entonces

$$(a_0 + a_1 u + \cdots + a_n u^n) + (b_0 + b_1 u + \cdots + b_m u^m)$$

$$= (a_0 + b_0) + (a_1 + b_1)u + \cdots + (a_n + b_n)u^n + b_{n+1}u^{n+1} + \cdots + b_m u^m$$

y como $(a_i u^i)(b_j u^j) = a_i b_j u^{i+j}$, por las leyes distributivas se tiene que

$$\begin{aligned} & (a_0 + a_1 u + \cdots + a_n u^n)(b_0 + b_1 u + \cdots + b_m u^m) \\ = \quad & p_0 + p_1 u + p_2 u^2 + \cdots + p_{n+m} u^{n+m} \end{aligned}$$

donde $p_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j+k=i} a_j b_k$. Además, 0 y 1 son polinomios en u, pues $0 = 0u$ y $1 = 0u+1$ y $-\sum_{i=1}^{n} a_i u^i = \sum_{i=1}^{n} (-a_i)u^i$. Por lo tanto, el conjunto de polinomios en u con coeficientes en R forma un subanillo de R'. Como éste subanillo es tal que está contenido en $R[u]$ y contiene tanto a R como a u, por la manera en que se definió $R[u]$, se tiene que coincide justamente con éste, es decir, $R[u]$ es el anillo de polinomios en la variable u con coeficientes en R.

Nuestra siguiente pregunta surge al decidir cuándo dos expresiones en u representan al mismo elemento, por ejemplo, si $u \in R$, el elemento $u \in R[u]$ puede ser representado como a_0, donde $a_0 = u$, o por $a_1 u$, con $a_1 = 1$. Otro ejemplo de esto, se obtiene al tomar $R = \mathbb{C}$,$R = \mathbb{R}$, y $u = \sqrt{-1}$, teniendo así que -1 tiene como representaciones $a_0 = -1$ y $u^2 = -1$. Construiremos ahora un anillo $R[x]$ donde las únicas relaciones de la forma $a_0 + a_1 u + \cdots + a_n u^n = b_0 + b_1 u + \cdots + b_m u^m$, son las triviales, es decir, si y sólo si $a_i = b_i$ para toda i, es decir, el anillo que estamos buscando es el conjunto de expresiones $a_0 + a_1 x + \cdots + a_n x^n$ donde la igualdad de elementos se identifica con la igualdad de coeficientes. La suma y multiplicación es totalmente análoga como se vió anteriormente, reemplazando x por u. Como cada polinomio es de grado finito, entonces se tiene una sucesión de los coeficientes de cada polinomio, en donde, a partir de una n, todos son cero, es decir, podemos identificar a cada polinomio con una sucesión $(a_1, \dots, a_n, 0, 0, \dots)$ con $a_i \in R$.

Sea R un anillo y sea $R[x]$ el conjunto de sucesiones infinitas $(a_1, a_2, a_3, \dots)$ que sólo tienen una cantidad finita de elementos distintos de cero. Decimos que las sucesiones $(a_1, a_2, a_3, \dots)$ y $(b_1, b_2, b_3, \dots)$ son iguales si $a_i = b_i$ para toda i. En otras palabras, $R[x]$ es el conjunto de funciones de $\mathbb{N}$ a R tal que $i \longmapsto a_i$ y donde $a_k = 0$ para toda k mayor que una $N \in \mathbb{N}$. Esta N depende de cada polinomio, es decir, para cada función $f : \mathbb{N} \longrightarrow R$ existe una $N_f \in \mathbb{N}$ tal que si $a_i > N_f$ entonces $a_i = 0$. Definimos la operación $+$ por coordenadas, es decir,

$$(a_1, a_2, a_3, \dots) + (b_1, b_2, b_3, \dots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \dots) \in R[x]$$

y al elemento 0 lo describiremos como $(0, 0, 0, \dots)$. De esta manera, es claro que $(R[x], +, 0)$ es un grupo abeliano, pues $a_i + b_i = b_i + a_i$ y el cero es el neutro aditivo para R, por lo que $a + 0 = a = 0 + a$. Introduciremos ahora una operación multiplicativa, dada por

$$(a_1, a_2, a_3, \dots) * (b_1, b_2, b_3, \dots) = (p_1, p_2, p_3, \dots)$$

donde p_i es la suma antes vista. Notemos que si $a_i = 0$ para $i > n$ y $b_j = 0$ para $j > m$ entonces para $k > n + m$, $p_k = \sum_{i+j=k} a_i b_j = 0$, ya que para cualquier término $a_{i_0} b_{j_0}$ se tiene que $i_0 + j_0 = k$. Si $i_0 \leq n$, entonces $j_0 = k - i_0 > (n + m) - n = m$, por lo que $j_0 = 0$. El caso $j_0 < m$, es totalmente análogo. De esta manera, la sucesión $(p_1, p_2, p_3, \dots) \in R[x]$. También denotamos a $1 = (1, 0, 0, \dots)$, y es tal que para cualquier

$$(a_0, a_1, \dots) * (1, 0, 0, \dots) = (a_0, a_1, \dots) = (1, 0, 0, \dots) * (a_0, a_1, \dots)$$

viendo así que es el neutro multiplicativo.

Sean $A = (a_0, a_1, \dots), B = (b_0, b_1, \dots), C = (c_1, c_2, \dots) \in R[x]$. Entonces el término $i-$ésimo del producto $(AB)C$ es la suma

$$\sum_{\substack{j+k=m \\ m+l=i}} (a_j b_k) c_l = \sum_{j+k+l=i} (a_j b_k) c_l$$

Análogamente, el término correspondiente a $A(BC)$ es

$$\sum_{j+k=i} a_j(\sum_{m+l=k} b_m c_l) = \sum_{j+m+l=i} a_j(b_m c_l)$$

Como el producto en R es asociativo, esto demuestra que $(AB)C = A(BC)$.

Consideremos ahora el producto $A(B+C)$. Notemos que el $i-$ ésimo término tiene la forma $\sum_{j+k=i} a_j(b_k + c_k)$. Como cada $a_j(b_k + c_k) \in R$, entonces $a_j(b_k+c_k) = a_j b_k + a_j c_k, \forall j, k$, por lo que esta última suma la podemos ver como $\left(\sum_{j+k=i} a_j b_k + \sum_{j+k=i} a_j c_k\right)$, donde $\sum_{j+k=i} a_j b_k$ y $\sum_{j+k=i} a_j c_k$ son los coeficientes del $i-$ésimo término de AB y AC respectivamente, pero que en conjunto es el $i-$ésimo término de la suma $AB + AC$. La otra igualdad es similar.

Por otra parte, la conmutatividad del producto en $R[x]$ se sigue de la definición de los p_i's y de que el producto en R es también conmutativo. Por lo tanto, $(R[x], +, *, 0, 1)$ es un anillo conmutativo.

Consideremos ahora la función $\phi : R \longrightarrow R[x]$ definida por $\phi(a) \longmapsto a' = (a, 0, 0, \dots)$. Por la definición de igualdad en $R[x]$, ϕ es inyectiva y además cumple con ser un homomorfismo, ya que $\phi(a+b) = (a+b, 0, 0, \dots) = (a, 0, 0, \dots) + (b, 0, 0, \dots) = \phi(a) + \phi(b)$ y $1 \longmapsto 1 = (1, 0, 0, \dots)$. Por lo tanto, $R[x]$ contiene una copia de R. De esta manera, podemos pensar que R es un subanillo de $R[x]$, teniendo en cuenta que ahora los elementos de R tienen la forma a'. Denotemos ahora al elemento $(0, 1, 0, 0, \dots) := x$. Notemos que

$$x^2 = x * x = (0, 1, 0, 0, \dots) * (0, 1, 0, 0, \dots) = (0, 0, 1, 0, 0, \dots)$$

entonces por inducción, suponiendo que $x^k = (0, \dots, 0, 1, 0, \dots)$ donde el 1 está en el lugar $k+1$, se tiene que

$$x^{k+1} = x^k * x = (0, \dots, 0, 1, 0, \dots) * (0, 1, 0, 0, \dots) = (p_1, p_2, \dots)$$

Notemos que todos los p_i son cero excepto p_{k+2}, ya que en x^{k+1}, el término $j-$ésimo es cero para toda $j > k+1$ y en x, el término $m-$ésimo es cero para toda $m > 1$, por lo que en el producto, si $i > k+2 = (k+1)+1$, por lo visto anteriormente, $p_i = 0$. Ahora, si $i \leq k+1$, basta fijarnos en los productos que tengan al 1 de x. Como 1 es la segunda coordenada de x que corresponde al término lineal, se tiene que en el producto de p_i, este va asociado con la coordenada $i-1$ de x^k, la cual es cero ya que $i-1 \leq k$. Si $i = k+2$ entonces el único producto distinto de cero es cuando se toma el uno de x^k, que está en la posición $k+1$ y el 1 de x, el cual es el segundo término de la sucesión. Cualquier otro producto en la suma p_{k+2} es cero, ya que el término asociado a x^k es cero por tener índice menor que $k+1$. Por lo tanto, $x^{k+1} = (0, 0, \dots, p_{k+2} = 1, 0, \dots)$.

Si $a \in R$, el cual está asociado con $a' = (a, 0, 0, \dots)$ entonces $a * x^k = (0, 0, \dots, a, 0, \dots)$ donde a está en el lugar $k+1$ en la sucesión. De esta manera, podemos ver a $(a_0, a_1, \dots, a_n, 0, \dots)$ como el polinomio $a_0 + a_1 x + \cdots + a_n x^n$. Por lo tanto, $R[x]$ es el anillo formado por R al pegarle x, al cual llamaremos *el anillo de polinomios sobre R en la variable indeterminada x*. De la fórmula anterior de la definición de igualdad se tiene que $\sum_{i=1}^n a_i x^i = \sum_{i=1}^n b_i x^i$, si

y sólo si $a_i = b_i, \forall i$, en particular, $\sum_{i=1}^{n} a_i x^i = 0 \Leftrightarrow a_i = 0, \forall i$. El siguiente teorema, se conoce como la *propiedad universal del anillo* R, y dice lo siguiente:

Teorema 29 *Sean R y S anillos conmutativos, $\eta : R \longrightarrow S$ un homomorfismo y $u \in S$. Sea $R[x]$ el anillo de polinomios en la variable indeterminada x. Entonces η se puede extender a uno y sólo un homomorfismo de $R[x]$ a S tal que $x \longmapsto u$.*

Demostración. Sea $\eta : R \longrightarrow S$ un homomorfismo de anillos y $u \in S$. Entonces se tiene el siguente diagrama

$$\begin{array}{ccccc} & & i & & \\ R & \hookrightarrow & R[x] & & \\ & \searrow & \downarrow & & \eta_u \\ & \eta & S & & \end{array}$$

donde $i : R \longrightarrow R[x]$ es la inmersión. Esto nos ayuda a definir la siguiente función: $\eta_u : R[x] \longrightarrow S$ dada por $a_0 + a_1 x + \cdots + a_n x^n \longmapsto \eta(a_0) + \eta(a_1)u + \cdots + \eta(a_n)u^n$. Veamos entonces que η_u es un homomorfismo. Si $A(x) = a_0 + a_1 x + \cdots + a_n x^n$ y $B(x) = b_0 + b_1 x + \cdots + b_m x^m$ entonces $A(x)B(x) = p_0 + p_1 x + \cdots + p_{n+m} x^{n+m}$, donde $p_i = \sum_{j+k=i} a_j b_k$. Ahora, como η es un homomorfismo, entonces $\eta(p_i) = \eta(\sum_{j+k=i} a_j b_k) = \sum_{j+k=i} \eta(a_j)\eta(b_k)$, por lo que

$$\eta_u(A(x)B(x)) = \eta(p_0)u + \eta(p_1)u + \cdots + \eta(p_{n+m})u^{n+m}$$

$$= \eta(\sum_{j+k=0} \eta(a_j)\eta(b_k)) + \eta(\sum_{j+k=1} \eta(a_j)\eta(b_k))u + \cdots + \eta(\sum_{j+k=m+m} \eta(a_j)\eta(b_k))u^{n+m}$$

Por otra parte, desarrollando $\eta_u(A(x))\eta_u(B(x))$ se tiene

$$\begin{aligned} &= (\eta(a_0) + \eta(a_1)u + \cdots + \eta(a_n)u^n)(\eta(b_0) + \eta(b_1)u + \cdots + \eta(b_m)u^m) \\ &= p'_0 + p'_1 u + \cdots + p'_{n+m} u^{n+m} \end{aligned}$$

donde $p'_i = \sum_{j+k=i} \eta(a_j)\eta(b_k)$, con lo cual se tiene que

$$\eta_u(AB(x)) = \eta_u(A(x))\eta_u(B(x))$$

Si $C(x) = A(x) + B(x)$ entonces, suponiendo sin pérdida de generalidad que $n > m$, se tiene que $C(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + (a_{m+1})x^{m+1} + \cdots + a_n x^n$. Aplicándole η_u a $C(x)$ se obtiene el polinomio $\eta(a_0 + b_0) + \eta(a_1 + b_1)u + \cdots + \eta(a_m + b_m)u^m + \eta(a_{m+1})u^{m+1} + \cdots + \eta(a_n)u^n$. Como η es un homomorfismo, entonces $\eta(a + b) = \eta(a) + \eta(b)$, teniendo así que esta última suma se puede separar como $\eta(a_0) + \eta(a_1)u + \cdots + \eta(a_n)u^n + \eta(b_0) + \eta(b_1)u + \cdots + \eta(b_m)u^m = \eta(A(x)) + \eta(B(x))$, lo cual demuestra que también es un homomorfismo para la operación aditiva. Notemos ahora que $\eta_u(1) = \eta(1) = 1$,la unidad de S, $\eta_u(r) = \eta(r), \forall r \in R$, por lo que η_u extiende a η y que $\eta_u(x) = \eta(1)u = 1u = u$. Por lo tanto, η_u es un homomorfismo de $R[x]$ que extiende a η y que manda a x en u. Como $R[x]$ está generado por R y por x, entonces el homomorfismo η_u, con dicha propiedad, es único. ■

Corolario 7 *$R[u] \cong R[x]/I$ donde x es una variable indeterminada e I es un ideal de $R[x]$ tal que $I \cap R = \{0\}$.*

Demostración. Sea R un anillo y $\mu := Id : R \longrightarrow R$ la función identidad. Sea $u \in R$. Por el teorema anterior, μ se puede extender a un homomorfismo μ_u :

$R[x] \longrightarrow R$ donde $x \longmapsto u$, es decir, $a_0+a_1x+\cdots+a_nx^n \longmapsto a_0+a_1u+\cdots+a_nu^n$. Como $u \in R$, entonces $a_iu^i \in R$ para toda i, por lo que $a_0+a_1u+\cdots+a_nu^n \in R$. Notemos que la imagen de este nuevo homomorfismo μ_u, es $R[u]$, por lo que $R[x]/I \cong R[u]$, con $I = \ker \mu_u$. Como μ_u es la extensión de la identidad, entonces $\mu_u(r) = r, \forall r \in R$, por lo que $I \cap R = \{0\}$.

Supongamos ahora que I es un ideal de $R[x]$ tal que $I \cap R = \{0\}$. Consideremos ahora el homomorfismo $\pi : R[x] \longrightarrow R[x]/I$. Como $I \cap R = \{0\}$, entonces el homomorfismo $\pi \mid_R : R \longrightarrow R[x]/I$ es inyectivo. De esta manera, podemos identificar a R con su imagen en $R[x]/I$, es decir, a cada $a \in R$ le asociamos la clase $a + I \in R[x]/I$, por lo que podemos pensar a $R \subset R[x]/I$ como un subanillo de este espacio cociente. Como $R[x]$ está generado por R y por x, su imagen homomorfa sobre π, está generada por $R \subset R[x]/I$ y por $u = x + I$, teniendo así que $R[x]/I \cong \operatorname{Im} \pi = R[u]$. ■

Por este corolario, en el problema de relacionar dos polinomios en $R[u]$ se sigue notando que $a_0 + a_1u + a_2u^2 + \cdots = b_0 + b_1u + b_2u^2 + \cdots$ si y sólo si $\sum (a_i - b_i) x^i = \sum a_ix^i - \sum b_ix^i = 0$, en otras palabras, $\sum a_ix^i \equiv \sum b_ix^i (\operatorname{mod} I)$, por lo tanto, las relaciones en $R[u]$, dependen del ideal $I = \ker Id_u$.

Notemos que el homomorfismo $\mu : R[x] \longrightarrow R[u]$ con regla de correspondencia $A(x) \longrightarrow A(u)$ es monomorfismo, si $A(u) = 0 \Longrightarrow A(x) = 0$, es decir, $a_0 + a_1u + \cdots + a_nu^n = 0$ implica que $a_i = 0$ para toda i. Si u es tal que $A(x) \longrightarrow A(u)$ es un monomorfismo, decimos que u es *trascendente sobre* R, en caso contrario, decimos que u es *algebráico sobre* R. A continuación, veremos la generalización del teorema anterior para una cantidad finita de indeterminadas.

Teorema 30 *Para cualquier anillo R y número natural n, existe un anillo $R[x_1, \ldots, x_n]$ con la siguiente propiedad universal: Si S es un anillo y η un homomorfismo de R a S, e $i \longmapsto u_i$ es una regla de correspondencia entre $\{1, \ldots, n\}$ a S, entonces existe una única extensión de η, que denotaremos $\eta_{u_1,\ldots,u_n} : R[x] \longrightarrow S$, tal que manda a $x_i \longmapsto u_i$, con $1 \leq i \leq n$.*

Demostración. La prueba se hará por inducción. Primero, definiremos inductivamente a $R[x_1, \ldots, x_n] : R[x_1]$ es el anillo de polinomios en la variable indeterminada x_1 sobre R, y en general, $R[x_1, \ldots, x_i] = R[x_1, \ldots, x_{i-1}][x_i]$, es decir, es el anillo de polinomios en la variable indeterminada x_i sobre el anillo de polinomios $R[x_1, \ldots, x_{i-1}]$. Por el teorema pasado, tenemos un homomorfismo $\eta_{u_1} : R[x_1] \longrightarrow S$ tal que extiende a η y manda $x_1 \longmapsto u_1$. Supongamos entonces que se tiene un homomorfismo $\eta_{u_1,\ldots,u_{n-1}} : R[x_1, \ldots, x_{n-1}] \longrightarrow S$, tal que extiende a η y manda a $x_i \longmapsto u_i$ para $1 \leq i \leq n-1$. De nuevo, por el teorema anterior, podemos extender a $\eta_{u_1,\ldots,u_{n-1}}$ a un homomorfismo $\eta_{u_1,\ldots,u_n}$

de $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ a S tal que $x_i \longmapsto u_i$, $\forall i \in \{1, \ldots, n\}$. Como $\eta_{u_1,\ldots,u_n}$ es una extensión de $\eta_{u_1,\ldots,u_{n-1}}$, la cual, por hipótesis de inducción es extensión de η, tenemos que $\eta_{u_1,\ldots,u_n}$ también es una extensión de η. La unicidad de $\eta_{u_1,\ldots,u_n}$ se sigue de que $R[x_1, \ldots, x_n]$ está generado por R y por x_i, con $1 \leq i \leq n$. ■

Por otra parte, veamos que el anillo con la propiedad del teorema anterior es único salvo isomorfismos. Supongamos que $R[y_1, \ldots, y_n]$ es otro anillo que cumple lo anterior, entonces, para $\eta := i : R \hookrightarrow R[x_1, \ldots, x_n]$, se tiene un homomorfismo $\zeta : R[y_1, \ldots, y_n] \longrightarrow R[x_1, \ldots, x_n]$ tal que $\zeta \mid_R = Id_R = i_R$ y que manda a $y_i \longmapsto x_i$, con $1 \leq i \leq n$. De manera análoga, tenemos un homomorfismo $\zeta' : R[x_1, \ldots, x_n] \longrightarrow R[y_1, \ldots, y_n]$ el cual, restringido a R es la función inclusión tal que manda a $x_i \longmapsto y_i$. Por lo tanto, la composición $\zeta\zeta' : R[x_1, \ldots, x_n] \longrightarrow R[x_1, \ldots, x_n]$ es un endomorfismo tal que restringido a R es la identidad y que manda a $x_i \longmapsto x_i$. Como $R[x_1, \ldots, x_n]$ está generado por R y por los x_i's, $\zeta\zeta'$ es el automorfismo identidad de $R[x_1, \ldots, x_n]$. De manera similar, $\zeta'\zeta : R[y_1, \ldots, y_n] \longrightarrow R[y_1, \ldots, y_n]$ es el automorfismo identidad en $R[y_1, \ldots, y_n]$, por lo que, tanto ζ como ζ', son isomorfismos, concluyendo que $R[y_1, \ldots, y_n] \cong R[x_1, \ldots, x_n]$. A este último anillo $R[x_1, \ldots, x_n]$ lo llamaremos el *anillo de polinomios de n variables indeterminadas sobre R.*

Teorema 31 *Sea $R[x_1, \ldots, x_n]$ el anillo de polinomios de n indeterminadas sobre R y sea π una permutación del conjunto $\{1, \ldots, n\}$. Entonces existe un único automorfismo ζ_π de $R[x_1, \ldots, x_n]$ tal que $\zeta_\pi \mid_R = Id_R$ y $x_i \longmapsto x_{\pi(i)}$ $\forall i \in \{1, \ldots, n\}$.*

Demostración. Por el teorema pasado, al tomar $\eta = i : R \longrightarrow R[x_1, \ldots, x_n]$, se tiene el endomorfismo $\zeta_\pi : R[x_1, \ldots, x_n] \longrightarrow R[x_1, \ldots, x_n]$ tal que extiende a η y manda a cada x_i a $x_{\pi(i)}$. Falta ver entonces que ζ_π es un automorfismo. Consideremos al conjunto generador de $R[x_1, \ldots, x_n]$, es decir, al conjunto $R \cup \{x_1, \ldots, x_n\}$. Notemos que si π_1 y π_2 son dos permutaciones del conjunto $\{1, \ldots, n\}$ entonces también lo es $\pi_1\pi_2$. Por lo tanto, al evaluar en cada x_i, se tiene que $\zeta_{\pi_1\pi_2} = \zeta_{\pi_1}\zeta_{\pi_2}$. De esta manera, basta demostrar que ξ_π es biyectiva.

Si π es una permutación, entonces podemos definir π^{-1}, con lo cual se tiene que $\zeta_\pi\zeta_{\pi^{-1}} = \zeta_{\pi\pi^{-1}} = \zeta_{Id} = Id_{R[x_1,\ldots,x_n]} = \zeta_{Id} = \zeta_{\pi^{-1}\pi} = \zeta_{\pi^{-1}}\zeta_\pi$, demostrando así que ζ_π tiene una función inversa. Por lo tanto, ζ_π es un automorfismo.

■

Sea $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$, es decir, una $n-$ada de números no negativos. A esta $n-$ada le podemos asociar el monomio $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ en las variables $x_1, \ldots, x_n$. Por otra parte, se tiene que

$$(x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n})(x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}) = x_1^{i_1+j_1}x_2^{i_2+j_2}\cdots x_n^{i_n+j_n}$$

Por lo tanto, se sigue que los elementos del anillo $R[x_1, \ldots, x_n]$ son de la forma de una suma finita $\sum a_{i_1\ldots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$, donde $a_{i_1\ldots i_n} \in R$. Por ejemplo,

al considerar $R[x,y]$ se tiene que sus elementos son los polinomios de la forma $a_{0_0} + a_{1_0}x + a_{0_1}y + a_{2_0}x^2 + a_{1_1}xy + a_{0_2}y^2 + \cdots$, donde $a_{i_j} \in R$. Veremos a continuación, que si $(i_1,\ldots,i_n) \neq (j_1,\ldots,j_n)$ entonces los monomios asociados a las $n-$adas, $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ y $x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}$, son distintos y que las únicas relaciones $\sum a_{i_1\ldots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} = 0$ son las triviales, es decir, donde cada $a_{i_1}\ldots a_{i_n} = 0$. Esto se sigue al demostrar que, si $\sum_{(i)} a_{i_1\ldots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} = 0$, donde $(i) = (i_1,\ldots,i_n)$ y la suma se toma sobre un número finito de elementos distintos de $(i) \in \mathbb{N}^n$, entonces todos los coeficientes son cero. Notemos que si $(i) \neq (j)$, esto último implicará que $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} \neq x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}$, ya que de lo contrario, se tendría la relación no trivial $1x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} - 1x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n} = 0$, contradiciendo lo anterior. La prueba se hará por inducción. La base de la inducción, es decir, el caso $n = 1$, ya está hecho. Supongamos entonces que se vale para $n-1$, con $n > 1$, y demostrémoslo para n. Notemos que la suma $\sum_{(i)} a_{i_1\ldots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ se puede escribir de la forma $\sum_{i_n} A_{i_n}x_n^{i_n}$, donde i_n varía en un subconjunto finito de $\mathbb{N}$ y $A_{i_n} = \sum_{\hat{i}} a_{i_1\ldots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_{n-1}}$, con $(\hat{i}) = (i_1,i_2,\ldots,i_{n-1})$ y donde la suma se toma sobre un conjunto finito de distintos $(\hat{i})$. Ahora, si $\sum a_{i_1\ldots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} = 0$, entonces $\sum_{i_n} A_{i_n}x_n^{i_n} = 0$, para $i_n = 1,2,\ldots$, de donde se tiene que $A_{i_n} = 0, \forall i_n$. Aplicando la hipótesis de inducción a cada $A_{i_n} = \sum_{\hat{i}} a_{i_1\ldots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_{n-1}}$, se tiene que, fija una i_n, $a_{i_1\ldots i_n} = 0$ para toda $(\hat{i})$, por lo que se cumple que $\forall i_n, \forall(\hat{i})$, $a_{i_1\ldots i_n} = 0$, teniendo así que $a_{i_1\ldots i_n} = 0$ para toda (i).

Como en el caso $n = 1$ tratado anteriormente, vemos que para cualquier $R[u_1,\ldots,u_s]$, el homomorfismo de $R[x_1,\ldots,x_s] \longrightarrow R[u_1,\ldots,u_s]$, que extiende a la identidad en R y manda a cada $x_i \longmapsto u_i$, es un isomorfismo si y sólo si $\sum_{(i)} a_{i_1\ldots i_s}u_1^{i_1}u_2^{i_2}\cdots u_s^{i_s} = 0 \Longrightarrow a_{i_1\ldots i_s} = 0, \forall(i)$. Si este es el caso, decimos que los s elementos $u_1,\ldots,u_s$ son *algebraicamente independientes sobre* R, en caso contrario, decimos que son *algebráicamente dependientes.*

Sea ahora M un monoide y R un anillo conmutativo. Definimos a $R[M] := R^{(M)}$ como el subconjunto de R^M tales que tienen soporte finito, es decir, las funciones $f : M \longrightarrow R$ tales que $f(m) = 0$ para toda $m \in M$, excepto para una cantidad finita. Definamos las operaciones suma, producto en $R[M]$ por:

$(f+g)(m) = f(m) + g(m)$ para cualquier $m \in M$

$(fg)(m) = \sum_{pq=m} f(p)g(q)$.

Veamos primero que $f+g$ y fg son funciones en $R^{(M)}$. Para esto, basta fijarnos en el soporte de $f+g$ y de fg. Como $f,g \in R^{(M)}$ entonces cada una tiene soporte finito, es decir, existen $x_1,\cdots,x_n$ y $y_1,\cdots,y_m$ elementos en M, tales que $f(x_i) \neq 0$ y $g(y_j) \neq 0, \forall i,j$ respectivamente. De esta manera, $f+g$ tiene como soporte a lo más los elementos $x_1,\ldots,x_n,y_1,\cdots,y_m$, ya que en cualquier otro elemento tanto f como g son cero. Por lo tanto, $f+g \in R^{(M)}$. Para el producto fg, basta fijarnos en los elementos de la forma $f(x_i)\,g(y_j)$, ya que dada $m \in M$, si $x_i \not| m, \forall i \in \{1,\ldots,n\}$, entonces para cualquier $z \mid m$, se tiene que $f(z) = 0$, por lo que al tomar la suma sobre los divisores de m, se tendria que $fg = 0$. De la misma manera, dada $m \in M$, si $y_j \not| m$ $\forall j \in \{1,\ldots,m\}$, entonces $\forall z$ tal que $z \mid m$, entonces $g(z) = 0$. De esta manera, el soporte de fg tiene lo más nm elementos, a saber, los $x_iy_j \in M$ para $i \in \{1,\ldots,n\}$ y

$j \in \{1, \ldots, m\}$.

Así mismo, definimos la función $0'(m) = 0, \forall m \in M$ y $1'(e) = 1, 1'(m) = 0, \forall m \neq e$, donde 1 es el neutro del anillo R y e el neutro del monoide M. Como $(f+g)(m) = f(m) + g(m) = g(m) + f(m) = (g+f)(m)$, $\forall m \in M$, la función $0(m) = 0$ es claramente el neutro para $+$ y si $f \in R[M]$, entonces también $-f \in R[M]$, con $(-f)(m) = -f(m)$ y es tal que $(f-f)(m) = 0, \forall m$, por lo que se tiene que $(R[M], +, 0)$ forma un grupo abeliano. Ahora, si $f \in R[M]$ entonces $(f1')(m) = \sum_{pq=m} f(p)1'(q) = \sum_{pe=m} f(p)1'(e) = f(m), \forall m \in M$, por lo que $(R[M], \cdot, 1')$ es un monoide. Para ver que $R[M]$ es un anillo, falta ver la ley distributiva, pero esta última se sigue de la distributividad en el anillo R. Por lo tanto, $R[M]$ es un anillo. Consideremos ahora la función $\alpha : R \longrightarrow R[M]$ definida por $\alpha(a) = a'$, donde $a'(e) = a$, y $a'(m) = 0, \forall m \neq e$. Veamos que α es un homomorfismo. Si $a, b \in R$ entonces por definición, $a + b \longmapsto (a+b)'$, donde $(a+b)'(e) = a + b, (a+b)(m) = 0, \forall m \neq e$. Ahora, notemos que $(a' + b')(e) = a'(e) + b'(e) = a + b$, y $(a' + b')(m) = a'(m) + b'(m) = 0 + 0 = 0, \forall m \neq e$, por lo que $(a+b)' = a' + b'$. Por otra parte, α manda $ab \longmapsto (ab)'$, donde $(ab)'(e) = ab$ y $(ab)'(m) = 0, \forall m \neq e$. Si consideramos el producto a' y b' se tiene que $(a'b')(m) = \sum_{pq=m} a'(p)b'(q) = \sum_{eq=m} a'(e)b'(q) = ab'(m)$, por lo que $(a'b')(m) = ab$ si $m = e$ y $(a'b')(m) = 0$ si $m \neq e$, teniendo así que $a'b' = (ab)'$. Claramente α manda $1 \longmapsto 1' \in R[M]$ por lo que α es un homomorfismo. Además, si $a \neq b \in R$ entonces claramente $a' \neq b'$, pues basta evaluarlos en e. Por lo tanto, $R[M]$ tiene un subanillo isomorfo a R. De manera casi análoga, se tiene que $\beta : M \longrightarrow R[M]$, definida por $n \longmapsto n'$, donde $n'(n) = 1$ y $n'(m) = 0, \forall m \neq n$, es un homomorfismo de monoides. Por definición, $(kl)'(kl) = 1$ y $(kl)'(m) = 0, \forall m \neq kl$, pero si consideramos el producto $k'l'$ se tiene que $(k'l')(m) = \sum_{pq=m} k'(p)l'(q)$. Como los únicos valores distintos que toman k' y l' son en k y l, respectivamente, se tiene que esta última suma es cero si $m \neq kl$ y 1 si $m = kl$, ya que $\sum_{pq=m} k'(p)l'(q) = \sum_{kl=m} k'(k)l'(l) = 11 = 1$. Por lo tanto $(k'l') = (kl)'$. Usando este resultado, se tiene que $\beta(e)\beta(m) = \beta(em) = \beta(m) = \beta(me) = \beta(m)\beta(e), \forall m \in M$, así que $\beta(e)$ es el neutro $1'$. Por lo tanto, $R[M]$ también tiene una copia del monoide M. Notemos de lo anterior que las funciones α y β mandan al neutro de R y M, respectivamente, al neutro de $R[M]$, es decir, se tiene que $\alpha(1) = \beta(e)$ donde 1 y e son los neutros multiplicativos para R y M respectivamente. Por otra parte, como R es conmutativo, si $a' \in R \subset R[M]$, se tiene que para cualquier $g \in R[M]$, $(a'g)(m) = \sum_{pq=m} a'(p)g(q) = \sum_{eq=m} a'(e)g(q) = \sum_{q=m} ag(q) = ag(m) = g(m)a$, donde $g(m)a = \sum_{q=m} g(q)a = \sum_{qe=m} g(q)a'(e) = \sum_{qp=m} g(q)a'(p) = (ga)(m)$, por lo que $a \in Z(R[M])$, por lo tanto, $R \subset Z(R[M])$.

Notemos que si $f \in R[M]$, entonces f tiene un soporte finito, por lo que se puede pensar como una suma de funciones que sólo actúa en los elementos que conforman al soporte, es decir, $f = \sum_{i=1}^{n} f'(m_i)m_i'$, donde los m_i son los elementos que bajo f son distintos de cero y las m_i' son funciones en $M \subset R[M]$. Veamos que esta afirmación se cumple: sea $f \in R[M]$ con soporte finito $m_1, \ldots, m_n$, es decir, $f(m_i) \neq 0$ y $f(m) = 0, \forall m \neq m_1, \ldots, m_n$. Como $f(m_i) \in R$, para cada m_i, entonces, por las observaciones anteriores, podemos pensar a cada $f(m_i)$ como una función en $R[M]$. Definamos ahora a $m_i' : M \longrightarrow R$ por

$m_i'(m_i) = 1$ y $m_i'(n) = 0, \forall n \neq m_i$. De esta manera, podemos suponer también que cada $m_i' \in M$. Definamos ahora $\sum_{i=1}^{n} f(m_i)m_i'$, la cual está en $R[M]$ puesto que, como el soporte de f es finito, la suma vuelve a ser finita . Evaluando esta última suma en m, se tiene que

$$(\sum_{i=1}^{n} f(m_i)m_i')(m) = \sum_{i=1}^{n} f(m_i)m_i'(m)$$

la cual es cero si $m \neq m_1, \ldots, m_n$, pues todos los sumandos lo serían, y es $f(m_i)$ cuando $m = m_i$, es decir,

$$(\sum_{i=1}^{n} f(m_i)m_i')(m) = f(m), \forall m \in M$$

Por lo tanto, cualquier elemento en $R[M]$ se puede ver como una suma de

productos entre elementos de R y M. Supongamos ahora que $\sum_{i=1}^{n} r_i m_i = 0'$, donde $r_i \in R$ y $m_i \in M$. Entonces, recordando que m_i es una función en $R[M]$ tal que evaluada en $m = m_i$ es 1, y cero si $m \neq m_i$, se tiene que $0 = 0'(m_i) = (\sum_{i=1}^{n} r_i m_i)(m_i) = r_i(m_i(m_i)) = r_i 1 = r_i, \forall i \in \{1, \ldots, n\}$, por lo que $r_i = 0$ para toda i. La otra implicación es clara, teniendo así que $\sum_{i=1}^{n} r_i m_i = 0'$ si y sólo si $r_i = 0$. Consideremos ahora la representación de cada f con los elementos que conforman su soporte, es decir, los $m_i's$. Afirmamos que esta representación es única: supongamos que $f = \sum_{i=1}^{n} s_i m_i = \sum_{i=1}^{n} r_i m_i$, por lo anterior, se tiene que $\sum_{i=1}^{n} (r_i - s_i)m_i = \sum_{i=1}^{n} r_i m_i - \sum_{i=1}^{n} s_i m_i = 0$, teniendo que $r_i = s_i$.

Supongamos ahora que se tiene el homomorfismo de anillos $\sigma_1 : R \longrightarrow S$, con $\sigma_1(R) \subset Z(S)$ y el homomorfismo de monoides $\sigma_2 : M \longrightarrow S$. Afirmamos que se tiene un único homomorfismo de anillos $\sigma : R[M] \longrightarrow S$ que extiende a σ_i, con $i = 1, 2$. Para esto, como a cada $f \in R[M]$ la podemos ver como $\sum_{i=1}^{n} r_i m_i$, con $r_i \in R$, $m_i \in M$, éstos siendo el soporte de f, podemos definir a $\sigma : R[M] \longrightarrow S$ por $\sigma(f) = \sigma(\sum_{i=1}^{n} r_i m_i) := \sum_{i=1}^{n} \sigma_1(r_i)\sigma_2(m_i)$. Notemos que σ está bien definida ya que la representación de f como suma de productos sobre su soporte es única. Como $r = r1 \in R[M]$, entonces $\sigma(r) = \sigma_1(r)\sigma_2(1) = \sigma_1(r)1' = \sigma_1(r)$, donde $1'$ es el neutro en S. Por lo tanto, $\sigma \mid_R = \sigma_1$. Análogamente, como $m = 1m \in R[M]$, $\sigma(m) = \sigma_1(1)\sigma_2(m) = 1'\sigma_2(m) = \sigma_2(m)$, teniendo así que $\sigma \mid_M = \sigma_2$. Además, $\sigma(1') = \sigma_1(1)\sigma_2(1) = 1'$. Veamos entonces que σ es un homomorfismo de grupos y monoide. Sean $f, g \in R[M]$ tales que $f = \sum_{i=1}^{n} r_i m_i$, $g = \sum_{i=1}^{m} s_i m_i$. Notemos que podemos suponer que ambas expresiones contienen a las mismas $m_i's$, ya que si en un inicio, m_i está en la expresión de f, entonces podemos sumarle el término $0 = 0m_i$ a g, obteniendo así la misma expresión de g pero con el término m_i. Por este mismo razonamiento, ambas expresiones tienen la misma cantidad de elementos, por lo que podemos suponer que $m = n$.

De esta manera, se tiene que $f+g=\sum_{i=1}^{n}\left(r_i+s_i\right)m_i$. Entonces,

$$\begin{aligned}\sigma(f+g) &= \sum_{i=1}^{n}\sigma_1\left(r_i+s_i\right)\sigma_2\left(m_i\right)=\sum_{i=1}^{n}\left(\sigma_1\left(r_i\right)+\sigma_1\left(s_i\right)\right)\sigma\left(m_i\right)= \\ & \sum_{i=1}^{n}\sigma_1\left(r_i\right)\sigma_2\left(m_i\right)+\sum_{i=1}^{n}\sigma_1\left(s_i\right)\sigma_2\left(m_i\right)\end{aligned}$$

Notemos que en la suma $\sum_{i=1}^{n}\sigma_1\left(r_i\right)\sigma_2\left(m_i\right)$, los elementos que son distintos de cero son justamente las $i's$ tal que m_i está en el soporte de f, por lo que $\sum_{i=1}^{n}\sigma_1\left(r_i\right)\sigma_2\left(m_i\right)=\sigma\left(f\right)$. Análogamente, $\sum_{i=1}^{n}\sigma_1\left(s_i\right)\sigma_2\left(m_i\right)=\sigma\left(g\right)$, ya que basta fijarnos en las $i's$ tales que m_i está en el soporte de g. Por lo tanto, $\sigma(f+g)=\sigma\left(f\right)+\sigma\left(g\right),\forall f,g\in R\left[M\right]$. Para el producto, tomemos las representaciones sobre su soporte para cada una de las funciones f y g. Notemos entonces que

$$\begin{aligned}fg &= \left(\sum_{i=1}^{n}r_im_i\right)\left(\sum_{j=1}^{k}s_jm_j\right)=\sum_{i=1}^{n}\left(\sum_{j=1}^{k}\left(r_im_i\right)\left(s_jm_j\right)\right) \\ &= \sum_{i=1}^{n}\left(\sum_{j=1}^{k}r_is_jm_im_j\right)\end{aligned}$$

, ya que $r_i,s_i\in R\subset Z\left(R\left[M\right]\right)$. Por lo tanto,

$$\sigma\left(fg\right)=\sigma\left(\sum_{i=1}^{n}\left(\sum_{j=1}^{k}r_is_jm_im_j\right)\right)=\sum_{i=1}^{n}\left(\sum_{j=1}^{k}\sigma_1\left(r_is_j\right)\sigma_2\left(m_im_j\right)\right)$$

esta última debido a la distribución sobre la suma se σ una cantidad finita de veces. Pero

$$\begin{aligned}\sum_{i=1}^{n}\left(\sum_{j=1}^{k}\sigma_1\left(r_is_j\right)\sigma_2\left(m_im_j\right)\right) &= \sum_{i=1}^{n}\left(\sum_{j=1}^{k}\sigma_1\left(r_i\right)\sigma_1(s_j)\,\sigma_2\left(m_i\right)\sigma_2(m_j)\right) \\ &= \sum_{i=1}^{n}\left(\sum_{j=1}^{k}\sigma_1(r_i)\;\sigma_2\left(m_i\right)\sigma_1(s_j)\sigma_2(m_j)\right)\end{aligned}$$

pues $\sigma_1\left(R\right)\subset Z\left(S\right)$. Pero esta última suma resulta ser

$$\left(\sum_{i=1}^{n}\sigma_1\left(r_i\right)\sigma_2\left(m_i\right)\right)\left(\sum_{j=1}^{k}\sigma_1\left(s_j\right)\sigma_2\left(m_j\right)\right)=\sigma\left(f\right)\sigma\left(g\right)$$

lo cual demuestra que σ es un homomorfismo de anillos. Para finalizar la afirmación, la unicidad de σ se sigue de la unicidad de la representación sobre el soporte de cada función $f\in R\left[M\right]$.

Definición 19 *Si M es un grupo, a $R[M]$ le llamamos el algebra-grupo de M sobre R.*

Consideremos ahora al conjunto $\mathbb{N}$ de los naturales y sea $\mathbb{N}^r$ el producto cartesiano de $\mathbb{N}$, r veces, es decir, los elementos de $\mathbb{N}^r$ tienen la forma de $r-tuples$ $(a_1,\ldots,a_r)$ donde $a_i \in \mathbb{N}$. Si definimos la suma en $\mathbb{N}^r$ por coordenadas, entonces se tiene que $\left(\mathbb{N},+,\widetilde{0}\right)$ es un anillo conmutativo, donde $\widetilde{0} = (0,\ldots,0)$. Sean $e_i = (0,\ldots,1,\ldots,0)$, donde el 1 está en el lugar $i-$ésimo. De esta manera, se tiene que para cualquier $(a_1,\ldots,a_r) \in \mathbb{N}^r$, $(a_1,\ldots,a_r) = \sum_{i=1}^{r} a_i e_i$, por lo que los $e_i\acute{s}$ generan a $\mathbb{N}^r$. Sea ahora un monoide M conmutativoy $x_1,\ldots,x_r \in M$ elementos de M. Definamos la función $\eta : \mathbb{N}^r \longrightarrow M$ dada por $(a_1,\ldots,a_r) \longmapsto x_1^{a_1}x_2^{a_2}\cdots x_r^{a_r}$. Como los $x_i\acute{s}$ conmutan, tenemos que

$$\begin{aligned}\eta\left((a_1,\ldots,a_r)\right)\eta\left(b_1,\ldots,b_r\right) &= \left(x_1^{a_1}x_2^{a_2}\cdots x_r^{a_r}\right)\left(x_1^{b_1}x_2^{b_2}\cdots x_r^{b_r}\right)\\ &= x_1^{a_1+b_1}x_2^{a_2+b_2}\cdots x_r^{a_r+b_r}\\ &= \eta\left((a_1+b_1,\ldots,a_r+b_r)\right)\end{aligned}$$

Como $\eta\left(\widetilde{0}\right) = x_1^0x_2^0\cdots x_r^0 = 1$, se tiene que η es un homomorfismo. Por otra parte, notemos que

$$e_i \longmapsto x_1^0x_2^0\cdots x_i^1\ldots x_r^0 = x_i$$

Como $\mathbb{N}^r$ está generado por los e_i, entonces sólo hay un homomorfismo de $\mathbb{N}^r$ a M tal que mande $e_i \longmapsto x_i$, $\forall i \in \{1,\ldots,r\}$.

Definición 20 *Al conjunto $\mathbb{N}^r$ se le conoce como el libre monoide conmutativo con r generadores e_i.*

Sea $\mathbb{N}$ el conjunto de los naturales y R un anillo conmutativo. Formemos primero al monoide libre conmutativo $\mathbb{N}^{(r)}$, con sus r generadores $e_1,\ldots,e_r$ donde cada e_i es una coordenada $r-$ésima de la forma $(0,\ldots,1,\ldots,0)$, con el 1 en el lugar $i-$ésimo y cero en los demás lugares. Como ya vimos, $\left(\mathbb{N}^r,+,\widetilde{0}\right)$ es un monoide donde la suma está definida por coordenadas, y el elemento neutro es el $\widetilde{0} = (0,\ldots,0)$. Ahora, como $\mathbb{N}^{(r)}$ es un monoide, podemos formar al anillo $R\left[\mathbb{N}^{(r)}\right]$. Afirmamos que $R\left[\mathbb{N}^{(r)}\right] \cong R[x_1,\ldots,x_r]$, es decir, $R\left[\mathbb{N}^{(r)}\right]$ es isomorfo al anillo de polinomios sobre R en las variables $x_1,\ldots,x_r$. Sea $i : R \hookrightarrow R\left[x_1,\ldots,x_r\right]$ el homomorfismo inclusión dado por $r \longmapsto r$, y sea la función $\delta : \mathbb{N}^{(r)} \longrightarrow R\left[x_1,\ldots,x_r\right]$ definido por $e_i \longmapsto x_i$ y $\widehat{0} \longmapsto 0 \in R$. Notemos que, como $\mathbb{N}^{(r)}$ está generado por los $e_i\acute{s}$, la imagen de δ está generada por los $x_i\acute{s}$, los cuales también forman un monoide. Como además $\widehat{0} \longmapsto 0$, δ es un homomorfismo de monoides. Por lo tanto, por el resultado anterior, se tiene un homomorfismo $\xi : R\left[\mathbb{N}^{(r)}\right] \longrightarrow R[x_1,\ldots,x_r]$ tal que $\xi\mid_R = i$, $\xi\mid_{\mathbb{N}^{(r)}} = \delta$. Veamos que ξ^{-1} existe. Para esto, por la propiedad universal, se tiene que el homomorfismo $i : R \hookrightarrow R\left[\mathbb{N}^{(r)}\right]$ se puede extender a un homomorfismo

$$\beta : R[x_1,\ldots,x_r] \longrightarrow R\left[\mathbb{N}^{(r)}\right]$$

de la siguiente manera

$$\begin{array}{ccc} & & \beta \\ R\left[x_1,\ldots,x_r\right] & \longrightarrow & R\left[\mathbb{N}^{(r)}\right] \\ i\ \uparrow & \nearrow & \\ R & & \end{array}$$

donde $x_i \longmapsto e_i$. Entonces, se tiene que

$$\left(\xi\circ\beta\right)\left(rx_i\right)=\xi\left(\beta\left(rx_i\right)\right)=\xi\left(r\beta(x_i)\right)=\xi\left(re_i\right)=r\xi\left(e_i\right)=rx_i$$

Análogamente,

$$\beta\circ\xi\left(re_i\right)=\beta\left(\xi\left(re_i\right)\right)=\beta\left(r\xi\left(e_i\right)\right)=\beta\left(rx_i\right)=r\beta\left(x_i\right)=re_i$$

Por lo tanto, $\xi\circ\beta=Id_{R[x_1,\ldots,x_r]}$ y $\beta\circ\xi=Id_{R\left[\mathbb{N}^{(r)}\right]}$, es decir, $\beta=\xi^{-1}$, por lo que ξ es invertible. De esta manera, concluimos que $R\left[\mathbb{N}^{(r)}\right]\cong R\left[x_1,\ldots,x_r\right]$.

Este último resultado nos permite construir un anillo de polinomios con n variables, para cualquier $n\in\mathbb{N}$. Es natural preguntarnos si es posible construir un anillo de polinomios en *cualquier* cantidad de variables, sea numerable o no numerable. La respuesta a esta pregunta es positiva, y la demostración es como sigue: Sea Y cualquier conjunto y R un anillo conmutativo. Formemos el monoide $\mathbb{N}^{(Y)}$, donde a cada elemento $y\in Y$, lo podemos identificar con una función $w_y:Y\longrightarrow\mathbb{N}$ dada por $w_y\left(y\right)=1$ y $w_y\left(z\right)=0,\forall z\neq y$. Como $\mathbb{N}^{(Y)}$ es un monoide, podemos construir el anillo $R\left[\mathbb{N}^{(Y)}\right]$. Notemos que en este caso, el anillo de polinomios con tantas variables como elementos de Y, tiene la forma $R\left[\left\{x_y\right\}_{y\in Y}\right]$. Por lo tanto, si $f:R\longrightarrow T$ es un homomorfismo tal que $f\left(R\right)\subset Z\left(T\right)$, entonces, por la propiedad universal de anillos aplicada a R, basta tomar un conjunto de valores $\left\{t_y\right\}_{y\in Y}\subset T$, para extender el homomorfismo f a un homomorfismo $\overline{f}:R\left[\left\{x_y\right\}_{y\in Y}\right]\longrightarrow T$, donde $r\longmapsto f\left(r\right)$ y $x_y\longmapsto t_y,\forall y\in Y$. Como caso particular, si $i:R\hookrightarrow R\left[\mathbb{N}^{(Y)}\right]$ dada por $r\longmapsto r$, se tiene que $i\left(R\right)\subset Z\left(R\left[\mathbb{N}^{(Y)}\right]\right)$, por lo que ésta se puede extender a un homomorfismo $\mu:R\left[\left\{x_y\right\}_{y\in Y}\right]\longrightarrow R\left[\mathbb{N}^{(Y)}\right]$ tal que $\mu\mid_R=Id$ y $x_y\longmapsto w_y,\forall y\in Y$. Por otra parte, dada la inclusión $i'':R\hookrightarrow R\left[\left\{x_y\right\}_{y\in Y}\right]$, y el homomorfismo de monoides $\lambda:\mathbb{N}^{(Y)}\longrightarrow R\left[\left\{x_y\right\}_{y\in Y}\right]$ definido por $w_y\longmapsto x_y,\forall y\in Y$, éstas se pueden extender a un homomorfismo $\nu:R\left[\mathbb{N}^{(Y)}\right]\longrightarrow R\left[\left\{x_y\right\}_{y\in Y}\right]$ tal que $r\longmapsto r,\forall r\in R$ y $w_y\longmapsto x_y,\forall w_y\in\mathbb{N}^{(Y)}$. Mediante un simple cálculo, se tiene que para toda $r\in R$, $\left(\mu\circ\nu\right)\left(r\right)=\mu\left(r\right)=r$, así como $\left(\mu\circ\nu\right)\left(w_y\right)=\mu\left(x_y\right)=w_y,\forall w_y\in\mathbb{N}^{(Y)}$. Como $R\left[\mathbb{N}^{(Y)}\right]$ está generado por R y por $\mathbb{N}^{(Y)}$ y $\left(\mu\circ\nu\right)\mid_R=Id_R$ y $\left(\mu\circ\nu\right)\mid_{\mathbb{N}^{(Y)}}=\mathbb{N}^{(Y)}$, entonces $\left(\mu\circ\nu\right)=Id_{R\left[\mathbb{N}^{(Y)}\right]}$. De manera similar, $\left(\nu\circ\mu\right)\left(r\right)=r$ y $\left(\nu\circ\mu\right)\left(x_y\right)=x_y,\forall r\in R,x_y\in R\left[\left\{x_y\right\}_{y\in Y}\right]$, por lo que $\left(\nu\circ\mu\right)=Id_{R\left[\left\{x_y\right\}_{y\in Y}\right]}$. Por lo tanto, $R\left[\left\{x_y\right\}_{y\in Y}\right]\cong R\left[\mathbb{N}^{(Y)}\right]$, lo cual demuestra

la construcción de un anillo de polinomios sobre R, con tantas variables como queramos.

Para finalizar esta sección, consideremos al anillo conmutativo R y al anillo de polinomios con una variable indeterminada $R[x]$. Si $f(x) \in R[x]$ con $f(x) \neq 0$, entonces podemos expresarlo como $f(x) = a_0 + a_1x + \cdots + a_nx^n$, donde $a_n \neq 0$.

Definición 21 *Si $f(x) \in R[x]$ es tal que se expresa como $f(x) = a_0 + a_1x + \cdots + a_nx^n$, con $a_n \neq 0$ y $a_m = 0, \forall m > n$, decimos que a_n es el coeficiente principal y que el grado de $f(x)$, denotado por* $\operatorname{grad} f$*, es n.*

Si $f(x) \in R[x]$ es el polinomio 0, diremos que $\operatorname{grad} f = -\infty$. Notemos también que $f(x) \in R$ si y sólo si $\operatorname{grad} f = 0$ ó $\operatorname{grad} f = -\infty$. En particular, se cumple que $f(x) \in R^*$ si y sólo si $\operatorname{grad} f = 0$. De ahora en adelante, adoptaremos las siguientes reglas:

$$\begin{aligned} -\infty &< n, \forall n \in \mathbb{N} \\ -\infty + (-\infty) &= -\infty \\ -\infty + n &= -\infty, \forall n \in \mathbb{N} \end{aligned}$$

Por otra parte, por la manera en que se definió la suma de polinomios, se tiene que para cualquier $f(x), g(x) \in R[x]$,

$$\operatorname{grad}(f+g) \leq \operatorname{máx}\{\operatorname{grad} f, \operatorname{grad} g\}$$

ya que al definir la suma de polinomios por coordenadas, basta fijarnos en el coeficiente principal de $f(x)$ y $g(x)$ y tomarnos el mayor natural asociado a estos coeficientes. Notemos también que $\operatorname{grad}(f+g) < \operatorname{máx}\{\operatorname{grad} f, \operatorname{grad} g\}$ si y sólo si el coeficiente principal de $f(x)$ es igual al coeficiente principal de $g(x)$ con signo cambiado. Ahora, si $f(x) = a_0 + a_1x + \cdots + a_nx^n$ y $g(x) = b_0 + b_1x + \cdots + b_mx^m$, entonces

$$f(x)\,g(x) = a_0b_0 + (a_0b_1 + a_1b_0)\,x + \cdots + a_nb_mx^{n+m}$$

Entonces, si a_n y b_m no son divisores de cero, se tiene que $a_nb_m \neq 0$, por lo que

$$\operatorname{grad} fg = n + m = \operatorname{grad} f + \operatorname{grad} m$$

En particular, si R es un dominio, esta última ecuación de grados se cumple para cualesquiera dos polinomios en $R[x]$, incluyendo el caso $\operatorname{grad} f = -\infty$.

Teorema 32 *Si D es un dominio entero, entonces el anillo de polinomios $D[x]$ es un dominio entero.*

Demostración. Ya sabemos que $D[x]$ es un anillo, por lo que falta entonces demostrar que no tiene divisores de cero. Si $f(x)\,g(x) = 0$. entonces $\operatorname{grad} fg = -\infty$. Ahora, por la ecuación de grados y las reglas antes definidas, esto pasa si y sólo si $\operatorname{grad} f = -\infty$ ó $\operatorname{grad} g = -\infty$, lo cual equivale a decir que $f(x) = 0$ ó $g(x) = 0$. Por lo tanto, $D[x]$ es un dominio entero. ■

Corolario 8 *Si D es un dominio entero, entonces $D[x_1, x_2, \ldots, x_n]$ es un dominio entero.*

Este resultado es inmediato al considerar el teorema anterior y aplicar inducción sobre el número de variables indeterminadas. Por otra parte, notemos que las unidades de $D[x]$ son también unidades en D. Esto se sigue considerando lo siguiente: si $f(x)\,g(x) = 1$, entonces $\operatorname{grad} fg = 0$. Por la ecuación de grados, se tiene que $\operatorname{grad} f + \operatorname{grad} g = 0$, por lo que $\operatorname{grad} f = 0 = \operatorname{grad} g$, lo cual equivale a decir que $f(x), g(x) \in D$. Por lo tanto,si $f(x)$ es unidad en $D[x]$, entonces $f(x) \in D$ y su inverso $g(x)$ también está en D. De esta manera, con un razonamiento inductivo, se tiene que las unidades en $D[x_1, x_2, \ldots, x_n]$ también están contenidas en el dominio entero D.

De la sección anterior, sabemos que todo dominio D tiene asosiado un campo de fracciones F. Si D es un dominio entero, por el corolario anterior, $D[x_1, x_2, \ldots, x_n]$ también es un dominio entero, por lo que también le podemos asignar su campo de fracciones de polinomios con n variables indeterminadas, al cual lo denotaremos por $D(x_1, \ldots, x_n)$.

0.15. DFU y Dominios Euclideanos

Sea D un dominio entero conmutativo. Empezaremos dando la noción de división en un dominio entero.

Definición 22 *Sean $a, b \in D$. Decimos que a **es un factor de** b o que a **es un divisor de** b, y lo denotaremos como $a \mid b$, si existe $c \in D$ tal que $b = ac$.*

Notemos que la relación de divisibilidad es una relación transitiva y reflexiva: como $a = a1$, entonces $a \mid a$, $\forall a \in D$ y si $a \mid b$ y $b \mid c$, entonces existen $x, y \in D$ tales que $b = ax$ y $c = by$, por lo que $c = by = (ax)\,y = a(xy)$, por lo que $a \mid c$. En general, no se cumple que si $a \mid b$, entonces $b \mid a$, de manera que la relación no es simétrica. Por otra parte, si $u \in D$ es una unidad, entonces existe $v \in D$ tal que $1 = uv$, por lo que $u \mid 1$. Ahora, si $u \mid 1$, entonces existe $v \in D$ tal que $uv = 1$, es decir, u es unidad. De esta manera, se tiene que $u \in D$ es unidad si y sólo si $u \mid 1$.

Definición 23 *Sean $a, b \in D$. Decimos que a **es un asociado de** b, y lo denotaremos por $a \sim b$, si $a = bu$, para alguna unidad $u \in D$.*

Notemos ahora que $\sim$ si es una relación de equivalencia, ya que, claramente $a \sim a$ pues $a = 1a$, si $a \sim b$ y $b \sim c$, entonces $a = bu$ y $b = cv$, con u, v unidades en D. De esta manera,

$$a = bu = (cv)\,u = c(vu)$$

con vu unidad en D, por lo que $a \sim c$. Ahora, si $a \sim b$, existe $u \in D$ unidad tal que $a = bu$. Como u es unidad, existe $v \in D \setminus \{0\}$ tal que $uv = vu = 1$, por lo que

$$av = (bu)\,v = b(uv) = b1 = b$$

es decir, $b \sim a$, por lo que $\sim$ es simétrica.

Por otra parte, si $a \mid b$ y $b \mid a$, entonces existen $u, v \in D$ tales que $b = au$ y $a = bv$, por lo que $b = (bv)\,u = b\,(vu)$. Como D es un dominio, las leyes de cancelación son válidas, por lo que $1 = vu$, es decir, u, v son unidades. Claramente, si $a \sim b$ entonces $a \mid b$ y $b \mid a$, por lo que hemos demostrado que $a \sim b$ si y sólo si $a \mid b$ y $b \mid a$. A los factores de a que no son son ni unidades ni asociados de a los llamaremos *factores propios* de a.

Definición 24 *Decimos que un elemento $p \in D$ es un **elemento irreducible de** D si i) $p \neq 0$, ii) p no es unidad y iii) p no tiene divisores propios; es decir, si $p = ab$, entonces a es unidad ó b es unidad.*

Ejemplo 3 *Si nuestro dominio es $D = \mathbb{Z}$, se tiene que los elementos que conocemos como primos son elementos irreducibles en $\mathbb{Z}$.*

Observemos que si p es irreducible, entonces up también lo es, para cualquier unidad $u \in D$: Si p es irreducible y u es una unidad, entonces *i)* $up \neq 0$, *ii)* up no es unidad, ya que de lo contrario, existiría $v \in D$ unidad tal que $(up)\,v = 1$. Como u es unidad, existe u^{-1}, por lo que $pv = u^{-1}$, lo cual nos lleva a que $p = u^{-1}v^{-1}$. Como tanto u^{-1} y v^{-1} son unidades, y éstas forman un grupo, se tendría que p es una unidad, lo cual es una contradicción, y *iii)* si $up = ab$ con u unidad, entonces $p = u^{-1}ab = a\left(bu^{-1}\right)$. De esta manera, $a \mid p$, por lo que si a no es unidad, como p no tiene factores propios, entonces $a \sim p$, es decir, existe una unidad v tal que $av = p$. Por lo tanto, se tiene que

$$a\,(uv) = u\,(av) = up = ab$$

cancelando a de ambos lados, se tiene que $b = uv$, con uv unidad.

Sea $a \in D$ y supongamos que hay elementos irreducibles $p_1, \ldots, p_n$ tales que

$$a = p_1 p_2 \cdots p_n$$

A esta última expresión la llamamos una factorización de a en elementos irreducibles. Notemos que si $u_1, \ldots, u_n$ son unidades tales que $u_1 u_2 \cdots u_n = 1$ entonces a también admite la factorización

$$a = (u_1 p_1)\,(u_2 p_2) \cdots (u_n p_n)$$

en elementos irreducibles. En este sentido, la factorización en irreducibles nunca es única. Nótese que $(u_1 p_1) \sim p_1, \ldots, (u_n p_n) \sim p_n$.

Definición 25 *Decimos que D es un **dominio de factorización única**, denotado por DFU, si i) todo elemento de $D \setminus \{0\}$ y no unidad puede ser expresado en la forma $p_1 p_2 \cdots p_n$ donde los p_i son irreducibles y, ii) siempre que*

$$p_1 \cdots p_n = q_1 \cdots q_m$$

donde p_i, q_i son irreducibles, entonces $n = m$ y podemos reacomodar los q_j en el producto de tal manera que $p_i \sim q_i$ para $1 \leq i \leq n$.

Consideremos ahora al anillo $\mathbb{Z}$. Este anillo no es un campo ya que no siempre es posible dividir un entero entre otro para obtener otro entero, pero sí podemos hablar de un concepto de división en $\mathbb{Z}$. Los siguientes teoremas se pueden verificar en el libro de David Sharpe, Rings and Factorizationz lo daremos por hecho.

Teorema 33 ***(Algoritmo de la división para Enteros)*** *Sean $m, n \in \mathbb{Z}$ con $n \neq 0$. Entonces existen enteros únicos q y r tales que $m = qn + r$ donde $0 \leq r < |n|$.*

De manera muy similar, se tiene el siguiente resultado para un anillo de polinomios.

Teorema 34 ***(Algoritmo de la división para polinomios)*** *Sea K un campo y sean $f(x), g(x) \in K[x]$ donde $g(x)$ no es el polinomio cero. Entonces existe polinomios únicos $q(x), r(x) \in K[x]$ tales que*

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

y

$$\operatorname{grad} r(x) < \operatorname{grad} g(x)$$

donde la función $\operatorname{grad} f(x)$ *es la antes definida.*

Notemos que si K es un campo y $f(x) \mid h(x)$ en $K[x]$, entonces existe $g(x) \in K[x]$ tal que $f(x)\, g(x) = h(x)$. Como se vio que $\operatorname{grad}(fg) = \operatorname{grad} f + \operatorname{grad} g$ en cualquier dominio, entonces

$$\operatorname{grad} h = \operatorname{grad}(fg) = \operatorname{grad} f + \operatorname{grad} g$$

por lo que $\operatorname{grad} f \leq \operatorname{grad} h$, es decir, hemos visto que

$$f(x) \mid h(x) \Longrightarrow \operatorname{grad} f \leq \operatorname{grad} h, \text{ para } f(x), h(x) \neq 0.$$

Estos últimos teoremas y la observación anterior, nos llevan a la siguiente

Definición 26 *Decimos que un dominio D es un* ***dominio euclideano*** *si existe una función $\delta : D^* = D \setminus \{0\} \longrightarrow \mathbb{N}$, llamada función de grado de D, tal que*

i) siempre que $a, b \in D^*$, con $a \mid b$, entonces $\delta(a) \leq \delta(b)$

ii) Dados $a, b \in D$, con $b \neq 0$, existen $r, q \in D$ tales que $a = qb + r$ donde o bien $r = 0$, o $\delta(r) < \delta(b)$.

Nos referimos a la segunda propiedad de la definición anterior como el *algoritmo de la división* en el dominio euclideano.

Ejemplo 4 *Los anillos $\mathbb{Z}$ y $K[x]$, donde K es un campo, son dominios euclideanos con normas $\delta(a) = |a|$ y $\gamma(f(x)) = \operatorname{grad} f$, respectivamente.*

Teorema 35 *Sea D un dominio euclideano con función de grado δ y sean $a, b \in D$ tales que $a \mid b$ y que $\delta(a) = \delta(b)$. Entonces a y b son asociados.*

Demostración. Usando el algoritmo de la división δ, al dividir a entre b se tiene que existen $q, r \in D$ tales que $a = qb + r$, donde $r = 0$ o $\delta(r) < \delta(b)$. Como $a \mid b$, entonces $ac = b$, para alguna $c \in D$. Por lo tanto, se tiene que $a = q(ac) + r$, lo cual implica que $a(1 - qc) = r$, por lo que $a \mid r$. Entonces, si $r \neq 0$, se tiene que $\delta(a) \leq \delta(r) < \delta(b)$, lo cual contradice la hipótesis inicial. Por lo tanto, $r = 0$ y así $b \mid a$, teniéndose que $a \sim b$. ■

En el caso del anillo $\mathbb{Z}$, para cualquier par de elementos $n, m \in \mathbb{Z}$, podemos hablar de un máximo común divisor d, es decir, un elemento que divida tanto a a como a b y que si c es otro número que divida tanto a a como a b, entonces $c \mid d$. Esta afirmación es válida para todo dominio entero, y más aún, éste máximo común divisor puede ser expresado en la forma $sa + tb$, con $s, t \in D$. Nótese que el máximo común divisor está bien definido salvo asociados.

Definición 27 *Si dos elementos de un dominio entero D tienen máximo común divisor 1, entonces decimos que son* ***coprimos****.*

Teorema 36 *Sea D un dominio euclideano y sean $a, b \in D$. Si $a \mid bc$ y a, b son coprimos entonces $a \mid c$.*

Demostración. Supongamos que $a \mid bc$ y que a, b son coprimos. Entonces existen $s, t \in D$ tal que $as + bt = 1$. Ahora, notemos que $a \mid bc$ y que $a \mid ac$, por lo que multiplicando esta última ecuación, se tiene que $acs + bct = c$. Como a divide a cada uno de los sumandos, entonces $a \mid acs + bct = c$. ■

Por otra parte, en el anillo $\mathbb{Z}$, si p es un número primo, se tiene que siempre que $p \mid ab$, entonces $p \mid a$ o $p \mid b$. Esto nos conduce a la siguiente

Definición 28 *Sea D un dominio entero y $p \in D$. Decimos que p es* ***primo*** *si i) $p \neq 0$, ii) p no es unidad y iii) siempre que $p \mid ab$ con $a, b \in D$, entonces $p \mid a$ o $p \mid b$.*

El siguiente teorema, nos ayudará a demostrar que todo dominio euclideano es un dominio de factorización única.

Teorema 37 *Sea D un dominio entero. Entonces i) todo elemento primo es irreducible en D, ii) si D es un dominio euclideano, todo elemento irreducible es primo, iii) si D es un DFU, todo elemento irreducible es primo.*

Demostración. *i*) Sea p un elemento primo en D y consideremos la factorización $p = ab$ con $a, b \in D$. Como p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$. Pero $p = ab$, por lo que $a \mid p$ y $b \mid p$. Por lo tanto, $p \sim a$ ó $p \sim b$. Sin pérdida de generalidad, si $p \sim a$, entonces $a = up$, para alguna unidad $u \in D$. Por lo tanto,

$$p = ab = (up)\, b = p\,(ub)$$

y cancelado p en ambo lados, se tiene que $ub = 1$, es decir, $b = u^{-1}$ es una unidad, por lo que p es irreducible.

ii) Sea D un dominio euclideano y $p \in D$ irreducible. Supongamos que $p = ab$, con $a, b \in D$ y que $p \not| a$. Como D es un dominio euclideano, a y p tienen un máximo común divisor d. Como p es irreducible, sólo asociados y unidades lo dividen, y como ningún asociado de p puede dividir a a, entonces el máximo común divisor es una unidad, es decir, $d = 1$, por lo que p y a son coprimos. Como a y p son coprimos y $p \mid ab$, entonces $p \mid b$, por lo que p es primo.

iii) Sea D un DFU. Sea $p \in D$ irreducible y supongamos que $a, b \in D$ son tales que $p \mid ab$. Entonces existe $c \in D$ tal que $pc = ab$. Si factorizamos a, b y c en irreducibles se tiene que, por unicidad, a o b tienen un factor irreducible asociado de p, de manera que $p \mid a$ o $p \mid b$, por lo que p es primo. ■

Finalizaremos esta sección con el siguiente

Teorema 38 *Todo dominio euclideano es un DFU.*

Demostración. Sea D un dominio euclideano y δ su función grado. Primero demostraremos que todo elemento no cero y no unidad puede ser factorizado en irreducibles. Supongamos lo contrario, es decir, que existe un elemento no cero y no unidad tal que no puede ser factorizado en irreducibles. Ahora, por el principio del buen orden en los naturales, podemos elegir un elemento a de grado mínimo. Notemos que a no puede ser irreducible, ya que en ese caso, a misma es una factorización en irreducibles. De esta manera, podemos suponer que existen $b, c \in D$ no unidades y no asociados de a tales que $a = bc$. Como $b \mid a$, entonces $\delta(b) \leq \delta(a)$, pero como b y a no son asociados, entonces $\delta(a) \neq \delta(b)$, por lo que $\delta(b) < \delta(a)$. Análogamente, se tiene que $\delta(c) < \delta(a)$. De la minimalidad de $\delta(a)$, se sigue que tanto b como c pueden ser factorizados como producto de un número finito de irreducibles. Si ponemos juntas estas dos factorizaciones, se tiene que que ésta última es una factorización en irreducibles de a, lo cual contradice la hipótesis inicial.

Falta demostrar la unicidad de las factorizaciones en irreducibles. Supongamos entonces que

$$p_1 \cdots p_n = q_1 \cdots q_m$$

son dos factorizaciones con p_i, q_i irreducibles. Como estamos en un dominio euclideano, cada p_i es primo, y como $p_i \mid q_1 \cdots q_m$, se tiene que $p_i \mid q_j$, para algún $j = 1, \ldots, m$. Como el orden de los factores no es importante, podemos reordenar los q_j's y suponer que $p_1 \mid q_1$. Como también los q_i's son irreducibles, éstos no tienen facotres propios, por lo que $p_1 \sim q_1$, es decir, $q_1 = p_1 u_1$, con u_1 unidad. De esta manera, podemos cancelar en nuestra factorización el término p_1 para obtener

$$p_2 \cdots p_n = u_1 q_2 \cdots q_m$$

Notemos que uq_2 vuelve ser irreducible. Repitiendo este argumento para los p_i's, se tiene que al hacer la $n-$ésima cancelación, asociada a p_n, del lado derecho se nos acabarán los irreducibles, obteniendo que

$$1 = (u_1 \cdots u_n)\, q_{n+1} \cdots q_m$$

Como los q_i´s son irreducibles, se tiene un producto de irreducibles igual a 1, lo cual es imposible. De esto se concluye que $n = m$, y al reordenar los q_j´s, se tiene que $p_i \sim q_i$, con $1 \leq i \leq n$. Esto demuestra la unicidad. ■

De este teorema, se sigue que los anillos $K[x]$, con K campo, son DFU.

Para finalizar este capítulo, daremos un criterio de irreducibilidad el anillo de polinomios $\mathbb{Q}[x]$ que nos será muy útil más adelante.

Teorema 39 *(Criterio de Eisenstein). Si* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *y existe un primo* p *tal que* $p \mid a_i, \forall i \in \{1, \ldots, n-1\}$, $p \not| a_n$ *y* $p^2 \not| a_0$, *entonces* $f(x)$ *es irreducible sobre* $\mathbb{Q}[x]$.

Demostración. Supongamos que a $f(x)$ lo podemos escribir de la forma $g(x)h(x)$, con $g(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots b_1 x + b_0$ y $h(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$, donde $r = \operatorname{grad} f$ y $s = \operatorname{grad} g$, y $n = r + s$. De esta manera, se tiene que cada coeficiente a_k de $f(x)$ tiene la forma $\sum_{j+i=k} b_j c_i$, para toda $k = 1, \ldots, n$. En particular, $a_0 = b_0 c_0$. Como $p^2 \not| a_0$, entonces p no puede dividir tanto a b_0 como a c_0, pero como $p \mid a_0$, se tiene que p divide a alguno de los elementos b_0, c_0. Supongamos que $p \mid b_0$ y $p \not| c_0$. Además, $p \not| a_n = b_r c_s$, por lo que p no divide a b_r ni a c_s. Por lo tanto, como p divide a b_0 pero no a b_r, existe un número $k \leq r$ tal que $p \not| b_k$ pero $p \mid b_i, \forall i < k$. De esta manera, p divide a cada término de la suma $\sum_{j+i=k} b_j c_i$, excepto a $b_k c_0$, por lo que $p \not| \sum_{j+i=k} b_j c_i = a_k$. Por hipótesis, p divide a todo a_i, excepto a a_n, por lo que $a_k = a_n$, teniendo así que $k = n$. Por lo tanto, de las desigualdades $k \leq r \leq r + s = n$, se tiene que $r = n$ y por lo tanto, $h(x)$ es una constante. Esto demuestra que $f(x)$ es irreducible. ■

Parte III

Campos

0.16. Extensiones de campos

Consideremos ahora dos campos, F y F', tales que F es un subcampo de F', es decir, $F \subset F'$ y las operaciones $*$ y $+$ de F' restringidas a F son cerradas, cumpliéndose las condiciones de la definición. En este caso, decimos que F' es una extensión de campo o simplemente una extensión de F. Notemos que a F' lo podemos ver como un espacio vectorial sobre el campo F. Para esto, basta ver que cumple las siguientes cuatro propiedades de espacio vectorial:

$i)$ $(F', +, 0)$ es un grupo abeliano, lo cual es inmediato por ser F' campo.

$ii)$ $\cdot : F \times F' \longrightarrow F'$ satisface: $\forall \overrightarrow{v}, \overrightarrow{w} \in F'$ y $\forall \lambda, \mu \in F$

$a) 1 \cdot \overrightarrow{v} = \overrightarrow{v}$

$b) (\lambda\mu) \cdot \overrightarrow{v} = \lambda \cdot (\mu \overrightarrow{v})$

$c) (\lambda + \mu) \cdot \overrightarrow{v} = \lambda \overrightarrow{v} + \mu \overrightarrow{v}$

$d) \lambda \cdot (\overrightarrow{v} + \overrightarrow{w}) = \lambda \overrightarrow{v} + \lambda \overrightarrow{w}$

Para el inciso $ii)$ debemos notar un par de cosas, la primera es que el neutro multiplicativo de F coincide con el de F', pues $F \subset F'$ y el neutro es único. La asociatividad del producto $\cdot$ se debe a que este mismo es asociativo dentro de F' y que $F \subset F'$, así como la distributividad del producto sobre la suma. De esta manera, se tiene que F' es un espacio vectorial sobre F.

El grado de la extension de campo F' sobre F es la dimension del espacio vectorial F' sobre el campo base F. A esto lo denotamos por $|F' : F|$. Si el grado es finito entonces decimos que F' es una extension finita. Denotaremos E_F para decir que el campo E es un espacio vectorial sobre el campo F, o lo que es análogo, que E es una extensión de campo sobre el campo base F.

Lema 4 *Si $F \subset E \subset G$ son campos con G una extensión finita sobre F entonces $|E : F|$ y $|G : E|$ son finitas y $|G : F| = |G : E|\,|E : F|$.*

Demostración. *Por hipótesis tenemos que $|G : F| = n$, para alguna $n \in \mathbb{N}$. Como $F \subset E$ y E, F son campos, entonces E es un espacio vectorial sobre el campo F. Por una parte, como $E \subset G$ y ambos son espacios vectoriales sobre el campo F entonces E es un subespacio de G. Como $|G : F| = n$ y $E \leq G_F$ entonces $|E : F|$ es finita y menor o igual a n.*

Por otra parte se tiene que G es un espacio vectorial sobre F de dimension finita. Sean $\{g_1, ..., g_n\}$ una base para G sobre F. Entonces $\forall g \in G$ $\exists' n$

$f_1, ..., f_n \in F$ tales que $g = f_1 g_1 + ... + f_n g_n$. Por hipótesis $F \subset E$ así que $f_i \in E$ $\forall i = 1, .., n$. Por lo tanto, para cualquier $g \in G$ existen escalares $e_1, ..., e_n \in E$, (a saber, $e_i = f_i \in F \subset E$ antes mencionadas) tales que $g = e_1 g_1 + ... + e_n g_n$,es decir, $\{g_1, ..., g_n\}$ es un conjunto generador del espacio vectorial G_E. Como este conjunto genera y es finito entonces la dimension de G_E es finita y $|G : E| \leq n$.Por lo tanto, $|E : F|$ y $|G : E|$ son finitas.

Para demostrar lo segundo, supongamos que $|G : F| = n, |G : E| = k, |E : F| = m$.Sean $\{g_1, \ldots, g_k\}, \{e_1, \ldots, e_m\}$ bases para G_E y E_F, respectivamente. Basta demostrar entonces que el conjunto $\{g_i e_j\}$, donde $i \in 1 \ldots k$ y $j \in 1 \ldots m$, es una base para G_F. Sea $g \in G$,entonces como G_E existen $\lambda_1, \ldots, \lambda_k \in E$ tales que $g = \lambda_1 g_1 + \cdots + \lambda_k g_k$. A su vez, como $\lambda_i \in E$, existen $\mu_{i,1}, \ldots, \mu_{i,m} \in F$

tales que $\lambda_i = \mu_{i,1}e_1 + \cdots + \mu_{i,m}e_m$, *entonces se tiene que* $g = (\mu_{1,1}e_1 + \cdots + \mu_{m,1}e_m)g_1 + (\mu_{2,1}e_1 + \cdots + \mu_{2,m}e_m)g_2 + \cdots + (\mu_{k,1}e_1 + \cdots + \mu_{k,m}e_m)g_k$. *Notando que al distribuir dentro del paréntesis se obtienen elementos de la forma* $\mu_{i,j}e_jg_i$, *se tiene que* $g = \sum \mu_{i,j}(g_ie_j)$ *donde* $i \in 1 \ldots k$, $j \in 1 \ldots m$ *y* $\mu_{i,j} \in F$, $\forall i, j$. *De esta manera se tiene que el conjunto* $\{g_ie_j\}$ *es un conjunto generador del espacio vectorial* G_F. *Falta demostrar que es linealmente independiente para que sea una base de dicho espacio.*

Sea $0 = \sum \lambda_{i,j}g_ie_j$ *donde* $\lambda_{i,j} \in F$.*Por demostrar que* $\lambda_{i,j} = 0, \forall i \in \{1, \ldots, k\}$ *y* $\forall j \in \{1, \ldots, m\}$. *Por una parte, como* $F \subset E$ *entonces* $\lambda_{i,j} \in E$ *y entonces también lo están los elementos de la forma* $\lambda_{i,j}e_j$. *Notemos ahora que* $\sum \lambda_{i,j}g_ie_j = \sum[\sum(\lambda_{i,j}e_j)]g_i$. *Como* $\{g_1, \ldots, g_k\}$ *es base de* G_E , $\lambda_{i,j}e_j \in E$ *y* $\sum[\sum(\lambda_{i,j}e_j)]g_i = 0$ *entonces* $\sum \lambda_{i,j}e_j = 0, \forall i \in \{1, \ldots, k\}$. *Ahora, para cada* i, *como* $\{e_1, \ldots, e_m\}$ *es base de* E_F *y* $\lambda_{i,j} \in F, \forall j \in \{1, \ldots, m\}$ *entonces* $\lambda_{i,j} = 0, \forall j \in \{1, \ldots, m\}$. *Como esto fue para cada* i, *entonces se tiene que* $\lambda_{i,j} = 0, \forall i \in \{1, \ldots, k\}$ *y* $\forall j \in \{1, \ldots, m\}$. *Por lo tanto, el conjunto* $\{g_ie_j\}$ *es una base para el espacio* G_F. *Notando que* $|\{g_ie_j\}| = km$ *se tiene que* $|G : F| = km = |G : E|\,|E : F|$. ■

Sea F un campo y $f(x) \in F[x]$. Queremos dar una extensión E de F tal que contenga una raíz del polinomio $f(x)$, es decir, un elemento $r \in E$ tal que cumpla con la ecuación $f(x) = 0$. Recordemos que $f(r) = 0$ si y sólo si, $f(x)$ es divisible entre $x - r$, y diremos que $f(x)$ se descompone en $E[x]$ si $f(x) = \prod_{i=1}^{n}(x - r_i)$, es decir, si es igual al producto de factores lineales en $E[x]$. Así, si r es una raíz de $f(x)$ en E, entonces $0 = f(r) = \prod_{i=1}^{n}(r - r_i) \in E[x]$, como $E[x]$ es dominio, $r = r_i$ para alguna $i \in \{1, \ldots, n\}$. Por otro lado, también se tiene la misma factorización $f(x) = \prod_{i=1}^{n}(x - r_i)$ en el anillo de polinomios $R[x]$ donde $R = F(r_1, \ldots, r_n)$. Estas dos maneras de ver la factorización de $f(x)$, nos serán útil más adelante.

Si F es un campo, de la sección anterior se tiene que $F[x]$ es un dominio entero, lo cual nos lleva a la siguiente

Definición 29 *Si* F *es un campo, decimos que un polinomio* $f(x) \in F[x]$ *es irreducible, si i)* $f(x) \neq 0$, *ii)* $f(x)$ *no es unidad y iii)* $f(x)$ *no tiene factores propios.*

Cuando el coeficiente principal de un polinomio es 1, decimos que el polinomio es **mónico**. Sea F un campo y $f(x) \in F[x]$ mónico e irreducible de grado n. Consideremos el siguiente diagrama

$$\begin{array}{ccc} & \overset{\mu}{\longrightarrow} & \\ F[x] & & F[x] \\ i \uparrow & \nearrow & \\ F & & \end{array}$$

donde i es la inclusión de $F \longrightarrow F[x]$ y $\mu : F[x] \longrightarrow F[x]$ está definida por $h(x) \longmapsto r(x)$, donde $r(x)$ es el residuo de dividir $h(x)$ entre $f(x)$, es decir, $h(x) = q(x) f(x) + r(x)$. Como μ es un homomorfismo, se tiene que por los teoremas de isomorfismos $\operatorname{Im}\mu \cong F[x] / \langle f(x) \rangle$ ya que $\ker \mu = \langle f(x) \rangle$.

Se puede demostrar que cualquier dominio euclideano es un *dominio de ideales principales*(DIP), es decir, que todo ideal en el dominio entero tiene la forma $\langle a \rangle$, para algún a en el dominio. Ahora bien, como $f(x)$ es irreducible, entonces $\langle f(x) \rangle$ en $F[x]$ es principal con generador $f(x)$. Afirmamos que $\langle f(x) \rangle$ es máximo. Si I fuese un ideal tal que $\langle f(x) \rangle \subset I \neq F[x]$, entonces, como $F[x]$ es un DIP, entonces $I = \langle g(x) \rangle$, para algún $g(x) \in F[x]$. Esto implica que $f(x) = h(x) g(x)$, con $h(x) \in F[x]$. Como $f(x)$ es irreducible, $h(x)$ o $g(x)$ tiene que ser una unidad. Si $g(x)$ es una unidad, entonces $g(x) \in F$, lo cual implicaría que $\langle g(x) \rangle = F[x]$, lo cual es una contradicción. Por lo tanto, $h(x)$ tiene que ser una unidad, y así $\langle f(x) \rangle = \langle h(x) g(x) \rangle = \langle g(x) \rangle$, por lo que $\langle f(x) \rangle$ es máximo. De esta manera, $F[x] / \langle f(x) \rangle$ es un campo. Nótese que $F \subset F[x] / \langle f(x) \rangle$. Por otra parte, notemos también que esta nueva extensión de campo $F[x] / \langle f(x) \rangle$ contiene un elemento, a saber, $x \in F[x] / \langle f(x) \rangle$ tal que el polinomio $f(t) \in F[x] / \langle f(x) \rangle$ se anula, ya que $f(x) = 0$ en $F[x] / \langle f(x) \rangle$. Denotaremos a $F[x] / \langle f(x) \rangle$ por $F(x)$. En general, si r es una raíz del polinomio $f(x) \in F[x]$, con $f(x)$ irreducible, entonces diremos que $F[x] / \langle f(x) \rangle \cong F(r)$.

Por lo tanto, hemos dado una extensión de campo de F tal que contiene una raíz del polinomio $f(x) \in F[x]$. Ahora, esta extensión de campo es de dimensión finita: para esto basta notar que el conjunto $\mathcal{L} = \left\{1, x, x^2, \ldots, x^{n-1}\right\}$ es linealmente independiente en $F(x)$ y que genera a todo elemento en $F(x)$. Notemos primero que $F(x) = \{r(x) \in F[x] \mid \operatorname{grad} r(x) < n\}$, ya que $F(x)$ el conjunto de residuos después de dividir entre $f(x)$, el cual tiene grado n. De esta manera, todo elemento en $F(x)$ tiene la fomra $a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, donde $a_i \in F$, por lo que $\mathcal{L}$ genera a $F(x)$. Ahora, para ver que $\mathcal{L}$ es linealmente independiente, si $0 = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, con $a_i \in F$ entonces, el polinomio $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ bajo la función μ va a dar a cero, por lo que $f(x) \mid p(x)$. Como el grado de $p(x)$ es menor que el grado de $f(x)$, entonces

$$f(x) \mid p(x) \Longleftrightarrow p(x) = 0$$

por lo que $a_i = 0, \forall i = \{1, \ldots, n-1\}$, es decir, $\mathcal{L}$ es linealmente independiente, por lo que $\mathcal{L}$ es una base para $F(x)$ sobre F y

$$|F(x) : F| = n = \operatorname{grad} f(x).$$

A continuación, damos la definición de la extensión de campo para un polinomio $f(x) \in F[x]$ que contiene todas las raíces de $f(x)$.

Definición 30 *Sea F un campo, $f(x) \in F[x]$ mónico. Decimos que una extensión de campo E de F es un campo de descomposición de $f(x)$ sobre E si:*

i) $f(x) = (x - r_1) \bullet (x - r_2) \bullet \cdots (x - r_n) \in E[x]$, *donde* $\operatorname{grad}(f) = n$

ii) $E = F(r_1, r_2, \ldots, r_n)$, *es decir, E esa generado por todas las raíces de $f(x)$.*

Teorema 40 *Cualquier polinomio $f(x) \in F[x]$ mónico con grado n positivo tiene un campo de descomposición.*

Demostración. Sea F un campo y $f(x) \in F[x]$ mónico. Factorizando $f(x)$ en polinomios irreducibles y mónicos en $F[x]$ se tiene que

$$f(x) = f_1(x) \bullet f_2(x) \bullet \cdots \bullet f_k(x).$$

Claramente $k \leq n = \operatorname{grad} f(x)$. Procederemos por inducción sobre $n - k \geq 0$. Para $n - k = 0$ se tiene que $n = k$, así que todos los $f_i(x)$ son lineales, por lo que F misma es su campo de descomposición.

Supongamos que $n - k > 0$. Sin pérdida de generalidad podemos suponer que $f_1(x)$ tiene grado mayor que 1. Sea $K = F[x]/\langle f_1(x)\rangle$. Como $f_1(x)$ es irreducible en $F[x]$ entonces K es un campo. Por otro lado, notemos que K es una extension de campo de F, teniendo como regla de correspondencia $a \in F \longmapsto a + \langle f_1(x)\rangle$ donde $K = F(r)$ y $r = x + \langle f_1(x)\rangle$ es una raíz de $f_1(x)$ en $K[x]$.

Hasta ahora hemos hecho una extension de campo K/F la cual es generada por una sola raíz del polinomio irreducible $f_1(x) \in F[x]$ y el campo F. Como $F \subset K$ entonces $F[x] \subset K[x]$ y como $f(x), f_1(x), f_2(x), \ldots, f_k(x) \in F[x] \subset K[x]$, se tiene que al factorizar cada $f_i(x)$ en polinomios mónicos irreducibles en $K[x]$, $f(x)$ tiene una factorización en polinomios irreducibles en $K[x]$. Por otro lado, $f_1(x) = (x - r) \bullet g(x) \in K[x]$, por lo que si l es el numero de factores irreducibles en la factorización de $f(x)$ en $K[x]$ se cumple que $l > k$, por lo que $n - l < n - k$. Por lo tanto, podemos aplicar la hipótesis de inducción a $n - l$ para $f(x)$ en K, teniendo así una extension de campo E tal que $E = K(r_1, r_2, \ldots, r_n)$ tal que $f(x) = \prod_{i=1}^{n}(x - r_i) \in E[x]$. Como $f_1(r) = 0$ y $f_1(x) \mid f(x)$ en $K[x]$, entonces $f(r) = 0$ por lo que $r = r_i$ para alguna $i \in \{1, \ldots, n\}$. Por lo tanto se tiene que $E = K(r_1, \ldots, r_n) = F(r)(r_1, \ldots, r_n) = F(r, r_1, \ldots, r_n) = F(r_1, \ldots, r_n)$, viendo así que E es un campo de descomposición para $f(x)$ sobre F. ■

Nótese que cuando se construye la extensión simple de F, es decir, $K = F[x]/\langle f(x)\rangle$, con $f(x)$ irreducible, al hacer la correspondencia $a \in F \longmapsto a + \langle f(x)\rangle$, se tiene en realidad una copia de F en K y no a F misma. Si llamamos a F' la copia de F en K, podemos hacer un nuevo conjunto K' tal que contenga a F y que en lo demás sea igual que K. Este conjunto se hace al quitar la copia de F en K, es decir, F' y después pegarle F, de tal manera que nuestro nuevo conjunto es $K' = (K/F') \cup F$, que tiene la misma estructura de campo que K y contiene a F.

Por otra parte, recordando de la sección de anillos, un elemento $u \in R$ es algebráico, si el homomorfismo $\phi : R[x] \longrightarrow R[u]$ con regla de correspondencia $r \longmapsto r, \forall r \in R$ y $x \longmapsto u$ no es inyectivo. Esto quiere decir que el $\ker \phi \neq \{0\}$, que equivale a decir que existe un polinomio $f(x) \in R[x]$ tal que $f(u) = 0$. Como estamos trabajando con campos, podemos tomar el polinomio mónico de grado menor, distinto de cero, tal que $f(u) = 0$. A este polinomio lo llamaremos el *polinomio mínimo* de $u \in R$.

A continuación, se muestra que la dimensión de cualquier campo de descomposición E_F de un polinomio $f(x) \in F[x]$, es finita.

Proposición 8 *Sea F un campo y E un campo de descomposición sobre F de $f(x) \in F[x]$. Entonces $|E : F|$ es finita y además $|E : F| \leq n!$, donde n es el grado de $f(x)$.*

Demostración. Sea F un campo y $f(x) \in F[x]$, y sea E un campo de descomposición sobre F de $f(x)$. Procederemos por inducción sobre n. Si $n = 1$, entonces $f(x)$ es un factor lineal, por lo que $f(x) = x - r_1$, donde $r_1 \in F$. Por lo tanto, F misma es el campo de descomposición para $f(x) \in F[x]$, y $|E : F| = |F : F| = 1 = 1!$.

Ahora supongamos que vale para todos los valores menores que n. Por una parte, como E es un campo de descomposición de $f(x)$, se tiene que a $f(x)$ la podemos ver como producto de factores lineales en $E[x]$, es decir, $f(x) = \prod_{i=1}^{n}(x - r_i)$ tal que $r_i \in E$, donde $n = \operatorname{grad} f(x)$ y $E = F(r_1 r_2 \dots r_n)$.

De esta manera se tiene el siguiente diagrama:

$$F \quad \hookrightarrow \quad F(r_1) \quad \hookrightarrow \quad F(r_1 r_2 \dots r_n) = E$$

donde $|E : F| = |F(r_1) : F|\,|E : F(r_1)|$.

Nótese que $|F(r_1) : F|$ es el grado del polinomio mínimo $g(x) \in F[x]$ tal que $g(r_1) = 0$. Por hipótesis, se tiene que $r_1$es una raíz de $f(x)$, por lo que $g(x) \mid f(x)$. Por lo tanto, $\operatorname{grad} g(x) \leq \operatorname{grad} f(x)$, y así $|F(r_1) : F| \leq n$. Por otra parte, se tiene también que al ser E campo de descomposición de $f(x)$ sobre F, también lo es sobre $F(r)$, ya que $f(x) = \prod_{i=1}^{n}(x - r_i) = (x - r_1)(x - r_2)\cdots(x - r_n) \in E[x]$, donde $n = \operatorname{grad} f(x)$ y, $E = F(r_1 r_2 \dots r_n) = F(r_1)(r_2 \dots r_n)$.Como $f(x)$ se factoriza en $F(r_1)$ como $(x - r_1)h(x)$, con $h(x) \in F(r_1)[x]$ y $\operatorname{grad} h(x) = n - 1$, entonces el grado del polinomio mínimo para cualquier r_i, con $i = 2, \dots, n$, sobre $F(r_1)$ tiene grado menor o igual que $n - 1$, por lo que le podemos aplicar la hipótesis de inducción. Así, $|E : F(r_1)| \leq (n - 1)!$ y por lo tanto, se tiene $|E : F| = |E : F(r_1)|\,|F(r_1) : F| \leq (n - 1)! \bullet n = n!$. ■

Definición 31 *Decimos que una extensión de campo E_F es algebraica sobre F si cualquier elemento de E es algebraico sobre F.*

Una característica de las extensiones de campo finitas, es la siguiente

Proposición 9 *Sea E una extensión de campo de F tal que $|E : F| = n$. Entonces E es una extension algebráica sobre F.*

Demostración. *Sea E_F tal que $|E : F| = n$ y sea $\alpha \in E$. Como $|E : F| = n$, entonces cualquier conjunto en E con mas de n elementos es linealmente dependiente. Consideremos ahora el conjunto $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$. Si $\alpha^i = \alpha^j$ para*

algún $i, j \in \{1, \ldots, n\}$ *con* $i \neq j$, *entonces se tiene que* $\alpha^i - \alpha^j = 0$, *por lo que* α *es una raíz del polinomio* $f(x) = x^i - x^j \in F[x]$. *Supongamos que* $\alpha^i \neq \alpha^j, \forall i \neq j \in \{1, \ldots, n\}$. *Entonces todos los elementos del conjunto* $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ *están en* E, *y además, son más de* n *elementos, por lo que existen coeficientes* $a_0, a_1, \ldots, a_n \in F$ *tales que* $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. *De esta manera, si definimos a* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, *entonces* $f(x)$ *es tal que* $f(x) \in F[x]$ *y* $f(\alpha) = 0$. *Por lo tanto,* E *es una extension algebraica.* ■

Nuestro siguiente objetivo es demostrar que cualesquiera dos campos de descomposición sobre el campo F de un polinomio $f(x) \in F[x]$, son isomorfos. Para esto, consideremos dos campos isomorfos F y $\overline{F}$, con el isomorfismo $\mu : F \longrightarrow \overline{F}$ dado por $a \longmapsto \overline{a}$. Por la propiedad universal del anillo F, este isomorfismo se puede extender a un único isomorfismo $\mu' : F[x] \longrightarrow \overline{F}[x]$ tal que $a \longmapsto \overline{a}$ y $x \longmapsto x$, en otras palabras, se cumple que

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longmapsto \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0}$$

Veremos que el isomorfismo μ puede ser extendido a un isomorfismo de E a $\overline{E}$, donde E es el campo de descomposición para $f(x)$ y $\overline{E}$ el campo de descomposición para $\overline{f(x)}$, con $\overline{f(x)} = \mu'(f(x))$. Para esto, demostraremos primero el caso para un elemento algebráico y su correspondiente polinomio mínimo.

Lema 5 *Sean* F *y* $\overline{F}$ *campos y* $\mu : F \longrightarrow \overline{F}$ *un isomorfismo. Sean* E *y* $\overline{E}$ *extensiones de campo para* F *y* $\overline{F}$ *respectivamente. Si* $r \in E$ *es algebráico sobre* F *con polinomio mínimo* $g(x) \in F[x]$ *entonces* μ *puede ser extendida a un monomorfismo* $\zeta : F(r) \longrightarrow \overline{E}$ *si y sólo si* $\overline{g}(x)$ *tiene una raíz en* $\overline{E}$, *en cuyo caso el número de dichas extensiones es igual al numero de raíces distintas de* $\overline{g}(x)$ *en* $\overline{E}$.

Demostración. Sea $\mu : F \longrightarrow \overline{F}$ un isomorfismo, E y $\overline{E}$ extensiones de campo para F y $\overline{F}$ respectivamente. Como $\mu : F \longrightarrow \overline{F}$ es un isomorfismo, por la propiedad universal de F, se tiene un isomorfismo $\overline{\mu} : F[x] \longrightarrow \overline{F}[x]$, con la regla de correspondencia

$$b_n x^n + \cdots b_1 x + b_0 \longmapsto \overline{b_n}x^n + \cdots \overline{b_1}x + \overline{b_0}$$

donde $\overline{b_i} = \mu(b_i)$. Denotaremos a $\overline{\mu}(g(x))$ por $\overline{g}(x)$.

Sea $r \in E$ algebráico con polinomio mínimo $g(x)$. Supongamos primero que $\zeta : F(r) \longrightarrow E$ es una extensión de μ. Sea $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in F, \forall i \in \{1, \ldots, n\}$. Afirmamos que $\zeta(r)$ es una raíz de $\overline{g}(x)$. Por una parte, como $g(r) = 0$ y ζ es un homomorfismo, se tiene que $\zeta(g(r)) = \zeta(0) = 0$.

Por otra parte, al ser ζ un homomorfismo, también se tiene que

$$\begin{aligned}
\zeta(g(r)) &= \zeta(a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0) \\
&= \zeta(a_n r^n) + \zeta(a_{n-1}r^{n-1}) + \cdots + \zeta(a_1 r) + \zeta(a_0) \\
&= \zeta(a_n)\zeta(r^n) + \zeta(a_{n-1})\zeta(r^{n-1}) + \cdots + \zeta(a_1)\zeta(r) + \zeta(a_0) \\
&= \overline{a_n}(\zeta(r))^n + \overline{a_{n-1}}(\zeta(r))^{n-1} + \cdots \overline{a_1}\zeta(r)) + \overline{a_0} \\
&= \overline{g}(\zeta(r))
\end{aligned}$$

donde la penúltima igualdad se debe a que ζ es una extension de μ y $a_i \in F$ para toda i. Por lo tanto, $\overline{g}(\zeta(r)) = 0$, y así $\zeta(r)$ es una raíz de $\overline{g}(x) \in \overline{F}[x]$.

Ahora supongamos que $\overline{g}(x) \in \overline{F}[x]$ tiene una raíz en $\overline{E}$. Sea $\alpha \in \overline{E}$ tal que $\overline{g}(\alpha) = \overline{a_n}\alpha^n + \overline{a_{n-1}}\alpha^{n-1} + \cdots \overline{a_1}\alpha + \overline{a_0} = 0$. Ahora, como $\overline{\mu} : F[x] \longrightarrow \overline{F}[x]$ es un isomorfismo, entonces $g(x)$ es irreducible en $F[x]$ si y sólo si, también lo es $\overline{g}(x)$ en $\overline{F}[x]$. De esta manera, tanto $F(r) \cong F[x]/\langle g(x)\rangle$ como$\overline{F}(\alpha) \cong \overline{F}[x]/\langle \overline{g}(x)\rangle$ son campos. Además, como $\overline{\mu}(g(x)) = \overline{g}(x)$, entonces

$$F(r) \cong F[x]/\langle g(x)\rangle \approxeq \overline{F}[x]/\langle \overline{g}(x)\rangle \cong \overline{F}(\alpha)$$

Sea $\varphi : F(r) \longrightarrow \overline{F}(\alpha)$ la composición de los isomorfismos anteriores. Nótese que φ manda $r \longmapsto \alpha$ y que $\varphi(a) = \mu(a),\ \forall a \in F$. Ahora consideremos el siguiente diagrama:

$$\begin{array}{cccc}
r \in & E & & \overline{E} \quad \ni \alpha \\
 & \uparrow & \nearrow & \uparrow i \\
\varphi: & F(r) & \longrightarrow & \overline{F}(\alpha) \\
 & \uparrow & & \uparrow \\
\mu: & F & \longrightarrow & \overline{F}
\end{array}$$

Consideremos la función $\zeta = (i \circ \varphi) : F(r) \longrightarrow \overline{E}$. Por una parte, como φ es un isomorfismo, en particular es monomorfismo, así como la $i : \overline{F}(\alpha) \longrightarrow \overline{E}$. Como la composición de monomorfismos es monomorfismo, se tiene que ζ también es monomorfismo. Por otra parte, ζ es una extension de μ, ya que $\forall a \in F$ se tiene que $\zeta(a) = (i \circ \varphi)(a) = i(\varphi(a)) = i(\mu(a)) = \mu(a)$.

Por lo tanto, $\zeta : F(r) \longrightarrow \overline{E}$ es un monomorfismo y extiende a μ. Como esta construcción fue para cualquier $\alpha \in \overline{E}$ tal que $\overline{g}(\alpha) = 0$, entonces hay tantas extensiones de μ como raíces de $\overline{g}(x)$ en $\overline{E}$. ■

Hemos visto que el isomorfismo $\mu : F \longrightarrow \overline{F}$ se puede extender a un monomorfismo de $F(r) \longrightarrow \overline{E}$, donde $r \in E_F$ y $\overline{E}$ es una extensión de $\overline{F}$. Ahora, veremos que, dado un polinomio cualquiera $f(x) \in F[x]$ y su campo de descomposición E, este isomorfismo puede ser extendido a un isomorfismo de E a $\overline{E}$, donde $\overline{E}$ es el campo de descomposición para $\overline{f}(x) \in \overline{F}[x]$.

Teorema 41 *Sea $\mu : a \longmapsto \overline{a}$ un isomorfismo del campo F sobre $\overline{F}$, $f(x) \in F[x]$ mónico de grado positivo y $\overline{f(x)}$ el correspondiente polinomio en $\overline{F}[x]$. Sean E y $\overline{E}$ los campos de descomposición para $f(x)$ y $\overline{f(x)}$ sobre F y $\overline{F}$ respectivamente. Entonces μ se puede extender a un isomorfismo de E sobre $\overline{E}$. Además, el numero de extensiones es menor o igual a la dimensión de E sobre F, y es precisamente igual a $|E : F|$ cuando $f(x)$ tiene raíces distintas en $\overline{E}$.*

Demostración. Notemos de nuevo que, como $\mu : F \longrightarrow \overline{F}$ es un isomorfismo, por la propiedad universal de F, se tiene un isomorfismo $\mu' : F[x] \longrightarrow \overline{F}[x]$, con regla de correspondencia

$$a_n x^n + \cdots a_1 x + a_0 \longmapsto \overline{a_n} x^n + \cdots \overline{a_1} x + \overline{a_0}$$

donde $\mu(a_i) = \overline{a_i}$, es decir, $x \longmapsto x$ y μ' extiende a μ. La prueba se hará por inducción sobre $|E : F|$.

Si $|E : F| = 1$ entonces $E = F$. Como F misma es el campo de descomposición de $f(x)$, se tiene que $f(x) = \prod_{i=1}^{n}(x - r_1) \in F[x]$ donde $r_i \in F$. Por otra parte, como μ' es un homomorfismo entre $F[x]$ y $\overline{F}[x]$, se tiene que

$$\mu'(f(x)) = \prod_{i=1}^{n}(x - \overline{r_i}) \in \overline{F}[x]$$

donde $\overline{r_i} = \mu(r_i) \in \overline{F}$. Pero $\overline{f}(x)$ es justamente $\mu'(f(x))$, por lo que

$$\overline{f}(x) = \prod_{i=1}^{n}(x - \overline{r_i}) \in \overline{F}[x],$$

es decir, $\overline{f}(x)$ se descompone en productos lineales en $\overline{F}[x]$, donde las $\overline{r_i}$ son raíces de $\overline{f}(x)$ en $\overline{E}$. Como $\overline{E}$ es el campo de descomposición de $\overline{f}(x)$ sobre $\overline{F}$, y esta generado por las raíces de $\overline{f}(x)$, las cuales están todas en $\overline{F}$, entonces $\overline{E} = \overline{F}(\overline{r_1}, \overline{r_2}, \ldots, \overline{r_n}) = \overline{F}$. Por lo tanto, $\overline{E} = \overline{F}$ y $\left|\overline{E} : \overline{F}\right| = 1$, por lo que hay sólo una extensión de μ, a saber, μ misma.

Supongamos que $|E : F| > 1$ y que se vale para todos los valores menores que $|E : F|$. Demostraremos que se cumple para $|E : F|$. Como $|E : F| > 1$, entonces $f(x)$ no es un producto de factores lineales en $F[x]$. Sea $g(x) \in F[x]$ un factor mónico irreducible de $f(x)$ con grado mayor que uno. Como $g(x) \mid f(x)$ entonces $f(x) = g(x)h(x)$, así que al aplicarle μ' se tiene que

$$\mu'(f(x)) = \mu'(g(x))\mu'(h(x)) = \overline{g}(x)\overline{h}(x),$$

por lo que $\overline{g}(x) \mid \overline{f}(x)$ en $\overline{F}[x]$. Sin pérdida de generalidad podemos suponer que $g(x) = \prod_{i=1}^{m}(x - s_i), f(x) = \prod_{i=1}^{n}(x - s_i)$ en $E[x]$ y $\overline{g}(x) = \prod_{j=1}^{m}(x - r_j), \overline{f}(x) = \prod_{j=1}^{n}(x - r_j)$ en $\overline{E}[x]$, donde $m < n$. Nótese que como $\overline{g}(x) = \prod_{j=1}^{m}(x - r_j)$ en $\overline{E}[x]$, entonces $r_j \in \overline{E}$ es raíz de $\overline{g}(x), \forall j \in \{1, \ldots, m\}$. Además, como $g(x)$ es irreducible en $F[x]$, entonces $\overline{g}(x)$ también es irreducible en $\overline{F}[x]$. Ahora, como s_1 es raíz de $g(x)$ y éste es irreducible en $F[x]$, entonces $g(x)$ es el polinomio mínimo para s_1 sobre F, teniendo así que s_1 es algebráico sobre F. De esta manera, si denotamos a $K = F(s_1)$, se tiene que

$$|F(s_1) : F| = m = \operatorname{grad} g(x).$$

Por el lema anterior, se tiene que existen k monomorfismos $\zeta_1, \ldots, \zeta_k : F(s_1) \longrightarrow \overline{E}$, cada uno extensión de μ, donde k es el número de r_j distintos, con $0 \leq j \leq m$. Ñotemos que si todos los r_j son distintos, entonces $k = m$.

Por otra parte, como E es un campo de descomposición para $f(x)$ sobre F, entonces también lo es sobre el campo K, pues

$$E = F(s_1, \ldots, s_n) = F(s_1)(s_2, \ldots, s_n) = K(s_2, \ldots, s_n)$$

y como $f(x) \in F[x] \subset F(s_1)[x] = K[x]$ se sigue cumpliendo que

$$f(x) = (x - s_1) \bullet \cdots \bullet (x - s_n) \in E[x].$$

De la misma manera, $\overline{E}$ es un campo de descomposición para $\overline{f}(x)$ sobre $\zeta_i(K)$, ya que $\zeta_i(K) = \overline{F}(r_j)$ para algún $j \in \{1, \ldots, m\}$. Como $|E : F| = |E : K| \bullet |K : F|$ entonces

$$|E : K| = |E : F| / |K : F| = |E : F| / m < |E : F|,$$

por lo que se le puede aplicar la hipótesis de inducción a $|E : K|$. Por lo tanto, cada ζ_i puede ser extendida a un isomorfismo de E sobre $\overline{E}$, y el número de dichas extensiones es menor o igual a $|E : K|$, y la igualdad se da cuando $\overline{f}(x)$ tiene raíces distintas en $\overline{E}$. Notemos que si η es una extensión de alguna ζ_i, entonces η sigue siendo una extension de μ, debido a que

$$\forall a \in F, \eta(a) = \zeta_i(a) = \mu(a) = \overline{a} \in \overline{F}.$$

Si denotamos a $\Delta = \{\eta_k \mid \eta_k \text{ es extension para alguna } \zeta_i\}$ entonces se tiene que $|\Delta| \leq m\ |E : K| = |E : F|$, es decir, el número de extensiones de μ es menor o igual a $|E : F|$ y justamente $|E : F|$ cuando $\overline{f}(x)$ tiene raíces distintas en $\overline{E}$.

Para terminar la demostración, falta ver que en este cálculo hemos contado todas las posibles extensiones de μ. Si ω es un isomorfismo entre E y $\overline{E}$ tal que extiende a $\mu : F \longrightarrow \overline{F}$, entonces si nos restringimos a $F(s_1)$ tenemos que ω manda a la raíz s_1 de $f(x)$ en una raíz r_j de $\overline{f}(x)$, coincidiendo de esta manera con ζ_i para alguna $i \in \{1, \ldots, k\}$. Por lo tanto, $\omega \in \Delta$ y de esta manera se tiene que se han contado todas las extensiones de μ. ■

Como caso particular, si consideramos a $F = \overline{F}$, y $\mu = id : F \longrightarrow \overline{F}$, se tiene que si E y $\overline{E}$ son dos campos de descomposición de $f(x)$ sobre F, entonces existe por lo menos un isomorfismo entre E y $\overline{E}$ tal que, restringido a F es la función identidad. Nos referiremos a este isomorfismo como el isomorfismo sobre F de E a $\overline{E}$. De esta manera, se tiene que el campo de descomposición de un polinomio $f(x) \in F[x]$ es único, salvo isomorfismos.

Consideremos ahora una extensión algebráica E de F y $\alpha, \beta \in E$. Denotaremos a $irr(\alpha, F)$ como el *polinomio mínimo en* $F[x]$ *asociado a* α. Veremos ahora que α y β tienen las mismas propiedades algebráicas si y sólo si $irr(\alpha, F) = irr(\beta, F)$. Esto lo haremos dando un isomorfismo de $F(\alpha)$ a $F(\beta)$ tal que deje fijo a F y mande $\alpha \longmapsto \beta$.

Definición 32 *Sea E una extensión algebráica de F. Dos elementos α y β son conjugados sobre F si $irr(\alpha, F) = irr(\beta, F)$, es decir, tienen el mismo polinomio mínimo sobre F.*

Teorema 42 *Sea F un campo y α, β algebraicos sobre F con* $\operatorname{grad} irr(\alpha, F) = n$. *Entonces la función $\psi : F(\alpha) \longrightarrow F(\beta)$ definida por $\psi(c_n\alpha^n + c_{n-1}\alpha^{n-1} \cdots + c_1\alpha + c_0) \longmapsto c_n\beta^n + c_{n-1}\beta^{n-1} + \cdots + c_1\beta + c_0$ es un isomorfismo si y solo si α y β son conjugados sobre F.*

Demostración. Sea $\psi : F(\alpha) \longrightarrow F(\beta)$ definida como en el teorema y supongamos que ψ es un isomorfismo. Sea

$$irr(\alpha, F) = c_n x^n + c_{n-1}x^{n-1} \cdots + c_1 x + c_0$$

Entonces $c_n\alpha^n + c_{n-1}\alpha^{n-1} \cdots + c_1\alpha + c_0 = 0$ y como ψ es isomorfismo se tiene que $\psi(c_n\alpha^n + c_{n-1}\alpha^{n-1} \cdots + c_1\alpha + c_0) = c_n\beta^n + c_{n-1}\beta^{n-1} \cdots + c_1\beta + c_0 = 0$. Como este ultimo es un polinomio con coeficientes en F tal que evaluado en β es cero entonces $irr(\beta, F) \mid c_n x^n + c_{n-1}x^{n-1} \cdots + c_1 x + c_0 = irr(\alpha, F)$. Veamos ahora que $irr(\alpha, F) \mid irr(\beta, F)$. Como ψ es isomorfismo, podemos considerar a $\psi^{-1} : F(\beta) \longrightarrow F(\alpha)$. Si $d_m x^m + d_{m-1}x^{m-1} + \cdots + d_1 x + d_0 = irr(\beta, F)$ entonces de manera análoga se tiene que $\psi^{-1}(d_m\beta^m + d_{m-1}\beta^{m-1} + \cdots + d_1\beta + d_0) = d_m\alpha^m + d_{m-1}\alpha^{m-1} + \cdots + d_1\alpha + d_0 = 0$ por lo que $irr(\alpha, F) \mid irr(\beta, F)$. Como ambos polinomios son mónicos entonces $irr(\alpha, F) = irr(\beta, F)$.

Supongamos ahora que $irr(\alpha, F) = irr(\beta, F) = p(x)$. Entonces tenemos los homomorfismos de evaluación $\phi_\alpha : F[x] \longrightarrow F(\alpha)$ y $\phi_\beta : F[x] \longrightarrow F(\beta)$ los cuales tienen kernel $\langle p(x) \rangle$. Por lo tanto, por el primer teorema de homomorfismos se tiene que ϕ_α induce un isomorfismo natural $\psi_\alpha$de $F[x]/\langle p(x) \rangle$ a $F(\alpha)$, así como ϕ_β induce un isomorfismo ψ_β de $F[x]/\langle p(x) \rangle$ sobre $F(\beta)$. Esto se vé claro en el siguiente diagrama:

$$\begin{array}{ccccc} & & F[x] & & \\ & \overset{\phi_\alpha}{\swarrow} & \downarrow \gamma & \overset{\phi_\beta}{\searrow} & \\ F(\alpha) & \underset{\psi_\alpha}{\longleftarrow} & F[x]/\langle p(x) \rangle & \underset{\psi_\beta}{\longrightarrow} & F(\beta) \end{array}$$

donde γ es la función $F[x] \longrightarrow F[x]/\langle p(x) \rangle$ definida por los residuos al dividir por $p(x)$. Consideremos ahora $\psi_\beta \circ \psi_\alpha^{-1} : F(\alpha) \longrightarrow F(\beta)$. Como ambas son isomorfismos, entonces la composición vuelve a ser un isomorfismo y además

$$\psi_\beta \circ \psi_\alpha^{-1}(c_n\alpha^n + c_{n-1}\alpha^{n-1} \cdots + c_1\alpha + c_0) = \psi_\beta(\psi_\alpha^{-1}(c_n\alpha^n + c_{n-1}\alpha^{n-1} \cdots + c_1\alpha + c_0))$$

$$= \psi_\beta((c_n x^n + c_{n-1}x^{n-1} \cdots + c_1 x + c_0) + \langle p(x) \rangle) = c_n\beta^n + c_{n-1}\beta^{n-1} \cdots + c_1\beta + c_0$$

por lo que $\psi_\beta \circ \psi_\alpha^{-1}$ está bien definida, teniendo así que $\psi_\beta \circ \psi_\alpha^{-1}$ es la ψ que buscábamos. ■

Para el siguiente resultado, que es un corolario del teorema anterior, usaremos el concepto de *cerradura algebráica* de un campo F, el cual denotaremos por $\overline{F}$. Por ahora, entenderemos como *cerradura algebráica* a la extensión de campo de F más chica tal que, para cualquier polinomio $f(x) \in F[x]$, existe $\omega \in \overline{F}$ tal que $f(\omega) = 0$. Más adelante, profundizaremos el tema de cerradura algebráica.

Corolario 9 *Sea α algebráico sobre el campo F. Para cualquier isomorfismo ψ que mande $F(\alpha)$ sobre algún subcampo de la cerradura algebráica $\overline{F}$, tal que $\psi(a) = a, \forall a \in F$, se cumple que ψ manda α en algún conjugado β de α sobre F. Por otra parte, si α y β son conjugados sobre F, entonces existe un sólo isomorfismo $\psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$ tal que $\psi_{\alpha,\beta}(\alpha) = \beta$ y $\psi_{\alpha,\beta}(a) = a, \forall a \in F$.*

Demostración. Sea $\psi : F(\alpha) \longrightarrow \overline{F}$ un monomorfismo tal que $\psi(a) = a, \forall a \in F$. Notemos que ψ es un isomorfismo si nos restringimos a la imagen de ψ en $\overline{F}$. Sea $irr(\alpha, F) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$, entonces

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

por lo que $0 = \psi(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots a_1\alpha + a_0) = a_n\psi(\alpha)^n + a_{n-1}\psi(\alpha)^{n-1} + \cdots + a_1\psi(\alpha) + a_0$, ya que ψ es un homomorfismo. Por lo tanto, $\psi(\alpha) = \beta$ es otra raíz de $irr(\alpha, F)$, por lo que $irr\,(\beta, F) \mid irr\,(\alpha, F)$. Como ψ es un isomorfismo restringido a la imagen, de manera análoga se tiene que $\psi^{-1} : \operatorname{Im}\psi \longrightarrow F\,(\alpha)$ es un isomorfismo tal que $\beta \longmapsto \alpha$ y $\psi^{-1}\,(a) = a, \forall a \in F \subset \overline{F}$. De esta manera, como β es raíz de $irr\,(\beta, F) = h\,(x)$, entonces

$$0 = \psi^{-1}\,(h\,(\beta)) = h\,(\alpha)$$

ya que $h\,(x) \in F\,[x]$ y ψ^{-1} deja invariante a los elementos de F. Como $h\,(\alpha) = 0$, esto implica que $irr\,(\alpha, F) \mid irr\,(\beta, F)$. Por lo tanto, $irr\,(\alpha, F) = irr\,(\beta, F)$, es decir, β y α son conjugados.

Supongamos ahora que α y β son conjugados. Por el teorema pasado, se tiene un isomorfismo $\psi : F(\alpha) \longrightarrow F(\beta)$ definido por $\psi(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots a_1\alpha + a_0) = a_n\beta^n + a_{n-1}\beta^{n-1} + \cdots a_1\beta + a_0$ tal que $\psi(\alpha) = \beta$. Ahora, para ver que ψ es único, si $\eta : F(\alpha) \longrightarrow \overline{F}$ es cualquier otro isomorfismo, éste queda determinado por los valores que toma sobre F y α, por lo que si $\eta(\alpha) = \beta$ y $\forall a \in F, \eta(a) = a$, entonces claramente $\eta = \psi$. Esto demuestra la unicidad. ■

Si F es un campo y $\mu : F \longrightarrow F$ es un homomorfismo, decimos que μ es un *automorfismo* si es un isomorfismo. Notemos que en este caso, el dominio y el codominio de μ coinciden. A continuación, daremos dos útiles resultados de automorfismos en extensiones de campo.

Proposición 10 *Sea E_F un campo de descomposición de $f(x)$ sobre F, y sea K cualquier subcampo de E_F. Entonces cualquier monomorfismo de K_F en E_F*

que deje fijo a los elementos de F, se puede extender a un automorfismo de E en E.

Demostración. Sea E un campo de descomposición de $f(x) \in F[x]$ y sea K un subcampo de E_F. Haremos la prueba por inducción sobre $|E : K|$. Si $|E : K| = 1$, entonces $E = K$, por lo que si $\varphi : K \longrightarrow E$ es un monomorfismo tal que $\varphi(a) = a, \forall a \in F$ entonces la misma φ es un automorfismo $\varphi : E = K \longrightarrow E$.

Supongamos ahora que $|E:K| = n > 1$, y que la hipótesis de inducción se vale para todos los valores $m < n$. Sea $\varphi : K_F \longrightarrow \overline{K} \subset E_F$ un monomorfismo tal que deja fijo a los elementos de F. Como $|E:K| = n$, E_K es una extensión algebráicaentonces y como $|E:K| > 1$ entonces $\exists r \in E$ tal que $r \in E \setminus K$, con r algebráico sobre K. Consideremos ahora el siguiente diagrama:

$$\begin{array}{ccc} E & & E \\ \uparrow & & \uparrow \\ K(r) & \underrightarrow{\varphi_1} & \overline{K}(r) \\ \uparrow & & \uparrow \\ K & \underrightarrow{\varphi} & \overline{K} \\ \uparrow & & \uparrow \\ F & \underrightarrow{Id} & F \end{array}$$

donde $\overline{K} = \operatorname{Im}\varphi$. Ahora, si $K(r) = E$, entonces por la propiedad universal del anillo K, el homomorfismo φ se puede extender a un homomorfismo $\varphi_1 : E = K(r) \longrightarrow \overline{K}(r)$ tal que $r \longmapsto r$. Notemos que como r es algebráico sobre K, entonces $K(r)$ es un campo de dimensión el grado del polinomio mínimo asociado a r. Por un resultado antes visto, como φ_1 es un homomorfismo del campo $K(r)$ a $\overline{K}(r)$, entonces φ_1 es monomorfismo. Ahora, como $\overline{K}(r) \subset E$, y

$$\varphi_1(E) = \varphi_1(K(r)) \subset \overline{K}(r)$$

con φ_1 inyectivo, se tiene que $E = \overline{K}(r)$, es decir, φ_1 es un automorfismo.

Supongamos entonces que $K(r) \subsetneq E$. De nuevo, por la propiedad universal del anillo K, se tiene una extensión $\varphi' : K(r) \longrightarrow \overline{K}(r)$ de φ tal que $\varphi'(r) = r$. Notemos también que $\varphi' : K(r) \longrightarrow \overline{K}(r)$ es un monomorfismo, pues $K(r)$ es un campo. Consideremos ahora el monomorfismo $\psi : i \circ \varphi_1 : K(r) \longrightarrow E$. Notemos que

$$\forall a \in F,\ \psi(a) = (i \circ \varphi_1)(a) = i(\varphi_1(a)) = i(\varphi(a)) = \varphi(a)$$

es decir, ψ extiende a φ. Además, como $\varphi(f) = f$, para toda $f \in F$, entonces $\psi(f) = f, \forall f \in F$. Por otra parte, notemos que $|E:K(r)| < n$, ya que $r \notin K$, $|K(r):K| > 1$ y

$$n = |E:K| = |E:K(r)|\,|K(r):K|.$$

Por lo tanto, por hipótesis de inducción, como ψ es un monomorfismo de $K(r) \longrightarrow E$ y $|E:K(r)| < n$, entonces ψ se puede extender a un automorfismo $\lambda : E \longrightarrow E$. Basta notar que como ψ es una extensión de φ, entonces λ también es una extensión de φ y de $Id : F \longrightarrow F$. ■

De ahora en adelante, asumiremos que si η es un homomorfismo de E_F a K_F, entonces $\eta\,|_F = Id$, es decir, η deja fijo a todos los elementos de F.

Proposición 11 *Sea E una extensión de campo de F tal que $|E:F| = n$. Sea K otra extensión de campo de F. Entonces el número de monomorfismos de E_F a K_F es a lo más n.*

Demostración. Empecemos notando que si no hay ningún morfismo, se cumple el resultado, pues en este caso, la cantidad de morfismos es cero que es menor que cualquier numero natural. Así, supongamos que existe por lo menos uno y veamos que el resultado es cierto.

Sean E_F y $K_{F'}$ extensiones de campo de F y F' respectivamente. Sea $\zeta : F \longrightarrow F'$ un isomorfismo y sea $\varphi : E_F \longrightarrow K_{F'}$ un monomorfismo tal que $\varphi_{|F} = \zeta$. La prueba se hará por inducción sobre $n = |E : F|$. Para $n = 1$ se tiene que $F = E$, por lo que la única extension de ζ es ella misma, por lo que el número de extensiones de ζ es a lo más $1 = |E : F|$.

Sea $|E : F| = n > 1$. Supongamos que se el resultado se cumple para toda extensión de campo D_F tal que

$$|E : D| = m < n,$$

es decir, que si $\vartheta : D_F \longrightarrow D'_{F'}$ es un isomorfismo, donde $D'_{F'}$ es un subcampo de $K_{F'}$, entonces existen a lo más m monomorfismos $\lambda_i : E_D \longrightarrow K_{D'}$, con $i \in \{1, \ldots, m\}$ tales que $\lambda_i \mid D = \vartheta, \forall i \in \{1, \ldots, m\}$. Como $|E : F| > 1$ entonces existe un elemento $\alpha_1 \in E/F$. De esta manera, se tiene que $|E : F| = |F(\alpha_1) : F|\,|E : F(\alpha_1)|$. Como la extensión E_F es de dimensión finita, entonces se cumple el siguiente diagrama:

$$\begin{array}{ccc} & \overset{\varphi}{\longrightarrow} & \\ E = F(\alpha_1, \alpha_2, \ldots, \alpha_k) & & K \\ \uparrow & & \uparrow \\ \vdots & & \vdots \\ \uparrow & & \uparrow \\ F(\alpha_1) & & F'(\beta_1) \\ \uparrow & & \uparrow \\ F & \underset{\zeta}{\rightarrow} & F' \end{array}$$

Sea $p(x) = x^k + \cdots + a_1 x + a_0$ el polinomio mínimo para α_1 sobre F. Entonces, esto nos induce un isomorfismo $\nu : F(\alpha_1) \longrightarrow F'(\beta_1)$, dado por la regla de correspondencia

$$a_n \alpha_1^{k-1} + \cdots + a_1\alpha_1 + a_0 \longrightarrow \zeta(a_n)\beta^{k-1} + \cdots + \zeta(a_1)\beta_1 + \zeta(a_0)$$

donde $\beta_1 \in K$ es raíz del polinomio $\overline{p}(x) \in F'[x]$, que se obtiene al aplicarle ζ a los coeficientes de $p(x)$. Afirmamos que $\overline{p}(x)$ es el polinomio mínimo para $\beta_1 \in K$. Si $\overline{g}(x) \in F'[x]$ es tal que $\operatorname{grad} \overline{g} < k$ y $\overline{g}(\beta_1) = 0$, entonces $\overline{g}(x) \mid \overline{p}(x)$, por lo que $\overline{p}(x) = \overline{g}(x)\overline{h}(x)$, con $\overline{h}(\beta_1) \in F'(\beta_1)$. Por lo tanto, si nos fijamos en la imagen inversa de $\overline{p}(x)$ se tiene que $p(x) = g(x)h(x)$. Evaluando esto último en α_1, se tiene que $h(\alpha_1) = 0$ o $g(\alpha_1) = 0$, lo cual es una contradicción pues $\operatorname{grad} h(x), \operatorname{grad} g(x) < \operatorname{grad} p(x)$ y $p(x)$ es el polinomio mínimo para α_1.

Por lo tanto, ν es isomorfismo si y solo si α_1 va a dar a una raíz del polinomio $\zeta(p(x))$. Como el $\operatorname{grad} p(x) = k$, entonces el $\operatorname{grad} \overline{p}(x) = k$, por lo que a lo más hay k raíces diferentes. Por lo tanto, el número de isomorfismos entre $F(\alpha_1)$ y $F'(\beta_1)$ es a lo más $\operatorname{grad} p(x) = k = |F(\alpha_1) : F|$.

Ahora, si $E = F(\alpha_1)$ entonces hay a lo mas k isomorfismos de $E = F(\alpha_1)$ a $F'(\beta_1) \subset K$ tal que restringidos a F nos da el isomorfismo $\zeta : F \longrightarrow F'$. Como $|E : F| = |E : F(\alpha_1)|\,|F(\alpha_1) : F| = 1 \bullet |F(\alpha_1) : F| = |F(\alpha_1) : F| = k$, entonces se tienen a lo más k monomorfismos de E_F a $K_{F'}$, cumpliéndose así el resultado.

Si $F(\alpha_1) \neq E$ entonces $|E : F(\alpha_1)| > 1$. Como también $|F(\alpha_1) : F| > 1$ entonces $|E : F(\alpha_1)| < n$ y así le podemos aplicar la hipótesis de inducción a $F(\alpha_1)$ y $\nu : F(\alpha_1) \longrightarrow F'(\beta_1)$. Por lo tanto, si $|E : F(\alpha_1)| = l < n$, se tiene que hay a lo más l monomorfismos $\nu_1, \ldots, \nu_l$ de E a K tales que $\nu_i \mid_{F(\alpha_1)} = \nu, \forall i \in \{1, \ldots, l\}$. Pero por otra parte, los isomorfismos de $F(\alpha_1)$ a $F'(\beta_1)$ son tantos como las maneras de definir el valor de α_1, que vimos que es a lo más k. Por lo tanto, el número de monomorfismos que extienden a ζ es a lo mas $l \bullet k = |E : F(\alpha_1)|\,|F(\alpha_1) : F| = |E : F|$. Si tomamos en particular $\zeta = Id$, se tiene lo deseado. ■

Para finalizar esta sección, daremos un campo de descomposición para el polinomio $f(x) = x^5 - 2 \in \mathbb{Q}[x]$.

Demostración. Sea $E = \mathbb{Q}(r_1 r_2 \ldots r_5)$ donde cada r_i es una raíz distinta de $f(x)$. Notemos primero que $\sqrt[5]{2} \in \mathbb{Q}(\sqrt[5]{2})$ es una raíz para $f(x)$, por lo que $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[5]{2})$. Por el criterio de Eisenstein, con $p = 2$, se tiene que $p \mid 2, p \nmid 1$ y $p^2 \nmid 2$, por lo que $f(x) = x^5 - 2$ es irreducible en $\mathbb{Q}[x]$ y así

$$\left|\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}\right| = \operatorname{grad} f(x) = 5.$$

Consideremos ahora la función $g(x) = x^5 - 1$. Una de sus raíces es $x = 1$, la cual esta en $\mathbb{Q} \subset \mathbb{R}$. Sea w otra raíz de $g(x)$. Como $|w| = 1$ y $w \neq 1$, entonces w^2, w^3, w^4 son distintas entre si y a w. Además, cada w^j es raíz para $g(x)$, ya que $(w^j)^5 - 1 = (w^5)^j - 1 = 1^j - 1 = 1 - 1 = 0$. De esta manera se tiene que $\sqrt[5]{2}w$ es raíz de $f(x)$, así como $\sqrt[5]{2}w^2$, $\sqrt[5]{2}w^3$, $\sqrt[5]{2}w^4$. Por lo tanto, si denotamos a $r_1 = \sqrt[5]{2}, r_2 = w, r_3 = \sqrt[5]{2}w^2, r_4 = \sqrt[5]{2}w^3$ y $r_4 = \sqrt[5]{2}w^4$, se tiene que $E = \mathbb{Q}(r_1 r_2 \ldots r_5) \subset \mathbb{Q}(\sqrt[5]{2}, w) = D$, por lo que D también es un campo de descomposición.

Para demostrar que $D = E$ falta demostrar que $D \subset E$. Como $\sqrt[5]{2}$ es una raíz, entonces $\sqrt[5]{2} \in E$, por lo que $\mathbb{Q}(\sqrt[5]{2}) \subset E$. De esta manera, falta ver que por lo menos una raíz de $g(x)$, distinta del uno, este en E, ya que con tan solo una, las otras se generan al elevar a una potencia menor o igual que cuatro. Sean $\rho_1 \neq \rho_2$ dos raíces de $f(x)$ en E. Como E es campo entonces $\rho_1/\rho_2 = \rho_1 \bullet \rho_2^{-1} \in E$. Por otra parte, $(\rho_1/\rho_2)^5 = \rho_1^5/\rho_2^5 = 2/2 = 1$. Como $\rho_1 \neq \rho_2$, entonces $\rho_1/\rho_2 \neq 1$, por lo que E tiene una raíz quinta de uno, distinta del uno. Por lo tanto, en E también están todas las demás raíces quintas de uno.

$\therefore w \in E$, y así $\mathbb{Q}(\sqrt[5]{2}, w) \subset E$, $\quad \therefore \mathbb{Q}(\sqrt[5]{2}, w) = E$.

Ahora veremos la dimension de $\mathbb{Q}(\sqrt[5]{2}, w)$ sobre $\mathbb{Q}$. Consideremos el siguiente diagrama:

$$\begin{array}{ccccc} & \overset{5}{} & & \overset{s}{} & \\ \mathbb{Q} & \hookrightarrow & \mathbb{Q}(\sqrt[5]{2}) & \hookrightarrow & \mathbb{Q}(\sqrt[5]{2}, w) \\ & \searrow & & \nearrow_{t} & \\ 4 & & \mathbb{Q}(w) & & \end{array}$$

donde $s = \left|\mathbb{Q}(\sqrt[5]{2}, w)) : \ \mathbb{Q}(\sqrt[5]{2})\right|$ y $t = \left|\mathbb{Q}(\sqrt[5]{2}, w) : \mathbb{Q}(w)\right|$. Para ver $|\mathbb{Q}(w) : \mathbb{Q}|$ consideremos lo siguiente:

Sea w es una raíz distinta de la unidad del polinomio $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1)$. De esta manera, queremos ver que $x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ es el polinomio mínimo de w sobre $\mathbb{Q}[x]$. Por una parte,

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

Notemos que $h(x) \in K[x]$ es irreducible si y solo si $h(x + c) \in K[x]$ es irreducible $\forall c \in K$, con K campo. Esto se sigue observando lo siguiente:

$$\begin{array}{ccc} K[x] & & ev_{x+c} \\ i \uparrow & \searrow & \\ K & \underset{i}{\longrightarrow} & K[x+c] \end{array}$$

donde las dos i son inclusiones de K en $K[x]$ y en $K[x+c]$ y ev_{x+c} es el homomorfismo manda $k \longmapsto k, \forall k \in K$ y $x \longmapsto x + c$. Notemos que ev_{x-c} es el homomorfismo inverso de ev_{x+c}, por lo que ev_{x+c} es un isomorfismo de anillos. De esta manera, se tiene que

$$h(x) = f(x)\, g(x) \Longleftrightarrow h(x + c) = f(x + c)\, g(x + c)$$

por lo que h es irreducible en $K[x]$ si y sólo si h es irreducible en $K[x + c]$.

Por lo tanto, basta demostrar que $\frac{(x+1)^p - 1}{(x+1) - 1}$ es irreducible. Si desarrollamos lo anterior se tiene

$$\begin{array}{rl} & \dfrac{\binom{p}{0}x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x + \binom{p}{p} - 1}{x} \\ = & \binom{p}{0}x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1} \end{array}$$

pues $\binom{p}{p} = 1$. De nuevo por el criterio de Eisenstein, se tiene que $p \nmid \binom{p}{0} = 1$, $p^2 \nmid \binom{p}{p-1} = p$, y $p \mid \binom{p}{i}, \forall i \in \{1, \ldots, p-1\}$. Esto ultimo se debe a que como p es primo, $\binom{p}{i} \in \mathbb{N}$ y p se encuentra en el numerador de $\binom{p}{i} = \frac{p!}{(p-i)!i!} = \frac{p(p-1)!}{(p-i)!i!}$, entonces $\frac{(p-1)!}{(p-i)!i!} \in \mathbb{N}$, pues ningún elemento en el denominador divide a p. De esta manera, $\frac{p(p-1)!}{(p-i)!i!} = \binom{p}{i} \in p\mathbb{Z}$, por lo que $p \mid \binom{p}{i}$.

Por lo tanto, $x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}$ es irreducible en $\mathbb{Q}[x+1]$ y entonces también lo es $x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ en $\mathbb{Q}[x]$. Se sigue entonces que w es raíz del polinomio irreducible $x^4 + x^3 + x^2 + x + 1$, con grado 4, por lo que $|\mathbb{Q}(w) : \mathbb{Q}| = 4$.

Por otra parte, tenemos que

$$\begin{array}{rcl} 5s & = & \left|\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}\right| \left|\mathbb{Q}(\sqrt[5]{2}, w) : \mathbb{Q}(\sqrt[5]{2})\right| \\ & = & \left|\mathbb{Q}(\sqrt[5]{2}, w) : \mathbb{Q}\right| = |\mathbb{Q}(w) : \mathbb{Q}| \left|\mathbb{Q}(w) : \mathbb{Q}(\sqrt[5]{2}, w)\right| \\ & = & 4t \end{array}$$

. Entonces, $5s = 4t$, por lo que $5 \mid 4t$, y $4 \mid 5s$. Como $(5,4) = 1$, entonces $5 \mid t, 4 \mid s$. Como s es el grado del polinomio mínimo para w sobre $\mathbb{Q}(\sqrt[5]{2})[x]$, y w es raíz del polinomio $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}(\sqrt[5]{2})[x]$, entonces se tiene que $s \leq 4$, y como $4 \mid s$, entonces $s = 4$. Análogamente, como t es el grado del polinomio mínimo para $\sqrt[5]{2}$ sobre $\mathbb{Q}(w)$, y $\sqrt[5]{2}$ es raíz de $x^5 - 2 \in \mathbb{Q}(w)[x]$, entonces $t \leq 5$. Como $5 \mid t$, por lo que $t = 5$.

Por lo tanto, $D = \mathbb{Q}(\sqrt[5]{2}, w)$ es el campo de descomposición más chico y $\left|\mathbb{Q}(\sqrt[5]{2}, w) : \mathbb{Q}\right| = 5 \bullet 4 = 20$. ■

0.17. Raíces Múltiples

Sea $f(x) \in F[x]$ mónico y de grado positivo . Sea E_F un campo de descomposición para $f(x)$. Entonces, a $f(x)$ la podemos ver en $E[x]$ como

$$f(x) = (x - r_1)^{k_1}(x - r_2)^{k_2} \cdots (x - r_n)^{k_n},$$

donde cada $r_i \in E$, $r_i \neq r_j$ si $i \neq j$. Diremos que r_i es una raíz con multiplicidad k_i de la ecuación $f(x) = 0$. En particular, si $k_i = 1$ entonces la raíz r_i es **simple**. Ahora, si $\overline{E}$ es otro campo de descomposición para $f(x) \in F[x]$, entonces, como se vio anteriormente, existe un isomorfismo $\mu : E_F \longrightarrow \overline{E}_F$ tal que extiende a $Id : F \longrightarrow F$. Por la propiedad universal del anillo E, μ se puede extender a un isomorfismo $\overline{\mu} : E[x] \longrightarrow \overline{E}[x]$ tal que $x \longmapsto x$ y $g \longmapsto \mu(g), \forall g \in E$. Por lo tanto, como

$$f(x) = (x - r_1)^{k_1}(x - r_2)^{k_2} \cdots (x - r_n)^{k_n} \in E[x],$$

entonces

$$\overline{\mu}(f(x)) = (x - \overline{r_1})^{k_1}(x - \overline{r_2})^{k_2} \cdots (x - \overline{r_n})^{k_n}$$

en $\overline{E}[x]$. Como $\overline{E}$ también es campo de descomposición para $f(x) \in F[x]$ y $\overline{\mu}\mid_F = \mu\mid_F = Id_F$, entonces $\overline{\mu}(f(x)) = f(x)$, por lo que

$$f(x) = (x - \overline{r_1})^{k_1}(x - \overline{r_2})^{k_2} \cdots (x - \overline{r_n})^{k_n} \in \overline{E}[x].$$

Entonces, se sigue que las multiplicidades k_i son independientes de la elección del campo de descomposición, en particular, el hecho de que $f(x)$ tenga raíces simples no depende del campo de descomposición.

Queremos demostrar que si F es un campo con característica cero, o F un campo finito, entonces se puede suponer, sin pérdida de generalidad, que todas sus raíces son simples. Supongamos que $f(x) \in F[x]$ se factoriza en primos, es decir, $f(x) = p_1^{k_1}(x)p_2^{k_2}(x) \ldots p_n^{k_n}(x)$ donde $(p_i(x), p_j(x)) = 1, \forall i, j \in \{1, \ldots, n\}$, y $i \neq j$.

Proposición 12 *E_F es un campo de descomposición para $f(x) = p_1^{k_1}(x)p_2^{k_2}(x) \ldots p_n^{k_n}(x)$ si y solo si E_F también lo es para $f_0(x) = p_1(x)p_2(x) \ldots p_n(x)$.*

Demostración. *Esto se sigue notando que $p_i^{ki}(a) = 0 \Longleftrightarrow p_i(a) = 0$, por lo que las raíces de los polinomios $p_i^{k_i}(x)$ y $p_i(x)$ son las mismas. Entonces, en*

el campo de descomposición E_F de $f(x) \in F[x]$, van a estar las raíces de cada $p_i^{k_i}(x), \forall i \in \{1, \dots n\}$, que son las mismas que de las $p_i(x)$. De esta manera, si E_F es un campo de descomposición para $f(x) \in F[x]$, también lo es para $f_0(x) \in F[x]$, ya que E_F está generado por las raíces de del polinomio $f(x)$, las cuales coinciden con las raíces del polinomio $f_0(x)$, por lo que también $f_0(x)$ se expresa como producto de factores lineales en $E_F[x]$. Con un razonamiento similar para $p_i(x)$, se tiene que todo campo de descomposición de $f_0(x)$ sobre F, también lo es para $f(x)$ sobre F. ■

De la última proposición podemos suponer, sin pérdida de generalidad, que $f(x)$ es un producto de primos distintos en $F[x]$, es decir, que la multiplicidad de los factores primos es uno. Notemos también que si $p(x)$ y $q(x)$ son dos polinomios primos distintos en $F[x]$, entonces se tiene que $(p(x), q(x)) = 1$, por lo que existen $a(x), b(x) \in F[x]$ tales que $p(x)a(x) + q(x)b(x) = 1$. Como $F[x] \subset E[x]$ entonces se puede descartar el hecho de que $p(x)$ y $q(x)$ tengan un cero común en $E[x]$. Por lo tanto, si $f(x)$ es un producto de primos distintos, entonces las raíces de estos polinomios primos son distintas entre cada uno de ellos. En particular, $f(x)$ tiene raíces simples si y sólo si sus factores primos lo son.

A continuación, desarrollaremos un criterio para raíces múltiples en $F[x]$ sin tener que tomar un campo de descomposición. Para esto, primero definiremos la derivada de un polinomio.

Definición 33 *Sea F un campo. Definimos la función derivada $\delta : F[x] \longrightarrow F[x]$ por la regla de correspondencia*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longmapsto n a_n x^{n-1} + (n-1)\, a_{n-1} x^{n-2} + \cdots + a_1$$

para cualquier polinomio tal que $\operatorname{grad} f(x) \geq 1$ *y si $f(x) = a_0$, entonces*

$$f(x) = a_0 \longmapsto 0$$

Para fines prácticos, denotaremos a $\delta(f(x)) := f'(x)$. Notemos que $\forall k > 0$, $(x^k)' = k x^{k-1}$ y si $f(x) \in F$, entonces $f'(x) = 0$.

Teorema 43 *Sea $f(x) \in F[x]$ mónico y con grado positivo. Entonces todas las raíces de $f(x)$ en cualquier campo de descomposición E_F son simples, si y sólo si, $(f, f') = 1$.*

Demostración. *Sea $d(x) = (f(x), f'(x))$ en $F[x]$. Hagamos primero el*

regreso. Supongamos que no todas las raíces de $f(x)$ son simples. Entonces $f(x) = (x-r)^k g(x)$, donde $g(r) \neq 0$ y $k > 1$. Si derivamos a $f(x)$, se obtiene $f'(x) = k(x-r)^{k-1} g(x) + (x-r)^k g'(x)$. Notemos que $(x-r)^{k-1}$ es un factor tanto de $f(x)$ como de $f'(x)$, pues $k-1 \geq 1$, por lo que $(x-r)^{k-1} \mid d(x)$. Como $(x-r)^{k-1} \neq 1$, entonces $d(x) \neq 1$.

Ahora supongamos que $f(x) = \prod_{i=1}^{n}(x - r_i) \in E[x]$, donde $r_i \neq r_j$ siempre que $i \neq j$. Afirmamos que $f'(x) = \sum_{i=1}^{n}(x-r_1)\cdots(x-r_{i-1})(x-r_{i+1})\cdots(x-r_n)$.

Procedamos por inducción sobre $n = \operatorname{grad} f(x)$. *Si* $n = 1$, *se tiene que* $f(x) = (x - r_1)$, *por lo que* $f'(x) = 1$. *Así,* $(f(x), f'(x)) = 1$. *Si* $n = 2$, *entonces* $f(x) = (x - r_1)(x - r_2)$, *donde* $f'(x) = 1(x - r_2) + (x - r_1)1 = \sum_{i=1}^{2}(x - r_1)\cdots(x - r_{i-1})(x - r_{i+1})\cdots(x - r_n)$. *Supongamos ahora que vale para toda* $m < n$. *Entonces, si* $f(x) = \prod_{i=1}^{n}(x - r_i) = (x - r_1)\prod_{i=2}^{n}(x - r_i)$ *entonces* $f'(x) = 1\prod_{i=2}^{n}(x - r_i) + (x - r_1)(\prod_{i=2}^{n}(x - r_i))'$. *Como podemos aplicar la hipótesis de inducción sobre* $\prod_{i=2}^{n}(x - r_i)$, *pues tiene grado* $n - 1$, *se tiene que* $(\prod_{i=2}^{n}(x-r_i))' = \sum_{i=2}^{n}(x-r_1)\cdots(x-r_{i-1})(x-r_{i+1})\cdots(x-r_n)$. *Por lo tanto,* $f'(x) = \prod_{i=2}^{n}(x-r_i)+(x-r_1)(\sum_{i=2}^{n}(x-r_2)\cdots(x-r_{i-1})(x-r_{i+1})\cdots(x-r_n)) = \sum_{i=1}^{n}(x - r_1)\cdots(x - r_{i-1})(x - r_{i+1})\cdots(x - r_n)$.

De esta última igualdad, se tiene que $(x - r_i) \nmid f'(x)$, *pues divide a todos los sumandos de* $f'(x)$,*excepto el* $i-$*ésimo. Como estos son los factores de* $f(x)$, *entonces* $(f(x), f'(x)) = 1$. ■

Sea $f(x) \in F[x]$ irreducible. Supongamos que $d(x) = (f(x), f'(x)) \neq 1$. Como $f(x)$ es irreducible, el único polinomio en $F[x]$ que lo divide es $f(x)$ misma y el polinomio constante 1, por lo que $d(x) = f(x)$ y entonces $f(x) \mid f'(x)$. Como $\operatorname{grad} f'(x) < \operatorname{grad} f(x)$, esto implica que $f'(x) = 0$. Ahora, si suponemos que $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, entonces, se tiene que

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

Si F es un campo de característica cero y $f'(x) = 0$, entonces $ia_i = 0, \forall i \in \{1, \ldots, n\}$, por lo que $a_i = 0, \forall i, 1 \leq i \leq n$. Por lo tanto, si F es de característica 0 y $f(x)$ es un polinomio irreducible en $F[x]$, entonces $f'(x) \neq 0$, pues de lo contrario, $f(x) \in F$, contradiciendo que $f(x)$ es irreducible.

Supongamos ahora que F es un campo de característica p, y $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$. Entonces $f'(x) = \sum_{i=1}^{n} ia_i x^{i-1}$. Notemos que $f'(x) = 0$ si y solo si $ia_i = 0, \forall i, 1 \leq i \leq n$. Como F es de característica p y p es primo, entonces $ia_i = 0$ implica que $p \mid i$ ó $p \mid a_i$. Si $p \not| i$, entonces $p \mid a_i$ por lo que $a_i \equiv 0 (\operatorname{mod} p)$. De esta manera se tiene que $f(x) = b_m x^{mp} + b_{m-1}x^{(m-1)p} + \cdots + b_1 x^p + b_0$, la cual lo podemos ver como la composición $g(x^p)$, donde $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$.

Por otra parte, se cumple que $1^p = 1$, y como el producto dentro de F es conmutativo, se tiene que $(ab)^n = a^n b^n$. Ahora, por el teorema del binomio, $(a+b)^p = \sum_{i=0}^{p}\binom{p}{i}a^{p-i}b^i = a^p + b^p + \sum_{i=1}^{p-1}\binom{p}{i}a^{p-i}b^i$. Notemos que los coeficientes $\binom{p}{i} = \frac{p!}{(p-i)!i!}$ son naturales, y como p es primo y los elementos de $(p-i)! \cdot i!$ del denominador son todos menores que p, entonces cada $\binom{p}{i} \in p\mathbb{Z}$, por lo todos son cero en el campo . Por lo tanto, $\sum_{i=1}^{p-1}\binom{p}{i}a^{p-i}b^i = 0$ y entonces $(a + b)^p = a^p + b^p, \forall a, b \in F$.

Lema 6 *Sea* F *un campo con característica* p *y* $a \in F$. *Entonces el polinomio* $x^p - a$ *es irreducible en* $F[x]$ *o es una potencia* p*-ésima en* $F[x]$.

Demostración. *Si* $f(x) = x^p - a$ *es irreducible ya acabamos. Supongamos que no lo es. Entonces* $f(x) = h(x)g(x)$,*con* $h(x), g(x) \in F[x]$, *donde*

$1 \leq \operatorname{grad} g(x) \leq p-1$ *y* $g(x)$ *mónico. Sea* E *el campo de descomposición de* $f(x)$ *sobre* F. *Sea* $b \in E$ *tal que* $b^p = a$. *Esto se puede ya que como* E *es el campo de descomposición de* $f(x)$, *entonces* E *contiene una raíz de* $f(x)$. *Por lo tanto, como* F *es de característica* p, *se tiene que* $x^p - a = x^p - b^p = (x-b)^p$. *Entonces,* $(x-b)^p = g(x)h(x)$. *Por lo tanto,* $g(x) = (x-b)^k$ *para algún* $1 \leq k \leq p-1$. *Como* $g(x) \in F[x]$ *entonces* $b^k \in F$. *Además, como* $k < p$ *se tiene que* $(k,p) = 1$, *por lo que existen* $n, m \in \mathbb{Z}$ *tales que* $nk + mp = 1$. *Por las leyes de exponentes y que* F *es campo, se tiene que* $b^1 = b^{(nk+mp)} = b^{nk} b^{mp} = b^{(k)^n} b^{(p)^m} \in F$, *teniendo así que* $b \in F$. *Por lo tanto,* $x - b \in F[x]$ *y así,* $f(x) = g(x)h(x) = (x-b)^p$ *es una potencia* p*-ésima en* $F[x]$. ■

El teorema pasado caracteriza los polinomios de la forma $x^p - a$ en $F[x]$, con F un campo de característica p, en irreducibles o en potencias $p-$ésimas en $F[x]$. A continuación se construirá un polinomio irreducible que además tenga una raíz multiple.

Consideremos el anillo $\mathbb{Z}_p$, y sea $F = \mathbb{Z}_p(t)$ el campo cociente de la variable independiente t sobre el campo $\mathbb{Z}_p$ con p elementos, es decir, F es el campo de fracciones del anillo de polinomios $\mathbb{Z}_p[t]$. Afirmamos que la clase de t no es una potencia p-ésima en este campo. Supongamos lo contrario, es decir, que $t = (f(t)/g(t))^p$ con $f(t), g(t) \in \mathbb{Z}_p[t]$, y

$$f(t) = a_n t^n + a_{n-1} t^{n-1} \cdots + a_1 t + a_0$$

y

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

Entonces, como $\mathbb{Z}_p$ es de característica p y $f(t), g(t) \in \mathbb{Z}_p[t]$, se tiene que

$$f(t)^p = a_n^p t^{pn} + a_{n-1}^p t^{p(n-1)} + \cdots + a_1^p t^p + a_0^p$$

y

$$g(x) = b_m^p t^{mp} + b_{m-1}^p t^{p(m-1)} + \cdots + b_1^p t^p + b_0^p.$$

Por lo tanto, se tiene que $(b_m^p t^{mp} + b_{m-1}^p t^{p(m-1)} + \cdots + b_1^p t^p + b_0^p)t = a_n^p t^{pn} + a_{n-1}^p t^{p(n-1)} + \cdots + a_1^p t^p + a_0^p$. Notemos que las potencias en $f(t)$ son todas múltiplos de p, mientras que en $g(t)t$ ninguna lo es. Igualando coeficientes se tiene que $a_i^p = 0$, por lo que $(b_m^p t^{mp} + b_{m-1}^p t^{p(m-1)} + \cdots + b_1^p t^p + b_0^p)t = 0$, y esto pasa si y sólo si $b_i^p = 0$, $\forall i = 1, \ldots, m$. Como F es campo, entonces esto pasa si y sólo si $b_i = 0$, lo cual contradice la hipótesis de que $g(t) \neq 0$, por lo tanto, t no es una potencia $p-$ésima. De esta manera, el polinomio $x^p - t$ no puede ser una potencia $p-$ésima. Por el lema anterior, se tiene que el polinomio $x^p - t \in \mathbb{Z}_p(t)[x]$ es irreducible. Ahora, por el criterio de la derivada, se tiene que $(x^p - t)' = px^{p-1} = 0$, por lo que $\left(x^p - t, (x^p - t)'\right) \neq 1$. De esta manera, no todas las raíces de $x^p - t$ son simples, es decir, $x^p - t$ tiene por lo menos una raíz con multiplicidad mayor que uno.

Definición 34 *Decimos que $f(x) \in F[x]$ es separable si sus factores irreducibles tienen raíces distintas.*

De lo anterior, se tienen dos observaciones:

Observación 1 (1). *Si F es un campo con característica cero, entonces cualquier polinomio $f(x) \in F[x]$ es separable.*

Observación 2 (2). *Si F tiene característica p, entonces existen polinomios no separables.*

Definición 35 *Un campo F es perfecto si cualquier polinomio en $F[x]$ es separable.*

Por la Observación (1), se tiene que todos los campos con característica cero son perfectos. El siguiente resultado nos da información cuando el campo tiene característica p.

Teorema 44 *Un campo de característica $p \neq 0$ es perfecto si y sólo si $F = F^p$, donde F^p es el subcampo de potencias $p-$ésimas de elementos de F.*

Demostración. Supongamos primero que $F^p \subsetneq F$ y demostraremos que F no es perfecto. Como $F^p \subsetneq F$, existe $a \in F$ tal que $a \notin F^p$. Como $a \notin F^p$, entonces, por el lema anterior, el polinomio $f(x) = x^p - a$ es irreducible, ya que si fuera una potencia $p-$ésima, entonces $a \in F^p$. Notemos ahora que $(x^p - a)' = px^{p-1} = 0$, por lo que $(f(x), f'(x)) = f(x) \neq 1$. Por lo tanto, $f(x)$ es un polinomio irreducible y no separable, teniendo así que F no es perfecto.

Supongamos ahora que F no es perfecto. Sea $f(x) \in F[x]$ un polinomio irreducible y no separable. Como $f(x)$ es no separable, se tiene que $(f(x), f'(x)) \neq 1$, y al ser F un campo de característica p, por lo visto anteriormente, $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots$. Afirmamos que alguna de estas a_i no es una potencia $p-$ésima. Supongamos lo contrario, es decir, que $a_i = b_i^p, \forall i$, donde $b_i \in F$. Entonces,

$$\begin{aligned} f(x) &= a_0 + a_p x^p + a_{2p} x^{2p} + \cdots = b_0^p + b_p^p x^p + b_{2p}^p x^{2p} + \cdots \\ &= (b_0 + b_p x + b_{2p} x^2 + \cdots)^p \end{aligned}$$

por ser F un campo de característica p. Pero esto último contradice el hecho de que $f(x)$ es irreducible. Por lo tanto, alguna a_i no es una potencia $p-$ésima, es decir, se tiene un $a_i \in F$ tal que $a_i \notin F^p$, teniendo así que $F \neq F^p$. ■

Corolario 10 *Cualquier campo finito es perfecto.*

Demostración. Consideremos la función $\mu : F \longrightarrow F$ con regla de correspondencia $a \longmapsto a^p, \forall a \in F$. Notemos primero que $\operatorname{Im}\mu = F^p$. Por otra parte, se tiene que $\mu(1) = 1^p = 1$ y además, $\mu(ab) = (ab)^p = a^p b^p = \mu(a)\mu(b)$, lo cual demuestra que μ es un homomorfismo de anillos. Ahora, como F es campo, entonces μ es un monomorfismo, y como F es finito, entonces μ también es un epimorfismo. De esta manera, se tiene que μ es un isomorfismo y por lo tanto $F = F^p$. Por el teorema anterior, F es perfecto. ■

0.18. Cerradura Algebráica.

Dado un campo K es natural que nos preguntemos por la existencia de una extensión de campo L de K, tal que, para cualquier polinomio $f(x) \in K[x]$, se cumpla que $f(x)$ tenga una raíz en L. Empezaremos la sección con la siguiente

Proposición 13 *Si K es un campo entonces son equivalentes:*

a) La única extensión algebráica de K es K

b) Si $f(x) \in K[x]$ es irreducible, entonces $\operatorname{grad} f(x) = 1$

c) Para cualquier polinomio no constante $f(x) \in K[x]$, se tiene $\alpha \in K$ tal que $f(\alpha) = 0$.

Demostración. $a) \Longrightarrow b)$. Sea $f(x) \in K[x]$ irreducible. Podemos formar al campo $E = K[x]/\langle f(x)\rangle$, el cual sabemos que es una extensión de campo de K. Por $a), E = K$, por lo que $\operatorname{grad} f(x) = |E : K| = |K : K| = 1$.

$b) \Longrightarrow c)$. Sea $f(x) \in K[x]$ un polinomio no constante. Sea $p(x)$ un factor irreducible de $f(x)$. Como se cumple $b)$, se tiene que $\operatorname{grad} p(x) = 1$, lo cual implica que $p(x) = x - \alpha$, pues éste se puede pedir mónico. Como $p(x) \in K[x]$, $\alpha \in K$, cumpliéndose así que $p(x)$ tiene una raíz en K y por lo tanto, también $f(x)$.

$c) \Longrightarrow a)$. Sea α algebráico sobre K. Sea $p(x) = irr(\alpha, K) \in K[x]$. Entonces $p(x)$ tiene una raíz β en K, por lo que $x - \beta \mid p(x)$. Como $\beta \in K$, entonces $x - \beta \in K[x]$, pero esto implica que $x - \beta = p(x)$, pues éste último es irreducible. Como α también es solución de $p(x)$, se tiene que $\alpha = \beta \in K$. Por lo tanto, todo elemento algebráico está en K, es decir, K es la única extensión algebraica sobre K. ■

Definición 36 *Un campo K es algebraicamente cerrado cuando satisface una(y por lo tanto todas) de las condiciones anteriores.*

El Teorema fundamental del Álgebra nos dice que el campo $\mathbb{C}$ es algebraicamente cerrado. Dados $\varphi : K \longrightarrow L$ un homomorfismo de un campo K a un campo algebraicamente cerrado L, se tiene la propiedad de que ésta puede ser extendida a un homomorfismo de cualquier extensión algebraica E de K en L:

Teorema 45 *Sea $\varphi : K \longrightarrow L$ un homomorfismo de un campo K a un campo algebraicamente cerrado L. Entonces φ puede ser extendido a un homomorfismo de $E \longrightarrow L$, para cualquier extensión algebraica E de K.*

Demostración. Sea E una extensión algebráica de K y $\varphi : K \longrightarrow L$ un homomorfismo. Supongamos que $E = K(\alpha)$ es una extensión simple de K y $p(x) = irr(\alpha, K)$. Consideremos el siguiente diagrama

$$\begin{array}{ccc} & \overline{\varphi} & \\ K[x] & \longrightarrow & L[x] \\ \uparrow & \varphi & \uparrow \\ K & \longrightarrow & L \end{array}$$

donde $\overline{\varphi}(a_n x^n + \cdots + a_0) \longmapsto \varphi(a_n) x^n + \cdots + \varphi(a_0)$. Denotemos a la image de $f \in K[x]$ por $\overline{f} \in L[x]$. De esta manera, se tiene que $\overline{p}(x) = \varphi(p(x)) \in L[x]$. Como L es algebráicamente cerrado, existe $\beta \in L$ tal que $\overline{p}(\beta) = 0$. Por la propiedad universal del anillo $K[\alpha] = K(\alpha)$ se tiene una única extensión $\mu : E = K(\alpha) \longrightarrow L$ de φ, tal que $\mu(\alpha) = \beta$ y $\mu(k) = \varphi(k), \forall k \in K$.

Para el caso general se usará el Lema de Zorn: Definamos al conjunto

$$S = \{(F, \psi) \mid K \subset F \subset E \text{ y } \psi : F \longrightarrow L \text{ es un homomorfismo que extiende a } \varphi\}$$

donde $K \subset F$ significa que K es un subcampo de F. Notemos que $S \neq \varnothing$ ya que la pareja $(K, \varphi) \in S$. Definamos la relación $\leq$ en S por $(F, \psi) \leq (G, \lambda)$ si $F \subset G$ y λ extiende a ψ. La relación $\leq$ es de orden: de la definición de $\leq$ se sigue que $(F, \psi) \leq (F, \psi), \forall (F, \psi) \in S$; si $(F, \psi) \leq (G, \lambda)$ y $(G, \lambda) \leq (F, \psi)$ entonces $F \subset G$ y $G \subset F$, por lo que $F = G$. Como el dominio de ψ y λ coinciden, esto implica que $\lambda = \lambda \mid_G = \lambda \mid_F = \psi$, por lo que $(G, \lambda) = (F, \psi)$. Por último, si $(G, \lambda) \leq (F, \psi) \leq (H, \delta)$ se tiene que $G \subset F \subset H$, y como $\lambda = \psi \mid_G = \psi \mid_{G \cap F} = \delta \mid_{G \cap F} = \delta \mid_G$, ya que $G \cap F = G$ pues $G \subset F$. Por lo tanto, $(G, \lambda) \leq (H, \delta)$. De esta manera se tiene que el conjunto S queda parcialmente ordenado por $\leq$. Sea $C = (F_i, \psi_i)_{i \in I}$ una cadena de elementos de S. Definimos a $F' = \cup_{i \in I} F_i$. Notemos que F' es un subcampo de E ya que para cualesquera dos elementos $x, y \in F'$, éstos pertenecen a un mismo subcampo F_i para alguna $i \in I$, en donde todas las operaciones de un campo se cumplen. Sea $\xi : F' \longrightarrow L$ definida por $\xi(x) = \psi_i(x)$, donde $x \in F_i$ correspondiente a (F_i, ψ_i). Veamos que está bien definida: si $x \in F_i \cap F_j$, sin pérdida de generalidad, podemos suponer que $F_i \subset F_j$. Como C es una cadena, ψ_j extiende a ψ_i, y como $x \in F_i \cap F_j \subset F_i$, se tiene que $\psi_i(x) = \psi_j(x)$, por lo que ξ está bien definida. Además, es claro que ξ extiende a cada ψ_i para $i \in I$ y además $\xi \mid_K = \varphi$. Ahora, si $x, y \in F'$, entonces $x, y \in F_i$ para alguna $i \in I$, por lo que $\xi(xy) = \psi_i(xy) = \psi_i(x)\psi_i(y) = \xi(x)\xi(y)$ y $\xi(1) = \psi_i(1) = 1$,para cualquier $i \in I$, teniendo así que ξ es un homomorfismo que extiende a toda ψ_i, con $i \in I$. Por lo tanto, $(F_i, \psi_i) \leq (F', \xi), \forall i \in I$, cumpliéndose así que toda cadena tiene una cota superior en S.

Por el Lema de Zorn, S tiene un elemento máximo (M, μ). Si $M \subsetneq E$, entonces existe $\alpha \in E \setminus M$ algebráico, por lo que $M(\alpha)$ es una extensión simple de M. Como vimos al principio de la demostración, μ se puede extender a un homomorfismo $\nu : M(\alpha) \longrightarrow L$ de tal manera que $(M, \mu) < (M(\alpha), \nu)$, ya que $M \subsetneq M(\alpha)$, lo cual contradice la hipótesis de elemento maximal de (M, μ). Por lo tanto $M = E$ y μ extiende a φ. ■

El resultado esencial de esta sección es el que cualquier campo K puede ser "incrustado.[en] un campo $\overline{K}$ algebráicamente cerrado que sea algebráico sobre K, siguiéndose así que cualquier extensión algebraica de K puede ser también incrustado en $\overline{K}$, por el teorema anterior.

Lema 7 *Para cualquier campo K, existe una extensión algebráica F, tal que F contiene una raíz para cualquier polinomio no constante con coeficientes en K.*

Demostración. Notemos que para cualquier cantidad finita de polinomios $f_1, \ldots, f_n \in K[x]$, K tiene una extensión algebraica H tal que f_i tiene una raíz en H, para toda $i = 1, \ldots, n$. Esto se sigue al tomar un factor irreducible $p_1(x)$ de $f_1(x)$ y formar la extensión de campo $H_1 = K[x]/\langle p_1(x)\rangle$. Como $K \subset K[x]/\langle p_1(x)\rangle = H_1$, repitiendo este procedimiento, se tiene al campo $H_2 = H_1/\langle p_2(x)\rangle$, donde $p_2(x)$ es un factor irreducible de $f_2(x)$. De esta manera se tiene una torre de subcampos que termina en $H_n = H_{n-1}/\langle p_n(x)\rangle$, donde por construcción, H_n tiene una raíz para cada $p_i(x)$ y por lo tanto para $f_i(x)$.

Denotemos al conjunto de polinomios $f(x) \in K[x]$ no constantes como la familia $\{f_i\}_{i\in I}$ para algún índice I. Formemos el anillo de polinomios sobre el campo K, con tantas variables como elementos en I, es decir, al anillo $K\left[\{x_i\}_{i\in I}\right]$. Sea Ω el ideal generado por los $f_i(x_i)$ en $K\left[\{x_i\}_{i\in I}\right]$. Afirmamos que $\Omega \subsetneq K\left[\{x_i\}_{i\in I}\right]$. Si $\Omega = K\left[\{x_i\}_{i\in I}\right]$, entonces $1 = \sum_{j\in J} \mu_j f_j(x_j)$, donde $J \subset I$ es un subconjunto finito y $\mu_j \in K\left[\{x_i\}_{i\in I}\right]$. Como J es un conjunto finito, entonces existe una extensión algebráica E de K, tal que $f_j(x_j)$ tiene una raíz $\alpha_j \in E$ para toda $j \in J$. Por la propiedad universal del anillo $K\left[\{x_i\}_{i\in I}\right]$, se tiene un homomorfismo $\varphi : K\left[\{x_i\}_{i\in I}\right] \longrightarrow E$ tal que $k \longmapsto k, \forall k \in K$, $x_i \longmapsto 0, \forall i \in I \setminus J$ y $x_j \longmapsto \alpha_j, \forall j \in J$. Por lo tanto,

$$1 = \varphi(1) = \varphi\left(\sum_{j\in J} \mu_j f_j(x_j)\right) = \sum_{j\in J} \varphi\left(\mu_j\right)\varphi\left(f_j(x_j)\right)$$

$$= \sum_{j\in J} \varphi\left(\mu_j\right) f_j\left(\varphi(x_j)\right) = \sum_{j\in J} \varphi\left(\mu_j\right) f_j(\alpha_j) = 0$$

que es claramente una contradicción. Por lo tanto, $\Omega \subsetneq K\left[\{x_i\}_{i\in I}\right]$. Ahora, Ω está contenido en un ideal máximo M de $K\left[\{x_i\}_{i\in I}\right]$. Como M es máximo, $F = K\left[\{x_i\}_{i\in I}\right]/M$ es un campo.

Sea $\omega : K \longmapsto F$ el homomorfismo canónico, es decir, $k \longmapsto k + M$. Este homomorfismo es inyectivo, ya que si $\omega(k) = M$, el neutro de F, entonces $k + M = M$, por lo que $k \in M$. Como M es un ideal máximo, $M \subsetneq K\left[\{x_i\}_{i\in I}\right]$, por lo que M no puede contener unidades, ya que de lo contrario, $1 \in M$ y $M = K\left[\{x_i\}_{i\in I}\right]$. Como cualquier $k \in K \setminus \{0\}$ es una unidad, entonces $M \cap K = \{0\}$, lo cual implica que si $k \in M$ entonces $k = 0, \forall k \in K$. Por lo tanto, ω es un monomorfismo. De esta manera se puede identificar a K con $\operatorname{Im}\omega \subset F$, teniéndose que F es una extensión de K. Denotemos ahora a $\beta_i = x_i + M$. Por la unicidad de la propiedad universal del anillo $K\left[\{x_i\}_{i\in I}\right]$, la proyección

canónica $\rho : K\left[\{x_i\}_{i\in I}\right] \longrightarrow F$ extiende a ω y manda a $x_i \longmapsto x_i + M = \beta_i$, $k \longmapsto k + M := k$. Como ρ es sobre, $F = \operatorname{Im}\rho$, por lo que F está generado por la imagen del conjunto generador de $K\left[\{x_i\}_{i\in I}\right]$, es decir, $F = K\left(\{\beta_i\}_{i\in I}\right)$. Notemos además que, como ρ es un homomorfismo se cumple que para cualquier $f_j(x_j) = a_n x_j^n + a_{n-1}x_{j-1}^{n-1} + \cdots + a_1 x_j + a_0$ se tiene que

$$f_j(x_j) + M = a_n x_j^n + a_{n-1}x_{j-1}^{n-1} + \cdots + a_1 x_j + a_0 + M$$

$$= \left(a_n x_j^n + M\right) + \left(a_{n-1}x_{j-1}^{n-1} + M\right) + \cdots + (a_1 x_j + M) + a_0 + M$$

$$= a_n\left(x_j^n + M\right) + a_{n-1}\left(x_j^{n-1} + M\right) + \cdots + a_1(x_j + M) + (a_0 + M)$$

$$= a_n(x_j + M)^n + a_{n-1}(x_j + M)^{n-1} + \cdots + a_1(x_j + M) + a_0$$

$$= a_n\beta_j^n + a_{n-1}\beta_j^{n-1} + \cdots + a_1\beta_j + a_0 = f_j\left(\beta_j\right)$$

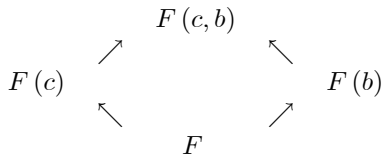
y como $f_j(x_j) \in \Omega \subset M, \forall j \in I$, entonces $f_j\left(\beta_j\right) = f_j(x_j) + M = 0$ en F, es decir, todo polinomio no constante con coeficientes en K tiene una raíz en F, a saber, el correspondiente β_i, por lo que cada β_j es algebráico sobre K. Como $F = K\left(\{\beta_i\}_{i\in I}\right)$, entonces F también es algebráico sobre K. ■

Notemos que en la demostración anterior, se construyó una extensión para una copia de K, concluyéndo que también es una extensión para K. Esto último está basado en el siguiente argumento: si $\varphi : K \longrightarrow F$ es un monomorfismo entre dos campos, se tiene que F es una extensión de campo para $\operatorname{Im}\varphi \cong K$. Si E es un conjunto con la misma cardinalidad de F, entonces se tiene una biyección $E \longrightarrow F$, la cual le da estructura de campo a E. Así mismo, podemos escoger a un conjunto E' tal que $K \subset E'$ y donde K sea un subcampo de E'. Este se forma tomando el conjunto $\wp(F \cup K) \setminus (F \cup K)$ y notando que en general $2|F \cup K| \leq |\wp(F \cup K)|$, por lo que $\wp(F \cup K)$ contiene un subconjunto totalmente ajeno a $F \cup K$. Por lo tanto, si E es otro conjunto con la misma cardinalidad de F y $\xi : E \longrightarrow F$ es un isomorfismo, entonces $\left(E \setminus \xi^{-1}(\operatorname{Im}\varphi)\right) \cup K$ es una extensión de campo de K, que hereda la estructura de campo via ξ^{-1}.

Finalizaremos esta sección demostrando que la cerradura algebraica $\overline{K}$ de un campo K es única salvo isomorfismos. Para esto, se demuestra primero el siguiente

Lema 8 *Si $F \subset K \subset E$ y K es algebráico sobre F y E algebráico sobre K, entonces E es algebráico sobre F.*

Demostración. Sea $\alpha \in E$. Por demostrar que $|F(\alpha) : F|$ es finita. Para esto, observemos que si b, c son algebráicos sobre F, entonces se tiene el siguiente diagrama



Como b, c son algebráicos, $|F(b) : F|$ y $|F(c) : F|$ son finitos. Además, como b satisface un polinomio $g(x) \in F[x] \subset F(c)[x]$, entonces el grado del polinomio mínimo $h(x)$ para b sobre $F(c)$ es menor que el grado de $g(x)$, y como $F(c)(b) = F(c, b)$, entonces se tiene que $\operatorname{grad} h(x) = |F(c, b) : F(c)|$ es finita y menor que $|F(b) : F| = \operatorname{grad} g(x)$. Ahora, como

$$|F(c, b) : F| = |F(c, b) : F(c)|\,|F(c) : F|$$

con $|F(c, b) : F(c)|$ y $|F(c) : F|$ finitos, entonces también $|F(c, b) : F|$ es finita, teniendo así que $F(c, b)$ es una extensión algebráica.

Ahora, como $\alpha \in E$, existe $g(x) = k_n x^n + k_{n-1}x^{n-1} + \cdots + k_1 x + k_0 \in K[x]$ tal que $g(\alpha) = 0$. Como $k_i \in K$, y K es algebráico sobre F, entonces por el razonamiento anterior, $F(k_0, \ldots, k_n)$ es algebráico sobre F. Consideremos ahora el siguiente diagrama

$$\begin{array}{ccccccc} F & \longrightarrow & K & \longrightarrow & K(\alpha) & \longrightarrow & E \\ \downarrow & & & & & \nearrow & \\ F(k_0, \ldots, k_n) & \longrightarrow & F(k_0, \ldots, k_n)(\alpha) & = & F(k_0, \ldots, k_n, \alpha) & & \end{array}$$

donde todas las flechas son inclusiones. Como α satisface $g(x)$, y $g(x) \in F(k_0, \ldots, k_n)[x]$, entonces

$$F(k_0, \ldots, k_n)(\alpha) = F(k_0, \ldots, k_n, \alpha)$$

es algebráico sobre $F(k_0, \ldots, k_n)$, es decir,

$$|F(k_0, \ldots, k_n, \alpha) : F(k_0, \ldots, k_n)| < \infty.$$

Por lo tanto, se tiene que

$$\begin{array}{ccccc} F & \longrightarrow & F(k_0, \ldots, k_n) & \longrightarrow & F(k_0, \ldots, k_n, \alpha) \\ & \searrow & & \nearrow & \\ & & F(\alpha) & & \end{array}$$

y como $|F(k_0, \ldots, k_n) : F|$ y $|F(k_0, \ldots, k_n, \alpha) : F(k_0, \ldots, k_n)|$ son finitas, entonces $|F(\alpha) : F|$ también lo es, por lo que α es algebráico sobre F. ■

Lema 9 *Si $F \subset K \subset E$ con E algebráico sobre F, entonces K es algebráico sobre F y E es algebráico sobre K.*

Demostración. Sea $\beta \in K$. Como $K \subset E$, entonces para $\beta \in E$ existe $g(x) \in F[x]$ tal que $g(\beta) = 0$, es decir, β es algebráico sobre F, $\forall \beta \in K$.

Sea $\alpha \in E$. Como E es algebráico sobre F, existe $f(x) \in F[x]$, tal que $f(\alpha) = 0$. Como $F \subset K$, entonces $F[x] \subset K[x]$, por lo que $f(x) \in K[x]$. Por lo tanto, α es algebráico sobre $K, \forall \alpha \in E$. ■

Teorema 46 *Cualquier campo K tiene una extensión algebráica $\overline{K}$ algebráicamente cerrada. Además, $\overline{K}$ es única salvo isomorfismos.*

Demostración. Por el lema antes visto, podemos suponer que se tiene una torre de campos $K = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_n \subset \cdots$ donde E_{n+1} es algebráico sobre E_n y contiene una raíz por cada polinomio no constante en $E_n[x]$. Además, por el lema anterior, E_n es algebráico sobre K, para toda $n \in \mathbb{N}$. Definimos a $\overline{K} = \cup_{n=0}^{\infty} E_n$. Claramente $K \subset \overline{K}$. Afirmamos que $\overline{K}$ es campo, ya que si $x, y \in \overline{K}$, entonces $x, y \in E_n$ para algún $n \in \mathbb{N}$. Como E_n es campo, entonces x y y se suman, restan, multiplican y dividen en $E_n \subset \overline{K}$, por lo que $\overline{K}$ es campo. Por otra parte, si $\alpha \in \overline{K}$, entonces $\alpha \in E_n$ para algún n, y como E_n es algebráico sobre K, se tiene que α es algebráico sobre K, para cualquier $\alpha \in \overline{K}$.

Sea $\overline{f}(x) \in \overline{K}[x]$ no constante. Como $\overline{f}(x)$ tiene grado finito, todos sus coeficientes caen dentro de un E_k. Por la manera en que se construyó, E_{k+1} tiene una raíz para cualquier polinomio con coeficientes en E_k, por lo que existe $\omega \in E_{k+1}$ tal que $\overline{f}(\omega) = 0$. Como $E_{k+1} \subset \overline{K}$, se tiene que $\overline{K}$ es algebráicamente cerrado. Supongamos ahora que L es una extensión algebráica de K, algebráicamente cerrada. Queremos ver que L y $\overline{K}$ son isomorfmos. Sea $i : K \hookrightarrow L$ el homomorfismo inclusión. Por el teorema anterior, se tiene una extensión $\varphi : \overline{K} \longrightarrow L$ tal que $\varphi \mid_K = Id$. Veamos que φ es inyectiva: Si $\alpha \in \overline{K}$ y $\alpha \neq 0$, es algebráico sobre K, por lo que existe un polinomio $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Supongamos que $f(x) = a_n x^n + \cdots + a_1 x + a_0$ es mínimo y que $\varphi(\alpha) = 0$. Como φ es un homomorfismo y $f(\alpha) = 0$, entonces

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

Como $f(0) = a_0$, se tiene que $f(x) = a_n x^n + \cdots + a_1 x = x\left(a_n x^{n-1} + \cdots + a_1\right)$, lo cual es una contradicción, ya que $f(x)$ es irreducible. Por lo tanto, para cualquier $0 \neq \alpha \in \overline{K}$, $\varphi(\alpha) \neq 0$, es decir, $\ker \varphi = \{0\}$, por lo que φ es inyectiva. De esta manera, se tiene que $\operatorname{Im} \varphi \cong \overline{K}$, y como $K \subset \operatorname{Im} \varphi$, se tiene que $\operatorname{Im} \varphi$ es una extensión algebráica algebráicamente cerrada sobre K. Por otra parte, como L es algebráico sobre K, $\operatorname{Im} \varphi$ es algebráica sobre K y $K \subset \operatorname{Im} \varphi \subset L$, entonces también L es algebráico sobre $\operatorname{Im} \varphi$. Por la primer proposición, como $\operatorname{Im} \varphi$ es algebráicamente cerrado y L es una extensión algebráica de $\operatorname{Im} \varphi$, entonces $\operatorname{Im} \varphi = L$, ya que su única extensión algebráica es ella misma. Por lo tanto, φ es sobre y así, φ es un isomorfismo. ■

0.19. El grupo de Galois

En esta sección daremos las bases para el resultado central de la teoría de Galois. Esta establece que bajo ciertas hipótesis, existe una correspondencia uno a uno entre el conjunto de subcampos de E_F, donde E es un campo de descomposición de un polinomio separable en $F[x]$, y el conjunto de subgrupos del grupo de automorfismos de E_F.

Sea E una extensión de campo de F, y sea $G = \{\eta \mid \eta \text{ es un automorfismo de } E_F\}$, es decir, η es un automorfismo de E tal que $\forall a \in F, \eta(a) = a$. Notemos que G es un grupo de transformaciones de E:

(i) $Id \in G$, pues $Id(a) = a$, $\forall a \in E,$ en particular para $a \in F$.

(*ii*) Si $\mu, \eta \in G$, entonces notemos que $\mu\eta = \mu \circ \eta : E \longrightarrow E$, es tal que $\mu\eta(a) = \mu(\eta(a)) = \mu(a) = a$, $\forall a \in F$, por lo que $\mu\eta \in G$.

(*iii*) Si $\mu \in G$, entonces $\mu : E \longrightarrow E$ es un automorfismo tal que $\mu(a) = a, \forall a \in F$, pero entonces μ^{-1} también es un automorfismo tal que $a = \mu^{-1}(a), \forall a \in F$, por lo que $\mu^{-1} \in G$.

Al conjunto de automorfismos de E_F lo llamaremos el grupo de Galois de E sobre F, y lo denotaremos por $Gal\, E_F$.

Sea G cualquier grupo de automorfismos de un campo E, es decir, un subgrupo del grupo de automorfismos de E. Sea

$$Inv\, G = \{a \in E \mid \eta(a) = a,\, \eta \in G\}.$$

En otras palabras, $Inv\, G$ es el conjunto de elementos en E tales que no son movidos por cualquier η en G. Notemos que $Inv\, G$ forma un subcampo de E :

(*i*) $1 \in Inv\, G$, ya que $\forall \eta \in G, \eta(1) = 1$.

(*ii*) Sean $a, b \in Inv\, G$. Entonces $\forall \eta \in G$, $\eta(a) = a$, $\eta(b) = b$. Como todas las η son automorfismos, se tiene que $\eta(ab) = \eta(a)\eta(b) = ab$, por lo que $ab \in Inv\, G$.

(*iii*) Sea $0 \neq a \in Inv\, G$. Entonces $\forall \eta \in G$, $1 = \eta(1) = \eta(aa^{-1}) = \eta(a)\eta(a^{-1}) = a\eta(a^{-1})$. Como $\eta(a^{-1}) \in E$ y E es un campo, se tiene que el inverso de a es único, por lo que $\eta(a^{-1}) = a^{-1}$, y así, $a^{-1} \in Inv\, G$.

Con esto hemos visto que $Inv\, G$ es un subgrupo, falta ver que la suma es cerrada y conmutativa:

(*iv*) Si $a, b \in Inv\ G$ entonces

$$\eta(a + b) = \eta(a) + \eta(b) = a + b,$$

por lo que $a + b \in Inv\, G$. Como también $\eta(b + a) = b + a$, se tiene que

$$a + b = \eta(a) + \eta(b) = \eta(a + b) = \eta(b + a) = b + a,$$

por lo que $a + b = b + a$.

$\therefore Inv\, G$ es un subcampo de E.

Dado un campo E, las definiciones de $InvG$, con G un grupo de automorfismos en E, y de $GalE_F$ para un subcampo F de E, nos proporcionan dos reglas de correspondencia:

$$\begin{aligned} G &\longmapsto InvG \\ F &\longmapsto GalE_F \end{aligned}$$

El primero va del conjunto de automorfismos de E, al conjunto de subcampos de E, y el segundo va del conjunto de subcampos de E al conjunto de grupos de automorfismos. Las propiedades básicas de estas funciones son:

i) $G_1 \supset G_2 \Longrightarrow InvG_1 \subset InvG_2$

ii) $F_1 \supset F_2 \Longrightarrow GalE_{F_1} \subset GalE_{F_2}$

iii) $F \subset Inv\,(GalE_F)$

iv) $G \subset GalE_{InvG}$

A continuación, se demuestran estos cuatro puntos.

Demostración. *i*) Supongamos que $G_2 \subset G_1$. Sea $x \in InvG_1 = \{a \in E \mid \mu(a) = a, \mu \in G_1\}$, entonces $\mu(x) = x, \forall \mu \in G_1$. Como $G_2 \subset G_1$ entonces en particular se cumple para toda $\eta \in G_2$, es decir, $\eta(x) = x, \forall \eta \in G_2$, por lo que $InvG_1 \subset InvG_2$.

ii) Sean F_1, F_2 campos tales que $F_2 \subset F_1$. Sea $\mu \in GalE_{F_1}$. Entonces, por definición, $\mu(a) = a, \forall a \in F_1$. Como $F_2 \subset F_1$, en particular $\mu(b) = b, \forall b \in F_2$. Como μ ya era un automorfismo de E, entonces $\mu \in GalE_{F_2}$.

iii) Sea $a \in F$ y $\mu \in GalE/F$. Entonces μ es un automorfismo tal que que fija F, por lo que $\mu(a) = a, \forall a \in F$. Como esto fue para toda $\mu \in GalE_F$, entonces $F \subset Inv(GalE_F)$.

iv) $GalE_{InvG}$ consta de los automorfismos de E tal que dejan fijo a $InvG$. Ahora, si $g \in G$, con g un automorfismo de E, y $a \in InvG$, entonces $\mu(a) = a, \forall \mu \in G$, en particular para g. Por lo tanto, $g(a) = a, \forall a \in InvG$, por lo que $G \subset Gal(E_{InvG})$. ■

Supongamos que E es un campo de descomposición del polinomio $f(x) \in F[x]$ sobre el campo F. Consideremos ahora el isomorfismo $Id : F \longrightarrow F$. Entonces, usando un teorema de la sección de extensiones de campos que hace referencia al número de posibles extensiones de un isomorfismo $\mu : F \longrightarrow \overline{F}$ a un isomorfismo $\overline{\mu} : E \longrightarrow \overline{E}$, donde E y $\overline{E}$ son los campos de descomposición de los polinomios $f(x) \in F[x]$ y $\overline{f}(x) \in \overline{F}[x]$ respectivamente, se tiene que $GalE_F$ es finito y además $|GalE_F| \leq |E : F|$. Mas aún, $|GalE/F| = |E : F|$ cuando $f(x)$ tiene raíces distintas. De esto último se tiene el siguiente

Lema 10 *Sea E_F un campo de descomposición de un polinomio separable en $F[x]$. Entonces $|GalE_F| = |E : F|$.*

Demostración. *Como vimos en la sección de raíces múltiples, si $f(x) =$*

$p_1^{k_1}(x)p_2^{k_2}(x)\ldots p_n^{k_n}(x)$ *entonces E_F es el campo de descomposición de $f(x)$ si y sólo si lo es del polinomio $f_0(x) = p_1(x)p_2(x)\ldots p_n(x)$, por lo que podemos suponer que $f(x)$ es un producto de factores primos. Ahora, como $(p_i(x), p_j(x)) = 1$ en $F[x]$ entonces existen $a(x), b(x) \in F[x]$ tales que*

$$p_i(x)\,a(x) + p_j(x)\,b(x) = 1$$

lo cual implica que los $p_i(x)$ no pueden tener raíces en común en E. Además, como $f(x)$ es separable, entonces también lo es $f_0(x)$, lo cual quiere decir que sus factores irreducibles $p_i(x)$ tienen raíces distintas. Por lo tanto, como E es un campo de descomposición de $f_0(x)$ sobre F, se tiene que todas las raíces de $f_0(x)$, y por lo tanto de $f(x)$, son distintas entre sí, por lo que $|GalE/F| = |E : F|$.
■

Ahora veremos un resultado que tiene que ver con el lado de grupos. Consideremos un campo E y cualquier grupo finito G de automorfismos de E. Entonces se tiene el siguiente:

Lema 11 *(Artin) Sea G cualquier grupo finito de automorfismos del campo E y sea $F = InvG$. Entonces $|E : F| \leq |G|$.*

Demostración. *Sea $n = |G|$. Basta demostrar que cualquier combinación de m elementos en E son linealmente dependientes sobre F si $m > n$, pues de esta manera, la dimensión del espacio vectorial de E sobre F será menor o igual que n. Supongamos que*

$G = \{g_1 = Id, g_2, \ldots, g_n\}$, y sean $u_1, u_2, \ldots, u_m \in E$ con $m > n$. Como $m > n$ entonces el sistema lineal de n ecuaciones con m incógnitas

$$\left\{\begin{array}{c} g_1(u_1)x_1 + g_1(u_2)x_2 + \cdots + g_1(u_m)x_m = 0 \\ g_2(u_1)x_1 + g_2(u_2)x_2 + \cdots + g_2(u_m)x_m = 0 \\ \vdots \\ g_n(u_1)x_1 + g_n(u_2)x_2 + \cdots + g_n(u_m)x_m = 0 \end{array}\right\}$$

$$= \left\{\begin{array}{c} \sum_{j=1}^{m} g_1(u_j)x_j = 0 \\ \sum_{j=1}^{m} g_2(u_j)x_j = 0 \\ \vdots \\ \sum_{j=1}^{m} g_n(u_j)x_j = 0 \end{array}\right\} \ldots\ldots (1)$$

con $1 \leq i \leq n$, tiene una solución no trivial $\widehat{x} = (a_1, a_2, \ldots, a_m)$, es decir, $\widehat{x} \neq \widehat{0}$. Sin pérdida de generalidad, podemos tomar la solución $(a_1, a_2, \ldots, a_m)$ con la menor cantidad de ceros posibles. Reordenando a $(a_1, a_2, \ldots, a_m)$ podemos suponer también que $a_1 \neq 0$. Como $a_1 \neq 0$, entonces a_1 tiene inverso, por lo que

$$a_1^{-1}(a_1, a_2, \ldots, a_m) := (b_1, b_2, \ldots, b_m),$$

donde $b_j = a_1^{-1}a_j$, también es solución, ya que como $(a_1, a_2, \ldots, a_m)$ lo es, entonces cumple el sistema (1), si éste lo multiplicamos por a_1^{-1}, se sigue cumpliendo el mismo sitema, teniendo así que $a_1^{-1}(a_1, a_2, \ldots, a_m)$ también es solución. Aseguramos que $b_j \in F = InvG, \forall j = 1, \ldots, m$, ya que si éste es el caso, de la primera ecuación del sistema (1), se tendría que $u_1 + u_2b_2 + \cdots + u_mb_m = 0$, es decir, el conjunto $\{u_1, u_2, \ldots, u_m\}$ sería linealmente dependiente sobre F.

Supongamos que $b_j \notin F = InvG$ para alguna $j \in \{2, \ldots, m\}$, ya que $b_1 = a_1a^{-1} = 1$. Sin pérdida de generalidad, podemos suponer que $b_j = b_2 \neq 0$. Por definición de $F = InvG$, existe un $g_k \in G$ tal que $g_k(b_2) \neq b_2$. Aplicando el automorfismo g_k al sistema de ecuaciones (1), evaluado en la solución $(1 = b_1, b_2, \ldots, b_m)$, se tiene el nuevo sistema $\sum_{j=1}^{m} g_k(g_i(u_j))g_k(b_j) = \sum_{j=1}^{m} g_kg_i(u_j)g_k(b_j) = 0$, para cada $i \in \{1, \ldots, n\}$. Notando que, como $g_kg_i \in G, \forall i \in \{1, \ldots, n\}$,entonces el conjunto $(g_kg_1, g_kg_2, \ldots, g_kg_n)$ es una permutación de $\{g_1, g_2, \ldots, g_n\}$, por lo que este último sistema tiene la forma $\sum_{j=1}^{m} g_i(u_j)g_k(b_j) = 0$, para cada $i \in \{1, \ldots, n\}$. Así, se tiene que $\widehat{y} = (1 = g_k(b_1), g_k(b_2), \ldots, g_k(b_n))$ también es solución de (1). Como el espacio solución del sistema de ecuaciones es cerrado bajo sumas y producto por escalares, entonces $\widehat{x} - \widehat{y}$ también es solu-

ción. Notando que

$$\begin{aligned}\widehat{x}-\widehat{y} &= (1-1, b_2-g_k(b_2), \ldots, b_n-g_k(b_n)) \\ &= (0, b_2-g_k(b_2), \ldots, b_n-g_k(b_n))\end{aligned}$$

es una solución no trivial, pues $g_k(b_2) \neq b_2$, *se llega a la contradicción de que* $\widehat{x}-\widehat{y}$ *es una solución con menos entradas distintas de cero que* $\widehat{x} = (1 = b_1, b_2, \ldots, b_m)$. *Por lo tanto,* $b_j \in F, \forall j \in \{1, \ldots, m\}$ *y así,* $|E : F| \leq n = |G|$. ■

Definición 37 *Sea* E_F *una extensión algebráica. Se dice que* E *es separable si para cualquier elemento de* E, *su respectivo polinomio mínimo es separable. Una extensión algebráica* E_F *es normal si cualquier polinomio irreducible en* $F[x]$ *que tenga raíz en* E, *es un producto de factores lineales en* $E[x]$.

Proposición 14 E_F *es una extensión algebráica normal si y sólo si* E *contiene un campo de descomposición para el polinomio mínimo de cualquier elemento de* E.

Demostración. Supongamos primero que E_F es una extensión algebraica normal. Sea $\alpha \in E$ y sea $p(x) \in F[x]$ su polinomio mínimo asociado. Como E_F es una extensión algebráica normal y $\alpha \in E$ es raíz del polinomio mínimo $p(x)$ entonces $p(x) = \prod_{i=1}^{k}(x - r_i) \in E[x]$, donde $k = \operatorname{grad} p(x), r_i \in E, \forall i \in \{1, \ldots, k\}$ y $\alpha = r_i$, para alguna $i \in \{1, \ldots, k\}$. De esta manera se tiene la siguiente cadena:

$$F \hookrightarrow F(r_1) \hookrightarrow F(r_1 r_2) \hookrightarrow \cdots \hookrightarrow F(r_1 r_2 \ldots r_k) \hookrightarrow E$$

Por lo tanto, $F(r_1 r_2 \ldots r_k)_F$ es un subcampo de E_F. Por la manera en que se construyó $F(r_1 r_2 \ldots r_k)$, éste es un campo de descomposición para $p(x)$.

Supongamos ahora que E contiene un campo de descomposición para el polinomio mínimo de cualquier elemento en E. Sea $\alpha \in E$ y $p\,(x) \in F\,[x]$ su polinomio mínimo. Queremos ver que $p(x)$ es un producto de factores lineales en $E[x]$. Por hipótesis, E contiene un campo de descomposición para $p(x)$. Sea K_F dicho campo de descomposición. Entonces $p(x) = \prod_{i=1}^{k}(x - r_i) \in K[x] \subset E[x]$. Por lo tanto, $p(x) = \prod_{i=1}^{k}(x - r_i) \in E[x]$, y así todo polinomio irreducible en $F[x]$ con alguna raíz en E, es producto de factores lineales en $E[x]$. ■

Notemos que si E_F es una extensión normal y separable entonces cada polinomio irreducible de $F[x]$ que tenga una raíz en E es un producto de factores lineales diferentes en $E[x]$. A continuación, se verá un resultados importante que caracteriza a los campos de descomposición de un polinomio separable $f(x) \in F[x]$.

Teorema 47 *Sea E una extensión de campo de F. Entonces las siguientes proposiciones son equivalentes para E_F.*

(1) E es un campo de descomposición del polinomio separable $f(x) \in F[x]$ sobre F

(2) $F = InvG$ para algún grupo G de automorfismos de E

(3) E es una extensión normal y separable con dimensión finita sobre F

Además, si E y F son como en (1) y $G = GalE_F$, entonces $F = InvG$ y si G y F son como en (2) entonces $G = GalE_F$.

Demostración. (1) $\Longrightarrow$ (2). Sea $f(x) \in F[x]$ un polinomio separable y E su campo de descomposición sobre F. Sea $G = GalE_F$ y sea $F' = InvG$. Por definición de $InvG$, se tiene que $F \subset F'$. Ahora, como vimos anteriormente, $InvG$ es un subcampo de E, por lo que F' es un subcampo de E que contiene a F. Además, como $f(x) \in F[x] \subset F'[x] \subset E[x]$, y E es el campo de descomposición para $f(x)$ sobre F, entonces también lo es sobre F'. Afirmamos que $G = GalE_F{}'$.Si $\eta \in GalE_F{}'$, η es un automorfismo de E tal que $\eta(a) = a, \forall a \in F'$. Como $F \subset F'$, en particular $\eta(a) = a, \forall a \in F$, por lo que también $\eta \in GalE_F$. Así, $GalE_F{}' \subset GalE_F$. Sea ahora $\zeta \in GalE_F$.Por definición de F', se tiene que

$$F' = InvG = \{a \in E \mid \eta(a) = a, \eta \in G\}.$$

En particular, para la ζ que tomamos, se tiene que $\zeta(a) = a$ para toda $a \in F'$. De esta manera, como ζ es un automorfismo de E que fija a cada elemento de F', se tiene que $\zeta \in GalE_F{}'$. Por lo tanto, $GalE_F \subset GalE_F{}'$ y así $G = GalE_F = GalE_F{}'$.

Por otra parte, como $F \subset F' \subset E$ entonces

$$|E : F| = |F' : F|\,|E : F'|\,.$$

Además, como E es un campo de descomposición del polinomio separable $f(x)$ sobre F, entonces $|E : F| = |G|$. Como $f(x) \in F[x] \subset F'[x]$ es separable en $F[x]$, entonces también lo es en $F'[x]$, y como E también es campo de descomposición de $f(x)$ sobre F', se tiene que $|E : F'| = |G|$. De esta manera, $|E : F| = |G| = |E : F'|$. Como $|E : F| = |F' : F|\,|E : F'|$ entonces $|F' : F| = 1$, lo cual implica que $F = F'$. Por lo tanto, $F = InvG$, donde $G = GalE_F$, con lo que también se prueba la primera parte de la última proposición.

(2) $\Longrightarrow$ (3). Como $F = InvG$, con G un grupo finito de automorfismos de E, entonces por el lema de Artin, se tiene que $|E : F| \leq |G|$, por lo que la dimensión de E sobre F es finita. Sea $f(x)$ un polinomio irreducible en $F[x]$ tal que tenga una raíz en E. Sea $r \in E$ tal que $f(r) = 0$. Sea $g = \{r = r_1, r_2, \ldots, r_k\}$ la órbita de r bajo G, es decir, $r_i = \eta(r)$, para alguna $\eta \in G$ y $r_i \neq r_j, \forall i \neq j \in \{1, \ldots, k\}$. Nótese que g es finito porque G lo es. Ahora, si $\mu \in G$ entonces el conjunto $\mu(g) = \{\mu(r_1), \mu(r_2), \ldots, \mu(r_k)\}$ es una permutación de g ya que μ es un automorfismo y todas las r_i son distintas. Además, afirmamos que si $f(r) = 0$ entonces $f(r_i) = 0$ para toda i. Sea $\mu \in G$ tal que $\mu(r) = r_i$ y supongamos que

$$f(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0.$$

con $f(r) = 0$. Entonces, como μ es un automorfismo, y

$$f(r) = b_n r^n + b_{n-1} r^{n-1} + \cdots + b_1 r + b_0 = 0,$$

se tiene que

$$0 = \mu(f(r)) = b_n(\mu(r))^n + b_{n-1}(\mu(r))^{n-1} + \cdots + b_1\mu(r) + b_0,$$

es decir, $\mu(r) = r_i$ también es raíz de $f(x)$. De esta manera, $r_i \in g$ es raíz de $f(x)$ para toda $i = 1, \ldots, k$, y por lo tanto, $x - r_i |\ f(x), \forall i \in \{1, \ldots, k\}$.

Sea $h(x) = \prod_{i=1}^{k}(x - r_i) \in E\,[x]$. Como todas las r_i son distintas, entonces $h(x)$ divide a $f(x)$ en $E\,[x]$. Ahora, si $\mu \in G$, por la propiedad universal del anillo E, μ puede ser extendida a un automorfismo $\overline{\mu} : E\,[x] \longrightarrow E\,[x]$, tal que $x \longmapsto x$ y $a \longmapsto \mu(a), \forall a \in E$. Notemos que

$$\overline{\mu}(h(x)) = \overline{\mu}(\prod_{i=1}^{k}(x - r_i)) = \prod_{i=1}^{k}(x - \mu(r_i)) = \prod_{i=1}^{k}(x - r_i),$$

Como esto pasa para cualquier extensión $\overline{\mu}$ de $\mu \in G$, entonces los coeficientes de $h(x)$ son $G-$invariantes. Como $F = InvG$ entonces $h(x) \in F[x]$. Por otra parte, como $f(x) \in F[x]$ es irreducible y $h(x) \mid f(x)$ con $h(x) \in F[x]$, entonces $h(x) = f(x) = \prod_{i=1}^{k}(x - r_i)$, es decir, $f\,(x)$ es un producto de factores lineales distintos en $E[x]$. Por lo tanto, E es separable y normal sobre F.

(3) $\Longrightarrow$ (1). Supongamos que E es normal y separable sobre F y que $|E : F| < \infty$. Entonces podemos suponer que $E = F(r_1, r_2, \ldots, r_l)$, donde cada $r_i \in E$ es algebráico sobre F con $r_i \neq r_j, \forall i, j \in \{1, \ldots, l\}$. Sea $f_i(x)$ el polinomio mínimo en $F[x]$ asociado a cada $r_i \in E$, con $i \in \{1, \ldots, l\}$, .

Como $f_i(x)$ es irreducible en $F[x]$ y E es una extensión separable, entonces $f_i(x)$ es separable, por lo que $f_i(x)$ tiene raíces diferentes. Como además E es un campo normal, entonces cada $f_i(x)$ es un producto de factores lineales en $E[x]$. Por lo tanto, si definimos a $f(x) = \prod_{i=1}^{l} f_i(x)$, se tiene que, como $r_i \neq r_j$, sus factores irreducibles son los $f_i(x)$ definidos anteriormente. Además, $f(x)$ es separable puesto que sus factores irreducibles $f_i(x)$ lo son, y además, como cada $f_i(x)$ es un producto de factores lineales en $E[x]$ entonces también $f(x)$ lo es. De esta manera, se tiene que $f(x) = \prod_{i=1}^{n}(x - s_i) \in E[x]$, donde cada $s_i \in E$. Nótese que, como $s_i \neq s_j, \forall i, j \in \{1, \ldots, n\}$ entonces $F(s_1, s_2, \ldots, s_n) \subset E$ es el campo de descomposición para $f(x) \in F\,[x]$. Pero como $r_1, \ldots, r_l \in E$ también son raíces de $f(x)$, entonces $E = F(r_1, r_2, \ldots, r_l) \subset F(s_1, s_2, \ldots, s_n)$. Por lo tanto,

$$E = F(r_1, r_2, \ldots, r_l) = F(s_1, s_2, \ldots, s_n),$$

y así $E = F(r_1, r_2, \ldots, r_l)$ es el campo de descomposición para el polinomio separable $f(x) = \prod_{i=1}^{l} f_i(x) \in F[x]$.

Para la segunda parte del suplemento, supongamos que $F = InvG$ para G un grupo de automorfismos de E. Bajo esta suposición, del último lema se tiene que $|E : F| \leq |G|$ .Como son equivalentes (2) $\Longleftrightarrow$ (1) entonces E también es un

campo de descomposición para $f(x) \in F(x)$ separable. Por el primer lema de esta sección, se tiene que $|GalE_F| = |E : F|$. Por lo tanto, $|GalE_F| \leq |G|$, y como G es un subgrupo de $GalE_F$, entonces $GalE_F = G$. ■

0.20. El Teorema fundamental de la Teoría de Galois

El siguiente resultado nos dice que bajo ciertas hipótesis de una extensión E_F, se tiene una biyección entre los subcampos de E_F con los subgrupos de G, donde G es el grupo de automorfismos de E que fijan a F.

Teorema 48 *(Teorema Fundamental de la Teoría de Galois). Sea E una extensión de campo de F tal que cumple una, y por lo tanto todas, de las condiciones del teorema anterior. Sea G el grupo de Galois de E sobre F. Sea $\Gamma = \{H \mid H \leq G\}$ y sea Σ el conjunto de campos intermedios entre E y F. Entonces la función $\alpha : H \longmapsto InvH$ y $\beta : K \longmapsto GalE_K$ son inversas, por lo que se tiene una biyección entre Γ y Σ. Además, se cumplen las siguientes propiedades:*

(a) $H_2 \subset H_1 \Longleftrightarrow InvH_1 \subset InvH_2$

(b) $|H| = |E : InvH|$, $|G : H| = |InvH : F|$

(c) H *es normal en* $G \Longleftrightarrow InvH$ *es normal sobre* F. *En tal caso,*

$$GalInvH_F \cong G/H.$$

Demostración. Sea $G = GalE/F$ y $H \leq G$. Sea $K = InvH$. Podemos suponer también que se cumplen las tres hipótesis del teorema anterior, por lo que podemos tomar a $f(x) \in F[x]$ separable tal que E es el campo de descomposición de $f(x)$ sobre F. Notemos que $K = InvH$ es un subcampo de E que contiene a F, ya que como $F = InvG$ y $H \leq G$ entonces $InvG \subset InvH$. Como $f(x) \in F[x] \subset K[x]$, K es un subcampo de E, y E es el campo de descomposición de $f(x)$ sobre F, entonces también E es el campo de descomposición para $f(x)$ sobre $K[x]$, con $f(x)$ separable. Por el teorema de la sección anterior, como $K = InvH$, por el segundo suplemento, se tiene que

$$H = GalE_K = GalE_{InvH} = \beta(K).$$

De esta manera, $\beta \circ \alpha(H) = H$. Además, por el primer lema de la sección anterior, como E es un capo de descomposición para $f(x) \in K[x]$ separable, entonces

$$|H| = |GalE_{InvH}| = |E : K| = |E : InvH|,$$

lo cual muestra la primera parte de (b).

Sea ahora K un subcampo de E_F, y sea $H = GalE_K$. Como $F \subset K$ y $H = GalE_K$, entonces es claro que $H \subset G = GalE_F$, por lo que $H \leq G$. Como E es un campo de descomposición de $f(x) \in K[x]$, con $f(x)$ separable y

$H = GalE_K$, por el primer suplemento del teorema de la sección anterior, se cumple que

$$K = InvH = Inv(GalE_K) = \alpha(GalE_K) = \alpha \circ \beta(K).$$

Por lo tanto, α y β son inversas.

Por otra parte, se demostró al principio de la sección anterior que si G_1 y G_2 son grupos tales que $G_2 \subset G_1$,entonces $InvG_1 \subset InvG_2$, así como si F_1 y F_2 son campos tales que $F_2 \subset F_1$ entonces $GalE_{F_1} \subset GalE_{F_2}$. En particular, tomando $H_1, H_2 \in \Sigma$ se tiene que si $H_2 \subset H_1$, entonces $InvH_1 \subset InvH_2$, y como también $InvH_1, InvH_2 \in \Gamma$ entonces si $InvH_1 \subset InvH_2$ se tiene que $H_2 = GalE_{InvH_2} \subset GalE_{InvH_1} = H_1$, por lo que se tiene (a).

Si $H \in \Sigma$, entonces $|G| = |GalE_F| = |E : F| = |E : InvH|\,|InvH : F|$. Como $|E : InvH| = |H|$, entonces $|G| = |H|\,|InvH : F|$. Pero sabemos también que $|G| = |H|\,|G : H|$, teniendo así que $|H|\,|G : H| = |H|\,|InvH : F|$, por lo que $|G : H| = |InvH : F|$, demostrando (b).

Para el inciso (c), notemos primero que, si $H \in \Sigma$ y $K = InvH \in \Gamma$ entonces $\eta H \eta^{-1}$ es un subgrupo de $G, \forall \eta \in G$. Afirmamos que su campo correspondiente es $\eta(K)$. Sabemos que bajo la correspondencia entre grupos y campos se tiene que el campo correspondiente a $\eta H \eta^{-1}$ es $Inv(\eta H \eta^{-1})$. Entonces

$$\begin{aligned} x \quad &\in \quad Inv(\eta H \eta^{-1}) \Longleftrightarrow \eta H \eta^{-1}(x) = x \Longleftrightarrow H\eta^{-1}(x) = \eta^{-1}(x) \\ &\Longleftrightarrow \quad \eta^{-1}(x) \in InvH \Longleftrightarrow x = \eta(\eta^{-1}(x)) \in \eta(InvH). \end{aligned}$$

Por lo tanto para cualquier $H \in \Sigma, \eta \in G$, $Inv(\eta H \eta^{-1}) = \eta(K)$ donde $K = InvH$. Se sigue entonces que si $H \trianglelefteq G$, como $\eta H \eta^{-1} = H, \forall \eta \in G$, entonces

$$K = InvH = Inv(\eta H \eta^{-1}) = \eta(InvH) = \eta(K),$$

es decir, η deja fijo a $K = InvH$ para cualquier $\eta \in G$. Consideremos ahora las restricciones de $\eta \in G$ a K, denotándolo por $\overline{\eta}$. Como cada $\eta \in G$ manda K en sí mismo, $\overline{\eta}$ es un automorfismo de K_F que además fija a F. Notemos que como $\eta\,(K) = K$, entonces $\eta \circ \mu\,|_K = \eta\,|_K \circ \mu\,|_K$, por lo que $\omega : GalE_F \longrightarrow GalK_F$ con regla de correspondencia $\eta \mapsto \overline{\eta} = \eta\,|_K$ es un homomorfismo. Además, si denotamos a la imagen como $\overline{G}$, entonces es claro que $Inv\overline{G} = F$, por lo que $\overline{G} = GalK_F$. Por el teorema de la sección anterior, como $F = Inv\overline{G}$ y $\overline{G}$ es un grupo finito de automorfismos de K_F, entonces K es un campo normal y separable sobre F. Además, como este último homomorfismo es suprayectivo se tiene que $GalK_F = \overline{G} \cong G/Ker\omega$. Ahora, notemos que el kernel de este homomorfismo son todos los automorfismos $\eta \in G$ tales que $\eta\,|_K = Id_K$. Por la correspondencia ya demostrada, se tiene

$$Ker\omega = GalE_K = GalE_{InvH} = H,$$

por lo que $GalK_F \cong G/H$.

Por otra parte, supongamos que K es normal sobre F. Sea $r \in K$ y sea $f(x) \in F[x]$ el polinomio mínimo asociado a r. Como K es normal, entonces

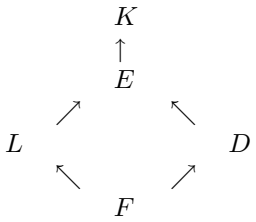
$f(x) = (x - a_1)(x - a_2)\cdots(x - a_k) \in K[x]$, donde, sin pérdida de generalidad, podemos suponer que $a_1 = r$. Además, notemos que para cualquier $\zeta \in G$ se tiene que $0 = \zeta(f(r)) = f(\zeta(r))$, pues ζ es homomorfismo y $\zeta(f) = f, \forall f \in F$. Por lo tanto, $\zeta(r)$ también es una raíz de $f(x), \forall \zeta \in G$, y así, se tiene que $\zeta(r) = a_i$ para alguna $i \in \{1, \ldots, k\}$. Como $a_i \in K$ entonces $\zeta(r) \in K, \forall \zeta \in G$. Como este argumento se cumple para cualquier $r \in K$ entonces $\zeta(K) \subset K, \forall \zeta \in G$. De esto último se sigue que $K \subset \zeta(K), \forall \zeta \in G$, ya que dado $k \in K$, como $\zeta^{-1}(K) \subset K$, entonces $\zeta^{-1}(k) \in K$, por lo que $k = \zeta(\zeta^{-1}(k)) \in \zeta(K)$. Por lo tanto, $K = \zeta(K)$ para toda $\zeta \in G$. Por la observación hecha anteriormente, como $Inv(\eta H \eta^{-1}) = \eta(InvH)$ entonces, si H es el subgrupo en G correspondiente a K, se tiene que $\forall \eta \in G$,

$$Inv(\eta H \eta^{-1}) = \eta(InvH) = \eta(K) = K = InvH.$$

Como ya se demostró la biyección entre Σ y Γ, entonces esta relación es inyectiva, por lo que $\eta H \eta^{-1} = H$, para toda $\eta \in G$, lo cual demuestra que H es normal en G. ■

A continuación, veremos un resultado que nos asocia la unión de campos con la intersección de grupos, así como la intersección de campos con la yunta de dos subgrupos.

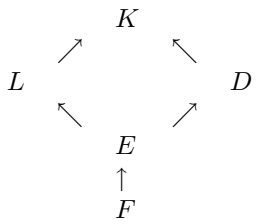
Proposición 15 *Si F, E, D, L, K son campos tales que $E = D \vee L$ y*



donde todas las flechas son inclusiones, entonces $GalK_E = GalK_D \cap GalK_L$, donde la yunta es el subcampo más pequeño que contiene tanto a D como a L en K.

Demostración. Sea $\eta \in GalK_E$, entonces por definición, η es un automorfismo de K tal que fija a E. Como $E = D \vee L$, entonces $D, L \subset E$, por lo que η también fija a D y L, teniendo así que $\eta \in GalK_D$ y $\eta \in GalK_L$, es decir, $\eta \in GalK_D \cap GalK_L$.
Sea $\zeta \in GalK_D \cap GalK_L$. Notemos que para D y L se tiene que $\zeta(D) = D$ y $\zeta(L) = L$, por lo que ζ también fija a todo lo generado por D y L. Como esto último es equivalente al subcampo más pequeño que los contiene, se tiene que $\zeta(D \vee L) = D \vee L = E$. Por lo tanto $\zeta(E) = E, \forall \zeta \in GalK_D \cap GalK_L$, teniendo así que $\zeta \in GalK_E$.
Por lo tanto, $GalK_E = GalK_D \cap GalK_L$. ■

Proposición 16 *Si F, E, D, L, K son campos tales que $E = D \cap L$ y*



donde todas las flechas son inclusiones, entonces $GalK_E = GalK_D \vee GalK_L$, donde la yunta es el menor subgrupo en $G = GalK_F$ que contenga tanto a $GalK_D$ como a $GalK_L$.

Demostración. Por el teorema fundamental de la teoría de Galois, basta demostrar que

$$Inv(GalK_D \vee GalK_L) = Inv(GalK_D) \cap Inv(GalK_L)$$

ya que esta última intersección es equivalente a $D \cap L = E$. De esta manera, se tendría que $Inv(GalK_D \vee GalK_L) = E$, y como se tiene una biyección entre subcampos y subgrupos, entonces

$$GalK_D \vee GalK_L = GalK_E.$$

Sea $x \in Inv(GalK_D \vee GalK_L)$. Entonces $\eta(x) = x, \forall x \in GalK_D \vee GalK_L$. Como $GalK_D, GalK_L \subset GalK_D \vee GalK_L$, entonces en particular $\zeta(x) = x, \forall \zeta \in GalK_D$ y $\forall \zeta \in GalK_L$, por lo que $x \in InvGalK_D$ y $x \in GalK_L$, es decir, $x \in Inv(GalK_D) \cap Inv(GalK_L)$.

Sea $x \in Inv(GalK_D) \cap Inv(GalK_L)$. Como $x \in Inv(GalK_D) \cap Inv(GalK_L)$, entonces $x \in Inv(GalK_D)$ y $x \in Inv(GalK_L)$. Por lo tanto,

$$\eta(x) = x, \forall \eta \in GalK_D \text{ y } \mu(x) = x, \forall \mu \in GalK_L.$$

Como $GalK_D \vee GalK_L$ es el subgrupo generado por $GalK_D$ y $GalK_L$, entonces para cualquier $\zeta \in GalK_D \vee GalK_L$, se tiene que $\zeta(x) = x$. Por lo tanto, $x \in Inv(GalK_D \vee GalK_L)$ y así se tiene la otra contención. ■

Como ejemplo de estos últimos dos resultados, se tiene el siguiente:

Ejemplo 5 *Consideremos el polinomio $f(x) = x^4 - 2$ sobre el campo $\mathbb{Q}$. Empezaremos encontrando un campo de descomposición de $f(x)$ sobre $\mathbb{Q}$. Una raíz de $f(x)$ es $\alpha = \sqrt[4]{2} \in \mathbb{R}$. Las demás son $-\sqrt[4]{2}$, $i\sqrt[4]{2}, -i\sqrt[4]{2}$, de las cuales, las dos últimas, están en $\mathbb{C}$. Si K es el campo de descomposición de $f(x)$ sobre $\mathbb{Q}$, entonces $i = i\sqrt[4]{2}(\sqrt[4]{2})^{-1} = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \in K$. Por otro lado, como $\alpha \in \mathbb{R}$ entonces $\mathbb{Q}(\alpha) \subsetneq \mathbb{R}$, teniendo así que $\mathbb{Q}(\alpha) \neq K$, pues $i \in K$. En cambio, el campo $\mathbb{Q}(\alpha, i)$ contiene a todas las raíces de $f(x)$ por lo que $K = \mathbb{Q}(\alpha, i)$. Por lo tanto, se tiene el siguiente diagrama:*

$$\begin{array}{c} K=\mathbb{Q}(\alpha,i) \\ \uparrow \\ \mathbb{Q}(\alpha) \\ \uparrow \\ \mathbb{Q} \end{array}$$

donde las flechas son inclusiones.

Notemos ahora que el conjunto $\{1,\alpha,\alpha^2,\alpha^3\}$ *es una base para* $\mathbb{Q}(\alpha)$ *sobre* $\mathbb{Q}$ *y* $\{1,i\}$ *un base para* K *sobre* $\mathbb{Q}(\alpha)$*. Por lo tanto,* $\{1,\alpha,\alpha^2,\alpha^3,i,i\alpha,i\alpha^2,i\alpha^3\}$ *es una base para* K *sobre* $\mathbb{Q}$*, por lo que* $|K:\mathbb{Q}|=8$*, y así* $|GalK_{\mathbb{Q}}|=8$*. Queremos entonces encontrar ocho automorfismos de* K *que dejen fijo a* $\mathbb{Q}$*. Si* η *es un automorfismo de* K*, entonces* η *queda determinado por los valores que toma en los elementos de la base, y por como está constituída, estos a su vez están determinados por los valores que toman en* α *e* i*. Como* α *es raíz de* x^4-2*,* $\eta(\alpha)$ *tiene que ir a un conjugado de* α*, es decir,* $\eta(\alpha)$ *tiene que ser una raíz de* x^4-2*. Análogamente, como* i *es raíz de* x^2+1*, entonces* $\eta(i)$ *también tiene que ser raíz de* x^2+1*. Por lo tanto, las cuatro posibles elecciones para* α *y las dos de* i *nos dan los ocho diferentes automorfismos de* K*.*

Por otra parte, por la correspondencia de Galois, se tienen los dos siguientes diagramas

$$\begin{array}{ccccc} & & K=\mathbb{Q}(i,\alpha) & & \\ & \nearrow_4 & \uparrow & \nwarrow_2 & \\ \mathbb{Q}(i) & & 8 & & \mathbb{Q}(\alpha) \\ & \nwarrow_2 & \uparrow & \nearrow_4 & \\ & & \mathbb{Q} & & \end{array}$$

y

$$\begin{array}{ccccc} & & G=GalK_{\mathbb{Q}} & & \\ & \nearrow & & \nwarrow & \\ GalK_{\mathbb{Q}(i)} & & & & GalK_{\mathbb{Q}(\alpha)} \\ & \nwarrow & & \nearrow & \\ & & GalK_K=Id & & \end{array}$$

Notemos lo siguiente:

Como $\mathbb{Q}(\alpha)\vee\mathbb{Q}(i)=K$*, se tiene que* $GalK_{\mathbb{Q}(i)}\cap GalK_{\mathbb{Q}(\alpha)}=GalK_K=Id$*. También, como* $\mathbb{Q}=\mathbb{Q}(\alpha)\cap\mathbb{Q}(i)$*, entonces* $G=GalK_{\mathbb{Q}}=GalK_{\mathbb{Q}(i)}\vee GalK_{\mathbb{Q}(\alpha)}$*. Ahora, como* $\left|GalK_{\mathbb{Q}(i)}\right|=|K:\mathbb{Q}(i)|=4$ *entonces* $\left[G:GalK_{\mathbb{Q}(\alpha)}\right]=2$*, teniendo así que* $GalK_{\mathbb{Q}(i)}\lhd G$*. Por lo tanto, como* $G=GalK_{\mathbb{Q}(i)}\vee GalK_{\mathbb{Q}(\alpha)}$ *y* $GalK_{\mathbb{Q}(\alpha)}\lhd G$*, se tiene que* $G=GalK_{\mathbb{Q}(i)}GalK_{\mathbb{Q}(\alpha)}$*, es decir,* G *es el producto de* $GalK_{\mathbb{Q}(i)}$ *y* $GalK_{\mathbb{Q}(\alpha)}$*. Como además* $GalK_{\mathbb{Q}(i)}\cap GalK_{\mathbb{Q}(\alpha)}=Id$*, tenemos que* $GalK_{\mathbb{Q}(i)}$ *es un complemento para* $GalK_{\mathbb{Q}(\alpha)}$*. Por lo tanto,* G *es el producto semidirecto de* $GalK_{\mathbb{Q}(i)}$ *y* $GalK_{\mathbb{Q}(\alpha)}$*, es decir,*

$$G=GalK_{\mathbb{Q}(i)}\rtimes GalK_{\mathbb{Q}(\alpha)}.$$

Notemos también que G *no es abeliano, ya que sólo* $GalK_{\mathbb{Q}(i)}$ *es normal en* G *y* $G=GalK_{\mathbb{Q}(i)}GalK_{\mathbb{Q}(\alpha)}$

Veamos ahora qué forma tienen $GalK_{\mathbb{Q}(i)}$ y $GalK_{\mathbb{Q}(\alpha)}$. Como

$$\left|GalK_{\mathbb{Q}(\alpha)}\right| = |K : \mathbb{Q}(\alpha)| = 2,$$

entonces $GalK_{\mathbb{Q}(\alpha)} \cong \mathbb{Z}_2$. Por otra parte, $\left|GalK_{\mathbb{Q}(i)}\right| = 4$, por lo que $GalK_{\mathbb{Q}(i)} \cong \mathbb{Z}_4$ o $\mathbb{Z}_2 \times \mathbb{Z}_2$. Para esto, $GalK_{\mathbb{Q}(i)}$ son los automorfismos de K que fijan a $\mathbb{Q}(i)$ y que mandan a α a un conjugado. Si $\tau \in GalK_{\mathbb{Q}(i)}$ es tal que $\alpha \longmapsto i\alpha$ se tiene que: τ^2 manda a $\alpha \longmapsto i(i\alpha) = -\alpha$, τ^3 manda $\alpha \longmapsto i(-\alpha) = -i\alpha$ y finalmente τ^4 manda $\alpha \longmapsto i(-i\alpha) = \alpha$, por lo que $\tau^4 = Id$. Por lo tanto, vemos que τ es un elemento de orden cuatro por lo que $\langle\tau\rangle = GalK_{\mathbb{Q}(i)}$, es decir, $GalK_{\mathbb{Q}(i)} \cong \mathbb{Z}_4$. Como $GalK_{\mathbb{Q}(\alpha)} \cong \mathbb{Z}_2$, entonces $GalK_{\mathbb{Q}(\alpha)} = \langle\rho\rangle$, donde ρ manda $i \longrightarrow -i$, y $\rho^2 = Id$. Analicemos ahora la composición $\rho\tau\rho\tau$ para los valores i y α:

$$\rho\tau\rho\tau(i) = \rho\tau\rho(i) = \rho\tau(-i) = \rho(-i) = i,$$

ya que τ fija a i Si ahora evaluamos en α, se tiene

$$\rho\tau\rho\tau(\alpha) = \rho\tau\rho(i\alpha) = \rho\tau(-i\alpha) = \rho(-i(i\alpha)) = \rho(\alpha) = \alpha,$$

por lo que $\rho\tau\rho\tau = Id$, es decir, $\rho\tau\rho = \tau^{-1}$.

Como G está generado por $GalK_{\mathbb{Q}(i)}$ y $GalK_{\mathbb{Q}(\alpha)}$, que a su vez están generados por los elementos $\langle\tau\rangle$ y $\langle\rho\rangle$, respectivamente, y son tales que $\tau^4 = Id$, $\rho^2 = Id$ y $\rho\tau\rho = \tau^{-1}$, se tiene que $G = D_8$. .

Como una segunda ilustración de la correspondencia de Galois, se obtendrá la teoría de expresiones racionales simétricas. Para esto, definamos primero lo que significa que un polinomio $f(x_1, \ldots, x_n)$ sea simétrico.

Sea R un anillo y $R[x_1, \ldots, x_n]$ el anillo de polinomios sobre R con n indeterminadas. Hemos visto que si π es una permutación $i \longmapsto i'$ del conjunto $\{1, \ldots, n\}$, entonces π determina un automorfismo $\zeta_\pi : R[x_1, \ldots, x_n] \longrightarrow R[x_1, \ldots, x_n]$ tal que $\zeta_\pi \mid_R = Id_R$ y que manda a cada $x_i \longmapsto x_{i'}$, para $1 \leq i \leq n$. Decimos que $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ es simétrico sobre las x_i's si $f(x_1, \ldots, x_n)$ es invariante bajo cualquier automorfismo ζ_π, para cualquier permutación π. Notemos que el conjunto de polinomios simétricos $\sum$ es un subanillo de $R[x_1, \ldots, x_n]$, que claramente contiene a R. Además,

$$\zeta_\pi(\{x_1, \ldots, x_n\}) = \{x_{1'}, \ldots, x_{n'}\} = \{x_1, \ldots, x_n\}.$$

Sea $g(x) = (x - x_1)(x - x_2)\cdots(x - x_n) \in R[x_1, \ldots, x_n][x]$. Afirmamos que los coeficientes de las potencias de x son polinomios simétricos. Por la propiedad universal del anillo $R[x_1, \ldots, x_n]$, cada ζ_π puede ser extendida a un automorfismo

$$\zeta'_\pi : R[x_1, \ldots, x_n][x] \longrightarrow R[x_1, \ldots, x_n][x]$$

tal que $\zeta'_\pi \mid_{R[x_1,\ldots,x_n]} = \zeta_\pi$ y $x \longmapsto x$. De esta manera,

$$\zeta'_\pi(g(x)) = (x - x_{1'})(x - x_{2'})\cdots(x - x_{n'}) = g(x), \forall \zeta'_\pi.$$

Por lo tanto, desarrollando a $g(x) = x^n - p_1x^{n-1} + p_2x^{n-1} + \cdots + (-1)^n p_n$, con $p_i \in R[x_1, \ldots, x_n]$, se tiene que $\zeta_\pi(p_i) = p_i$, para cualquier automorfismo ζ_π y

permutación π, por lo que $p_i \in \sum$. Comparando esta última igualdad de $g(x)$ con el producto de factores lineales, se tiene que

$$\begin{aligned} p_1 &= \sum_{i=1}^{n} x_i, \\ p_2 &= \sum_{i<j} x_i x_j, \\ p_3 &= \sum_{i<j<k} x_i x_j x_k, \\ &\vdots \\ p_n &= x_1 \cdots x_n. \end{aligned}$$

A los polinomios p_i los llamaremos los **polinomios elementales simétricos** en $x_1, \ldots, x_n$.

Sea F un campo y $F[x_1, \ldots, x_n]$ el anillo de polinomios de n indeterminadas sobre F. Sea $F(x_1, \ldots, x_n)$ el campo de fracciones del anillo $F[x_1, \ldots, x_n]$. Si π es una permutación del conjunto $\{1, \ldots, n\}$ entonces se tiene un automorfismo de $F[x_1, \ldots, x_n]$ que fija a F y manda a cada $x_i \longmapsto x_{\pi(i)}$. Como $F(x_1, \ldots, x_n)$ está generado por elementos de la forma ab^{-1}, con $0 \neq b, a \in F[x_1, \ldots, x_n]$, y ζ_π es un automorfismo de $F[x_1, \ldots, x_n]$, se tiene que ζ_π tiene una única extensión a un automorfismo $\acute{\zeta}_\pi$ de $F(x_1, \ldots, x_n)$, a saber,

$$\acute{\zeta}_\pi(ab^{-1}) := \zeta(a)\zeta(b^{-1})$$

donde $\zeta(b^{-1}) = \frac{1}{\zeta(b)}$, la cual está bien definida ya que, al ser $b \neq 0$, $\zeta_\pi(b) \neq 0$. Además, para cualesquiera dos permutaciones, π_1, π_2, se tiene que $\zeta_{\pi_1\pi_2} = \zeta_{\pi_1}\zeta_{\pi_2}$ en $F[x_1, \ldots, x_n]$. Como cada uno de estos automorfismos tiene una única extensión sobre $F(x_1, \ldots, x_n)$, se tiene que también $\acute{\zeta}_{\pi_1\pi_2} = \acute{\zeta}_{\pi_1}\acute{\zeta}_{\pi_2}$ sobre $F(x_1, \ldots, x_n)$. Por lo tanto, el conjunto $\{\acute{\zeta}_\pi\}$ de automorfismos forma un grupo G de automorfismos de $F(x_1, \ldots, x_n)$ isomorfo a S_n. A los elementos invariantes bajo la acción de G los llamaremos **expresiones racionales simétricas** y al conjunto $InvG$ le llamaremos el **campo de expresiones racionales simétricas**. Determinaremos este campo usando la correspondencia de Galois.

Sea $E = F(x_1, \ldots, x_n)$ y $E[x]$ el anillo de polinomios sobre E. Sea

$$g(x) = (x - x_1)(x - x_2) \cdots (x - x_n) \in E[x],$$

el cual lo podemos desarrollar como

$$g(x) = x^n - p_1 x^{n-1} + p_2 x^{n-1} + \cdots + (-1)^n p_n,$$

con los p_i's descritos anteriormente. Ahora, por la propiedad universal del anillo $E = F(x_1, \ldots, x_n)$, cada automorfismo ζ_π de $F(x_1, \ldots, x_n)$ se puede extender a un automorfismo $\acute{\zeta}_\pi$ de $E[x]$, tal que manda $x \longmapsto x$ y $\acute{\zeta}_\pi \mid_E = \zeta_\pi$. De esta manera,

$$g(x) \longmapsto (x - x_{\pi(1)})(x - x_{\pi(2)}) \ldots (x - x_{\pi(n)}) = g(x)$$

ya que π es una permutación de $\{1,\ldots,n\}$. Por lo tanto, $\xi_\pi(g(x)) = g(x)$, para cualquier extensión de algún automorfismo ζ_π y para cualquier $\pi \in S_n$, por lo que $\zeta_\pi(p_i) = p_i$, para todo ζ_π. Por lo tanto, $p_i \in InvG$. Como $F, p_1, \ldots, p_n \in InvG$ entonces $F(p_1,\ldots,p_n)$ es un subcampo de $InvG$.

Por otra parte, notemos que

$$\begin{aligned} E &= F(x_1,\ldots,x_n) = F(x_1,\ldots,x_n,p_1,\ldots,p_n) \\ &= F(x_1,\ldots,x_n)(p_1,\ldots,p_n) = F(p_1,\ldots,p_n)(x_1,\ldots,x_n) \end{aligned}$$

es un campo de descomposición de $g(x)$ sobre $F(p_1,\ldots,p_n)$, donde cada $x_i \neq x_j, \forall i \neq j$.

Sea a $G' = GalE_{F(p_1,\ldots,p_n)}$ y $\rho \in G'$. Como $g(x_i) = 0$, entonces $\rho(g(x_i)) = g(\rho(x_i)) = 0$, por lo que $\rho(x_i)$ es una raíz de $g(x)$. Como esto último sucede para cualquier x_i y cualquier ρ automorfismo de G', se tiene que

$$\rho\,|_{\{x_1,\ldots,x_n\}} = \{x_1,\ldots,x_n\}$$

es decir, ρ permuta los elementos en $\{x_1,\ldots,x_n\}$, por lo que coincide con ζ_π, para algún $\pi \in S_n$. Por lo tanto, $G' = GalE_{F(p_1,\ldots,p_n)} \subset G$. Afirmamos que $G' = G$. Para ver la otra contención, si $\varphi \in G$, φ permuta al conjunto $\{x_1,\ldots,x_n\}$, por lo que también lo fija. De nuevo, por la propiedad universal del anillo E, φ tiene una única extensión $\overline{\varphi} : E[x] \longrightarrow E[x]$ tal que $x \longmapsto x$ y $\overline{\varphi}\,|_E = E$. De esta manera,

$$\begin{aligned} \overline{\varphi}(g(x)) &= \overline{\varphi}((x-x_1)(x-x_2)\cdots(x-x_n)) \\ &= (x-x_{\pi(1)})(x-x_{\pi(2)})\cdots(x-x_{\pi(n)}) = g(x) \end{aligned}$$

donde $\pi \in S_n$ es la permutación asociada a φ. Como $\overline{\varphi}$ es un homomorfismo y $g(x)$ es invariante bajo $\overline{\varphi}$, si desarrollamos el producto de los factores lineales de $g(x)$, se tiene que $\varphi(p_i) = p_i$,para toda i. Como este argumento se cumple para cualquier $\varphi \in G$, entonces

$$\varphi\,|_{F(p_1,\ldots,p_n)} = F(p_1,\ldots,p_n)$$

y así $\varphi \in GalE_{F(p_1,\ldots,p_n)}$, concluyendo que $G = G'$.

De esta manera, por la correspondencia de Galois, se tiene una biyección entre subgrupos de G y los subcampos de E que contienen a $F(p_1,\ldots,p_n)$. Consideremos el siguiente diagrama

$$F(p_1,\ldots,p_n) \quad \hookrightarrow \quad InvG \quad \hookrightarrow \quad F(x_1,\ldots,x_n) = E$$

Por una parte, E es el campo de descomposición de $g(x)$ sobre $F(p_1,\ldots,p_n)$, por lo que E es de Galois sobre $F(p_1,\ldots,p_n)$. Como E es de Galois sobre $F(p_1,\ldots,p_n)$, entonces es una extensión normal y separable, cumpliendo así las hipótesis del teorema fundamental de Galois. Por lo tanto, tenemos que

$$|F(x_1,\ldots,x_n) : F(p_1,\ldots,p_n)| = |G'| = n!.$$

Por otra parte, $GalE_{InvG}$ es un grupo *finito* de automorfismos de E tale que $InvG = Inv\left(GalE_{InvG}\right)$ por lo que también se cumplen las hipótesis del teorema fundamental de Galois. De esta manera, se tiene que

$$|F\left(x_1, \ldots, x_n\right) : InvG| = |G| = n!.$$

Por lo tanto,

$$\begin{aligned} n! &= |F\left(x_1, \ldots, x_n\right) : F\left(p_1, \ldots, p_n\right)| = |E : F\left(p_1, \ldots, p_n\right)| \\ &= |E : InvG|\,|InvG : F\left(p_1, \ldots, p_n\right)| \\ &= |F\left(x_1, \ldots, x_n\right) : InvG|\,|InvG : F\left(p_1, \ldots, p_n\right)| \\ &= n!\,|InvG : F\left(p_1, \ldots, p_n\right)|, \end{aligned}$$

lo cual implica que $|InvG : F\left(p_1, \ldots, p_n\right)| = 1$, es decir, $InvG = F\left(p_1, \ldots, p_n\right)$. De esta manera, se tiene que cualquier polinomio simétrico se puede expresar con polinomios elementales simétricos p_i.

0.21. Grupos Solubles

Sea G un grupo. La sucesión de subgrupos

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_n \rhd G_{n+1} = \{e\}$$

tiene el nombre de **serie normal** para el grupo G. Notemos que sólo se pide que $G_i \rhd G_{i+1}$, es decir, no necesariamente se cumple que $G_i \rhd G$, para cada i.

Definición 38 *Se dice que un grupo G es soluble si existe una serie normal para el grupo G,*

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_n \rhd G_{n+1} = \{e\},$$

tal que G_i/G_{i+1} es abeliano.

Notemos que cualquier grupo abeliano es soluble, pues se tiene la serie normal $G \trianglerighteq \{e\}$ donde $G/\{e\} \cong G$, el cual es abeliano.

Teorema 49 *Cualquier grupo finito G tal que $|G| = p^n$, con p primo, es soluble.*

Demostración. Sea G un p-grupo, es decir, $|G| = p^n$. Se vió anteriormente

que para cualquier p-grupo G, su centro C es no trivial. Si $G \neq C$ entonces definamos a $C_1 = C$. Consideremos el $p-$grupo G/C_1 con centro no trivial de la forma C_2/C_1. Notemos que como C_2/C_1 es abeliano en G/C_1, entonces $C_2/C_1 \lhd G/C_1$. Por el teorema de la correspondencia, se tiene que $C_2 \lhd G$. Si $G \neq C_2$, definimos de la misma manera a C_3 como el subgrupo de G tal que C_3/C_2 es el centro de G/C_2. De esta forma, se tiene la cadena $\{e\} \subsetneq C_1 \subsetneq$

$C_2 \subsetneq \cdots \subsetneq C_k \subsetneq \cdots$ de subgrupos normales en G. Ahora, como G es finito, eventualmente se llega a que $G = C_{s+1}$, por lo que se tiene la serie normal

$$G = C_{s+1} \rhd C_s \rhd \cdots \rhd C_2 \rhd C_1 \rhd \{e\}.$$

Como por construcción, C_{i+1}/C_i es el centro de G/C_i entonces C_{i+1}/C_i es abeliano. Esto demuestra que el grupo es soluble. ■

Sean $g, h \in G$, definimos el **conmutador** *de* g y h como $(g,h) = g^{-1}h^{-1}gh$. De esta manera, se tiene que $gh = hg(g,h)$, por lo que g y h conmutan si y solo si $(g,h) = e$. No siempre se cumple que el conjunto de conmutadores forma un grupo. Por esta razón, se tiene la siguiente

Definición 39 *Dado un grupo G, se define a su* ***subgrupo conmutador*** *G' con el subgrupo de G generado por todos los conmutadores (g,h) tales que $g, h \in G$.*

Notemos que como $(g,h)^{-1} = (g^{-1}h^{-1}gh)^{-1} = (h^{-1}g^{-1}hg) = (h,g)$ entonces G' coincide con el conjunto de productos de la forma $(g_1,h_1)(g_2,h_2)\cdots(g_i,h_i)$ con $g_j, h_j \in G$.

Sea η un homomorfismo de G en algún otro grupo $\overline{G}$. Entonces $\eta((g,h)) = \eta(g^{-1}h^{-1}gh) = \eta(g^{-1})\eta(h^{-1})\eta(g)\eta(h) \in \overline{G}'$. Por lo tanto, $\eta(G') \subset \overline{G}'$. Si además η es un epimorfismo, entonces se tiene la otra contención $\overline{G}' \subset \eta(G')$, por lo que $\eta(G') = \overline{G}'$. Esto se puede aplicar a cualquier endomorfismo η de G.

Supongamos que $K \lhd G$. Entonces cualquier automorfismo de la forma $I_a : G \longrightarrow G$ dado por $x \longmapsto axa^{-1}$ induce un endomorfismo de K, pues este es normal en G. Por lo antes visto, $I_a(K') \subset K'$,$\forall a \in G$, es decir, $aK'a^{-1} \subset K'$, lo cual quiere decir que K' es normal en G. Por lo tanto, se tiene que si $K \lhd G$, entonces $K' \lhd G$. En particular, como $G \lhd G$, se tiene que $G' \lhd G$.

De manera similar, podemos definir el segundo *subgrupo conmutador* como $G'' = (G')'$. Iterando este procedimiento, se tiene al $k-$ésimo conmutador $G^k = (G^{k-1})'$ para $k \geq 1$. Como $G' \lhd G$ entonces $G'' \lhd G$. Usando inducción, se tiene que $G^k \lhd G$, para toda k en $\mathbb{N}$.

Lema 12 *Sea G un grupo y G' su subgrupo conmutador. Entonces G/G' es abeliano y además G' esta contenido en cualquier subgrupo normal K tal que G/K sea abeliano.*

Demostración. De la definición de subgrupo conmutador, se tiene que G

es abeliano si y sólo si $G' = \{e\}$. Supongamos que $K \leq G$ tal que $K \lhd G$ y que G/K es abeliano. Notemos que en G/K, se tiene que $(aK, bK) = (a^{-1}K)(b^{-1}K)(aK)(bK) = a^{-1}b^{-1}abK$. Por lo tanto, si G/K es abeliano entonces $(G/K)' = \{K\}$. Como $(aK, bK) = a^{-1}b^{-1}abK \in K$ entonces esto último pasa si y sólo si $a^{-1}b^{-1}ab \in K$, es decir $(a,b) \in K, \forall a, b \in G$, por lo que $G' \subset K$. En particular, como $G' \lhd G$, entonces G/G' es abeliano. ■

Teorema 50 *Un grupo G es soluble si y solo si $G^{(k)} = \{e\}$ para alguna $1 \leq k \in \mathbb{N}$.*

Demostración. Supongamos que existe una $k \in \mathbb{N}$ tal que $G^{(k)} = \{e\}$.

Entonces se tiene la siguiente sucesión normal

$$G \rhd G' \rhd G'' \rhd \cdots G^{(k-1)} \rhd G^{(k)} = \{e\},$$

donde por el lema anterior, $G^i/G^{(i+1)}$ es abeliano. Por lo tanto, G es soluble.

Supongamos ahora que G es soluble. Entonces se tiene una serie normal $G = G_1 \rhd G_2 \rhd G_3 \cdots G_{n-1} \rhd G_n = \{e\}$, para alguna $n \in \mathbb{N}$, y tal que G_i/G_{i+1} es abeliano. Por el lema anterior, como $G_{i+1} \lhd G_i$ y G_i/G_{i+1} es abeliano, entonces $G_i' \subset G_{i+1}$, para $i \in \{1, \ldots, n-1\}$. Notemos ahora por inducción que $G^{(i)} \subset G_i$, para toda i. Como $G_1 = G$, entonces $G' \subset G = G_1$. Supongamos que $G^{(k)} \subset G_k$, entonces se tiene que $G^{(k+1)} = (G^{(k)})' \subset G_k' \subset G_{k+1}$. Por lo tanto, $G^{(i)} \subset G_i$ para toda i, y como $G_n = \{e\}$, entonces $G^{(n)} = \{e\}$. ■

Del criterio anterior de solubilidad se tiene el siguiente

Teorema 51 *Cualquier subgrupo e imagen homomorfa de un grupo soluble es soluble. Además, si $K \rhd G$, con K y G/K solubles, entonces G es soluble.*

Demostración. Sea H un subgrupo de G. Como $H \subset G$ entonces es claro que $H^{(k)} \subset G^{(k)}$. Como G es soluble, entonces existe una $n \in \mathbb{N}$ tal que $G^{(n)} = \{e\}$. Por lo tanto, para esa misma n, $H^{(n)} = \{e\}$, pues $H^{(n)} \subset G^{(n)} = \{e\}$. Sea η un homomorfismo suprayectivo de G a H. Como hicimos notar anteriormente, $\eta(G') = (\eta(G))'$, así que η restringido a G' es un homomorfismo suprayectivo de G' sobre $\eta(G)'$. De la misma manera, como η es un homomorfismo de G' sobre $\eta(G)'$ entonces

$$\eta((G')') = \eta(G'') = \eta(G')' = (\eta(G))''.$$

Por inducción, suponiendo que $\eta(G^{(i)}) = (\eta(G))^i$, se tiene un homomorfismo suprayectivo de $G^{(i)}$ sobre $\eta(G)^i$. Entonces

$$\eta((G^{(i)})') = \eta(G^{(i+1)}) = (\eta(G)^i)' = \eta(G)^{i+1}.$$

Por lo tanto, $\eta(G^{(i)}) = (\eta(G))^i$, para toda i. Ahora, como G es soluble, existe una $k \in \mathbb{N}$ tal que $G^{(k)} = \{e\}$, teniendo así que

$$\{e\} = \eta(e) = \eta(G^{(k)}) = (\eta(G))^k,$$

demostrando así que $\eta(G)$ es soluble.

Por otra parte, supongamos que K es soluble, con $K \lhd G$, y que G/K también es soluble. Consideremos ahora el homomorfismo natural $\mu : G \longrightarrow G/K$ tal que $g \longmapsto gK$. Este homomorfismo es suprayectivo, por lo que $\mu(G^i) = (G/K)^i$, para toda i. Como G/K es soluble, entonces existe $n \in \mathbb{N}$ tal que $(G/K)^n = \{e\}$. De esta manera, $\mu(G^n) = \{e\}$ en G/K, por lo que $G^n \subset K$.

Ahora, como K es soluble, se tiene una $m \in \mathbb{N}$ tal que $K^m = \{e\}$. Por lo tanto $G^{n+m} \subset K^m = \{e\}$, y así $G^{n+m} = \{e\}$. Esto demuestra que G es soluble. ■

Decimos que un grupo G es **simple** si G y $\{e\}$ son los únicos subgrupos normales de G. Ahora, si G es abeliano, cualquier subgrupo es normal, por lo que G es simple si y sólo si no tiene subgrupos propios distintos del trivial $\{e\}$. Por otra parte, definimos la **serie de composición** de un grupo G como la serie normal

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$$

tal que cada G_{i+1} es un subgrupo normal maximal de G_i, es decir, que no exista un subgrupo normal $H \leq G_i$ tal que $G_{i+1} \subsetneq H \subsetneq G_i$.

Sea $K \lhd G$. Por el teorema de la correspondencia, se tiene una biyección entre los subgrupos de G que contienen a K y los subgrupos de G/K. Además, subgrupos normales van a subgrupos normales. Por lo tanto, se sigue que K es maximal en G si y sólo si G/K es simple y distinto al grupo trivial. Por lo tanto, una serie normal $G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$ es una serie de composición del grupo G si y sólo si G_i/G_{i+1} es simple ($\neq \{e\}$). A estos factores les llamaremos **factores de composición** asociada a la serie de composición.

Sea G un grupo finito. Entonces $G = G_1$ contiene a un subgrupo normal maximal G_2, el cual a su vez contiene a un subgrupo normal maximal G_3, etc. Como G es finito, este procedimiento termina para alguna n, donde $G_n = \{e\}$, construyendo así una serie de composición para G.

Finalizaremos esta sección con un criterio de solubilidad para grupos finitos.

Teorema 52 *Un grupo G finito es soluble si y sólo si cualquier factor de composición G_i/G_{i+1} de la serie de composición $G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$ es cíclico y de orden primo.*

Demostración. Supongamos que G es soluble. Sea

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$$

una serie de composición para G. Por una parte, como G es soluble y $G_i \leq G$ para cualquier i, por el teorema anterior, G_i también es soluble para toda $i \in \{1, \ldots, n\}$. Sea $\eta_i : G_i \longrightarrow G_i/G_{i+1}$ el homomorfismo canónico. Como η_i es suprayectivo y G_i es soluble, por el teorema anterior, G_i/G_{i+1} también es soluble. Ahora, como cada factor de composición es simple, se tiene que la única serie normal para G_i/G_{i+1} es $G_i/G_{i+1} \rhd \{e\}$, y como G_i/G_{i+1}es soluble, se tiene que $(G_i/G_{i+1})/\{e\} \cong G_i/G_{i+1}$ es abeliano. Notemos que como G_i/G_{i+1} es simple, no tiene subgrupos normales distintos al trivial o a G_i/G_{i+1}, por lo tanto, si además es finito y abeliano, se tiene que G_i/G_{i+1} es isomorfo a un grupo cíclico de orden p. Como este argumento se hizo para cualquier G_i/G_{i+1}, se tiene que todos los factores de composición de la serie de composición

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$$

son cíclicos y de orden p, p primo.

Supongamos ahora que G tiene una serie de composición $G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$ tal que cada factor G_i/G_{i+1} es cíclico y de orden primo. Como G_i/G_{i+1} es cíclico entonces es abeliano y por lo tanto se tiene una serie normal

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$$

tal que cada G_i/G_{i+1} es abeliano, es decir, G es soluble. ■

0.22. Criterio de Galois para la solubilidad por radicales

Sea F un campo y $f(x) \in F[x]$ un polinomio. Necesitamos definir lo que significa que la ecuación $f(x) = 0$ sea soluble por radicales.

Definición 40 *Sea $f(x) \in F[x]$ mónico de grado positivo. Decimos que la ecuación $f(x) = 0$ es **soluble por radicales** sobre F si existe una extensión de campo K_F tal que tenga una torre de subcampos de la siguiente manera:*

$$F = F_1 \subset F_2 \subset \cdots \subset F_{n-1} \subset F_n = K$$

tal que cada $F_{i+1} = F_i(d_i)$, donde $d_i \in F_{i+1}$ es tal que $d_i^{n_i} = a_i \in F_i$, para alguna $n_i \in \mathbb{N}$ y que K contenga un campo de descomposición para $f(x)$ sobre F.

A esta última sucesión de torres de subcampos, se le llama *torre de raíces de K sobre F*. Notemos que cada F_{i+1} se obtiene adjuntando una raíz $\sqrt[n_i]{a_i}$ de la ecuación $x^{n_i} - a_i = 0$ al campo F_i. Como todas las raíces de $f(x)$ están contenidas en K, cada una se encuentra en algún F_k de la sucesión, por lo que cualquier raíz de $f(x)$ se obtiene por medio de operaciones racionales a los elementos del campo base junto con soluciones de ecuaciones de la forma $x^n = a$.

Supongamos ahora que $f(x)$ tiene raíces distintas en un campo de descomposición E_F. Definimos ahora el **grupo de galois** del polinomio $f(x)$, o de la ecuación $f(x) = 0$ como el grupo de Galois del campo de descomposición E_F. Como cualesquiera dos campos de descomposición de $f(x)$ sobre F son isomorfos, entonces este grupo está bien definido y es independiente de la elección del campo de descomposición. Sea $f(x) = \prod_{i=1}^{n}(x - r_i) \in E[x]$, con $E = F(r_1, \ldots, r_n)$ y donde $R = \{r_1, r_2, \ldots, r_n\}$ son las distintas raíces de $f(x)$ en E. Veremos que uno puede identificar el grupo de Galois $GalE_F$ con el grupo de permutaciones del conjunto de raíces R.

Si $\eta \in GalE_F$ entonces η manda R en sí misma, pues manda raíces en raíces, por lo que a η la podemos ver como una permutación del conjunto R. De esta manera se tiene un homomorfismo $f : GalE_F \longrightarrow S_n$, donde S_n es el grupo simétrico de permutaciones de $R = \{r_1, r_2, \ldots, r_n\}$. Como las r_i generan a E_F

y para cualquier $\mu \in GalE_F$, ésta queda determinada por los valores en los r_i, se tiene que f es un homomorfismo inyectivo, por lo que su imagen, que denotaremos por G_f, es un subgrupo de S_n isomorfo a $G = GalE_F$.

Nuestro deseo es poder encontrar un criterio de solubilidad por radicales de cualquier ecuación $f(x) \in F[x]$. Los siguientes lemas nos ayudarán a probar el siguiente

Criterio 53 *La ecuación $f(x) = 0$ es soluble por radicales sobre el campo F de característica 0 si y sólo si su grupo de Galois es soluble.*

De ahora en adelante, nos referiremos al campo de descomposición de $x^n - 1$ sobre el campo F como el **campo ciclotómico de orden n sobre F.**

Hemos visto que un grupo G de orden n es cíclico si y sólo si existe a lo más un subgrupo cíclico por cada divisor del orden. Esto equivale a decir que si G es un grupo cíclico de orden n y d es un divisor de n, entonces hay a lo más d soluciones en G de la ecuación $x^d = 1$. Notemos que si dos subgrupos cíclicos de orden d fueran distintos, entonces la ecuación $x^d - 1$ tendría más de d soluciones, lo cual es una contradicción.

Proposición 17 *Si F es un campo y G es un subgrupo finito de la parte multiplicativa de F, entonces G es cíclico. Además, si F es un campo finito, entonces el grupo multiplicativo de F es cíclico.*

Demostración. Si $|G| = n$ y $a \in G$ es tal que $a^d = 1$, con d un divisor de n, entonces a es una raíz del polinomio $x^d - 1 \in F[x]$. Como un polinomio de grado d sobre un campo tiene a lo más d raíces, por la observación anterior, tenemos que esto es equivalente a que G tenga un y sólo un subgrupo cíclico de orden d, donde $d \mid n$. Por lo tanto, G es cíclico.

Ahora, si F es finito, entonces el grupo multiplicativo F^* de elementos distintos de cero de F es un subgrupo finito. Como $F^* \leq F^*$ y F^* es finito, entonces F^* es cíclico. ■

Empezaremos entonces con el primer

Lema 13 *El grupo de Galois de un campo ciclotómico de orden n sobre F de característica cero es abeliano.*

Demostración. *Como $(x^n - 1)' = nx^{n-1}$ y F es de característica cero, entonces $(x^n - 1, nx^{n-1}) = 1$, por lo que $x^n - 1$ tiene n distintas raíces. Sea $U = \{z_1, \ldots, z_n\}$ el conjunto de las distintas raíces y E_F el campo ciclotómico de orden n sobre F. Como $z_i \neq 0, \forall i = 1, \ldots, n$, U forma un subgrupo de la parte multiplicativa del campo F. y que, como ya se demostró, este subgrupo es cíclico. Consideremos ahora la función $f : G \longrightarrow AutU$, donde G es el grupo de Galois del campo ciclotómico y $AutU$ los automorfismos de U en U definida, por $f(\eta) = \eta \mid U$. Como todas las funciones de G son automorfismos de E_F, y cada automorfismo queda determinado por los valores que toma en las raíces de $x^n - 1$, se tiene que f es un monomorfismo, por lo que $G \cong \operatorname{Im} f \leq AutU$. Por otra parte, si $h \in AutU$ entonces, al ser U cíclico se tiene que h manda*

generadores en generadores, por lo que a AutU los podemos identificar con los $Aut\,(genU)$*, donde genU son el conjunto de generadores de* U*. Ahora, como* U *es cíclico y de orden* n*,* $|genU| = \varphi\,(n) = |\mathbb{Z}_n^\bullet|$*. Por lo tanto, podemos también identificar a* $Aut\,(genU)$ *con* $\mathbb{Z}_n^\bullet$*, teniendo así que* $AutU \cong Aut\,(genU) \cong \mathbb{Z}_n^\bullet$*. De esta manera, se tiene que*

$$G \cong \operatorname{Im} f \leq AutU \cong Aut\,(genU) \cong \mathbb{Z}_n^\bullet$$

con $\mathbb{Z}_n^\bullet$ *abeliano, por lo que también* G *es abeliano.* ■

De ahora en adelante, llamaremos una extensión de campo E_F **Galois sobre** F si satisface que E_F es de dimensión finita, E es normal y separable sobre F. Si E_F es Galois sobre F por el teorema fundamental de Galois, tenemos una correspondencia biyectiva entre los subgrupos de $GalE_F$ y los subcampos de E_F. Diremos también que E_F es *abeliano* o *cíclico* cuando es Galois sobre F y $G = GalE_F$ es abeliano o cíclico, respectivamente.

Los siguientes resultados son bajo la suposición de la existencia de algunas raíces de unidad en un campo base.

Lema 14 *Si* F *contiene* n *distintas raíces* $n-$*ésimas de la unidad, entonces el grupo de Galois de* $x^n - a$ *sobre* F *es cíclico y de orden un divisor de* n*.*

Demostración. Sea U el subgrupo de las n raíces $n-$ésimas de la unidad contenidas en F, y sea E el campo de descomposición sobre F del polinomio $x^n - a$. Sea $r \in E$ tal que $r^n - a = 0$. Entonces si $z \in U$, rz también es una raíz del polinomio $x^n - a$, entonces esta ecuación tiene las n raíces distintas rz_i, donde $i \in \{1, \ldots, n\}$ y $z_i \in U$. Por lo tanto, el campo de descomposición para $x^n - a$ se forma con cualquier raíz r de $x^n - a$ y los elementos de $U \subset F$, es decir, $E = F(r)$.

Sean $\eta, \mu \in GalE_F$, entonces $\eta(r) = zr$ y $\mu(r) = wr$, con $z, w \in U$. Notemos que $\eta \circ \mu(r) = \eta(\mu(r)) = \eta(wr) = w\eta(r) = (wz)r$ que de nuevo es raíz. Por lo tanto, la función $f : GalE_F \longrightarrow U$ definida por $\eta \longmapsto z$ es un monomorfismo de $G = GalE_F$ al grupo cíclico U de orden n. Como todos los subgrupos de un grupo cíclico son cíclicos y como G es isomorfo a un subgrupo de U se obtiene el resultado deseado. ■

A continuación se tiene un resultado parcial para el regreso del lema anterior

Lema 15 *Sea* p *primo y supongamos que* F *contiene las* p *distintas raíces* p*-ésimas de la unidad. Sea* E_F *cíclico y de dimension* p*. Entonces* $E = F(d)$ *donde* $d^p \in F$*.*

Demostración. Sea $c \in E/F$. Como $F \hookrightarrow F(c) \hookrightarrow E$ y $p = |E : F| =$

$|F(c) : F|\,|E : F(c)|$, con p primo y $c \in E/F$ entonces $|F(c) : F| > 1$ por lo que $E = F(c)$. Sea $U = \{z_1, \ldots, z_p\}$ el conjunto de las raíces p-ésimas contenidas

en F. Como $G = GalE_F$ es cíclico podemos tomar $\eta \in G$ tal que $\langle \eta \rangle = G$. Definamos a $c_i = \eta^{i-1}(c)$ para $i = 1, \ldots, p$. Notemos que $c_1 = c$ y que

$$\eta(c_i) = \eta(\eta^{i-1}(c)) = \eta^i(c) = c_{i+1}$$

para $i = 1, \ldots, p-1$, ya que $\eta(c_p) = \eta^p(c) = c = c_1$.

Ahora introduciremos la **resolvente de Lagrange**:

$$(z_i, c) = c_1 + c_2 z_i + c_3 z_i^2 + \cdots + c_p z^{p-1}$$

Notemos que

$$\begin{aligned} \eta(z_i, c) &= \eta(c_1) + \eta(c_2 z_i) + \eta(c_3 z_i^2) + \cdots + \eta(c_p z^{p-1}) \\ &= \eta(c_1) + \eta(c_2) z_i + \eta(c_3) z_i^2 + \cdots + \eta(c_p) z^{p-1} \end{aligned}$$

ya que $U \subset F$, por lo que

$$\eta(z_i, c) = c_2 + c_3 z_i + c_4 z_i^2 + \cdots + c_p z^{p-2} + c_1 z^{p-1} = (z_i, c) z_i^{-1}.$$

Por lo tanto,

$$\eta((z_i, c)^p) = ((z_i, c) z_i^{-1})^p = (z_i, c)^p \bullet 1 = (z_i, c)^p,$$

por lo que (z_i, c) es un elemento fijo de $\eta \in G$, es decir, $(z_i, c) \in F$. Notemos ahora que se pueden ver a $c = c_1, c_2, \ldots, c_p$ como combinación lineal de $(z_1, c), \ldots, (z_p, c)$ de la siguiente manera:

$$\begin{bmatrix} 1 & z_1 & z_1^2 & \ldots & z_1^{p-2} & z_1^{p-1} \\ 1 & z_2 & z_2^2 & \ldots & z_2^{p-2} & z_2^{p-1} \\ \vdots & & & & & \vdots \\ 1 & z_p & z_p^2 & \ldots & z_p^{p-2} & z_p^{p-1} \end{bmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_p \end{pmatrix} = \begin{pmatrix} (z_1, c) \\ (z_2, c) \\ \vdots \\ (z_p, c) \end{pmatrix}$$

en donde, si denotamos a

$$A = \begin{bmatrix} 1 & z_1 & z_1^2 & \ldots & z_1^{p-2} & z_1^{p-1} \\ 1 & z_2 & z_2^2 & \ldots & z_2^{p-2} & z_2^{p-1} \\ \vdots & & & & & \vdots \\ 1 & z_p & z_p^2 & \ldots & z_p^{p-2} & z_p^{p-1} \end{bmatrix}$$

se tiene que $\det(A) = \prod_{i>j}(z_i - z_j)$, el cual es distinto de cero ya que $z_i \neq z_j, \forall i, j \in \{1, \ldots, p\}$ e $i \neq j$. Como $\det(A) \neq 0$ entonces la matriz A es invertible y entonces $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_p \end{pmatrix} = A^{-1} \begin{pmatrix} (z_1, c) \\ (z_2, c) \\ \vdots \\ (z_p, c) \end{pmatrix}$, obteniendo así las c_i a partir de la matriz inversa A^{-1} y los (z_i, c). Por una parte, notemos que la matriz A está compuesta de elementos del campo F. Por otra parte, como $c_1 = c \in E \setminus F$,

entonces se afirma que algún $(z_i, c) \in E \setminus F$, pues de lo contrario se tendría que el producto de A^{-1} con los (z_i, c) como entradas, estarían todas en F, contradiciendo que $c = c_1 \notin F$. Por lo tanto, existe una $i \in \{1, \ldots, p\}$ tal que $(z_i, c) \notin F$. Como se demostró que, para cualquier $c \in E \setminus F$, $E = F(c)$, entonces, si denotamos a $d_i = (z_i, c)$, se tiene que $E = F(d_i)$, ya que $d_i \in E \setminus F$, y además $d_i^p = (z_i, c)^p \in F$. ■

El siguiente resultado nos da información acerca del grupo de Galois de una ecuación cuando extendemos el campo base.

Lema 16 *Sea $f(x) \in F[x]$ y sea K una extensión de F. Entonces el grupo de Galois de $f(x)$ sobre K es isomorfo a un subgrupo del grupo de Galois de $f(x)$ sobre F.*

Demostración. Sea L el campo de descomposición de $f(x)$ sobre el campo K. Notemos que si L es el campo de descomposición de $f(x)$ sobre K, entonces L está generado por K y las raíces $r_1, \ldots, r_k$ de $f(x)$. De esta manera, si E denota el campo de descomposición de $f(x)$ sobre F, como $F \subset K$, entonces

$$E = F(r_1, \ldots, r_k) \subset K(r_1, \ldots, r_k) = L$$

es decir, L contiene un campo de descomposición de $f(x)$ sobre el campo F.

Como L es el campo de descomposición de $f(x)$ sobre K, podemos suponer que $f(x) = \prod_{i=1}^{k}(x - r_i) \in L[x]$ y $L = K(r_1, \ldots, r_k)$, por lo que $E = F(r_1, \ldots, r_k)$.

Sea $\eta \in GalL_K$. Notemos que $\eta(r_i) = r_j$, para alguna $j \in \{1, \ldots, k\}$, por lo que manda al conjunto $R = \{r_1, \ldots, r_k\}$ en sí mismo. Por lo tanto, como η también fija a K, en particular fija a F, teniendo así que fija a todo el campo E. Como η está determinado por los valores que toma en el conjunto R, entonces, podemos definir la función $f : GalL_K \longrightarrow GalE_F$ determinada por $\eta \longmapsto \eta \mid_E$. Falta demostrar que esta función es un monomorfismo. Claramente f es un homomorfismo, pues manda a la identidad en la identidad y

$$\eta \circ \mu \longmapsto \eta \circ \mu \mid_E = \eta(\mu \mid_E) = (\eta \mid_E) \circ (\mu \mid_E),$$

esta última igualdad se da porque para cualquier $\nu \in GalL_K$, $\nu(E) = E$. Veamos que f es inyectiva. Para esto, basta ver que $\ker f = \{Id\}$. Si $\rho \in \ker f$ entonces $\rho(a) = a, \forall a \in E$, en particular para $a = r_1, r_2, \ldots, r_k$. Por lo tanto, $\rho(r_i) = r_i, \forall r_i \in R$. Como $\rho \in GalL_K$, entonces también fija a K, por lo que ρ fija a cualquier elemento en $K(r_1, \ldots, r_k) = L$, es decir, $\rho = Id$.

De esta manera se tiene que f es un monomorfismo y entonces $GalL_K \cong \operatorname{Im} f \leq GalE_F$. ■

Consideremos ahora una extensión de campo finita E sobre F. Entonces, E está generado sobre F por un conjunto finito $\{a_1, a_2, \ldots, a_k\}$ donde cada a_i es

algebráico sobre F. Sea $f_i(x)$ el polinomio mínimo asociado a a_i, en $F[x]$ y sea $f(x) = \prod_{i=1}^{k} f_i(x)$. Como $f_i(x) \in F[x]$, entonces $f(x) \in F[x] \subset E[x]$. Sea K el campo de descomposición de $f(x)$ sobre E. Como $E = F(a_1, \ldots, a_k) \subset K$, K está formado por las raíces de $f(x) \in E[x]$ y $f(a_i) = 0, \forall i = 1, \ldots, k$, entonces K también es un campo de descomposición de $f(x)$ sobre F. Para lo que sigue, necesitaremos la siguiente

Proposición 18 *Cualquier campo de descomposición E de un polinomio $f(x) \in F[x]$ es una extensión normal.*

Demostración. Sea E el campo de descomposición de $f(x) \in F[x]$. Sea $g(x) \in F[x]$ irreducible tal que $g(r) = 0$, con $r \in E$. Por demostrar que las demás raíces de $g(x)$ están en E. Sea $G = GalE_F$ y $\eta \in G$. Como η es un automorfismo y $g(r) = 0$ entonces $0 = \eta(g(r)) = g(\eta(r))$, por lo que $\eta(r)$ también es una raíz de $g(x)$. Consideremos ahora el conjunto $R = \{\mu(r) \mid \mu \in G\}$, la órbita de r bajo G, y formemos el polinomio $\prod(x - \mu(r)) \in E[x]$, donde $\mu(r) \in R$.

Como cada $\mu(r)$ es raíz, entonces $\prod(x-\mu(r)) \mid g(x)$ en $E[x]$. Por otra parte, si $\eta \in G$ entonces por la propiedad universal del anillo E, podemos extender a η de la siguiente manera

$$\begin{array}{ccc} & \overline{\eta} & \\ E[x] & \longrightarrow & E[x] \\ \uparrow & & \uparrow \\ E & \longrightarrow & E \\ & \eta & \end{array}$$

tal que $\overline{\eta}$ manda $x \longmapsto x$ y $\overline{\eta} \mid_E = \eta$. Notemos que si $h(x) = a_n x^n + \cdots + a_1 x + a_0 \in E[x]$ es tal que $\overline{\eta}(h(x)) = h(x)$, entonces $h(x) \in F[x]$, ya que como $\overline{\eta}$ es homomorfismo, igualando los coeficientes se tiene que $\eta(a_i) = a_i$, lo cual implica que $a_i \in F$ para toda i. De esta manera, para cualquier $\zeta \in G$, y su correspondiente $\overline{\zeta} : E[x] \longrightarrow E[x]$, se tiene que

$$\overline{\zeta}(\prod(x - \mu(r))) = \prod(x - \zeta(\mu(r))) = \prod(x - \gamma(r))$$

donde $\zeta \circ \mu = \gamma \in G$, por lo que el polinomio $\prod(x - \mu(r))$ es invariante bajo cualquier $\overline{\zeta} \in G$, es decir, $\prod(x-\mu(r)) \in F[x]$. Por lo tanto, como $\prod(x-\mu(r)) \in F[x]$ y $\prod(x-\mu(r)) \mid g(x)$, con $g(x) \in F[x]$ irreducible, entonces $\prod(x-\mu(r)) =$

$g(x)$, por lo que E es normal. ■

Por ahora, sólo estaremos considerando el caso en que $f(x)$ es separable, lo cual incluye a cualquier caso con un campo F de característica cero. Volviendo a las mismas hipótesis, como $f(x)$ es separable y K es su campo de descomposición, entonces por un teorema que nos asegura la equivalencia entre ser un campo de descomposición de un polinomio separable y ser una extensión de campo normal, se tiene que K es normal y separable sobre F. Si K' es otra

extensión normal de E, como $f(a_i) = 0$ y $a_i \in E$, entonces K' contiene al campo de descomposición de $f(x)$ sobre F, por lo que también contiene a un subcampo isomorfo a K. De esta manera se tiene que el campo K es único salvo isomorfismos, y está determinado solamente por E_F.

Veamos que tampoco depende del conjunto generador $\{a_1, \ldots, a_k\}$. Si $\{b_1, \ldots, b_m\}$ es otro conjunto generador de E sobre F, es decir, $E = F(b_1, \ldots, b_m)$, entonces para este conjunto, existe un campo normal K' que contiene a $E \supset F$. Como K' es normal y $f(x) \in F[x]$ es tal que $f(a_i) = 0$, con $a_i \in E$, entonces $K' \supset K$. De manera análoga, si $g(x) = \prod g_i(x)$, donde $g_i(x)$ es el polinomio mínimo asociado a b_i sobre F, se tiene que $g(x) \in F[x]$, por lo que al ser K normal sobre F y $g(x) \in F[x]$ es tal que $g(b_i) = 0$, entonces K contiene al campo de descomposición K' de $g(x) \in F[x]$, por lo que $K' \subset K$. Por lo tanto, $K = K'$. De esta manera, se tiene la siguiente

Definición 41 *Al campo K_F mencionado anteriormente se le llama la* ***cerradura normal de*** *E_F.*

Supongamos de nuevo que $f(x) \in F[x]$ es separable, E_F es una extensión finita y sea $G = GalK_F$, con K la cerradura normal de E_F. Si $\eta \in G$ entonces $\eta(E)$ es un subcampo isomorfo a E_F. A los subcampos $\eta(E)$ los llamaremos *conjugados* de E_F en K.

Afirmamos que $K' := \vee\{\eta(E)\}_{\eta \in G} = K$. Claramente $K' \subset K$. Notemos también que $E \subset \vee\{\eta(E)\}_{\eta \in G}$, ya que $Id \in G$ y $Id(E) = E$. Sea $H \leq G = GalK_F$ tal que $E = InvH$. Como $H \leq G$, entonces también $gHg^{-1} \leq G, \forall g \in G$. Ahora, $x \in Inv\left(gHg^{-1}\right)$ si y sólo si para toda $h \in H$, se cumple que

$$\begin{aligned} ghg^{-1}(x) &= x \Leftrightarrow h(g^{-1}(x)) = g^{-1}(x) \\ &\iff g^{-1}(x) \in InvH \iff x \in g(InvH) = g(E). \end{aligned}$$

Por lo tanto, $Inv(gHg^{-1}) = g(E)$. Además, notemos que $H \lhd G$, si y sólo si se tiene lo siguiente

$$gHg^{-1} = H, \forall g \in G \iff Inv(gHg^{-1}) = Inv(H) \iff g(E) = E.$$

Entonces, como $\vee\{\eta(E)\}_{\eta \in G}$ es invariante bajo cualquier $\zeta \in G$, se tiene que $GalK_{K'} \lhd G = GalK_F$. Como la correspondencia de Galois manda extensiones normales a subgrupos normales y viceversa, se tiene que K' es una extensión normal de F que contiene a E. Como K es la cerradura normal de E_F entonces $K \subset K'$. Por lo tanto, se tiene que $K = K'$.

Lema 17 *Sea E_F y sea $F = F_1 \subset F_2 \subset \cdots \subset F_{r+1} = E$ una torre de raíces sobre F, es decir, donde $F_{i+1} = F_i(d_i)$ con $d_i^{n_i} \in F_i$. Supongamos que E es generado sobre F por un conjunto finito de elementos cuyos polinomios mínimos son separables. Entonces la cerradura normal K_F de E_F tiene una torre de raíces sobre F tal que, los distintos n_i para esta torre, son los mismos que de la torre de E sobre F.*

Demostración. Sea E_F y sea $F = F_1 \subset F_2 \subset \cdots \subset F_{r+1} = E$ una

torre de raíces sobre F. Recordemos que la cerradura normal K_F está generada por los campos conjugados $\eta(E)$ con $\eta \in GalK_F$. Ahora, si aplicamos η a la torre de raíces se tiene que la siguiente torre $F = \eta(F_1) \subset \eta(F_2) \subset \cdots \subset \eta(F_{r+1}) = \eta(E)$. Como $F_2 = F_1(d_1) = F(d_1)$, entonces $\eta(F_2) = \eta(F(d_1)) = F(\eta(d_1))$ pues $\eta \in GalK_F$. Análogamente, $F_3 = F_2(d_2)$ por lo que $\eta(F_3) = \eta(F_2(d_2)) = \eta(F(d_1)(d_2)) = F(\eta(d_1,d_2)) = F(\eta(d_1)(\eta(d_2)) = \eta(F_2)(\eta(d_2))$. En general, $\eta(F_{i+1}) = \eta(F_i)(\eta(d_i))$. Usando recursión, se tiene que

$$\eta\left(F_{i+1}\right) = F\left(\eta\left(d_1\right)\eta\left(d_2\right)\cdots\eta\left(d_i\right)\right).$$

Notemos además que como $d_i^{n_i} \in F_i, \forall i \in \{1,\ldots,r\}$, se tiene que $\eta(d_i)^{n_i} = \eta(d_i^{n_i}) \in \eta(F_i)$. Por lo tanto, para cada $\eta \in GalK_F$ se tiene una torre de raíces $F = \eta(F_1) \subset \eta(F_2) \subset \cdots \subset \eta(F_{r+1}) = \eta(E)$ tales que $\eta(d_i)^{n_i} \in \eta(F_i)$, es decir, la torre tiene a los mismos exponentes n_i, asociados antes a cada d_i. Por otra parte, por recursión, se tiene que $\eta(E) = F(\eta(d_1),\ldots,\eta(d_r))$, y como $K = \vee\left\{\eta(E)\right\}_{\eta\in GalK_F}$, si $GalK_F = \{\eta_1,\eta_2,\ldots\}$ entonces

$$K = F(\eta_1(d_1),\eta_1(d_2),\ldots,\eta_1(d_r);\eta_2(d_1),\ldots,\eta_2(d_r);\ldots)$$

Ahora, organizaremos los $\eta_i\left(d_j\right)$ de tal manera que nos quede una torre de campos con la propiedad deseada. Supongamos que $|GalK_F| = n$. Consideremos la siguiente sucesión

$$F \hookrightarrow F\left(\eta_1\left(d_1\right)\right) \hookrightarrow F\left(\eta_1\left(d_1\right)\eta_2\left(d_1\right)\right) \hookrightarrow \cdots \hookrightarrow F\left(\eta_1(d_1),\eta_2(d_1),\ldots,\eta_n(d_1)\right)$$

Notemos que como $\eta_i\left(d_1\right)^{n_1} \in F$, entonces $\eta_i\left(d_1\right)^{n_1} \in F\left(\eta_1(d_1),\eta_2(d_2),\ldots,\eta_{i-1}(d_1)\right)$, por lo que esta sucesión cumple con la propiedad deseada. Si volvemos a repetir el argumento, ahora con $F\left(\eta_1(d_1),\eta_2(d_1),\ldots,\eta_n(d_1)\right)$ como campo base, y vamos adjuntando los $\eta_i\left(d_2\right)$, se tiene otra sucesión de subcampos tales que

$$\eta_i\left(d_2\right)^{n_2} \in F\left(\eta_i\left(d_1\right)\right) \subset F\left(\eta_1(d_1),\eta_2(d_1),\ldots,\eta_r(d_1)\right).$$

para toda $i \in \{1,\ldots,n\}$, por lo que vuelve a cumplir las propiedades de una torre de raíces. Como tenemos un número finito de d_i's y de η_j's, este procedimiento termina, y lo hace justamente con el campo K. ■

Hemos alcanzado el punto para establecer el criterio de Galois para la solubilidad de una ecuación por radicales. Supongamos que $f(x) \in F\left[x\right]$ es soluble por radicales, con F un campo de característica cero. Entonces existe una extensión de campo E_F y una torre de raíces

$$F = F_1 \subset F_2 \subset \cdots \subset F_{r+1} = E$$

tal que tiene contenida un campo de descomposición para $f(x)$. Por el lema anterior, podemos suponer que E es normal sobre F. Por otra parte, como F es de característica 0, entonces la separabilidad es automática, por lo que E es Galois sobre F.

Sea n el mínimo común múltiplo asociado a las n_i de la torre de raíces y sea z una raíz $n-$ésima de la unidad, es decir, z es solución de x^n-1. De esta manera, podemos construir el campo $E(z)$ y alargar la torre de raíces un término más. Ahora, si E es el campo de descomposición del polinomio $g(x) \in F[x]$, entonces $E(z)$ es el campo de descomposición de $h(x) := g(x)(x^n-1) \in F[x]$. Como F es de característica cero, $E(z)_F$ es separable, en particular, $h(x)$ lo es. Además, como $E(z)_F$ es el campo de descomposición de $h(x) \in F[x]$, entonces $E(z)$ es normal sobre F, teniendo así que $E(z)$ es Galois sobre F. Por otra parte, como $z^n = 1 \in F$, entonces podemos reacomodar la torre de raíces de la siguiente manera:

$$F = F_1 \subset F_2 = F(z) \subset F_3 = F_2(d_1) \subset \cdots \subset E(z).$$

Sea $G = GalE_F$ y H el grupo de Galois de $E(z)$ sobre F. Como $F_2 = F(z)$ es el campo de descomposición de $x^n - 1 \in F[x]$, por el primer lema visto en esta sección, $GalF_{2F}$ es abeliano. Por otra parte, como $F_{i+1} = F_i(d_{i-1})$, y $z \in F_i, \forall i > 1$, entonces F_{i+1} contiene a las n raíces $n-$ésimas de la unidad y a d_{i-1}, por lo que F_{i+1} es el campo de descomposición del polinomio $x^n - d_{i-1}^n \in F_i[x]$. Por el segundo lema de esta sección, se tiene que $GalF_{i+1F_i}$ es cíclico, y por lo tanto, también F_{i+1} es abeliano sobre F_i. Sea $H_i = GalE(z)_{F_i}$, es decir, el subgrupo de H correspondiente al campo F_i. Como $F \subset F_i$, y F es de característica 0, entonces F_i también lo es para toda i. Además, como F_{i+1} es el campo de descomposición de $x^n - d_{i-1}^n \in F_i[x]$, por la proposición anterior se tiene que F_{i+1} es normal y separable sobre F_i, para toda i. De esta manera, por la correspondencia de Galois para el grupo H, se tiene que $H_{i+1} \lhd H_i$.

Por otra parte, $E(z)$ es normal y separable sobre cualquier F_i, por lo que $E(z)$ es Galois sobre F_i para toda i. Por lo tanto, como $H_{i+1} \lhd H_i$, por el teorema fundamental de Galois, $GalF_{i+1F_i} = GalInvH_{i+1F_i} \cong H_i/H_{i+1}$. Por lo tanto, $H_i/H_{i+1} \cong GalF_{i+1F_i}$, y como éste último es abeliano, se tiene que H_i/H_{i+1} es un grupo abeliano para toda i. Por lo tanto, de nuevo por la correspondencia de Galois, se tiene una sucesión de subgrupos

$$H = H_1 \supset H_2 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$$

tales que $H = H_1 \rhd H_2 \rhd \cdots \rhd H_{n-1} \rhd H_n = \{e\}$ y H_i/H_{i+1} es abeliano para toda i, es decir, el grupo H es soluble. Como el campo de descomposición de $f(x)$ está contenido en E_F, el cual a su vez está contenido en la torre de raíces de $E(z)_F$, entonces el grupo de Galois G de $f(x)$ es isomorfo a un subgrupo de H, por lo que también es soluble.

Supongamos ahora que el grupo G de Galois de $f(x) \in F[x]$ es soluble. Sea E_F un campo de descomposición de $f(x)$ y supongamos que $n = |G| = [E : F]$. Sea z una raíz primitiva n-ésima de la unidad y sean $F = F_1, F_2 = F(z)$ y $K = E(z)$. Como $F \hookrightarrow F_2$ y K es el campo de descomposición de $f(x) \in F_2[x]$, entonces por el cuarto lema visto en esta sección, el grupo de Galois de K_{F_2} es isomorfo a un subgrupo H de G. Como el grupo G es soluble por hipótesis, H también lo es. Ahora, por el teorema de la sección de grupos solubles que

nos asegura que un grupo finito es soluble si y sólo si para cualquier serie de composición

$$H = H_1 \rhd H_2 \rhd \cdots \rhd H_{s+1} = \{e\}$$

los factores de composición H_i/H_{i+1} son cíclicos y de orden primo, como H es finito y soluble, entonces se tiene una serie de composición

$$H = H_1 \rhd H_2 \rhd \cdots \rhd H_{s+1} = \{e\},$$

donde cada H_i/H_{i+1} es cíclico y de orden p_i primo, con $i = 1, \ldots, s$. Por la correspondencia entre subgrupos y campos, se tiene una cadena creciente de subcampos

$$F_2 \subset F_3 \subset \cdots \subset F_{s+2} = K$$

tal que $H_i = GalK_{F_{i+1}}$. Como $H_{i+1} \lhd H_i$, entonces F_{i+1} es normal sobre F_i y además el grupo de Galois de F_{i+1} sobre F_i es cíclico y de orden primo p_i. Notemos ahora que en esta cadena creciente de subcampos, como $F_2 = F(z)$, entonces F_2 contiene una raíz primitiva $n-$ésima de la unidad, por lo que cualquier F_i también la contiene. Por otra parte, $p_i \mid n$, ya que $H_i \leq G$. Como F_i contiene una raíz primitiva $n-$ésima de la unidad, existe un elemento ω tal que $\omega^n = 1$, pero como $p_i \mid n$, existe $m \in \mathbb{N}$ tal que $mp_i = n$, por lo que $(\omega^m)^{p_i} = \omega^n = 1$, es decir, F_i también contiene una raíz primitiva $p-$ésima de la unidad, por lo que contiene también a las p_i restantes. Por el tercer lema de esta sección, $F_{i+1} = F_i(d_i)$, donde $d_i \in F_{i+1}$ es tal que $d_i^{p_i} \in F_i$. Por lo tanto, como este argumento fue para cualquier F_i en la cadena creciente de subcampos de K, se tiene que esta misma cadena es una torre de raíces para K sobre F, y como en un principio $E \subset K$, con E el campo de descomposición de $f(x) \in F[x]$, se tiene que $f(x)$ es soluble por radicales sobre F.

0.23. Ecuación general de grado n.

Nos referimos a la **ecuación general de grado** n como el polinomio mónico cuyos coeficientes son distintas indeterminadas, es decir, si F es un campo y $t_1, \ldots, t_n$ son variables indeterminadas, entonces la ecuación

$$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^n t_n$$

es *la ecuación general de grado* n sobre F.

Decimos que $f(x)$ es soluble por radicales si es soluble por radicales sobre el campo $F(t_1, \ldots, t_n)$, es decir, sobre el campo de cocientes del anillo de polinomios $F[t_1, \ldots, t_n]$. Por ejemplo, la ecuación general de segundo grado $x^2 - t_1 x + t_2$, con solución $x = \frac{t_1}{2} \pm \frac{\sqrt{t_1^2 - 4t_2}}{2}$, es soluble por radicales ya que, como las raíces están contenidas en $F(t_1, t_2, d)$, con $d^2 = t_1^2 - 4t_2 \in F(t_1, t_2)$, se tiene a la torre de raíces

$$F \hookrightarrow F(t_1, t_2) \hookrightarrow F(t_1, t_2, d)$$

tal que $d^2 = t_1^2 - 4t_2 \in F(t_1, t_2)$ y con $F(t_1, t_2, d)$ el campo de descomposición para $f(x)$.

Nos surge entonces la siguiente pregunta: ¿cuándo es soluble una ecuación $f(x)$ por radicales sobre un campo F? Para poder determinarlo, usando el criterio de Galois, necesitamos encontrar al grupo de Galois de $f(x)$ sobre $F(t_1, \ldots, t_n)$. Supondremos que el grado del polinomio $f(x)$ es $n > 4$.

Sea E el campo de descomposición de $f(x)$ sobre $F(t_1, \ldots, t_n)$ y supongamos que $f(x) = (x - y_1) \cdots (x - y_n) \in E[x]$. Si desarrollamos este producto y lo comparamos con la definición de la ecuación general, se tiene que

$$t_1 = \sum_{i=1}^{n} y_i, t_2 = \sum_{i<j} y_i y_j, \ldots, t_n = t_1 t_2 \cdots t_n.$$

Por lo tanto, $E = F(t_1, \ldots, t_n, y_1, \ldots, y_n) = F(y_1, \ldots, y_n)$. Obtendremos al grupo de Galois de $f(x)$ usando resultados anteriores acerca de expresiones racionales simétricas.

Sean $x_1, \ldots, x_n$ las n indeterminadas y sea el campo $F(x_1, \ldots, x_n)$ con su *subcampo de expresiones racionales simétricas*, es decir, el campo $F(p_1, \ldots, p_n)$ donde los p_i's son los polinomios elementales simétricos

$$p_1 = \sum x_i,\ p_2 = \sum_{i<j} x_i x_j, \ldots,\ p_n = x_1 \cdots x_n,$$

y donde $F(x_1, \ldots, x_n)$ es el campo de descomposición de $g(x) = \prod_{i=1}^{n}(x - x_i)$ sobre $F(p_1, \ldots, p_n)$, con grupo de Galois $G_g = S_n$. Llevaremos los resultados relacionados con $F(x_1, \ldots, x_n)$ y $F(p_1, \ldots, p_n)$ con los campos $F(y_1, \ldots, y_n)$ y $F(t_1, \ldots, t_n)$. Para esto, definiremos un isomorfismo entre $F(x_1, \ldots, x_n)$ y $F(y_1, \ldots, y_n)$ tal que restringido a $F(p_1, \ldots, p_n)$ se tenga un isomorfismo con $F(t_1, \ldots, t_n)$. Como las t_i son indeterminadas, por la propiedad universal de anillos, podemos definir el homomorfismo $\xi : F[t_1, \ldots, t_n] \longrightarrow F[p_1, \ldots, p_n]$ dado por $t_i \longmapsto p_i$, para toda i, con $1 \leq i \leq n$, y $a \longmapsto a, \forall a \in F$. De nuevo por la propiedad universal de anillos, pero esta vez con $F[x_1, \ldots, x_n]$ y $F[y_1, \ldots, y_n]$, se tiene el homomorfismo

$$\omega : F[x_1, \ldots, x_n] \longmapsto F[y_1, \ldots, y_n]$$

tal que $\omega \mid_F = Id_F$ y mande a $x_i \longmapsto y_i$. De esta manera, se tiene el siguiente diagrama

$$\begin{array}{ccc} & \overset{\omega}{\longrightarrow} & \\ F[x_1, \ldots, x_n] & & F[y_1, \ldots, y_n] \\ \uparrow & & \uparrow \\ F[p_1, \ldots, p_n] & \underset{\xi}{\longleftarrow} & F[t_1, \ldots, t_n] \end{array}$$

de donde podemos definir a la composición $\lambda = \omega\xi : F[t_1, \ldots, t_n] \to F[y_1, \ldots, y_n]$.

Notemos que

$$\lambda(t_j) = \omega\xi(t_j) = \omega(p_j) = \omega(\sum_{i_1<i_2<\cdots<i_j} x_{i_1}\cdots x_{i_j}) = \sum_{i_1<i_2<\cdots<i_j} y_{i_1}\cdots y_{i_j} = t_j$$

por las fórmulas que relacionaban las x_i´s con p_i´s y y_i´s con t_i´s. Por lo tanto, $\lambda : F[t_1,\ldots,t_n] \to F[t_1,\ldots,t_n]$ es tal que $\lambda(t_i) = t_i$. Por la propiedad universal, se tiene que $\lambda = Id$. Ahora, como $Id = \lambda = \omega\xi$ y la función Id es claramente inyectiva, se tiene que ξ también es inyectiva. Además, es claro que ξ también es sobre, por lo que ξ es un isomorfismo entre $F[t_1,\ldots,t_n]$ y $F[p_1,\ldots,p_n]$. De esta manera $\omega\mid_{F[p_1,\ldots,p_n]} = \xi^{-1}$, ya que ξ es un isomorfismo y $\omega\mid_{F[p_1,\ldots,p_n]}$ es un inverso derecho. Por otra parte, observemos también que ω es un isomorfismo.

Consideremos ahora el siguiente diagrama

$$\begin{array}{ccc} & \overset{\omega'}{\longrightarrow} & \\ F(x_1,\ldots,x_n) & & F(y_1,\ldots,y_n) \\ \uparrow & & \uparrow \\ F(p_1,\ldots,p_n) & \underset{\xi'}{\longleftarrow} & F(t_1,\ldots,t_n) \end{array}$$

donde ξ' es un isomorfismos que extiende a ξ de $F(t_1,\ldots,t_n)$ a $F(p_1,\ldots,p_n)$, y ω' un isomorfismo que extiende a ω. Notemos que se tiene un nuevo isomorfismo $\sigma : F(t_1,\ldots,t_n)[x] \longrightarrow F(p_1,\ldots,p_n)[x]$ tal que extiende a ξ' y manda $x \longmapsto x$. Notemos también que

$$\begin{aligned} \sigma(f(x)) &= \sigma(x^n - t_1x^{n-1} + t_2x^{n-2} - \cdots + (-1)^n t_n) \\ &= x^n - p_1x^{n-1} + p_2x^{n-2} - \cdots + (-1)^n p_n = g(x) \end{aligned}$$

Recordemos que si se tiene un isomorfismo μ entre dos campos F y F', con $f(x) \in F[x]$ y $g(x) \in F'[x]$ tales que $f(x) \longmapsto g(x)$ bajo el homomorfismo $\eta : F[x] \longrightarrow F'[x]$ que extiende a μ y manda $x \longmapsto x$, entonces μ se puede extender a un isomorfismo entre E y E', donde E y E' son los campos de descomposición para $f(x)$ y $g(x)$ sobre F y F', respectivamente. Ahora, como $F(y_1,\ldots,y_n)$ es un campo de descomposición de $f(x)$ sobre $F(t_1,\ldots,t_n)$, $F(x_1,\ldots,x_n)$ es un campo de descomposición para $g(x)$ sobre $F(p_1,\ldots,p_n)$, ξ' es un isomorfismo de $F(t_1,\ldots,t_n) \longrightarrow F(p_1,\ldots,p_n)$ y σ manda $f(x) \longmapsto g(x)$, entonces ξ' se puede extender a un isomorfismo $\psi : F(y_1,\ldots,y_n) \longrightarrow F(x_1,\ldots,x_n)$.

Afirmamos que esto último implica que los grupos de Galois G_f y G_g son isomorfos. Para esto, definiremos una función biyectiva entre G_f y G_g. Consideremos el siguiente diagrama y a la función $\varphi : G_f \longrightarrow G_g$ definida por $\varphi(\eta) = \psi\eta\psi^{-1}$.

$$\begin{array}{ccccccc} & \overset{\psi^{-1}}{} & & \overset{\eta}{} & & \overset{\psi}{} & \\ F(x_1,\ldots,x_n) & \longrightarrow & F(y_1,\ldots,y_n) & \longrightarrow & F(y_1,\ldots,y_n) & \longrightarrow & F(x_1,\ldots,x_n) \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ F(p_1,\ldots,p_n) & \longrightarrow & F(t_1,\ldots,t_n) & \longrightarrow & F(t_1,\ldots,t_n) & \longrightarrow & F(p_1,\ldots,p_n) \\ & \underset{\xi^{-1}}{} & & & & \underset{\xi}{} & \end{array}$$

Si $\eta \in G_f$, entonces del diagrama se sigue que $\psi\eta\psi^{-1} : F(x_1,\ldots,x_n) \longrightarrow F(x_1,\ldots,x_n)$. Además, como ψ y η son isomorfismos, entonces la composición también lo es. Finalmente, φ es biyectiva ya que la función $\phi : G_g \longrightarrow G_f$ definida por $\phi(\nu) = \psi^{-1}\nu\psi$ es su inversa:

$$(\phi \circ \varphi)(\eta) = \phi(\varphi(\eta)) = \phi\left(\psi\eta\psi^{-1}\right) = \psi^{-1}\left(\psi\eta\psi^{-1}\right)\psi = \eta$$

análogamente $(\varphi \circ \phi)(\nu) = \nu$.

Falta ver entonces que para cada $\eta \in G_f$, $\psi\eta\psi^{-1} \in G_g$. Para esto, sólo hay que demostrar que $\psi\eta\psi^{-1}$ deja fijo al campo $F(p_1,\ldots,p_n)$, ya que acabamos de ver que $\psi\eta\psi^{-1}$ es un automorfismo. Observemos dos cosas; la primera es que, como ψ extiende a ξ, entonces ψ^{-1} extiende a ξ^{-1}, y la segunda es que, para cualquier $\eta \in G_f$, $\eta\mid_{F(t_1,\ldots,t_n)} = Id$. Ahora, si $h \in F(p_1,\ldots,p_n)$, se tiene que

$$\psi\eta\psi^{-1}(h) = \psi\eta\left(\psi^{-1}(h)\right) = \psi\left(\psi^{-1}(h)\right) = h,$$

ya que $\psi^{-1}(h) \in F(t_1,\ldots,t_n)$ y $\eta(k) = k, \forall k \in F(t_1,\ldots,t_n)$. Por lo tanto $\psi\eta\psi^{-1} \in G_g$ y de esta manera se tiene que $G_f \cong G_g$. Como G_g coincidía con S_n, entonces $G_f \cong G_g = S_n$.

Por último, notemos que como por construcción $x_1,\ldots,x_n$ son distintas indeterminadas y $F(x_1,\ldots,x_n) \cong F(y_1,\ldots,y_n)$, entonces también las y_i's son distintas. Además, $f(x)$ es irreducible en $F(t_1,\ldots,t_n)[x]$ ya que, de lo contrario, $g(x)$ no sería irreducible sobre $F(p_1,\ldots,p_n)[x]$. Si $u(x)$ es un factor irreducible de $g(x)$ en $F(p_1,\ldots,p_n)[x]$, entonces cualquier automorfismo de $F(x_1,\ldots,x_n)[x]$ deja fijo a $u(x)$. Ahora,

$$g(x) = (x - x_1)\cdots(x - x_n) \in F(x_1,\ldots,x_n)$$

por lo que $u(x) = (x - x_{i_1})\cdots(x - x_{i_k})$ donde $k < n$ y $x_{i_j} \in \{x_1,\ldots,x_n\}, \forall j = 1,\ldots,k$. Como el grupo de Galois de $g(x)$ sobre $F(p_1,\ldots,p_n)$ es S_n, existe cuando menos una permutación que nos mande una raíz de $u(x)$ en cualquier otra raíz de $g(x)$ que no sea de $u(x)$, lo cual es una contradicción a la invarianza de $u(x) \in F(p_1,\ldots,p_n)$. Por lo tanto, $f(x)$ es irreducible en $F(t_1,\ldots,t_n)[x]$.

De lo anterior, se tiene el siguiente

Teorema 54 *La ecuación general de grado n,*

$$x^n - t_1x^{n-1} + t_2x^{n-2} - \cdots + (-1)^n t_n,$$

es irreducible en $F(t_1,\ldots,t_n)[x]$ con raíces distintas para $n \geq 5$. Además, el grupo de Galois de $f(x) = 0$ es el grupo simétrico S_n.

Como S_n no es soluble para $n > 4$, se tiene el siguiente importante resultado

Teorema 55 *(Ruffini-Abel) La ecuación general de grado n sobre un campo de característica cero, no es soluble para $n \geq 5$.*

El siguiente lema nos es de gran utilidad, ya que nos da información acerca del grupo de Galois de un polinomio irreducible, de grado primo, sobre el campo de racionales $\mathbb{Q}$.

Lema 18 *Sea $f(x) \in \mathbb{Q}[x]$ irreducible y de grado p, con p primo. Supongamos que $f(x)$ tiene dos raíces no reales en $\mathbb{C}$. Entonces el grupo de Galois de $f(x)$ sobre $\mathbb{Q}$ es isomorfo al grupo simétrico S_p.*

Demostración. Como $\mathbb{C}$ es la cerradura algebraica de $\mathbb{R}$, entonces $\mathbb{C}$ tiene un campo de descomposición $\sum$ de $f(x)$ sobre $\mathbb{Q}$. Sea G_f el grupo de Galois de $f(x)$ sobre $\mathbb{Q}$, el cual lo podemos considerar como el grupo de permutaciones sobre los ceros de $f(x)$. Como estamos trabajando en $\mathbb{C}$, se tiene que $f(x)$ es separable sobre $\mathbb{Q}$, por lo que sus raíces son todas distintas. Por lo tanto, G_f es un grupo isomorfo a un subgrupo de S_p.

Por otra parte, cuando se construye el campo de descomposición $\sum$ de $f(x)$ sobre $\mathbb{Q}$, se construye primero la raíz $p-$ésima ω de la unidad, la cual al tener orden p, cumple que $p = |[\mathbb{Q}(\omega) : \mathbb{Q}]| \mid |\sum : \mathbb{Q}| = |G_f|$. Por el teorema de Cauchy, G_f contiene un elemento de orden p. Pero como en S_p los únicos elementos de orden p son los $p-$ciclos se tiene que G_f contiene un $p-$ciclo. Ahora, la conjugación compleja deja fijo a $\mathbb{R} \supset \mathbb{Q}$, por lo que también es un $\mathbb{Q}-$automorfismo de $\mathbb{C}$ y por lo tanto, induce un $\mathbb{Q}-$automorfismo sobre $\sum$, ya que si α es raíz compleja, entonces $\overline{\alpha}$ también lo es. De esta manera, se tiene que la conjugación compleja deja fija a las $p-2$ raíces reales de $f(x)$ y transpone a las dos raíces no reales, por lo que también G_f contiene un ciclo de orden 2.

Podemos entonces suponer que G_f contiene un $2-$ciclo y un $p-$ciclo a los cuales representaremos como $(1,2)$ y $(1,\ldots,p)$ respectivamente. Afirmamos que $\langle (1,2),(1,\ldots,p)\rangle = S_p$, lo cual daría por terminada la prueba. Sea $a = (1,2)$ y $b = (1,\ldots,p)$, y sea $G = \langle a, b\rangle$. Entonces el elemento $bab^{-1} \in G$. Veamos quién es bab^{-1} : si $i \geq 4$, se tiene que $bab^{-1}(i) = ba(i-1) = b(i-1) = i$, pues a no mueve a i si $i-1 \geq 3$, o lo que equivale a decir, si $i \geq 4$. También si $i = 1$ entonces $bab^{-1}(1) = ba(p) = b(p) = 1$. Por otra parte, $bab^{-1}(2) = ba(1) = b(2) = 3$ y $bab^{-1}(3) = ba(2) = b(1) = 2$, por lo que $bab^{-1} = (2,3)$. Con un argumento similar, se tiene que $b(2,3)b^{-1} = (3,4)$, por lo que cualquier transposición de la forma $(i, i+1)$, con $1 \leq i \leq p-1$, está en G. Notemos también que

$$G \ni (1,2)(2,3)(1,2) = (1,3),$$

y de manera análoga, $(1,4) = (1,3)(3,4)(1,3) \in G$. En general,

$$(1, i+1) = (1,i)(i,i+1)(1,i),$$

por lo que también las transposiciones de la forma $(1,i) \in G$, $\forall i$. Finalmente, los elementos

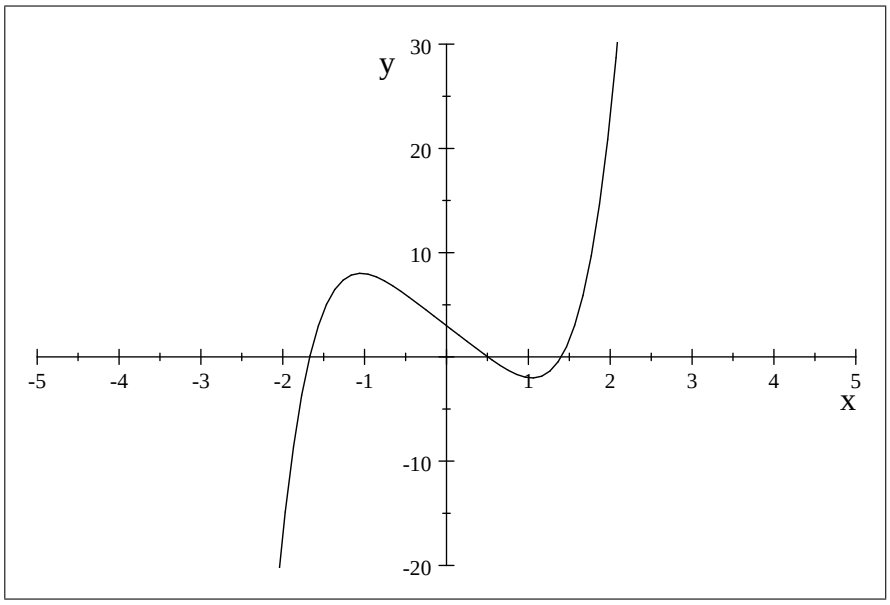
$$(m,n) = (1,m)(1,n)(1,m) \in G,$$

por lo que cualquier transposición está en G. Como cualquier permutación es un producto de transposiciones se tiene que $\langle a, b\rangle = G = S_p$, demostrando así que $G_f = S_p$. ■

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

Demostración. Sea $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Por el criterio de Eisenstein, $f(x)$ es irreducible sobre $\mathbb{Q}$. Demostraremos que $f(x)$ tiene sólo tres ceros reales, cada uno de multiplicidad 1, con lo cual tendría dos raíces no reales. Como $\operatorname{grad} f(x) = 5$ es primo, por el lema anterior el grupo de Galois G_f sobre $\mathbb{Q}$ es isomorfo a S_5, el cual no es soluble. Por lo tanto, al ser no soluble G_f, se tiene que $f(x) = 0$ no es soluble por radicales. Falta entonces demostrar que el polinomio tiene exactamente tres raíces reales.

Notemos primero que $f(-2) = -17,\ f(-1) = 8, f(0) = 3,\ f(1) = -2,\ f(2) = 23$. La gráfica de $f(x)$ tiene la forma



Por el teorema de Rolle, los ceros de $f(x)$ están separados por los ceros de $f'(x)$. Como $f'(x) = 5x^4 - 6$, entonces los números $\pm\sqrt[4]{\frac{6}{5}}$ son ceros de $f'(x)$. Como además $\mathbb{Q}$ es de característica cero y $f'(x) \neq 0$, entonces $(f(x), f'(x)) = 1$, teniendo así que $f(x)$ no tiene raíces repetidas, por lo que $f(x)$ tiene a lo más 3 raíces reales. Pero ciertamente, $f(x)$ tiene cuando menos tres raíces reales, ya que al ser una función continua definida en todo $\mathbb{R}$, no puede cambiar de signo excepto cuando pasa por el cero. Por lo tanto, $f(x)$ tiene exactamente tres raíces reales.

Como $f(x)$ tiene tres raíces reales, entonces tiene dos raíces complejas, cumpliendo así con las hipótesis del lema anterior. Por lo tanto, $G_f \cong S_5$, el cual no es soluble. ■

0.24. Campos Finitos

Sea F un campo finito. Como F es finito, podemos identificar a su anillo primo por $\mathbb{Z}_p$ para algún primo p. Afirmamos que $|F| = p^n$. Para esto, veremos a F como un espacio vectorial sobre el campo $\mathbb{Z}_p$. Claramente $|F : \mathbb{Z}_p|$ es finito, ya que $F \supset \mathbb{Z}_p$ lo es. Sea $n = |F : \mathbb{Z}_p|$ y sea $\{v_1, \ldots, v_n\}$ una base para F sobre $\mathbb{Z}_p$. De esta manera, $\mathcal{L}_{\mathbb{Z}_p}(\{v_1, \ldots, v_n\}) = F$, es decir, todo elemento se puede escribir de la forma $a_1v_1 + a_2v_2 + \cdots + a_nv_n$, con $a_i \in \mathbb{Z}_p$. Notando que, para cada v_i, hay p posibles $a_i \in \mathbb{Z}_p$, se tiene que $|F| = \left|\mathcal{L}_{\mathbb{Z}_p}(\{v_1, \ldots, v_n\})\right| = p^n$.

Ahora veremos la existencia de un campo con p^n elementos y concluiremos que ésta es única salvo isomorfismos. Comenzaremos considerando al campo base $\mathbb{Z}_p = F$ y E el campo de descomposición del polinomio $f(x) = x^{p^n} - x$ sobre F. Como $F \subset E$, E es de característica p. De esta manera, $f'(x) = p^n x^{p^n-1} - 1 = -1$, por lo que $(f, f') = 1$, es decir, $f(x)$ tiene p^n raíces simples.

Afirmamos que E coincide con el conjunto $R = \{u_1, \ldots, u_{p^n}\}$ de distintas raíces de $f(x)$. Para esto, notemos que al conjunto R lo podemos denotar como el conjunto $A = \left\{a \in E \mid a^{p^n} = a\right\}$. Por otra parte, si $b \in \mathbb{Z}_p$ entonces $b^p = b$, por lo que $b^{p^2} = b^p = b$. Por inducción, se tiene que $b^{p^n} = b, \forall n \in \mathbb{N}$, por lo que $b \in A, \forall b \in \mathbb{Z}_p$, es decir, $\mathbb{Z}_p \subset A = R$. Veamos ahora que A es un subcampo de E. Para esto, basta demostrar que $\forall a, b \in A$, $(a-b)^{p^n} = a - b$ y que $\left(\frac{a}{b}\right)^{p^n} = \frac{a}{b}$. Como E tiene característica p, al desarrollar el binomio $(a-b)^{p^n}$ se tiene que todos los factores se van, excepto el primero y el último, es decir, $(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b$. Por otra parte, $\left(\frac{a}{b}\right)^{p^n} = \frac{a^{p^n}}{b^{p^n}} = \frac{a}{b}$. Por lo tanto, A es un subcampo de E. Como $\mathbb{Z}_p \subset A$ y A contiene a todas las raíces de $f(x)$,

$$E = \mathbb{Z}_p(u_1, \ldots, u_{p^n}) \subset A \subset E,$$

teniendo así que $R = A = E$, concluyendo que $p^n = |R| = |A| = |E|$.

Por otra parte, si E' es otro campo con p^n elementos, entonces $\mathbb{Z}_p \subset E'$. Ahora, la cardinalidad del conjunto E'^* es $p^n - 1$, es decir, $|E'^*| = p^n - 1$. Además, como E' es finito, entonces $(E'^*, \bullet, 1)$ es cíclico, por lo que para toda $a \in E'^*$ se tiene que $a^{p^n-1} = 1$, lo cual implica que $a^{p^n} = a, \forall a \in E'^*$. Como también $0^{p^n} = 0$, entonces cualquier elemento $z \in E'$ es una raíz de $f(x) = x^{p^n} - x$. Como $f(x)$ tiene a lo más p^n raíces distintas y cada elemento de E es raíz de $f(x)$, con $|E'| = p^n$, entonces E' es un campo de descomposición de $f(x)$ sobre $\mathbb{Z}_p$. Como los campos de descomposición son únicos salvo isomorfismos, se tiene que $E' \cong E$, demostrando así el siguiente

Teorema 56 *El número de elementos de un campo finito es una potencia de un primo. Además, para cualquier potencia de primo p^n existe un campo F, salvo isomorfismos, con $|F| = p^n$.*

El siguiente resultado nos caracteriza a las extensiones de campo finitas, de un campo finito. Para esto, se tiene la siguiente

Definición 42 *Decimos que E tiene un elemento primitivo u sobre F si $F(u) = E$.*

Teorema 57 *Sea F un campo finito y E una extensión de F tal que $|E : F| = n$. Entonces E tiene un elemento primitivo sobre F.*

Demostración. Con un razonamiento totalmente análogo al anterior, como F es finito y $|E : F| = n$, entonces también E es finito y $|E| = m^n$, donde $m = |F|$. Por otra parte, sabemos que cualquier subgrupo finito del grupo multiplicativo de un campo es cíclico. En particular, si el campo E es finito, entonces $(E^*, \bullet, 1)$ es cíclico. Sea z un generador de E^*. Ahora, si $\{v_1, \ldots, v_n\}$ es una base de E_F, entonces

$$E = \mathcal{L}_F(v_1, \ldots, v_n) = \mathcal{L}_F\left(z_1^{i_1}, \ldots, z_n^{i_n}\right) \subset F(z),$$

ya que $v_i = z_i^{j_i}$, para algún $j_i \in \mathbb{N}$. Pero como $z \in E$, entonces $F(z) \subset E$, lo cual implica que $E = F(z)$, es decir, E tiene un elemento primitivo sobre F. ■

Notemos que de la definición anterior, es equivalente decir que E es una extensión simple sobre F y que E tiene un elemento primitivo u sobre F. Si E es una extensión finita del campo F, ¿será cierto que E tiene un elemento primitivo sobre F? A continuación, se tiene un resultado que nos caracteriza a las extensiones que sí tienen elementos primitivos sobre F

Teorema 58 *Sea E una extensión de campo finita sobre F. Entonces E_F tiene un elemento primitivo si y sólo si hay una cantidad finita de subcampos intermedios entre F y E.*

Demostración. Supongamos primero que $E = F(u)$ y sea K un campo intermedio de E_F. Como $|E : F| < \infty$, entonces $|K : F| < \infty$. Sea $f(x)$ el polinomio mínimo asociado a u sobre F y sea $g(x)$ el polinomio mínimo sobre K de u. Notemos que, como $F \subset K$, entonces $F[x] \subset K[x]$ por lo que $g(x) \mid f(x)$ en $K[x]$. Supongamos que $g(x) = a_n x^n + \cdots + a_1 x + a_0$, y sea K' el subcampo de E_F generado por los coeficientes de $g(x)$, es decir, $F(a_0, \ldots, a_n)$. Como $g(x) \in K[x]$, entonces $K' \subset K$. Afirmamos que $g(x)$ también es el polinomio mínimo de u sobre K'. Si $g'(x)$ es el polinomio mínimo de u sobre K', como $K' \subset K$, se tiene que $g(x) \mid g'(x)$. Por construcción, también se tiene que

$$g(x) \in K'[x] = F(a_0, \ldots, a_n)[x],$$

y como $g'(x)$ es el polinomio mínimo para u sobre K', entonces $g'(x) \mid g(x)$, por lo que $g(x) = g'(x)$. Por lo tanto, como

$$\operatorname{grad} g(x) = |E : K'| = |E : K|\,|K : K'| = (\operatorname{grad} g(x))\,|K : K'|,$$

entonces $|K : K'| = 1$, es decir, $K = K'$. De esta manera, hemos visto que los campos intermedios de E_F están formados por los coeficientes de un factor irreducible de $f(x)$ en $E[x]$. Por el Teorema de factorización única, $f(x)$ se factoriza en un producto finito de polinomios irreducibles $p_1(x) \cdots p_n(x)$. Como los campos intermedios están generados por los coeficientes de algún p_i sobre F, esto implica que sólo hay una cantidad finita de campos intermedios de E_F.

Supongamos ahora que E_F tiene una cantidad finita de subcampos intermedios. Si F es finito, por el teorema anterior, como $|E : F| < \infty$, E tiene un elemento primitivo sobre F. Supongamos entonces que F tiene cardinalidad infinita. Como $|E : F| < \infty$, podemos suponer sin pérdida de generalidad que $E = F(a_1, \ldots, a_n)$ para algún $n \in \mathbb{N}$. La prueba se hará por inducción. Para esto, demostraremos que para cualquier $u, v \in E$, $F(u, v) = F(w)$, para algún w, ya que de esta manera,

$$F(a_1, \ldots, a_n) = F(a_1, a_2)(a_3, \ldots, a_n) = F(b)(a_3, \ldots, a_n),$$

éste último con $n - 1$ factores, con lo cual se le puede aplicar la hipótesis de inducción.

Si $n = 1$, el resultado es claro. Supongamos entonces que $E = F(a_1, \ldots, a_n)$ para $n > 1$. Sean $u, v, F(u), F(v)$. Para cada $a \in F$, definamos al subcampo intermedio $F(av + u)$. Nótese que $F \subset F(av + u) \subset F(u, v)$ para toda $a \in F$. Como por hipótesis hay una cantidad finita de subcampos intermedios en E_F, esto implica que algunos subcampos intermedios definidos anteriormente se repiten, es decir, existen $a, b \in F$ con $a \neq b$, tales que $F(av + u) = F(bv + u)$. Ahora, si $a, b \in F$ son tales que $a \neq b$ y $F(av + u) = F(bv + u)$, entonces $bv + u \in F(av + u)$. De esta manera,

$$v = \frac{av + u - bv - u}{a - b} \in F(av + u),$$

por lo que $av \in F(av + u)$, y $u = av + u - av \in F(av + u)$. Por lo tanto, $F(u, v) \subset F(av + u)$. Como ya se tenía la otra contención, se tiene que $F(u, v) = F(av + u)$, es decir, $w = av + u$.

Como

$$E = F(a_1, \ldots, a_n) = F(a_1, a_2)(a_3, \ldots, a_n) = F(b)(a_3, \ldots, a_n),$$

por hipótesis de inducción,

$$E = F(b)(a_3, \ldots, a_n) = F(w),$$

por lo que E tiene un elemento primitivo sobre F. ■

Corolario 11 *Si E es una extensión separable de F con $|E : F| < \infty$, entonces E contiene un elemento primitivo sobre F.*

Demostración. Sea E es una extensión separable de F dimensionalmente finita y sea K la cerradura normal de E_F. Como vimos anteriormente, K es

normal y separable sobre F, por lo que es Galois sobre F. Sea $G = GalK_F$. Como $|G| = |K : F| < \infty$, G tiene una cantidad finita de subgrupos. Por la correspondencia de Galois, esto equivale a decir que hay una cantidad finita de subcampos intermedios de K_F. Como $F \subset E \subset K$, se tiene que E_F también tiene una cantidad finita de subcampos intermedios. Por el teorema anterior, E tiene un elemento primitivo u sobre F. ■

0.25. Campos Reales Cerrados.

Definición 43 *Un campo ordenado (F, P) es un campo F junto con un subconjunto P (el subconjunto de los elementos positivos) de F tal que cumple lo siguiente: (1) $0 \notin P$,(2) si $a \in F$ entonces se cumple una y sólo una de las siguientes condiciones: $a \in P$, $a = 0$, o $-a \in P$, (3) si $a, b \in P$ entonces $a + b \in P$ y $ab \in P$. Se dice que un campo F es* ***ordenable*** *si es posible encontrar un subconjunto P de F que cumpla las tres propiedades anteriores.*

Como cualquier campo contiene más de un elemento, si (F, P) es un campo ordenado entonces P es distinto del conjunto vacío. Si N denota el conjunto $\{-a \mid a \in P\}$ entonces $N \cap \{0\} = \varnothing$, pues si $0 \in N \cap \{0\}$ entonces en particular $0 \in N$, por lo que $0 = -a$ para alguna $a \in P$. Pero la única solución a esta igualdad es $a = 0$, lo cual nos lleva a la contradicción de que $0 \in P$. Otra observación es que $P \cap N = \varnothing$,ya que si $x \in P \cap N$ entonces en particular $x \in N$, y como $x = -(-x)$, por definición de N, se tendría que $-x \in P$, pero esto implica que $x + (-x) = 0 \in P$ lo cual contradice (1). Como $P \cap N = \varnothing$ y se cumple la propiedad (2) de la definición de campo ordenado, se tiene que $F = P \cup \{0\} \cup N$, es decir, F es la unión ajena de P, N, y $\{0\}$. Notemos también que N es cerrado bajo la adición, ya que si $a, b \in P$ entonces $-a, -b \in N$ y $-a + (-b) = -(a + b) \in N$, ya que $a + b \in P$ por (3). Además, si $a, b \in N$ entonces $-a, -b \in P$, por lo que $ab = (-a)(-b) \in P$, teniendo así que N no es cerrado bajo multiplicación.

Ahora introduciremos una relación de orden en (F, P) definida por $b < a$ si y sólo si $a - b \in P$. De esta manera, dados $a, b \in F$ se cumple una y sólo una de las siguientes condiciones, $a - b \in P, a - b = 0$ ó $a - b \notin P$. Notemos que si $a - b \notin P$ y $a - b \neq 0$ entonces $a - b \in N$, por lo que $b - a = -(a - b) \in P$. De esta manera, se cumple la tricotomía en el campo ordenado (F, P), es decir, $\forall a, b \in F$, se cumple una y sólo una de las siguientes condiciones: $b < a$, $a = b$, o $a < b$. Ahora, si $b < a$ entonces $b + c < a + c, \forall c \in F$ ya que esto pasa si y sólo si $(a + c) - (b + c) \in P$ pero

$$(a + c) - (b + c) = a + c - b - c = a + b + (c - c) = a + b \in P.$$

Por otra parte, también se cumple que $bp < ap$ para cualquier $p \in P$, pues por definición $bp < ap$ si y sólo si $(ap - bp) \in P$ pero $ap - bp = p(a - b)$ y como

tanto p como $a-b$ están en P, el cual es cerrado bajo multiplicación, entonces $ap-bp=p(a-b)\in P$.

De manera similar podemos empezar considerando la relación $>$ en el campo F tal que satisfaga la ley de tricotomía, la ley de transitividad y las dos propiedades siguientes, (a) $a>b\Longrightarrow a+c>b+c,\forall c\in F$ y (b) $ap>bp\ \forall p>0$. Definamos ahora el conjunto $P=\{p\mid p>0\}$. Veamos que (F,P) es un campo ordenado: por definición, $P=\{p\mid p>0\}$, así que $0\notin P$. Si $a\in F$, entonces por la tricotomía se tiene que para $a,0\in F$ se cumple una y sólo una de las siguientes relaciones: $a>0, a=0, 0>a$. Si $a=0$ no hay nada que demostrar, por lo que podemos suponer que $a\neq 0$. Si $a>0$ entonces $a\in P$. Ahora, si $0>a$, entonces por la propiedad (a), tomando $c=-a$ se tiene que

$$-a=0+(-a)>a+(-a)=0,$$

por lo que $-a>0$, es decir, $-a\in P$. De esta manera, para cualquier $a\in F$, se cumple una y sólo una de las siguientes condiciones, $a\in P, a=0, -a\in P$. Falta demostrar que P es cerrado bajo sumas y productos. Sean $a,b\in P$. Entonces por definición se tiene que $a>0$ y $b>0$, así que usando la propiedad (a) y la transitividad de $>$, se tiene que $a+b>0+b=b>0$, lo cual implica que $a+b>0$, por lo que $a+b\in P$. Por otra parte, como $a>0$ y $b>0$, por la propiedad (b) se tiene que $ab>0b=0$, por lo que $ab\in P$. Por lo tanto, (F,P) es un campo ordenado inducido por la relación $>$ antes definida.

Si F'es un subcampo de (F,P) entonces (F',P') es un campo ordenado donde $P'=F'\cap P\subseteq P$. A esto lo llamaremos la ordenación inducida en F'. Si (F,P) y (F',P') son cualesquiera dos campos ordenados, entonces un isomorfismo $\eta: F\longmapsto F'$ se dice que es ordenado si $\eta(P)\subset P'$. Notemos que como η es isomorfismo cumple que $\eta(0)=0$. Ahora, basta ver que $\eta(N)\subset N'$ para tener que $\eta(P)=P'$. Si $\eta(N)\nsubseteq N'$ entonces existe un $z\in N$, con $z\neq 0$ tal que $\eta(z)\in P'$. Notemos que se descarta el caso $\eta(z)=0$ porque η es

isomorfismo. Ahora, si $\eta(z)\in P'$ entonces $-\eta(z)\in N'$, pero $-\eta(z)=\eta(-z)$, y como $z\in N$, entonces $-z\in P$. Esto último nos lleva a la contradicción de que $-z\in P$ y $\eta(-z)\in N$, cuando habíamos supuesto que $\eta(P)\subset P'$. Por lo tanto se tiene que $\eta(N)\subset N'$ y así $\eta(P)=P'$.

Notemos ahora que en cualquier campo ordenado (F,P), si $a\in F$ y $a\neq 0$, entonces $0<a^2$, ya que si $a\in P$, como P es cerrado bajo productos, entonces $a^2\in P$, teniendo así que $0<a^2$. Si $a\in N$ entonces $-a\in P$, y así $a^2=(-a)(-a)=P$. De esto hecho se sigue que si $a_1,a_2,....,a_n\neq 0$ entonces $\sum a_i^2\neq 0$. En particular

$$1+1+.....+1=1^2+1^2+.....+1^2\neq 0,$$

lo cual nos dice que cualquier campo ordenado tiene característica 0. Otra observación es que no se puede tener en un campo que $-1=\sum a_i^2$, pues de lo contrario se tendría que

$$1+\sum a_i^2=1^2+\sum a_i^2=0$$

lo cual contradice lo anterior. De esta manera, $-1 \neq a^2\ \forall a \in F$, concluyendo así que F no tiene raíces cuadradas de -1. Con esto se demuestra la siguiente

Proposición 19 *El campo de los complejos $\mathbb{C}$ no tiene un orden compatible con las operaciones.*

Definición 44 *Sea R un campo y (R, P) un campo ordenado. Se dice que R es real cerrado si cumple las siguientes propiedades:*

(i) $\forall a \in P\ \exists b \in R$ tal que $b^2 = a$, es decir todo elemento positivo de R tiene raíz cuadrada.

(ii) Cualquier polinomio $f(x) \in R[x]$ con grado impar tiene una raíz en R.

Teorema 59 *Un campo R real cerrado tiene un único orden que le proporciona la estructura de campo ordenado. Cualquier automorfismo del campo R en R es un isomorfismo ordenado. Además, si R es real cerrado entonces el subcampo de elementos algebraicos sobre $\mathbb{Q} \subset R$ es real cerrado.*

Demostración. Sea (R, P) real cerrado y sea (R, P') cualquier otro campo ordenado. Para la primera parte de la demostración vamos a ver que $P = P'$. Si $a \in P$ entonces existe $b \neq 0$ en R tal que $a = b^2$ con $b \neq 0$, pues (R, P) es real cerrado. Como $b \neq 0$ entonces tenemos dos casos posibles, $b \in P'$ o $-b \in P'$. Si $b \in P'$, como P'es cerrado bajo producto se tiene que $a = b^2 \in P'$, por lo que $a \in P'$. Si $-b \in P'$, de nuevo se tiene que $a = b^2 = (-b)(-b) \in P'$, por lo que $P \subset P'$. Veamos la otra contención. Supongamos lo contrario, es decir, que existe $0 \neq b \in P'$ tal que $b \notin P$. Como $b \neq 0$ y $b \notin P$ entonces $-b \in P$, pero como R es real cerrado se tiene que $\exists c \in R$ tal que $c^2 = -b$, pero esto equivale a decir que $-b \in P'$ pues $c^2 > 0$. Como P' es cerrado bajo la suma, se tiene que $0 = b + (-b) \in P'$, lo cual es una contradicción. Por lo tanto $P' \subset P$ y de esta manera $P = P'$, por lo que R tiene un único orden de estructura de campo ordenado.

Veamos ahora la segunda parte del teorema. Sea $\Psi : R \longrightarrow R$ un automorfismo. Por definición tenemos que Ψ es un isomorfismo, y de esta manera sabemos que $Ker\Psi = \{0\}$. Basta demostrar que $\Psi(P) = P$, ya que así $\Psi(N) = N$ es inmediato. Veamos primero que $\Psi(P) \subset P$. Sea $a \in \Psi(P)$. Entonces, por definición, existe $b \in P$ tal que $\Psi(b) = a$. Como $b \in P$ y R es real cerrado, existe $c \in R$ con $c \neq 0$ tal que $c^2 = b$. Ahora, como Ψ es un isomorfismo se tiene que

$$(\Psi(c))^2 = \Psi(c)\Psi(c) = \Psi(c^2) = \Psi(b) = a.$$

De esta manera se tiene que $a = (\Psi(c))^2$, y por lo tanto $a \in P$. Así, $\Psi(P) \subset P$.

Sea ahora $a \in P$. Como Ψ es un isomorfismo existe $b \in R$ tal que $\Psi(b) = a$. Basta entonces demostrar que $b \in P$. Supongamos que $b \notin P$. Como $b \neq 0$

entonces $-b \in P$. Así, $-b = c^2$ para algún $c \in R$, con $c \neq 0$. De esta manera, se tiene que

$$(\Psi(c))^2 = \Psi(c)\Psi(c) = \Psi(cc) = \Psi(c^2) = \Psi(-b) = -\Psi(b) = -a.$$

Como $(\Psi(c))^2 \in P$ entonces $-a \in P$. Pero esto nos lleva a la contradicción de $0 = a+(-a) \in P$. Por lo tanto $b \in P$, y así $\Psi(P) = P$. Como Ψ es un isomorfismo y se cumple que $R = P \cup \{0\} \cup N$ y $\Psi(P) = P$ entonces $\Psi(N) = N$.

Sea R real cerrado y sea R_0 el subcampo de elementos algebráicos sobre $\mathbb{Q}$. Sea $a \in R_0 \cap P$, con P el subconjunto de R de elementos positivos. Como $R_0 \subset R$ y R es real cerrado entonces $\exists b \in R$ tal que $b^2 = a$, por lo que b satisface el polinomio $x^2 - a = 0$, teniendo así que b es algebráico sobre R_0. Ahora, como a es algebráico sobre $\mathbb{Q}$, entonces la dimensión de $\mathbb{Q} \hookrightarrow \mathbb{Q}(a)$ es finita. Por otra parte, como b satisface el polinomio $x^2 - a = 0$ entonces $\mathbb{Q}(a) \hookrightarrow \mathbb{Q}(ab)$ también es de dimensión finita, así que $\mathbb{Q} \hookrightarrow \mathbb{Q}(a) \hookrightarrow \mathbb{Q}(ab)$ es de dimensión finita. Por lo tanto, del siguiente diagrama

$$\begin{array}{ccccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}(a) & \hookrightarrow & \mathbb{Q}(ab) \\ & \searrow & & \nearrow & \\ & & \mathbb{Q}(b) & & \end{array}$$

se concluye que también $\mathbb{Q} \hookrightarrow \mathbb{Q}(b) \hookrightarrow \mathbb{Q}(ab)$ tiene dimensión finita y así $\mathbb{Q} \hookrightarrow \mathbb{Q}(b)$ es también dimensionalmente finito, por lo que b es algebráico sobre $\mathbb{Q}$, es

decir, $b \in R_0$. Con esto queda demostrado que R_0 cumple (i).

Sea $f(x) \in R_0[x]$ con grado impar. Por una parte, como $R_0 \subset R$ entonces $R_0[x] \subset R[x]$ así que $f(x) \in R[x]$. Como R es real cerrado, $f(x)$ tiene una raíz en R. Sea $\alpha \in R$ tal que $f(\alpha) = 0$. Queremos ver que $\alpha \in R_0$, es decir, que α es algebráico sobre $\mathbb{Q}$, o lo que es equivalente, a decir que $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha)$ es de dimensión finita. Si $f(x) = a_0 + a_1x + ... + a_nx^n$, entonces se

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(a_0) \hookrightarrow \mathbb{Q}(a_0, a_1) \hookrightarrow .... \hookrightarrow \mathbb{Q}(a_0, a_1, ..., a_n).$$

Cada extensión es de dimensión finita ya que todos los $a_i \in R_0$, es decir, son algebráicos sobre $\mathbb{Q}$. Por otro lado, como α es raíz de $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Q}(a_0, a_1, ..., a_n)[x]$ entonces $\mathbb{Q}(a_0, a_1, ..., a_n) \hookrightarrow \mathbb{Q}(a_0, a_1, ..., a_n)(\alpha)$ es de dimensión finita. Por lo tanto, se tiene el siguiente diagrama

$$\begin{array}{ccccccccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}(a_0) & \hookrightarrow & \cdots & \hookrightarrow & \mathbb{Q}(a_0, \cdots, a_n) & \hookrightarrow & \mathbb{Q}(a_0, \cdots, a_n)(\alpha) \\ & \searrow & & & & & & \nearrow & \\ & & \searrow & & & & \nearrow & & \\ & & & \searrow & & \nearrow & & & \\ & & & & \mathbb{Q}(\alpha) & & & & \end{array}$$

Ahora, como la dimensión entre $\mathbb{Q} \hookrightarrow \mathbb{Q}(a_0, a_1...a_n)$ es finita y también lo es la de $\mathbb{Q}(a_0, a_1, ..., a_n) \hookrightarrow \mathbb{Q}(a_0, a_1, ..., a_n)(\alpha)$ entonces $\mathbb{Q} \hookrightarrow \mathbb{Q}(a_0, a_1, ..., a_n)(\alpha)$ también es de dimensión finita. Como $a_0, \ldots, a_n$ son algebráicos sobre $\mathbb{Q}$, entonces

$$|\mathbb{Q}(a_0, a_1, ..., a_n)(\alpha) : \mathbb{Q}(\alpha)| = |\mathbb{Q}(\alpha)(a_0, a_1, ..., a_n) : \mathbb{Q}(\alpha)| < \infty.$$

Por lo tanto, como $|\mathbb{Q}(a_0, a_1, ..., a_n)(\alpha) : \mathbb{Q}| < \infty$ y

$$|\mathbb{Q}(a_0, a_1, ..., a_n)(\alpha) : \mathbb{Q}| = |\mathbb{Q}(a_0, a_1, ..., a_n)(\alpha) : \mathbb{Q}(\alpha)|\,|\mathbb{Q}(\alpha) : \mathbb{Q}|$$

con $|\mathbb{Q}(a_0, a_1, ..., a_n)(\alpha) : \mathbb{Q}(\alpha)| < \infty$, entonces $|\mathbb{Q}(\alpha) : \mathbb{Q}| < \infty$, concluyendo así que α es algebráico sobre $\mathbb{Q}$, es decir, $\alpha \in R_0$. ■

Teorema 60 *Si R es real cerrado entonces $R(\sqrt{-1})$ es algebraicamente cerrado.*

Demostración. Notemos primero que $\sqrt{-1} \notin R$, ya que de lo contrario, se tendría que $(\sqrt{-1})^2 = -1 \in P$ y como $1 \in P$ se tendría que $0 = 1 + (-1) \in P$, lo cual es una contradicción. Ahora tomemos el automorfismo $\varphi : R(\sqrt{-1}) \longrightarrow R(\sqrt{-1})$ definido por $a + b\sqrt{-1} \longmapsto a - b\sqrt{-1}$, donde $a, b \in R$. A esta función, también se le conoce como la función conjugar. Para facilitar la notación, definamos $C \equiv R(\sqrt{-1})$. Observemos que, si $r \in C$ y $r = \overline{r}$ entonces $r \in R$, pues si $a + b\sqrt{-1} = r = \overline{r} = a - b\sqrt{-1}$ entonces $b\sqrt{-1} = -b\sqrt{-1}$, lo cual implica que $b = 0$, teniendo así que $r = a$ con $a \in R$.

Sea $f(x) \in C[x]$. Afirmamos que $f(x)\overline{f(x)} \in R[x]$. Si $f(x) = a_0 + a_1x + ... + a_nx^n$ entonces $\overline{f(x)} = \overline{a_0} + \overline{a_1}x + ... + \overline{a_n}x^n$, por lo que $f(x)\overline{f(x)} = \sum d_i x^i$ donde $i = \{0, 1, 2, ..., 2n\}$ y $d_k = \sum_{i+j=k} a_i\overline{a_j}$. Nótese que

$$d_k = \sum_{i+j=k} a_i\overline{a_j} = \sum_{i+j=k} \overline{a_i}a_j = \overline{\sum_{i+j=k} a_i\overline{a_j}} = \overline{d_k},$$

ya que $i + j = k = j + i$. Como $d_k = \overline{d_k}$ entonces $d_k \in R$ para toda k, y así

$$f(x)\overline{f(x)} \in R[x].$$

Ahora, si $f(x)\overline{f(x)} = 0$, entonces $f(x) = 0$ o $\overline{f(x)} = 0$. Notemos que si α es tal que $\overline{f(\alpha)} = 0$, entonces $f(\alpha) = \overline{\left(\overline{f(\alpha)}\right)} = \overline{0} = 0$, por lo que en cualquier caso se tiene que $f(x) = 0$. Por lo tanto, si $f(x)\overline{f(x)}$ tiene una raíz en C entonces también $f(x)$ la tiene. De esta manera, para demostrar que C es algebráicamente cerrado basta probar que cualquier polinomio mónico con coeficientes en R tiene una raíz en C. Esto es es claro si el polinomio tiene grado impar pues R es real cerrado y $R \subset C \equiv R(\sqrt{-1})$.

Demostraremos primero que cualquier elemento de C tiene raíz cuadrada en C. Si $a \in R$ y $0 < a$ entonces el resultado se cumple ya que R es real cerrado. Si $a \in R$ y es tal que $a < 0$, entonces $-a > 0$ por lo que $b^2 = -a$ para alguna $b \in R$, es decir, $(\sqrt{-1}b)^2 = -b^2 = a$. Supongamos entonces que $r = a + b\sqrt{-1}$ con $a, b \in R$, y $b \neq 0$. Para facilitar la notación, tomaremos a $i := \sqrt{-1}$. Sean $x, y \in R$, entonces $(x + iy)^2 = r$ si y sólo si $x^2 - y^2 = a$ y $2xy = b$.(1).

Como $b \neq 0$ podemos suponer que $b = 2$, así que la segunda ecuación toma la forma $xy = 1$ y esto pasa si y sólo si $y = x^{-1}$. Así, la primera ecuación toma la forma $x^2 - x^{-2} = a$. Si hacemos el cambio de variable $z = x^2$, tenemos que esta última ecuación toma la forma $z - z^{-1} = a$, que equivale multiplicando ambos lados por z a $z^2 - az - 1 = 0$. Con esto tenemos una nueva ecuación de segundo grado de una sola variable, así que usando la formula general de segundo grado o la fórmula del chicharronero como también se conoce, se tiene que la solución $(a \pm \sqrt{a^2 + 4})/2$ esta en R pues $a^2 + 4 > 0$. Recordemos que queremos una raíz en C, así que sin pérdida de generalidad podemos tomar la solución $a + \sqrt{a^2 + 4})/2$. Notemos que $a + \sqrt{a^2 + 4} > 0$ pues en caso contrario se tendría que

$$a + \sqrt{a^2 + 4} \leq 0 \Longrightarrow 0 \leq \sqrt{a^2 + 4} \leq -a \Longrightarrow a^2 + 4 \leq (-a)^2 = a^2 \Longrightarrow 4 \leq 0$$

lo cual es una contradicción. Así, se tiene que existe $x \neq 0$ en R tal que

$$x^2 = z = a + \sqrt{a^2 + 4})/2.$$

Por lo tanto, x cumple las ecuaciones $x^4 - ax^2 = 1$ y $x^2 - x^{-2} = a$. Ahora, para $b = 2$ se tiene que tanto x y $y = x^{-1}$ satisfacen (1), por lo que queda demostrado que todo elemento en C tiene una raíz cuadrada en C.

Notemos que no hay extensiones de campo E de C tales que $|E : C| = 2$. Para ver esto supongamos lo contrario. Sea E una extension de C tal que $|E : C| = 2$. Sea $\alpha \in E/C$. Fijémonos en el siguiente diagrama:

$$\begin{array}{ccc} C & \hookrightarrow & E \\ \downarrow & \nearrow & \\ C(\alpha) & & \end{array}$$

Como $2 = |E : C| = |C(\alpha) : C|\,|E : C(\alpha)|$, entonces $|C(\alpha) : C| = 1$ ó $|C(\alpha) : C| = 2$, pues estos son los dos únicos divisores positivos de 2 en $\mathbb{Z}$. Ahora, $|C(\alpha) : C| \neq 1$ ya que si $|C(\alpha) : C| = 1$, entonces $C(\alpha) = C$, por lo que $\alpha \in C$, lo cual nos lleva a la contradicción de la elección de α. Por lo tanto, $|C(\alpha) : C| = 2$. Por otra parte, como $\alpha \in C(\alpha)$ y la extensión $C(\alpha)$ de C es finita, entonces α es algebráico sobre C, por lo que existe $f(x) \in C[x]$ tal que $f(x) = x^2 + bx + c$ con

$b, c \in C$ y $f(\alpha) = 0$.Usando la fórmula general de segundo grado se tiene que $\alpha = (-b \pm \sqrt{b^2 - 4c})/2$. Notemos que como $b, c \in C$ entonces $(b^2 - 4c) \in C$ y así$\sqrt{b^2 - 4c} \in C$, por lo que $\alpha = ((-b \pm \sqrt{b^2 - 4c})/2) \in C$, lo cual contradice de nuevo la elección de α. Así, hemos demostrado que no hay extensiones de C de dimensión dos. Esto lo usaremos para probar que todo polinomio mónico con coeficientes en R tiene raíces en C.

Sea $f(x) \in R[x]$ mónico. Sea E un campo de descomposición sobre R de $f(x)(x^2+1)$. Por definición, $R \subset E$ y como $\sqrt{-1}$ es raíz de x^2+1, entonces $\sqrt{-1} \in E$ por lo que $C \subset E$. Además, como R tiene característica 0 por ser campo real cerrado y $R \subset E$, entonces E también es de característica cero, por lo que E es de Galois sobre R. Sea $G = GalE_R$. Entonces $|G| = 2^n k$ donde k es impar y $n > 0$. Ahora, por el teorema de Sylow tenemos que existe $H \leq G$ tal que $|H| = 2^n$.

Sea D el subcampo correspondiente a H en E_R. Notemos que $|E:D| = |H|$. Como $[E:D]\,[D:R] = [E:R] = 2^n k$ y $[E:D] = 2^n$ entonces $[D:R] = k$. Como R es real cerrado, R no tiene extensiones de campo de dimensión impar, así que $k = 1$, por lo que $R = D$. De esta manera, $[E:R] = 2^n$ y así $H = G$. Ahora, si $n > 1$, por la teoría de Galois E contiene un subcampo F tal que $C \subset F$ y $[F:C] = 2$, lo cual es una contradicción a lo demostrado anteriormente. Por lo tanto, $n = 1$. Consideremos el siguiente diagrama:

$$\begin{array}{ccc} R & \hookrightarrow & E \\ \downarrow & \nearrow & \\ C & & \end{array}$$

Como $R \subset C \subset E$ se tiene que $[E:C][C:R] = [E:R] = 2$. Por lo tanto, se tienen dos casos posibles, $[C:R] = 1$ ó $[C:R] = 2$. Como $R \subsetneq C$ entonces $[C:R] \neq 1$ por lo que $[C:R] = 2$. De esta manera, $[E:C] = 1$ y así $E = C$. Por lo tanto, como $E = C$ es el campo de descomposición de $f(x) \in R[x]$, entonces C contiene una raíz de $f(x)$, demostrando que C es algebráicamente cerrado. ■

Corolario 12 *El campo de los complejos* $\mathbb{C}$ *es algebráicamente cerrado.*

Notemos que del teorema anterior se deduce que los únicos polinomios irreducibles en $R[x]$ son de primer o segundo grado. Esto se debe a que, por una parte, si el grado del polinomio es impar y mayor que uno entonces por ser R real cerrado, $f(x)$ tiene una solución α en R, por lo que se le puede factorizar a $f(x)$ un término de la forma $x-\alpha \in R[x]$. Si $f(x)$ tiene grado $2n$ con $1 < n$, por el teorema anterior tenemos que $f(x)$ tiene una raíz $w \in C$. Como $f(w) = 0$ entonces $0 = \overline{0} = \overline{f(w)} = f(\overline{w})$. Por lo tanto, $\overline{w}$ también es raíz de $f(x)$ y entonces $f(x) = (x-w)(x-\overline{w})g(x)$ donde $g(x)$ tiene grado $2n-2$. Por la observación hecha en el teorema anterior $(x-w)(x-\overline{w}) \in R[x]$ el cual tiene grado 2. De esta manera, $f(x)$ tiene un factor irreducible de grado 2 en $R[x]$, por lo que $f(x)$ no es irreducible.

Otra observación del teorema anterior es que la ecuación cuadrática x^2+bx+c es irreducible en $R[x]$ si y solo si $b^2 < 4c$, ya que $b^2 - 4c$ es el discriminante de

la ecuación cuadrática, y esta no tiene solución en R si $b^2 - 4c < 0$, es decir, cuando $b^2 < 4c$.

Ahora probaremos el siguiente resultado, que nos será de utilidad para nuestra siguiente sección, las sucesiones de Sturm.

Teorema 61 *Sea R un campo real cerrado y $f(x) \in R[x]$. Sean $a, b \in R$ tales que $f(a)f(b) < 0$. Entonces existe $c \in R$ tal que $a < c < b$ y $f(c) = 0$.*

Demostración. Sin pérdida de generalidad podemos suponer que $f(x)$ es mónico y que $a < b$. Por las observaciones anteriores, $f(x)$ se factoriza en $R[x]$ como

$$f(x) = (x - r_1) \cdots (x - r_k) g_1(x) \cdots g_n(x)$$

donde cada $g_i(x) = x^2 + b_i x + c_i$, con $b_i^2 < 4c_i$ y $r_1 < r_2 < \ldots < r_k$. Notemos que a cada $g_i(x)$ la podemos ver de la siguiente manera:

$$g_i(x) = x^2 + b_i x + c_i = x^2 + b_i x + (\frac{b_i^2}{4} - \frac{b_i^2}{4}) + c_i = (x + \frac{b_i}{2})^2 + \frac{1}{4}(4c_i - b_i^2).$$

Si denotamos a $e_i := \sqrt{\frac{1}{4}(4c_i - b_i^2)}$, el cual está bien definido ya que por hipótesis $b_i^2 < 4c_i$, se tiene que para toda $i \in 1, \ldots, n$, $g_i(x) = (x + \frac{b_i}{2})^2 + e_i^2$. Notemos ahora que $g_i(x) > 0$, $\forall x \in R$, pues es la suma de dos cuadrados.

Ahora, si $a, b < r_i \forall i \in \{1, \ldots, n\}$ entonces $a - r_i < 0$ y $b - r_i < 0$ por lo que

$(a - r_i)(b - r_i) > 0$. De esta manera

$$f(a)f(b) = \prod (a - r_i)(b - r_i) g_i(a) g_i(b) > 0.$$

Análogamente, si $a, b > r_i$, $\forall i \in \{1, \ldots, n\}$ se tiene que $a - r_i > 0$ y $b - r_i > 0$,

y así $(a - r_i)(b - r_i) > 0$ por lo que de nuevo $f(a)f(b) > 0$. Como por hipótesis $f(a)f(b) < 0$ entonces afirmamos que alguna de las r_i queda en medio de a y b. Supongamos que no, es decir, que se tiene un arreglo de la forma

$$r_1 < r_2 < \ldots < r_m < a < b < r_{m=1} < \ldots < r_k$$

donde $m \in \{1, \ldots, k-1\}$. Notando que $a - r_j > 0, b - r_j > 0$ para $j \in 1, \ldots, m$ y $a - r_l < 0, b - r_l < 0$ para $l \in m+1, \ldots, k$ se tiene que

$$f(a)f(b) = \prod (a - r_i)(b - r_i) g_i(a) g_i(b) > 0$$

puesto que $(a - r_j)(b - r_j) > 0$ y $(a - r_l)(b - r_l) > 0$, para $j \in \{1, \ldots, m\}$ y $l \in \{m+1, \ldots, k\}$, lo cual contradice la hipótesis.

Por lo tanto, alguna de las r_i se encuentra en medio de a y b y r_i es tal que $f(r_i) = 0$. ■

Proposición 20 *Sea F un campo ordenado y $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ tal que $a_i \in F$. Sea $M = \text{máx}(1, \sum_{i=0}^{n-1} |a_i|)$. Entonces, si $|x| > M$, $|f(x)| > 0$, es decir, las raíces de $f(x)$ en F se encuentran en el intervalo $-M \leq x \leq M$.*

Demostración. Sea F un campo ordenado y

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = f(x) \in F[x].$$

Sea $M = \text{máx}(1, \sum_{i=0}^{n-1} |a_i|)$ y sea x tal que $|x| > M$. Notemos lo siguiente:

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

$$= |x| \left|x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right| - |a_0|$$

Como $|x| > M = \text{máx}(1, \sum_{i=0}^{n-1} |a_i|)$, en particular $|x| > 1$ por lo que

$$|x| \left|x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right| - |a_0| > \left|x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right| - |a_0|$$

Ahora,

$$\left|x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right| - |a_0| \geq \left|x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2x\right| - |a_0| - |a_1|$$

$$= |x| \left|x^{n-2} + a_{n-1}x^{n-3} + \cdots + a_2\right| - (|a_0| + |a_1|)$$

$$> \left|x^{n-2} + a_{n-1}x^{n-3} + \cdots + a_2\right| - (|a_0| + |a_1|)$$

$$\geq \left|x^{n-2} + a_{n-1}x^{n-3} + \cdots + a_3x\right| - (|a_0| + |a_1| + |a_2|).$$

Prosiguiendo de esta manera se tiene que

$$|f(x)| > \left|x^{n-((n-2)-1)} + a_{n-1}x^{(n-1)-((n-2)-1)} + a_{n-2}x\right| - (\sum_{i=0}^{n-3} |a_i|)$$

$$= \left|x^3 + a_{n-1}x^2 + a_{n-2}x\right| - (\sum_{i=0}^{n-3} |a_i|) = |x| \left|x^2 + a_{n-1}x^2 + a_{n-2}\right| - (\sum_{i=0}^{n-3} |a_i|)$$

$$> \left|x^2 + a_{n-1}x + a_{n-2}\right| - (\sum_{i=0}^{n-3} |a_i|)$$

Por lo tanto, se tiene que

$$|f(x)| > \left|x^2 + a_{n-1}x + a_{n-2}\right| - (\sum_{i=0}^{n-3} |a_i|) \geq \left|x^2 + a_{n-1}x\right| - (\sum_{i=0}^{n-2} |a_i|)$$

$$= |x| \, |x + a_{n-1}| - (\sum_{i=0}^{n-2} |a_i|) > |x + a_{n-1}| - (\sum_{i=0}^{n-2} |a_i|)$$

$$\geq |x| - |a_{n-1}| - (\sum_{i=0}^{n-2} |a_i|) = |x| - (\sum_{i=0}^{n-1} |a_i|)$$

Como se eligió $|x| > M$, con $M = \text{máx}(1, \sum_{i=0}^{n-1} |a_i|)$, en particular $M > \sum_{i=0}^{n-1} |a_i|$, por lo que $|x| - (\sum_{i=0}^{n-1} |a_i|) > |x| - M > 0$.

Por lo tanto, $|f(x)| > |x| - (\sum_{i=0}^{n-1} |a_i|) > |x| - M > 0$, por lo que las raíces de $f(x)$ en F se encuentran todas en el intervalo $-M \leq x \leq M$. ■

0.26. Teorema de Sturm

En esta sección se demostrará el teorema de Sturm, el cual nos ayudará a determinar el número exacto de raíces de un polinomio $f(x)$ en un intervalo de campo real cerrado R.

Definición 45 *Sea R un campo real cerrado y sea $f(x)\in R[x]$. Diremos que la*

sucesión de polinomios $f(x) = f_0(x), f_1(x), \ldots, f_n(x)$ es una sucesión de Sturm de polinomios para $f(x)$ en el intervalo $[a, b]$ si $f_i(x) \in R[x]$ y cumplen las siguientes propiedades:

(i) $f_n(x)$ no tiene raíces en $[a, b]$

(ii) $f_0(a)f_0(b) \neq 0$

(iii) Si $c \in [a, b]$ es una raíz de $f_j(x)$, con $0 < j < n$ entonces

$$f_{j-1}(c)f_{j+1}(c) < 0.$$

(iv) Si $f(c) = 0$ con $c \in (a, b)$ entonces existen intervalos abiertos (c_1, c) y (c, c_2), tal que $\forall u \in (c_1, c)$ y $\forall v \in (c, c_2)$ se tiene que $f_0(u)f_1(u) < 0$ y $f_0(v)f_1(v) > 0$.

Antes de demostrar la existencia de éstas sucesiones, veremos la manera en que ésta sucesión puede ser usada para determinar las raíces de $f(x)$ en el intervalo (a, b). Para esto, consideraremos el número de variaciones o cambios

en el signo de las sucesiones

$$\{f_0(a), f_1(a), \ldots, f_n(a)\} \text{ y } \{f_0(b), f_1(b), \ldots, f_n(b)\}$$

para cualquier par de elementos en R. Sea $c = \{c_1, c_2, \ldots, c_m\}$ una sucesión de elementos en R tal que $c_i \neq 0, \forall i \in \{1, \ldots, m\}$. Definimos el *número de variaciones en el signo de c*, denotándolo por V_c, como el número de *i's*, con $1 \leq i \leq m - 1$, tales que $c_ic_{i+1} < 0$. Si $c = \{c_1, c_2, \ldots, c_m\}$ es cualquier sucesión de elementos en R, entonces definimos el número de cambios en el signo de c como el número de variaciones de signo de la sucesión c', donde c' se obtiene de la sucesión c al quitarle los ceros. Por ejemplo, la sucesión $c = \{-2, 0, 9, 0, 0, 7, -1, 0, 5\}$ tiene tres variaciones de signo, que corresponden a la sucesión $c' = \{-2, 9, 7, -1, 5\}$.

Teorema 62 *Sea $f(x) \in R[x]$ donde R es un campo real cerrado, y sea*

$$f_0(x) = f(x), f_1(x), f_2(x), \ldots, f_n(x)$$

una sucesión de Sturm para la función $f(x)$ en el intervalo $[a, b]$. Entonces el número de raíces distintas de $f(x)$ en el intervalo (a, b) es $V_a - V_b$, donde en general, V_k es el número de cambios de signo de la sucesión $\{f_0(k), f_1(k), \ldots, f_n(k)\}$.

Demostración. Sea $f(x) \in R[x]$ con R un campo real cerrado y sea $f_0(x) = f(x), f_1(x), f_2(x), \ldots, f_n(x)$ una sucesión de Sturm para la función $f(x)$ en el intervalo $[a, b]$. Notemos que el intervalo $[a, b]$ queda partido por subintervalos de la forma $[x_i, x_j]$ donde $i \neq j$ y cada x_i es una raíz de alguna de las $f_s(x)$ elementos de la sucesión de Sturm. De esta manera se tiene una sucesión $a = a_0, a_1, \ldots, a_m = b$ tal que $a_i < a_{i+1}$ y ninguna de las $f_s(x)$ tiene una raíz en (a_i, a_{i+1}) con $0 \leq i \leq m-1$.

Sea $c \in (a_0, a_1)$. Por la observación anterior, $f_j(x)$ no tiene raíces en (a_0, a_1) y en particular en (a_0, c). Por el teorema del valor intermedio se cumple que $0 \leq f_j(a_0) \bullet f_j(c)$ para $0 \leq j \leq n$. Por lo tanto, si ninguna $f_j(x)$ cumple $f_j(a_0) = 0$ entonces $f_j(a_0)$ y $f_j(c)$ tienen el mismo signo para toda j, por lo que $V_{a_0} = V_c$. Supongamos ahora que $f_j(a_0) = 0$ para alguna j. Por hipótesis, se tiene que $f_0(a_0) \neq 0$ y que $f_n(x) \neq 0, \forall x \in [a, b]$, por lo que $j \in \{1, \ldots, n-1\}$. Por la propiedad *iii*) de la sucesión de Sturm tenemos que $f_{j-1}(a_0) \bullet f_{j+1}(a_0) < 0$, teniendo así que $f_{j-1}(a_0), f_{j+1}(a_0) \neq 0$. Como $f_{j-1}(x)$ y $f_{j+1}(x)$ no tienen raíces en (a_0, c) entonces, por el teorema del valor intermedio y la última observación, se tiene que

$$f_{j-1}(a_0) \bullet f_{j-1}(c) > 0 \text{ y } f_{j+1}(a_0) \bullet f_{j+1}(c) > 0.$$

Como $f_{j-1}(a_0) \bullet f_{j+1}(a_0) < 0$, entonces $f_{j-1}(a_0)$ y $f_{j+1}(a_0)$ tienen signos contrarios, por lo que de las últimas desigualdades se sigue que también $f_{j-1}(c)$ y $f_{j+1}(c)$ tienen signos contrarios, es decir, $f_{j-1}(c) \bullet f_{j+1}(c) < 0$. De esta manera, $\{f_{j-1}(a_0), 0 = f_j(a_0), f_{j+1}(a_0)\}$ y $\{f_{j-1}(c), f_j(c), f_{j+1}(c)\}$ aportan cada una de ellas un cambio en el signo en V_a y V_c respectivamente, ya que la elección del signo de $f_j(c)$ no altera en los cambios de signo. Repitiendo esto para todas las j tales que $f_j(a_0) = 0$ se tiene que $V_a = V_c$. Un razonamiento análogo se utiliza para demostrar que $V_d = V_{a_m}$ donde $d \in (a_{m-1}, a_m)$.

Ahora, sea $c \in (a_{i-1}, a_i)$ y $d \in (a_i, a_{i+1})$, con $1 < i < n-1$. Supongamos que

$f(a_i) \neq 0$. Entonces f no tiene raíces en el intervalo (c, d), por lo que $f(c) \bullet f(d) > 0$, y así $f(c)$ y $f(d)$ tienen el mismo signo. Observemos que $\forall j \in \{1, \ldots, n\}$, $f_j(x)$ no tiene raíces en (c, a_i) y en (a_i, d), por lo que $f_j(c) \bullet f_j(a_i) \geq 0$ y

$f_j(a_i) \bullet f_j(d) \geq 0$. Si $f_j(a_i) \neq 0$ para alguna $j \in \{1, \ldots, n\}$, entonces $f_j(c), f_j(a_i)$,

$f_j(d)$ tienen el mismo signo en sus respectivos V_c, V_{a_i} y V_d. Ahora, si $f_j(a_i) = 0$ con $j \in \{1, \ldots, n-1\}$, pues estamos suponiendo que $f(a_i) \neq 0$ y se cumple la propiedad i) de la sucesión de Sturm, por la propiedad *iii*) se tiene que $f_{j-1}(a_i) \bullet f_{j+1}(a_i) < 0$. Como ambas funciones no se anulan en (c, a_i) y (a_i, d) se tiene que

$$\begin{aligned} f_{j-1}(c) \bullet f_{j-1}(a_i) &> 0,\ f_{j+1}(c) \bullet f_{j+1}(a_i) > 0 \\ \text{y } f_{j-1}(a_i) \bullet f_{j-1}(d) &> 0,\ f_{j+1}(a_i) \bullet f_{j+1}(d) > 0, \end{aligned}$$

por lo que $f_{j-1}(c)$ y $f_{j-1}(a_i)$ tienen el mismo signo, así como las parejas $f_{j+1}(c)$ y $f_{j+1}(a_i)$, $f_{j-1}(a_i)$ y $f_{j-1}(d)$, $f_{j+1}(a_i)$ y $f_{j+1}(d)$.

Como $f_{j-1}(a_i)$ y $f_{j+1}(a_i)$ tienen signos contrarios, pues $f_{j-1}(a_i) \bullet f_{j+1}(a_i) < 0$, entonces $f_{j-1}(c)$ y $f_{j+1}(c)$ también los tienen. De manera análoga se deduce que $f_{j-1}(d)$ y $f_{j+1}(d)$ tienen signos contrarios. Así, se tiene que $\{f_{j-1}(c), f_j(c), f_{j+1}(c)\}$ aporta un cambio en el signo así como $\{f_{j-1}(d), f_j(d), f_{j+1}(d)\}$ con $j \in \{1, \ldots, n-1\}$. Por lo tanto, tomando en cuenta los dos casos se tiene que $V_c = V_d$.

Supongamos ahora que $f(a_i) = 0$. Por la propiedad $iv)$ de la sucesión de Sturm, existen intervalos (c', a_i) y (a_i, d') tales que $f_0(u) \bullet f_1(u) < 0$, y $f_0(v) \bullet f_1(v) > 0, \forall u \in (c', a_i), \forall v \in (a_i, d')$. Sin pérdida de generalidad, podemos suponer que $c \in (c', a_i)$ y $d \in (a_i, d')$. Así, tenemos que $f_0(c) \bullet f_1(c) < 0$, y $f_0(d) \bullet f_1(d) > 0$. Por lo tanto, la sucesión $\{f_0(c), f_1(c)\}$ tiene un cambio en el signo mientras que $\{f_0(d), f_1(d)\}$ no lo tiene. Ahora, notemos que si $j > 1$ entonces $\{f_{j-1}(c), f_j(c), f_{j+1}(c)\}$ y $\{f_{j-1}(d), f_j(d), f_{j+1}(d)\}$ aportan el mismo numero de variaciones en el signo por el argumento anterior. Por lo tanto $V_c - V_d = 1$ si $f(a_i) = 0$.

Sea $a_i' \in (a_{i-1}, a_i)$, con $1 < i \leq n$. Entonces se tiene lo siguiente:

$$V_a - V_b = (V_a - V_{a_1'}) + (V_{a_1'} - V_{a_2'}) + (V_{a_2'} - V_{a_3'}) + \cdots + (V_{a_{n-1}'} - V_{a_n'}) + (V_{a_n'} - V_b)$$

$$= (V_a - V_{a_1'}) + \sum_{i=1}^{n-1} (V_{a_i'} - V_{a_{i+1}'}) + (V_{a_n'} - V_b) = \sum_{i=1}^{n-1} (V_{a_i'} - V_{a_{i+1}'})$$

Esta última igualdad se da porque como

$$a_1' \in (a_0, a_1) = (a, a_1) y a_n' \in (a_{n-1}, a_n) = (a_{n-1}, b)$$

entonces $V_a = V_{a_1'}$ y $V_{a_n'} = V_b$. Notemos ahora que en cada paréntesis de la suma restante, para cada $i \in \{1, \ldots, n-1\}$, le corresponde un 0 o 1 dependiendo si $f(a_i) \neq 0$ o $f(a_i) = 0$, respectivamente. Por lo tanto, el número de unos equivale al número de a_i, con $1 \leq i \leq n$, tales que a_i es raíz de $f(x)$. Por lo tanto, $V_a - V_b$ es el número de raíces de $f(x)$ en el intervalo (a, b). ■

Ahora demostraremos la existencia de una sucesión de Sturm. Para esto, definimos la sucesión estandar para $f(x) \in R[x]$ como sigue:

$$f_0(x) = f(x), \ f_1(x) = f_0'(x), \text{ donde } f_0'(x) \text{ es la derivada de } f(x).$$

Dividiendo $f_0(x)$ entre $f_1(x)$ se tiene que

$$f_0(x) = q_1(x) f_1(x) - f_2(x), \text{ donde } \operatorname{grad} f_2(x) < \operatorname{grad} f_1(x).$$

Dividiendo ahora $f_1(x)$ entre $f_2(x)$ se tiene que

$$f_1(x) = q_2(x) f_2(x) - f_3(x), \text{ donde } \operatorname{grad} f_3(x) < \operatorname{grad} f_2(x).$$

Continuando de esta manera, llegamos a $\vdots$

$$f_{n-2}(x) = q_{n-1}(x)f_{n-1}(x) - f_n(x), \text{ con } \operatorname{grad} f_n(x) < \operatorname{grad} f_{n-1}(x),$$

y

$$f_{n-1}(x) = q_n(x)f_n(x).$$

Notemos que las $f_j(x)$ las obtenemos modificando el algoritmo de Euclides para encontrar el máximo común divisor entre $f(x)$ y $f'(x)$, de tal manera que el polinomio que se obtiene en cada paso, es el residuo negativo en el proceso de división. Para darnos una idea, tomemos la siguiente función:

$f(x) = x^3+x+1$. Entonces, siguiendo el procedimiento, tenemos que $f_1(x) = f'(x) = 3x^2 + 1$. Usando el algoritmo de Euclides para $f(x)$ y $f_1(x)$ se obtiene $f(x) = (\frac{1}{3}x) \bullet (3x^2+1)+(\frac{2}{3}x+1)$. Notemos que esto último lo podemos escribir como

$$f(x) = (\frac{1}{3}x) \bullet (3x^2 + 1) - (-(\frac{2}{3}x + 1)) = f(x) = (\frac{1}{3}x) \bullet (3x^2 + 1) - (-\frac{2}{3}x - 1),$$

de tal manera que $f_2(x) = -\frac{2}{3}x - 1$. Usando de nuevo el algoritmo, se tiene que

$$f_1(x) = (-\frac{9}{2}x + \frac{27}{4}) \bullet (-\frac{2}{3}x - 1) + (\frac{31}{4}) = (\frac{-9}{2}x + \frac{27}{4}) \bullet (-\frac{2}{3}x - 1) - (-\frac{31}{4}),$$

por lo que $f_3(x) = -\frac{31}{4}$. Así, la sucesión estandar para $f(x) = x^3 + x + 1$ es, $\{x^3 + x + 1, 3x^2 + 1, -\frac{2}{3}x - 1, -\frac{31}{4}\}$.

De lo anterior notemos que $f_n(x)$ es factor de cada $f_i(x)$ y así es un máximo común divisor entre $f(x)$ y $f'(x)$. Sea $g_i(x) = f_i(x) \bullet f_n(x)^{-1}$ y la sucesión $\{g_0(x), g_1(x), \ldots, g_{n-1}(x), g_n(x)\}$. Demostraremos que esta es una sucesión de Sturm para $g_0(x)$ para cualquier intervalo $[a, b]$ tal que $g_0(a), g_0(b) \neq 0$. Como $g_0(a) \neq 0$ y $g_0(b) \neq 0$ entonces la condición $ii)$ se cumple. Observemos que $g_n(x) = f_n(x) \bullet f_n(x)^{-1} = 1$ por lo que $i)$ también se cumple. Multiplicando la ecuación $f_{i-1}(x) = q_i(x)f_i(x) - f_{i+1}(x)$ por $f_n(x)^{-1}$, se obtiene los siguiente:

$$\begin{aligned} g_{i-1}(x) &= f_{i-1}(x) \bullet f_n(x)^{-1} = q_i(x) \bullet f_i(x) \bullet f_n(x)^{-1} - f_{i+1}(x) \bullet f_n(x)^{-1} \\ &= q_i(x) \bullet g_i(x) - g_{i+1}(x). \end{aligned}$$

Por lo tanto, $g_{i-1}(x) = q_i(x) \bullet g_i(x) - g_{i+1}(x)$.

Supongamos que $g_j(c) = 0$ para alguna $j \in \{1, \ldots, n-1\}$ y $c \in [a, b]$. De la igualdad anterior se tiene que

$$g_{j-1}(c) = q_j(c) \bullet 0 - g_{j+1}(c) = -g_{j+1}(c).$$

Por lo tanto, $g_{j-1}(c) = -g_{j+1}(c)$, es decir, $g_{j-1}(c) \bullet g_{j+1}(c) \leq 0$, donde la igualdad se da si y sólo si $g_{j-1}(c) = g_{j+1}(c) = 0$. Afirmamos que esta última desigualdad es estricta. Si $0 = g_{j-1}(c) = g_j(c) = g_{j+1}(c)$ entonces tendríamos que $g_j(c) = q_{j+1}(c) \bullet g_{j+1}(c) - g_{j+2}(c)$, lo cual se reduce a $0 = q_{j+1}(c) \bullet 0 - g_{j+2}(c) = -g_{j+2}(c)$, por lo que $g_{j+2}(c) = 0$. Prosiguiendo de esta manera,

llegamos a que $g_n(c) = 0$, lo cual es una contradicción. Por lo tanto, $g_{j-1}(c) \bullet g_{j+1}(c) < 0$, y de esta manera se tiene la propiedad *iii*).

Supongamos ahora que $g_0(c) = 0$, con $c \in (a, b)$. Por una parte, como

$$0 = g_0(c) = f(c) \bullet f_n(c)^{-1},$$

con $f(c)^{-1} \neq 0$, entonces $f(c) = 0$, por lo que $f(x) = (x-c)^e h(x)$, donde $e > 0$, $h(x)$ diferenciable, y $h(c) \neq 0$. De esta manera se tiene que $f'(x) = e(x-c)^{e-1}h(x) + (x-c)^e h'(x)$. Como $f_n(x)$ es un máximo común divisor de $f(x)$ y $f'(x)$, entonces $f_n(x) = (x-c)^{e-1}k(x)$, donde $k(c) \neq 0$, y $h(x) = k(x)l(x)$, $h'(x) = k(x)m(x)$ con $l(c) \neq 0$.

Tomando esto en cuenta, se tienen las siguientes relaciones:

$$\begin{aligned} g_0(x) &= f(x)f_n(x)^{-1} = [(x-c)^e h(x)][(x-c)^{e-1}k(x)]^{-1} \\ &= (x-c)\frac{h(x)}{k(x)} = (x-c)l(x), \end{aligned}$$

y

$$\begin{aligned} g_1(x) &= f'(x)f_n(x)^{-1} = [e(x-c)^{e-1}h(x) + (x-c)^e h'(x)][(x-c)^{e-1}k(x)]^{-1} \\ &= e\frac{h(x)}{k(x)} + (x-c)\frac{h'(x)}{k(x)} = el(x) + (x-c)m(x). \end{aligned}$$

Nótese que $g_1(c) = el(c) \neq 0$. Como $g_1(c), l(c) \neq 0$, entonces podemos dar un intervalo $[c_1, c_2]$ tal que $c \in [c_1, c_2]$, y que $g_1(x) \bullet l(x) \neq 0, \forall x \in [c_1, c_2]$. Por el Teorema del valor intermedio y del hecho que $g_1(c) = el(c) \neq 0$, (pues $e > 0$ y $l(c) \neq 0$) se tiene que $g_1(x) \bullet l(x) > 0, \forall x \in [c_1, c_2]$. Por lo tanto,

$$g_0(x)g_1(x) = [(x-c)l(x)]g_1(x) = (x-c)g_1(x)l(x).$$

Como $g_1(x)$ y $l(x)$ tienen el mismo signo en $[c_1, c_2]$, entonces el signo de $g_0(x)\, g_1(x)$ está determinado por el signo que $x - c$ en el intervalo $[c_1, c_2]$, es decir, para $c_1 \leq x < c$, $g_0(x) \bullet g_1(x) < 0$, y para $c < x \leq c_2$, $g_0(x) \bullet g_1(x) > 0$. Esto demuestra *iv*), y así $\{g_0, g_1, \ldots, g_n\}$ es una sucesión de Sturm para $g(x)$.

Notemos que si $f(x)$ no tiene raíces multiples, entonces el máximo común divisor entre $f(x)$ y $f'(x)$ es ± 1. De esta manera, $f_n(x) = \pm 1$ y así las sucesiones

$$\{f_0(x), f_1(x), \ldots, f_n(x)\} \text{ y } \{g_0(x), g_1(x), \ldots, g_n(x)\}$$

difieren únicamente por el signo, es decir, $f_n(x)$ es 1, las sucesiones son iguales y si $f_n(x) = -1$, las sucesiones tienen signos contrarios. En este caso, la misma sucesión estandar $\{f_i(x)\}_{i=0}^n$ es una sucesión de Sturm para $f(x)$. Por otro lado, si $f(x)$ tiene raíces multiples, la sucesión estandar asociada a $f(x)$ no sería una sucesión de Sturm para $f(x)$ en intervalos que contengan cualquier raíz multiple de $f(x)$. Aún así, podemos utilizar la sucesión estandar para determinar el número de raíces distintas de $f(x)$ en (a, b).

Teorema 63 *(Teorema de Sturm) Sea R un campo real cerrado y $f(x) \in R[x]$ con grado positivo. Sea $\{f_0(x) = f(x), f_1(x), \ldots, f_n(x)\}$ la sucesión estandar para $f(x)$. Supongamos que $[a, b]$ es un intervalo en el cual $f(a) \neq 0, f(b) \neq 0$. Entonces el número de raíces distintas de $f(x)$ en (a, b) es $V_a - V_b$, donde V_c denota el número de variaciones en el signo de la sucesión $\{f_0(c), f_1(c), \ldots, f_n(c)\}$.*

Demostración. Sea $g_i(x) = f_i(x) \bullet f_n(x)^{-1}$. Ahora, sin contar multiplicidades, como $g_0(x) = f_0(x) \bullet f_n(x)^{-1} = f(x) \bullet f_n(x)^{-1}$, los polinomios $g_0(x)$ y $f(x)$ tienen las mismas raíces en (a, b). Como $\{g_i(x)\}_{i=0}^n$ es una sucesión de Sturm para $g_0(x)$ entonces el número de raíces distintas de $g_0(x)$ en (a, b) es $V_{g(a)} - V_{g(b)}$ donde $V_{g(c)}$ denota el número de variaciones en el signo de la sucesión $\{g_0(c), g_1(c), \ldots, g_n(c)\}$.

Notemos ahora que $f_n(a) \neq 0$ y $f_n(b) \neq 0$. Esto se debe a que, como $f_n(x)$ es un máximo común divisor de $f(x)$ y $f'(x)$, entonces en particular $f_n(x) \mid f(x)$. Si $f_n(a) = 0$, entonces $x = a$ es una raíz de $f_n(x)$, por lo que $x - a \mid f_n(x)$. Como $x - a \mid f_n(x)$ y $f_n(x) \mid f(x)$ entonces $x - a \mid f(x)$, teniendo así que $x = a$ es una raíz de $f(x)$, es decir, $f(a) = 0$, lo cual es una contradicción. Este razonamiento es totalmente análogo para b. Por lo tanto, $f_n(a), f_n(b) \neq 0$.

Fijémonos ahora en

$$V_{g(a)} = \{\frac{f(a)}{f_n(a)}; \frac{f_1(a)}{f_n(n)}, \ldots, \frac{f_n(a)}{f_n(a)}\}$$

y

$$V_{f(a)} = \{f(a), f_1(a), \ldots, f_n(a)\}$$

Si $f_n(a) > 0$ entonces $f_i(a)$ y $\frac{f_i(a)}{f_n(a)}$ tendrán el mismo signo, por lo que $V_{g(a)} = V_{f(a)}$. Si $f_n(a) < 0$ entonces $f_i(a)$ y $\frac{f_i(a)}{f_n(a)}$ tendrán signos contrarios, manteniéndose sin embargo los cambios de signo en las sucesiones. Por lo tanto, en cualquier caso, $V_{g(a)} = V_{f(a)}$. De manera análoga, $V_{g(b)} = V_{f(b)}$, teniendo así que $V_{g(a)} - V_{g(b)} = V_{f(a)} - V_{f(b)}$. Por lo tanto, $V_{f(a)} - V_{f(b)}$ es el número de raíces distintas de $f(x)$ en (a, b). ■

Ejemplo 7 *Consideremos la función $f(x) = x^3 - 7x - 7$ y el intervalo $(-2, -1)$.*

Para empezar, notemos que

$$f(-2) = (-2)^3 - 7(-2) - 7 = -8 + 14 - 7 = -1 \neq 0$$

y

$$f(-1) = (-1)^3 - 7(-1) - 7 = -1 + 7 - 7 = -1 \neq 0$$

por lo que cumple la hipótesis del teorema de Sturm. Construyamos ahora la sucesión estandar para $f(x)$:

$$\begin{aligned} f_0(x) &= f(x) = x^3 - 7x - 7, \\ f_1(x) &= f'(x) = 3x^2 - 7. \end{aligned}$$

Dividiendo $f_0(x)$ entre $f_1(x)$ se tiene que

$$x^3 - 7x - 7 = (\frac{1}{3}x)(3x^2 - 7) - (\frac{14}{3}x - 7)$$

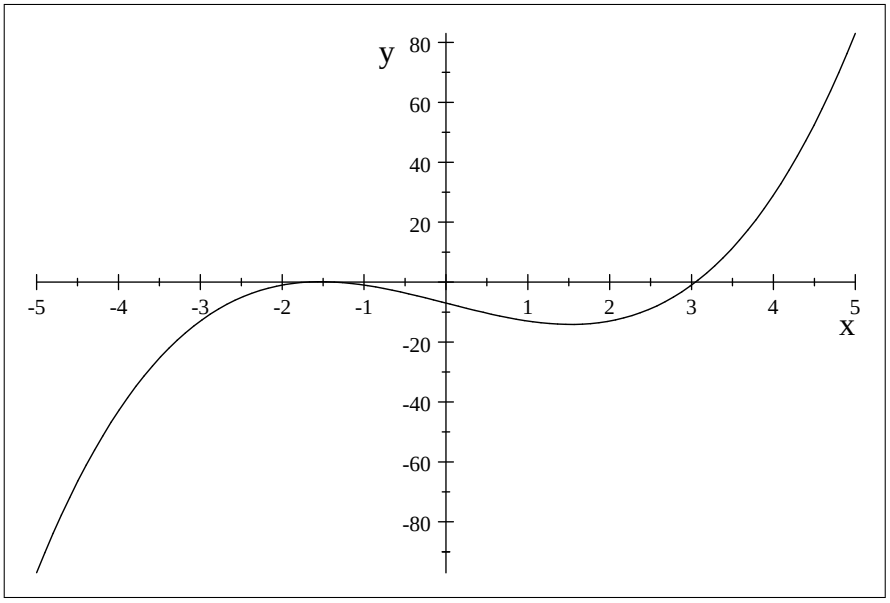
por lo que $f_2(x) = \frac{14}{3}x - 7$. Dividiendo de nuevo, ahora $f_1(x)$ entre $f_2(x)$ tenemos que

$$3x^2 - 7 = (\frac{9}{14}x - \frac{27}{28})(\frac{14}{3}x + 7) - (7),$$

obteniendo $f_3(x) = 7$. Por lo tanto, la sucesión estandar para $f(x)$ es

$$\{x^3 - 7x - 7, 3x^2 - 7, \frac{14}{3}x - 7, 7\}.$$

Ahora, V_{-2} se calcula viendo las variaciones en el signo de la sucesión $\{f_0(x), f_1(x), f_2(x), f_3(x)\}$ evaluada en $x = -2$, lo cual nos da la sucesión $\{-1, 5, -\frac{49}{3}, 7\}$, que tiene 3 variaciones en el signo, por lo que $V_{-2} = 3$. De la misma manera, $\{f_0(x), f_1(x), f_2(x), f_3(x)\}$ evaluada en $x = -1$ nos da $\{-1, -4, -\frac{35}{3}, 7\}$, la cual tiene una sóla variación en el signo, por lo que $V_{-1} = 1$. Por lo tanto, el número de raíces diferentes de $f(x)$ en el intervalo $(-2, -1)$ es $V_{-2} - V_{-1} = 3 - 1 = 2$. La gráfica de $f(x) = x^3 - 7x - 7$ se muestra a continuación.



Hemos visto anteriormente que las raíces de $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ en R se encuentran en el intervalo $[-M, M]$ donde $M = \text{máx}\{1, \sum_{i=0}^{n-1} |a_1|\}$. Sea $\mu = 1 + |a_0| + |a_2| + \cdots + |a_{n-1}|$. Notemos que $M < \mu$, por lo que las raíces de $f(x)$ en R también están en el intervalo abierto $(-\mu, \mu)$. Por lo tanto si $\{f_0(x), f_1(x), \ldots, f_k(x)\}$ es la sucesión estandar para $f(x)$, entonces el número de raíces de $f(x)$ en R es $V_{-\mu} - V_{\mu}$, donde de nuevo, V_c denota las variaciones en el signo de la sucesión $\{f_0(x), f_1(x), \ldots, f_k(x)\}$.

Ejemplo 8 *Ahora consideremos la función* $f(x) = x^4 + 12x^2 + 5x - 9$, *con* $f(x) \in \mathbb{R}$. *Primero saquemos la sucesión estandar para* $f(x)$. *Los primeros dos términos son*

$$f_0(x) = f(x) \text{ y } f_1(x) = f'(x) = 4x^3 + 24x + 5.$$

Dividiendo $f_0(x)$ *entre* $f_1(x)$ *se obtiene*

$$f_0(x) = (\frac{1}{4}x)f_1(x) - (-6x^2 - \frac{15}{4}x + 9),$$

por lo que $f_2(x) = -6x^2 - \frac{15}{4}x + 9$. *Dividiendo ahora* $f_1(x)$ *entre* $f_2(x)$ *tenemos que*

$$f_1(x) = (-\frac{2}{3}x + \frac{5}{12})f_2(x) - (-\frac{505}{16}x - \frac{5}{4}),$$

obteniendo así a $f_3(x) = -\frac{505}{16}x - \frac{5}{4}$. *Siguiendo con este proceso se tiene que*

$$f_2(x) = (\frac{96}{505}x + \frac{4 \bullet 1419}{5 \bullet (101)^2})f_3(x) - (-\frac{93,228}{(101)^2}).$$

Por lo tanto, la sucesión estandar para $f(x)$ *es*

$$\{x^4 + 12x^2 + 5x - 9, 4x^3 + 24x + 5, -6x^2 - \frac{15}{4}x + 9, -\frac{505}{16}x - \frac{5}{4}, -\frac{93,228}{(101)^2}\}.$$

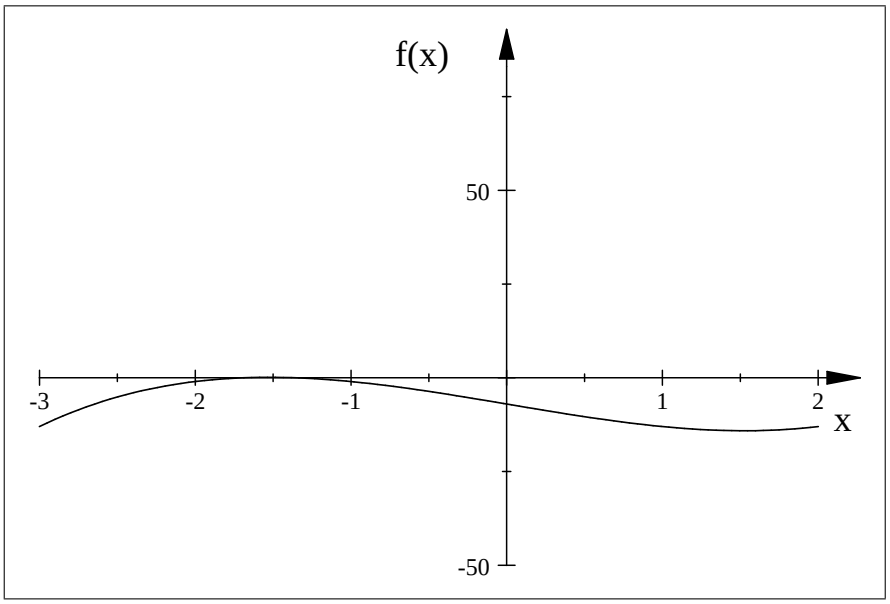
Ahora, para ver cuántas raíces reales tiene $f(x)$ *tomemos* $\mu = 1 + |12| + |5| + |-9| = 27$. *Por lo anterior, tenemos que el numero de raíces de* $f(x)$ *en* $\mathbb{R}$ *es* $V_{-\mu} - V_{\mu}$. *Para calcular* $V_{-\mu}$ *se toma la sucesión estandar y se evalúa en* $x = -\mu$ *lo cual nos da la sucesión de números reales*

$$\{540045, -79375, -4263{,}75, \frac{13615}{16}, -\frac{93,228}{(101)^2}\},$$

que tiene tres cambios de signo. De la misma manera, la sucesión para V_{μ} *es*

$$\{540315, 79385, -4466{,}25, \frac{-13655}{16}, -\frac{93,228}{(101)^2}\}$$

la cual tiene sólo un cambio de signo. Por lo tanto, $V_{-\mu} - V_{\mu} = 3 - 1 = 2$. *A continuación se ilustra la gráfica de* $y = x^4 + 12x^2 + 5x - 9$:



0.27. Bibliografía

· Jacobson, N., *Basic Algebra I*, Segunda Edición, Nueva York, EUA., Dover, 2009.

· Stewart, I., *Galois Theory*, Tercera Edición, Coventry, Reino Unido, Chapman & Hall/CRC, 2004.

· Rotman, J., *An Introduction to the Theory of Groups*, Cuarta Edición, Urbana Illinois, EUA., Springer-Verlag, 1995.

· Sharpe, D., *Rings and Factorization*, Primera Edición, Nueva York, EUA., Cambridge University Press, 1987.

· Grillet, Pierre A., *Abstract Algebra*, Segunda Edición, Nueva York, EUA., Springer Verlag, 2007.