Universidad Nacional Federico Villarreal

Vicerrectorado de INVESTIGACIÓN

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

"EXTENSIÓN DEL CUERPO K EN L, EN GRUPOS DE GALOIS A PARTIR DE UN GRUPO FINITO"

Tesis para optar el Título Profesional de

Licenciado en Matemática

AUTOR

Ramírez Palomino, Samuel Jacob

ASESOR

Lic. Velasquez Alarcón, Jorge

JURADO

Dr. Anaya Calderón, Agustín E.

Lic. Díaz Mauricio, Hugo U.

Mg. Contreras Tito, Vladimiro

Mg. Quicaño Barrientos, Carlos G.

Lima – Perú

2018

En primer lugar a Dios por darme las fuerzas suficientes para seguir adelante en los momentos de adversidades.

A mis padres Víctor Ramírez y Maximiliana Palomino por darme su gran amor y apoyo en todo momento en este trabajo de tesis.

AGRADECIMIENTOS

En primer lugar a Dios por haberme permitido concluir mis estudios de pregrado y mi investigación.

A mis padres y hermanos por su dedicación, esfuerzo y apoyo que siempre me han dado.

A todos mis profesores de Matemática en la UNFV por todas las cosas aprendidas a lo largo de la formación, de quienes tuve el placer de adquirir muchos de los conocimientos iniciales que ahora poseo, en especial a los profesores Mg. Carlos Quicaño Barrientos y Mg. Vladimiro Contreras Tito.

A mi asesor Lic. Jorge Velasquez Alarcón por el apoyo, la paciencia y el impulso que me dio para la ejecución del presente trabajo de tesis.

A mis amigos por sus apoyos y sus palabras de motivación en todo momento, en especial a la Bach. Rosmery Pineda Remón.

TABLA DE CONTENIDOS

RESUMEN

La presente investigación tuvo como objetivo general probar la existencia de la extensión del cuerpo L/K tal que G es el grupo de Galois de L/K con G finito.

El estudio fue de tipo Investigación Básica, pues se recopiló toda la información necesaria de los libros y papers, luego se separó en 3 capítulos para así avanzar de forma ordenada hasta concluirlo, finalmente por medio del programa Word se tipeó este trabajo de investigación.

Los resultados fueron que dado una extensión de Galois, se le puede asociar un grupo finito: grupo de Galois de dicha extensión y que el "Teorema Fundamental de las Funciones Racionales Simétricas", el "Teorema de Cayley" y el "Teorema Fundamental de Galois" son importantes para la demostración del teorema principal. La conclusión a la que se llegó fue que sí es posible probar la existencia de la extensión del cuerpo L/K tal que G es el grupo de Galois de L/K con G finito, por medio de un cuerpo cualquiera F se tomó

$L = F(x_1, x_2, \ldots, x_n)$ el cuerpo de las funciones racionales de $x_1, x_2, \ldots, x_n$ y $K = L_G$ el cuerpo fijo de G.

Palabras Clave: Polinomio, extensión del cuerpo, algebraico, cuerpo de descomposición, separable, cuerpo fijo, extensión normal, extensión de Galois, grupo de Galois.

ABSTRACT

The present investigation had as general objective to prove the existence of the extension of the field L/K such that G is the Galois group of L/K with finite G.

The study was of the Basic Investigation type, since all the necessary information of the books and papers was collected, then separated in 3 chapters to advance in an orderly way until finishing it, finally through the program Word this investigation work was typed. The results were that given an extension of Galois, you can associate a finite group: Galois group of said extension and that the “Fundamental Theorem of Symmetric Rational Functions”, “Cayley's Theorem” and “Fundamental Theorem of Galois” are important for the proof of the main theorem. The conclusion reached was that yes it is possible to prove the existence of the extension of the field L/K such that G is the Galois group of L/K with finite G, by means of a field anyone F it was take $L = F(x_1, x_2, \ldots, x_n)$ the field of the rational functions of $x_1, x_2, \ldots, x_n$ and $K = L_G$ the fixed field of G.

Keywords: Polynomial, field extension, algebraic, decomposition field, separable, fixed field, normal extension, Galois extension, Galois group.

INTRODUCCIÓN

La teoría de Galois toma su nombre de “Evariste Galois” (1811-1832) quien fue un matemático francés que se dedicó a la resolución de ecuaciones de polinomios de quinto o mayor grado en términos de los coeficientes del polinomio, con la utilización de operaciones algebraicas o la extracción de raíces. Debido a que no se pudo encontrar resolución por medio de radicales para estos polinomios, Galois introduce el concepto de Grupo, el cual se centra en el grupo de permutaciones de las raíces del polinomio, es así que, la teoría de Galois es una colección de resultados que conectan la teoría de grupos con la teoría de cuerpos.

Como es usual en la teoría de Galois, a cada extensión de Galois, se le puede asociar un grupo finito: grupo de Galois de dicha extensión, esto nos lleva a preguntarnos: ¿Es posible probar la existencia de la extensión del cuerpo L/K tal que G es el grupo de Galois de L/K con G finito? Entonces tendremos como objetivo general: probar la existencia de la extensión del cuerpo L/K tal que G es el grupo de Galois de L/K con G finito, y como objetivos específicos: desarrollar la teoría de Galois para entender los resultados obtenidos. Explicar la importancia de los polinomios y sus raíces en los grupos de Galois. Explicar la importancia del grupo S_n en la teoría de Galois y probar que dado una extensión de Galois, se le puede asociar un grupo finito: grupo de Galois de dicha extensión.

En la presente tesis desarrollaremos nuestros objetivos las cuales serán de la siguiente manera:

En el primer capítulo veremos el marco teórico en la cual se va a subdividir en antecedentes y generalidades siendo las herramientas base para este trabajo de tesis.

En el segundo capítulo veremos los materiales y métodos para este trabajo de tesis.

En el tercer capítulo veremos los resultados, nos dedicaremos en la demostración del teorema principal de este trabajo de tesis.

Finalmente, mencionaremos la discusión, las conclusiones, las referencias y los anexos de este trabajo de tesis.

CAPÍTULO 1

MARCO TEÓRICO

En este capítulo mencionaremos algunos aportes por tesistas que desarrollaron su trabajo de investigación en relación a este trabajo de tesis, además mencionaremos algunas definiciones, ejemplos, teoremas, proposiciones, corolarios y lemas ya estudiadas, las cuales utilizaremos a lo largo de esta tesis.

1.1. Antecedentes

Hernández, (2010), en su Tesina para optar el Grado Académico de Licenciado en Matemática, titulado: *"Extensiones de Galois".* Llegó a las siguientes conclusiones:

1. Al estudiar un polinomio con coeficientes en un campo K, en donde no todas sus raíces estén dentro del campo K , siempre podemos construir una extensión de ese campo que contenga a la ó las raíces del polinomio y, así formar un nuevo campo, un campo de extensión de K.
2. Dado un campo K , siempre podemos construir una extensión algebraica que contenga las raíces de todo polinomio en $K[x]$.
3. Evariste Galois estudió en particular extensiones L/K que cumplen ciertas características:

   Que son separables, es decir, extensiones en donde cada polinomio irreducible en $K[x]$ sus raíces son simples

   Que son Normales, es decir, que contenga a todas las raíces de cualquier polinomio en $K[x]$.

Riquelme, (2007), en su Tesis para optar el Grado Académico de Licenciado en Educación Matemática, titulado: *"Teoria de Galois y ecuaciones algebraicas".* Llegó a las siguientes conclusiones:

Al tratar de conocer la respuesta a la pregunta ¿Existen fórmulas para resolver ecuaciones de grado mayor o igual que cinco?, nos encontramos con diferentes maneras de pensar que se utilizaron para resolver las ecuaciones polinomiales, las cuales tienen un gran valor a la hora de observar como de acuerdo a lo conocido en su época los matemáticos intentaron abordar el tema, puesto que intentando dar con la solución del problema se encontraron con obstáculos impensados que los llevaron a cuestionar la existencia de la solución del problema y finalmente probar la imposibilidad de obtener el resultado buscado.

Además de aprender acerca de las distintas maneras de pensar nos encontramos con potentes teorías desarrolladas para resolver el problema, como la de Galois que no solo nos permite dar con la respuesta a la pregunta planteada, sino que también nos entrega herramientas para saber como abordar otros problemas importantes como el teorema fundamental del álgebra trasladando problemas acerca de cuerpos y extensiones a otros de grupos finitos, ampliando la visión y la madurez matemática.

Por último es importante mencionar que aunque algunas de las herramientas aprendidas nos permiten dar soluciones generales resultando de un gran interés teórico, estas tienen algunos inconvenientes prácticos, por ejemplo calcular el grupo de Galois de una ecuación particular para saber si esta es soluble por radicales.

1.2. Generalidades

1.2.1. Teoría de Grupos

Definición 1.2.1.1.

Herstein (1970) mencionó:

> Un conjunto no vacío de elementos G se dice que forma un grupo si en G está definida una operación binaria, llamada producto y denotada por $(\cdot)$ tal que:
>
> 1. $a,b \in G$ implica que $a \cdot b \in G$ (cierre).
> 2. $a,b,c \in G$ implica que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ley asociativa).
> 3. Existe un elemento $e \in G$ tal que $a \cdot e = e \cdot a = a$ para todo $a \in G$ (existencia de un elemento identidad en G).
> 4. Para todo $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$ (existencia de inversos en G). (p. 39)

Ejemplo 1.2.1.2. Defínase la operación binaria $*$ en $\mathbb{Q}^+$ por:

$$a * b = \frac{a \cdot b}{2}$$

Entonces: $(\mathbb{Q}^+, *)$ es un grupo.

Demostración: Sean $a,b,c \in \mathbb{Q}^+$, entonces:

1. $a * b = \frac{a \cdot b}{2} \in \mathbb{Q}^+$
2. $(a * b) * c = \frac{a \cdot b}{2} * c = \frac{a \cdot b \cdot c}{4}$

Por otro lado:

$$a*(b*c)=a*\frac{b\cdot c}{2}=\frac{a\cdot b\cdot c}{4}$$

Por lo tanto:

$$(a*b)*c=a*(b*c)$$

3. Se puede ver: $a*2=\frac{a\cdot 2}{2}=a$

   Además: $2*a=\frac{2\cdot a}{2}=a$

   Entonces:

$$\exists\ e=2\in\mathbb{Q}^{+}\ /\ a*2=a=2*a$$

   Unicidad:

   Supongamos que existe $f\in\mathbb{Q}^{+}\ \wedge\ f\neq e\ /\ a*f=a=f*a$

   Por otro lado: $a*e=a=e*a$

   Luego:

$$a*f=a*e$$

$$\frac{a\cdot f}{2}=\frac{a\cdot e}{2}$$

$$f=e\ (\Rightarrow\Leftarrow)$$

4. Se puede ver: $a*\frac{4}{a}=\frac{a\cdot\frac{4}{a}}{2}=\frac{4}{2}=2$

Además: $\frac{4}{a} * a = \frac{\frac{4}{a} \cdot a}{2} = \frac{4}{2} = 2$

Entonces:

$$\exists\ b = \frac{4}{a} \in \mathbb{Q}^+ \ / \ a * \frac{4}{a} = 2 = \frac{4}{a} * a$$

Unicidad:

Supongamos que existe $c \in \mathbb{Q}^+ \ \wedge \ c \neq b \ / \ a * c = e = c * a$

Por otro lado: $a * b = e = b * a$

Luego:

$$a * c = a * b$$

$$\frac{a \cdot c}{2} = \frac{a \cdot b}{2}$$

$$c = b \ \ (\Rightarrow\Leftarrow)$$

Finalmente, concluimos que:

$(\mathbb{Q}^+, *)$ es un grupo □

Definición 1.2.1.3.

Herstein (1970) mencionó: "Un subconjunto H de un grupo G se dice que es subgrupo de G si respecto al producto en G, H mismo forma un grupo" (p. 45).

Lema 1.2.1.4.

Herstein (1970) mencionó: "Un subconjunto no vacío H del grupo G es un subgrupo de G si y sólo si

1) $a, b \in H$ implica que $ab \in H$;

2) $a \in H$ implica que $a^{-1} \in H$ " (p. 46).

Demostración. (Ver demostración en [9], p. 46) □

Ejemplo 1.2.1.5. Sea $(\mathbb{Z}, +)$ un grupo. Dado $n \in \mathbb{Z}, n \geq 0$ se define el conjunto:

$$n\mathbb{Z} = \{nz / z \in \mathbb{Z}\}$$

Entonces: $(n\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Z}, +)$.

Demostración. Veamos:

Tenemos: $n\mathbb{Z} \subset \mathbb{Z}$

Sean $a, b \in n\mathbb{Z}$, entonces:

$$\exists\ r \in \mathbb{Z}\ /\ a = nr\ \ \wedge\ \exists\ t \in \mathbb{Z}\ /\ b = nt$$

Luego:

$$a - b = nr - nt = n(r - t) \in n\mathbb{Z}$$

Por el lema 1.2.1.4. se obtiene:

$(n\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Z}, +)$ □

Definición 1.2.1.6.

Fraleigh (1987) mencionó: "Si G es un grupo finito, entonces el orden $|G|$ de G es el número de elementos en G. En general, para cualquier conjunto finito S, $|S|$ es el número de elementos en S" (p. 30).

Herstein (1970) mencionó:

> Otra característica natural de un grupo G es el número de elementos de que consta. Llamamos a este orden de G y lo denotamos por $\circ(G)$.

Este número es, desde luego, más interesante cuando es finito. En tal caso decimos que G es un grupo finito. (p. 40)

Ejemplo 1.2.1.7. Sea el grupo $G=\{1,-1,i,-i\}$ con la operación multiplicación de los complejos, se tiene que $|G|=4$.

Definición 1.2.1.8.

Fraleigh (1987) mencionó: "Si A es el conjunto finito $\{1,2,\ldots,n\}$, entonces el grupo de todas las permutaciones de A es el grupo simétrico de n letras y se denota por S_n" (p. 42).

Notación:

Para los elementos de S_n se usará la notación usual de aplicaciones, o bien, dado $\sigma \in S_n$ con $\sigma(1)=a_1,\ \sigma(2)=a_2,\ \ldots,\ \sigma(n)=a_n$, se escribirá:

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix} \tag{1.1}$$

Se entenderá que σ hace corresponder a cada uno de los números que están en la primera fila el que está debajo.

Ejemplo 1.2.1.9. $(S_3,\circ)$ es un grupo con el operador composición "$\circ$".

Demostración. Sea el conjunto $A=\{1,2,3\}$, veamos las permutaciones de A denotando con una letra griega:

$$\rho_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \tag{1.2}$$

$$\rho_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} \tag{1.3}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \tag{1.4}$$

$$\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \tag{1.5}$$

$$\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \tag{1.6}$$

$$\rho_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{1.7}$$

Ahora, veamos quien es: $\rho_1 \circ \rho_1$

$$(\rho_1 \circ \rho_1)(1) = \rho_1(\rho_1(1)) = \rho_1(1) = 1$$

$$(\rho_1 \circ \rho_1)(2) = \rho_1(\rho_1(2)) = \rho_1(2) = 2$$

$$(\rho_1 \circ \rho_1)(3) = \rho_1(\rho_1(3)) = \rho_1(3) = 3$$

Por lo tanto:

$$\rho_1 \circ \rho_1 = \rho_1$$

De esta manera, obtendremos la siguiente tabla:

Tabla 1

Operación de la composición

$\circ$	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
ρ_1	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
ρ_2	ρ_2	ρ_3	ρ_1	ρ_5	ρ_6	ρ_4
ρ_3	ρ_3	ρ_1	ρ_2	ρ_6	ρ_4	ρ_5
ρ_4	ρ_4	ρ_6	ρ_5	ρ_1	ρ_3	ρ_2
ρ_5	ρ_5	ρ_4	ρ_6	ρ_2	ρ_1	ρ_3
ρ_6	ρ_6	ρ_5	ρ_4	ρ_3	ρ_2	ρ_1

En base a esta tabla, se puede ver: la cerradura, la asociatividad, $id = \rho_1$ y además:

Para ρ_1 su inversa única es ρ_1 / $\rho_1 \circ \rho_1 = id$

Para ρ_2 su inversa única es ρ_3 / $\rho_2 \circ \rho_3 = id$

Para ρ_3 su inversa única es ρ_2 / $\rho_3 \circ \rho_2 = id$

Para ρ_4 su inversa única es ρ_4 / $\rho_4 \circ \rho_4 = id$

Para ρ_5 su inversa única es ρ_5 / $\rho_5 \circ \rho_5 = id$

Para ρ_6 su inversa única es ρ_6 / $\rho_6 \circ \rho_6 = id$

Por lo tanto:

$(S_3, \circ)$ es un grupo □

Definición 1.2.1.10.

Herstein (1970) mencionó: "Una aplicación ϕ de un grupo G en un grupo $\overline{G}$ se dice que es un homomorfismo si para $a, b \in G$ cualesquiera siempre se tiene $\phi(ab) = \phi(a)\phi(b)$" (p. 61).

Ejemplo 1.2.1.11. Sean $(\mathbb{R}, +)$ y $(\mathbb{R}, \cdot)$ grupos.

Sea la función exponencial:

$$f : (\mathbb{R}, +) \to (\mathbb{R}, \cdot) \ / \ f(x) = e^x$$

Entonces f es un homomorfismo de grupos.

Demostración. Veamos:

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y); \ \forall \ x, y \in \mathbb{R}$$

Por lo tanto:

f es un homomorfismo de grupos □

Definición 1.2.1.12.

Herstein (1970) mencionó: "Por automorfismo de un grupo G entenderemos un isomorfismo de G sobre sí mismo" (p. 72).

Lema 1.2.1.13.

Herstein (1970) mencionó: "Si G es un grupo, entonces $A(G)$, el conjunto de los automorfismos de G, es un grupo" (p. 73).

Demostración. (Ver demostración en [9], pp. 72-73) □

Ejemplo 1.2.1.14. Sea $G=(\mathbb{Z},+)$ el grupo de los enteros, entonces $(Aut(G),\circ)$ es un grupo.

Demostración. Sea $G=(\mathbb{Z},+)$ el grupo conmutativo de los enteros, los automorfismos son homomorfismos biyectivas, definidas así

$$f_{1,2}:\mathbb{Z}\to\mathbb{Z}/\ f_1(x)=x\ \wedge\ f_2(x)=-x$$

Entonces:

$Aut(G)=\{f_1,f_2\}$ es el conjunto de automorfismos de G

Se puede ver que $(Aut(G),\circ)$ cumple con las 4 condiciones de grupo.

Por lo tanto:

$(Aut(G),\circ)$ es un grupo □

Teorema 1.2.1.15. (Cayley).

Fraleigh (1987) mencionó: "Todo grupo es isomorfo a un grupo de permutaciones" (p. 72).

Demostración. Sea G un grupo.

Piénsese G como un conjunto y sea S_G el grupo simétrico de G.

Definamos:

$G'=\{\rho_a\in S_G\ /\ a\in G\wedge a\neq 0\}$, donde: ρ_a es una permutación de G en G

Afirmación 1: $G'\neq\varnothing$

En efecto: Sea $a\in G\ \wedge\ a\neq 0$.

Definamos:

$$\rho_a : G \to G \,/\, \rho_a(x) = a \cdot x$$

Veamos que ρ_a es inyectiva.

Sean $x, y \in G \,/\, \rho_a(x) = \rho_a(y)$, entonces:

$$a \cdot x = a \cdot y \tag{1.8}$$

Como $a \in G \;\wedge\; a \neq 0 \;\Rightarrow\; \exists!\; a^{-1} \in G \,/\, a \cdot a^{-1} = e = a^{-1} \cdot a$

Entonces en (1.8), se tiene:

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

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

$$e \cdot x = e \cdot y$$

$$x = y$$

Por lo tanto:

ρ_a es inyectiva

Veamos que ρ_a es sobreyectiva.

Sea $y \in G$, entonces:

$$y = (a \cdot a^{-1}) \cdot y = a \cdot (a^{-1} \cdot y) = \rho_a(a^{-1} \cdot y)$$

Luego:

$$\forall y \in G, \; \exists \;\; x = a^{-1} \cdot y \in G \,/\, y = \rho_a(x)$$

Por lo tanto:

ρ_a es sobreyectiva

Así, obtenemos:

$$\rho_a \quad \text{es biyectiva} \Rightarrow \rho_a \text{ es una permutación de } \quad G \text{ en } \quad G$$

Entonces:

$$\rho_a \in S_G$$

Se concluye:

$$G' \neq \varnothing$$

Afirmación 2: G' es subgrupo de S_G

En efecto:

Parte 1: Veamos que G' es cerrado bajo la composición.

Sean $\rho_a, \rho_b \in G' \Rightarrow \rho_a, \rho_b \in S_G \ / \ a \neq 0 \in G \ \wedge \ b \neq 0 \in G$

Sea $x \in G$, entonces:

$$(\rho_a \circ \rho_b)(x) = \rho_a(\rho_b(x)) = \rho_a(b \cdot x) = a \cdot (b \cdot x) = (a \cdot b) \cdot x = \rho_{ab}(x) \in G$$

Además, la composición de biyecciones es una biyección, entonces:

$$\rho_a \circ \rho_b = \rho_{ab} \in S_G \quad \text{con} \quad ab \in G \ \wedge \ ab \neq 0$$

Luego:

$$\rho_a \circ \rho_b \in G'$$

Por lo tanto:

G' es cerrado bajo la composición

Parte 2: Veamos que G' es asociativa.

Sean $\rho_a, \rho_b, \rho_c \in G' \ \wedge \ x \in G$, entonces:

$$[(\rho_a \circ \rho_b) \circ \rho_c](x) = [\rho_a \circ \rho_b](\rho_c(x)) = [\rho_a \circ \rho_b](c.x) = \rho_a(\rho_b(c.x))$$

$$[(\rho_a \circ \rho_b) \circ \rho_c](x) = \rho_a(b \cdot (c \cdot x)) = a \cdot [b \cdot (c \cdot x)] \qquad (1.9)$$

Por otro lado:

$$[\rho_a \circ (\rho_b \circ \rho_c)](x) = \rho_a((\rho_b \circ \rho_c)(x)) = \rho_a(\rho_b(\rho_c(x))) = \rho_a(\rho_b(c \cdot x))$$

$$[\rho_a \circ (\rho_b \circ \rho_c)](x) = \rho_a(b \cdot (c \cdot x)) = a \cdot [b \cdot (c \cdot x)] \qquad (1.10)$$

Por lo tanto, de (1.9) y (1.10) se concluye:

$$(\rho_a \circ \rho_b) \circ \rho_c = \rho_a \circ (\rho_b \circ \rho_c)$$

Es decir:

G' es asociativa

Parte 3: Sea $\rho_a \in G'$ P.D $\exists! \ \rho_e \in G' \ / \ \rho_a \circ \rho_e = \rho_a = \rho_e \circ \rho_a$

Sea $\rho_a \in G' \ \Rightarrow \ \rho_a \in S_G \ / \ a \in G \ \wedge \ a \neq 0$

Como $a \in G \ \Rightarrow \ \exists! \ e \in G \ / \ a \cdot e = a = e \cdot a$

Sea $x \in G$, entonces:

$$\rho_e(x) = e \cdot x = x$$

Además, ρ_e es biyectivo $\Rightarrow \ \rho_e \in S_G$ (permutación identidad de S_G)

Por lo tanto:

$$\exists! \ \rho_e \in G' \ / \ \rho_a \circ \rho_e = \rho_a = \rho_e \circ \rho_a$$

Parte 4: Sea $\rho_a \in G'$ P.D $\exists!\ \rho_{a^{-1}} \in G' \ / \ \rho_a \circ \rho_{a^{-1}} = \rho_e = \rho_{a^{-1}} \circ \rho_a$

Sea $\rho_a \in G' \Rightarrow \rho_a \in S_G \ / \ a \in G \ \wedge \ a \neq 0$

Como $a \in G \ \wedge \ a \neq 0 \Rightarrow \exists!\ a^{-1} \in G \ / \ a \cdot a^{-1} = e = a^{-1} \cdot a$

De la afirmación 2 (Parte 1), se tiene:

$$\rho_a \circ \rho_b = \rho_{ab},\ \forall a,b \in G \ \text{ con } \ a \neq 0,\ b \neq 0$$

Entonces:

$$\rho_a \circ \rho_{a^{-1}} = \rho_{a \cdot a^{-1}}$$

$$\rho_a \circ \rho_{a^{-1}} = \rho_e$$

Luego:

$$(\rho_a)^{-1} = \rho_{a^{-1}}$$

Además:

$$\rho_a \in S_G \ \Rightarrow \ \rho_a \ \text{ es biyectivo } \Rightarrow \ \rho_{a^{-1}} \ \text{ es biyectivo } \Rightarrow \ \rho_{a^{-1}} \in S_G \ \text{con} \quad a^{-1} \in G$$

Por lo tanto:

$$\exists!\ \rho_{a^{-1}} \in G' \ / \ \rho_a \circ \rho_{a^{-1}} = \rho_e = \rho_{a^{-1}} \circ \rho_a$$

Finalmente, de las 4 partes demostradas, se obtiene:

$$G' \ \text{ es subgrupo de } \ S_G$$

Afirmación 3: G es isomorfo al grupo G'

En efecto: Sea $a \in G$

Definamos:

$$\phi: G \to G' \,/\, \phi(a) = \rho_a$$

Veamos que ϕ es un isomorfismo.

Parte 1: ϕ es homomorfismo de grupos.

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

$$\phi(a \cdot b) = \rho_{ab} = \rho_a \circ \rho_b \text{ (De afirmación 2 (parte 1))}$$

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

Por lo tanto:

ϕ es homomorfismo de grupos

Parte 2: ϕ es inyectiva.

Sean $a, b \in G \,/\, \phi(a) = \phi(b) \;\Rightarrow\; \rho_a = \rho_b$.

Sea $x \in G \;\wedge\; x \neq 0$, entonces:

$$\rho_a(x) = \rho_b(x)$$

$$a \cdot x = b \cdot x$$

Sea $x \in G \;\wedge\; x \neq 0 \;\Rightarrow\; \exists!\; x^{-1} \in G \,/\, x \cdot x^{-1} = e = x^{-1} \cdot x$

Entonces:

$$(a \cdot x) \cdot x^{-1} = (b \cdot x) \cdot x^{-1} \;\Rightarrow\; a \cdot (x \cdot x^{-1}) = b \cdot (x \cdot x^{-1}) \;\Rightarrow\; a \cdot e = b \cdot e \;\Rightarrow\; a = b$$

Por lo tanto:

ϕ es inyectiva

Parte 3: ϕ es sobreyectiva.

Sea $z \in G' \Rightarrow z = \rho_a \in S_G \,/\, a \in G \wedge a \neq 0$

Entonces:

$$z = \phi(a)\,,\ a \in G \wedge a \neq 0$$

Luego:

$$\forall\ z \in G'\,,\ \exists\ a \neq 0 \in G \,/\, z = \phi(a)$$

Por lo tanto:

$$\phi \text{ es sobreyectiva}$$

Así, de las partes 1, 2 y 3 se obtiene:

$$\phi \text{ es isomorfismo}$$

Finalmente:

$$G \text{ es isomorfo al grupo } G'$$ □

Observación 1.2.1.16. Si el grupo G es finito con $\circ(G) = n$, entonces G es isomorfo a un subgrupo del grupo S_n.

Ejemplo 1.2.1.17. El grupo 4-Klein es isomorfo al subgrupo $\{id, (12)(34), (13)(24), (14)(23)\}$ de S_4.

Demostración. Sea $(G, \cdot)$ el grupo 4-Klein definido de esta forma:

$$G = \{1, a, b, ab\}\,,\ a^2 = 1 \wedge b^2 = 1 \wedge ab = ba$$

Denotaremos:

$$1 \to 1$$

$$a \to 2$$

$$b \to 3$$

$$ab \to 4$$

Usando la permutación ρ_1 inducido por la acción de la multiplicación a la izquierda se tiene:

$$1 \cdot 1 = 1 \Rightarrow \rho_1(1) = 1 \Rightarrow \rho_1(1) = 1$$

$$1 \cdot a = a = 2 \Rightarrow \rho_1(a) = 2 \Rightarrow \rho_1(2) = 2$$

$$1 \cdot b = b = 3 \Rightarrow \rho_1(b) = 3 \Rightarrow \rho_1(3) = 3$$

$$1 \cdot (ab) = ab = 4 \Rightarrow \rho_1(ab) = 4 \Rightarrow \rho_1(4) = 4$$

Obteniendo así:

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \tag{1.11}$$

Ahora construyamos el ρ_a de forma análoga a la anterior:

$$a \cdot 1 = a \Rightarrow \rho_a(1) = a \Rightarrow \rho_a(1) = 2$$

$$a \cdot a = a^2 = 1 \Rightarrow \rho_a(a) = 1 \Rightarrow \rho_a(2) = 1$$

$$a \cdot b = 4 \Rightarrow \rho_a(b) = 4 \Rightarrow \rho_a(3) = 4$$

$$a \cdot (ab) = a^2 b = b \Rightarrow \rho_a(ab) = 3 \Rightarrow \rho_a(4) = 3$$

Obteniendo así:

$$\rho_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \tag{1.12}$$

De forma análoga obtenemos:

$$\rho_b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \tag{1.13}$$

$$\rho_{ab} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \tag{1.14}$$

De esta forma conseguimos:

$$G' = \{\rho_1, \rho_a, \rho_b, \rho_{ab}\} \text{ es subgrupo de } (S_4, \circ)$$

Es decir:

$$G' = \{id, (12)(34), (13)(24), (14)(23)\} \text{ es subgrupo de } (S_4, \circ)$$

Ahora, definamos:

$$\phi : G \to G' \,/\, \phi(z) = \rho_z$$

Veamos que ϕ es un isomorfismo.

Parte 1: ϕ es un homomorfismo de grupos.

Sean $u, v \in G \ \wedge \ w \in G$, entonces:

$$[\phi(u \cdot v)](w) = \rho_{u \cdot v}(w) = (u \cdot v) \cdot w = u \cdot (v \cdot w) = u \cdot \rho_v(w) = \rho_u(\rho_v(w))$$

$$[\phi(u \cdot v)](w) = \phi(u)(\phi(v)(w)) = [\phi(u) \circ \phi(v)](w)$$

$$\phi(u \cdot v) = \phi(u) \circ \phi(v)$$

Por lo tanto:

ϕ es un homomorfismo de grupos

Parte 2: ϕ es biyectiva.

La prueba es análoga a la prueba de la Afirmación 3 que se hizo en el Teorema de Cayley.

Por lo tanto:

ϕ es un isomorfismo

Finalmente:

G es isomorfo a G' □

1.2.2. Teoría de Anillos

Definición 1.2.2.1.

Herstein (1970) mencionó:

> Un conjunto no vacío R se dice que es un anillo asociativo si en R están definidas dos operaciones, denotadas por "+" y "·" respectivamente tales que para cualesquiera a, b, c de R :

1. $a+b$ está en R.
2. $a+b=b+a$.
3. $(a+b)+c=a+(b+c)$.
4. Hay un elemento 0 en R tal que $a+0=a$ (para todo a en R).
5. Existe un elemento $-a$ en R tal que $a+(-a)=0$.
6. $a \cdot b$ está en R.

7. $a\cdot(b\cdot c)=(a\cdot b)\cdot c$.
8. $a\cdot(b+c)=a\cdot b+a\cdot c$ y $(b+c)\cdot a=b\cdot a+c\cdot a$ (las dos leyes distributivas). (p. 104)

Ejemplo 1.2.2.2. Sea $R=\mathbb{Z}x\mathbb{Z}$

Para todo $(a,b),(c,d)\in R$, se definen las operaciones binarias:

$$(a,b)+(c,d)=(a+c,b+d)$$

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

Entonces: $(R,+,\cdot)$ es un anillo.

Demostración. Sean $(a,b),(c,d),(e,f)\in R=\mathbb{Z}x\mathbb{Z}$.

1. $(a,b)+(c,d)=(a+c,b+d)\in R$
2. $[(a,b)+(c,d)]+(e,f)=(a+c,b+d)+(e,f)$

   $[(a,b)+(c,d)]+(e,f)=((a+c)+e,(b+d)+f)$

   Como en $\mathbb{Z}$ se cumple la asociatividad, entonces:

   $[(a,b)+(c,d)]+(e,f)=(a+(c+e),b+(d+f))$

   $[(a,b)+(c,d)]+(e,f)=(a,b)+[(c+e,d+f)]$

   $[(a,b)+(c,d)]+(e,f)=(a,b)+[(c,d)+(e,f)]$
3. Sea $(a,b)\in R=\mathbb{Z}x\mathbb{Z}\ \Rightarrow\ a\in\mathbb{Z}\ \wedge\ b\in\mathbb{Z}$

   Como $a,b\in\mathbb{Z}\ \Rightarrow\ \exists!\ 0\in\mathbb{Z}\ /\ a+0=a=0+a\ \wedge\ b+0=b=0+b$

   Luego:

   $$(a,b)=(a+0,b+0)\ \wedge\ (a,b)=(0+a,0+b)$$

   $$(a,b)=(a,b)+(0,0)\ \wedge\ (a,b)=(0,0)+(a,b)$$

Por lo tanto:

$$\exists\ (0,0) \in R\ /\ (a,b)+(0,0)=(a,b)=(0,0)+(a,b)$$

Unicidad:

Supongamos que existe $(0',0') \in R=\mathbb{Z}x\mathbb{Z}\ \wedge\ (0',0') \neq (0,0)$ tal que

$$(a,b)+(0',0')=(a,b)=(0',0')+(a,b)$$

Además: $(a,b)+(0,0)=(a,b)=(0,0)+(a,b)$

Luego:

$$(a,b)+(0',0')=(a,b)+(0,0)$$

$$(a+0',b+0')=(a+0,b+0)$$

$$a+0'=a+0\ \wedge\ b+0'=b+0$$

$$0'=0\ \wedge\ 0'=0$$

$$(0',0')=(0,0)\ (\Rightarrow\Leftarrow)$$

4. Sea $(a,b) \in R=\mathbb{Z}x\mathbb{Z}\ \Rightarrow\ a \in \mathbb{Z}\ \wedge\ b \in \mathbb{Z}$

   Como $a,b \in \mathbb{Z}\ \Rightarrow\ \exists!\ c,d \in \mathbb{Z}$ tal que

$$a+c=0=c+a\ \wedge\ b+d=0=d+b$$

Luego:

$$(a,b)+(c,d)=(0,0)\ \wedge\ (c,d)+(a,b)=(0,0)$$

Por lo tanto:

$$\exists\ (c,d) \in R=\mathbb{Z}x\mathbb{Z}\ /\ (a,b)+(c,d)=(0,0)=(c,d)+(a,b)$$

Unicidad:

Supongamos que existe $(e,f) \in R = \mathbb{Z}x\mathbb{Z} \ \wedge \ (e,f) \neq (c,d)$ tal que

$$(a,b)+(e,f)=(0,0)=(e,f)+(a,b)$$

Además: $(a,b)+(c,d)=(0,0)=(c,d)+(a,b)$

Luego:

$$(a,b)+(e,f)=(a,b)+(c,d)$$

$$(a+e,b+f)=(a+c,b+d)$$

$$a+e=a+c \ \wedge \ b+f=b+d$$

$$e=c \ \wedge \ f=d$$

$$(c,d)=(e,f) \ (\Rightarrow\Leftarrow)$$

5. $(a,b)+(c,d)=(a+c,b+d)$

   Como en $\mathbb{Z}$ se cumple la conmutatividad, entonces:

$$(a,b)+(c,d)=(c+a,d+b)$$

$$(a,b)+(c,d)=(c,d)+(a,b)$$

6. $(a,b)\cdot(c,d)=(a\cdot c,b\cdot d)\in R$

7. $[(a,b)\cdot(c,d)]\cdot(e,f)=(a\cdot c,b\cdot d)\cdot(e,f)=((a\cdot c)\cdot e,(b\cdot d)\cdot f)$

   Como en $\mathbb{Z}$ se cumple la asociatividad, entonces:

   $[(a,b)\cdot(c,d)]\cdot(e,f)=(a\cdot(c\cdot e),b\cdot(d\cdot f))=(a,b)\cdot[(c\cdot e,d\cdot f)]$

   $[(a,b)\cdot(c,d)]\cdot(e,f)=(a,b)\cdot[(c,d)\cdot(e,f)]$

8. $[(a,b)+(c,d)]\cdot(e,f)=(a+c,b+d)\cdot(e,f)=((a+c)\cdot e,(b+d)\cdot f)$

Como en $\mathbb{Z}$ se cumple la distribución, entonces:

$$[(a,b)+(c,d)]\cdot(e,f)=(a\cdot e+c\cdot e, b\cdot f+d\cdot f)=(a\cdot e, b\cdot f)+(c\cdot e, d\cdot f)$$

$$[(a,b)+(c,d)]\cdot(e,f)=[(a,b)\cdot(e,f)]+[(c,d)\cdot(e,f)]$$

9. $(a,b)\cdot[(c,d)+(e,f)]=(a,b)\cdot(c+e,d+f)=(a\cdot(c+e), b\cdot(d+f))$

   Como en $\mathbb{Z}$ se cumple la distribución, entonces:

   $$(a,b)\cdot[(c,d)+(e,f)]=(a\cdot c+a\cdot e, b\cdot d+b\cdot f)=(a\cdot c, b\cdot d)+(a\cdot e, b\cdot f)$$

   $$(a,b)\cdot[(c,d)+(e,f)]=[(a,b)\cdot(c,d)]+[(a,b)\cdot(e,f)]$$

Por lo tanto:

$(R,+,\cdot)$ es un anillo □

Definición 1.2.2.3.

Fraleigh (1987) mencionó: “Un subanillo de un anillo es un subconjunto del anillo que es anillo bajo las operaciones inducidas de todo el anillo” (p. 212).

Proposición 1.2.2.4.

Nachbin (1980) mencionó: “Para que un subconjunto B del anillo A sea un subanillo es necesario y suficiente que:

1. B sea un subgrupo aditivo de A,
2. $x, y \in B$ impliquen $xy \in B$ (p. 96).

Demostración. (Ver demostración en [15], pp. 96-97) □

Ejemplo 1.2.2.5. Sea $(M_2(\mathbb{R}),+,\cdot)$ el anillo de las matrices cuadradas de orden 2 con las operaciones usuales. Se considera el conjunto de las matrices:

$$A=\left\{\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\in M_2(\mathbb{R}); x,y\in\mathbb{R}\right\} \tag{1.15}$$

Entonces: $(A,+,\cdot)$ es un subanillo de $(M_2(\mathbb{R}),+,\cdot)$.

Demostración. Veamos:

1. Tenemos: $A\subset M_2(\mathbb{R})$.
2. Sean $M,N\in A$, entonces:

$$M=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\in M_2(\mathbb{R})\wedge a,b\in\mathbb{R} \tag{1.16}$$

$$N=\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\in M_2(\mathbb{R})\wedge c,d\in\mathbb{R} \tag{1.17}$$

Luego:

$$M-N=\begin{pmatrix} a-c & b-d \\ -b+d & a-c \end{pmatrix}\in M_2(\mathbb{R})\wedge a-c,b-d\in\mathbb{R} \tag{1.18}$$

$$M-N=\begin{pmatrix} a-c & b-d \\ -(b-d) & a-c \end{pmatrix}\in M_2(\mathbb{R})\wedge a-c,b-d\in\mathbb{R} \tag{1.19}$$

$$M-N\in A$$

3. Tenemos:

$$M\cdot N=\begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix}\in M_2(\mathbb{R})\wedge ac-bd,ad+bc\in\mathbb{R} \tag{1.20}$$

$$M\cdot N=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}\in M_2(\mathbb{R})\wedge ac-bd,ad+bc\in\mathbb{R} \tag{1.21}$$

$$M\cdot N\in A$$

Por lo tanto, por la proposición 1.2.2.4. se obtiene:

$(A,+,\cdot)$ es un subanillo de $(M_2(\mathbb{R}),+,\cdot)$ □

Definición 1.2.2.6.

Herstein (1970) mencionó: "Una aplicación ϕ del anillo R en el anillo R' se dice que es un homomorfismo si

1. $\phi(a+b)=\phi(a)+\phi(b)$,
2. $\phi(ab)=\phi(a)\phi(b)$,

para $a,b\in R$ cualesquiera" (p. 113).

Ejemplo 1.2.2.7. En $\mathbb{R}^2$ se consideran las operaciones:

$$(x,y)+(x',y')=(x+x',y+y')$$

$$(x,y)\cdot(x',y')=(x\cdot x',y\cdot y')$$

Para a,b números reales fijos, se define la aplicación:

$$\varphi: F(\mathbb{R},\mathbb{R})\to\mathbb{R}^2 /\ \varphi(f)=(f(a),f(b))$$

Entonces: φ es un homomorfismo de anillos.

Demostración. Para todo par de funciones $f,g\in F(\mathbb{R},\mathbb{R})$, entonces:

1. $\varphi(f+g)=((f+g)(a),(f+g)(b))=(f(a)+g(a),f(b)+g(b))$

   $\varphi(f+g)=(f(a),f(b))+(g(a),g(b))=\varphi(f)+\varphi(g)$

   $\varphi(f+g)=\varphi(f)+\varphi(g)$

2. $\varphi(f\cdot g)=((f\cdot g)(a),(f\cdot g)(b))=(f(a)\cdot g(a),f(b)\cdot g(b))$

   $\varphi(f\cdot g)=(f(a),f(b))\cdot(g(a),g(b))=\varphi(f)\cdot\varphi(g)$

   $\varphi(f\cdot g)=\varphi(f)\cdot\varphi(g)$

Por lo tanto:

φ es un homomorfismo de anillos □

Definición 1.2.2.8.

Herstein (1970) mencionó: "Un subconjunto no vacío U de R se dice que es un ideal (bilateral) de R si:

1) U es un subgrupo de R bajo la adición.
2) Para todo $u \in U$ y $r \in R$, tanto ur como ru están en U" (p. 116).

Definición 1.2.2.9.

Lang (1971) mencionó:

> Si $a_1, \ldots, a_n$ son elementos de un anillo A, representaremos por $(a_1, \ldots, a_n)$ la intersección de todos los ideales de A que contienen a estos elementos, o la intersección de todos los ideales a la izquierda que contienen a estos elementos. (…) . Se ve en seguida que el ideal a la izquierda engendrado por $a_1, \ldots, a_n$ consta de todos los elementos que se pueden escribir en la forma
>
> $$x_1 a_1 + \ldots + x_n a_n$$
>
> con $x_i \in A$. (p. 68)

Ejemplo 1.2.2.10. Sea $(\mathbb{Z}, +, \cdot)$ un anillo, entonces:

Para todo $a \in \mathbb{Z}$, $< a >= \{n \cdot a / n \in \mathbb{Z}\}$ es un ideal de $(\mathbb{Z}, +, \cdot)$.

Demostración. Demostraremos que $< a >$ es un ideal de $(\mathbb{Z}, +, \cdot)$

1. Sea $w \in < a >$ entonces existe $n \in \mathbb{Z}$ tal que $w = n \cdot a \in \mathbb{Z}$

   Por lo tanto:

   $$< a > \subset \mathbb{Z}$$

2. Sean $w_1, w_2 \in <a>$ entonces existen $n_1, n_2 \in \mathbb{Z}$ tal que

$$w_1 = n_1 \cdot a \ \wedge \ w_2 = n_2 \cdot a$$

Luego:

$$w_1 - w_2 = n_1 \cdot a - n_2 \cdot a = (n_1 - n_2) \cdot a \in <a>$$

Por lo tanto:

$$w_1 - w_2 \in <a>$$

3. Sea $r \in \mathbb{Z}$

Sea $w \in <a>$ entonces existe $n \in \mathbb{Z}$ tal que $w = n \cdot a$

Entonces:

$$w \cdot r = (n \cdot a) \cdot r = n \cdot (a \cdot r) = n \cdot (r \cdot a) = (n \cdot r) \cdot a \in <a>$$

Por lo tanto:

$$w \cdot r \in <a>$$

Además:

$$r \cdot w = r \cdot (n \cdot a) = (r \cdot n) \cdot a \in <a>$$

Por lo tanto:

$$r \cdot w \in <a>$$

Finalmente, se concluye que:

$$\forall a \in \mathbb{Z}, <a> \text{ es un ideal de } (\mathbb{Z}, +, \cdot)$$ □

Definición 1.2.2.11.

Fraleigh (1987) mencionó:

Si N es un ideal en un anillo R, entonces, el anillo de las clases laterales $r+N$ bajo las operaciones inducidas es el anillo cociente, o el anillo factor, o el anillo de las clases residuales de R módulo N, y se denota por R/N. Las clases laterales son las clases residuales módulo N. (p. 253)

Lema 1.2.2.12.

Herstein (1970) mencionó: "Si U es un ideal del anillo R, entonces R/U es un anillo y es una imagen homomorfa de R" (p. 117).

Demostración. (Ver demostración en [9], pp. 116-117) □

Ejemplo 1.2.2.13. Considérese el anillo $\mathbb{Z}$, entonces $\mathbb{Z}/<a>$ es un anillo, bajo las operaciones inducidas de suma y multiplicación.

Demostración. Del ejemplo 1.2.2.10. tenemos que $\forall a \in \mathbb{Z}$ se tiene $<a>$ es un ideal de $(\mathbb{Z},+,\cdot)$. Por el lema 1.2.2.12. se tiene que $\mathbb{Z}/<a>$ es un anillo, bajo las operaciones inducidas de suma y multiplicación. □

Definición 1.2.2.14.

Dummit y Foote (2004) mencionaron:

Let I and J be ideals of R.

1. Define the sum of I and J by $I+J=\{a+b \mid a\in I, b\in J\}$.
2. Define the product of I and J, denoted by IJ, to be the set of all finite sums of elements of the form ab with $a\in I$ and $b\in J$.
3. For any $n\geq 1$, define the n^{th} power of I, denoted by I^n, to be the set consisting of all finite sums of elements of the form $a_1a_2\ldots a_n$ with $a_i\in I$ for all i.
   Equivalently, I^n is defined inductively by defining $I^1=I$, and $I^n=II^{n-1}$ for

$n = 2, 3, \ldots$ (p. 247)

Definición 1.2.2.15.

Fraleigh (1987) mencionó: "Si a y b son dos elementos distintos de cero de un anillo R tal que $ab = 0$, entonces a y b son divisores de 0. En particular, a es un divisor izquierdo de 0 y b es un divisor derecho de 0" (p. 216).

Ejemplo 1.2.2.16. Sea $(\mathbb{Z}_6, +, \cdot)$ el anillo cociente conmutativo con identidad, entonces $\overline{4}$ es un divisor de cero.

Demostración. Se puede ver:

$$\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$$

Por lo tanto:

$\overline{4}$ es un divisor de cero □

Definición 1.2.2.17.

Herstein (1970) mencionó: "Sea R un anillo conmutativo con elemento unitario.
Dos elementos a y b de R se dice que son asociados si $b = ua$ para alguna unidad u de R" (p. 129).

Ejemplo 1.2.2.18. Sea el anillo $(\mathbb{Z}, +, \cdot) \ \wedge \forall n \in \mathbb{Z} - \{0\}$, entonces: n y $-n$ son asociados.

Demostración. Podemos ver:

$n = (-n) \cdot (-1)$ y -1 es invertible

Por lo tanto:

n y $-n$ son asociados □

Definición 1.2.2.19.

Fraleigh (1987) mencionó: "Un dominio entero D es un anillo conmutativo unitario que no contiene divisores de 0" (p. 217).

Ejemplo 1.2.2.20. $(\mathbb{Z},+,\cdot)$ es un dominio entero.

Demostración. Se sabe que $\mathbb{Z}$ cumple con las condiciones de anillo conmutativo con identidad, además no tiene divisores de cero, es decir:

$$\forall\ a,b\in\mathbb{Z}\ /\ a\cdot b=0\ \Leftrightarrow\ a=0\vee b=0$$

Por lo tanto:

$(\mathbb{Z},+,\cdot)$ es un dominio entero □

Definición 1.2.2.21.

Fraleigh (1987) mencionó: "Si R es un anillo conmutativo con unitario y $a\in R$, el ideal $\{ra\ /\ r\in R\}$ de todos los múltiplos de a es el ideal principal generado por a y se denota por $<a>$. Un ideal N de R es un ideal principal si $N=<a>$ para alguna $a\in R$" (p. 285).

Ejemplo 1.2.2.22. $(\mathbb{Z},+,\cdot)$ es un ideal principal.

Demostración. Se puede ver que -1 y 1 son los generadores de los números enteros. □

Definición 1.2.2.23.

Herstein (1970) mencionó: "Un ideal $M\neq R$ es un anillo R se dice que es un ideal máximo de R si siempre que U es un ideal de R tal que $M\subset U\subset R$ se tiene que $R=U$ o $M=U$" (p. 120).

Observación 1.2.2.24.

Herstein (1970) mencionó: “Un elemento primo es un elemento en R que no puede ser factorizado en R en forma que no sea trivial” (p. 129).

Ejemplo 1.2.2.25. Sea $\mathbb{Z}$ el anillo de los enteros y sea $P =< p >$ con p primo, un ideal de $\mathbb{Z}$ entonces P es un ideal maximal de $\mathbb{Z}$.

Demostración. Sea U un ideal de $\mathbb{Z}$ $/ P \subset_{\neq} U \subset \mathbb{Z}$.

Como U es ideal de $\mathbb{Z} \Rightarrow U =< n_0 > \subset \mathbb{Z}$, para algún $n_0 \in \mathbb{Z}$ (fijo).

Como $p \in P \subset U \Rightarrow p = mn_0 \in \mathbb{Z}$, para algún $m \in \mathbb{Z} \Rightarrow n_0 \mid p$.

Como p es primo $\Rightarrow n_0 = 1 \vee n_0 = p$

Si: $n_0 = 1$, entonces:

$$U =< 1 > \Rightarrow U = \mathbb{Z}$$

Si: $n_0 = p$, entonces:

$$U =< p >= P \Rightarrow U = P \ (\Rightarrow\Leftarrow)$$

Así, se obtiene:

$$U = \mathbb{Z}$$

Por lo tanto:

$$P \text{ es un ideal maximal de } \mathbb{Z}$$ □

Observación 1.2.2.26.

Fraleigh (1987) mencionó:

Todo anillo R tiene dos ideales, el ideal impropio R y el ideal trivial $\{0\}$. Para estos ideales, los anillos factores son R/R, que tiene un solo elemento y $R/\{0\}$, el cual es claramente isomorfo a R. Estos casos no son interesantes. Igual que para un subgrupo de un grupo, un ideal no trivial propio de un anillo R es un ideal N de R tal que $N \neq R$ y $N \neq \{0\}$. (p. 254)

Proposición 1.2.2.27.

Dummit y Foote (2004) mencionaron: "In a ring with identity every proper ideal is contained in a maximal ideal" (p. 254).

Demostración. Sea R un anillo con identidad y sea I un ideal propio entonces R no puede ser el anillo cero.

Sea S el conjunto de todos los ideales propios de R que contienen a I. Entonces, $S \neq \varnothing$ pues $I \in S$ y es parcialmente ordenado por inclusión.

Si C es una cadena en S, definamos:

$$J = \bigcup_{A \in C} A$$

Afirmación 1: $J \neq \varnothing$

En efecto:

Como cada $A \in C$ son ideales propios de R, entonces:

$A \in C$ son subgrupos aditivos de R

$$0 \in A \subset \bigcup_{A \in C} A,\ i = 1, 2, \ldots$$

Entonces:

$$0 \in J$$

Por lo tanto:

$$J \neq \varnothing$$

Afirmación 2: J es un ideal de R.

En efecto:

1. Sea $z \in J = \bigcup_{A \in C} A \Rightarrow \exists\ A \in C\ /\ z \in A$

   Como $A \in C$ es un ideal propio de R, se obtiene:

   $$J \subset R \tag{1.22}$$

2. Sean $z, w \in J = \bigcup_{A \in C} A$, entonces:

   $$\exists\ A \in C\ /\ z \in A\ \wedge\ \exists\ B \in C\ /\ w \in B$$

   Por definición de una cadena, puede ser: $A \subset B\ \vee\ B \subset A$.

   Si: $A \subset B$

   $$z - w \in B \subset \bigcup_{A \in C} A$$

   $$z - w \in J$$

   Si: $B \subset A$

   $$z - w \in A \subset \bigcup_{A \in C} A$$

   $$z - w \in J$$

   Por lo tanto, en cualquier caso, se obtiene:

   $$z - w \in J \tag{1.23}$$

3. Sea $r \in R \ \wedge \ z \in J = \bigcup_{A \in C} A \ \Rightarrow \ \exists \ A \in C \ / \ z \in A$

   Como A es un ideal propio de R, entonces:

$$r \cdot z \in A \ \wedge \ z \cdot r \in A$$

$$r \cdot z \in \bigcup_{A \in C} A \ \wedge \ z \cdot r \in \bigcup_{A \in C} A$$

   Por lo tanto, se obtiene:

$$r \cdot z \in J \wedge z \cdot r \in J \qquad (1.24)$$

Finalmente, de (1.22), (1.23) y (1.24) se obtiene:

$$J \text{ es un ideal de } R$$

Afirmación 3: J es un ideal propio de R.

En efecto:

Supongamos: J no es un ideal propio de R, entonces:

$$J = 0 \ \vee \ J = R$$

Si: $J = 0$ entonces:

$$\bigcup_{A \in C} A = 0$$

$$A \subset 0 \text{; para algún } A \in C$$

Como A es ideal de $R \ \Rightarrow \ A$ es subgrupo aditivo de $R \ \Rightarrow \ 0 \in A$

Luego:

$$0 \in A \subset 0 \ \Rightarrow \ 0 \subset A \subset 0 \ \Rightarrow \ A = 0 \ (\Rightarrow\Leftarrow) \ (\ A \text{ es propio})$$

Si: $J = R$ entonces:

$$1 \in J$$

Luego:

$$1 \in \bigcup_{A \in C} A$$

$$1 \in A \text{, para algún } A \in C$$

Sea $r \in R \ \wedge \ 1 \in A \subset R$, por ser A un ideal propio de R, entonces:

$$r \cdot 1 \in A \subset R$$

Como R es un anillo con elemento identidad, entonces:

$$r \in A$$

Por lo tanto:

$$R \subset A$$

Además: A es ideal propio de $R \Rightarrow A \subset R$, por lo tanto:

$$R = A \ (\Rightarrow\Leftarrow) \text{ (Pues } A \text{ es ideal propio de } R \text{)}$$

Finalmente:

$$J \text{ es un ideal propio de } R$$

Esto prueba que cada cadena tiene una cota superior en S, por el lema de Zorn concluimos que S tiene un elemento maximal, es decir, un ideal propio maximal que contiene a I. □

Definición 1.2.2.28.

Fraleigh (1987) mencionó: "Un dominio entero D es un dominio de ideales principal (DIP), si todo ideal en D es un ideal principal" (p. 292).

Ejemplo 1.2.2.29. El dominio entero $\mathbb{Z}$ de los números enteros es un DIP.

Demostración. Tenemos que los ideales del dominio entero $\mathbb{Z}$ son de la forma: $n\mathbb{Z} =< n >$ para todo $n \in \mathbb{Z}$, por lo tanto: $\mathbb{Z}$ es un DIP. □

Definición 1.2.2.30.

Fraleigh (1987) mencionó:

> Un dominio entero D es un dominio de factorización única (DFU), si se satisfacen las siguientes condiciones:
>
> 1. Todo elemento de D que no sea ni 0 ni una unidad, se puede factorizar en un número finito de irreducibles.
> 2. Si $p_1,\ldots,p_r$ y $q_1,\ldots,q_r$ son dos factorizaciones en irreducibles del mismo elemento de D, entonces $r = s$ y los q_j pueden renumerarse de manera que p_i y q_i sean asociados. (p. 292)

Teorema 1.2.2.31.

Fraleigh (1987) mencionó: "Todo DIP es un DFU" (p. 296).

Demostración. (Ver demostración en [7], p. 296) □

Ejemplo 1.2.2.32. El anillo $\mathbb{Z}$ de los enteros es un DFU.

Demostración. Del ejemplo 1.2.2.29. tenemos que $\mathbb{Z}$ es un DIP. Por el Teorema 1.2.2.31. se concluye que $\mathbb{Z}$ es un DFU. □

Definición 1.2.2.33.

Fraleigh (1987) mencionó: "Sea D un dominio entero y $a, b \in D$. Si existe $c \in D$ tal que $b = ac$, entonces a divide b (o a es un factor de b), se denota $a \mid b$" (p. 291).

Ejemplo 1.2.2.34. Sea R un DFU $\wedge$ $\forall$ $k \in R$, se puede ver que:

$$1 \mid k \text{ y si } k \neq 0,\ k \mid k$$

Definición 1.2.2.35.

Fraleigh (1987) mencionó: "Sea D un DFU. Un elemento $d \in D$ es un máximo común divisor (mcd) de los elementos a y b en D si $d \mid a$, $d \mid b$ y además, $c \mid d$ para todos los c que dividan a y b" (p. 307).

Teorema 1.2.2.36.

Fraleigh (1987) mencionó: "Si D es un DIP y a y b son elementos distintos de cero de D , entonces existe algún mcd de a y b . Más aún, cada mcd de a y b puede expresarse en la forma $\lambda a + \mu b$ para algunos $\lambda, \mu \in D$ " (p. 307).

Demostración. (Ver demostración en [7], pp. 307-308) □

Definición 1.2.2.37.

Zaldívar (1996) mencionó: "Sea A un DIP. Un elemento $\pi \in A$ no unidad, se llama primo o irreducible si siempre que $a \mid \pi$ se tiene que a es una unidad o un asociado de π , es decir, siempre que $\pi = ab$ en A , entonces a ó b es unidad.

Dos elementos $a, b \in A$ se llaman coprimos o primos relativos si su $mcd(a,b)$ es una unidad de A " (p. 25).

Observación 1.2.2.38.

Zaldívar (1996) mencionó: "Como es obvio que el asociado de cualquier $mcd(a,b)$ sigue siendo un mcd de a y b , entonces si a y b son coprimos, como 1 es asociado a cualquier

unidad, entonces un $mcd(a,b)$ es 1. Por la proposición (1.37), existen $s,t \in A$ tales que $1 = as + bt$. Cuando a y b sean coprimos, escribiremos $mcd(a,b) = 1$ " (p. 25).

Proposición 1.2.2.39.

Zaldívar (1996) mencionó: "Sea A un DIP y sean $a,b,c \in A$. Si $a \mid bc$ y $mcd(a,b) = 1$, entonces $a \mid c$ " (p. 25).

Demostración. Como $a \mid bc$ entonces existe $k \in A$ tal que $bc = ka$.

Como $mcd(a,b) = 1$, por la observación 1.2.2.38. se tiene:

$$\exists m,n \in A / ma + nb = 1$$

Entonces:

$$c = c \cdot 1 = c(ma + nb) = acm + bcn$$

Reemplazando:

$$c = acm + kan = acm + akn = a(cm + kn)$$

Por lo tanto:

$$a \mid c$$

□

Corolario 1.2.2.40.

Zaldívar (1996) mencionó: "Sea A un DIP, y sea $\pi \in A$ un primo. Si $\pi \mid ab$, con $a,b \in A$, entonces $\pi \mid a$ ó $\pi \mid b$ " (p. 26).

Demostración. Si $\pi \nmid b$ entonces $mcd(b,\pi) = 1$.

Luego, tenemos que $\pi \mid ab$ y $mcd(b,\pi) = 1$ por la proposición 1.2.2.39. se tiene $\pi \mid a$.

En forma análoga, si $\pi \nmid a$ entonces $mcd(a,\pi)=1$.

Luego, tenemos que $\pi \mid ab$ y $mcd(a,\pi)=1$ por la proposición 1.2.2.39. se tiene $\pi \mid b$. □

Definición 1.2.2.41.

Fraleigh (1987) mencionó: "Un ideal $N \neq R$ en un anillo conmutativo R es un ideal primo si $ab \in N$ implica que $a \in N$ o $b \in N$ para todas las $a,b \in R$ " (p. 261).

Ejemplo 1.2.2.42. Si n es un número primo entonces $n\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$.

Demostración. Sean $a,b \in \mathbb{Z}$ tal que $a \cdot b \in n\mathbb{Z}$

Entonces, existe $l \in \mathbb{Z}$ tal que $a \cdot b = n \cdot l$, es decir: $n \mid ab$

Como n es primo y $n \mid ab$ por el corolario 1.2.2.40. se tiene:

$$n \mid a \vee n \mid b$$

Luego, existen $c,d \in \mathbb{Z}$ tal que $a = c \cdot n \ \vee \ b = d \cdot n$

Entonces:

$$a \in n\mathbb{Z} \vee b \in n\mathbb{Z}$$

Por lo tanto:

$n\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ □

Definición 1.2.2.43.

Dummit y Foote (2004) mencionaron:

> The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ with $n \geq 0$ and each $a_i \in R$.

If $a_n \neq 0$ then the polynomial is of degree n, $a_n x^n$ is the leading term, and a_n is the leading coefficient (where the leading coefficient of the zero polynomial is defined to be 0). The polynomial is monic if $a_n = 1$. Addition of polynomials is "componentwise":

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

(here a_n or b_n may be zero in order for addition of polynomials of different degrees to be defined). Multiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ and then extending to all polynomials by the distributive laws so that in general

$$(\sum_{i=0}^{n} a_i x^i).(\sum_{i=0}^{m} b_i x^i) = \sum_{k=0}^{n+m} (\sum_{i=0}^{k} a_i b_{k-i}) x^k \ .$$

In this way $R[x]$ is a commutative ring with identity (the identity 1 from R) in which we identify R with the subring of constant polynomials. (p. 295)

Ejemplo 1.2.2.44. Sea $(\mathbb{R}, +, \cdot)$ un anillo conmutativo.

Entonces: $(\mathbb{R}[x], +, \cdot)$ es el anillo de polinomios conmutativo.

Definición 1.2.2.45.

Herstein (1970) mencionó:

Si $f(x) = a_0 + a_1 x + \ldots + a_n x^n \neq 0$ y $a_n \neq 0$, entonces el grado de $f(x)$, escrito: $\deg f(x)$, es n.

Es decir, el grado de $f(x)$ es el mayor entero i para el que el i-ésimo coeficiente de $f(x)$ no es 0. No definimos el grado del polinomio cero.

Decimos que un polinomio es una constante si es de grado 0 o es el polinomio cero. La función de grado definida sobre los elementos de $F[x]$ distintos del cero nos provee de la función $d(x)$ necesaria para que $F[x]$ sea un anillo euclideano. (p. 138)

Ejemplo 1.2.2.46. Sea $(\mathbb{R},+,\cdot)$ un anillo conmutativo.

Entonces: $(\mathbb{R}[x],+,\cdot)$ es el anillo de polinomios conmutativo.

Si: $p(x)=3x^2+5x+8$ entonces $\deg p(x)=2$.

Lema 1.2.2.47.

Herstein (1970) mencionó: "Si $f(x), g(x)$ son dos elementos distintos del cero de $F[x]$ entonces $\deg(f(x)g(x))=\deg f(x)+\deg g(x)$" (p. 138).

Demostración. (Ver demostración en [9], pp. 138-139) □

Definición 1.2.2.48.

Herstein (1970) mencionó: "Un polinomio $p(x)$ en $F[x]$ se dice que es irreducible sobre F si siempre que $p(x)=a(x)b(x)\in F[x]$, entonces uno de los dos, $a(x)$ o $b(x)$, tiene grado cero (es decir, es una constante)" (p. 140).

Ejemplo 1.2.2.49. Sea $(\mathbb{R},+,\cdot)$ un anillo conmutativo.

Entonces: $(\mathbb{R}[x],+,\cdot)$ es el anillo de polinomios conmutativo.

Si: $p(x)=x^2+1$ entonces el polinomio es irreducible en $\mathbb{R}$.

Proposición 1.2.2.50.

Castellanos (2013) mencionó: "Si D es DFU, entonces, y $p\in D-\{0\}$ $(p)\subset D$ es ideal primo $\Leftrightarrow$ p es irreducible (o primo)" (p. 76).

Demostración. (Ver demostración en [3], p. 77) □

Proposición 1.2.2.51.

Castellanos (2013) mencionó: "Si D es DIP, entonces

(p) es ideal primo $\Leftrightarrow$ (p) es ideal maximal" (p. 79).

Demostración. (Ver demostración en [3], p. 79) □

1.2.3. Cuerpos y Subcuerpos

Definición 1.2.3.1.

Hernández (2010) mencionó: "Si R es un anillo conmutativo con unitario e, que tiene la propiedad de que $\forall a \in R \setminus \{0\}$ $\exists a' \in R$ tal que $a * a' = e$ entonces R es llamado CAMPO" (p. 8).

Ejemplo 1.2.3.2. Sea $(\mathbb{Q}, +, \cdot)$ un cuerpo.

Definamos:

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \,/\, a, b \in \mathbb{Q} \right\}$$ el espacio generado sobre $\mathbb{Q}$ y $\sqrt{2}$

con sus operaciones binarias "+" y "." de esta forma:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (a \cdot c + 2 \cdot b \cdot d) + (a \cdot d + b \cdot c)\sqrt{2}$$

Entonces: $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ es un cuerpo.

Demostración. Sean:

$$z_1 = a + b\sqrt{2} \;,\; z_2 = c + d\sqrt{2} \;,\; z_3 = e + f\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

Entonces:

1. $z_1+z_2=(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$

   $z_1+z_2\in\mathbb{Q}(\sqrt{2})$

2. $(z_1+z_2)+z_3=((a+b\sqrt{2})+(c+d\sqrt{2}))+(e+f\sqrt{2})$

   $(z_1+z_2)+z_3=((a+c)+(b+d)\sqrt{2})+(e+f\sqrt{2})$

   $(z_1+z_2)+z_3=((a+c)+e)+((b+d)+f)\sqrt{2}$

   $(z_1+z_2)+z_3=(a+(c+e))+(b+(d+f))\sqrt{2}$

   $(z_1+z_2)+z_3=(a+b\sqrt{2})+((c+e)+(d+f)\sqrt{2})$

   $(z_1+z_2)+z_3=(a+b\sqrt{2})+((c+d\sqrt{2})+(e+f\sqrt{2}))$

   $(z_1+z_2)+z_3=z_1+(z_2+z_3)$

3. Sea $z_1\in\mathbb{Q}(\sqrt{2})\ \Rightarrow\ z_1=a+b\sqrt{2}$, para algún $a,b\in\mathbb{Q}$

   Como $a,b\in\mathbb{Q}\ \Rightarrow\ \exists!\ 0\in\mathbb{Q}\ /\ a+0=a=0+a\ \wedge\ b+0=b=0+b$

   Luego:

   $$z_1=(a+0)+(b+0)\sqrt{2}\ \wedge\ z_1=(0+a)+(0+b)\sqrt{2}$$

   $$z_1=(a+b\sqrt{2})+(0+0\sqrt{2})\ \wedge\ z_1=(0+0\sqrt{2})+(a+b\sqrt{2})$$

   $$z_1=z_1+0\ \wedge\ z_1=0+z_1$$

   Por lo tanto:

   $$\exists\ 0\in\mathbb{Q}(\sqrt{2})\ /\ z_1+0=z_1=0+z_1$$

   Unicidad:

   Supongamos que existe $0'\in\mathbb{Q}(\sqrt{2})\ \wedge\ 0'\neq 0$ tal que

   $$z_1+0'=z_1=0'+z_1$$

Además: $z_1+0=z_1=0+z_1$

Luego:

$$z_1+0'=z_1+0$$

$$(a+b\sqrt{2})+(0'+0'\sqrt{2})=(a+b\sqrt{2})+(0+0\sqrt{2})$$

$$(a+0')+(b+0')\sqrt{2}=(a+0)+(b+0)\sqrt{2}$$

$$a+0'=a+0 \wedge b+0'=b+0$$

$$0'=0 \wedge 0'=0$$

$$(0+0\sqrt{2})=(0'+0'\sqrt{2})$$

$$0=0' \in \mathbb{Q}(\sqrt{2}) \quad (\Rightarrow\Leftarrow)$$

4. Sea $z_1 \in \mathbb{Q}(\sqrt{2}) \Rightarrow z_1=a+b\sqrt{2}$, para algún $a,b \in \mathbb{Q}$

   Como $a,b \in \mathbb{Q} \Rightarrow \exists!\ c,d \in \mathbb{Q}\ /\ a+c=0=c+a \wedge b+d=0=d+b$

   Luego:

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(0+0\sqrt{2}) \wedge (c+d\sqrt{2})+(a+b\sqrt{2})=(0+0\sqrt{2})$$

$$z_1+w_1=0 \wedge w_1+z_1=0$$

   Por lo tanto:

$$\exists\ w_1 \in \mathbb{Q}(\sqrt{2})\ /\ z_1+w_1=0=w_1+z_1$$

   Unicidad:

   Supongamos que existe $r_1 \in \mathbb{Q}(\sqrt{2}) \wedge r_1 \neq w_1$ tal que

$$z_1+r_1=0=r_1+z_1$$

Además: $z_1 + w_1 = 0 = w_1 + z_1$

Luego:

$$z_1 + r_1 = z_1 + w_1$$

$$(a + b\sqrt{2}) + (e + f\sqrt{2}) = (a + b\sqrt{2}) + (c + d\sqrt{2})$$

$$(a + e) + (b + f)\sqrt{2} = (a + c) + (b + d)\sqrt{2}$$

$$a + e = a + c \ \wedge \ b + f = b + d$$

$$e = c \ \wedge \ f = d$$

$$(c + d\sqrt{2}) = (e + f\sqrt{2})$$

$$w_1 = r_1 \ (\Rightarrow\Leftarrow)$$

5. $z_1 + z_2 = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$

   Como en $\mathbb{Q}$ se cumple la conmutatividad, entonces:

   $z_1 + z_2 = (c + a) + (d + b)\sqrt{2} = (c + d\sqrt{2}) + (a + b\sqrt{2})$

   $z_1 + z_2 = z_2 + z_1$

6. $z_1 \cdot z_2 = (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (a \cdot c + 2b \cdot d) + (a \cdot d + b \cdot c)\sqrt{2}$

   $z_1 . z_2 \in \mathbb{Q}(\sqrt{2})$

7. $(z_1 \cdot z_2) \cdot z_3 = ((a + b\sqrt{2}) \cdot (c + d\sqrt{2})) \cdot (e + f\sqrt{2})$

   $(z_1 \cdot z_2) \cdot z_3 = ((a \cdot c + 2b \cdot d) + (a \cdot d + b \cdot c)\sqrt{2}) \cdot (e + f\sqrt{2})$

   $(z_1 \cdot z_2) \cdot z_3 = ((a \cdot c + 2b \cdot d) \cdot e + 2(a \cdot d + b \cdot c) \cdot f) + ((a \cdot c + 2b \cdot d) \cdot f + (a \cdot d + b \cdot c) \cdot e)\sqrt{2}$

   Por otro lado:

$$z_1 \cdot (z_2 \cdot z_3) = (a + b\sqrt{2}) \cdot ((c + d\sqrt{2}) \cdot (e + f\sqrt{2}))$$

$$z_1 \cdot (z_2 \cdot z_3) = (a + b\sqrt{2}) \cdot ((c \cdot e + 2d \cdot f) + (c \cdot f + d \cdot e)\sqrt{2})$$

$$z_1 \cdot (z_2 \cdot z_3) = (a \cdot (c \cdot e + 2d \cdot f) + 2b \cdot (c \cdot f + d \cdot e)) + (a \cdot (c \cdot f + d \cdot e) + b \cdot (c \cdot e + 2d \cdot f))\sqrt{2}$$

Arreglando la expresión se tiene:

$$z_1 \cdot (z_2 \cdot z_3) = ((a \cdot c + 2b \cdot d) \cdot e + 2(a \cdot d + b \cdot c) \cdot f) + ((a \cdot c + 2b \cdot d) \cdot f + (a \cdot d + b \cdot c) \cdot e)\sqrt{2}$$

Por lo tanto:

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

8. Sea $z_1 \in \mathbb{Q}(\sqrt{2}) \Rightarrow z_1 = a + b\sqrt{2}$, para algún $a, b \in \mathbb{Q}$

   Como $a, b \in \mathbb{Q} \Rightarrow \exists!\ 1 \in \mathbb{Q} \ / \ a \cdot 1 = a = 1 \cdot a \ \wedge \ b \cdot 1 = b = 1 \cdot b$

   Además: $a \cdot 0 = 0 = 0 \cdot a \ \wedge \ b \cdot 0 = 0 = 0 \cdot b$

   Luego:

$$z_1 = a + b\sqrt{2} = (a \cdot 1 + 2 \cdot b \cdot 0) + (a \cdot 0 + b \cdot 1)\sqrt{2}$$

$$z_1 = (a + b\sqrt{2}) \cdot (1 + 0\sqrt{2})$$

$$z_1 = z_1 \cdot e$$

   En forma análoga, se tiene: $e \cdot z_1 = z_1$

   Por lo tanto:

$$\exists\ e = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \ / \ z_1 \cdot e = z_1 = e \cdot z_1$$

Unicidad:

Supongamos que existe $f \in \mathbb{Q}(\sqrt{2}) \ \wedge \ f \neq e$ tal que

$$z_1 \cdot f = z_1 = f \cdot z_1$$

Además: $z_1 \cdot e = z_1 = e \cdot z_1$

Luego:

$$z_1 \cdot f = z_1 \cdot e$$

$$(a+b\sqrt{2}) \cdot (1' + 0'\sqrt{2}) = (a+b\sqrt{2}) \cdot (1+0\sqrt{2})$$

$$(a+0') + (0' + b)\sqrt{2} = (a+0) + (0+b)\sqrt{2}$$

$$a + 0' = a + 0 \ \wedge \ 0' + b = 0 + b$$

$$0' = 0 \wedge 0' = 0 \qquad (1.25)$$

Por otro lado:

$$a \cdot 1' = a = 1' \cdot a \ \wedge \ a \cdot 1 = a = 1 \cdot a$$

Como $\mathbb{Q}$ tiene como único elemento identidad a 1, entonces:

$$1' = 1 \qquad (1.26)$$

Usando (1.25) y (1.26) se tiene:

$$1 + 0\sqrt{2} = 1' + 0'\sqrt{2}$$

$$e = f \ (\Rightarrow\Leftarrow)$$

9. Sea $z_1 \in \mathbb{Q}(\sqrt{2}) \ \Rightarrow \ z_1 = a + b\sqrt{2}$, para algún $a, b \in \mathbb{Q}$

Tomando: $z_1^{-1} = \frac{-a}{2b^2 - a^2} + \frac{b}{2b^2 - a^2}\cdot\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

Luego:

$$z_1 \cdot z_1^{-1} = (a + b\sqrt{2}) \cdot (\frac{-a}{2b^2 - a^2} + \frac{b}{2b^2 - a^2}\sqrt{2})$$

$$z_1 \cdot z_1^{-1} = 1 + 0\sqrt{2}$$

$$z_1 \cdot z_1^{-1} = e$$

De forma análoga se obtiene: $z_1^{-1} \cdot z_1 = e$

Por lo tanto:

$$\exists\ z_1^{-1} = \frac{-a}{2b^2 - a^2} + \frac{b}{2b^2 - a^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})\ /\ \ z_1 \cdot z_1^{-1} = e = z_1^{-1} \cdot z_1$$

Unicidad:

(La prueba consiste en suponer que existe otro elemento inverso y encontrar una contradicción.)

10. $z_1 \cdot z_2 = (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (a \cdot c + 2b \cdot d) + (a \cdot d + b \cdot c)\sqrt{2}$

Por otro lado:

$$z_2 \cdot z_1 = (c + d\sqrt{2}) \cdot (a + b\sqrt{2}) = (c \cdot a + 2d \cdot b) + (c \cdot b + d \cdot a)\sqrt{2}$$

Como en $\mathbb{Q}$ se cumple la conmutatividad, entonces:

$$z_2 \cdot z_1 = (a \cdot c + 2b \cdot d) + (a \cdot d + b \cdot c)\sqrt{2}$$

Por lo tanto:

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

11. $(z_1+z_2)\cdot z_3=((a+b\sqrt{2})+(c+d\sqrt{2}))\cdot(e+f\sqrt{2})$

$(z_1+z_2)\cdot z_3=((a+c)+(b+d)\sqrt{2})\cdot(e+f\sqrt{2})$

$(z_1+z_2)\cdot z_3=((a+c)\cdot e+2(b+d)\cdot f)+((a+c)\cdot f+(b+d)\cdot e)\sqrt{2}$

Por otro lado:

$z_1\cdot z_3+z_2\cdot z_3=(a+b\sqrt{2})\cdot(e+f\sqrt{2})+(c+d\sqrt{2})\cdot(e+f\sqrt{2})$

$z_1\cdot z_3+z_2\cdot z_3=((a\cdot e+2b\cdot f)+(a\cdot f+b\cdot e)\sqrt{2})+((c\cdot e+2d\cdot f)+(c\cdot f+d\cdot e)\sqrt{2})$

$z_1\cdot z_3+z_2\cdot z_3=(a\cdot e+2b\cdot f+c\cdot e+2d\cdot f)+(a\cdot f+b\cdot e+c\cdot f+d\cdot e)\sqrt{2}$

Arreglando la expresión se tiene:

$z_1\cdot z_3+z_2\cdot z_3=((a+c)\cdot e+2(b+d)\cdot f)+((a+c)\cdot f+(b+d)\cdot e)\sqrt{2}$

Por lo tanto:

$$(z_1+z_2)\cdot z_3=z_1\cdot z_3+z_2\cdot z_3$$

12. $z_3\cdot(z_1+z_2)=(e+f\sqrt{2})\cdot((a+b\sqrt{2})+(c+d\sqrt{2}))$

$z_3\cdot(z_1+z_2)=(e+f\sqrt{2})\cdot((a+c)+(b+d)\sqrt{2})$

$z_3\cdot(z_1+z_2)=(e\cdot(a+c)+2\cdot f(b+d))+(e\cdot(b+d)+f\cdot(a+c))\sqrt{2}$

Por otro lado:

$z_3\cdot z_1+z_3\cdot z_2=(e+f\sqrt{2})\cdot(a+b\sqrt{2})+(e+f\sqrt{2})\cdot(c+d\sqrt{2})$

$z_3\cdot z_1+z_3\cdot z_2=((e\cdot a+2f\cdot b)+(e\cdot b+f\cdot a)\sqrt{2})+((e\cdot c+2f\cdot d)+(e\cdot d+f\cdot c)\sqrt{2})$

$z_3\cdot z_1+z_3\cdot z_2=(e\cdot a+2f\cdot b+e\cdot c+2f\cdot d)+(e\cdot b+f\cdot a+e\cdot d+f\cdot c)\sqrt{2}$

Arreglando la expresión se tiene:

$$z_3 \cdot z_1 + z_3 \cdot z_2 = (e \cdot (a+c) + 2f \cdot (b+d)) + (e \cdot (b+d) + f \cdot (a+c))\sqrt{2}$$

Por lo tanto:

$$z_3 \cdot (z_1 + z_2) = z_3 \cdot z_1 + z_3 \cdot z_2$$

Finalmente:

$(\mathbb{Q}(\sqrt{2}), +, \cdot)$ es un cuerpo □

Definición 1.2.3.3.

Hernández (2010) mencionó: "Si R es un campo un subcampo se define como un subconjunto de R que es a su vez un campo bajo las operaciones inducidas por el campo R " (p. 8).

Teorema 1.2.3.4.

Ferrando y Gregori (1995) mencionaron: "Sea H un subconjunto no vacío contenido en K. Entonces $(H, +, \cdot)$ es un subcuerpo de $(K, +, \cdot)$ si y sólo si $\forall x, y \in H$ se cumple que $x - y \in H$ y $\forall x, y \in H - \{0\}$ se cumple que $x \cdot y^{-1} \in H - \{0\}$" (p. 108).

Demostración. Veamos:

$(\Rightarrow)$ Tenemos: $(H, +, \cdot)$ es subcuerpo de $(K, +, \cdot)$

Sean $x, y \in H \Rightarrow \exists!\ -y \in H$

Por definición de cuerpo:

$$x - y = x + (-y) \in H$$

Además:

Sean $x, y \in H - \{0\} \Rightarrow \exists! y^{-1} \in H - \{0\}$

Por definición de cuerpo:

$$x \cdot y^{-1} \in H - \{0\}$$

$(\Leftarrow)$ Tenemos: $(K, +, \cdot)$ es cuerpo y $H \subset K$

Además:

$$\forall x, y \in H \Rightarrow x - y \in H \tag{1.27}$$

$$\forall x, y \in H - \{0\} \Rightarrow x \cdot y^{-1} \in H - \{0\} \tag{1.28}$$

Veamos que $(H, +, \cdot)$ es un cuerpo

a. Como $+$ es conmutativo en $K \Rightarrow +$ es conmutativo en H.
b. Como $+$ es asociativo en $K \Rightarrow +$ es asociativo en H.
c. En (1.27), tomando $y = x \in H$, reemplazando:

$$x - x = 0 \in H$$

Por lo tanto:

$$\forall\ x \in H,\ \exists!\ y = -x \in H\ /\ x + y = 0 = y + x$$

d. En (1.27), tomando $y = 0 \in H \Rightarrow \exists!\ -y = 0 \in H$, reemplazando:

$$x + 0 = x \in H$$

Por lo tanto:

$$\forall\ x \in H,\ \exists!\ 0 \in H\ /\ x + 0 = x = 0 + x$$

e. En (1.27), tomando $x, -y \in H$, reemplazando:

$$x-(-y)\in H$$

Por lo tanto:

$$x+y\in H$$

f. Como $\cdot$ es conmutativo en $K \Rightarrow \cdot$ es conmutativo en H .

g. Como $\cdot$ es asociativo en $K \Rightarrow \cdot$ es asociativo en H .

h. En (1.28), tomando $y=x\in H-\{0\}$, reemplazando:

$$x\cdot x^{-1}=e\in H-\{0\}$$

Por lo tanto:

$$\forall\, x\in H-\{0\},\ \exists!\ z=x^{-1}\in H\ /\ x\cdot z=e=z\cdot x$$

i. En (1.28), tomando $y=e\in H-\{0\}$, reemplazando:

$$x\cdot e^{-1}\in H-\{0\}$$

$$x\cdot e=x\in H-\{0\}$$

Por lo tanto:

$$\forall x\in H\ ,\ \exists!\ e\in H\ /\ x\cdot e=x=e\cdot x$$

j. En (1.28), tomando $x, y^{-1}\in H-\{0\}$, reemplazando:

$$x\cdot (y^{-1})^{-1}\in H-\{0\}$$

Por lo tanto:

$$x\cdot y\in H$$

k. Como las leyes distributivas se cumplen en K entonces se cumplen en H .

Finalmente:

$(H,+,\cdot)$ es subcuerpo de $(K,+,\cdot)$ □

Ejemplo 1.2.3.5. Sea $(\mathbb{C},+,\cdot)$ el cuerpo de los complejos y $\mathbb{Q}(i)=\{a+bi\in\mathbb{C}/a,b\in\mathbb{Q}\}$ el subconjunto de los complejos.

Entonces: $(\mathbb{Q}(i),+,\cdot)$ es el subcuerpo de los números complejos $(\mathbb{C},+,\cdot)$.

Demostración. Veamos:

1. Tenemos: $\mathbb{Q}(i)\subset\mathbb{C}$
2. Sean $z,w\in\mathbb{Q}(i)$ entonces:

$$\exists\ a,b\in\mathbb{Q}\ /\ z=a+bi\in\mathbb{C}\ \wedge\ \exists\ c,d\in\mathbb{Q}\ /\ w=c+di\in\mathbb{C}$$

Como $w\in\mathbb{C}\ \Rightarrow\ \exists!\ -w\in\mathbb{C}$

Luego:

$$z-w=(a+bi)-(c+di)=(a-c)+(b-d)i\in\mathbb{Q}(i)$$

3. Sean $z,w\in\mathbb{Q}(i)-\{0\}$ entonces:

$$\exists\ a,b\in\mathbb{Q}-\{0\}\ /\ z=a+bi\in\mathbb{C}\ \wedge\ \exists\ c,d\in\mathbb{Q}-\{0\}\ /\ w=c+di\in\mathbb{C}$$

Como $w\in\mathbb{C}\ \wedge\ w\neq 0\ \Rightarrow\ \exists!\ w^{-1}\in\mathbb{C}$

Luego:

$$z\cdot w^{-1}=(a+bi)\cdot(c+di)^{-1} \tag{1.29}$$

Veamos, quien es $(c+di)^{-1}$

Si: $(c+di)\cdot(\alpha+\beta i)=e$, donde $e=1+0i$ es la identidad en $\mathbb{C}$

Al desarrollar, obtendremos:

$$\alpha=\frac{c}{c^2+d^2}\ \wedge\ \beta=\frac{-d}{c^2+d^2}$$

Por lo tanto:

$$(c+di)^{-1}=\frac{c}{c^2+d^2}+\frac{-d}{c^2+d^2}i$$

Reemplazando en (1.29)

$$z\cdot w^{-1}=(a+bi)\cdot(\frac{c}{c^2+d^2}+\frac{-d}{c^2+d^2}i)\in\mathbb{Q}(i)-\{0\}$$

Finalmente, por el teorema 1.2.3.4. obtenemos:

$(\mathbb{Q}(i),+,\cdot)$ es el subcuerpo de $(\mathbb{C},+,\cdot)$ □

Proposición 1.2.3.6.

Castellanos (2013) mencionó: "Dados A anillo, $m\subset A$ ideal

m es maximal $\Leftrightarrow$ A/m es cuerpo" (p. 57).

Demostración. (Ver demostración en [3], pp. 57-58) □

Teorema 1.2.3.7.

Fraleigh (1987) mencionó: "Todo campo F es un dominio entero" (p. 217).

Demostración. Si F es un cuerpo entonces es un anillo conmutativo con identidad, solo falta demostrar que no existen divisores de cero.

Supongamos que F tiene divisores de cero, es decir, sean $a,b\in F-\{0\}$ tal que $a\cdot b=0$

Luego:

$$a\cdot b=0\ \Rightarrow\ a^{-1}(a\cdot b)=a^{-1}\cdot 0\ \Rightarrow\ (a^{-1}a)\cdot b=0\ \Rightarrow\ 1\cdot b=0\ \Rightarrow\ b=0\ (\Rightarrow\Leftarrow)$$

Entonces:

No existen divisores de cero

Por lo tanto:

F es un dominio entero

En general, se concluye que:

Todo cuerpo es un dominio entero □

Teorema 1.2.3.8.

Fraleigh (1987) mencionó: "Si F es un campo, todo ideal en $F[x]$ es principal" (p. 285).

Demostración. (Ver demostración en [7], p. 286) □

Corolario 1.2.3.9.

Zaldívar (1996) mencionó: "Si k es un campo, sus únicos ideales son el 0 y el total k" (p. 11).

Demostración. En primer lugar, demostraremos la siguiente afirmación que nos ayudará a probar esta proposición.

Afirmación: Los únicos ideales de k son $\{0\}$ y k.

En efecto:

Sea I un ideal de k.

Si $I=\{0\}$ queda demostrado.

Si $I\neq\{0\}$, entonces existe $x\in I$ con $x\neq 0$.

Entonces, para todo $a\in k$ (cuerpo), se puede expresar en la forma:

$$a=1\cdot a=(x^{-1}\cdot x)\cdot a=x^{-1}\cdot(x\cdot a)=x^{-1}\cdot(a\cdot x)=(x^{-1}\cdot a)\cdot x\in I$$

Luego:

$$k \subset I$$

Además, I es un ideal de k se tiene $I \subset k$.

Por lo tanto:

$$I = k$$

Finalmente:

Los únicos ideales de k son $\{0\}$ y k □

Observación 1.2.3.10.

Zaldívar (1996) mencionó: "Si k es un campo, entonces $0 \subseteq k$ es el único ideal máximo de k " (p. 14).

Demostración.

Sea M un ideal de k con $M \neq k$ entonces $M = \{0\}$

Sea I un ideal de k tal que $\{0\} \subset_{\neq} I \subset k$

Como I es un ideal de k entonces $I = \{0\}$ $(\Rightarrow\Leftarrow)$ $\vee$ $I = k$

$$I = k$$

Por lo tanto:

$$\{0\} \text{ es un ideal maximal de } k$$

Por otro lado, se puede ver que k no es ideal maximal de k, pues si suponemos que lo es, entonces:

$$k \subset_{\neq} I \subset k$$

$$I = k \ (\Rightarrow\Leftarrow)$$

Por lo tanto:

$\{0\}$ es el único ideal maximal de k □

Definición 1.2.3.11.

Fraleigh (1987) mencionó: "Un isomorfismo de un campo sobre sí mismo es un automorfismo del campo" (p. 371).

Teorema 1.2.3.12.

Revilla (2014) mencionó: Sea $f : K \to L$ un homomorfismo de cuerpos. Demostrar que:

1. $f(0) = 0$ y $f(-a) = -f(a)$, $\forall a \in K$.
2. $f(1) = 1$ y $f(a^{-1}) = f(a)^{-1}$, $\forall a \in K$, $a \neq 0$.
3. Im f es un subcuerpo de L.
4. f es inyectivo.

Demostración. Veamos:

1. Se deduce del hecho de ser f un homomorfismo entre los grupos aditivos de K y de L, es decir:

$$f(0) = f(0+0) = f(0) + f(0) \ \Rightarrow \ f(0) = 0$$

$$0 = f(0) = f(a+(-a)) = f(a) + f(-a) \ \Rightarrow \ f(-a) = -f(a)$$

2. Se deduce del hecho de ser f un homomorfismo entre los grupos multiplicativos de $K - \{0\}$ y de $L - \{0\}$, es decir:

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \;\Rightarrow\; f(1) = 1$$

$$1 = f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1}) \;\Rightarrow\; f(a^{-1}) = (f(a))^{-1}$$

3. Sea $z \in Im(f) \;\Rightarrow\; \exists\; a \in K \;/\; z = f(a) \in L$

   Entonces:

$$Im(f) \subset L \tag{1.30}$$

   Sean $z_1, z_2 \in Im(f) \;\Rightarrow\; \exists\; a, b \in K$ tal que:

$$z_1 = f(a) \;\wedge\; z_2 = f(b)$$

   Luego:

$$z_1 - z_2 = f(a) - f(b)$$

   Como f es homomorfismo de K en L, entonces:

$$z_1 - z_2 = f(a - b) \in Im(f)$$

   Entonces:

$$z_1 - z_2 \in Im(f) \tag{1.31}$$

   Sean $z_1, z_2 \in Im(f) - \{0\} \;\Rightarrow\; \exists\; a, b \in K - \{0\}$ tal que:

$$z_1 = f(a)\;,\; z_2 = f(b)$$

   Luego:

$$z_1 \cdot z_2^{-1} = f(a) \cdot (f(b))^{-1}$$

   De la parte (2) se tiene:

$$z_1 \cdot z_2^{-1} = f(a) \cdot f(b^{-1})$$

Como f es homomorfismo de K en L , entonces:

$$z_1 \cdot z_2^{-1} = f(a \cdot b^{-1}) \in Im(f) - \{0\}$$

Entonces:

$$z_1 \cdot z_2^{-1} \in Im(f) - \{0\} \qquad (1.32)$$

Finalmente, de (1.30), (1.31) y (1.32) se concluye por el teorema 1.2.3.4.

$Im(f)$ es subcuerpo de L

4. Tenemos que f es un homomorfismo de cuerpos entre K y L, demostremos que $Ker(f)$ es un ideal de K.

   En efecto: Veamos:

   a. Sea $x \in Ker(f) \Rightarrow x \in K \ / \ f(x) = 0$

      Por lo tanto:

      $$Ker(f) \subset K \qquad (1.33)$$

   b. Sean $x, y \in Ker(f) \Rightarrow f(x) = 0 \ \wedge \ f(y) = 0$

      $$f(x) - f(y) = 0$$

      Como f es un homomorfismo de cuerpos, entonces:

      $$f(x - y) = 0$$

      $$x - y \in Ker(f) \qquad (1.34)$$

   c. Sean $r \in K (f(r) \in L) \ \wedge \ x \in Ker(f) \Rightarrow f(x) = 0$

      Luego:

      $$f(r) \cdot f(x) = f(r) \cdot 0$$

      Como f es un homomorfismo de cuerpos, entonces:

      $$f(r \cdot x) = 0$$

$$r \cdot x \in Ker(f) \tag{1.35}$$

De forma análoga:

$$f(x) \cdot f(r) = 0 \cdot f(r)$$

Como f es un homomorfismo de cuerpos, entonces:

$$f(x \cdot r) = 0$$

$$x \cdot r \in Ker(f) \tag{1.36}$$

Por lo tanto, de (1.33), (1.34), (1.35) y (1.36) se obtiene:

$Ker(f)$ es un ideal de K

Luego, al ser K un cuerpo, en el corolario 1.2.3.9. hemos visto que sus únicos ideales son K y $\{0\}$ entonces:

$$Ker(f) = K \ \vee \ Ker(f) = \{0\}$$

Si: $Ker(f) = K$, entonces f sería el homomorfismo nulo, es decir:

$$Im(f) = \{0\} \ (\Rightarrow\Leftarrow)$$

Pues de la parte (3) se tiene que $Im(f) = \{0\}$ es subcuerpo de L pero $\{0\}$ no es cuerpo, luego $Ker(f) = \{0\}$

Por lo tanto:

f es inyectivo □

1.2.4. Teoría de Espacio Vectorial

Definición 1.2.4.1.

Lázaro (2005) mencionó:

Un conjunto V, no vacio, se llama ESPACIO VECTORIAL sobre K, si está provisto de dos operaciones: suma $(+)$ y producto $(\cdot)$, definidos de la siguiente manera:

$$+ : VxV \to V \qquad \cdot : KxV \to V$$

$$(u, v) \to u + v \qquad (\alpha, v) \to \alpha v$$

"La suma de dos vectores es otro vector" "El producto de un escalar por un vector, es otro vector"

y que cumple las siguientes propiedades:

A1) $u + v = v + u \ ; \ u, v \in V$

A2) $(u + v) + w = u + (v + w) \ ; \ u, v, w \in V$

A3) $\exists! 0 \in V / v + 0 = v \ , \ \forall v \in V$ (0 es el elemento cero)

A4) $\forall v \in V, \exists! - v / v + (-v) = 0$ ($-v$ se llama opuesto de v)

P1) $\alpha(\beta v) = (\alpha\beta)v \ , \ \forall \alpha, \beta \in K \ , \ v \in V$

P2) $1 \cdot v = v \ , \ \forall v \in V \ , \ 1 \in K$

DISTRIBUTIVIDAD:

D1) $(\alpha + \beta)v = \alpha v + \beta v \ , \ \alpha, \beta \in K \ ; \ v \in V$

D2) $\alpha(u + v) = \alpha u + \alpha v \ , \ \alpha \in K \ ; \ u, v \in K$. (pp. 95-96)

Ejemplo 1.2.4.2. Si $K = \mathbb{R}$, entonces $V = K^{nxm}$ el conjunto de matrices sobre $\mathbb{R}$ de orden nxm y con sus operaciones:

$$+ : VxV \to V$$

$$\cdot : KxV \to V$$

definidas de esta forma:

$$(a_{ij})_{nxm} + (b_{ij})_{nxm} = (a_{ij} + b_{ij})_{nxm}$$

$$\lambda \cdot (a_{ij})_{nxm} = (\lambda \cdot a_{ij})_{nxm}$$

es un $\mathbb{R}-$ espacio vectorial.

Demostración. Sean $K = \mathbb{R} \ \wedge \ A, B, C \in V = K^{nxm} \ \wedge \ \lambda, \beta \in K$

1. $A + B = (a_{ij})_{nxm} + (b_{ij})_{nxm} = (a_{ij} + b_{ij})_{nxm} \in V$
2. $(A+B)+C = ((a_{ij})_{nxm} + (b_{ij})_{nxm}) + (c_{ij})_{nxm}$

   Como en $\mathbb{R}$ se cumple la asociatividad, entonces:

   $(A+B)+C = (a_{ij})_{nxm} + ((b_{ij})_{nxm} + (c_{ij})_{nxm})$

   $(A+B)+C = A+(B+C)$

3. Sea $A \in \mathbb{R}^{nxm} \ \Rightarrow \ \exists \ (a_{ij})_{nxm} \in \mathbb{R}^{nxm} \ / \ A = (a_{ij})_{nxm}$

   Como $a_{ij} \in \mathbb{R} \ \Rightarrow \ \exists! \ 0_{ij} \in \mathbb{R} \ / \ a_{ij} + 0_{ij} = a_{ij} = 0_{ij} + a_{ij}$

   Luego:

   $$A = (a_{ij} + 0_{ij})_{nxm} \ \wedge \ A = (0_{ij} + a_{ij})_{nxm}$$

   $$A = (a_{ij})_{nxm} + (0_{ij})_{nxm} \ \wedge \ A = (0_{ij})_{nxm} + (a_{ij})_{nxm}$$

   $$A = A + 0 \ \wedge \ A = 0 + A$$

   Por lo tanto:

   $$\exists \ 0 \in \mathbb{R}^{nxm} \ / \ A + 0 = A = 0 + A$$

Unicidad:

Supongamos que existe $0' \in \mathbb{R}^{nxm} \ \wedge \ 0' \neq 0 \ / \ A+0' = A = 0' + A$

Por otro lado: $A+0 = A = 0+A$

Luego:

$$A+0 = A+0'$$

$$(a_{ij})_{nxm} + (0_{ij})_{nxm} = (a_{ij})_{nxm} + (0'_{ij})_{nxm}$$

$$(a_{ij} + 0_{ij})_{nxm} = (a_{ij} + 0'_{ij})_{nxm}$$

$$a_{ij} + 0_{ij} = a_{ij} + 0'_{ij}$$

$$0_{ij} = 0'_{ij}$$

$$(0_{ij})_{nxm} = (0'_{ij})_{nxm}$$

$$0 = 0' \ (\Rightarrow\Leftarrow)$$

4. Sea $A \in \mathbb{R}^{nxm} \ \Rightarrow \ \exists \ (a_{ij})_{nxm} \in \mathbb{R}^{nxm} \ / \ A = (a_{ij})_{nxm}$

   Como $a_{ij} \in \mathbb{R} \ \Rightarrow \ \exists! \ b_{ij} \in \mathbb{R} \ / \ a_{ij} + b_{ij} = 0_{ij} = b_{ij} + a_{ij}$

   Luego:

$$(a_{ij} + b_{ij})_{nxm} = (0_{ij})_{nxm} \ \wedge \ (b_{ij} + a_{ij})_{nxm} = (0_{ij})_{nxm}$$

$$(a_{ij})_{nxm} + (b_{ij})_{nxm} = (0_{ij})_{nxm} \ \wedge \ (b_{ij})_{nxm} + (a_{ij})_{nxm} = (0_{ij})_{nxm}$$

$$A+B = 0 \ \wedge \ B+A = 0$$

   Por lo tanto:

$$\exists\ B \in \mathbb{R}^{nxm}\ /\ A+B=0=B+A$$

Unicidad:

Supongamos que existe $C \in \mathbb{R}^{nxm}\ \wedge\ C \neq B\ /\ A+C=0=C+A$

Por otro lado: $A+B=0=B+A$

Luego:

$$A+C=A+B$$

$$(a_{ij})_{nxm}+(c_{ij})_{nxm}=(a_{ij})_{nxm}+(b_{ij})_{nxm}$$

$$(a_{ij}+c_{ij})_{nxm}=(a_{ij}+b_{ij})_{nxm}$$

$$a_{ij}+c_{ij}=a_{ij}+b_{ij}$$

$$c_{ij}=b_{ij}$$

$$(c_{ij})_{nxm}=(b_{ij})_{nxm}$$

$$C=B\ \ (\Rightarrow\Leftarrow)$$

5. $A+B=(a_{ij})_{nxm}+(b_{ij})_{nxm}$

   Como en $\mathbb{R}$ se cumple la conmutatividad, entonces:

$$A+B=(b_{ij})_{nxm}+(a_{ij})_{nxm}$$

   Por lo tanto:

$$A+B=B+A$$

6. $\lambda \cdot A=\lambda \cdot (a_{ij})_{nxm}=(\lambda \cdot a_{ij})_{nxm} \in V$

7. $(\lambda \cdot \beta) \cdot A = (\lambda \cdot \beta) \cdot (a_{ij})_{nxm} = ((\lambda \cdot \beta) \cdot a_{ij})_{nxm}$

   Como en $\mathbb{R}$ se cumple la asociatividad, entonces:

$$(\lambda \cdot \beta) \cdot A = (\lambda \cdot (\beta \cdot a_{ij}))_{nxm} = \lambda \cdot (\beta \cdot a_{ij})_{nxm} = \lambda \cdot (\beta \cdot (a_{ij})_{nxm})$$

$$(\lambda \cdot \beta) \cdot A = \lambda \cdot (\beta \cdot A)$$

8. Por la existencia única del elemento neutro e en $\mathbb{R}$ en la multiplicación, entonces:

$$e \cdot A = e \cdot (a_{ij})_{nxm} = (e \cdot a_{ij})_{nxm} = (a_{ij})_{nxm} = A$$

9. $\lambda \cdot (A+B) = \lambda \cdot ((a_{ij})_{nxm} + (b_{ij})_{nxm}) = \lambda \cdot ((a_{ij} + b_{ij})_{nxm})$

   $\lambda \cdot (A+B) = (\lambda \cdot (a_{ij} + b_{ij}))_{nxm}$

   Como en $\mathbb{R}$ se cumple la distribución, entonces:

$$\lambda \cdot (A+B) = (\lambda \cdot a_{ij} + \lambda \cdot b_{ij})_{nxm}$$

$$\lambda \cdot (A+B) = (\lambda \cdot a_{ij})_{nxm} + (\lambda \cdot b_{ij})_{nxm}$$

$$\lambda \cdot (A+B) = \lambda \cdot (a_{ij})_{nxm} + \lambda \cdot (b_{ij})_{nxm}$$

$$\lambda \cdot (A+B) = \lambda \cdot A + \lambda \cdot B$$

10. $(\lambda + \beta) \cdot A = (\lambda + \beta) \cdot (a_{ij})_{nxm} = ((\lambda + \beta) \cdot a_{ij})_{nxm}$

    Como en $\mathbb{R}$ se cumple la distribución, entonces:

$$(\lambda + \beta) \cdot A = (\lambda \cdot a_{ij} + \beta \cdot a_{ij})_{nxm} = (\lambda \cdot a_{ij})_{nxm} + (\beta \cdot a_{ij})_{nxm}$$

$$(\lambda + \beta) \cdot A = \lambda \cdot (a_{ij})_{nxm} + \beta \cdot (a_{ij})_{nxm}$$

$$(\lambda + \beta) \cdot A = \lambda \cdot A + \beta \cdot A$$

Finalmente:

$V = K^{nxm}$ es un $\mathbb{R}$ – espacio vectorial □

Definición 1.2.4.3.

Lázaro (2005) mencionó:

Sea V un $K-$ espacio vectorial.

Un subespacio vectorial de V es un subconjunto $W \subset V$, con las siguientes propiedades:

1. $0 \in W$
2. Si $(w_1 \in W \wedge w_2 \in W)$ entonces $(w_1 + w_2) \in W$.

   Esta propiedad indica que "Si dos vectores pertenecen al conjunto W, implica que la suma de dichos vectores también pertenece al conjunto W".
3. Si $v \in W$ entonces, para todo $\alpha \in K$, $\alpha v \in W$.

   Esta propiedad indica: "si α es un escalar cualquiera y w es un vector perteneciente a W, implica que el producto αw es un vector de W". (p. 97)

Ejemplo 1.2.4.4. Sea $\mathbb{R}^2$ un $\mathbb{R}-$espacio vectorial.

Sea $H = \{(a,b) \in \mathbb{R}^2 / a+b=0\}$ un subconjunto de $\mathbb{R}^2$. Entonces: H es un subespacio vectorial de $\mathbb{R}^2$.

Demostración. Veamos:

1. Sea $(0,0) \in \mathbb{R}^2$, $0+0=0 \Rightarrow (0,0) \in H$
2. Sean $u=(u_1,u_2)$, $v=(v_1,v_2) \in H$

   Entonces:

$$(u_1,u_2) \in \mathbb{R}^2 / u_1+u_2=0 \wedge (v_1,v_2) \in \mathbb{R}^2 / v_1+v_2=0$$

   Luego:

$$(u_1+v_1)+(u_2+v_2)=0$$

$$(u_1+v_1,u_2+v_2)\in H$$

$$(u_1,u_2)+(v_1,v_2)\in H$$

$$u+v\in H$$

3. Sean $v=(v_1,v_2)\in H \ \wedge \ \alpha\in\mathbb{R}$

   Entonces:

$$(v_1,v_2)\in\mathbb{R}^2/\ v_1+v_2=0$$

   Luego:

$$\alpha\cdot(v_1+v_2)=0$$

$$\alpha\cdot v_1+\alpha\cdot v_2=0$$

$$(\alpha\cdot v_1,\alpha\cdot v_2)\in H$$

$$\alpha\cdot(v_1,v_2)\in H$$

$$\alpha\cdot v\in H$$

Por lo tanto:

H es un subespacio vectorial de $\mathbb{R}^2$ □

Definición 1.2.4.5.

Lázaro (2005) mencionó: "Sea $v_1,v_2,\ldots,v_n$ un conjunto de vectores pertenecientes al espacio vectorial V.

Diremos que el vector $v\in V$ es COMBINACION LINEAL de los vectores $v_1,v_2,\ldots,v_n$, si existen escalares $\alpha_1,\alpha_2\ldots,\alpha_n$ tales que:

$v = \alpha_1.v_1 + \alpha_2.v_2 + \ldots + \alpha_n.v_n$ los α_i son únicos" (p. 105).

Ejemplo 1.2.4.6. El vector $(4,-9) \in \mathbb{R}^2$ es combinación lineal de $(2,-3)$ y $(0,-3)$.

Demostración. Podemos ver que:

$$(4,-9) = 2 \cdot (2,-3) + 1 \cdot (0,-3)$$

Por lo tanto:

$(4,-9)$ es combinación lineal de $(2,-3)$ y $(0,-3)$ □

Definición 1.2.4.7.

Lázaro (2005) mencionó: "Sean $v_1, v_2, \ldots, v_n$ vectores de un espacio vectorial V, definimos:

$$L\{v_1, v_2, \ldots, v_n\} = \{v \in V / v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n, \alpha_i \in K\}$$

Se lee "El espacio generado por $\{v_1, v_2, \ldots, v_n\}$ es el conjunto de combinaciones lineales de $v_1, v_2, \ldots, v_n$ "" (p. 107).

Ejemplo 1.2.4.8. Sea $\mathbb{R}^3$ un $\mathbb{R}-$ espacio vectorial.

Sea $W = \{(x,y,z) \in \mathbb{R}^3 / x - y - z = 0\}$ un subconjunto de $\mathbb{R}^3$, se puede ver que W es el espacio generado por los vectores $(1,1,0)$ y $(1,0,1)$.

Demostración. Veamos:

1. Sea $(u,v,w) \in W$ entonces $(u,v,w) \in \mathbb{R}^3 \ / \ u - v - w = 0$

   Luego:

$$(u,v,w) = (v+w,v,w) = v(1,1,0) + w(1,0,1)$$

$$(u,v,w) \in L\{(1,1,0),(1,0,1)\}$$

$$W \subset L\{(1,1,0),(1,0,1)\}$$

2. Sea $(x,y,z) \in L\{(1,1,0),(1,0,1)\}$ entonces existen λ , $\beta \in \mathbb{R}$ /

$$(x,y,z) = \lambda(1,1,0) + \beta(1,0,1)$$

$$(x,y,z) = (\lambda + \beta, \lambda, \beta)$$

$$x - y - z = 0$$

$$L\{(1,1,0),(1,0,1)\} \subset W$$

Entonces:

$$W = L\{(1,1,0),(1,0,1)\}$$

Por lo tanto:

W es el espacio generado por los vectores $(1,1,0)$ y $(1,0,1)$ □

Teorema 1.2.4.9.

Lázaro (2005) mencionó: " $L\{v_1, v_2, ..., v_n\}$ es un subespacio de V " (p. 107).

Demostración. (Ver demostración en [9], p. 163) □

Definición 1.2.4.10.

Lázaro (2005) mencionó: "Sea $S = \{v_1, v_2, ..., v_n\}$ un subconjunto de vectores distintos de un espacio vectorial V.

Diremos que el conjunto S es LINEALMENTE DEPENDIENTES (l.d.) si existen n escalares $\alpha_1, \alpha_2, \ldots, \alpha_n$, no todos cero, tales que:

$\alpha_1.v_1 + \alpha_2.v_2 + ... + \alpha_n.v_n = 0$ (vector nulo)" (p. 110).

Ejemplo 1.2.4.11. Dados los vectores $(-6, -\frac{3}{2}, 9)$ y $(4,1,-6)$ de $\mathbb{R}^3$, entonces: $(-6, -\frac{3}{2}, 9)$ y $(4,1,-6)$ son L.D.

Demostración. Veamos:

$$\lambda\cdot(-6,-\frac{3}{2},9)+\beta\cdot(4,1,-6)=(0,0,0)$$

$$(-6\lambda+4\beta,-\frac{3}{2}\lambda+\beta,9\lambda-6\beta)=(0,0,0)$$

Luego:

$$\lambda=\frac{2}{3}\beta$$

Por lo tanto:

$(-6,-\frac{3}{2},9)$ y $(4,1,-6)$ son L.D. □

Definición 1.2.4.12.

Lázaro (2005) mencionó: "Un conjunto S que no es linealmente dependiente se define linealmente independiente.

Dicho de otra manera:

$S=\{v_1,v_2,...,v_n\}$ es LINEALMENTE INDEPENDIENTE (l.i) si la ecuación

$\alpha_1.v_1+\alpha_2.v_2+...+\alpha_n.v_n=0$ implica $\alpha_1=\alpha_2=...=\alpha_n=0$" (p. 110).

Ejemplo 1.2.4.13. Dados los vectores $(3,-8)$ y $(-2,3)$ de $\mathbb{R}^2$, entonces: $(3,-8)$ y $(-2,3)$ son L.I.

Demostración. Veamos: $\lambda(3,-8)+\beta(-2,3)=(0,0)$

$$(3\lambda-2\beta,-8\lambda+3\beta)=(0,0)$$

$$3\lambda-2\beta=0\ \wedge\ -8\lambda+3\beta=0$$

$$\lambda=\beta=0$$

Por lo tanto:

$(3,-8)$ y $(-2,3)$ son L.I. □

Definición 1.2.4.14.

Lázaro (2005) mencionó: "Sea V un $K-$ espacio vectorial y $S=\{v_1,v_2,...,v_n\}$ un subconjunto de V.

Diremos que el conjunto de vectores $S=\{v_1,v_2,...,v_n\}$ es una BASE del espacio vectorial V, si:

1. $\{v_1,v_2,...,v_n\}$ es linealmente independiente
2. $\{v_1,v_2,...,v_n\}$ genera V. Esto es: $V=L\{v_1,...,v_n\}$

El espacio V es de dimensión finita si tiene una base finita" (p. 111).

Ejemplo 1.2.4.15. Sea $V=\{a_0+a_1t+a_2cos2t+a_3e^{3t}/\ a_i\in\mathbb{R},t\in\mathbb{R}\}$ un $\mathbb{R}$-espacio vectorial. Veamos que las funciones:

$$f_1(t)=2t-1,\ f_2(t)=t+cos2t,\ f_3(t)=3+e^{3t},\ f_4(t)=-t+e^{3t}$$

constituyen una base de V.

Demostración. Demostraremos las dos siguientes condiciones para que

$\{f_1(t),f_2(t),f_3(t),f_4(t)\}$ sea una base de V.

Afirmación 1: $\{f_1(t),f_2(t),f_3(t),f_4(t)\}$ genera V.

En efecto:

Sea $g(t)\in V\ \Rightarrow\ \exists\ k_0,k_1,k_2,k_3\in\mathbb{R}\ /\ g(t)=k_0+k_1t+k_2cos2t+k_3e^{3t}$

Veamos si $g(t)$ es combinación lineal de $f_1(t),f_2(t),f_3(t),f_4(t)$.

$$g(t) = k_0 + k_1 t + k_2 cos 2t + k_3 e^{3t} = af_1(t) + bf_2(t) + cf_3(t) + df_4(t)$$

$$k_0 + k_1 t + k_2 cos 2t + k_3 e^{3t} = a(2t-1) + b(t + cos 2t) + c(3 + e^{3t}) + d(-t + e^{3t})$$

$$k_0 + k_1 t + k_2 cos 2t + k_3 e^{3t} = (-a + 3c) + (2a + b - d)t + b cos 2t + (c + d)e^{3t}$$

Igualando se tiene el siguiente sistema de ecuaciones:

$$-a + 3c = k_0$$

$$2a + b - d = k_1$$

$$b = k_2$$

$$c + d = k_3$$

Resolviendo el sistema de ecuaciones, se obtiene:

$$a = \frac{1}{7}(-k_0 + 3k_1 - 3k_2 + 3k_3)$$

$$b = k_2$$

$$c = \frac{1}{7}(2k_0 + k_1 - k_2 + k_3)$$

$$d = -\frac{1}{7}(2k_0 + k_1 - k_2 - 6k_3)$$

Entonces, existen escalares $a, b, c, d \in \mathbb{R}$ tal que $g(t) = af_1(t) + bf_2(t) + cf_3(t) + df_4(t)$

Por lo tanto:

$$V \subset L\{f_1(t), f_2(t), f_3(t), f_4(t)\}$$

Además, por el teorema 1.2.4.9. se tiene:

$$L\{f_1(t), f_2(t), f_3(t), f_4(t)\} \subset V$$

Entonces:

$$V = L\{f_1(t), f_2(t), f_3(t), f_4(t)\}$$

Por lo tanto:

$\{f_1(t), f_2(t), f_3(t), f_4(t)\}$ genera V.

Afirmación 2: $\{f_1(t), f_2(t), f_3(t), f_4(t)\}$ es L.I.

Veamos: Supongamos que:

$$c_1 f_1(t) + c_2 f_2(t) + c_3 f_3(t) + c_4 f_4(t) = 0$$

$$c_1(2t-1) + c_2(t + cos2t) + c_3(3 + e^{3t}) + c_4(-t + e^{3t}) = 0$$

$$(-c_1 + 3c_3) + (2c_1 + c_2 - c_4)t + c_2 cos2t + (c_3 + c_4)e^{3t} = 0$$

Igualando se tiene el siguiente sistema de ecuaciones:

$$-c_1 + c_3 = 0$$

$$2c_1 + c_2 - c_4 = 0$$

$$c_2 = 0$$

$$c_3 + c_4 = 0$$

Resolviendo el sistema de ecuaciones, se obtiene:

$$c_1 = c_2 = c_3 = c_4 = 0$$

Por lo tanto:

$\{f_1(t), f_2(t), f_3(t), f_4(t)\}$ es L.I.

Finalmente, de la afirmación 1 y 2, se obtiene:

$\{f_1(t), f_2(t), f_3(t), f_4(t)\}$ es una base de V □

Definición 1.2.4.16.

Fraleigh (1987) mencionó: "Si V es un espacio vectorial de dimensión finita sobre un campo F, el número de elementos en una base (por teorema 36.3, es independiente de la selección de la base) es la dimensión de V sobre F" (p. 337).

Ejemplo 1.2.4.17. Sea $V = \{a_0 + a_1 t + a_2 cos 2t + a_3 e^{3t} / a_i \in \mathbb{R}, t \in \mathbb{R}\}$ un $\mathbb{R}-$ espacio vectorial, entonces $dim_K V = 4$.

Demostración. Del ejemplo 1.2.4.15. hemos obtenido que:

$$f_1(t) = 2t - 1,\ f_2(t) = t + cos 2t,\ f_3(t) = 3 + e^{3t},\ f_4(t) = -t + e^{3t}$$

constituyen una base de V.

Por lo tanto:

$$dim_K V = 4$$ □

Corolario 1.2.4.18.

Hoffman K. y Kunze R. (1973) mencionaron: "Sea V un espacio vectorial de dimensión finita y sea $n = dim V$. Entonces

1. cualquier subconjunto de V que contenga más de n vectores es linealmente dependiente;
2. ningún subconjunto de V que contenga menos de n vectores puede generar V" (pp. 44-45).

Demostración. (Ver demostración en [10], pp. 44-45) □

Definición 1.2.4.19.

Herstein (1970) mencionó: "Si U y V son espacios vectoriales sobre F, entonces la aplicación T de U en V se dice que es un homomorfismo si

1. $(u_1+u_2)T=u_1T+u_2T$
2. $(\alpha u_1)T=\alpha(u_1T)$

para cualesquiera $u_1,u_2\in U$, y $\alpha\in F$" (p. 158).

Ejemplo 1.2.4.20. Dado $f:\mathbb{R}[x]\to\mathbb{R}$ una aplicación tal que:

$$f(a_0+a_1x+\ldots+a_nx^n)=a_0$$

entonces f es un homomorfismo de espacios vectoriales.

Demostración. Sea $\lambda\in\mathbb{R}$ y sean:

$p(x)=c_0+c_1x+\ldots+c_nx^n\in\mathbb{R}[x]$, para algún $c_i\in\mathbb{R}$, $i=0,1,\ldots,n$

$q(x)=d_0+d_1x+\ldots+d_nx^n\in\mathbb{R}[x]$, para algún $d_i\in\mathbb{R}$, $i=0,1,\ldots,n$

Entonces:

1. $f(p(x)+q(x))=f((c_0+c_1x+\ldots+c_nx^n)+(d_0+d_1x+\ldots+d_nx^n))$

   $f(p(x)+q(x))=f((c_0+d_0)+(c_1+d_1)x+\ldots+(c_n+d_n)x^n)$

   Por la definición de f se tiene:

   $f(p(x)+q(x))=c_0+d_0$

   $f(p(x)+q(x))=f(c_0+c_1x+\ldots+c_nx^n)+f(d_0+d_1x+\ldots+d_nx^n)$

   Entonces:

$$f(p(x)+q(x))=f(p(x))+f(q(x))$$

2. $f(\lambda \cdot p(x)) = f(\lambda \cdot (c_0 + c_1 x + \ldots + c_n x^n))$

$f(\lambda \cdot p(x)) = f(\lambda \cdot c_0 + \lambda \cdot c_1 x + \ldots + \lambda \cdot c_n x^n)$

Por definición de f se tiene:

$$f(\lambda \cdot p(x)) = \lambda \cdot c_0 = \lambda \cdot f(c_0 + c_1 x + \ldots + c_n x^n)$$

Entonces:

$$f(\lambda \cdot p(x)) = \lambda \cdot f(p(x))$$

Por lo tanto:

f es un homomorfismo de espacios vectoriales □

1.2.5. Teoría de Cuerpos

Definición 1.2.5.1.

Zaldivar (1996) mencionó: "Si k y K campos tal que $k \subseteq K$ y las operaciones $(+,\cdot)$ de k son las mismas que las de K, entonces diremos que k es un subcampo de K o que K es una extensión de k" (p. 48).

Ejemplo 1.2.5.2. Ya hemos visto que $\mathbb{Q}$ es subcuerpo de $\mathbb{Q}(\sqrt{2})$.

Observación 1.2.5.3.

Zaldivar (1996) mencionó: "Si K/k es una extensión de campos, entonces con las operaciones de campo de K, K es un espacio vectorial sobre k (de hecho, al multiplicar por un escalar $\lambda \in k$, un elemento $v \in K$, se considera $\lambda \in K$ y al producto de K: $\lambda v \in K$)" (p. 48).

Definición 1.2.5.4.

Zaldivar (1996) mencionó: "A la dimensión $\dim_k K$ de K como espacio vectorial sobre k se le llama el grado de la extensión K/k y lo denotaremos por $[K:k]$. Por supuesto que esta dimensión puede ser finita ó infinita" (p. 48).

Observación 1.2.5.5.

Fraleigh (1987) mencionó: "Usaremos a menudo el hecho de que si E es una extensión finita de F, entonces $[E:F]=1$ si y sólo si $E=F$" (p. 348).

Demostración. (Ver demostración en [7], p. 348) □

Teorema 1.2.5.6.

Herstein (1970) mencionó: "Si L es una extensión finita de K y K una extensión finita de F, entonces L es una extensión finita de F. Además, $[L:F]=[L:K][K:F]$" (p. 198).

Demostración. Para que $\{x_i \cdot y_j\}_{(i,j)\in I_r \times I_s}$ sea una base para L sobre F, tenemos que demostrar que sea un generador para L sobre F y sea Linealmente Independiente.

Afirmación 1: $\{x_i \cdot y_j\}_{(i,j)\in I_r \times I_s}$ es un generador para L sobre F

En efecto:

$(\subset)$ Sea $z \in L$ y $\{y_j\}_{j\in I_s}$ es una base para L sobre K, entonces:

$$\exists\ a_j \in K \text{ (no todos ceros) } / \ z=\sum_{j\in I_s} a_j \cdot y_j\ ;\ \forall\ j\in I_s$$

Como $a_j \in K$ y $\{x_i\}_{i\in I_r}$ es una base para K sobre F, entonces:

$$\exists\ b_{ij} \in F \text{ (no todos ceros) } / \ a_j=\sum_{i\in I_r} b_{ij} \cdot x_i\ ;\ \forall\ i\in I_r$$

Reemplazando:

$$z = \sum_{j \in I_s} \sum_{i \in I_r} b_{ij} \cdot (x_i \cdot y_j)$$

Por lo tanto:

$$L \subset L\left\{\left\{x_i \cdot y_j\right\}_{(i,j) \in I_r x I_s}\right\}$$

$(\supset)$ Usando el teorema 1.2.4.9. obtenemos:

$$L\left\{\left\{x_i \cdot y_j\right\}_{(i,j) \in I_r x I_s}\right\} \subset L$$

Finalmente, de $(\subset)$ y $(\supset)$ obtenemos:

$$L = L\left\{\left\{x_i \cdot y_j\right\}_{(i,j) \in I_r x I_s}\right\}$$

Es decir:

$\left\{x_i \cdot y_j\right\}_{(i,j) \in I_r x I_s}$ es un generador para L sobre F

Afirmación 2: $\left\{x_i \cdot y_j\right\}_{(i,j) \in I_r x I_s}$ es Linealmente Independiente

En efecto:

Sean $\left\{c_{ij}\right\}_{(i,j) \in I_r x I_s}$ una familia de elementos de F tal que:

$$\sum_{j \in I_s} \sum_{i \in I_r} c_{ij} \cdot (x_i \cdot y_j) = 0$$

Como $\left\{y_j\right\}_{j \in I_s}$ es una base para L sobre K, entonces:

$$\sum_{i \in I_r} c_{ij} \cdot x_i = 0 \ ; \ \forall \ j \in I_s$$

Como $\left\{x_i\right\}_{i \in I_r}$ es una base para K sobre F, entonces:

$$c_{ij} = 0 ; \ \forall \ i \in I_r , \ \forall \ j \in I_s$$

Por lo tanto:

$\{x_i \cdot y_j\}_{(i,j)\in I,xI_s}$ es Linealmente Independiente

Finalmente, de las Afirmaciones 1 y 2, se obtiene:

$\{x_i \cdot y_j\}_{(i,j)\in I,xI_s}$ es una base para L sobre F

Afirmación 3: $[L:F]=[L:K]\cdot[K:F]$

En efecto:

Podemos ver que:

$$[L:F]=dim_F L=s\cdot r$$

Por otro lado:

$$[L:K]=dim_K L=s \ \wedge [K:F]=dim_F K=r$$

Por lo tanto:

$$[L:F]=[L:K]\cdot[K:F]$$ □

Corolario 1.2.5.7.

Lang (1971) mencionó: "La extensión E de k es finita si, y solo si, E es finita sobre F y F es finita sobre k" (p. 193).

Demostración. Veamos:

$(\Leftrightarrow)$ Del teorema 1.2.5.6. se tiene:

$$[E:k]=[E:F]\cdot[F:k]<\infty$$

Entonces:

$$[E:F]<\infty \ \wedge [F:k]<\infty$$

Por lo tanto:

$$E / F \text{ es finito y } F / k \text{ es finito} \qquad \square$$

Observación 1.2.5.8.

Lang (1971) mencionó: “Como para los grupos, definimos una torre de cuerpos como una sucesión

$$F_1 \subset F_2 \subset \ldots \subset F_n$$

de cuerpos extensión” (p. 193).

Corolario 1.2.5.9.

Fraleigh (1987) mencionó: “Si F_i es un campo para $i = 1, \ldots, r$ y F_{i+1} es una extensión finita de F_i, entonces F_r es una extensión finita de F_1 y

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \ldots [F_2 : F_1]$$” (p. 350).

Demostración. Sea:

$$A = \{r \in \mathbb{N} / \, F_{i+1} / F_i, \forall i = 1, 2, \ldots, r \text{ (finitos)} \Rightarrow F_r / F_1 \text{ es finito}\}$$

Si $r = 1$:

Tenemos inmediatamente:

$$F_2 / F_1 \text{ es finito}$$

Si $r = 2$:

Tenemos:

$$F_{i+1} / F_i, \; i = 1, 2 \text{ son finitos}$$

$$F_3 / F_2 \ \wedge \ F_2 / F_1 \text{ son finitos}$$

Por el corolario 1.2.5.7. se tiene que:

$$F_3 / F_1 \text{ es finito}$$

Si $r = h$ (Hipótesis Inductiva)

$$F_{i+1} / F_i, \ \forall i = 1, 2, \ldots, h \text{ (finitos)} \ \Rightarrow \ F_{h+1} / F_1 \text{ es finito}$$

Si $r = h+1$:

Si $F_{i+1} / F_i, \ \forall i = 1, 2, \ldots, h+1$ (finitos) demostraremos que F_{h+2} / F_1 es finito

En efecto:

Tenemos:

$$F_{i+1} / F_i, \ \forall i = 1, 2, \ldots, h+1 \text{ (finitos)}$$

Entonces:

$$F_{i+1} / F_i, \ \forall i = 1, 2, \ldots, h \ \text{ (finitos)} \ \wedge \ F_{h+2} / F_{h+1} \text{ (finito)}$$

De la Hipótesis Inductiva se tiene que:

$$F_{h+1} / F_1 \text{ es finito}$$

Por el corolario 1.2.5.7. se tiene que:

$$F_{h+2} / F_1 \text{ es finito}$$

Por lo tanto:

$$A = \mathbb{N}$$

Además, haciendo inducción en el teorema 1.2.5.6. se tiene:

$$[F_r : F_1] = [F_r : F_{r-1}] \ldots [F_2 : F_1] \qquad \square$$

Definición 1.2.5.10.

Herstein (1970) mencionó: "Si $p(x) \in F[x]$ entonces un elemento a que se encuentra en algún campo extensión del F se llama raíz de $p(x)$ si $p(a) = 0$ " (p. 210).

Lema 1.2.5.11.

Herstein (1970) mencionó: "Si $p(x) \in F[x]$ y si K es una extensión de F, entonces para cualquier elemento $b \in K$, $p(x) = (x-b)q(x) + p(b)$, donde $q(x) \in K[x]$ y donde

$\deg q(x) = \deg p(x) - 1$" (p. 210).

Demostración. Sea K / F una extensión de cuerpo y $b \in K$.

Como $F \subset K \Rightarrow F[x] \subset K[x]$.

Como $p(x) \in F[x] \Rightarrow p(x) \in K[x] \wedge x - b \in K[x]$.

Luego, por el algoritmo de la división para polinomios en $K[x]$:

$$\exists q(x), r(x) \in K[x] / \; p(x) = (x-b)q(x) + r(x) \qquad (1.37)$$

Donde: $r(x) = 0 \vee \deg r(x) < \deg(x-b) = 1$

Entonces:

$$r = r(x)$$

Reemplazando en (1.37)

$$p(x) = (x-b)q(x) + r \qquad (1.38)$$

Evaluando el polinomio en b se tiene:

$$p(b) = (b-b)q(b)+r$$

$$p(b) = r$$

Reemplazando en (1.38) se obtiene:

$$p(x) = (x-b)q(x) + p(b)$$

Además, tomando límite al residuo cuando tienda a cero, se tiene:

$$p(x) = (x-b)q(x)$$

Luego:

$$\deg\, p(x) = \deg((x-b)q(x))$$

Por el lema 1.2.2.47. se tiene:

$$\deg\, p(x) = \deg(x-b) + \deg\, q(x)$$

Por lo tanto:

$$\deg\, p(x) = 1 + \deg\, q(x)$$

Es decir:

$$\deg\, q(x) = \deg\, p(x) - 1$$ □

Corolario 1.2.5.12.

Herstein (1970) mencionó: "Si $a \in K$ es una raíz de $p(x) \in F[x]$, donde $F \subset K$, entonces en $K[x]$, $(x-a) \mid p(x)$ " (p. 211).

Demostración. De acuerdo con el lema 1.2.5.11. en $K[x]$ se tiene:

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

Como $a \in K$ es raíz de $p(x)$, se tiene:

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

Por lo tanto:

$$(x-a) \mid p(x)$$ □

Definición 1.2.5.13.

Herstein (1970) mencionó: "El elemento $a \in K$ es una raíz de $p(x) \in F[x]$ de multiplicidad m si $(x-a)^m \mid p(x)$, mientras que $(x-a)^{m+1} \nmid p(x)$" (p. 211).

Observación 1.2.5.14.

Lang (1971) mencionó: "Si $p(X)$ es un polinomio irreducible de $k[X]$ que divide a $f(X)$, toda raíz de $p(X)$ será también raíz de $f(X)$, por lo que podemos limitarnos a considerar polinomios irreducibles" (p. 199).

Demostración. Como $p(X) \mid f(X)$ entonces existe $q(X) \in k[X]$ tal que

$$f(X) = q(X) \cdot p(X)$$

Sea α una raíz arbitraria de $p(X)$, entonces:

$$f(\alpha) = q(\alpha) \cdot p(\alpha)$$

$$f(\alpha) = q(\alpha) \cdot 0$$

$$f(\alpha) = 0$$

Por lo tanto:

α es una raíz arbitraria de $f(X)$ □

Teorema 1.2.5.15.

Herstein (1970) mencionó: "Si $p(x)$ es un polinomio en $F[x]$ de grado $n \geq 1$ y es irreducible sobre F, entonces hay una extensión E de F tal que $[E:F]=n$ en que $p(x)$ tiene una raíz" (p. 212).

Demostración. Como F es cuerpo, por el teorema 1.2.3.8. se tiene $F[x]$ es DIP. Por el teorema 1.2.2.31. $F[x]$ es DFU.

Sea $p(x) \in F[x]$ un polinomio irreducible con $\deg p(x) = n \geq 1$.

Como $p(x)$ es irreducible, por la proposición 1.2.2.50. se tiene $< p(x) >$ es un ideal primo y por la proposición 1.2.2.51. se tiene $< p(x) >$ es un ideal maximal en $F[x]$.

Por la proposición 1.2.3.6. se tiene:

$$\exists \text{ un cuerpo } E = \frac{F[x]}{< p(x) >}$$

Ahora, definamos la aplicación:

$$\sigma : F[x] \to \frac{F[x]}{< p(x) >} = E \ / \ \sigma(f(x)) = f(x) + < p(x) >$$

Usaremos la restricción a K:

$$\sigma|_F : F \to \frac{F[x]}{< p(x) >} = E \ / \ \sigma|_F (a) = a + < p(x) >$$

Afirmación 1: $\sigma|_F$ es un homomorfismo de cuerpos

En efecto:

Sean $a, b \in F$

$$\sigma|_F(a+b)=(a+b)+<p(x)>=(a+<p(x)>)+(b+<p(x)>)$$

$$\sigma|_F(a+b)=\sigma|_F(a)+\sigma|_F(b)$$

Además:

$$\sigma|_F(a\cdot b)=(a\cdot b)+<p(x)>=(a+<p(x)>)\cdot(b+<p(x)>)$$

$$\sigma|_F(a\cdot b)=\sigma|_F(a)\cdot\sigma|_F(b)$$

Por lo tanto:

$\sigma|_F$ es un homomorfismo de cuerpos

Afirmación 2: $\sigma|_F$ es inyectiva

En efecto:

Como F, E son cuerpos y $\sigma|_F$ es un homomorfismo de cuerpos, por el teorema 1.2.3.12. (parte 4) se concluye:

$\sigma|_F$ es inyectiva

Afirmación 3: F es subcuerpo de E

En efecto:

Sabemos que F y E son cuerpos, solo falta demostrar que $F\subset E$

Sea $a\in F$, entonces:

$$\sigma|_F(a)\in E$$

$$a+<p(x)>\in E$$

$$a\in a+<p(x)>\in E$$

$$a \in E$$

Por lo tanto:

$$F \subset E$$

Finalmente:

F es subcuerpo de E

Es decir, demostramos que E / F es una extensión de cuerpo, ahora probemos:

Afirmación 4: $[E : F] = n$

En efecto:

Sabemos que E / F es una extensión de cuerpo.

Veamos que

$$S = \left\{1 + < p(x) >, x + < p(x) >, \ldots, (x + < p(x) >)^{n-1}\right\} \subset E$$

es una base de E sobre F

a. $E = L\{S\}$

En efecto:

Por el teorema 1.2.4.9. se tiene que: $L\{S\} \subset E$

Por otro lado:

Sea $q(x) \in E = \dfrac{F[x]}{< p(x) >} \Rightarrow \exists\ r(x) \in F[x]$ tal que

$$q(x) = r(x) + < p(x) >$$

$$q(x) = (c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}) + < p(x) >$$

$$q(x) = (c_0 + < p(x) >) + (c_1 x + < p(x) >) + \ldots + (c_{n-1} x^{n-1} + < p(x) >)$$

$$q(x) = c_0(1 + < p(x) >) + c_1(x + < p(x) >) + \ldots + c_{n-1}(x^{n-1} + < p(x) >)$$

$$q(x) = c_0(1 + < p(x) >) + c_1(x + < p(x) >) + \ldots + c_{n-1}(x + < p(x) >)^{n-1}$$

Por definición de espacio generado, se tiene:

$$q(x) \in L\{S\}$$

Por lo tanto:

$$E \subset L\{S\}$$

Se concluye:

$$E = L\{S\}$$

b. S es Linealmente Independiente

En efecto:

$$\lambda_0(1 + < p(x) >) + \ldots + \lambda_{n-1}(x + < p(x) >)^{n-1} = 0$$

$$(\lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1} x^{n-1}) + < p(x) >= 0$$

Como $\sigma|_F$ es homomorfismo, por el teorema 1.2.3.12. se tiene:

$$\sigma|_F\,(\lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1} x^{n-1}) = \sigma|_F\,(0)$$

Como $\sigma|_F$ es inyectiva, entonces:

$$\lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1} x^{n-1} = 0$$

Entonces:

$$\lambda_i = 0 \quad \forall i = 0, 1, \ldots, n-1$$

Por lo tanto:

S es Linealmente Independiente

Con esto, hemos demostrado que:

$$S = \left\{1 + < p(x) >, x + < p(x) >, \ldots, (x + < p(x) >)^{n-1}\right\}$$

es una base de E sobre F

Además:

$$[E : F] = dim_F E = n = \deg p(x)$$

Ahora probemos que $p(x)$ tiene una raíz en E .

Afirmación 5: Existe $\alpha \in E \ / \ p(\alpha) = 0$

En efecto:

Llamemos: $\alpha = x + < p(x) > \in E$

Sea el homomorfismo de evaluación:

$$\sigma_\alpha : F[x] \to \frac{F[x]}{< p(x) >} \text{ tal que } \sigma_\alpha(p(x)) = p(\alpha)$$

Se puede ver:

$\sigma_\alpha(p(x)) = p(x) + < p(x) >= p(x) + q(x) \cdot p(x)$, para algún $q(x) \in F[x]$

$$\sigma_\alpha(p(x)) = (1 + q(x)) \cdot p(x)$$

$$\sigma_\alpha(p(x)) \in < p(x) >$$

$$\sigma_\alpha(p(x)) = 0$$

$$p(\alpha) = 0$$

Por lo tanto:

$$\exists\ \alpha \in E\ /\ p(\alpha) = 0$$ □

Corolario 1.2.5.16.

Herstein (1970) mencionó: "Si $f(x) \in F[x]$, entonces hay una extensión finita E de F en que $f(x)$ tiene una raíz. Además, $[E:F] \leq \deg f(x)$" (p. 213).

Demostración. Sea $f(x) \in F[x]$ con $\deg f(x) = n \geq 1$.

Sea $p(x) \in F[x]$ un factor irreducible de $f(x)$ con $\deg p(x) \leq \deg f(x)$. Usando el teorema 1.2.5.15. existe una extensión finita E/F con:

$$[E:F] = \deg p(x) \leq \deg f(x)$$

$$[E:F] \leq \deg f(x)$$

Además:

$$\exists\ \alpha \in E\ /\ \alpha \text{ es raíz de } p(x)$$

De la observación 1.2.5.14. se tiene que cualquier raíz de $p(x)$ es una raíz de $f(x)$.

Por lo tanto:

$$\exists\ \alpha \in E\ /\ \alpha \text{ es raíz de } f(x)$$ □

Corolario 1.2.5.17.

Lang (1971) mencionó: "Sea k un cuerpo, y $f_1, \ldots, f_n$, polinomios de $k[X]$ de grados ≥ 1. Existe una extensión E de k en la que cada f_i tiene una raíz, $i = 1, \ldots, n$" (p. 200).

Demostración. Sea k un cuerpo y $f_i(x) \in k[x]$ (irreducibles) $\forall i = 1, \ldots, n$ de grados $n \geq 1$

Definamos:

$$A = \{n \in \mathbb{N} / \ f_n(x) \in k[x] \text{ tiene una raíz en } E, \text{ para algún } E/k \text{ (extensión)}\}$$

Procediendo por inducción:

a. Si $n = 1$

   Si k es un cuerpo y $f_1(X) \in k[X]$ (irreducible) de grado $n \geq 1$, del teorema 1.2.5.15. se obtiene que existe E/k (extensión) tal que $f_1(X)$ tiene una raíz en E

b. Si $n = h$ (Hipótesis Inductiva)

   Si k es un cuerpo y $f_1(X), f_2(X), \ldots, f_h(X) \in k[X]$ (irreducibles) de grados $n \geq 1$, entonces existe F/k (extensión) tal que $f_j(X)$ tiene una raíz en F; $\forall j = 1, 2, \ldots, h$

c. Si $n = h+1$

   Si k es un cuerpo y $f_1(X), f_2(X), \ldots, f_h(X), f_{h+1}(X) \in k[X]$ (irreducibles) de grados $n \geq 1$, demostraremos que existe E/k (extensión) tal que $f_j(X)$ tiene una raíz en E; $\forall j = 1, 2, \ldots, h+1$

   En efecto:

   Sea $f_{h+1}(X) \in k[X] \subset F[X]$ (irreducible) de grado $n \geq 1$, por el teorema 1.2.5.15. se obtiene que existe E/F (extensión) tal que $f_{h+1}(X)$ tiene una raíz en E.

   De la Hipótesis Inductiva se tiene que:

   $f_1(X), \ldots, f_h(X) \in k[X]$ (irreducibles) de grados $n \geq 1$ tienen una raíz en F. Pero, si $f_1(X), \ldots, f_h(X)$ tienen una raíz en $F \subset E$ entonces tienen una raíz en E.

   Por lo tanto:

$f_1(X), f_2(X), \ldots, f_h(X), f_{h+1}(X) \in k[X]$ (irreducibles) de grados $n \geq 1$ tienen una raíz en E

Finalmente:

$$A = \mathbb{N} \qquad \square$$

Teorema 1.2.5.18.

Herstein (1970) mencionó: "Sea $f(x) \in F[x]$ de grado $n \geq 1$. Entonces hay una extensión E de F de grado cuando más $n!$ en que $f(x)$ tiene n raíces (y, por tanto, un juego completo de raíces)" (p. 213).

Demostración. Sea $f(x) \in F[x]$ con $\deg f(x) = n \geq 1$, por el corolario 1.2.5.16. existe una extensión finita L_1 / F tal que $[L_1 : F] \leq \deg f(x) = n$ y además $f(x)$ tiene una raíz $\alpha_1 \in L_1$. Así pues, en $L_1[x]$, $f(x)$ se factoriza como $f(x) = (x - \alpha_1) \cdot q(x)$ donde $q(x) \in L_1[x]$ con $\deg q(x) = n - 1$.

Luego, $q(x) \in L_1[x]$ con $\deg q(x) = n - 1$, por el corolario 1.2.5.16. existe una extensión finita L_2 / L_1 tal que $[L_2 : L_1] \leq \deg q(x) = n - 1$ y además $q(x)$ tiene una raíz $\alpha_2 \in L_2$. De esta manera, en $L_2[x]$, $q(x)$ se factoriza como $q(x) = (x - \alpha_2) \cdot r(x)$ donde $r(x) \in L_2[x]$ con $\deg r(x) = n - 2$.

Si reemplazamos, se tiene:

$$f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot r(x)$$

En forma inductiva y por el corolario 1.2.5.9. existe una extensión finita E / F donde:

$$[E : F] = [E : L_{n-1}] \cdot [L_{n-1} : L_{n-2}] \ldots [L_2 : L_1] \cdot [L_1 : F]$$

$$[E : F] \leq 1 \cdot 2 \ldots \cdot (n-1) \cdot n$$

$$[L : K] \leq n!$$

Además, reemplazando en forma inductiva:

$$f(x) = c \cdot (x - \alpha_1) \cdot (x - \alpha_2) \ldots (x - \alpha_n)$$

Obtenemos: $c \in F \ \wedge \ \alpha_1, \alpha_2, \ldots, \alpha_n \in E$ son las n raíces de $f(x)$. □

Definición 1.2.5.19.

Herstein (1970) mencionó: "Un elemento $a \in K$ se dice que es algebraico sobre F si existen elementos $\alpha_0, \alpha_1, \ldots, \alpha_n$ en F, no todos 0, tales que $\alpha_0 a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0$ " (p. 200).

Observación 1.2.5.20.

Herstein (1970) mencionó: "En estos términos, $a \in K$ es algebraico sobre F si existe un polinomio distinto de cero $p(x) \in F[x]$ que a satisface, es decir, para el cual $p(a) = 0$ " (p. 200).

Proposición 1.2.5.21.

Dummit y Foote (2004) mencionaron: "Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$ " (p. 520).

Demostración. Demostraremos por medio de afirmaciones.

Afirmación 1: $\exists \ m_{\alpha,F}(x) \in F[x]$ (mónico) con grado mínimo $/ \ m_{\alpha,F}(\alpha) = 0$

En efecto:

Tenemos que α es algebraico sobre F, entonces:

$$\exists \ p(x) \in F[x] \ / \ p(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

Si dividimos por $a_n \neq 0$, se obtiene:

$$\exists\ q(x) \in F[x]\ /\ q(\alpha) = b_0 + b_1\alpha + \ldots + \alpha^n \text{ con } \quad b_j = \frac{a_j}{a_n} \in F$$

Además:

$$q(\alpha) = 0$$

Este polinomio $q(x) \in F[x]$ cuyo coeficiente principal es 1 se le llama mónico.

Ahora, diremos que si α es algebraico sobre F, del conjunto de polinomios de $F[x]$, de manera análoga a la construcción anterior, tendremos varios polinomios mónicos, por el principio del buen orden en $\mathbb{N}$, se obtiene:

$$\exists\ m_{\alpha,F}(x) \in F[x] \text{ (mónico) con grado mínimo } /\ m_{\alpha,F}(\alpha) = 0$$

Afirmación 2: $m_{\alpha,F}(x)$ es único

En efecto:

Si $m_{\alpha,F}(x), r_{\alpha,F}(x) \in F[x]$ son mónicos diferentes de menor grado tal que

$m_{\alpha,F}(\alpha) = 0 = r_{\alpha,F}(\alpha)$.

Sea $n = \deg m_{\alpha,F}(x) = \deg r_{\alpha,F}(x)$, hagamos:

$$h_{\alpha,F}(x) = m_{\alpha,F}(x) - r_{\alpha,F}(x) \in F[x] \text{ con } \deg h_{\alpha,F}(x) < n$$

Además: $h_{\alpha,F}(\alpha) = m_{\alpha,F}(\alpha) - r_{\alpha,F}(\alpha) = 0$

Luego, si $\tilde{h}_{\alpha,F}(x)$ es el mónico asociado a $h_{\alpha,F}(x)$ con $\deg \tilde{h}_{\alpha,F}(x) = \deg h_{\alpha,F}(x) < n$, entonces:

$$\exists\ c \in F \text{ (invertible) } /\ h_{\alpha,F}(x) = c \cdot \tilde{h}_{\alpha,F}(x)$$

$$h_{\alpha,F}(\alpha) = c \cdot \tilde{h}_{\alpha,F}(\alpha)$$

$$\tilde{h}_{\alpha,F}(\alpha) = 0$$

Por lo tanto:

$$\tilde{h}_{\alpha,F}(x) \in F[x] \text{ (mónico) con } \deg \tilde{h}_{\alpha,F}(x) < n \ / \ \tilde{h}_{\alpha,F}(\alpha) = 0 \ (\Rightarrow\Leftarrow)$$

La contradicción se debe a la minimalidad del grado de $m_{\alpha,F}(x)$ y $r_{\alpha,F}(x)$.

Por lo tanto:

$$m_{\alpha,F}(x) = r_{\alpha,F}(x) \text{ (Unicidad)}$$

Afirmación 3: $m_{\alpha,F}(x)$ es irreducible

En efecto:

Supongamos que $m_{\alpha,F}(x) \in F[x]$ es reducible, entonces:

$$\exists \ f(x), g(x) \in F[x] \text{ (mónicos) } / \ m_{\alpha,F}(x) = f(x) \cdot g(x)$$

Donde: $\deg f(x), \deg g(x) < \deg m_{\alpha,F}(x)$

Luego:

$$m_{\alpha,F}(\alpha) = f(\alpha) \cdot g(\alpha)$$

$$0 = f(\alpha) \cdot g(\alpha) \in L$$

Como L es cuerpo, por el teorema 1.2.3.7. se tiene que L es un dominio entero, entonces L no tiene divisores de cero, luego:

$$f(\alpha) = 0 \ \vee \ g(\alpha) = 0$$

Por lo tanto:

$f(x), g(x) \in F[x]$ (mónicos) con $\deg f(x), \deg g(x) < \deg m_{\alpha,F}(x)$ / $f(\alpha) = 0 \vee g(\alpha) = 0$

$(\Rightarrow\Leftarrow)$

La contradicción se debe a la minimalidad del grado de $m_{\alpha,F}(x)$.

Finalmente:

$$m_{\alpha,F}(x) \text{ es irreducible}$$

Afirmación 4: $\forall\ f(x) \in F[x]$ con $f(\alpha) = 0 \Leftrightarrow m_{\alpha,F}(x) \mid f(x)$ en $F[x]$

En efecto:

$(\Rightarrow)$ Sea $f(x) \in F[x]$ con $f(\alpha) = 0$, dividiendo entre $m_{\alpha,F}(x)$ se tiene:

$$f(x) = m_{\alpha,F}(x).q(x) + r(x) \text{ , con } r(x) = 0 \ \vee\ \deg r(x) < \deg m_{\alpha,F}(x)$$

Pero:

$$f(\alpha) = m_{\alpha,F}(\alpha).q(\alpha) + r(\alpha)$$

$$0 = 0.q(\alpha) + r(\alpha)$$

$$r(\alpha) = 0$$

Hasta ahora, tenemos:

$$r(\alpha) = 0 \text{ , donde: } r(x) = 0 \ \vee\ \deg r(x) < \deg m_{\alpha,F}(x)$$

Si: $\deg r(x) < \deg m_{\alpha,F}(x)$ $(\Rightarrow\Leftarrow)$ (Por la minimalidad del $\deg m_{\alpha,F}(x)$)

Entonces:

$$r(x) = 0$$

Finalmente:

$$f(x) = m_{\alpha,F}(x).q(x)$$

Es decir:

$$m_{\alpha,F}(x) \mid f(x) \text{ en } F[x]$$

($\Leftarrow$) Como $m_{\alpha,F}(x) \mid f(x)$ en $F[x]$, entonces:

$$\exists\ q(x) \in F[x] \ / \ f(x) = q(x).m_{\alpha,F}(x)$$

$$f(\alpha) = q(\alpha) \cdot m_{\alpha,F}(\alpha)$$

$$f(\alpha) = q(\alpha) \,.0$$

$$f(\alpha) = 0$$

Por lo tanto:

$$\forall\ f(x) \in F[x] \text{ se tiene que } f(\alpha) = 0$$ □

Observación 1.2.5.22.

Zaldivar (1996) mencionó: "En cualquier caso, al polinomio mónico irreducible $m(x) \in k[x]$ de grado menor del cual $\alpha \in K$ es raíz, se le llama el polinomio mínimo (irreducible) de α, y se denota

$$m(x) = Irr(\alpha, k) \in k[x]$$" (p. 58).

Observación 1.2.5.23. El polinomio mínimo irreducible depende del cuerpo sobre el que se considere. Por ejemplo, $Irr(\sqrt{5}, \mathbb{Q}) = x^2 - 5$, mientras que $Irr(\sqrt{5}, \mathbb{R}) = x - \sqrt{5}$, así que siempre hablaremos del "polinomio mínimo irreducible sobre".

Definición 1.2.5.24.

Zaldivar (1996) mencionó: “Una extensión K/k se llama algebraica si todos los elementos de K son algebraicos sobre k” (p. 61).

Corolario 1.2.5.25.

Zaldivar (1996) mencionó: “Toda extensión finita K/k es algebraica” (p.61).

Demostración. Sea $[K:k]=n$

Sea $\beta \in K \ \wedge \ \beta \neq 0 \Rightarrow \exists \ \{1,\beta,\beta^2,\ldots,\beta^n\} \subset K$

Si sus elementos son distintos, por el corolario 1.2.4.18. se tiene que $\{1,\beta,\beta^2,\ldots,\beta^n\}$ es L.D.

Entonces:

$$\exists \ p(x) \in k[x] \text{ (no nulo) } / \ p(\beta)=0$$

$$\beta \text{ es algebraico sobre } k$$

Por lo tanto:

$$K/k \text{ es algebraico}$$

Si sus elementos no son distintos, entonces:

$$\beta^i = 1 \text{ , para algún } i=1,2,\ldots,n$$

$$\beta^i - 1 = 0$$

Luego:

$$\exists \ p(x)=x^i-1 \ \in \ k[x] \text{ (no nulo) para algún } i=1,2,\ldots,n \ / \ p(\beta)=0$$

$$\beta \text{ es algebraico sobre } k$$

Por lo tanto:

$$K/k \text{ es algebraico} \qquad \square$$

Observación 1.2.5.26.

Zaldivar (1996) mencionó: "Observemos primero que si K es un campo y $\{L_\alpha\}$ es una familia de subcampos de K, entonces la intersección $L=\bigcap_\alpha L_\alpha \subseteq K$ es de nuevo un subcampo de K " (p. 54).

Demostración. Veamos:

a. Sea $z \in \bigcap_\alpha L_\alpha \Rightarrow z \in L_\alpha \; ; \; \forall \alpha$

Como L_α son subcuerpos de K, entonces:

$$z \in K$$

Por lo tanto:

$$\bigcap_\alpha L_\alpha \subset K$$

b. Sean $z_1, z_2 \in \bigcap_\alpha L_\alpha \Rightarrow z_1, z_2 \in L_\alpha \; ; \; \forall \alpha$

Como L_α son subcuerpos de K, entonces:

$$z_1 - z_2 \in L_\alpha \; ; \; \forall \alpha$$

Por lo tanto:

$$z_1 - z_2 \in \bigcap_\alpha L_\alpha$$

c. Sean $z_1, z_2 \in \bigcap_\alpha L_\alpha - \{0\}$, entonces:

$$z_1, z_2 \in L_\alpha \; , \; \forall \alpha \wedge z_1, z_2 \neq 0$$

Como L_α son subcuerpos de K, entonces:

$$\exists!\ z_2^{-1} \in L_\alpha$$

Además:

$$z_1 \cdot z_2^{-1} \in L_\alpha\ ,\ \forall \alpha$$

$$z_1 \cdot z_2^{-1} \in \bigcap_\alpha L_\alpha - \{0\}$$

Por lo tanto, del teorema 1.2.3.4. se obtiene:

$\bigcap_\alpha L_\alpha$ es subcuerpo de K □

Observación 1.2.5.27. $\bigcap_\alpha L_\alpha$ es el subcuerpo más pequeño de K que contiene a k y α.

Demostración. Supongamos que $\bigcap_\alpha L_\alpha$ no es el más pequeño de K que contiene tanto a k como α, entonces:

$\exists\ H$ es el más pequeño de K que contiene tanto a k como α

$$k \subset H \subset \bigcap_\alpha L_\alpha \subset K$$

Pero:

$$H \subset \bigcap_\alpha L_\alpha \subset H$$

$$\bigcap_\alpha L_\alpha = H\ \ (\Rightarrow\Leftarrow)$$

Por lo tanto:

$\bigcap_\alpha L_\alpha$ es el subcuerpo más pequeño de K que contiene a k y α □

Definición 1.2.5.28.

Zaldivar (1996) mencionó:

Sea K/k una extensión y sea $X \subseteq K$ un subconjunto. Sea $\Im$ la familia de subcampos de K que contienen a k y a X. Esta familia $\Im$ es no vacía ya que $K \in \Im$. El subcampo $k(X) := \bigcap_{F \in \Im} F$ se llama el campo obtenido adjuntando X a k.

Claramente $k \subseteq k(X) \subseteq K$, y $k(X)$ es el menor subcampo de K que contiene a k y a X. Si $X = \{a_1, \ldots, a_n\} \subseteq K$ es un conjunto finito, usaremos la notación

$$k(\{a_1, \ldots, a_n\}) = k(a_1, \ldots, a_n).$$

En particular, si $X = \{a\} \subseteq K$, diremos que se tiene una extensión simple $k(a)/k$.

Comenzamos describiendo, internamente, estas extensiones simples. (p. 56)

Proposición 1.2.5.29.

Zaldivar (1996) mencionó: "Sean K/k una extensión, $\alpha \in K$. Sea $k(\alpha)/k$ la extensión simple obtenida al adjuntar α a k. Entonces,

$$k(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in k[x] \text{ y } g(\alpha) \neq 0 \right\}$$ " (p. 56).

Demostración. Sea $W = \left\{ \frac{f(\alpha)}{g(\alpha)} / f(x), g(x) \in k[x] \wedge g(\alpha) \neq 0 \right\}$

$(\subset)$ Demostremos las siguientes afirmaciones:

Afirmación 1: W es subcuerpo de K

En efecto:

a. Sea $z \in W \Rightarrow z = \frac{f(\alpha)}{g(\alpha)} / f(x), g(x) \in k[x] \wedge g(\alpha) \neq 0$

$$z \in K$$

Por lo tanto:

$$W \subset K$$

b. Sean $a, b \in W \Rightarrow a = \frac{f(\alpha)}{g(\alpha)} \ / \ f(x), g(x) \in k[x] \ \wedge \ g(\alpha) \neq 0$

Además: $b = \frac{\varphi(\alpha)}{\psi(\alpha)} \ / \ \varphi(x), \psi(x) \in k[x] \ \wedge \ \psi(\alpha) \neq 0$

Como $b \in K \ \wedge \ K$ es cuerpo $\Rightarrow \exists! \ -b \in K$

Luego:

$$a - b = \frac{f(\alpha)}{g(\alpha)} - \frac{\varphi(\alpha)}{\psi(\alpha)} = \frac{f(\alpha).\psi(\alpha) - \varphi(\alpha).g(\alpha)}{g(\alpha).\psi(\alpha)} = \frac{r(\alpha)}{s(\alpha)}$$

Donde:

$$r(x) = f(x).\psi(x) - \varphi(x).g(x) \in k[x] \ \wedge \ s(x) = g(x).\psi(x) \in k[x] \ \wedge \ s(\alpha) \neq 0$$

Entonces:

$$a - b \in W$$

c. Sean $a, b \in W - \{0\}$, entonces:

$$a = \frac{f(\alpha)}{g(\alpha)} \ / \ f(x), g(x) \in k[x] \ \wedge \ f(\alpha) \neq 0 \wedge g(\alpha) \neq 0$$

Además:

$$b = \frac{\varphi(\alpha)}{\psi(\alpha)} \ / \ \varphi(x), \psi(x) \in k[x] \ \wedge \ \psi(\alpha) \neq 0 \ \wedge \ \varphi(\alpha) \neq 0$$

Como $b \in K \ \wedge \ b \neq 0 \ \wedge \ K$ es cuerpo $\Rightarrow \exists! \ b^{-1} \in K$

Luego:

$$a.b^{-1} = \frac{f(\alpha)}{g(\alpha)}.\left(\frac{\varphi(\alpha)}{\psi(\alpha)}\right)^{-1} = \frac{f(\alpha).\psi(\alpha)}{g(\alpha).\varphi(\alpha)}$$

Luego:

$$a.b^{-1} = \frac{r(\alpha)}{s(\alpha)}$$

Donde:

$$r(x) = f(x).\psi(x) \in k[x] \ \wedge \ s(x) = g(x).\varphi(x) \in k[x] \ \wedge \ s(\alpha) \neq 0$$

Entonces:

$$a \cdot b^{-1} \in W - \{0\}$$

Finalmente, por el teorema 1.2.3.4. se obtiene:

W es subcuerpo de K

Afirmación 2: $k \subset W$

En efecto:

Sea $z \in k$.

Sean $f(x) = z \in k[x] \ \wedge \ g(x) = 1 \in k[x]$, entonces:

$$z = \frac{f(\alpha)}{g(\alpha)} \ / \ f(x), g(x) \in k[x] \ \wedge \ g(\alpha) \neq 0$$

$$z \in W$$

Por lo tanto:

$$k \subset W$$

Afirmación 3: $\alpha \in W$

En efecto:

Sean $f(x) = x \in k[x] \ \wedge \ g(x) = 1 \in k[x]$, entonces:

$$\alpha = \frac{\alpha}{1} = \frac{f(\alpha)}{g(\alpha)} \ / \ f(x), g(x) \in k[x] \ \wedge \ g(\alpha) \neq 0$$

Por lo tanto:

$$\alpha \in W$$

Afirmación 4: $k(\alpha) \subset W$

En efecto:

Sabemos: $k(\alpha) = \bigcap_{F \in \Im} F$; $\Im$: colección de subcuerpos de K que contienen a k y α

De las afirmaciones 1, 2 y 3 se tiene que $W \in \Im$

Entonces:

$$k(\alpha) = \bigcap_{F \in \Im} F \subset W$$

Por lo tanto:

$$k(\alpha) \subset W$$

$(\supset)$ Sea $z \in W \ \Rightarrow \ z = \frac{f(\alpha)}{g(\alpha)} \ / \ f(x), g(x) \in k[x] \ \wedge \ g(\alpha) \neq 0$

Sea $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in k[x]$ con $a_j \in k$

Usando hipótesis se tiene:

$$f(\alpha) = a_0 + a_1 \alpha + \ldots + a_n \alpha^n \in k(\alpha)$$

En forma análoga:

$$g(\alpha) \in k(\alpha)$$

Como $g(\alpha) \in k(\alpha) \ \wedge \ g(\alpha) \neq 0 \ \wedge \ k(\alpha)$ es cuerpo, entonces:

$$\exists! \ g^{-1}(\alpha) \in k(\alpha)$$

Luego:

$$z = \frac{f(\alpha)}{g(\alpha)} = f(\alpha).g^{-1}(\alpha) \in k(\alpha)$$

$$z \in k(\alpha)$$

Por lo tanto:

$$W \subset k(\alpha)$$

Finalmente, de $(\subset)$ y $(\supset)$ se obtiene:

$$k(\alpha) = W$$

Es decir:

$$k(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} / \; f(x), g(x) \in k[x] \wedge g(\alpha) \neq 0 \right\}$$ □

Proposición 1.2.5.30.

Zaldivar (1996) mencionó: "Sea $\alpha \in K$ algebraico sobre k y sea $m(x) = Irr(\alpha, k) \in k[x]$.

Entonces,

$$k(\alpha) = \{ p(\alpha) : p(x) \in k[x] \wedge gr(p(x)) < gr(m(x)) \}$$ " (p. 58).

Demostración. Veamos:

$(\subset)$ Sea $\beta \in k(\alpha) \Rightarrow \beta = \frac{p(\alpha)}{q(\alpha)} \; / \; p(x), q(x) \in k[x] \; \wedge \; q(\alpha) \neq 0$

Como $q(\alpha) \neq 0$, por la proposición 1.2.5.21. se tiene:

$$m(x) \nmid q(x)$$

Entonces:

$$mcd(m(x), q(x)) = 1$$

Como k es cuerpo, por el teorema 1.2.3.8. se tiene $k[x]$ es DIP.

Usando la observación 1.2.2.38. se tiene:

$$\exists\ a(x), b(x) \in k[x]\ /\ m(x).a(x) + q(x).b(x) = 1$$

$$m(\alpha).a(\alpha) + q(\alpha).b(\alpha) = 1$$

$$0.a(\alpha) + q(\alpha).b(\alpha) = 1$$

$$q(\alpha).b(\alpha) = 1$$

Como $q(\alpha) \in K \ \wedge\ q(\alpha) \neq 0 \ \wedge\ K$ es cuerpo $\Rightarrow\ \exists!\ \dfrac{1}{q(\alpha)} \in K$

Luego:

$$\frac{1}{q(\alpha)}.q(\alpha).b(\alpha) = \frac{1}{q(\alpha)}.1$$

$$b(\alpha) = \frac{1}{q(\alpha)}$$

Por lo tanto:

$$\beta = \frac{p(\alpha)}{q(\alpha)} = p(\alpha).b(\alpha)$$

Sea $h(x) = p(x).b(x) \in k[x]\ /\ \beta = h(\alpha)$

Ahora, analicemos el grado de $h(x)$

$$gr(h(x)) < gr(m(x)) \ \vee\ gr(h(x)) \geq gr(m(x))$$

Si: $gr(h(x)) < gr(m(x))$

Juntando los resultados, se tiene:

$$\beta = h(\alpha)\ /\ h(x) \in k[x] \ \wedge\ gr(h(x)) < gr(m(x))$$

$$\beta \in \{p(\alpha)\ /\ p(x) \in k[x] \wedge gr(p(x)) < gr(m(x))\}$$

Así se obtiene:

$$k(\alpha) \subset \{ p(\alpha) \,/\, p(x) \in k[x] \wedge gr(p(x)) < gr(m(x)) \}$$

Si: $gr(h(x)) \geq gr(m(x))$

Por el algoritmo de la división, se tiene:

$$\exists \;\; q(x), r(x) \in k[x] \;\; / \;\; h(x) = m(x).q(x) + r(x)$$

Donde: $r(x) = 0 \;\; \vee \;\; gr(r(x)) < gr(m(x))$

Luego:

$$h(\alpha) = m(\alpha).q(\alpha) + r(\alpha)$$

$$h(\alpha) = 0.q(\alpha) + r(\alpha)$$

$$h(\alpha) = r(\alpha)$$

$$\beta = r(\alpha)$$

Afirmación: $r(x) \neq 0$

En efecto:

Supongamos que $r(x) = 0$, además se tiene: $r(\alpha) = \beta$, entonces:

$$\beta = 0$$

Así se obtiene:

$$k(\alpha) \subset \{0\}$$

Por otro lado, se sabe $k(\alpha)$ es subcuerpo de $K \;\Rightarrow\; 0 \in k(\alpha)$, luego:

$$\{0\} \subset k(\alpha)$$

Entonces:

$$k(\alpha) = \{0\} \quad (\Rightarrow\Leftarrow) \text{ (Pues } \{0\} \text{ no es cuerpo)}$$

Por lo tanto:

$$r(x) \neq 0 \;\Rightarrow\; gr(r(x)) < gr(m(x))$$

Juntando los resultados, se tiene:

$$\beta = r(\alpha) \;/\; r(x) \in k[x] \;\wedge\; gr(r(x)) < gr(m(x))$$

$$\beta \in \{p(\alpha) \,/\, p(x) \in k[x] \wedge gr(p(x)) < gr(m(x))\}$$

Así se obtiene:

$$k(\alpha) \subset \{p(\alpha) \,/\, p(x) \in k[x] \wedge gr(p(x)) < gr(m(x))\}$$

$(\supset)$ Sea $w \in \{p(\alpha) \,/\, p(x) \in k[x] \wedge gr(p(x)) < gr(m(x))\}$, entonces:

$$w = \frac{p(\alpha)}{1} \;/\; p(x) \in k[x] \;\wedge\; gr(p(x)) < gr(m(x))$$

Sea $q(\alpha) = 1$, donde: $q(x) \in k[x]$

Luego:

$$w = \frac{p(\alpha)}{q(\alpha)} \;/\; p(x), q(x) \in k[x] \;\wedge\; q(\alpha) \neq 0$$

$$w \in k(\alpha)$$

Por lo tanto:

$$\{p(\alpha) \,/\, p(x) \in k[x] \wedge gr(p(x)) < gr(m(x))\} \subset k(\alpha)$$

Finalmente, de $(\subset)$ y $(\supset)$ se obtiene:

$$k(\alpha) = \{p(\alpha) \,/\, p(x) \in k[x] \wedge gr(p(x)) < gr(m(x))\}$$ □

Observación 1.2.5.31. Sea L/k una extensión de cuerpo y $\alpha \in L$.

Diferenciemos las siguientes expresiones:

$k[\alpha]$ es el subanillo más pequeño de L que contiene a k y α

$k(\alpha)$ es el subcuerpo más pequeño de L que contiene a k y α

Proposición 1.2.5.32.

Lang (1971) mencionó: "Si α es algebraico sobre k, se verifica que $k(\alpha) = k[\alpha]$ y $k(\alpha)$ es finito sobre k. El grado $[k(\alpha) : k]$ es igual al grado de $Irr(\alpha, k, X)$" (p. 193).

Demostración. Vamos a demostrar que: $k(\alpha) = k[\alpha]$

Sea $m(x) = Irr(\alpha, k, X)$

Sea $f(\alpha) \in k[\alpha]$ tal que $f(\alpha) \neq 0$, por la proposición 1.2.5.21. se tiene:

$$m(x) \nmid f(x)$$

Entonces:

$$mcd(m(x), f(x)) = 1$$

Como k es cuerpo, por el teorema 1.2.3.8. se tiene que:

$k[x]$ es un DIP

Por la observación 1.2.2.38. se tiene que:

$$\exists \ g(x), h(x) \in k[x] \ / \ g(x) \cdot m(x) + h(x) \cdot f(x) = 1$$

Como: $m(x) = Irr(\alpha, k, x)$ entonces $m(\alpha) = 0$

Reemplazando:

$$g(\alpha)\cdot 0 + h(\alpha)\cdot f(\alpha) = 1$$

$$h(\alpha)\cdot f(\alpha) = 1$$

Ordenando:

$$f(\alpha) \in k[\alpha] \ \wedge \ f(\alpha) \neq 0 \ \Rightarrow \ \exists! \ h(\alpha) \in k[\alpha] \ / \ f(\alpha)\cdot h(\alpha) = 1 = h(\alpha)\cdot f(\alpha)$$

Obtenemos:

$f(\alpha)$ es invertible en $k[\alpha]$

Por lo tanto:

$k[\alpha]$ es un cuerpo

Hemos obtenido que $k[\alpha]$ es el subcuerpo más pequeño de L que contiene a k y α , finalmente:

$$k(\alpha) = k[\alpha]$$

Ahora, demostraremos que $k(\alpha) / k$ es finito

En efecto:

Sea $m(x) \in k[x]$ con $\deg m(x) = d \ \wedge \ \alpha \neq 0 \in L$

Afirmación 1: $\{1, \alpha, \alpha^2, \ldots \alpha^{d-1}\}$ genera $k[\alpha]$

En efecto:

($\subset$) Sea $f(\alpha) \in k[\alpha]$ tal que $f(\alpha) \neq 0$, donde $f(x) \in k[x]$

Por la proposición 1.2.5.21. se tiene que $m(x) \nmid f(x)$ entonces existen $q(x), r(x) \in k[x]$ tal que

$$f(x) = m(x) \cdot q(x) + r(x)$$

Donde: $r(x) = 0 \ \vee \ \deg r(x) < \deg m(x) = d$

Si $x = \alpha$, entonces:

$$f(\alpha) = m(\alpha) \cdot q(\alpha) + r(\alpha)$$

Como $m(x) = Irr(\alpha, k, X) \in k[x]$, entonces:

$$f(\alpha) = 0 \cdot q(\alpha) + r(\alpha)$$

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

$$f(\alpha) = z_0 + z_1\alpha + z_2\alpha^2 + \ldots + z_{d-1}\alpha^{d-1} \text{; para algún } z_i \in k,\ i = 0, \ldots, d-1$$

$$f(\alpha) \in L\left\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\right\}$$

Por lo tanto:

$$k[\alpha] \subset L\left\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\right\}$$

($\supset$) Sea $z \in L\left\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\right\}$

Entonces, existen $c_0, c_1, \ldots, c_{d-1} \in k$ tal que

$$z = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{d-1}\alpha^{d-1} \in k[\alpha]$$

$$z \in k[\alpha]$$

Por lo tanto:

$$L\left\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\right\} \subset k[\alpha]$$

De $(\subset)$ y $(\supset)$ se tiene:

$$k[\alpha] = L\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$$

Afirmación 2: $\{1, \alpha, \alpha^2, \ldots \alpha^{d-1}\}$ es L.I sobre k

En efecto:

Supongamos que $\{1, \alpha, \alpha^2, \ldots \alpha^{d-1}\}$ es L.D sobre k , entonces existen $c_0, c_1, \ldots, c_{d-1} \in k$ (no todos ceros) tal que

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{d-1}\alpha^{d-1} = 0$$

Entonces:

$$\exists g(x) \in k[x] \text{ (no nulo) con } \deg g(x) = d-1 \,/\, g(\alpha) = 0 \qquad (1.39)$$

Por otro lado, tenemos:

$$m(x) = Irr(\alpha, k, x) \text{ con } \deg m(x) = d \Rightarrow m(\alpha) = 0 \qquad (1.40)$$

De (1.39) y (1.40), usando la proposición 1.2.5.21. se obtiene:

$$m(x) \mid g(x)$$

Entonces:

$$\deg g(x) \geq \deg m(x) \quad (\Rightarrow\Leftarrow)$$

Por lo tanto:

$\{1, \alpha, \alpha^2, \ldots \alpha^{d-1}\}$ es L.I sobre k

De Afirmación 1 y 2:

$\{1, \alpha, \alpha^2, \ldots \alpha^{d-1}\}$ es una base de $k[\alpha]$

Entonces:

$$dim_k k[\alpha] = d < \infty$$

Luego:

$$k[\alpha] / k \text{ es finito}$$

Por lo tanto:

$$k(\alpha) / k \text{ es finito}$$

Por otro lado:

$$[k(\alpha) : k] = dim_k k(\alpha) = d \ \wedge \ \deg Irr(\alpha, k, x) = \deg m(x) = d$$

Se concluye:

$$[k(\alpha) : k] = \deg Irr(\alpha, k, x)$$

□

Ejemplo 1.2.5.33. Veamos cómo se cumple la proposición 1.2.5.32.

Tenemos $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ es algebraico sobre $\mathbb{Q}$ y de hecho:

$$m(x) = Irr(\sqrt{2}, \mathbb{Q}, x) = x^2 - 2 \in \mathbb{Q}[x]$$

Además, por la proposición 1.2.5.30. se tiene:

$$\mathbb{Q}(\sqrt{2}) = \left\{ p(\sqrt{2}) / \ p(x) \in \mathbb{Q}[x] \wedge gr(p(x)) < gr(m(x)) \right\}$$

$$\mathbb{Q}(\sqrt{2}) = \left\{ p(\sqrt{2}) / \ p(x) \in \mathbb{Q}[x] \wedge gr(p(x)) < 2 \right\}$$

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

Se puede ver que $\{1,\sqrt{2}\}$ es una base de $\mathbb{Q}(\sqrt{2}) \Rightarrow [\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$

Se concluye:

$$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = \deg Irr(\sqrt{2},\mathbb{Q},x)$$

Definición 1.2.5.34.

Lang (1971) mencionó: "Sean E , F extensiones de un cuerpo k . Si E y F están contenidos en algún cuerpo L , denotaremos por EF el mínimo subcuerpo de L que contiene a E y a F , y que llamaremos el compuesto de E y F , en L " (p. 194).

Ejemplo 1.2.5.35. Veamos que la composición de los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$ es el cuerpo $\mathbb{Q}(\sqrt[6]{2})$.

Demostración. Tenemos:

$\mathbb{Q}(\sqrt{2})$ es el menor subcuerpo de L que contiene a $\mathbb{Q}$ y $\sqrt{2}$

$\mathbb{Q}(\sqrt[3]{2})$ es el menor subcuerpo de L que contiene a $\mathbb{Q}$ y $\sqrt[3]{2}$

$\mathbb{Q}(\sqrt[6]{2})$ es el menor subcuerpo de L que contiene a $\mathbb{Q}$ y $\sqrt[6]{2}$

Ahora, demostremos que $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$ están incluidos en $\mathbb{Q}(\sqrt[6]{2})$.

a. Sea $z \in \mathbb{Q}(\sqrt{2}) \Rightarrow z = a+b\sqrt{2}$, para algún $a,b \in \mathbb{Q}$

   Luego:

$$z = a+b\sqrt{2} = a+b(\sqrt[6]{2})^3 \in \mathbb{Q}(\sqrt[6]{2})$$

   Por lo tanto:

$$\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$$

b. Sea $z \in \mathbb{Q}(\sqrt[3]{2}) \Rightarrow z = a+b\sqrt[3]{2}$, para algún $a,b \in \mathbb{Q}$

Luego:

$$z = a + b\sqrt[3]{2} = a + b(\sqrt[6]{2})^2 \in \mathbb{Q}(\sqrt[6]{2})$$

Por lo tanto:

$$\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[6]{2})$$

Entonces:

$\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$ están incluidos en $\mathbb{Q}(\sqrt[6]{2})$

Finalmente:

La composición de los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$ es el cuerpo $\mathbb{Q}(\sqrt[6]{2})$ □

Observación 1.2.5.36.

Lang (1971) mencionó: "Si E, F no se dan como sumergidos en un cuerpo común L, no es posible definir el compuesto" (p. 194).

Observación 1.2.5.37. Sea L/k una extensión de cuerpos y sean $\alpha_1, \alpha_2 \in L$ (no necesariamente algebraicos), entonces:

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

Demostración. Se puede ver por la proposición 1.2.5.29. que:

$$F(\alpha_1, \alpha_2) = \left\{ \frac{p(\alpha_1, \alpha_2)}{q(\alpha_1, \alpha_2)} / \, p(x_1, x_2), q(x_1, x_2) \in k[x_1, x_2] \wedge q(\alpha_1, \alpha_2) \neq 0 \right\}$$

$$F(\alpha_1, \alpha_2) = \left\{ \frac{(p(\alpha_1))(\alpha_2)}{(q(\alpha_1))(\alpha_2)} / \, (p(x_1))(x_2), (q(x_1))(x_2) \in k[x_1, x_2] \wedge (q(\alpha_1))(\alpha_2) \neq 0 \right\}$$

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

De manera análoga se demuestra que:

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

Por lo tanto:

$$F(\alpha_1, \alpha_2) = (F(\alpha_1))(\alpha_2) = (F(\alpha_2))(\alpha_1) \qquad \square$$

De forma análoga a la construcción anterior de la extensión simple $k(\alpha)/k$, podemos construir para $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$, entonces podemos generalizar como menciona la siguiente definición.

Definición 1.2.5.38.

Lang (1971) mencionó: "Sea k un subcuerpo de E, y $\alpha_1, \ldots, \alpha_n$, elementos de E. Representaremos por

$$k(\alpha_1, \ldots, \alpha_n)$$

el subcuerpo más pequeño de E que contiene a k y a $\alpha_1, \ldots, \alpha_n$.

Sus elementos son todos los cocientes

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$$

donde f, g son polinomios en n variables con coeficientes en k, siendo $g(\alpha_1, \ldots, \alpha_n) \neq 0$" (p. 194).

Definición 1.2.5.39.

Lang (1971) mencionó: "Podríamos definir el compuesto de una subfamilia arbitraria de subcuerpos de un cuerpo L como el menor subcuerpo que contiene a todos los cuerpos de la familia" (p. 194).

Definición 1.2.5.40.

Lang (1971) mencionó: “Diremos que E es de generación finita sobre k si hay una familia finita de elementos $\alpha_1,\ldots,\alpha_n$ de E tal que

$$E = k(\alpha_1,\ldots,\alpha_n)$$ ” (pp. 194-195)

Observación 1.2.5.41. E es la composición de todos estos subcuerpos finitamente generados sobre k, gráficamente:

$$E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

$$\nearrow \qquad \uparrow \qquad \ldots \qquad \nwarrow$$

$$E_1 = k(\alpha_1) \qquad E_2 = k(\alpha_1, \alpha_2) \quad \ldots \quad E_{n-1} = k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$$

Proposición 1.2.5.42.

Lang (1971) mencionó: “Si E es una extensión finita de k, E es de generación finita” (p. 195).

Demostración. Como E/k es una extensión finita por el corolario 1.2.5.25. se tiene que E/k es algebraico.

Si $E = k$ por la observación 1.2.5.5. nos dice que $[E:k] = 1$, entonces:

$E(1) = k(1)$ es el mínimo subcuerpo de E y $E \subset E(1)$

Luego:

$$E = E(1)$$

Por lo tanto:

$$E = k(1)$$

y queda demostrado.

Si $E \neq k$, existe $\alpha_1 \in E - k$, por la proposición 1.2.5.32. se tiene

$$[k(\alpha_1) : k] = \deg Irr(\alpha_1, k, x) > 1$$

Pues si el polinomio $Irr(\alpha_1, k, x) = x - \alpha_1$ fuera lineal entonces $\alpha_1 \in k$ y esto sería una contradicción.

Si $k(\alpha_1) = E$ queda demostrado. En caso contrario, $k(\alpha_1) \neq E$, existe $\alpha_2 \in E - k(\alpha_1)$, por el teorema 1.2.5.6. se tiene

$$[k(\alpha_1, \alpha_2) : k] = [k(\alpha_1, \alpha_2) : k(\alpha_1)].[k(\alpha_1) : k]$$

Usando la observación 1.2.5.37. y la proposición 1.2.5.32. se tiene

$$[k(\alpha_1, \alpha_2) : k(\alpha_1)] = [k(\alpha_1)(\alpha_2) : k(\alpha_1)] = \deg Irr(\alpha_2, k(\alpha_1), x) > 1$$

Pues si el polinomio $Irr(\alpha_2, k(\alpha_1), x)) = x - \alpha_2$ fuera lineal entonces $\alpha_2 \in k(\alpha_1)$ y esto sería una contradicción.

Luego:

$$[k(\alpha_1, \alpha_2) : k] = [k(\alpha_1, \alpha_2) : k(\alpha_1)].[k(\alpha_1) : k] > 2$$

Continuando este proceso, y teniendo en cuenta que $[E : k] < \infty$, se tendrá un número finito de pasos, encontrando así $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ tal que

$$E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

Por lo tanto:

E / k es finitamente generado □

Observación 1.2.5.43.

Lang (1971) mencionó: "Si $E = k(\alpha_1, \ldots, \alpha_n)$ es de generación finita, y F es una extensión de k, estando F y E contenidos en L,

$$EF = F(\alpha_1, \ldots, \alpha_n),$$

y EF es de generación finita sobre F" (p. 195).

Demostración. Como EF es el mínimo subcuerpo de $L \wedge E, F \subset EF$, entonces:

$$EF = min\{H \subset L / H \text{ es subcuerpo de } L \wedge E, F \subset H\}$$

Como EF es el mínimo subcuerpo de L entonces $EF \subset L$, además E / k es de generación finita, entonces:

$$\exists\ \alpha_1, \alpha_2, \ldots, \alpha_n \in k(\alpha_1, \alpha_2, \ldots, \alpha_n) = E \subset H$$

Luego:

$$EF = min\{H \subset L / H \text{ es subcuerpo de L } \wedge F \subset H \wedge \alpha_1, \ldots, \alpha_n \in H\}$$

$$EF = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$ □

Observación 1.2.5.44.

Lang (1971) mencionó: "Sea una torre de cuerpos

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \ldots \subset k(\alpha_1, \ldots, \alpha_n),$$

cada uno engendrado a partir del precedente por un solo elemento" (p. 195).

Proposición 1.2.5.45.

Lang (1971) mencionó: "Si $E = k(\alpha_1, \ldots, \alpha_n)$ es una extensión de generación finita de un cuerpo k, y α_i es algebraico sobre k para cada $i = 1, \ldots, n$, E es finito y algebraico sobre k" (p. 196).

Demostración. Sea la torre de cuerpos:

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset k(\alpha_1, \alpha_2, \alpha_3) \subset \ldots \subset k(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$$

Por la proposición 1.2.5.32. y de la observación 1.2.5.37. se tiene:

$$k(\alpha_1) / k \text{ es finito}$$

$$k(\alpha_1, \alpha_2) / k(\alpha_1) = (k(\alpha_1))(\alpha_2) / k(\alpha_1) \text{ es finito}$$

$$k(\alpha_1, \alpha_2, \alpha_3) / k(\alpha_1, \alpha_2) = (k(\alpha_1, \alpha_2))(\alpha_3) / k(\alpha_1, \alpha_2) \text{ es finito}$$

$$\vdots$$

$$k(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n) / k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) \text{ es finito}$$

Por el corolario 1.2.5.9. se tiene:

$$k(\alpha_1, \alpha_2, \ldots, \alpha_n) / k \text{ es finito}$$

$$E / k \text{ es finito}$$

Finalmente, por el corolario 1.2.5.25. se concluye que:

$$E / k \text{ es algebraico}$$ □

Teorema 1.2.5.46.

Herstein (1970) mencionó: "Si L es una extensión algebraica de K y si K es una extensión algebraica de F, entonces L es una extensión algebraica de F" (p. 204).

Demostración. Tenemos:

$$L/K \ \wedge \ K/F \text{ son extensiones algebraicas}$$

Sea $\alpha \in L \ \wedge \ L/K$ es algebraico entonces satisface la ecuación:

$$a_0 + a_1\alpha + \ldots + a_n\alpha_n = 0 \qquad (1.41)$$

Con $a_i \in K$ (no todos ceros), $i = 0,1,\ldots,n$

Sea $K_0 = F(a_0, a_1, \ldots, a_n)$ y $a_i \in K$ son algebraicos sobre F.

Por la proposición 1.2.5.45. se tiene:

$$K_0 / F \text{ es finito}$$

Además $a_i \in K_0$ con $i = 0,1,\ldots,n$ entonces de (1.41) se tiene que:

$$\alpha \text{ es algebraico sobre } K_0$$

De la torre de cuerpos:

$$F \subset K_0 = F(a_0, a_1, \ldots, a_n) \subset K_0(\alpha)$$

De la proposición 1.2.5.32. se tiene que:

$$K_0(\alpha) / K_0 \text{ es finito}$$

Como $K_0(\alpha) / K_0$ y K_0 / F son finitos, por el corolario 1.2.5.7. se tiene:

$$K_0(\alpha) / F \text{ es finito}$$

Por el corolario 1.2.5.25. se tiene:

$$K_0(\alpha)/F \text{ es algebraico}$$

Como $\alpha \in K_0(\alpha)$ entonces:

$$\alpha \text{ es algebraico sobre } F$$

Por lo tanto:

$$L/F \text{ es algebraico} \qquad \square$$

Definición 1.2.5.47.

Lang (1971) mencionó: "Diremos que un cuerpo L es algebraicamente cerrado si todo polinomio de $L[X]$, de grado ≥ 1, tiene una raíz en L" (p. 201).

Observación 1.2.5.48.

Lang (1971) mencionó: "Observemos que, si L es un cuerpo algebraicamente cerrado, y $f \in L[X]$ es de grado ≥ 1, existen $c \in L$ y $\alpha_1,\ldots,\alpha_n \in L$ tales que

$$f(X) = c(X-\alpha_1)\ldots(X-\alpha_n)$$" (p. 202).

Demostración. Sea $f(X) \in L[X]$ con $\deg f(X) = n \geq 1$

Como L es un cuerpo algebraicamente cerrado, entonces $f(X)$ tiene una raíz α_1 en L, así que existe $g(X) \in L[X]$ con $\deg g(X) = n-1$ tal que

$$f(X) = (X-\alpha_1)g(X)$$

Como $g(X) \in L[X]$ con $\deg g(X) = n-1$ y L es un cuerpo algebraicamente cerrado, entonces $g(X)$ tiene una raíz α_2 en L, asi que existe $h(X) \in L[X]$ con $\deg h(X) = n-2$ tal que

$$g(X) = (X - \alpha_2)h(X)$$

Reemplazando, se tiene:

$$f(X) = (X - \alpha_1)(X - \alpha_2)h(X)$$

El razonamiento se puede repetir por inducción y esto acabará cuando el polinomio es constante, es decir, cuando exista $c \in L$ y $\alpha_1, \alpha_2, \ldots \alpha_n \in L$ tal que:

$$f(X) = c(X - \alpha_1)\ldots(X - \alpha_n)$$ □

Teorema 1.2.5.49.

Lang (1971) mencionó: "Sea k un cuerpo. Existe un cuerpo L algebraicamente cerrado que contiene a k como subcuerpo" (p. 201).

Demostración. Sea k un cuerpo.

Sea $f = f(x) \in k[x]$ un polinomio no constante irreducible, denotemos x_f una indeterminada y consideremos el anillo de polinomios $k[\ldots, x_f, \ldots]$ generado sobre k por las variables x_f.

En este anillo de polinomios consideremos el ideal I generado por los polinomios $f(x_f)$.

Afirmación 1: El ideal $I =< f(x_f) >$ es propio, donde: $f(x_f) = \{f_1(x_{f_1}), \ldots, f_n(x_{f_n})\}$

En efecto:

Supongamos que el ideal $I =< f(x_f) >$ no es propio, entonces:

$$< f(x_f) >= k[\ldots, x_f, \ldots]$$

Entonces:

$$1 \in < f(x_f) >$$

Luego:

$$\exists\ g_i \in k[\ldots, x_f, \ldots] \text{ con } i = 1, 2, \ldots, n\ /\ \sum_{i=1}^{n} g_i f_i(x_{f_i}) = 1$$

Para $i = 1, 2, \ldots, n$ sea $x_{f_i} = x_i$ y sean $x_{n+1}, \ldots, x_m$ las variables que faltan en los polinomios g_j, $j = 1, 2, \ldots, n$. Entonces:

$$\sum_{i=1}^{n} g_i(x_1, x_2, \ldots, x_m) \cdot f_i(x_i) = 1$$

$$g_1(x_1, x_2, \ldots, x_m) \cdot f_1(x_1) + \ldots + g_n(x_1, x_2, \ldots, x_m) \cdot f_n(x_n) = 1$$

Sea F / k una extensión finita que contiene una raiz α_i de $f_i(x_i)$ para $i = 1, 2, \ldots, n$.

Reemplazando $x_i = \alpha_i$, $i = 1, 2, \ldots, n$ y sea $x_{n+1} = \ldots = x_m = 0$, se tiene:

$$g_1(\alpha_1, \alpha_2, \ldots, \alpha_m) \cdot f_1(\alpha_1) + \ldots + g_n(\alpha_1, \alpha_2, \ldots, \alpha_m) \cdot f_n(\alpha_n) = 1$$

$$g_1(\alpha_1, \alpha_2, \ldots, \alpha_m) \cdot 0 + \ldots + g_n(\alpha_1, \alpha_2, \ldots, \alpha_m) \cdot 0 = 1$$

$$0 = 1\ (\Rightarrow\Leftarrow)$$

Por lo tanto:

$$I = < f(x_f) > \text{ es un ideal propio}$$

Dado que el anillo $k[\ldots, x_f, \ldots]$ presenta identidad y el ideal $I = < f(x_f) >$ es propio de $k[\ldots, x_f, \ldots]$, por la proposición 1.2.2.27. I es contenido en un ideal maximal m, por la proposición 1.2.3.6. se tiene:

$$\exists\ L_1 = \frac{k[\ldots, x_f, \ldots]}{m} \text{ (cuerpo)}$$

Así obtenemos la aplicación canónica:

$$\sigma : k[\ldots, x_f, \ldots] \to \frac{k[\ldots, x_f, \ldots]}{m}$$

Usaremos la restricción en k :

$$\sigma|_k : k \to \frac{k[\ldots, x_f, \ldots]}{m} \ / \ \sigma|_k (a) = a + m$$

De forma análoga al teorema 1.2.5.15. (afirmación 3) se tiene que k es subcuerpo de $L_1 = \frac{k[\ldots, x_f, \ldots]}{m}$, es decir:

$$L_1 / k \text{ es una extensión de cuerpo}$$

Como $f(x_f) \in I \subset m$, de forma análoga al teorema 1.2.5.15. (afirmación 5) se tiene que cada f tienen una raíz en L_1 .

Ahora, si cada uno de los polinomios $f \in L_1[\ldots, x_f, \ldots]$, por el corolario 1.2.5.17. existe una extensión L_2 / L_1 en la que cada polinomio f tiene una raíz en L_2 .

Continuando así, obtenemos una torre de cuerpos:

$$k = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_j \subset L_{j+1} \subset \ldots \qquad (1.42)$$

Donde cada polinomio con coeficientes en L_j tiene una raíz en L_{j+1}, $\forall j = 0, 1, \ldots$

Sea $L = \bigcup_{i=0}^{\infty} L_i$ donde: L_i son cuerpos.

Afirmación 2: L es un cuerpo

En efecto:

Sean $x, y \in L = \bigcup_{i=0}^{\infty} L_i$, entonces $x, y \in L_i$; para algún $i = 0, 1, 2, \ldots$

Se puede tomar la suma $x + y$ o el producto xy en L_i , esto es independiente de la elección de i tal que $x, y \in L_i$, y define una estructura de cuerpo sobre L .

Por lo tanto:

$$L = \bigcup_{i=0}^{\infty} L_i \text{ es un cuerpo que contiene a } k$$

Afirmación 3: L es algebraicamente cerrado

En efecto:

Sea $f(x) \in L[x] \Rightarrow \exists\ a_k \in L\ /\ f(x) = \sum_{k=0}^{n} a_k x^k \in L[x]$

Entonces:

$$a_k \in \bigcup_{i=0}^{\infty} L_i\ ,\ \forall k = 0,1,\ldots,n$$

Luego:

$$a_k \in L_i\ \text{, para algún}\ i = 0,1,2,\ldots$$

Entonces:

$$f(x) \in L_i[x]\ \text{, para algún}\ i = 0,1,\ldots$$

Por el corolario 1.2.5.16. se tiene:

$$f(x)\ \text{tiene una raíz en}\ L_{i+1}\text{, para algún}\ i = 0,1,\ldots$$

Luego:

$$f(x)\ \text{tiene una raíz en}\ \bigcup_{i=0}^{\infty} L_i$$

Así se obtiene:

$$f(x)\ \text{tiene una raíz en}\ L$$

Por lo tanto:

$$L\ \text{es algebraicamente cerrado}$$ □

Observación 1.2.5.50. Sea $\mathbb{R}$ el cuerpo de los reales. Usando el teorema 1.2.5.49. nos garantiza la existencia de un cuerpo, en este caso los complejos $\mathbb{C}$ que es algebraicamente cerrado y que contiene a $\mathbb{R}$, esto es llamado el "Teorema Fundamental del Álgebra".

La demostración formal del Teorema Fundamental del Álgebra se puede ver en: [7] p. 357

Corolario 1.2.5.51.

Lang (1971) mencionó: "Sea k un cuerpo. Existe una extensión $\bar{k}$ que es algebraica sobre k y algebraicamente cerrada" (p. 202).

Demostración. Sea k un cuerpo.

Por el Teorema 1.2.5.49. existe un cuerpo L algebraicamente cerrado que contiene a k como subcuerpo.

De la construcción (1.42) del teorema 1.2.5.49. se tiene:

$$k = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n \subset \ldots$$

Con L_i subextensiones de L que son algebraicas sobre k; $\forall i = 0,1,2,\ldots$

Definamos: $\bar{k} = \bigcup_{i=0}^{\infty} L_i$ (Cuerpo)

Afirmación 1: $\bar{k} / k$ es algebraico

En efecto:

Sea $z \in \bar{k}$, entonces:

$$z \in \bigcup_{i=0}^{\infty} L_i \Rightarrow z \in L_i \text{ ; para algún } i = 0,1,\ldots$$

Como L_i / k es algebraico $\forall\ i = 0,1,\ldots$, entonces:

z es algebraica sobre k

Por lo tanto:

$$\bar{k} / k \text{ es algebraico}$$

Afirmación 2: $\bar{k}$ es algebraicamente cerrado

En efecto:

Si $\bar{k}$ es cuerpo y $f(x) \in \bar{k}[x]$ con grado $n \geq 1$, por el corolario 1.2.5.16. se tiene que existe una extensión $L / \bar{k}$ tal que $f(x)$ tiene una raíz en L.

Entonces:

$$\exists\ \alpha \in L\ /\ f(\alpha) = 0$$

Es decir:

$$\alpha \text{ es algebraico sobre } \bar{k}$$

De la afirmación 1, se tiene:

$$\bar{k} / k \text{ es algebraico}$$

Usando el teorema 1.2.5.46. se tiene:

$$\alpha \text{ es algebraico sobre } k$$

Ordenando, tenemos que $\alpha \in L \ \wedge\ \alpha$ es algebraico sobre k, entonces:

$$\alpha \in L_i \text{, para algún } i = 0,1,\ldots$$

Luego:

$$\alpha \in \bar{k}$$

Por lo tanto:

$\bar{k}$ es algebraicamente cerrada □

Definición 1.2.5.52.

Zaldivar (1996) mencionó: "Sea k un campo. Una cerradura algebraica de k es una extensión L/k tal que

(i) L/k es algebraica.

(ii) L es algebraicamente cerrado" (p. 72).

Ejemplo 1.2.5.53.

Zaldivar (1996) mencionó: "Como $\mathbb{C}$ es algebraicamente cerrado y $\mathbb{C}/\mathbb{R}$ es finita, entonces $\mathbb{C}$ es una cerradura algebraica de $\mathbb{R}$.

Nótese que $\mathbb{C}$ no es una cerradura algebraica de $\mathbb{Q}$ ya que $\mathbb{C}/\mathbb{Q}$ no es algebraica" (p. 72).

Definición 1.2.5.54.

Herstein (1970) mencionó: "Si $f(x) \in F[x]$, una extensión finita E de F se dice que es un campo de descomposición de $f(x)$ sobre F si $f(x)$ puede ser descompuesto en un producto de factores lineales sobre E (es decir, en $E[x]$), pero no en ningún subcampo propio de E" (p. 214).

Ejemplo 1.2.5.55. Veamos los siguientes ejemplos que nos harán entender la relación entre el cuerpo de descomposición y las raíces:

a. El cuerpo de descomposición para $p(x) = x^2 - 2 \in \mathbb{Q}[x]$ es el cuerpo $\mathbb{Q}(\sqrt{2})$, pues las dos raíces son $\sqrt{2}$, $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, pero vemos que no se puede descomponer en $\mathbb{Q}$.
b. El cuerpo de descomposición para $q(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ es el cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ generado sobre $\mathbb{Q}$ por $\sqrt{2}$ y $\sqrt{3}$, pues las raíces del polinomio son

$\pm\sqrt{2}$ y $\pm\sqrt{3}$, pero vemos que no se puede descomponer en $\mathbb{Q}(\sqrt{2})$ ni en $\mathbb{Q}(\sqrt{3})$.

Definición 1.2.5.56.

Zaldivar (1996) mencionó: "Un polinomio irreducible $f(x) \in k[x]$ se llama separable sobre k si no tiene raíces múltiples (en su campo de descomposición). Un polinomio irreducible $f(x) \in k[x]$ se llama inseparable (sobre k) si no es separable" (p. 98).

Definición 1.2.5.57.

Zaldivar (1996) mencionó: "Si L/k es una extensión, un elemento $\alpha \in L$ algebraico sobre k , se llama separable sobre k , si $Irr(\alpha, k) \in k[x]$ es separable" (p. 101).

Definición 1.2.5.58.

Zaldivar (1996) mencionó: "Una extensión algebraica L/k es separable si todo $\alpha \in L$ es separable sobre k" (p. 101).

Proposición 1.2.5.59.

Zaldivar (1996) mencionó: "Sea L/k una extensión algebraica separable. Si $k \subseteq M \subseteq L$ es un campo intermedio, entonces las subextensiones L/M y M/k también son separables" (p. 101).

Demostración. Demostremos por medio de afirmaciones:

Afirmación 1: M/k es separable.

En efecto:

Sea $\alpha \in M \subset L \ \wedge \ L/k$ es separable, entonces:

α es separable sobre k

Por lo tanto:

$$M / k \text{ es separable}$$

Afirmación 2: L / M es separable.

En efecto:

Sea $\alpha \in L$ un elemento arbitrario, y sean $m_k(x) = Irr(\alpha, k, x) \in k[x]$ y

$m_M(x) = Irr(\alpha, M, x) \in M[x]$.

En $M[x]$, usando la proposición 1.2.5.21. se tiene:

$$m_M(x) \mid m_k(x) \qquad (1.43)$$

Como $\alpha \in L \ \wedge \ L / k$ es separable $\Rightarrow \alpha$ es separable sobre k

Entonces:

$$m_k(x) \text{ es separable sobre } k$$

Es decir:

$$m_k(x) \text{ no tiene raíces múltiples} \qquad (1.44)$$

Como $m_M(x)$ es un factor de $m_k(x)$, de (1.43) y (1.44) se obtiene:

$$m_M(x) \text{ no tiene raíces múltiples}$$

Es decir:

$$Irr(\alpha, M, x) \text{ no tiene raíces múltiples}$$

Entonces:

$$\alpha \text{ es separable sobre } M$$

Por lo tanto:

L / M es separable □

Definición 1.2.5.60.

Zaldivar (1996) mencionó: "Si $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in k[x]$, su derivada es el polinomio

$f'(x) := a_1 + 2a_2 x + \ldots + n a_n x^{n-1} \in k[x]$ " (p. 99).

Lema 1.2.5.61.

Zaldivar (1996) mencionó: "Sea k un campo. Un polinomio $f(x) \in k[x]$ no cero, tiene una raíz múltiple (en un campo de descomposición) si y sólo si f y f' tienen un factor de grado ≥ 1 en $k[x]$" (p. 99).

Demostración. (Ver demostración en [5], p. 547) □

Corolario 1.2.5.62.

Dummit D. y Foote R. (2004) mencionaron: "Every irreducible polynomial over a field of characteristic 0 (for example, $\mathbb{Q}$) is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials" (p. 547).

Demostración. (Ver demostración en [5], pp. 547-548) □

Observación 1.2.5.63. El corolario 1.2.5.62. nos garantiza que alguna extensión finita de $\mathbb{Q}$ es separable ya que todo polinomio irreducible en $\mathbb{Q}[x]$ es separable y por medio de los cuerpos intermedios, por la proposición 1.2.5.59. nos garantiza que existen subextensiones separables.

CAPÍTULO 2

MATERIALES Y MÉTODOS

Materiales:

1. Libros
2. Papers
3. Copias de artículos
4. Útiles de escritorio
5. Computadora
6. Impresora
7. Programa Word

Métodos:

El presente trabajo corresponde a un tipo de “Investigación Básica”, ya que profundizamos los conocimientos ya existidos en la realidad y de esta forma se construye un mayor conocimiento.

El procedimiento de este trabajo de investigación fue en primer lugar recopilar toda la información necesaria en los libros y papers para así después empezar a revisar y armar el trabajo.

A continuación se separará este trabajo en 3 capítulos para así tener una secuencia correcta, de esta forma se podrá avanzar de forma ordenada y exponer ante mi asesor los primeros capítulos hasta concluirlo.

Después de haber expuesto y en conforme con mi asesor seguirá el tipeo de todo el contenido del trabajo de tesis. Finalmente se imprimirá el trabajo de tesis completo y ordenado.

CAPÍTULO 3

RESULTADOS

La Teoría de Galois lleva su nombre en honor a Evariste Galois (1811-1832) que a pesar de fallecer antes de cumplir 21 años y de no ser reconocido en su época, fue quien dio respuesta al problema de la solubilidad de ecuaciones algebraicas por medio de radicales y de paso creó una de las más hermosas teorías algebraicas.

En este capítulo presentaremos los elementos de la Teoría de Galois, las demostraciones del Teorema Fundamental de las Funciones Racionales Simétricas y del Teorema Fundamental de Galois y finalmente la demostración del Teorema de Artin.

3.1. Teoría de Galois

3.1.1. Grupo de Automorfismos y el Cuerpo Fijo

Definición 3.1.1.1.

Herstein (1970) mencionó:

> Sea K un campo y sea F un subcampo de K. Entonces el grupo de automorfismos de K relativos a F, que representaremos por $G(K,F)$, es el conjunto de todos los automorfismos de K que dejan fijos todos los elementos de F; es decir, el automorfismo σ de K está en $G(K,F)$ si y sólo si $\sigma(\alpha)=\alpha$ para todo $\alpha \in F$. (p. 231)

Lema 3.1.1.2.

Herstein (1970) mencionó: "$G(K,F)$ es un subgrupo del grupo de todos los automorfismos de K" (p. 231).

Demostración. Veamos:

a. Por la definición 3.1.1.1. se tiene $G(K,F) \subset Aut(K)$

b. Sean automorfismos $\sigma,\ \tau \in G(K,F) \ \wedge\ \tau \neq 0 \ \Rightarrow\ \sigma,\tau \in Aut(K)$ /

$$\sigma(x) = x, \forall x \in F \wedge \tau(x) = x, \forall x \in F \tag{3.1}$$

Como $\tau \in Aut(K) \ \wedge\ \tau \neq 0 \ \Rightarrow\ \exists\ \tau^{-1} \in Aut(K)$

Luego:

$$\sigma \circ \tau^{-1} \in Aut(K)$$

De (3.1) se tiene:

$$\tau(x) = x \ \Rightarrow\ \tau^{-1}(\tau(x)) = \tau^{-1}(x) \ \Rightarrow\ (\tau^{-1} \circ \tau)(x) = \tau^{-1}(x)$$

$$\Rightarrow id(x) = \tau^{-1}(x) \ \Rightarrow\ x = \tau^{-1}(x) \ \Rightarrow\ \tau^{-1} \in G(K,F)$$

Además, para todo $x \in F$ se cumple:

$$(\sigma \circ \tau^{-1})(x) = \sigma(\tau^{-1}(x)) = \sigma(x) = x$$

Entonces:

$$\sigma \circ \tau^{-1} \in G(K,F)$$

Por lo tanto, por el lema 1.2.1.4. se tiene:

$G(K,F)$ es un subgrupo del grupo $(Aut(K),\circ)$ □

Definición 3.1.1.3.

Herstein (1970) mencionó: "Si G es un grupo de automorfismos de K, entonces el campo fijo de G es el conjunto de todos los elementos $a \in K$ tales que $\sigma(a) = a$ para todo $\sigma \in G$" (p. 230).

La notación que usaremos para el cuerpo fijo (campo fijo), según el contexto de Herstein, será: K_G

Lema 3.1.1.4.

Herstein (1970) mencionó: “El campo fijo de G es un subcampo de K ” (p. 230).

Demostración.

Por la definición 3.1.1.3. se tiene $K_G \subset K$

a. Sean $a,b \in K_G$, se tiene:

$$a,b \in K \ / \ \sigma(a) = a \ \wedge \ \sigma(b) = b \ ; \ \forall \sigma \in G$$

Por la definición de homomorfismo, se tiene:

$$a-b \in K \ / \ \sigma(a-b) = \sigma(a) - \sigma(b) = a-b$$

$$a-b \in K_G$$

b. Sean $a,b \in K_G - \{0\} \ \Rightarrow \ a,b \in K_G$, se tiene:

$$a,b \in K \ / \ \sigma(a) = a \ \wedge \ \sigma(b) = b \ ; \ \forall \sigma \in G$$

Como $b \in K \ \Rightarrow \ \exists! \ b^{-1} \in K$ luego por la definición de homomorfismo, se tiene:

$$a \cdot b^{-1} \in K \ / \ \sigma(a \cdot b^{-1}) = \sigma(a) \cdot \sigma(b^{-1})$$

Por el teorema 1.2.3.12. (parte 2) se tiene:

$$\sigma(a \cdot b^{-1}) = \sigma(a) \cdot (\sigma(b))^{-1} = a \cdot b^{-1}$$

$$a.b^{-1} \in K_G - \{0\}$$

Por lo tanto, del teorema 1.2.3.4. se obtiene:

K_G es un subcampo de K □

Observación 3.1.1.5. Veamos un ejemplo para entender estas definiciones:

Sea L el cuerpo de los números complejos y sea k el cuerpo de los números reales. Veamos quien es $G(L,k)$.

Si $\sigma \in G(L,k)$ es un automorfismo cualquiera que va de L en L, se puede ver:

$$(\sigma(i))^2 = \sigma(i)\cdot\sigma(i) = \sigma(i^2) = \sigma(-1) = -\sigma(1)$$

Por el teorema 1.2.3.12. (parte 2) se tiene:

$$(\sigma(i))^2 = -1$$

$$\sigma(i) = \pm i \qquad (3.2)$$

Si además, σ deja fijos a todos los reales, entonces para cualquier $a+bi \in L$ donde $a,b \in k$ se tiene que:

$$\sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i)$$

Usando (3.2) se tiene:

$$\sigma(a+bi) = a \pm bi$$

Así obtenemos los siguientes automorfismos de L:

$$\sigma_1(a+bi) = a+bi$$

$$\sigma_2(a+bi) = a-bi$$

Se puede ver que σ_1 es el automorfismo identidad y σ_2 es la conjugación compleja.

Por lo tanto:

$G(L,k) = \{\sigma_1, \sigma_2\}$ es un grupo de orden 2

Ahora, veamos quien es el cuerpo fijo de $G(L,k)$

Afirmación 1: $k \subset L_{G(L,k)}$

En efecto:

Sean $z \in k \ \wedge \ \sigma \in G(L,k)$, entonces:

$$\sigma : L \to L \text{ (Automorfismo) } / \ \sigma(z) = z \ ; \ \forall z \in k$$

Luego:

$$z \in L \ / \ \sigma(z) = z \ ; \ \forall \sigma \in G(L,k)$$

Entonces:

$$z \in L_{G(L,k)}$$

Por lo tanto:

$$k \subset L_{G(L,k)}$$

Afirmación 2: $L_{G(L,k)} \subset k$

Sea $z = a + bi \in L_{G(L,k)}$ con $a,b \in k$, entonces:

$$z \in L \ / z = \sigma_2(z) \ , \ \sigma_2 \in G(L,k)$$

$$a + bi = \sigma_2(a + bi)$$

Luego:

$$a + bi = a - bi$$

$$b = 0$$

Entonces:

$$z = a + bi = a \in k$$

Por lo tanto:

$$L_{G(L,k)} \subset k$$

Finalmente, de las afirmaciones 1 y 2 se obtiene:

$$L_{G(L,k)} = k \qquad \square$$

Teorema 3.1.1.6.

Herstein (1970) mencionó: "Si K es un campo y si $\sigma_1,\ldots,\sigma_n$ son distintos automorfismos de K, entonces es imposible encontrar elementos $a_1,\ldots,a_n$, no todos 0, en K, tales que $a_1\sigma_1(u)+a_2\sigma_2(u)+\ldots+a_n\sigma_n(u)=0$ para todo $u \in K$" (p. 229).

Demostración. Supongamos que pudiéramos encontrar un conjunto de elementos $a_1, a_2, \ldots, a_m$ en K, no todos ceros, tales que:

$$a_1\sigma_1(u)+a_2\sigma_2(u)+\ldots+a_n\sigma_n(u)=0\,;\ \forall u \in K$$

Entonces podríamos encontrar una relación tal que tuviera tan pocos términos como fuera posible; renumerando, si fuera preciso, podemos suponer que esta relación mínima es:

$$a_1\sigma_1(u)+a_2\sigma_2(u)+\ldots+a_m\sigma_m(u)=0 \qquad (3.3)$$

Donde: $a_1, a_2, \ldots, a_m$ son todos diferentes de 0.

Si $u=0$, entonces:

$$\sigma_1(u)=\sigma_2(u)=\ldots=\sigma_m(u) \quad (\Rightarrow\Leftarrow)$$

Pues: $\sigma_1, \sigma_2, \ldots, \sigma_n$ son distintos automorfismos de K

Si $u \neq 0$, analizemos los siguientes casos:

Para $m = 1$ entonces:

$$a_1 \cdot \sigma_1(u) = 0 \tag{3.4}$$

Si $\sigma_1(u) \neq 0$, entonces en (3.4)

$$a_1 \cdot \sigma_1(u) \cdot \sigma_1^{-1}(u) = 0 \cdot \sigma_1^{-1}$$

$$a_1 = 0 \ (\Rightarrow\Leftarrow)$$

Si $\sigma_1(u) = 0$, y por ser σ_1 homomorfismo de cuerpos, se tiene:

$$\sigma_1(u) = \sigma_1(0)$$

Pero σ_1 es inyectiva, entonces:

$$u = 0 \ (\Rightarrow\Leftarrow)$$

Para $m > 1$ entonces:

Como los automorfismos son distintos hay un elemento $c \in K$ tal que

$$\sigma_1(c) \neq \sigma_m(c) \tag{3.5}$$

Como $cu \in K$, $\forall u \in K$, la relación (3.3) debe también verificarse para cu , es decir:

$$a_1\sigma_1(cu) + a_2\sigma_2(cu) + \ldots + a_m\sigma_m(cu) = 0; \forall u \in K \tag{3.6}$$

Usando la hipótesis de que las σ son automorfismos de K, esta relación (3.6) toma la forma:

$$a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_2(c)\sigma_2(u) + \ldots + a_m\sigma_m(c)\sigma_m(u) = 0 \tag{3.7}$$

Luego, multiplicando la relación (3.3) por $\sigma_1(c)$

$$a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_1(c)\sigma_2(u) + \ldots + a_m\sigma_1(c)\sigma_m(u) = 0 \tag{3.8}$$

Restando (3.7) y (3.8) entonces:

$$a_2(\sigma_2(c)-\sigma_1(c))\sigma_2(u)+\ldots+a_m(\sigma_m(c)-\sigma_1(c))\sigma_m(u)=0$$

Haremos que: $b_i=a_i(\sigma_i(c)-\sigma_1(c))\in L$ para $i=2,3,\ldots,m$

Por otro lado:

$$b_i=a_i(\sigma_i(c)-\sigma_1(c))\neq 0 \text{ , para } i=2,3,\ldots,m$$

Pues de (3.5): $\sigma_m(c)-\sigma_1(c)\neq 0$ con $m>1$ y $a_i\neq 0$

Así, reemplazando obtenemos:

$$b_2\sigma_2(u)+b_3\sigma_3(u)+\ldots+b_m\sigma_m(u)=0\,;\ \forall u\neq 0\in K\ \ (\Rightarrow\Leftarrow)$$

Se obtiene una contradicción pues esto produce una relación más corta, en contra de la elección que hicimos. □

Teorema 3.1.1.7.

Herstein (1970) mencionó: "Si K es una extensión finita de F, entonces $G(K,F)$ es un grupo finito y su orden, $\circ(G(K,F))$, satisface $\circ(G(K,F))\leq[K:F]$" (p. 232).

Demostración. Sea $[K:F]=n$ y $\{u_1,u_2,\ldots,u_n\}$ es una base de K sobre F.

Supongamos que $\circ(G(K,F))>[K:F]$ es decir, podemos encontrar $n+1$ automorfismos distintos $\sigma_1,\sigma_2,\ldots,\sigma_{n+1}\in G(K,F)$

De acuerdo con el corolario del teorema de las ecuaciones lineales homogéneas (ver demostración en [9], p. 177), el sistema de n ecuaciones lineales homogéneas en las $n+1$ incógnitas $x_1,x_2,\ldots,x_{n+1}$:

$$\sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \ldots + \sigma_{n+1}(u_1)x_{n+1} = 0$$

$$\vdots$$

$$\sigma_1(u_i)x_1 + \sigma_2(u_i)x_2 + \ldots + \sigma_{n+1}(u_i)x_{n+1} = 0$$

$$\vdots$$

$$\sigma_1(u_n)x_1 + \sigma_2(u_n)x_2 + \ldots + \sigma_{n+1}(u_n)x_{n+1} = 0$$

tiene una solución no trivial (no todos ceros), entonces:

$$x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_{n+1} = \alpha_{n+1} \text{ en } K$$

Luego:

$$\alpha_1\sigma_1(u_j) + \alpha_2\sigma_2(u_j) + \ldots + \alpha_{n+1}\sigma_{n+1}(u_j) = 0, \forall j = 1, 2, \ldots, n \qquad (3.9)$$

Sea $t \in K$ y como $\{u_1, u_2, \ldots, u_n\}$ es una base de K sobre F, entonces:

$$\exists\ c_1, c_2, \ldots, c_n \in F\ /\ t = c_1u_1 + c_2u_2 + \ldots + c_nu_n$$

Entonces:

$$\sigma_i(t) = \sigma_i(c_1u_1 + c_2u_2 + \ldots + c_nu_n),\ \forall\ i = 1, 2, \ldots, n+1$$

Como cada uno de los σ_i deja fijo a todo elemento de F, luego:

$$\sigma_i(t) = c_1\sigma_i(u_1) + c_2\sigma_i(u_2) + \ldots + c_n\sigma_i(u_n)$$

$$\sigma_i(t) = \sum_{j=1}^{n} c_j\sigma_i(u_j)$$

Por otro lado:

$$\alpha_1\sigma_1(t) + \alpha_2\sigma_2(t) + \ldots + \alpha_{n+1}\sigma_{n+1}(t) = \sum_{i=1}^{n+1} \alpha_i\sigma_i(t)$$

$$\alpha_1\sigma_1(t)+\alpha_2\sigma_2(t)+\ldots+\alpha_{n+1}\sigma_{n+1}(t)=\sum_{i=1}^{n+1}\alpha_i\sum_{j=1}^{n}c_j\sigma_i(u_j)$$

$$\alpha_1\sigma_1(t)+\alpha_2\sigma_2(t)+\ldots+\alpha_{n+1}\sigma_{n+1}(t)=\sum_{j=1}^{n}c_j(\sum_{i=1}^{n+1}\alpha_i\sigma_i(u_j))$$

Usando (3.9) se obtiene:

$$\alpha_1\sigma_1(t)+\alpha_2\sigma_2(t)+\ldots+\alpha_{n+1}\sigma_{n+1}(t)=\sum_{j=1}^{n}c_j.(0)$$

$$\alpha_1\sigma_1(t)+\alpha_2\sigma_2(t)+\ldots+\alpha_{n+1}\sigma_{n+1}(t)=0$$

Así, obtenemos:

$$\alpha_1\sigma_1(t)+\alpha_2\sigma_2(t)+\ldots+\alpha_{n+1}\sigma_{n+1}(t)=0,\ \forall t\in K\ \ (\Rightarrow\Leftarrow)$$

Pero esto contradice al teorema 3.1.1.6. por lo tanto:

$$\circ(G(K,F))\leq[K:F]$$ □

3.1.2. El Teorema Fundamental de las Funciones Racionales Simétricas

Las definiciones y resultados ya vistos son importantes para el teorema principal, pero no basta, en esta parte haremos actuar el grupo S_n sobre un cuerpo, construir las funciones simétricas elementales, demostrar unos resultados, y por último demostrar el Teorema Fundamental de las Funciones Racionales Simétricas.

Observación 3.1.2.1.

Herstein (1970) mencionó:

> Sea S_n el grupo simétrico de grado n considerado como si actuara sobre el conjunto $[1,2,\ldots,n]$; para $\sigma\in S_n$ e i un entero con $1\leq i\leq n$, sea $\sigma(i)$ la imagen de i bajo σ. Podemos hacer actuar a S_n sobre $F(x_1,\ldots,x_n)$ en la siguiente forma: para $\sigma\in S_n$ y $r(x_1,\ldots,x_n)\in F(x_1,\ldots,x_n)$, definimos la aplicación que lleva $r(x_1,\ldots,x_n)$ sobre $r(x_{\sigma(1)},\ldots,x_{\sigma(n)})$. Representaremos a esta aplicación de $F(x_1,\ldots,x_n)$ sobre sí mismo

también por σ . Es obvio que estas aplicaciones definen automorfismos de $F(x_1,\ldots,x_n)$. (p. 233)

Observación 3.1.2.2. Debido a la definición de ψ se puede ver:

$$(S_n,\circ) \text{ es subgrupo del grupo } (Aut(F(x_1,\ldots,x_n)),\circ)$$

Demostración. Sabemos que $(S_n,\circ)$ y $(Aut(F(x_1,\ldots,x_n)),\circ)$ son grupos. Además:

Sea $\sigma \in S_n$, por definición de ψ

$$\sigma \in Aut(F(x_1,\ldots,x_n))$$

Entonces:

$$S_n \subset Aut(F(x_1,\ldots,x_n))$$

Por lo tanto:

$$(S_n,\circ) \text{ es subgrupo del grupo } (Aut(F(x_1,\ldots,x_n)),\circ) \qquad \square$$

Observación 3.1.2.3.

Como S_n es subgrupo del grupo $Aut(F(x_1,\ldots,x_n))$ entonces podemos hablar del cuerpo fijo de S_n . El cuerpo fijo $F(x_1,\ldots,x_n)_{S_n}$ por definición se tiene a todas las funciones racionales $r(x_1,x_2,\ldots,x_n) \in F(x_1,x_2,\ldots,x_n)$ tales que:

$$\sigma(r(x_1,x_2,\ldots,x_n)) = r(x_1,x_2,\ldots,x_n)\,;\ \forall \sigma \in S_n$$

Por definición de σ se tiene:

$$r(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)}) = r(x_1,x_2,\ldots,x_n)\,;\ \forall \sigma \in S_n$$

Herstein (1970) mencionó: “Pero estos son precisamente aquellos elementos en $F(x_1,\ldots,x_n)$ que se conocen como funciones racionales simétricas. Como son el campo fijo de S_n forman

un subcampo de $F(x_1,\ldots,x_n)$ llamado el campo de las funciones racionales simétricas al que representaremos por S " (p. 234).

Es decir:

$$S=\left\{r(x_1,\ldots,x_n)\in F(x_1,\ldots,x_n)\,/\,r(x_1,\ldots,x_n)=r(x_{\sigma(1)},\ldots,x_{\sigma(n)});\forall\sigma\in S_n\right\}$$

En conclusión:

$$F(x_1,\ldots,x_n)_{S_n}=S \ \wedge\ S \text{ es subcuerpo de } F(x_1,\ldots,x_n)$$

Definición 3.1.2.4.

Herstein (1970) mencionó: "Podemos presentar explícitamente algunas funciones particularmente sencillas de S construidas con $x_1,\ldots,x_n$ conocidas como funciones simétricas elementales en $x_1,\ldots,x_n$. Las definimos como sigue:

$$a_1=x_1+x_2+\ldots+x_n=\sum_{i=1}^{n}x_i$$

$$a_2=\sum_{i<j}x_ix_j$$

$$a_3=\sum_{i<j<k}x_ix_jx_k$$

$$\vdots$$

$$a_n=x_1x_2\ldots x_n.$$

Para $n=2,3y4$ las escribimos explícitamente a continuación.

$n=2$

$$a_1 = x_1 + x_2 .$$

$$a_2 = x_1 x_2 .$$

$n = 3$

$$a_1 = x_1 + x_2 + x_3 .$$

$$a_2 = x_1 x_2 + x_1 x_3 + x_2 x_3 .$$

$$a_3 = x_1 x_2 x_3 .$$

$n = 4$

$$a_1 = x_1 + x_2 + x_3 + x_4 .$$

$$a_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 .$$

$$a_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4 .$$

$$a_4 = x_1 x_2 x_3 x_4$$ " (p. 234).

Observación 3.1.2.5.

Veamos que:

Para: $n = 2$

x_1 y x_2 son las raíces de $t^2 - a_1 t + a_2$

Para: $n = 3$

x_1, x_2 y x_3 son las raíces de $t^3 - a_1 t^2 + a_2 t - a_3$

En general:

$x_1, \ldots, x_n$ son las raíces de $t^n - a_1 t^{n-1} + \ldots + (-1)^n a_n$

Proposición 3.1.2.6.

Dummit D. y Foote R. (2004) mencionaron: “The association of groups to fields and fields to groups defined above is inclusion reversing, namely

1. if $F_1 \subseteq F_2 \subseteq K$ are two subfields of K then $Aut(K / F_2) \leq Aut(K / F_1)$, and
2. if $H_1 \leq H_2 \leq Aut(K)$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2, respectively, then $F_2 \subseteq F_1$” (p. 560).

Demostración. Veamos:

1. Sabemos que $Aut(K / F_1)$ y $Aut(K / F_2)$ son grupos de automorfismos.

   Sea $\sigma \in Aut(K / F_2) \Rightarrow \sigma \in Aut(K) \ / \ \sigma(x) = x ; \ \forall x \in F_2$

   Para todo automorfismo de K que deja fijo F_2 también deja fijo al subcuerpo F_1, entonces:

   $$\sigma \in Aut(K) \ / \ \sigma(z) = z ; \ \forall x \in F_1$$

   $$\sigma \in Aut(K / F_1)$$

   Por lo tanto:

   $$Aut(K / F_2) \subset Aut(K / F_1)$$

   Se concluye que

   $Aut(K / F_2)$ es subgrupo de $Aut(K / F_1)$

2. Sabemos que F_1 y F_2 son cuerpos.

   Sea $z \in F_2 \Rightarrow z \in K \ / \ \sigma(z) = z ; \ \forall \sigma \in H_2$

   Pero si cumple para H_2 también cumple para el subgrupo H_1, entonces:

   $$z \in K \ / \ \sigma(z) = z ; \ \forall \sigma \in H_1$$

$$z \in F_1$$

Por lo tanto:

$$F_2 \subset F_1$$

Se concluye que

F_2 es subcuerpo de F_1 □

Teorema 3.1.2.7. (Teorema Fundamental de las Funciones Racionales Simétricas)

Herstein (1970) mencionó:

Sea F un campo y $F(x_1,\ldots,x_n)$ el campo de las funciones racionales en $x_1,\ldots,x_n$ sobre F. Supongamos que S es el campo de las funciones racionales simétricas; entonces

1. $[F(x_1,\ldots,x_n):S]=n!$.
2. $G(F(x_1,\ldots,x_n),S)=S_n$, el grupo simétrico de grado n.
3. Si $a_1,\ldots,a_n$ son las funciones simétricas elementales en $x_1,\ldots,x_n$, entonces $S=F(a_1,\ldots,a_n)$.
4. $F(x_1,\ldots,x_n)$ es el campo de descomposición sobre $F(a_1,\ldots,a_n)=S$ del polinomio $t^n-a_1t^{n-1}+a_2t^{n-2}\ldots+(-1)^n a_n$. (pp. 235-236)

Demostración. Demostraremos las siguientes afirmaciones:

Afirmación 1: $S_n \subset G(F(x_1,x_2,\ldots,x_n),S)$

En efecto:

De la observación 3.1.2.2. se tiene que S_n es subgrupo de $Aut(F(x_1,x_2,\ldots,x_n))$

Sea $\sigma \in S_n \Rightarrow \sigma \in Aut(F(x_1,x_2,\ldots,x_n))$

Sea $r(x_1,\ldots,x_n) \in S$, por la observación 3.1.2.3. se tiene:

$$r(x_1,\ldots,x_n) \in S = F(x_1,\ldots,x_n)_{S_n}$$

$$\sigma(r(x_1,\ldots,x_n)) = r(x_1,\ldots,x_n)$$

Luego:

$$\sigma \in Aut(F(x_1,\ldots,x_n)) \ / \ \sigma(r(x_1,\ldots,x_n)) = r(x_1,\ldots,x_n) \ ; \ \forall \ \ r(x_1,\ldots,x_n) \in S$$

Así se obtiene:

$$\sigma \in G(F(x_1,x_2,\ldots,x_n),S)$$

Por lo tanto:

$$S_n \subset G(F(x_1,x_2,\ldots,x_n),S)$$

Sean $a_1,a_2,\ldots,a_n$ las funciones simétricas elementales en $x_1,x_2,\ldots,x_n$

Afirmación 2: $F(a_1,a_2,\ldots,a_n)$ es un subcuerpo de S

a. Sabemos que $F(a_1,a_2,\ldots,a_n)$ y S son cuerpos.

b. Sea $r(a_1,a_2,\ldots,a_n) \in F(a_1,a_2,\ldots,a_n)$

   Como $a_1,a_2,\ldots,a_n$ son funciones simétricas elementales, es decir $a_1,a_2,\ldots,a_n \in S$ y $F \subset S$ ($\forall$ $p(x)$ cte es simétrico), entonces:

$$r(a_1,a_2,\ldots,a_n) = \frac{p(a_1,a_2,\ldots,a_n)}{q(a_1,a_2,\ldots,a_n)} \in S$$

   Luego:

$$r(a_1,a_2,\ldots,a_n) \in S$$

   Por lo tanto:

$$F(a_1, a_2, \ldots, a_n) \subset S$$

Se concluye que:

$F(a_1, a_2, \ldots, a_n)$ es un subcuerpo de S

Demostración parte 1 y 3:

Sea $p(t) \in F(a_1, \ldots, a_n)[t]$ de grado n, por el teorema 1.2.5.18. obtenemos:

$$[F(x_1, \ldots, x_n) : F(a_1, \ldots, a_n)] \leq n!$$

De la afirmación 2 se tiene:

$$\exists \ S / F(a_1, \ldots, a_n)$$

Por el teorema 1.2.5.6. se tiene:

$$[F(x_1, \ldots, x_n) : S][S : F(a_1, \ldots, a_n)] \leq n! \qquad (3.10)$$

Por otro lado, de la afirmación 1:

$$S_n \subset G(F(x_1, \ldots, x_n), S)$$

$$n! = \circ(S_n) \leq \circ(G(F(x_1, \ldots, x_n), S))$$

Además, $F(x_1, \ldots, x_n) / F(a_1, \ldots, a_n)$ es finito, por el corolario 1.2.5.7. $F(x_1, \ldots, x_n) / S$ y $S / F(a_1, \ldots, a_n)$ son finitos.

Por el teorema 3.1.1.7. se tiene:

$$n! = \circ(S_n) \leq \circ(G(F(x_1, \ldots, x_n), S)) \leq [F(x_1, \ldots, x_n) : S]$$

$$n! \leq [F(x_1, \ldots, x_n) : S] \qquad (3.11)$$

De (3.10) y (3.11) se obtiene:

$$[S : F(a_1,\ldots,a_n)] = 1 \ \wedge\ [F(x_1,\ldots,x_n) : S] = n!$$

Por lo tanto, usando la observación 1.2.5.5. se obtiene:

$$S = F(a_1,\ldots,a_n) \ \wedge\ [F(x_1,\ldots,x_n) : S] = n!$$

Demostración parte 2:

De la afirmación 1 se tiene:

$$S_n \subset G(F(x_1,x_2,\ldots,x_n),S) \tag{3.12}$$

Usando el teorema 3.1.1.7. y la parte 1 se tiene:

$$n! \leq \circ(G(F(x_1,\ldots,x_n),S)) \leq [F(x_1,\ldots,x_n) : S] = n!$$

$$\circ(G(F(x_1,\ldots,x_n),S)) = n! \tag{3.13}$$

De (3.12) y (3.13) se concluye:

$$G(F(x_1,x_2,\ldots,x_n),S) = S_n$$

Demostración parte 4:

Sea $p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} - \ldots + (-1)^n a_n \in F(a_1,\ldots,a_n)[t]$

De la observación 3.1.2.5. se tiene:

$x_1, x_2, \ldots, x_n$ son las raíces de $p(t)$

Entonces:

$$p(t) = (t - x_1).(t - x_2)\ldots(t - x_n) \in F(x_1,\ldots,x_n)[t]$$

Por lo tanto:

$p(t)$ se descompone en un producto de factores lineales sobre $F(x_1,\ldots,x_n)$

Por otro lado:

Supongamos que $p(t) \in F(a_1,\ldots,a_n)[t]$ puede descomponerse sobre un subcuerpo propio de $F(x_1,\ldots,x_n)$ que contenga a $F(a_1,\ldots,a_n)$, entonces:

$$\exists H \subset_{\neq} F(x_1,\ldots,x_n) \text{ (Propio) } / F(a_1,\ldots,a_n) \subset H \tag{3.14}$$

$$F \subset H \wedge a_1, a_2, \ldots, a_n \in H \tag{3.15}$$

Como $p(t)$ puede descomponerse en $H[t]$, entonces:

$$p(t) = (t-x_1)\cdot(t-x_2)\ldots(t-x_n); x_i \in H, \forall i = 1,2,\ldots,n \tag{3.16}$$

Entonces de (3.15) y (3.16)

$$F \subset H \ \wedge \ x_1, x_2, \ldots, x_n \in H$$

$$F(x_1, x_2, \ldots, x_n) \subset H \tag{3.17}$$

Por lo tanto, de (3.14) y (3.17) se obtiene:

$$F(x_1, x_2, \ldots, x_n) = H \quad (\Rightarrow\Leftarrow)$$

Entonces $p(t)$ no puede descomponerse en ningún subcuerpo propio de $F(x_1,\ldots,x_n)$.

Además, hemos visto $F(x_1,\ldots,x_n) / F(a_1,\ldots,a_n)$ es finito.

Finalmente, se concluye:

$F(x_1,\ldots,x_n)$ es el cuerpo de descomposición de $p(t)$ sobre $F(a_1,\ldots,a_n)$ □

3.1.3. Extensión Normal

Definición 3.1.3.1.

Herstein (1970) mencionó: " K es una extensión normal de F si K es una extensión finita de F tal que F es el campo fijo de $G(K,F)$ " (p. 236).

Teorema 3.1.3.2.

Herstein (1970) mencionó: "Sea K una extensión normal de F y sea H un subgrupo de $G(K,F)$; sea $K_H = \{x \in K / \sigma(x) = x$ para toda $\sigma \in H\}$ el campo fijo de H . Entonces:

1. $[K : K_H] = \circ(H)$.
2. $H = G(K, K_H)$

(En particular, cuando $H = G(K,F)$, $[K : F] = \circ(G(K,F))$.)" (p. 236).

Demostración. Vamos a demostrar que $[K : K_H] = \circ(H)$, pero por medio de afirmaciones.

Afirmación 1: $H \subset G(K, K_H)$

En efecto:

Sea $\sigma \in H \subset G(K,F) \subset Aut(K) \Rightarrow \sigma \in Aut(K)$

Sea $x \in K_H \Rightarrow x \in K \ / \ \sigma(x) = x$

Luego:

$$\sigma \in Aut(K) \ / \ \sigma(x) = x; \ \forall \ x \in K_H$$

Así se obtiene:

$$\sigma \in G(K, K_H)$$

Por lo tanto:

$$H \subset G(K, K_H)$$

Afirmación 2: K / K_H es una extensión finita

En efecto:

Tenemos que H es subgrupo de $G(K, F)$ entonces:

$$H \subset G(K, F) \subset Aut(L)$$

Usando la proposición 3.1.2.6. se tiene:

$$K_{G(K,F)} \text{ es subcuerpo de } K_H \qquad (3.18)$$

Por otro lado, K / F es una extensión normal, entonces:

$$K / F \text{ es una extensión finita y } F = K_{G(K,F)} \qquad (3.19)$$

Reemplazando (3.19) en (3.18) se tiene:

$$F \text{ es subcuerpo de } K_H \text{, es decir, } \exists \ K_H / F$$

Como K / F es una extensión finita y K / K_H, K_H / F son extensiones de cuerpos, por el corolario 1.2.5.7. se tiene:

$$K / K_H \text{ es una extensión finita}$$

Afirmación 3: $\circ(H) \leq [K : K_H]$

En efecto:

Como K / K_H es una extensión finita, por el teorema 3.1.1.7. se tiene

$$\circ(G(K, K_H)) \leq [K : K_H] \qquad (3.20)$$

Además, de la afirmación 1 se tiene:

$$H \subset G(K, K_H)$$

$$\circ(H) \leq \circ(G(K, K_H)) \qquad (3.21)$$

Por lo tanto, de (3.20) y (3.21) se tiene:

$$\circ(H) \leq [K : K_H]$$

Afirmación 4: $\circ(H) \geq [K : K_H]$

En efecto:

Tenemos que K / K_H es una extensión finita, por la proposición 1.2.5.42. se tiene:

K / K_H es finitamente generado

$$\exists \ a \in K \ / \ K = K_H(a)$$

Como K / K_H es finito, por el corolario 1.2.5.25. K / K_H es algebraico, entonces:

$a \in K$ es algebraico sobre K_H

Luego, por la proposición 1.2.5.21. se tiene:

$$\exists! \ m(x) = Irr(a, K_H, x) \in K_H[x] \ \text{ con } \ \deg m(x) = d$$

Por el teorema 1.2.5.15. se tiene:

$$[K : K_H] = d = \deg m(x) \qquad (3.22)$$

Por otro lado, sean $\sigma_1, \sigma_2, \ldots, \sigma_h \in H$ donde: σ_1 es la identidad de $G(K, F)$ y $\circ(H) = h$.

Consideremos las funciones simétricas elementales de $a = \sigma_1(a), \sigma_2(a), \ldots, \sigma_h(a)$, definidas así:

$$\alpha_1 = \sum_{i=1}^{h} \sigma_i(a)$$

$$\alpha_2 = \sum_{i<j} \sigma_i(a).\sigma_j(a)$$

$$\alpha_3 = \sum_{i<j<k} \sigma_i(a).\sigma_j(a).\sigma_k(a)$$

$$\alpha_h = \sigma_1(a).\sigma_2(a).\sigma_h(a)$$

Afirmación 5: Cada α_i es invariante bajo cualquier $\tau \in H$

En efecto:

Sea $\tau \in H \subset G(K,F) \Rightarrow \tau \in \{\sigma_1 = id, \sigma_2, \ldots, \sigma_h\}$

Si se tiene:

$$\tau \circ \sigma_1, \tau \circ \sigma_2, \tau \circ \sigma_3, \ldots, \tau \circ \sigma_h$$

Se tendrá de nuevo la sucesión $\sigma_1, \sigma_2, \ldots, \sigma_h$ excepto por el orden debido a que H es un grupo.

Veamos que pasa con los α_i

$$\tau(\alpha_1) = \tau(\sum_{i=1}^{h} \sigma_i(a)) = \tau(\sigma_1(a)) + \tau(\sigma_2(a)) + \ldots + \tau(\sigma_h(a))$$

$$\tau(\alpha_1) = (\tau \circ \sigma_1)(a) + (\tau \circ \sigma_2)(a) + \ldots + (\tau \circ \sigma_h)(a)$$

Por lo mencionado anteriormente, se puede suponer que:

$$\tau(\alpha_1) = \sigma_2(a) + \sigma_1(a) + \ldots + \sigma_h(a) = \sigma_1(a) + \sigma_2(a) + \ldots + \sigma_h(a) = \alpha_1$$

De forma análoga, cumplirá con cada α_i , por lo tanto:

Cada α_i es invariante bajo cualquier $\tau \in H$

Continuando con la demostración, usando la afirmación 5, podemos ver:

$$\alpha_i \in K_H,\ \forall i = 1,2,\ldots,h$$

Por otro lado, de la observación 3.1.2.5. se tiene:

$$\sigma_1(a), \sigma_2(a), \ldots, \sigma_h(a) \text{ son raíces de } p(x) \in K_H[x]$$

Donde:

$$p(x) = (x-\sigma_1(a))\cdot(x-\sigma_2(a))\ldots(x-\sigma_h(a)) = x^h - \alpha_1 x^{h-1} + \ldots + (-1)^h \alpha_h$$

Con: $\alpha_i \in K_H \ \wedge\ \forall i = 1,2,\ldots,h$

Por la naturaleza de a esto obliga a que:

$$d \leq h$$

Usando (3.22), se tiene:

$$[K : K_H] \leq \circ(H)$$

Por lo tanto, de las afirmaciones 3 y 4, se obtiene:

$$[K : K_H] = \circ(H)$$

Afirmación 6: $H = G(K, K_H)$

En efecto:

De (3.20) y (3.21), se tiene:

$$\circ(H) \leq \circ(G(K, K_H)) \leq [K : K_H]$$

Usando la parte 1, tenemos:

$$\circ(H) \leq \circ(G(K, K_H)) \leq \circ(H)$$

$$\circ(H) = \circ(G(K, K_H))$$

Como $H \subset G(K, K_H)$ con $\circ(H) = \circ(G(K, K_H))$, por lo tanto:

$$H = G(K, K_H) \qquad \square$$

3.1.4. Extensión de Galois y Grupo de Galois

Definición 3.1.4.1.

Lang (1971) mencionó: "Una extensión algebraica K de un cuerpo k se llama de Galois si es normal y separable" (p. 229).

Definición 3.1.4.2.

Lang (1971) mencionó: "El grupo de automorfismos de K sobre k recibe el nombre de grupo de Galois de K sobre k, y se representa por $G(K/k)$, o simplemente por G " (p. 229).

Según la demostración del teorema principal en el paper de López (2011), se usará la siguiente definición:

Si L/K es una extensión de Galois y $\circ(G(L, K)) = [L : K]$ entonces el grupo de automorfismos $G(L, K)$ será llamado el grupo de Galois de L/K .

Ejemplo 3.1.4.3. Veamos que $\mathbb{C}/\mathbb{R}$ es una extensión de Galois y $G(\mathbb{C}, \mathbb{R})$ es un grupo de Galois.

Demostración. Veamos que $\mathbb{C}/\mathbb{R}$ es una extensión de Galois:

Sabemos que $\mathbb{C}/\mathbb{R}$ es una extensión finita con $[\mathbb{C} : \mathbb{R}] = 2$, por el corolario 1.2.5.25. se tiene:

$\mathbb{C}/\mathbb{R}$ es una extensión algebraica

Además, usando el corolario 1.2.5.62. se tiene que $\mathbb{C}/\mathbb{R}$ es una extensión separable y de la observación 3.1.1.5. se obtiene que:

$$\mathbb{C}/\mathbb{R} \text{ es una extensión normal}$$

Por lo tanto:

$$\mathbb{C}/\mathbb{R} \text{ es una extensión de Galois}$$

De la observación 3.1.1.5. se obtiene que:

$$G(\mathbb{C},\mathbb{R}) = \{\sigma_1, \sigma_2\}$$

Donde $\sigma_1 = id \wedge \sigma_2$: conjugada en $\mathbb{C}$

Y se puede ver que:

$$\circ(G(\mathbb{C},\mathbb{R})) = [\mathbb{C}:\mathbb{R}] = 2$$

Se concluye:

$$G(\mathbb{C},\mathbb{R}) = \{\sigma_1, \sigma_2\} \text{ es un grupo de Galois}$$ □

Definición 3.1.4.4.

Herstein (1970) mencionó: "Sea $f(x)$ un polinomio en $F[x]$ y sea K su campo de descomposición sobre F. El grupo de Galois de $f(x)$ es el grupo $G(K,F)$ de todos los automorfismos de K que dejan fijos todos los elementos de F " (p. 239).

Observación 3.1.4.5.

Herstein (1970) mencionó: "Nótese que el grupo de Galois de $f(x)$ puede considerarse como un grupo de permutaciones de sus raíces, pues si α es una raíz de $f(x)$ y si $\sigma \in G(K,F)$ entonces $\sigma(\alpha)$ es también una raíz de $f(x)$ " (p. 239).

Demostración. Sea $f(x) \in F[x]$, $\sigma \in G(K,F)$ y α es una raíz de $f(x)$, entonces:

$$f(\sigma(\alpha)) = a_0 + a_1\sigma(\alpha) + a_2\sigma^2(\alpha) + \ldots + a_n\sigma^n(\alpha)\,;\; a_i \in F,\; i = 1,\ldots,n$$

Como σ deja fijo los elementos de F, entonces:

$$f(\sigma(\alpha)) = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \sigma(a_2)\sigma^2(\alpha) + \ldots + \sigma(a_n)\sigma^n(\alpha)$$

Por ser σ automorfismo en K, entonces:

$$f(\sigma(\alpha)) = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \sigma(a_2)\sigma(\alpha^2) + \ldots + \sigma(a_n)\sigma(\alpha^n)$$

$$f(\sigma(\alpha)) = \sigma(a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n)$$

Como α es una raíz de $f(x)$, entonces:

$$f(\sigma(\alpha)) = \sigma(0)$$

Como σ es un automorfismo, entonces:

$$f(\sigma(\alpha)) = 0$$

Por lo tanto:

$\sigma(\alpha)$ es también una raíz de $f(x)$ □

3.1.5. El Teorema Fundamental de Galois

En esta parte, presentaremos la demostración del Teorema Fundamental de Galois que es una pieza importante para el teorema principal pero antes veamos una observación.

Observación 3.1.5.1. El "Teorema Fundamental de Galois" es también llamado el "Teorema de Correspondencia". Es un teorema fuerte en la Teoría de Galois que establece una correspondencia biyectiva entre los subcuerpos del cuerpo de descomposición de $f(x)$ y

los subgrupos de su grupo de Galois. Vamos a extraer una de las condiciones del Teorema Fundamental de Galois que nos será de utilidad.

Teorema 3.1.5.2. (Teorema Fundamental de Galois)

Herstein (1970) mencionó:

> Sea $f(x)$ un polinomio en $F[x]$, K su campo de descomposición sobre F y $G(K,F)$ su grupo de Galois. Para cualquier subcampo T de K que contiene a F sea $G(K,T)=\{\sigma \in G(K,F) / \sigma(t)=t$ para todo $t \in T\}$ y para cualquier subgrupo H de $G(K,F)$ sea $K_H=\{x \in K / \sigma(x)=x$ para todo $\sigma \in H\}$. Entonces la asociación de T con $G(K,T)$ establece una correspondencia biyectiva del conjunto de subcampos de K que contienen a F sobre el conjunto de subgrupos de $G(K,F)$ tal que:
>
> 1. $T=K_{G(K,T)}$.
> 2. $H=G(K,K_H)$.
> 3. $[K:T]=\circ(G(K,T))$. (pp. 239-240)

Demostración. Definamos:

$$\psi: A=\{T / F \subset T \subset K\} \to B=\{H / H \text{ es subgrupo de } G(K,F)\}$$

Tal que $\psi(T)=G(K,T)$

$$\phi: \{H / H \text{ es subgrupo de } G(K,F)\} \to \{T / F \subset T \subset K\}$$

Tal que $\phi(H)=K_H$

Afirmación 1: ψ y ϕ están bien definidas.

En efecto:

a. Sea $T \in A$, entonces $\psi(T) = G(K,T)$.

Veamos que $G(K,T)$ es subgrupo de $G(K,F)$.

Tenemos $F \subset T \subset K$ son dos subcuerpo de K , por la proposición 3.1.2.6. se obtiene:

$$G(K,T) \text{ es subgrupo de } G(K,F)$$

Esto quiere decir:

$$\psi(T) = G(K,T) \in B \text{ (} \quad \psi \text{ está bien definido)}$$

b. Sea $H \in B$, entonces $\phi(H) = K_H$.

Veamos que $F \subset K_H \subset K$.

Sea $z \in F \ \wedge \ \sigma \in H \subset G(K,F)$, entonces:

$$\sigma : K \to K \text{ (automorfismo) / } \sigma(z) = z \ ; \quad \forall z \in F$$

Luego:

$$z \in K \ / \ \sigma(z) = z \ ; \ \forall \sigma \in H$$

Así obtenemos:

$$z \in K_H$$

Por lo tanto:

$$F \subset K_H$$

Además, por el lema 3.1.1.4. se tiene:

$$K_H \text{ es subcuerpo de } K \text{ , es decir: } K_H \subset K$$

Así concluimos:

$$F \subset K_H \subset K$$

Esto quiere decir:

$\phi(H) = K_H \in A$ (ϕ está bien definido)

Para demostrar la biyeccion, necesitaremos demostrar la siguiente afirmación:

Afirmación 2: $\psi \circ \phi = id_B \wedge \phi \circ \psi = id_A$

En efecto:

a. Sea $H \in B \Rightarrow H$ es subgrupo de $G(K,F)$

Por el teorema 3.1.3.2. se tiene:

$$H = G(K, K_H) = G(K, \phi(H)) = \psi(\phi(H)) = (\psi \circ \phi)(H)$$

Por lo tanto:

$$\psi \circ \phi = id_B$$

b. Sea $T \in A \Rightarrow F \subset T \subset K$

Aplicando $\psi(T) = G(K,T) \Rightarrow G(K,T)$ es subgrupo de $G(K,F)$

Por el teorema 3.1.3.2. se tiene:

$$G(K,T) = G(K, K_{G(K,T)})$$

Entonces:

$$T = K_{G(K,T)}$$

$$T = K_{\psi(T)}$$

$$T = \phi(\psi(T)) = (\phi \circ \psi)(T)$$

Por lo tanto:

$$\phi \circ \psi = id_A$$

Finalmente, se concluye:

ψ es biyectiva

Demostración parte 1:

De lo anterior, hemos probado que:

$$T = K_{G(K,T)}$$

Demostración parte 2:

De lo anterior, hemos probado que:

$$H = G(K, K_H)$$

Demostración parte 3:

Sea $F \subset T \subset K$ una torre de cuerpos, como K / F es finito por el corolario 1.2.5.7. K / T es finito. Además, de la parte 1 se tiene: $T = K_{G(K,T)}$, por lo tanto:

K / T es una extensión normal

Por el teorema 3.1.3.2. se obtiene:

$$[K : T] = [K : K_{G(K,T)}] = \circ(G(K,T))$$

Por lo tanto:

$$[K : T] = \circ(G(K,T))$$ □

3.2. El Teorema de Artin y su consecuencia en la Teoría de Galois

3.2.1. El Teorema de Artin

López (2011) mencionó:

> Como es usual en teoría de Galois, a cada extensión de Galois $K \supset k$ asociamos un grupo finito: el grupo de Galois de la extensión. Nos hacemos ahora la pregunta inversa: es todo grupo finito el grupo de Galois de alguna extensión de campos? Como lo dice el siguiente teorema, la respuesta es positiva. (p. 1)

Teorema 3.2.1.1. (Artin)

López (2011) mencionó: "Sea G un grupo finito. Entonces existe una extensión de Galois $L \supset K$ tal que G es el grupo de Galois de dicha extensión" (p. 1).

Demostración. Sea F un cuerpo cualquiera, sean $x_1, x_2, \ldots, x_n$ variables distintas y consideremos las funciones simétricas elementales $a_1, a_2, \ldots, a_n$ de los $x_1, x_2, \ldots, x_n$.

Sea k el cuerpo de las funciones racionales simétricas, por el teorema 3.1.2.7. (parte 3) se tiene:

$$k = F(a_1, a_2, \ldots, a_n)$$

Sea ahora $L = F(x_1, x_2, \ldots, x_n)$ el cuerpo de las funciones racionales de $x_1, x_2, \ldots, x_n$, demostremos:

Afirmación 1: k es subcuerpo de L

En efecto: Veamos:

a. Sabemos que $k = F(a_1, a_2, \ldots, a_n)$ y $L = F(x_1, x_2, \ldots, x_n)$ son cuerpos.

b. Por definición del cuerpo de las funciones racionales simétricas, se tiene:

$$k = F(a_1, a_2, \ldots, a_n) \subset F(x_1, x_2, \ldots, x_n) = L$$

$$k \subset L$$

Por lo tanto, juntando los resultados se obtiene:

k es subcuerpo de L

Es decir:

$\exists\ L/k$ (extensión de cuerpo)

Afirmación 2: $G(L,k)$ es un grupo de Galois

En efecto:

Del teorema 3.1.2.7. (parte 1) se tiene $[L:k] = n!$, entonces:

L/k es finito (3.23)

Por el corolario 1.2.5.25. se tiene:

L/k es algebraico

Del teorema 3.1.2.7. (parte 4) tenemos que $L = F(x_1, x_2, \ldots, x_n)$ es el cuerpo de descomposición sobre $k = F(a_1, a_2, \ldots, a_n)$ del polinomio irreducible

$p(t) = t^n - a_1 t^{n-1} + \ldots + (-1)^n a_n \in k[t]$.

Como $p(t) \in k[t]$ es general y de la observación 3.1.2.5. los $x_1, x_2, \ldots, x_n$ son raíces diferentes de $p(t)$, entonces:

L/k es separable

Por otro lado, del teorema 3.1.2.7. (parte 2) tenemos:

$$G(F(x_1, x_2, \ldots, x_n), k) = S_n$$

$$G(L, k) = S_n \tag{3.24}$$

Además, de la observación 3.1.2.3. se tiene:

$$k = F(x_1, x_2, \ldots, x_n)_{S_n}$$

De (3.24) se tiene:

$$k = L_{G(L,k)} \tag{3.25}$$

Por lo tanto, de (3.23) y (3.25) se obtiene:

L / k es normal

Luego, ordenando los resultados, tenemos que L / k es algebraico, normal y separable.

Por lo tanto:

L / k es una extensión de Galois

Además:

$$\circ(G(L, k)) = [L : k] = n!$$

Finalmente:

$G(L, k)$ es un grupo de Galois

Afirmación 3: $\exists$ L / K (Galois) $\wedge$ $G(L, K)$ es un grupo de Galois.

En efecto:

Sea G un grupo finito con $\circ(G) = n$, por el teorema 1.2.1.15. (Cayley), se tiene:

G es isomorfo a un subgrupo de $S_n = G(L,k)$

G es subgrupo de $G(L,k)$ $\wedge$ $G(L,k)$ es subgrupo de $Aut(L)$

Entonces:

G es subgrupo de $Aut(L)$

Podemos definir el cuerpo fijo de G de esta forma: $K = L_G$, así se obtiene:

L/K (extensión de cuerpo)

Además:

$$G \subset G(L,k) \subset Aut(L)$$

Por la proposición 3.1.2.6. se obtiene:

$$L_{G(L,k)} \subset L_G \subset L$$

Es decir:

$$k \subset K \subset L$$

Como L/k es una extensión finita, por el corolario 1.2.5.7. se tiene:

L/K es una extensión finita

Por el corolario 1.2.5.25. se tiene:

L/K es una extensión algebraica

Además, como L/k es separable, por la proposición 1.2.5.59. se tiene:

L/K es separable

Por otro lado, por el teorema 3.1.5.2. (Teorema Fundamental de Galois) se tiene:

$$K = L_{G(L,K)} \ \wedge \ [L:K] = \circ(G(L,K))$$

Juntando los resultados obtenidos, se tiene:

L/K es algebraico, normal y separable con $[L:K] = \circ(G(L,K))$

Por lo tanto:

L/K es una extensión de Galois y $G(L,K)$ es un grupo de Galois

Afirmación 4: $G = G(L,K)$

En efecto:

Tenemos que $p(t) \in k[t]$, L es su cuerpo de descomposición sobre k y $G(L,k)$ su grupo de Galois. Además, $K = L_G$ el cuerpo fijo de G es el cuerpo intermedio de L/k con $G(L,K)$ su grupo de automorfismo y G es un subgrupo de $G(L,k)$, por el teorema 3.1.5.2. (Teorema Fundamental de Galois), se concluye:

$$G = G(L,K) \qquad \square$$

3.2.2. Consecuencia

Observación 3.2.2.1.

López (2011) mencionó:

> Por el teorema anterior, sabemos encontrar una extensión $L \supset K$ con grupo de Galois un grupo dado: basta tomar L y k los campos de funciones racionales como en la demostración del teorema y después aplicar el teorema de correspondencia. Pero dado un campo prefijado, por ejemplo $k = \mathbb{Q}$, existe una extensión de Galois $L \supset \mathbb{Q}$ con grupo de

Galois un grupo dado?. Este es un problema que aún está abierto, aunque mucho se ha hecho al respecto. (p. 2)

DISCUSIÓN

A continuación se presenta la discusión de los resultados obtenidos. Se pudo ver en el teorema principal que era necesario usar el “Teorema Fundamental de las Funciones Racionales Simétricas”, el “Teorema de Cayley” y finalizarlo con el “Teorema Fundamental de Galois”, entonces eso nos permite afirmar que la hipótesis mencionada es verdadera.

Pero para poder llegar a esa verdad, se han consultado varios autores que se mencionan en las referencias de este trabajo de tesis, en las cuales todos los autores coinciden en las definiciones a excepción de la extensión normal, extensión de Galois y grupo de Galois, además las proposiciones y teoremas son demostrados de forma diferente y unos más complicados que otros, a pesar de eso sus aportes fueron valiosos para la demostración del teorema principal.

En base a toda esta investigación se pudo entender la teoría de cuerpos, la teoría de Galois y su relación estrecha con las raíces del polinomio dado.

Este teorema principal se encuentra demostrado en el paper de: López Daniel, El Problema Inverso de Galois, con lo cual fue nuestra guía y camino en este trabajo de tesis.

Los resultados de los tesistas mencionados en los antecedentes se relacionan con el estudio de este trabajo de investigación y nos da veracidad en el contenido de este trabajo de tesis.

Como se puede ver, la teoría de Galois es una matemática rica por su contenido con lo cual este trabajo de tesis tuvo como justificación de estudio en aportar conocimientos matemáticos para así poder entender la conjetura llamado “El Problema Inverso de Galois” ya que sigue siendo un problema abierto propuesta por Hilbert en el siglo XIX.

CONCLUSIONES

1. Sí es posible probar la existencia de la extensión del cuerpo L/K tal que G es el grupo de Galois de L/K con G finito, por medio de un cuerpo cualquiera F se tomó $L = F(x_1, x_2, \ldots, x_n)$ el cuerpo de las funciones racionales de $x_1, x_2, \ldots, x_n$ y $K = L_G$ el cuerpo fijo de G.

2. Sí es necesario desarrollar la teoría de Galois, ya que nos llena de conocimientos previos como son el grupo de automorfismos, el cuerpo fijo, las funciones racionales simétricas, las funciones simétricas elementales, la extensión normal, la extensión de Galois y los grupos de Galois.

3. Sí son importantes los polinomios y sus raíces en los grupos de Galois ya que son los requisitos para formar el grupo de Galois, pues como hemos visto, los grupos de Galois son un cierto grupo de permutaciones de las raíces del polinomio.

4. Sí es importante el grupo S_n en la teoría de Galois ya que nos ayuda a construir: una aplicación que hace actuar a S_n sobre $Aut(F(x_1, \ldots, x_n))$, el cuerpo de las funciones racionales simétricas y las funciones simétricas elementales. Por lo tanto, estas construcciones son utilizadas para demostrar el Teorema Fundamental de las Funciones Racionales Simétricas.

5. Sí es posible probar que dado una extensión de Galois, se le puede asociar un grupo finito: grupo de Galois de dicha extensión, esto se debe al Teorema 3.1.5.2. (Teorema Fundamental de Galois).

RECOMENDACIONES

1. Para entender este trabajo de tesis es necesario tener conocimientos previos sobre la teoría de grupos, la teoría de anillos, la teoría de espacio vectorial y la teoría de cuerpos.
2. El estudio de los grupos de Galois no solo se puede estudiar con grupos finitos, sino que se puede enfocar también para grupos infinitos pero con otro enfoque estructural.
3. Los grupos de Galois es muy importante en el estudio del GPS y en las demostraciones matemáticas como se puede ver en los anexos de este trabajo de tesis.
4. Para las definiciones de extensión normal, extensión de Galois y grupo de Galois se puede encontrar de diferentes maneras pero es recomendable manejar de un libro para después usar en las demostraciones matemáticas.
5. Este trabajo de tesis fue una excusa para entender el problema abierto llamado "El problema inverso de Galois".

REFERENCIAS

[1] Artin M. (1991). *Álgebra*. USA: Edit. Prentice-Hall.

[2] Baldo H. (2013). *Problema Inverso de Galois*. Universidad Estatal de Campinas, Brasil.

[3] Castellanos J. (2013). *Estructuras Algebraicas*. Universidad Complutense de Madrid, España.

[4] Chamizo F. (2004). *¡Qué bonita es la teoría de Galois!* Universidad Autónoma de Madrid, España.

[5] Dummit D. y Foote R. (2004). *Abstract Algebra*. USA: Edit. John Wiley y Sons.

[6] Ferrando J. y Gregori V. (1995). *Matemática Discreta*. España: Edit. Reverté, S. A.

[7] Fraleigh J. (1987). *Álgebra Abstracta*. USA: Edit. Addison-Wesley Iberoamericana.

[8] Hernández J. (2010). *Extensiones de Galois*. (Tesis de licenciatura). México: Universidad Nacional Autónoma de México.

[9] Herstein I. (1970). *Álgebra Moderna*. México: Edit. Trillas.

[10] Hoffman K. y Kunze R. (1973). *Álgebra Lineal*. México: Edit. Prentice-Hall Hispanoamericana.

[11] Lang S. (1971). *Álgebra*. España: Edit. Aguilar.

[12] Lázaro M. (2005). *Álgebra Lineal*. Perú: Edit. Moshera.

[13] López D. (2011). *El Problema Inverso de Galois*, pp. 1-2.

[14] Machiavelo A. (1997). *Notas de Álgebra II*. Universidad de Oporto, Portugal.

[15] Nachbin L. (1980). *Introducción al Álgebra*. España: Edit. Reverté.

[16] Revilla F. (15 de abril de 2014). *Homomorfismos entre cuerpos*. Recuperado de http://fernandorevilla.es/blog/2014/04/15/homomorfismos-entre-cuerpos/

[17] Riquelme E. (2007). *Teoría de Galois y ecuaciones algebraicas*. (Tesis de Licenciatura). Chillán, Chile: Universidad del Bío-Bío.

[18] Rodríguez N., López P. y Villanueva E. (2013). *Curso de Teoría de Galois*. Santiago de Compostela, España.

[19] Stewart I. (2004). *Galois Theory*. EE.UU.: Edit. Chapman y Hall.

[20] Zaldívar F. (1996). *Teoría de Galois*. Universidad Autónoma Metropolitana, México: Edit. Anthropos.

ANEXOS

En esta parte presentaremos dos aplicaciones matemáticas de este trabajo de tesis, estos son las demostraciones de un corolario y de un teorema usando el Teorema de Artin.

Corolario:

Lang (1971) mencionó: "Sea K una extensión finita de Galois de k, y sea G su grupo de Galois. Todo subgrupo de G corresponde a cierto subcuerpo F tal que $k \subset F \subset K$" (p. 232).

Demostración. Tenemos que $G(K,k)$ es un grupo de Galois, entonces:

$$\circ(G) = \circ(G(K,k)) = [K:k] < \infty$$

Luego:

$$G \text{ es finito} \tag{5.1}$$

Sea H un subgrupo de $G \subset Aut(L) \Rightarrow \exists\ K_H \,/\, k \subset F = K_H \subset K$

Usando (5.1) se tiene:

$$H \text{ es finito}$$

Usando el Teorema de Artin se tiene:

$$K/F \text{ (Galois) } / \ H = G(K,F) \qquad \square$$

Teorema:

Machiavelo (1997) mencionó: "Sejam $K \subseteq E \subseteq \mathbb{C}$. Então: E/K é Galoisiana se e só se $\#Gal(E/K) = [E:K]$" (p.59).

Demostración. Veamos:

$(\Rightarrow)$ Tenemos de hipótesis que E/K es una extensión finita, por el teorema 3.1.1.7. se tiene:

$$\exists\ Gal(E/K) \text{ un grupo finito}$$

Además, tenemos que E/K es de Galois entonces:

$$E/K \text{ es normal } \Rightarrow K = E_{Gal(E/K)}$$

Ordenando, tenemos:

E/K es normal, $Gal(E/K)$ es subgrupo de $Gal(E/K)$ y $K = E_{Gal(E/K)}$ es el cuerpo fijo de $Gal(E/K)$

Por el teorema 3.1.3.2 se tiene:

$$[E: E_{Gal(E/K)}] = \#Gal(E/K)$$

Por lo tanto:

$$[E:K] = \#Gal(E/K)$$

($\Leftarrow$) Tenemos de hipótesis:

$$\#Gal(E/K) = [E:K] < \infty \Rightarrow Gal(E/K) \text{ es un grupo finito}$$

Por otro lado, $Gal(E/K) \subset Aut(E) \Rightarrow \exists\ E_{Gal(E/K)} \subset E$

Sea $K_0 = E_{Gal(E/K)}$, por el Teorema de Artin se tiene:

$$E/K_0 \text{ (Galois) } / \ Gal(E/K) = Gal(E/K_0) \qquad (5.2)$$

Entonces, de (5.2) se tiene:

$$Gal(E/K) \text{ es un grupo de Galois}$$

Por lo tanto:

$$E/K \text{ es una extensión de Galois}$$ □