Universidad Nacional Autónoma de México

Facultad de Ciencias

Algunos aspectos sobre Teoría de Galois y Álgebra lineal

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
JOSÉ MARTÍN CASTREZANA LÓPEZ

DIRECTORA DE TESIS:
MAT.DANIELA MARIYET TERÁN GUERRERO

2012

1.Datos del alumno	
Apellido paterno	Castrezana
Apellido materno	López
Nombre(s)	José Martín
Teléfono	55249040
Universidad	Universidad Nacional - Autónoma de México
Facultad o escuela	Facultad de Ciencias
Carrera	Matemáticas
Número de cuenta	406099402
2. Datos del tutor	
Grado	Mat.
Nombre(s)	Daniela Mariyet
Apellido paterno	Terán
Apellido materno	Guerrero
3. Datos del sinodal 1	
Grado	Dr.
Nombre(s)	Hugo
Apellido paterno	Rincón
Apellido materno	Mejía
4. Datos del sinodal 2	
Grado	Dr.
Nombre(s)	José
Apellido paterno	Ríos
Apellido materno	Montes
5. Datos del sinodal 3	
Grado	Mat.
Nombre(s)	Juan
Apellido paterno	Orendain
Apellido materno	Almada
6. Datos del sinodal 4	
Grado	Dr.
Nombre(s)	César
Apellido paterno	Hernández
Apellido materno	Cruz
7.Datos del trabajo escrito.	
Algunos aspectos sobre Teoría de Galois y Álgebra lineal	
N˙mero de paginas	63p.
Año	2012

A todas las personas que amo,
por hacer de mi quien soy.

Índice general

Capítulo 1

Introducción

El siguiente trabajo consiste de una argumentada explicacion, detallada y ejemplificada, de las primeras tres secciones del articulo *Galois theory and linear algebra* (Teoria de Galois y Algebra lineal) publicado por Rod Gow y Rachel Quinlan en la revista Linear Algebra and its applications numero 430. Dicha explicación fue hecha con el fin de hacer los resultados mas accesibles al publico medianamente estudiado en matemáticas.

En esta primera sección, se enuncian conceptos y resultados preliminares, necesarios y suficientes para esclarecer este trabajo. Si el lector lo considera pertinente, puede ahondar en resultados o ejemplos en la Bibliografía, principalmente [7], [5], o [3].

1.1. Teoría de Grupos

El concepto de grupo como es conocido actualmente, responde a la descripción de estructuras que subyacen en varios problemas matemáticos, desde el estudio de los números enteros iniciado hace cientos de años, o el estudio de las posibles transformaciones geométricas de un objeto, hasta la búsqueda de soluciones para ecuaciones polinomiales.

Definición 1.1.1. Un par $(G, \cdot)$, donde G es un conjunto no vacío provisto de una operación $\cdot : G \times G \longrightarrow G$, es un *monoide* bajo $\cdot$ si:

- Para toda $a, b \in G$, $a \cdot b \in G$.
- Para toda $a, b, c \in G$, $a(bc) = (ab)c$

- Existe un único elemento e tal que $a \cdot e = e \cdot a = a$ para toda $a \in G$

Si además

- Para cada $a \in G$, existe un elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$ (llamado el inverso de a en G), G es un *grupo*.
- Si para toda $a, b \in G$ se cumple que $ab = ba$ entonces el grupo es *abeliano*.

En el futuro, y cuando no genere confusión, se escribirá ab en lugar de $a \cdot b$.

Ejemplo.

- $(\mathbb{Z}, +)$, el conjunto de los números enteros con la suma usual, forman un grupo abeliano. Así también $(\mathbb{Z}_n, +)$ con $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ y $+$ la suma módulo n, donde para cada $a \in \mathbb{Z}_n$ su inverso es $n - a$.
- $(\mathbb{Q}, +)$ como en el ejemplo anterior, es un grupo abeliano, pero $(\mathbb{Q}, \cdot)$ los racionales con el productor usual, no es grupo ya que el cero no tiene inverso multiplicativo, sin embargo $(\mathbb{Q} \setminus \{0\}, \cdot)$ es un también un grupo abeliano.
- Consideremos ahora un triángulo equilátero, y todas sus simetrías, es decir, los movimientos que lo dejan ocupando el mismo espacio. De estos, llamemos ρ_0 al que lo deja fijo, ρ_1 al que lo rota 120º en dirección contraria a las manecillas de reloj, ρ_2 al que lo rota 240º en la misma dirección, y por ultimo, μ_1, μ_2, μ_3 a las reflexiones respecto a las lineas que bisecan el triángulo.

  Viendo a cada uno de estos movimientos como funciones que van del conjunto $\{1, 2, 3\}$ en si mismo, aplicar dos movimientos seguidos puede traducirse en componer las funciones antes descritas. Así $\rho_2\mu_3 = \rho_2(\mu_3) = \mu_1$. De lo anterior, podemos afirmar intuitivamente que dichas funciones, bajo composición, forman un grupo, sin embargo, en este caso en particular, dicho grupo puede ser nombrado de dos formas distintas: por un lado puede verse como el grupo de simetrías del polígono de 3 lados (triángulo), denotado D_3, y por el otro puede considerarse como el grupo de permutaciones de un conjunto de 3 elementos denotado por S_3 . Claramente, puede obtenerse con un procedimiento análogo el grupo pertinente para cada $n \in \mathbb{N}$. Sin embargo, es fácil ver que estos grupos no siempre son iguales; comparando las simetrías del cuadrado, con las permutaciones de un conjunto con 4

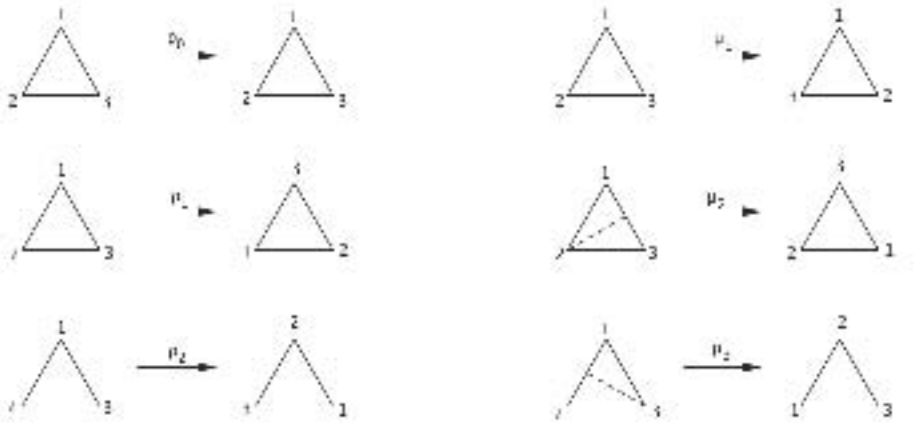


Figura 1.1: Simetrías del triángulo

elementos, se puede ver que en el caso de las simetrías, los numeros asignados a esquinas opuestas jamás podrán tener una arista en común (dado que lo único permitido en este caso es rotar el cuadrado respecto al centro, o a un eje de simetría, dejándolo en su posición original), sin embargo, en las permutaciones, esto si está permitido. Una forma clara de ver como se comporta nuestro ejemplo concreto, es construir una tabla, en donde la entrada localizada en el i-ésimo renglon, j-ésima columna, represente el resultado de la composición $ij = i(j)$.

$\cdot$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_3	μ_2	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

Además S_3 no es abeliano, ya que $\mu_3\mu_2 = \rho_1 \neq \rho_2 = \mu_2\mu_3$.

En general, las funciones biyectivas de un conjunto en sí mismo forman un grupo bajo composición.

S_n es conocido como el *grupo simétrico*, y D_n como el *grupo diédrico*. Definimos el *orden* de un grupo como el número de elementos del conjunto G, denotado $|G|$. G es *finito* si $|G|$ es finito, en caso contrario G es *infinito*.

Ejemplo.
- $(\mathbb{Z}, +)$ es infinito, y $(\mathbb{Z}_n, +)$ finito.
- Para calcular el orden de S_3, usando conocimientos básicos de combinatoria (véase [7]), es claro ver que $|S_3| = |\mathcal{B}\{1,2,3\}| = 3!$ donde $\mathcal{B}\{1,2,3\}$ es el cunjunto de funciones biyectivas de $\{1,2,3\}$ en $\{1,2,3\}$. En general $|S_n| = n!$.

Analizando su estructura interna, un grupo admite en su interior otros grupos que pueden tener propiedades que no se cumplen para el grupo que lo contiene, y bajo algunas condiciones se puede formar con ambos (el grupo, y algún grupo en su interior) un tercer grupo que resulta de gran importancia en la teoría de grupos.

Si $(G, \cdot)$ es un grupo, un subconjunto $H \subseteq G$ es un *subgrupo* de G, denotado $H \leq G$, si $(H, \cdot)$ es un grupo donde $\cdot$ es la restricción de la operación de G a H. De donde obtenemos que un subconjunto no vacío H de un G grupo, es un subgrupo si y sólo si para toda $a, b \in H$, $ab^{-1} \in H$.

Ejemplo.
- Si $\mathbb{R}^\times = \mathbb{R}\setminus\{0\}$, $\mathbb{C}^\times = \mathbb{Q}\setminus\{0\}$ verificar que $(\mathbb{R}^\times, \cdot) \leq (\mathbb{C}^\times, \cdot)$ se sigue de que $\forall r \in \mathbb{R}^\times, 1/r \in \mathbb{R}^\times$, y también, si $r, s \in \mathbb{R}^\times$, $r \cdot s \in \mathbb{R}^\times$.
- El conjunto $H \subset \mathbb{Z}$ de los números impares no es un subgrupo de los enteros ya que $1 - 3 = -2 \notin H$ sin embargo si se considera $K \subset \mathbb{Z}$ el conjunto de los números pares si es subgrupo de $\mathbb{Z}$

Para describir las funciones que existen entre grupos, dado que un grupo es un conjunto dotado de una operación, es necesario que dichas funciones preserven la estructura. Esto será muy útil en el caso de que dicha función sea biyectiva ya que entonces hablaremos de dos grupos que además de ser estructuralmente iguales, tendrán el mismo tamaño, lo cual les hará esencialmente el mismo.

Si G, G' son grupos, una función $\phi : G \longrightarrow G'$ es un *homomorfismo* si $\phi(a \cdot b) = \phi(a) * \phi(b)$ donde $\cdot$ es la operación de G y $*$ la de G'; si ϕ es inyectiva es un *monomorfismo*, si es suprayectiva es un *epimorfismo* y si ϕ es biyectiva entonces es un *isomorfismo* denotado como $G \cong G'$. Si $G = G'$, ϕ es un *endomorfismo* que si además resulta biyectivo, sera llamado *automorfismo*, obsérvese que un automorfismo es también una permutación en el conjunto G. En todos los casos la *imágen* de un homomorfismo ϕ es $\text{Im}\phi = \{y \in G' | y = \phi(x) \text{ para alguna } x \in G\}$. Se define también el *núcleo* de ϕ como $Nuc(\phi) = \{x \in G | \phi(x) = e'\}$.

Sea G un grupo y H un subgrupo, si para toda $g \in G$ se tiene que $gH = Hg$, entonces H es *normal* en G, denotado $H \lhd G$; de esto se deduce que $Nuc(\phi) \lhd G$. Si H es un subgrupo normal de G, el conjunto $\{gH | g \in G\}$ forma un grupo, llamado *grupo cociente*, con la operación definida por

$$gHg'H = gg'H.$$

Se puede deducir facilmente de las definiciones que un homomorfismo $\phi : G \longrightarrow G'$ es inyectivo si y sólo si $Nuc(f) = \{e\}$ donde e es el neutro de G

Ejemplo.

- Si $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^{\times}, \cdot)$ está dada por $f(x) = e^x$, es un isomorfismo.

- El conjunto de automorfismos de un grupo en sí mismo
  $\mathrm{Aut}(G) = \{\phi : G \longrightarrow G | \phi \text{ es isomorfismo}\}$, es subgrupo de un grupo de permutaciones dado que si consideramos ϕ, $\tau \in \mathrm{Aut}(G)$, se tiene que para toda
  $x, y \in G$
  $$\phi\tau(xy) = \phi(\tau(x)\tau(y)) = \phi(\tau(x))\phi(\tau(y))$$
  Entonces $\phi\tau \in \mathrm{Aut}(G)$.

  Por otro lado,

  $$\phi(\phi^{-1}(x)\phi^{-1}(y)) = \phi\phi^{-1}(x)\phi\phi^{-1}(y) = xy.$$

  Entonces $\phi^{-1}(x)\phi^{-1}(y) = \phi^{-1}(xy)$, y $\phi^{-1} \in \mathrm{Aut}(G)$. De donde se tiene que $\mathrm{Aut}(G) \leq S_n$ para alguna $n \in \mathbb{N}$.

De todos los homomorfismos de grupos, aquellos que proveen más información son los que son biyectivos (isomorfismos), ya que además de asegurar la preservación estructural de grupos y garantizar la completa similitud, forman éstos a su vez un grupo bajo composición que puede también proveer mucha información.

Existen tres teoremas muy importantes en la teoría de grupos que enunciaremos a continuación, las demostraciones pueden encontrarse en [8]

Teorema 1.1.2 (Primer Teorema de Isomorfismo)**.** *Si $\phi : G \longrightarrow G'$ es un homomorfismo de grupos con $nucf = K$, entonces*

$$G/K \cong \phi(G)$$

Teorema 1.1.3 (Segundo Teorema de Isomorfismo)**.** *Sea G un grupo con un subgrupo normal K, y un subgrupo arbitrario H, entonces*

$$HK/K \cong H/(H \cap K).$$

Teorema 1.1.4 (Tercer Teorema de Isomorfismo)**.** *Si G es un grupo con M, N subgrupos normales de G tales que $M \leq N$, entonces*

$$G/N \cong (G/M)/(N/M).$$

Teorema 1.1.5 (Teorema de la Correspondencia Biyectiva)**.** *Si $\phi : G \longrightarrow G'$ es un homomorfismo de grupos, $H \mapsto \phi(H)$ es una correspondencia biyectiva entre la familia de subgrupos de G que contienen $Nuc\phi$ y la familia de subgrupos de G'. Además, subgrupos normales de G se corresponden con subgrupos normales de G'.*

1.2. Álgebra Lineal

En esta sección se darán los conceptos y resultados básicos y que se usarán en el resto del trabajo sobre la estructura de espacio vectorial, estructuras con las que el lector seguramente está más relacionado debido al gran uso que tienen en distintas áreas; se definirán los conceptos básicos y enunciarán teoremas que describan relaciones entre dichos conceptos y las propiedades de un espacio.

Definición 1.2.1. $(F, +, \cdot, 0, 1)$ es un *campo* si $(F, +, 0)$ es un grupo abeliano, $(F \setminus \{0\}, \cdot, 1)$ es un grupo abeliano, $1 \neq 0$, y además la multiplicación se distribuye sobre la suma, es decir para toda $a, b, c \in F$:

$$(a + b)c = ac + bc.$$

Un subconjunto K de un campo F es un *subcampo*, si K es un campo con la operación de F restringida a K, denotado $K \leq F$.

Ejemplo.

- $\mathbb{Z}_2$ es un campo con el producto usual y la $+_{mod2}$
- $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, los números racionales, reales y complejos, respectivamente, son campos con la suma y el producto usuales.

Definición 1.2.2. Un *espacio vectorial* V sobre un campo F, denotado V_F (F- espacio vectorial) es un conjunto dotado de una *suma* $+ : V \times V \longrightarrow V$ y una *multiplicación escalar* $\cdot : F \times V \longrightarrow V$ tales que para cada par de elementos x, $y \in V$ y $a \in V$, existen únicos elementos $x + y$, $ax \in V$ tales que:

- Para toda $x, y \in V$, $x + y = y + x$.
- Para toda $x, y, z \in V$, $(x + y) + z = x + (y + z)$.
- Existe $0_V \in V$ tal que $x + 0_V = x$ para toda $x \in V$.
- Para toda $x \in V$ existe un elemento $y \in V$ tal que $x + y = 0_V$.
- Para toda $x \in V$ $1x = x$.
- Para toda $a, b \in F$, $x \in V$, $(ab)x = a(bx)$
- Para toda $a \in F$, $x, y \in V$ se tiene que $a(x + y) = ax + ay$.
- Para toda $a, b \in F$, $x \in V$ se tiene que $(a + b)x = ax + by$.

A los elementos de V se les llama *vectores*, mientras que a los de F *escalares*. Nótese que $0_V \in V$ no necesariamente es igual que $0 \in F$.

Ejemplo.

- Todo campo F es un F-espacio vectorial sobre sí mismo, y $F^n = \{(a_1, a_2, ..., a_n) | a_i \in F 1 \leq i \leq n\}$ es también un espacio vectorial sobre el campo F con la suma definida entrada a entrada, es decir $(x_1, x_2, ..., a_n)+(b_1, b_2, ..., b_2) = (a_1+b_1, a_2+b_2, ..., a_n+b_n)$ y el producto escalar como $a(a_1, a_2, ..., a_n) = (aa_1, aa_2, ..., aa_n)$.
- El conjunto de todas las matrices de tamaño $m \times n$ con entradas en un campo F, denotado $M_{n\times n}(F)$ es un espacio vectorial cuya suma se define para $A, B \in M_{n\times n}(F)$ como $(A + B)_{ij} = A_{ij} + B_{ij}$ y si $c \in F$, el producto por escalares es $(cA)_{ij} = cA_{ij}$, para $1 \leq i \leq m$, $1 \leq j \leq n$, donde A_{ij} es la entrada de la matriz localizada en la columna j, en el renglón i.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in M_{n\times n}(F)$$

La identidad $I \in M_{m\times n}(F)$ es tal que $A_{ij} = 1$ si $i = j$ y $A_{ij} = 0$ si $i \neq j$.

- Sea X un conjunto distinto del vacío, y F un campo arbitrario. Si consideramos al conjunto F^X de todas las funciones de X en F, donde la suma de $f, g \in F^X$ es la función $f + g \in F^X$ definida por $(f + g)(x) = f(x) + g(x)\ \forall x \in X$, y el producto de un escalar $k \in F$ con una función $f \in F^X$ es la función $kf \in F^X$ definida por $(kf)(x) = kf(x)\ \forall x \in X$; F^X es un espacio vectorial sobre F.

Al igual que en el caso de grupos, un espacio vectorial contiene espacios vectoriales que naturalmente se llaman *subespacios vectoriales* y están dotados de las mismas operaciones que el espacio que les contiene, de éstos siempre tendremos dos casos triviales, V y $\{0_V\}$, y al igual que en el caso de grupos, tenemos una caracterización de los subespacios que reduce enormemente la tarea de comprobar si un subconjunto es subespacio o no.

La notación para un subespacio W de un espacio vectorial V es la misma que aquella usada para indicar subgrupos, es decir $W \leq V$. Se hará uso de ésta cuando el contexto no genere confusión.

Teorema 1.2.3. *Sea V un F-espacio vectorial, un subconjunto $W \subseteq V$ es subespacio vectorial de V si y solo si:*

(i) $0_V \in W$.

(ii) *Si* $x, y \in W$, $x + y \in W$.

(iii) *Si* $c \in F$ $x \in W$, $cx \in W$.

ambas partes son consecuencia de la definición de espacio vectorial.

Ejemplo.

- Los números complejos $\mathbb{C}$ son un $\mathbb{R}$-espacio vectorial, donde $\mathbb{R} \leq \mathbb{C}$
- El conjunto de matrices en $M_{n\times n}(F)$ cuyas entradas son no-negativas, es decir $A_{ij} \geq 0$ para toda $1 \leq i \leq m$, $1 \leq j \leq n$ no es subespacio de $M_{n\times n}(F)$ porque al multiplicar alguna de ellas por un escalar negativo, se viola la tercera condición del teorema.
- $\{(x, y) \in \mathbb{R}^2 | y = kx \text{ con} k \in \mathbb{R}\}$ es el conjunto de todas las rectas por el origen y es un subespacio de $\mathbb{R}^{\mathbb{R}}$.

Dados dos subconjuntos no vacíos de vectores $S_1, S_2 \subseteq V$, al conjunto de vectores $\{x+y|x \in S_1\ y \in S_2\}$ denotado $S_1 + S_2$ se le llama la *suma* de S_1 y S_2. Si se tiene que $S_1, S_2 \leq V$ tales que $S_1 \cap S_2 = \emptyset$ y $W_1 + W_2 = V$ entonces se dice que V es la *suma directa* de W_1 con W_2, denotado $V = W_1 \oplus W_2$.

Ejemplo.
- Si en $M_{n\times n}(F)$ definimos $W_1 = \{A \in M_{n\times n}(F)|A_{ij} = 0 \text{ si } i > j\}$ y $W_2 = \{A \in M_{n\times n}(F)|A_{ij} = 0 \text{ si } i \leq j\}$, entonces $M_{n\times n}(F) = W_1 \oplus W_2$
- $\mathbb{C} = W_1 \oplus W_2$ si $W_1 = \mathbb{R}$ y $W_2 = \{\ ia|i = \sqrt{-1}$ y $a \in \mathbb{R}\}$

Como un espacio vectorial V es cerrado bajo suma y producto escalar, la suma arbitraria de vectores, o la multiplicación de un vector por cualquier elemento del campo, resultan en elementos del espacio vectorial. A continuación mostraremos al conjunto de vectores que puede ser obtenido a partir de un conjunto dado $S \subseteq V$.

Definición 1.2.4. Para V un F-espacio vectorial, y un subconjunto no vacío $S \subset V$, un vector $v \in V$ es *combinación lineal* de los vectores de S, si en S existen un número finito de vectores, $v_1, v_2, \ldots, v_n \in S$, y escalares en el campo $a_1, a_2, \ldots, a_n \in F$ tales que $v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$, donde dichos escalares son los *coeficientes* de tal combinación.

Al conjunto $\{a_1v_1 + a_2v_2 + \cdots + a_nv_n|a_i \in Fv_i \in S\}$ de todas las combinaciones lineales de un subconjunto $S \subset V_F$ se le conoce como el *generado de S*, o simplemente las combinaciones *K-lineales*, que se denota $\langle S\rangle$, donde se define $\langle\emptyset\rangle = 0$; se dice que S *genera* un F-espacio vectorial V si $\langle S\rangle = V$.

Un conjunto S es *linealmente dependiente* si existen vectores $v_1, v_2, \ldots, v_n \in S$ y escalares $a_1, a_2, \ldots, a_n \in F$ con al menos una $a_i \neq 0$ tales que

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0,$$

consecuentemente, un conjunto S es *linealmente independiente* si no es linealmente dependiente.

Ejemplo.
- Considere $S = \{(0,0),(1,0),(0,1)\} \subset \mathbb{R}^2$. Notemos que para $(x,y) \in \mathbb{R}^2$, $(x,y) = x(1,0) + y(0,1) + k(0,0)$ es una combinación lineal de elementos de S, lo que implica que $(x,y) \in \langle S\rangle = \mathbb{R}^2$. Por otro lado $4(0,0) + 0(1,0) + 0(0,1) = (0,0)$, es una combinación lineal de elementos de S cuyos coeficientes no son todos cero, que resulta en el vector cero, lo que implica la dependencia lineal de S.

- $\left\{\begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & a_{22} \end{pmatrix}\right\} \subset M_{2\times 2}(F)$ es un subconjunto de elementos linealmente independientes que genera un subespacio conocido como el espacio de las matrices *triangulares superiores* de 2×2 con coeficientes en F.

- Los vectores $v = (1+i, 2i)$, $w = (1, 1+i) \in \mathbb{C}^2$ son linealmente dependientes, considerando a $\mathbb{C}^2$ como un $\mathbb{C}$-espacio vectorial ya que $v - (1+i)w = 0$, sin embargo son linealmente independientes cuando $\mathbb{C}^2$ es un $\mathbb{R}$-espacio vectorial.

Del primer inciso del ejemplo anterior, se puede ver que

$$\langle\{(0,0),(1,0),(0,1)\}\rangle = \langle\{(1,0),(0,1)\}\rangle = \mathbb{R}^2,$$

sin embargo $\{(1,0),(0,1)\}$ es linealmente independiente, lo que ejemplifica que todo conjunto de vectores contiene un subconjunto linealmente independiente cuyo generado será igual al del conjunto original; de ahí la importancia de encontrar subconjuntos linealmente independientes con el menor número de elementos posible para generar un espacio vectorial V; dado que todo vector $v \in V$ es combinación lineal de vectores generadores, serán estos los que determinen la estructura del espacio en cuestión.

Definición 1.2.5. Un subconjunto β de un F-espacio vectorial V es una *base* si es un conjunto linealmente independiente tal que $\langle\beta\rangle = V$, denotada $\beta \hookrightarrow V$. La cardinalidad $|\beta|$ es la *dimensión* del espacio vectorial denotada $\dim V$. Un espacio es de dimensión finita si $|\beta| < \infty$.

Sean $e_1 = (1,0,0,\ldots,0)$, $e_2 = (0,1,0,\ldots,0)$, $\ldots$, $e_n = (0,0,0,\ldots,1)$ elementos en F^n, $\{e_1, e_2, \ldots, e_n\}$ es la base *canónica* de F^n con $\dim F^n = n$. En $M_{m\times n}(F)$, si E^{ij} la matriz cuya única entrada distinta de cero es un 1 en el i-ésimo renglón y la j-ésima columna $\{E^{ij} | 1 \leq i \leq m, 1 \leq j \leq n\}$ es la base canónica del espacio de matrices de tamaño $m \times n$, con $\dim M_{m\times n}(F) = mn$.

Observemos que vector $v \in V$ se expresa de forma única como combinación lineal de elementos de la base. Considerense $\{v_1, v_2, ..., v_n\} = \beta \hookrightarrow V$ y

$$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n, v = b_1v_1 + b_2v_2 + \cdots + b_nv_n$$

dos combinaciones lineales distintas, entonces

$$(a_1 - b_1)v_1 + (a_2b_2)v_2 + \cdots + (a_nb_n)v_n = 0.$$

Dado que $\beta \hookrightarrow V$, $a_1 - b_1 = a_2 - b_2 = \cdots = a_n - b_n = 0$, y $a_1 = b_1$, $a_2 = b_2 \cdots a_n = b_n$, es decir, las combinaciones lineales son iguales. Si V es un espacio vectorial de dimensión $\dim V = n$, y $\beta \subset V$ es un subconjunto de vectores con $|\beta| = n$, β es base. Así, todo subconjunto $S \subset V$ linealmente independiente se puede extender a una base, añadiendo vectores linealmente independientes a S hasta que tenga cardinalidad igual a $\dim V$.

Si V es un espacio vectorial de dimensión $\dim V = n$, un K-hiperplano es un subespacio de dimensión $n - 1$.

Definiremos ahora las funciones entre espacios vectoriales que preservan estructura, veremos algunos resultados que profundizan el estudio estructural de dichos espacios, algunos otros análogos a los vistos previamente, y encontraremos que éstas funciones quedan completamente determinadas por un elemento en $M_{m\times n}(F)$.

Definición 1.2.6. Sean V y W dos F-espacios vectoriales. Se dice que una función $T : V \longrightarrow W$ es una *transformación lineal* si para todo $x, y \in V$, $c \in F$ se tiene que

(i) $T(x + y) = T(x) + T(y)$.

(ii) $T(cx) = cT(x)$.

Se define también al conjunto $N(T) := \{x \in V | T(x) = 0\}$ como el *núcleo* de T, que es un subespacio vectorial de V. Definimos así $\dim N(T)$=nul(T), conocida como la *nulidad de* T.

Por otro lado definimos $R(T) := \{T(x) | x \in V\}$ llamado el conjunto *imagen* de T, que de igual forma constituye un subespacio vectorial, ésta vez en W, análogamente definimos $\dim R(T)$:=ran(T) como el *rango* de T.

Ejemplo.

- $T : F^n \longrightarrow F^n$, donde

$$T(a_1, a_2, \ldots, a_i, \ldots, a_n) = (0, 0, \ldots, a_i, \ldots, 0)$$

  conocida como la *proyección en la i-ésima entrada* , es una transformación lineal. Donde $N(T) = \{(a_1, a_2, \ldots, a_i, \ldots, a_n) \in F^n | a_i = 0\}$, y nul$T = n - 1$; por otro lado $R(T) = \{(0, 0, \ldots, a_i, \ldots, 0) | a_i \in F\}$, entonces ran$(T) = 1$.

- Si $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, con $T(a_1, a_2) = (1, a_2)$. Vemos que

$$T((a_1, a_2) + (b_1, b_2)) = T(a_1 + b_1, a_2 + b_2) = (1, a_2 + b_2)$$

por otro lado

$$T(a_1, a_2) + T(b_1, b_2) = (2, a_2 + b_2)$$

, de donde se sigue que T no es lineal.

Observación 1.2.7. Sea $T : V \longrightarrow W$ una transformación lineal, con dim$V$ finita y $\beta = \{v_1, v_2, \ldots, v_n\} \hookrightarrow V$ entonces

$$\langle T(\beta) \rangle = \langle \{T(v_1), T(v_2), \ldots, T(v_k)\} \rangle = Im(T).$$

Demostración. Claramente $T(v_i) \in \text{Im}(T)$, y por eso $\langle \{T(v_1), T(v_2), \ldots T(v_n)\} \rangle \subseteq \text{Im}(T)$. Por otro lado, si $w \in \text{Im}(T)$ entonces $w = T(v)$ para alguna $v \in V$, pero $v = \sum_{i=1}^{n} a_i v_i$, entonces

$$w = T(\sum_{i=1}^{n} a_i v_i) = \sum_{i=1}^{n} aT(v_i)$$

. ■

Teorema 1.2.8 (Teorema de la dimensión)**.** *Si V, W son espacios vectoriales, $T : V \longrightarrow W$ es una transformación lineal entre ellos y dim$V = n$, entonces*

$$nul(T) + ran(T) = dimV.$$

La demostración se obtiene extendiendo $\beta' = \{v_1, v_2, \ldots, v_k\} \hookrightarrow N(T)$ una base para el núcleo de T, a $\beta = \{v_1, v_2, \ldots, v_k, v_{k+1}, \ldots, v_n\} \hookrightarrow V$ una base para V, y demostrando que $\{T(v_1), T(v_2), \ldots, T(v_n)\} \hookrightarrow R(T)$ es una base para la imagen de T.

Ejemplo.

$T : M_{n\times n}(F) \longrightarrow F$, con $T(A) = \Sigma_{i=1}^{n} A_{ii}$, (la suma de los elementos de la diagonal de una matriz cuadrada) conocida como la *traza matricial* de A, es una transformación lineal. Como ran(T) = dim$R(T)$ = F, ran(T) = dim$\langle \{0, 1\} \rangle$ = dim$F$ = 1, Por el teorema de la dimensión tenemos que nul(T) = dim$V$ − ran$T = n^2 - 1$.

Corolario 1.2.9. *Una transformación lineal $T : V \longrightarrow W$ es inyectiva si y sólo si $N(T) = \{0_W\}$.*

Demostración. Si T es inyectiva y $x \in N(T)$, entonces $T(x) = 0 = T(0)$, es decir $x = 0$ y $N(T) = \{0\}$. Si $N(T) = \{0\}$ y tenemos que $T(x) = T(y)$, entonces $0 = T(x) - T(y) = T(x - y)$, es decir, $x - y \in N(T) = \{0\}$ y $x = y$. ■

Teorema 1.2.10. *Si T es una transformación lineal de V en W con $dim(V) = dim(W) = n$, entonces son equivalentes*

(1) T es inyectiva.

(2) T es suprayectiva.

(3) $ran(T) = dim(W)$.

Demostración. Del teorema de la dimensión tenemos que

$$\text{nul}(T) + \text{ran}(T) = \dim(T).$$

Y por el corolario anterior, tenemos que T es inyectiva si y sólo si $N(T) = \{0\}$, si y sólo si $\text{Nul}T = 0$, si y sólo si $\dim(V) = \dim W$, si y sólo si $R(T) = W$, es decir T es suprayectiva. ■

A continuación describiremos la relación entre las transformaciones lineales entre espacios vectoriales de dimensión n y las matrices $M_{n\times n}(F)$.

Si V es un espacio vectorial, β es una *base ordenada* para V, si es una base con un orden especifico denotada $\beta \overset{b.o.}{\hookrightarrow} V$.

Si $\beta = \{v_1, v_2, \ldots, v_n\} \overset{b.o.}{\hookrightarrow} V$, para todo vector $v \in V$, existen únicos $a_i \in F$ tal que $x = \Sigma_{i=1}^{n} a_i v_i$, entonces definimos el *vector coordenado de x respecto a la base β* como

$$[x]_\beta = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

Análogamente, si $\beta = \{v_1, v_2, \ldots, v_n\} \overset{b.o.}{\hookrightarrow} V$, $\gamma = \{w_1, w_2, \ldots, w_m\} \overset{b.o.}{\hookrightarrow} W$ son bases ordenadas para espacios vectoriales de dimensión finita, y $T : V \longrightarrow W$ es una transformación lineal, entonces para cada j, $1 \leq j \leq n$, existen únicos escalares $a_{ij} \in F$, con $1 \leq i \leq n$ tales que $T(v_j) = \Sigma_{i=1}^{m} a_{ij} w_i$, para $1 \leq j \leq n$. Usando ésta notación, podemos finalmente definir la matriz $A \in M_{m\times n}(F)$ tal que $A_{ij} = a_{ij}$ como la *matriz de representación de T con respecto a β en γ*, denotada $A = [T]_\beta^\gamma$. En el caso de que $\beta = \gamma$, $A = [T]_\beta$.

Ejemplo. ▪ Considere $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ dada por $T(a_1, a_2) = (a_1 + a_2, a_1)$ lineal y sean $\beta = \{(0,4),(2,1)\}$, $\gamma = \{(1,1),(0,1)\}$ bases ordenadas de $\mathbb{R}^2$. Tenemos que:

$$\begin{array}{l} T(0,4) = (4,0) = 4(1,1) - 4(0,1) \\ T(2,1) = (3,2) = 3(1,1) - 1(0,1) \end{array} \implies [T]^{\gamma}_{\beta} = \begin{pmatrix} 4 & 3 \\ -4 & -1 \end{pmatrix}$$

Por otro lado,

$$\begin{array}{l} T(1,1) = (2,1) = 0(0,4) + 1(2,1) \\ T(0,1) = (1,1) = \frac{1}{8}(0,4) + \frac{1}{2}(2,1) \end{array} \implies [T]^{\gamma}_{\beta} = \begin{pmatrix} 0 & 1 \\ \frac{1}{8} & \frac{1}{2} \end{pmatrix}$$
$$\therefore [T]^{\gamma}_{\beta} \neq [T]^{\beta}_{\gamma}.$$

Además, cambiar el orden de las bases cambiará el orden de los renglones o columnas, dependiendo de que base se cambie.

Observación 1.2.11. Si V, W son espacios vectoriales de dimensión finita con bases $\beta = \{v_1, v_2, \ldots, v_n\}$, $\gamma = \{w_1, w_2, \ldots, w_n\}$ respectivamente, y $T, U : V \longrightarrow W$ son dos transformaciones lineales, se tiene que $T(v_j) = \Sigma_{i=1}^{m} a_{ij} w_i$, $U(v_j) = \Sigma_{i=1}^{m} b_{ij} w_i$ (con $1 \leq j \leq n$) para escalares únicos a_{ij}, b_{ij} $(1 \leq i \leq m, 1 \leq j \leq n)$, entonces

$$(T+U)(v_j) = \textstyle\sum_{i=1}^{m} (a_{ij} + b_{ij}) w_i$$

y así $([T+U]^{\gamma}_{\beta})_{ij} = a_{ij} + b_{ij} = ([T]^{\gamma}_{\beta})_{ij} + ([U]^{\gamma}_{\beta})_{ij}$, es decir, $[T+U]^{\gamma}_{\beta} = [T]^{\gamma}_{\beta} + [U]^{\gamma}_{\beta}$. Análogamente $[aT]^{\gamma}_{\beta} = a[T]^{\gamma}_{\beta}$

Si definimos la suma de transformaciones lineales $T, U : V \longrightarrow W$ como $(T+U)(x) = T(x) + U(x)$ para toda $x \in V$, y definimos $aT : V \longrightarrow W$ como $(aT)(x) = aT(x)$, es fácil ver que el conjunto de transformaciones lineales de V en W forma a su vez un espacio vectorial, evidentemente llamado el *espacio vectorial de las transformaciones lineales de V a W*, denotado $\mathcal{L}(V, W)$, que cuando $V = W$ es simplemente $\mathcal{L}(V)$. Dicho resultado queda también respaldado en su análogo matricial por los últimos dos incisos del ejemplo anterior.

Si $A \in M_{m \times n}(F)$, $B \in M_{n \times p}(F)$, el *producto matricial* de A y B es la matriz denotada $AB \in M_{m \times p}(F)$ tal que $(AB)_{ij} = \Sigma_{k=i}^{n} A_{ik} B_{kj}$ para $1 \leq i \leq m$, $1 \leq j \leq p$. Por otro lado si V, W, Z son espacios vectoriales con

bases ordenadas α, β, γ respectivamente, y $T : V \longrightarrow W$, $U : W \longrightarrow Z$ son transformaciones lineales con matrices asociadas $[T]_\alpha^\beta$, $[T]_\beta^\gamma$, entonces

$$[UT]_\alpha^\gamma = [U]_\beta^\gamma [T]_\alpha^\beta,$$

es decir,la composición de transformaciones se corresponde con un producto de matrices, y viceversa.

Toda matriz $A \in M_{m\times n}(F)$ define una transformación $L_A : F^n \longrightarrow F^m$ definida por $L_A(x) = Ax$, el producto matricial de A y el vector columna $x \in F^n$. Esta transformacion es conocida como la *multiplicación izquierda.*

Definición 1.2.12. Una matriz $A \in M_{n\times n}(F)$ es *invertible* si existe una matriz denotada $A^{-1} \in M_{n\times n}$ (la matriz *inversa* de A) tal que $AA^{-1} = A^{-1}A = I$. Análogamente una transformación lineal entre espacios vectoriales $T : V \longrightarrow W$ es *invertible* si existe una transformación lineal entre espacios vectoriales denotada $T^{-1} : W \longrightarrow V$ (la transformacion *inversa* de T) tal que $TT^{-1} = I_V$ y $T^{-1}T = I_W$. En el caso de existir una función biyectiva entre ambos, se habla de un *isomorfismo* entre espacios vectoriales.

Observación 1.2.13. V y W dos espacios F-vectoriales de dimensión finita son isomorfos si y solo si dim$V$=dim$W$=n; la primera implicación es consecuencia de la existencia de un isomorfismo, y el reciproco se obtiene demostrando que una transformación que mande la base de V en la base de W es un isomorfismo. De esto se sigue que V un F-espacio vectorial de dimensión dim$V$=n es también isomorfo a F^n.

Observación 1.2.14. Si V y W son F-espacios vectoriales de dimensión finita, con bases ordenadas β, γ respectivamente, la función $\Phi : \mathcal{L}(V, W) \longrightarrow M_{m\times n}(F)$, definida para $T \in \mathcal{L}(V, W)$ como $\Phi(T) = [T]_\beta^\gamma$ es un isomorfismo; De esto, se desprende que cualquier concepto o resultado en $M_{m\times n}(F)$ tenga su equivalencia en $\mathcal{L}(V, W)$. Es decir, $\mathcal{L}({}_FV, {}_F W) \cong M_{m\times n}(F)$.

Consideremos ahora un tipo especial de funciones lineales; si V es un F-espacio vectorial, una transformación lineal f es una *funcional lineal* si $f : V \longrightarrow F$, denotadas en minúsculas para distinguirles de las demás transformaciones. Por ser un caso particular de las transformaciones lineales (que forman un espacio vectorial sobre F), se tiene que $\mathcal{L}(V, F)$ es un F-espacio vectorial llamado *espacio dual* de V, denotado V^*, cuya dimensión es dimV^*=dim$(\mathcal{L}(V, F))$ =dim$V$dim$F = m \cdot 1$ =dim$V$, lo cual implica que $V \cong V^*$.

Si $\beta = \{v_1, v_2, \ldots, v_n\} \overset{b.o.}{\hookrightarrow} V$ es una base ordenada para un F-espacio vectorial, se define para cada $i = 1, 2, \ldots, n$, $f_i : V \longrightarrow F$ por $f_i(v) = a_i$ donde

$$[x]_\beta = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

es el vector de coordenado respecto a la base β. A f_i se le conoce como la *i-ésima función coordenada respecto a* β.

Teorema 1.2.15. *Sean V es un espacio vectorial de dimensión finita con base ordenada $\beta = \{v_1, v_2, \ldots, v_n\}$, y f_i $(1 \leq i \leq n)$ la i-ésima función coordenada respecto a β, entonces $\beta^* = \{f_1, f_2, \ldots, f_n\}$ es una base ordenada para V^* y se tiene que*

$$f = \sum_{i=1}^{n} f(x_i) f_i$$

La base β^* del teorema se llama la *base dual* de β.

Ejemplo.

- Si $V = \mathbb{R}^2$, V es un $\mathbb{R}$-espacio vectorial, y por eso el espacio dual es $V^* = \{f | f : \mathbb{R}^2 \longrightarrow \mathbb{R}\}$.
- Consideremos $\beta = \{(2,1), (3,1)\} \hookrightarrow \mathbb{R}^2$. Si $\beta^* = \{f_1, f_2\}$ es la base dual de β, entonces

$$\begin{aligned} 1 &= f_1(2,1) = f_1(2e_1 + e_2) = 2f_1(e_1) + f_1(e_2) \\ 0 &= f_1(3,1) = f_1(3e_1 + e_2) = 3f_1(e_1) + f_1(e_2). \end{aligned}$$

  de donde $f_1(e_1) = -1$ y $f_1(e_2) = 3$, es decir $f_1(x, y) = -x + 3y$. Análogamente se tiene que $f_2(x, y) = x - 2y$, y hemos obtenido explícitamente a β^*.

1.3. Teoría de Galois

A su corta edad, Evariste Galois (1811–1832) encontró relaciones entre los polinomios, lo que conocemos ahora como teoría de grupos, y la teoría de campos, abriendo paso a una de las ramas principales del álgebra abstracta, que permitió resolver problemas antiquísimos (como determinar el tipo

de construcciones que es posible construir con regla y compás, planteado por los griegos varios siglos antes), y encontrar relaciones entre áreas de las matemáticas que entonces parecían ser independientes.

Definición 1.3.1. Si R es un conjunto, $(R, +, \cdot, 0)$ es un *anillo* si $(R, +, 0)$ es un grupo abeliano y para toda $a, b, c \in R$ se tiene que:

- $ab \in R$
- $a(bc) = (ab)c$
- $a(b + c) = ab + ac$ y $(b + c)a = ba + ca$.

Si además $ab = ba$ para toda $a, b \in R$ es un *anillo conmutativo*. Si existe un elemento 1_R tal que $1_R a = a1_R = a$ para toda $a \in R$, es un *anillo con unitario*. Un elemento no cero $a \in R$ es un *divisor de cero izquierdo* (*derecho*) si existe un elemento no cero $b \in R$ tal que $ab = 0$ ($ba = 0$),o simplemente un *divisor de cero* si es izquierdo y derecho. Si R es un anillo con unidad, un elemento $a \in R$ es *invertible por la izquierda* (*derecha*) si existe $c \in R$ tal que $ca = 1_R$ ($ac = 1_R$), y c es el elemento *inverso izquierdo* (*derecho*). Si un elemento es invertible por ambos lados es una *unidad* de R. Un anillo conmutativo R con identidad $1_R \neq 0$ sin divisores de cero es un *dominio entero*. Un anillo D con identidad $1_D \neq 0$ donde todo elemento distinto de cero es unidad es un *anillo con división*. En cualquier caso, si en un anillo R existe un mínimo entero n tal que $n \cdot a = 0$ para toda $a \in R$, se dice que el anillo es de *característica* n, denotada $\text{char}R = n$; si no existe tal n entonces R es de característica 0.

Si un subconjunto $S \subset R$ es un anillo bajo las mismas operaciones que R, entonces es un *subanillo*, denotado como $S \leq R$. Un subanillo $I \leq R$ tal que para toda $r \in R$, $x \in I$, $rx \in I$ [respectivamente $xr \in I$] es un *ideal izquierdo* [derecho] de R; si I es ideal izquierdo y derecho, es un ideal *bilateral* o simplemente un *ideal*. Si un ideal I es *generado* por un solo elemento $x \in R$ (denotado $I = (x)$) entonces se dice que el ideal es *principal*; un anillo en el que todo ideal sea generado por un solo elemento es un *anillo de ideales principales*, y si el anillo es dominio entero, *dominio de ideales principales*. Si $I \leq R$ es un ideal de R, y siempre que para cualquier otro ideal J tal que $I \supseteq J \supseteq R$ se tiene que $I = J$ o $J = R$, entonces I es un ideal *máximo*.

Si R es un anillo y $I \leq R$ un ideal de R, entonces el grupo aditivo cociente R/I es un anillo con producto dado por $(a + I)(b + I) = ab + I$.

Ejemplo.

- $\mathbb{Z}$ es un dominio entero, mientras que el conjunto E de todos los números pares es un anillo conmutativo sin identidad. Por otro lado $E = (2)$ es un ideal principal y además, si $p \in \mathbb{Z}$ es otro número primo, el generado de p, $(p) = \{kp | k \in \mathbb{Z}\}$ es también un ideal principal. Análogamente se demuestra que los ideales pricipales en $\mathbb{Z}$ son generados por números primos, y por esto $\mathbb{Z}$ es un dominio de ideales principales. Por otro lado, $\mathbb{Z}$ es de caracteristica $\text{char}\mathbb{Z} = 0$, mientras que $\text{char}\mathbb{Z}_n = n$.

- Un campo F es un anillo de división conmutativo, pero $M_{n\times n}(F)$ es solamente un anillo no conmutativo con identidad, donde las unidades son las matrices invertibles. Un ideal en $M_{n\times n}(F)$ son las matrices triangulares superiores.

- Si R es un anillo, y $R[x]$ denota el conjunto de sucesiones de elementos de R $(a_0, a_2, \dots)$ tales que $a_i \neq 0$ para un número finito de índices i, bajo las operaciones

  - $(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$
  - $(a_0, a_1, \dots)(b_0, b_1) = (c_0, c_1, \dots)$, donde
    $c_n = \sum_{i=0}^{n} a_{n-i}b_i = a_nb_0 + a_{n-1}b_1 + \cdots + a_1b_{n-1} + a_0b_n = \sum_{k+j=n} a_kb_j$.

  forman un anillo donde el 0 es $(0, 0, \cdots)$ la identidad en $R[x]$ (en caso de existir en R) es $(1_R, 0, 0, \dots)$

El anillo descrito en el inciso anterior es el *anillo de polinomios en* R, y sus elementos son obviamente *polinomios* en R con *variable* x. ésta notación puede ser distinta a la que comúnmente se da para los polinomios (expresiones de la forma $a^nx^n + \cdots + a_1x + a_0$ donde $a_i \in R$), sin embargo es la manera más formal.

La equivalencia entre una definición y la otra proviene de identificar a x con $(0, 1_R, 0, 0, \dots) \in R[x]$, x^n con $(0, 0, \dots, 1_R, 0, \dots)$ (donde 1_R ocupa la coordenada $(n + 1)$), y si $r \in R$ entonces para cada $n \geq 0$, $rx^n = x^nr = (0, \dots, 0, r, 0, \dots)$ (donde r ocupa la coordenada $(n + 1)$). Así, para cada polinomio $f \in R[x]$ existen únicos $n \in \mathbb{N}$ y $a_0, \dots, a_n \in R$ tales que $f = a_0x^0 + a_1x^1 + \cdots + a_nx^n$; es decir, si $f = b_0x^0 + b_1x^1 + \cdots + b_mx^m$, con $b_i \in R$ y $m \geq n$ entonces $a_i = b_i$ para $i = 1, \dots, n$ y $b_i = 0$ para $n < i \leq m$. Si el R es un anillo con unidad entonces $x^0 = 1_R$ y con el fin de facilitar la notación $f = a_0x_0 + a_1x^1 + \cdots + a_nx^n = a_0 + a_1x + \cdots + a_nx^n$.

Si $f = a_0+a_1x+\cdots+a_nx^n = a_nx^n+\cdots+a_1x+a_0 = \sum_{i=0}^{n} a_ix^i \in R[x]\setminus\{0\}$ es un polinomio en R, los elementos $a_i \in R$ son los *coeficientes* del polinomio, donde a_0 es el *termino constante*, a_n es el *coeficiente principal*, y n es el *grado* de f denotado $\delta(f)$ [1], el grado del polinomio 0 se define como $\delta(0) := -\infty$. Un polinomio es *constante* si $a_i = 0$ para toda $i \neq 0$, y es *mónico* si $a_n = 1_R$. Un elemento $r \in R$ es *raíz* del polinomio $f = a_nx^n + \cdots + a_1x + a_0 \in R[x]$, si $a_nr^n + \cdots + a_1r + a_0 = 0_R$.

Todos las definiciones anteriores se conservan cuando el anillo R es un campo, y se han definido así los conceptos para dejar en claro que los polinomios se pueden definir desde una estructura mas general, sin embargo, en nuestro caso trabajaremos con el anillo de polinomios definido sobre un campo F, y denotaremos al anillo de polinomios como $F[x]$.

Ejemplo.

- Consideremos el polinomio mónico de segundo grado x^2-2, como sus coeficientes son $0, 2 \in \mathbb{Z}_3$ $0, 2 \in \mathbb{Q}$ $0, 2 \in \mathbb{R}$ etcétera, primero debemos indicar en qué anillo de polinomios lo vamos considerar, tomemos $x^2 - 2 \in \mathbb{Q}[x]$. Por simple aritmética se tiene que $x^2-2 = (x+\sqrt{2})(x-\sqrt{2})$, $(\sqrt{2})^2-2 = 2-2 = 0$ y $(-\sqrt{2})^2-2 = 2-2 = 0$; por eso $\sqrt{2}$ y $-\sqrt{2}$ son dos números para los cuales $x^2 - 2 = 0$, sin embargo $-\sqrt{2}, \sqrt{2} \notin \mathbb{Q}$, entonces el polinomio no tiene raíces en $\mathbb{Q}$, y en éste caso no tiene sentido escribir $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$.

- Consideremos dos elementos de un mismo anillo de polinomios $2x^3 + 5x^2 + 6x + 1$, $x^2 + x \in \mathbb{Q}[x]$, nótese ambos están relacionados en el sentido de que $(x^2 + x)(2x + 3) + (3x + 1) = 2x^3 + 5x^2 + 6x + 1$.

Es claro que no todo polinomio $f \in F[x]$ tiene sus raíces en F, pero hemos visto que si existiera una raíz $a \in F$ podríamos expresar al polinomio como el producto $f(x) = (x - a)p(x)$, donde $p(x)$ es otro polinomio (de grado menor) en $F[x]$, por otro lado, en el segundo inciso del ejemplo vimos una manera de relacionar dos polinomios, que en realidad se cumple para cualquier par de elementos $f, g \in G$. Estos resultados conducen al hecho de que un polinomio $f \in F[x]$ puede descomponerse de manera única como el producto de polinomios de grado menor o igual a $\delta(f)$, y en el caso de que las raíces se encuentren en el campo, éstos serán de primer grado.

Teorema 1.3.2. *Si F es un campo, para todo $f, g \in F[x]$:*

[1] también se suele decir que $f \in F[x]$ es de primer, segundo grado, etc.

(i) $\delta(f+g) \leq max(\delta(f), \delta(g))$

(ii) $\delta(fg) = \delta(f) + \delta(g)$

(iii) (Algoritmo de la División en $F[x]$) Existen únicos polinomios $q, r \in F[x]$ tales que $f = qg + r$ con $\delta(r) < \delta(g)$, o $\delta(r) = 0$.

Los primeros dos incisos se siguen de la definición de suma y producto de polinomios en $F[x]$ donde F es un campo, mientras que el tercero se demuestra por inducción sobre $n = \delta f$ en el caso de que $\delta f \geq \delta g$ y cuando $\delta g > \delta f$ se corrobora con $q = 0$, $r = f$.

Teorema 1.3.3 (Teorema del Factor)**.** *Si F es un campo y $f(x) \in F[x]$, $a \in F$ es raíz de $f(x)$ si y solamente si $f(x) = (x-a)q(x)$.*

Demostración. Si $a \in F$ es una raíz de $f \in F[x]$, por el algoritmo de la división podemos escribir a f como $f(x) = q(x)(x-a) + r(x)$ donde $\delta(r) < \delta(x-a) = 1$, es decir que $r(x) = c$ una constante, pero $0 = f(a) = q(a)(a-a) + r(a) = c$, entonces $f(x) = q(x)(x-a)$. Por otro lado si $f(x) = q(x)(x-a)$, $a \in F$ es una raíz de f, y si $f(x) = q(x)(x-a)^n$, a es una raíz de *multiplicidad* n. Demostración obtenida de [2]. ■

Si $f \in F[x]$, y $f(x) = q(x)g(x) + r(x)$, a $q(x)$ se le llama el *cociente* y a $r(x)$ el *residuo* de la división de $f(x)$ por $g(x)$. Si $q(x) = 0$ se dice que $g(x)$ es *divisor* de $f(x)$, que $g(x)$ *divide* a $f(x)$ (denotado $g(x)|f(x)$), o que $f(x)$ es un *multiplo* de $g(x)$. Si $f \in F[x]$ puede expresarse como producto de dos o mas polinomios de grado menor se dice que es *reducible* y que tiene una *factorización* compuesta por el producto de dichos polinomios, y en caso contrario $f(x)$ es *irreducible*. Si para $f, g \in F[x]$, existe un $c \in F[x]$ tal que $c(x)|f(x)$, $c(x)|g(x)$ entonces $c(x)$ es *divisor común* de $f, g \in F[x]$, si para cualquier otro divisor común $d(x)$, se tiene que $d(x)|c(x)$, entonces $c(x)$ es un *máximo común divisor*, denotado $c = mcd(f, g)$.

Teorema 1.3.4. *Si F es un campo, y $f \in F[x]$ es un polinomio no constante, entonces hay una factorización única (salvo el orden de los polinomios) para $f(x) = up_1(x)p_2(x)\cdots p_s(x)$ donde $u \in F$, $0 \neq u$, y cada p_i es un polinomio mónico irreducible.*

Tanto la existencia como la unicidad se demuestran por inducción sobre $n = \delta(f)$, y se puede consultar en [5].

Ejemplo. $f(x) = 1 - x^2 \in \mathbb{R}[x]$ no tiene factorización, entonces es irreducible en $\mathbb{R}[x]$, mientras que en $\mathbb{C}[x]$, $1 - x^2 = (x + i)(x - i)$; por otro lado considerando el polinomio $\mathbb{C}[x]$ $g(x) = x^3 + ix^2 + x + i = (x + i)^2(x - i)$, tenemos que $-i \in \mathbb{C}$ es una raíz de *multiplicidad* 2 de $g(x)$. Así que $1 + i$ e $1 - i$ son ambos divisores comunes, sin embargo $1 - x^2 = mcd(f, g)$.

Definición 1.3.5. Considere tres campos K, E, F tales que $K \subseteq E \subseteq F$. Se dice que F es *extensión* de E y K, y que a su vez E es extensión de K; a E se le llama *campo intermedio*.

Si un campo F es una extensión de un campo K, claramente $1_F = 1_K$. Además, F es también un espacio vectorial sobre K, cuya dimensión es denotada por $[F : K]$; se dice que F es una extensión de *dimensión finita* o *infinita* dependiendo si $[F : K]$ es finita o infinita.

Teorema 1.3.6. *Sean $K \subset E \subset F$ campos, entonces*

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

.

Demostración. Si $[K : E] = m$ con $\{v_1, \ldots, v_m\} \hookrightarrow K_E$ y $[E : F] = n$ con $\{w_1, \ldots, w_n\} \hookrightarrow E_F$, el teorema se reduce a demostrar que el conjunto de mn elementos $\{v_i w_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ es una base para K_F ■

Si F es un campo y X es un subconjunto $X \subseteq F$, el subcampo *generado* por X es la intersección de todos los subcampos $F_i \leq F$ tales que $X \subseteq F_i$ donde $i \in I$ es un conjunto de indices. Si F es extensión de un campo K, y $X \subseteq F$, el subcampo generado por $K \cup X$ se llama el subcampo *generado por X sobre K*, y es denotado $K(X)$. Si $X = \{u_1, \ldots, u_n\}$, el subcampo $K(X) \leq F$, denotado $K(u_1, \ldots, u_n)$, es una extensión *finitamente generada* de K. Si $X = \{u\}$ entonces es una extensión *simple*. De estas definiciones se sigue que $F(u_1, \ldots, u_n) = F(u_1, \ldots, u_{n-1})(u_n)$.

Si F es un campo y se tiene que $u, v \in F$, con $v \neq 0$, entonces $uv^{-1} \in F$ será denotado también por u/v.

Teorema 1.3.7. *Si $K \leq F$ son campos con $u, \in F$, y $X \subset F$, entonces*

(i) El subanillo $K[u]$ consiste de todos los elementos de la forma $f(u)$, donde f es un polinomio con coeficientes en K (es decir, $f \in K[x]$)

(ii) El subcampo $K(u)$ consiste de elementos de la forma $f(u)/g(u) = f(u)g(u)^{-1}$, donde $f, g \in K[x]$ y $g(u) \neq 0$.

Nótese que el anillo del primer inciso resulta de evaluar a cada polinomio de $K[x]$ en $u \in F$, y además es el subanillo más pequeño que contiene a $K \cup \{u\}$. Por otro lado $K(u)$ es el *anillo de cocientes* de $K[u]$, también conocida como la extensión generada de *agregar* u a F.

Ejemplo. Consideremos a $\mathbb{Q}(\sqrt{2}) =< \mathbb{Q} \cup \{\sqrt{2}\} >$; según el teorema anterior $\mathbb{Q}(\sqrt{2}) = \{\frac{f(\sqrt{2})}{g(\sqrt{2})} | f, g \in \mathbb{Q}[x], \text{ y } g(\sqrt{2}) \neq 0\}$, indicaremos el motivo de las dos contenciones:

$\subseteq$ Si $k \in \mathbb{Q}(\sqrt{2})$, la definición implica que $k = b + \alpha\sqrt{2}$, con b , $\alpha \in \mathbb{Q}$. Para encontrar $f, g \in \mathbb{Q}$ tal que $k = \frac{f(\sqrt{2})}{g(\sqrt{2})}$ y $g \neq 0$, basta considerar $f(\sqrt{2}) = k$ y $g = 1$ (la constante 1), de esa forma

$$\frac{f(\sqrt{2})}{g(\sqrt{2})} = \frac{k}{1} = k.$$

Entonces $k \in \{\frac{f(\sqrt{2})}{g(\sqrt{2})} | f, g \in \mathbb{Q}[x], \text{ y } g(\sqrt{2}) \neq 0\}$.

$\supseteq$ Si $k \in \{\frac{f(\sqrt{2})}{g(\sqrt{2})} | f, g \in \mathbb{Q}[x], g(\sqrt{2}) \neq 0\}$ entonces $k = \frac{f(\sqrt{2})}{g(\sqrt{2})}$ para algún $f, g \in \mathbb{Q}[x]$ y $g(\sqrt{2}) \neq 0$. Digamos que $f(\sqrt{2}) = a_0 + a_1\sqrt{2} + \cdots + a_n\sqrt{2}^n$ y $g(\sqrt{2}) = b_0 + b_1\sqrt{2} + \cdots + b_n\sqrt{2}^m \neq 0$; para que mostrar que $\frac{f(\sqrt{2})}{g(\sqrt{2})} \in \mathbb{Q}(\sqrt{2})$, supongamos que m es par, entonces $\sqrt{2}^m = 2^{\frac{m}{2}}$, y

$$g(\sqrt{2}) = b_0 + b_1\sqrt{2} + b_2 2 + b_3 2\sqrt{2} + \cdots + 2^{\frac{m}{2}}$$

es decir,

$$g(\sqrt{2}) = (b_0 + 2b_2 + 2^2 b_4 + \cdot + 2^{\frac{m}{2}} b_m) + \sqrt{2}(b_1 + 2b_3 + 2^2 b_5 + \cdot + 2^{\frac{m-1}{2}} b_{m-1}).$$

Por eso $g(\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$, de esta manera $f(\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$ también; como $\mathbb{Q}(\sqrt{2})$ es un campo podemos decir que $k \in \mathbb{Q}(\sqrt{2})$. El caso en que n es impar es análogo.

Definición 1.3.8. Sea F una extensión de un campo K. Un elemento $u \in F$ es *algebraico* en K si es raíz de un polinomio $f \in K[x]$, si por el contrario $u \in F$ no es raíz de ningún polinomio $f \in K[x]$ entonces es *trascendente* en K. Una extensión es *algebraica* si todo elemento de F es algebraico en K, y es *trascendente* si existe un elemento de F que sea trascendente en K.

Ejemplo. Sean $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ el conjunto de números racionales, reales, y complejos respectivamente, entonces tenemos que $\mathbb{C} = \mathbb{R}(i)$ y a su vez $\mathbb{R} = \mathbb{Q}(\mathbb{I})$, donde $\mathbb{I}$ es el conjunto de números irracionales. Por lo anterior, $\mathbb{C}$ y $\mathbb{R}$ son extensiones algebraicas de $\mathbb{Q}$; resultados mas complejos demuestran que $e, \pi \in \mathbb{R}$ son elementos trascendentes en $\mathbb{Q}$, por lo tanto $\mathbb{R}$ es también una extensión trascendente de $\mathbb{Q}$.

Teorema 1.3.9. *Si F es extensión de un campo K y $u \in F$ es trascendente sobre K, entonces existe un isomorfismo de campos* [2] $K(u) \cong K(x)$ *que es la identidad en K.*

Demostración. Como u es trascendente en K se tiene que $f(u) \neq 0$ y $g(u) \neq 0$ para toda $f, g \in R[x]$ distintas de cero, por eso $\phi : K(x) \longrightarrow F$ dada por $f/g \mapsto f(u)/g(u) = f(u)g(u)^{-1}$ es un homomorfismo bien definido que es la identidad en K, donde además $\text{Im}\phi = K(u)$, lo que implica que $K(x) \cong K(u)$. ■

Ejemplo. Recordemos que $\mathbb{Q}(\pi) = \{\frac{f(\pi)}{g(\pi)} | f, g \in \mathbb{Q}[x], g(x) \neq 0\}$, y definamos $\phi : \mathbb{Q}(x) \longrightarrow \mathbb{R}$ dada por $\phi(\frac{f(x)}{g(x)}) = \frac{f(\pi)}{g(\pi)}$. Es fácil ver que ϕ es un homomorfismo bien definido, con núcleo $\text{Nuc}\phi = \{\frac{f(x)}{g(x)} | f, g \in \mathbb{Q}, g(x) \neq 0 \frac{f(\pi)}{g(\pi)} = 0\} = \{0\}$ la función constante 0, e imagen $\text{Im}\phi = \{\frac{f(\pi)}{g(\pi)} | g \neq 0 f, g \in \mathbb{Q}[x]\} = \mathbb{Q}(\pi)$, y por el primer teorema de isomorfismo para anillos [3]

$$\mathbb{Q}(\pi) \cong \mathbb{Q}(x)/\ \text{Nuc}\phi = \mathbb{Q}(x)/\{0\} \cong \mathbb{Q}(x)$$

Teorema 1.3.10. *Si F es extensión de un campo K, y $u \in F$ es algebraico sobre K, entonces:*

(i) $K(u) = K[u]$*;*

(ii) $K(u) \cong K[x]/(f)$*, donde $f \in K[x]$ es un polinomio mónico irreducible de grado $n \geq 1$ determinado de manera única por las condiciones de que $f(u) = 0$, donde $\forall g \in K[x]$, $g(u) = 0$ si y sólo si f divide a g, y (f)*

[2] Si F, F' son dos campos, un *homomorfismo* de anillos (campos) $\phi : F \longrightarrow F'$ es una función tal que para toda $a, b \in F$, $\phi(a + b) = \phi(a) + \phi(b)$ y $\phi(ab) = \phi(a)\phi(b)$. Si ϕ es biyectiva, entonces es un isomorfismo. Definiciones como núcleo e imagen se preservan en éste caso.

[3] análogo inmediato del Primer Teorema de Isomorfismo para grupos

(iii) $[K(u) : K] = n$;

(iv) $\{1, u, u^2, \ldots, u^{n-1}\}$ *es una base para el espacio vectorial* $K(u)$ *sobre* K, *y por eso cada elemento de* $K(u)$ *puede ser escrito de manera única como* $a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$ $(a_i \in K)$.

La demostración de éste teorema puede encontrarse en [5], y el polinomio f del teorema anterior se llama el *polinomio mónico mínimo irreducible de* u y su grado es $\delta f = [K(u) : K]$.

Ejemplo. Consideremos $\mathbb{Q} \leq \mathbb{R}$, y a $\sqrt{2} \in \mathbb{R}$ algebraico en $\mathbb{Q}$. Demostrar que $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.

$\subseteq$ Sea $y = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Es claro que si $f(x) = a + bx$, entonces $y = f(\sqrt{2}) = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

$\supseteq$ Si ahora tenemos $g(x) \in \mathbb{Q}[x]$, $g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, y entonces $g(\sqrt{2}) = a_0 + a_1\sqrt{2} + a_2(\sqrt{2})^2 + \cdots + a_n(\sqrt{2})^n$, donde $a_i \in \mathbb{Q}$ y además:

$$(\sqrt{2})^n = \begin{cases} 2^{\frac{n}{2}} & \text{si } n \text{ es par} \\ 2^{\frac{n}{2}}\sqrt{2} & \text{si } n \text{ es impar} \end{cases}$$

Así que podemos agrupar y obtener que $g(\sqrt{2}) = a + b\sqrt{2}$ para algúnos $a, b \in \mathbb{Q}$, es decir $g(\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$.

Tenemos que $x^2 - 2 \in \mathbb{Q}[x]$ es el polinomio mínimo irreducible en $\mathbb{Q}[x]$ asociado a $\sqrt{2}$, y una base para el espacio vectorial ${}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2})$ es $\{1, \sqrt{2}\}$, por eso $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Proposición 1.3.11. *Sean* E *y* F *extensiones de un campo* K, *y sean* $u \in E$, $v \in F$ *elementos algebraicos sobre* K. *Entonces,* u *y* v *son raíces del mismo polinomio irreducible* $f \in K[x]$ *si y solamente si existe un isomorfismo* ϕ *de campos* $K(u) \cong K(v)$ *tal que mande* u *en* v, *y fija a los elementos de* K.

Demostración. Si $K(u) \cong K(v)$, bajo $\phi(u) = v$ $\phi(k) = k$ para toda $k \in K$, sea $f \in K[x]$ el polinomio irreducible de u, es decir, $0 = f(u) = \sum_{i=0}^{n} k_iu^i$, entonces

$$0 = \phi(\sum_{i=0}^{n} k_iu^i) = \sum_i \phi(k_iu^i) = \sum_i \phi(k_i)\phi(v^i) = \sum_{i=0}^{n} k_iv^i = f(v).$$

■

Teorema 1.3.12. *Si K es un campo y $f \in K[x]$ un polinomio de grado n, entonces existe una extensión de campo simple $F = K(u)$ tal que:*

(i) u es raíz de f;

(ii) $[K(u) : K] \leq n$, donde la igualdad se cumple únicamente cuando f es irreducible en $K[x]$;

(iii) Si f es irreducible en $K[x]$, entonces $K(u)$ es única salvo isomorfismos que sean la identidad en K.

Ejemplo. Consideremos $f(x) = x^3 - 2x^2 + x - 2 \in \mathbb{Q}[x]$, que se puede factorizar en $\mathbb{Q}[x]$ como $(x^2 + 1)(x - 2)$, de donde sabemos que la única raíz de f en $\mathbb{Q}$ es 2. Así pues la extensión de la que habla el teorema es $\mathbb{Q}(i) =< \mathbb{Q} \cup \{i\} >$; así tenemos que $[\mathbb{Q} : \mathbb{Q}(i)] = 2 < 3 = \delta f$.

Si ahora consideramos al polinomio irreducible $g(x) = x^2+1 \in \mathbb{Q}[x]$, la extensión es la misma $\mathbb{Q}(i)$, sin embargo ahora tenemos que $[\mathbb{Q} : \mathbb{Q}(i)] = 2 = \delta g$.

El resultado anterior conduce a uno más general en el que para un campo K y un polinomio $f \in K[x]$ de grado n, existe un campo F con $K \leq F$ donde f tiene a todas sus n raíces, conocido como el *campo de descomposición* de f.

Teorema 1.3.13. *Si $f(x)$ es un polinomio de grado n en $F[x]$, entonces existe un campo en donde $f(x)$ tiene todas sus n raíces.*

La demostración se hace por inducción sobre $n = \delta f$, donde para $n = 1$ se tiene una función lineal cuya raíz se encuentra en K, y para el paso inductivo se usa el resultado anterior.

Teorema 1.3.14. *Si F es una extensión del campo K de dimensión finita, entonces F esta finitamente generada y es algebraica sobre F.*

Demostración. Si $[F : K] = n$ y $u \in F$, entonces el conjunto de $n+1$ elementos $\{1_K, u, u^2, \ldots, u^n\}$ debe ser linealmente dependiente. Entonces existen $a_i \in K$ no todas cero, tales que $a_0 + a_1u + \cdots + a_nu^n = 0$, lo que implica que u es algebraica sobre K. Dado que la elección de $u \in F$ fue arbitraria, entonces F es algebraica en K. Además, es fácil ver que si $\{v_1, v_2, \ldots, v_n\} \hookrightarrow_K F$, entonces $F = K(v_1, \ldots, v_n)$. ■

Teorema 1.3.15. *Si F es una extensión de un campo K, y $E \subseteq F$ es el conjunto de todos los elementos de F algebraicos sobre K, entonces E es un subcampo de F.*

Demostración. Si $u, v \in E$, entonces $K(u, v) \geq K$ es una extensión algebraica donde claramente $u - v$ y uv^{-1} $(v \neq 0)$ están en $K(u, v)$, por tanto están en E, haciendo a éste un campo. ■

Nos encaminamos finalmente a abordar el Teorema Fundamental de la Teoría de Galois, que relaciona los polinomios y las extensiones de un campo con un grupo de automorfismos, encontrando una biyección entre los campos intermedios de una extensión, y los subgrupos del grupo definido a continuación.

Definición 1.3.16. Sean E y F extensiones de un campo K. Una función $\phi : E \longrightarrow F$ tal que para todo $a, b \in E$, $\alpha \in K$ se tiene que:

- $\phi(ab) = \phi(a)\phi(b)$
- $\phi(a + b) = \phi(a) + \phi(b)$
- $\phi(\alpha a) = \alpha\phi(a)$

es un *K-homomorfismo*, análogamente, si un K-homomorfismo es también un automorfismo, entonces es un *K-automofismo*. Las definiciones como K-isomorfismo, etc. son definidas de manera obvia.

En la primera sección señalamos que los automorfismos bajo composición forman un grupo. En éste caso, el *Grupo de Galois* es el formado por todos los K-automorfismos de F, denotado $\mathrm{Aut}_K F$ o $Gal(F/K)$.

Teorema 1.3.17. *Sea F extensión de un campo K, y $f \in K[x]$. Si $\phi \in Gal(F/K)$, $u \in F$ es raíz de f si y sólo si $\phi(u) \in F$ es también una raíz de f.*

Demostración. Se sigue de considerar $f = \sum_{i=1}^{n} k_i x^i$, donde $f(u) = 0$ si y sólo si

$$0 = \phi(f(u)) = \phi(\sum k_i u^i) = \sum \phi(k_i)\phi(u^i) = \sum k_i \phi(u)^i = f(\phi(u)).$$

■

Véase también que si F es extensión de un campo K, y $\beta = \{v_1, \ldots, v_n\}$ es una base para el espacio vectorial ${}_KF$, entonces toda $\phi \in Gal(F/K)$ está completamente determinada por $\phi(v_i)$ $1 \leq i \leq n$, ya que $\phi \in Gal(F/K)$ es entonces una transformación lineal. En el caso de que $F = E(\alpha_1, \ldots, \alpha_n)$, entonces $\phi \in Gal(F/K)$ está determinada por $\phi(\alpha_i)$, con $1 \leq i \leq n$

Ejemplo. Consideremos el polinomio $p(x) = x^3 - 2 \in \mathbb{Q}$; se puede ver que $\sqrt[3]{2} = 2^{1/3}$ es una de sus raíces, sin embargo, si ω es una raíz cúbica primitiva de la unidad $\left(\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ tenemos que $2^{1/3}\omega$ y $2^{1/3}\omega^2$ son las otras dos raíces de $p(x)$. De lo anterior tenemos que el campo de descomposición de $p(x)$ es $F = \mathbb{Q}(2^{1/3}, \omega)$, y la base para el espacio vectorial $F_{\mathbb{Q}}$ es $\{1, 2^{1/3}, 2^{2/3}, \omega, 2^{1/3}\omega, 2^{1/3}\omega^2\}$, de donde un automorfismo en el grupo de Galois $\phi \in Gal(\mathbb{Q}(2^{1/3}/\mathbb{Q}), \omega)$ está determinado por $\phi(2^{1/3})$ y $\phi(\omega)$.

Tomando en cuenta que el polinomio mínimo irreducible de ω es x^2+x+1 (cuya segunda raíz es ω^2), el teorema anterior dice que las raíces de polinomios bajo un K-automorfismo de Galois, deben ser raíces del mismo polinomio, lo que nos deja seis posibles homomorfismos en $Gal(\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q})$:

1. $\phi_1(2^{1/3}) = 2^{1/3}$, $\phi_1(\omega) = \omega$ (la identidad)
2. $\phi_2(2^{1/3}) = 2^{1/3}\omega$, $\phi_2(\omega) = \omega$
3. $\phi_3(2^{1/3}) = 2^{1/3}\omega^2$, $\phi_3(\omega) = \omega$
4. $\phi_4(2^{1/3}) = 2^{1/3}$, $\phi_4(\omega) = \omega^2$
5. $\phi_5(2^{1/3}) = 2^{1/3}\omega$, $\phi_5(\omega) = \omega^2$
6. $\phi_6(2^{1/3}) = 2^{1/3}\omega^2$, $\phi_6(\omega) = \omega^2$

Si de estos homomorfismos notamos que $\phi_2 \circ \phi_4 = 2^{1/3}\omega \neq 2^{1/3}\omega^2 = \phi_4 \circ \phi_2$, se tiene que el grupo de Galois es un grupo no abeliano de orden 6, por tanto $Gal(\mathbb{Q}(2^{1/3}, \omega), \mathbb{Q}) \cong S_3$.

Para obtener la correspondencia entre los campos intermedios de una extensión y los subgrupos de su grupo de Galois, el primer paso es el siguiente:

Teorema 1.3.18. *Si F es extensión de un campo K, E es un campo intermedio y H es un subgrupo de $Gal(F/K)$, entonces:*

- $H' = \{v \in F | \phi(v) = v$ *para todo* $\phi \in H\}$ *es un campo intermedio.*

- $E' = \{\sigma \in Gal(F/K) | \phi(u) = u \text{ para toda } u \in E\} = Gal(F/E)$ *es un subgrupo de* $Gal(F/K)$.

El campo H' del teorema anterior es el *campo fijo* de H en F (que también es denotado F^H), es importante resaltar: $Gal(F/K) = E'$, $F' = Gal(F/F) = 1$ (el K-automofismo identidad).

En caso de que $H \leq Gal(F/K)$, H' será un subcampo intermedio, y cuando E sea un subcampo intermedio, $E' \leq Gal(F/K)$ será un subgrupo del grupo de Galois, la notacíon es la misma porque será por medio de éstas que encontremos la biyección buscada.

Ejemplo. Continuando con el ejemplo 1.3 , consideremos de nuevo $\mathbb{Q}$ y su extensíón $\mathbb{Q}(2^{1/3})$. Obtendremos el campo intermedio asociado a un subgrupo de $Gal(\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q})$. Por definición $Gal(\mathbb{Q}(2^{1/3}/\mathbb{Q}(2^{1/3})), \omega)$ es el conjunto de los $\mathbb{Q}(2^{1/3})$-automorfismos, es decir, automorfismos que dejan fijos los elementos de $\mathbb{Q}(2^{1/3})$, en particular a los de $\mathbb{Q}$, de observar que estos automorfismos también forman un grupo bajo composición podemos decir que $Gal(\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q}(2^{1/3}))$ es un subgrupo de $Gal(\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q})$. Por lo anterior podemos claramente ver que $Gal(\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q}(2^{1/3}))'$ es justamente el campo intermedio $\mathbb{Q}(2^{1/3})$.

Partiendo ahora del campo intermedio $K_1 = \mathbb{Q}(\omega)$, análogamente tenemos que $Gal(\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q}(\omega))$ es un subgrupo de $Gal(\mathbb{Q}(2^{1/3}, \omega), \mathbb{Q})$. Además K_1 es el campo de descomposción de $x^3 - 2 \in K_1[x]$, y por esto

$$|Gal(F/K_1)| = [F : K_1] = 3$$

Donde el único subgrupo de orden 3 en S_3 es A_3. Así tenemos que

$$Gal(\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q}(\omega)) \cong A_3$$

Definición 1.3.19. Si F es extensión de un campo K tal que el campo fijo de $Gal(F/K)$ es K mismo, entonces F es una *extensión de Galois.*

Ejemplo.

- La extensión del ejemplo anterior ($\mathbb{Q}(2^{1/3}, \omega)$), es de Galois.
- $\mathbb{Q}(2^{1/3})$ no es de Galois. Es fácil ver que $Gal(\mathbb{Q}(2^{1/3})/\mathbb{Q}) = \text{Id}$ el automorfismo identidad, de donde se tiene que el campo fijo del grupo de Galois es $\mathbb{Q}(2^{1/3}) \neq \mathbb{Q}$.

Enunciaremos el Teorema Fundamental de la Teoría de Galois, con el fin de saber con precisión el sentido que tienen los lemas que se expondrán antes de demostrarlo.

Teorema 1.3.20 (Teorema Fundamental de la Teoría de Galois)**.** *Si F es una extensión de Galois de dimensión finita de un campo K, entonces existe una correspondencia biyectiva entre el conjunto de todos los campos intermedios y el conjunto de todos los subgrupos del grupo de Galois $GalF/K$ dada por $E \mapsto E' = Gal(F/E)$ tal que:*

- *La dimensión relativa de dos campo intermedios es igual al indice relativo de los correspondientes subgrupos; en particular, $GalF/K$ tiene orden $[F : K]$*
- *F es Galois sobre todo campo intermedio E, pero E es Galois sobre K si y solamente si el subgrupo correspondiente $E' = Gal(F/E)$ es normal en $Gal(K/F)$; en cuyo caso G/E' es isomorfo al grupo de Galois $Gal(E/K)$ de E sobre K.*

$$\begin{array}{ccc} F & \longmapsto & 1 \\ \cup & & \vee \\ M & \longmapsto & M' \\ \cup & & \vee \\ L & \longmapsto & L' \\ \cup & & \vee \\ K & \longmapsto & G; \end{array} \qquad \begin{array}{ccc} F & \longmapsfrom & 1 \\ \cup & & \wedge \\ H' & \longmapsfrom & H \\ \cup & & \wedge \\ J' & \longmapsfrom & J \\ \cup & & \wedge \\ K & \longmapsfrom & G. \end{array}$$

Es posible que L'' contenga a L propiamente, y también que H'' contenga a H. Véase que G es Galois sobre K si y sólo si $K = K''$, análogamente F es Galois sobre un campo intermedio E si y sólo si $E = E''$. Un campo intermedio o un subgrupo de Galois X, se dice que es *cerrado* cuando $X = X''$, de ésta definición se sigue que F es extensión de Galois sobre un campo imtermedio si y solamente si $E = E''$.

Teorema 1.3.21. *Si F es extensión de un campo K, entonces existe una correspondencia biyectiva entre los campos intermedios de la extensión que son cerrados y los subgrupos cerrados del grupo de Galois, dada por $E \mapsto E' = Gal(F/E)$.*

Las demostraciones de los siguientes lemas pueden consultarse en [5], en el presente trabajo se omiten debido a que exceden la naturaleza del mismo.

Lema 1.3.22. *Sea F extensión del campo K, y L, M campos intermedios con $L \subset M$. Si $[M : L]$ es finita, entonces $[L' : M'] \leq [M : L]$. En particular si $[F : K]$ es finita, entonces $|Gal(F/K)| \leq [F : K]$*

Lema 1.3.23. *Sea F extensión de un campo K, y sean H, J subgrupos de $Gal(F/K)$ tal que $H < J$. Si $[J : H]$ es finito, entonces $[H' : J'] \leq [J : H]$.*

Lema 1.3.24. *Sea F extensión de un campo K, L y M campos intermedios tales que $L \subset M$, y H, J subgrupos del grupo de Galois $Gal(F/K)$ con $H < J$, entonces:*

(i) Si L es cerrado y $[M : L]$ es finito, entonces M es cerrado y

$$[L', M'] = [M : L];$$

(ii) Si H es cerrado y $[J : H]$ es finito, entonces J es cerrdo y

$$[H' : J'] = [J : H]$$

;

(iii) Si F es extensión de Galois de dimensión finita de K, entonces todos los campos intermedios y todos los subgrupos del grupo de Galois son cerrados, y además $Gal(F/K)$ tiene orden $[F : K]$.

Demostración. Véase que si en *(ii)* $H = 1$, se tiene que todo subgrupo finito de Gal(F/K) es cerrado. Para éste mismo inciso, considerando que $J \subset J''$ y $H = H''$, por los lemas 1.3.22 y 1.3.23 tenemos que

$$[J : H] \leq [J'' : H] = [J'' : H''] \leq [H' : J'] \leq [J : H];$$

lo que implica que $J = J''$ y que $[H' : J'] = [J : H]$. La demostración del inciso *(ii)* es análoga.

Para el inciso *(iii)*, como E es un campo intermedio y $[F : K]$ es finita, entonces $[E : K]$ es finita. Como F es Galois sobre K, K es cerrada y por el primer inciso E también es cerrada y $[K' : E'] = [E : K]$. En el caso de que $E = F$, entonces $|Gal(F/K)| = [Gal(F/K) : 1] = [K' : F'] = [F : K]$ es finita. Entonces todo subgrupo J de $Gal(F/K)$ es finito, y como 1 es cerrado, entonces J es cerrado también. ■

Si F es extensión del campo K, y E es un campo intermedio, E es *estable* (en relación a K y F) si todo K-automorfismo $\phi \in Gal(F/K)$ manda E en sí mismo. Si E es estable y $\phi^{-1} \in Gal(F/K)$ es el automorfismo inverso, entonces ϕ^{-1} también manda E en sí mismo, esto implica que $\phi|_E$ es de hecho un K-automorfismo de E (es decir $\phi|_E \in GAL(E/K)$) con inversa $\phi^{-1}|_E$. En el caso finitamente dimensional, E resultará estable si y sólo si E es Galois sobre K.

Lema 1.3.25. *Sea F una extensión de un campo K.*

(i) Si E es un campo intermedio estable de la extensión, entonces $E' = Gal(F/E)$ es un subgrupo normal del grupo de Galois $Gal(F/K)$;

(ii) Si H es un subgrupo normal de $Gal(F/K)$, entonces el campo fijo H' de H es un campo intermedio estable de la extensión.

Demostración. (i) Si $u \in E$ y $\phi \in Gal(K/F)$, $\phi(u) \in E$ por estabilidad, y entonces $\tau \circ \phi(u) = \phi(u)$ para toda $\tau \in E' = Gal(F/E)$. Entonces, para toda $\phi \in Gal(F/K)$, $\tau \in E'$ y $u \in E$, $\phi^{-1}\tau\phi(u) = \phi^{-1}\phi(u)$. Consecuentemente, $\phi^{-1}\tau\phi \in E'$, entonces $E' \lhd Gal(F/K)$

(ii) Si $\phi \in Gal(F/K)$ y $\tau \in H$, entonces $\phi^{-1}\tau\phi \in H$ por normalidad. Entonces para todo $u \in H'$, $\phi^{-1}\tau\phi(u) = u$, lo que implica que 4 $\tau\phi(u) = \phi(u)$ para toda $\tau \in H$. Entonces $\phi(u) \in H'$ para toda $u \in H'$, es decir, H' es estable.

■

Considerando la extensión del ejemplo anterior ($\mathbb{Q}(2^{1/3}, \omega)$), notemos que $Gal(\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q}(\omega))$ es estable, y $A_3 \lhd S_3$.

Lema 1.3.26. *Si F es extensión de Galois de un campo K, y E es un campo intermedio estable de la extensión, entonces E es Galois sobre K.*

Demostración. Si $u \in F \setminus K$ entonces existe un $\phi \in Gal(F/K)$ tal que $\phi(u) \neq u$ ya que F es Galois sobre K. Pero $\phi|_E \in Gal(E/K)$ por estabilidad. Entonces E es Galois sobre K. ■

Lema 1.3.27. *Si F es extensión de un campo K y E es un campo intermedio de la extensión tal que E es algebraico y Galois sobre K, entonces E es estable en relación a F y K.*

Si F es extensión de un campo K, y E es campo intermedio, un K-automorfismo $\tau \in Gal(E/K)$ es *extensible* a F si existe un $\phi \in Gal(F/K)$ tal que $\phi|_E = \tau$. Es fácil ver que los K-automorfismos extensibles forman un subgrupo de $Gal(E/K)$, además si E es estable, $E' = Gal(F/E)$ es un subgrupo normal de $Gal(F/K)$, y por tanto el grupo cociente está definido.

Lema 1.3.28. *Sea F una extensión de un campo K, y E un campo intermedio estable de la extensión. Entonces el grupo cociente $Gal(F/K)/Gal(F/E)$ es isomorfo al grupo de todos los K-automorfismos de E que son extensibles a F.*

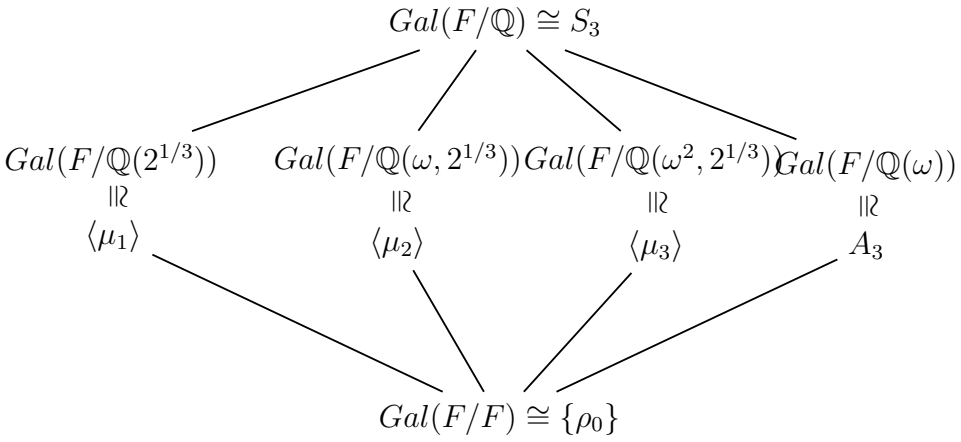
Demostración. Como E es estable, la regla de correspondencia $\phi \mapsto \phi|_E$ define un homomorfismo de grupos $Gal(F/K) \longrightarrow Gal(E/K)$ cuya imagen es claramente el subgrupo de todos los K-automorfismos de E que son extensibles a F. El resultado se sigue de aplicar el primer teorema de isomorfismo, observando que el núcleo de dicho homomorfismo es $Gal(F/E)$. ■

Demostración del Teorema Fundamental de la Teoría de Galois El teorema 1.3.21 muestra que existe una correspondencia biyectiva entre los campos intermedios de una extensión que son cerrados y los subgrupos cerrados del grupo de Galois; pero en este caso todos los campos intermedios y todos los subgrupos son cerrados por el tercer inciso del lema 1.3.24. Así el primer inciso del teorema se sigue inmediatamente del primer inciso del lema 1.3.24.

(ii) F es Galois sobre E ya que E es cerrado ($E = E''$). E es de dimensión finita sobre K (ya que F lo es), y entonces es algebraico sobre K. Así mismo, si E es Galois sobre K, entonces E es estable por el lema 1.3.27. Por el lema 1.3.25 *(i)* $E' = Gal(F/E)$ es normal en $Gal(F/K)$. Por otro lado si E' es normal en $Gal(F/K)$ entonces E'' es un campo intermedio estable (lema 1.3.25 *(ii)*). Pero $E = E''$ ya que todos los campos intermedios son cerrados, y por tanto Galois sobre K por el lema 1.3.26.

Supongamos que E es un campo intermedio que es Galois sobre K (así E' es normal en $Gal(F/K)$). Como E y E' son cerrados y $G' = K$ (F es Galois sobre K), el lema 1.3.24 implica que $|G/E'| = [G : E'] = [E'' : G'] = [E : K]$. Por el lema 1.3.28 $G/E' = Gal(F/K)/Gal(F/E)$ es isomorfo a un subgrupo (de orden $[E : K]$) de $Gal(E/K)$. Por la parte *(i)* del teorema muestra que $|Gal(E/K)| = [E : K]$ (ya que E es Galois sobre K). Lo que implica que $G/E' \cong Gal(E/K)$ ■

Ejemplo. Sea $F = \mathbb{Q}(2^{1/3}, \omega)$. La correspondencia entre los subgrupos del $Gal(F/\mathbb{Q}$ y los subcampos de $\mathbb{Q}(2^{1/3}, \omega)$ es como en el diagrama.



Capítulo 2

Resultados

Antes de empezar, indicaremos una generalización del concepto de espacio vectorial y algunos conceptos y resultados análogos.

Definición 2.0.29. Sea R un anillo, un *módulo izquierdo* (*módulo derecho*) denotado ${}_RM$ (M_R) es un grupo abeliano aditivo M con una función $\vdots R \times M \to M$ ($\vdots M \times R \to M$), tal que $(r, m) \mapsto rm$ ($(m, r) \mapsto mr$) tal que para cualesquiera $r, s \in R$ y $m, n \in M$ se cumple:

- $r(m + n) = rm + rn$ ($(m + n)r = mr + nr$).
- $(r + s)m = rm + sm$ ($m(r + s) = mr + ms$).
- $r(sm) = (rs)m$ ($(mr)s = m(rs)$).

Si R tiene elemento identidad 1_R y es tal que $1_R m = m$ para toda $m \in M$, entonces es llamado R-módulo *unitario*. Una definición y notación análoga, mutatis mutandis, se tiene para un bimodulo.

En el resto de este trabajo trabajaremos con R-módulos izquierdos

Ejemplo.

- Un espacio vectorial V sobre un campo F es un modulo izquierdo y derecho, por tanto es un bimodulo.
- Un grupo abeliano G es un $\mathbb{Z}$-módulo definiendo $\cdot : \mathbb{Z} \times G \longrightarrow G$ con $(n, g) \mapsto ng = \underbrace{g + g + \cdots + g}_{\text{n veces}}$ para $n > 0$ y $(-n)g = -(ng)$ para $n < 0$.

Al igual que en los espacios vectoriales, entre R-módulos existen funciones que preserven la estructura, naturalmente llamados *R-homomorfismos*. Así, si M y N son R-módulos izquierdos, una función $f :_R M \longrightarrow_R N$ es R-homomorfismo si

- Para toda $m_1, m_2 \in {}_R M$, $f(m_1 + m_2) = f(m_1) + f(m_2)$
- Para toda $m \in_R M$ y $r \in R$, $f(rm) = rf(m)$.

Del ejemplo anterior podemos ver que las transformaciones lineales entre dos espacios vectoriales $T : V \longrightarrow W$ sobre el mismo campo K son K-homomorfismos. De igual forma los homomorfismos entre grupos abelianos son todos $\mathbb{Z}$-homomorfismos.

Si N y M son R-módulos izquierdos, el conjunto de todos los R-homomorfismos de M en N es

$$Hom_R(M, N) = \{f : M \longrightarrow N | f \text{ es } R\text{-homomorfismo } \}$$

Si tenemos que $N = M$ entonces Los R-homomorfismos son llamados *endomorfismos* y el conjunto de todos los endomorfismos de un módulo M es denotado por $\text{End}_R(M)$.

Si R es un campo, entonces los R-homomorfismos resultan ser transformaciones R lineales (es decir abren sumas y sacan escalares en R). De esta manera y sabiendo que en álgebra lineal el conjunto de todas las transformaciones lineales de dos R espacios vectoriales M y N se denota por

$$\mathcal{L}(V, W)$$

entonces tenemos que

$$\mathcal{L}(V, W) = Hom(V, W).$$

Para hablar de la estructura del conjunto $\text{End}_K(V)$, definamos, para K un anillo conmutativo una *K-álgebra* como el anillo R tal que R es un K-módulo y los escalares $k \in K$ conmutan, es decir para todo $k \in K$, $r, s \in R$:

$$k(rs) = (kr)s = r(ks)$$

Ejemplo.

- Todo anillo R es un grupo abeliano aditivo, y por ello un $\mathbb{Z}$-módulo. Es fácil ver que R es también una $\mathbb{Z}$-álgebra ya que si $n \in \mathbb{Z}$ y $r, s \in R$, entonces

$$n(rs) = \begin{cases} n(rs) = \underbrace{rs + rs + \cdots + rs}_{\text{n veces}} \\ n(rs) = \underbrace{(-rs) + (-rs) + \cdots + (-rs)}_{\text{n veces}} \\ n(rs) = r\underbrace{(s + s + \cdots + s)}_{\text{n veces}} \end{cases}$$

y en cualquier caso $n(rs) = r(ns) = s(rn)$. Haciendo de R una $\mathbb{Z}$-álgebra.

- $\mathbb{C}[x]$ es un $\mathbb{R}$-módulo, y si consideramos dos polinomios $r = (r_0, r_1, \dots)$, $s = (s_0, s_1, \dots) \in \mathbb{C}[x]$ tenemos que el producto es

$$rs = (c_0, c_1, \dots) \text{ donde } c_k = \sum_{i+j=k} r_i s_j = \sum_{i=0}^{k} s_i t_{k-1}.$$

De donde es claro ver que para toda $n \in \mathbb{R}$, tenemos que

$$n(rs) = r(ns) = s(nr),$$

y entonces $\mathbb{C}[x]$ es una $\mathbb{R}$-álgebra. Análogamente se puede ver que $\mathbb{C}[x]$ también es una $\mathbb{C}$-álgebra.

Consideremos ahora un monoide G y un campo K. Un *carácter* de G en K es un homomorfismo $\chi : G \longrightarrow K^\times$ de G en $K^\times$ el grupo multiplicativo de K. Las funciones $f_i : G \longrightarrow K$ son *linealmente independientes* sobre K si siempre que $a_1 f_1 + \cdots + a_n f_n = 0$ con $a_i \in K$, se tiene que $a_i = 0$ para toda $i \in I$ un conjunto de índices.

Teorema 2.0.30 (Artin)**.** *Para G un monoide y K un campo, si $\chi_1, \dots, \chi_n$ son caracteres distintos de G en K, entonces son linealmente independientes sobre K.*

Demostración. Por inducción sobre el número de caracteres distintos de G en K.

Un carácter es linealmente independiente ya que como $\chi : G \longrightarrow K^\times$ es un homomorfismo de grupos y $0 \notin K$ entonces a cualquier $g \in G$ le sucede que $\chi(g) \neq 0$. Por tanto $\chi \neq 0$ y de esta manera es claro que si se tiene

un único caracter entonces es linealmente independiente. Consideremos la relación

$$a_1\chi_1 + \cdots + a_n\chi_n = 0$$

con $a_i \in K$ pero no toda $a_i = 0$. Tomando n mínima, tenemos que $n \geq 2$ y ninguna $a_i = 0$. Como $\chi_1 \neq \chi_2$, entonces existe $z \in G$ tal que $\chi_1(z) \neq \chi_2(z)$. Y para toda $x \in G$ tenemos que

$$a_1\chi_1(xz) + \cdots + a_n\chi_n(xz) = 0$$

y como χ_i es carácter, para toda i y para toda $x \in G$ tenemos que $a_i\chi_i(xz) = a_i\chi_i(z)\chi(x)$ es decir,

$$a_1\chi_1(z)\chi_1 + \cdots + a_n\chi_n(z)\chi_n = 0$$

Dividiendo por $\chi_1(z)$ obtenemos

$$a_1\chi_1 + \left(\frac{a_2\chi_2(z)}{\chi_1(z)}\right)\chi_2 + \cdots = 0.$$

Restando a la primera ecuación, el termino $a_1\chi_1$ se cancela, y obtenemos que

$$\left(a_2\frac{\chi_2(z)}{\chi_1(z)} - a_2\right)\chi_2 + \cdots = 0.$$

Donde el primer coeficiente es distinto de 0. Obtuvimos una relación de longitud menor a n, lo cual es una contradicción. Por lo tanto $\chi_1, \ldots, \chi_n$ son linealmente independientes. ■

Sea K un campo y L una extensión de Galois de grado n; sea G el grupo de Galois de L sobre K y consideremos a L como un K-espacio vectorial de dimensión n. Entonces tenemos:

Observación 2.0.31. $\mathrm{End}_K L$ es una K-álgebra.

Demostración. Defínase puntualmente

$$+ : \mathrm{End}_K L \times End_K L \longrightarrow End_K L$$

como

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

para cualquier $f, g \in End_K L$ y $x \in L$. También defínase

$$\cdot : K \times \mathrm{End}_K L \longrightarrow \mathrm{End}_K L$$

como

$$(k \cdot g)(x) = k \cdot g(x)$$

para cualesquiera $k \in K$ y $g \in \mathrm{End}_K L$. Definidas de esta manera las operaciones y debido a que para cualquesquiera $f, g \in \mathrm{End}_K L$ y $k \in K$ se tiene

$$(k(f \cdot g))(x) = k(f(x) \cdot g(x)) = (k \cdot f(x)) \cdot g(x) = f(x) \cdot (k \cdot g(x))$$

para cualquier $x \in L$ y teniendo en cuenta que $f(x), g(x) \in L$ y L es un campo. Por tanto $\mathrm{End}_K L$ es una K-álgebra ■

Observación 2.0.32. $\mathrm{End}_K L$ es un espacio vectorial de dimensión n^2 sobre K.

Demostración. Por la observación 2.0.31 sabemos que $\mathrm{End}_K L$ es un K-módulo con K campo, por tanto es un espacio vectorial sobre K. Basta entonces ver que su dimensión es n^2.

Por la observación 1.2.14 $End_K L \cong M_{n\times n}(K)$ y por tanto como $\dim(M_{n\times n}(K)) = n^2$ entonces $dim(End_K L) = n^2$ ■

El primer resultado demostrado por Gow y Quilan [4] usa el lema de Artin 2.0.30 para demostrar que $End_K L$ es igual al conjunto de las combinaciones L-lineales de elementos en G.

Considerese $G = Gal(L/K) = Aut_K L = \{\phi_1, \ldots, \phi_n\}$ donde $\phi_1 = Id$ y $\lambda_1, \ldots, \lambda_n$ son elementos de L. Se define la función $\tau : L \longrightarrow L$ dada por

$$\tau(x) = \lambda_1\phi_1(x) + \cdots + \lambda_n\phi_n(x)$$

para cualquier $x \in L$ y se escribirá

$$\tau = \lambda_1\phi_1 + \cdots + \lambda_n\phi_n$$

Observación 2.0.33. $\tau = \lambda_1\phi_1 + \cdots + \lambda_n\phi_n$ es elemento de $End_K L$

Demostración. Sabemos que para cualesquiera $\phi_i \in Aut_K L = Gal(L/K)$ y $\lambda_i \in L^\times$ se tiene que

$$\lambda_i\phi_i : L \longrightarrow L$$

y además debido a que L es un campo se tiene que para cualesquiera $k \in K$ y $x \in L$

$$(\lambda_i\phi_i)(kx) = \lambda_i \cdot (\phi_i(kx)) = \lambda_i \cdot (k \cdot \phi_i(x)) =$$
$$= (\lambda_i \cdot k) \cdot \phi_i(x) = k \cdot (\lambda_i \cdot \phi_i(x))$$

Por tanto $\lambda_1\phi_1 + \cdots + \lambda_n\phi_n \in End_K L$ ■

Teorema 2.0.34. *Todo elemento en $End_K(L)$ puede expresarse de la forma*

$$\lambda_1\phi_1 + \cdots + \lambda_n\phi_n$$

para elementos únicos $\lambda_1, \ldots, \lambda_n$ en L.

Demostración. En la observación 2.0.32 se demostró que $End_K(L)$ es un espacio vectorial de dimensión n^2. Veamos ahora que si se denota por E al conjunto de todos los endomorfismos de L que tienen la forma requerida en el teorema, entonces $E = End_K(L)$.

E es un subespacio vectorial de $End_K(L)$ ya que:

- Claramente $E \subseteq End_K(L)$
- τ_0 (la función cero) trivialmente está en E con

  $$\tau_0 = 0\phi_1 + \cdots + 0\phi_n$$

- Si τ_i, τ_j son elementos de E y debido a que la suma de endomorfismos se hace puntual, entonces $\tau_i + \tau_j \in E$
- Si $\alpha \in K$ y $\tau \in E$ entonces

  $$\alpha\tau = \alpha(\lambda_1\phi_1 + \cdots + \lambda_n\phi_n) = \alpha\lambda_1\phi_1 + \cdots + \alpha\lambda_n\phi_n$$

  Como $\alpha\lambda_j \in L$ (por ser K subcampo de L) entonces

  $$\alpha\tau \in E$$

Para concluir la demostración del teorema basta demostrar que E tiene la misma dimensión que $End_K L$. Para ello se demostará que hay un conjunto en E linealmente independiente con n^2 elementos.

Considérense $\{\mu_1, \ldots, \mu_n\}$ una K-base de L y los n^2 elementos $\mu_i\phi_j$ de E con $1 \leq i, j \leq n$. Supóngase que se tiene la combinación lineal

$$\sum_{1\leq i,j\leq n} \alpha_{ij}\mu_i\phi_j = 0 \text{ con } \alpha_{ij} \in K \tag{1}$$

Desarrollemos las sumas:

$$\begin{array}{rc} \sum_{1\leq j\leq n} & (\alpha_{1j}\mu_1\phi_j + \alpha_{2j}\mu_2\phi_j + \cdots + \alpha_{nj}\mu_n\phi_j) = \\ & +\alpha_{11}\mu_1\phi_1 + \alpha_{21}\mu_2\phi_1 + \cdots + \alpha_{n1}\mu_n\phi_1 \\ & +\alpha_{12}\mu_1\phi_2 + \alpha_{22}\mu_2\phi_2 + \cdots + \alpha_{n2}\mu_n\phi_2 \\ & \vdots \\ & +\alpha_{1n}\mu_1\phi_n + \alpha_{2n}\mu_2\phi_n + \cdots + \alpha_{nn}\mu_n\phi_n \end{array}$$

Consideremos ahora $\lambda_j = \sum_{1\leq i\leq n} \alpha_{ij}\mu_i$, es decir

$$\begin{array}{c} \lambda_1 = \alpha_{11}\mu_1 + \alpha_{21}\mu_2 + \cdots + \alpha_{n1}\mu_n \\ \lambda_2 = \alpha_{12}\mu_1 + \alpha_{22}\mu_2 + \cdots + \alpha_{n2}\mu_n \\ \vdots \\ \lambda_n = \alpha_{1n}\mu_1 + \alpha_{2n}\mu_2 + \cdots + \alpha_{nn}\mu_n \end{array}$$

De esta manera se obtiene:

$$\sum_{1\leq j\leq n} (\alpha_{1j}\mu_1\phi_j + \alpha_{2j}\mu_2\phi_j + \cdots + \alpha_{nj}\mu_n\phi_j) = \lambda_1\phi_1 + \lambda_2\phi_2 + \cdots + \lambda_n\phi_n$$

Por el lema de Artin 2.0.30 $\lambda_i = 0$ para toda $1 \leq i \leq n$, es decir:

$$\begin{array}{c} 0 = \alpha_{11}\mu_1 + \alpha_{21}\mu_2 + \cdots + \alpha_{n1}\mu_n \\ 0 = \alpha_{12}\mu_1 + \alpha_{22}\mu_2 + \cdots + \alpha_{n2}\mu_n \\ \vdots \\ 0 = \alpha_{1n}\mu_1 + \alpha_{2n}\mu_2 + \cdots + \alpha_{nn}\mu_n \end{array}$$

Debido a que $\{\mu_1, \ldots, \mu_n\}$ es una K-base de L y que $\alpha_{ij} \in K$ se obtiene $\alpha_{ij} = 0$ para cualesquiera $i, j \in \{1, \ldots, n\}$.

Entonces $\{\mu_i\phi_j\}$ con $1 \leq i, j \leq n$ es linealmente independiente con n^2 elementos, tal como se quería demostrar ■

Ejemplo. Consideremos a $\mathbb{C}$ la extensión de Galois de $\mathbb{R}$.

Sabemos que $G = Gal(\mathbb{C}/\mathbb{R}) = \{\sigma_1 = Id, \sigma_2 = f\}$ donde $f = \overline{()}$, es decir f es la conjugación compleja.

Para poder determinar completamente cualquier endomorfismo de ${}_{\mathbb{R}}\mathbb{C}$ hay que recordar que según el Teorema 2.0.34 si se considera la $\mathbb{R}$-base canónica de $\mathbb{C}$, $\beta = \{\mu_1 = 1, \mu_2 = i\}$, entonces el conjunto:

$$\gamma = \{\mu_1\sigma_1, \mu_1\sigma_2, \mu_2\sigma_1, \mu_2\sigma_2\} = \{Id, f, i \cdot Id, i \cdot f\}$$

Es una base para $End_{\mathbb{R}}\mathbb{C}$ y según la observación 1.2.14 $End_{\mathbb{R}}\mathbb{C} \cong M_{2\times 2}(\mathbb{R})$ por lo que, si $g \in End_{\mathbb{R}}\mathbb{C}$ entonces:

$$[g]_\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ con } a, b, c, d \in \mathbb{R}.$$

Consideremos ahora la representación matricial de la base γ respecto a la base β:

$$[\gamma]_\beta = \{[Id]_\beta, [f]_\beta, [i \cdot Id]_\beta, [i \cdot f]_\beta\}$$

Calculemos cuidadosamente cada elemento:

- $[\mu_1\sigma_1]_\beta = [Id]_\beta = \begin{pmatrix} [Id(1)]_\beta & [Id(i)]_\beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- $[\mu_1\sigma_2]_\beta = [f]_\beta = \begin{pmatrix} [f(1)]_\beta & [f(i)]_\beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- $[\mu_2\sigma_1]_\beta = [i \cdot Id]_\beta = \begin{pmatrix} [i \cdot Id(1)]_\beta & [i \cdot Id(i)]_\beta \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
- $[\mu_2\sigma_2]_\beta = [i \cdot f]_\beta = \begin{pmatrix} [i \cdot f(1)]_\beta & [i \cdot f(i)]_\beta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

De ésta manera, se ha asociado la base γ de $End_{\mathbb{R}}\mathbb{C}$ a la base:

$$\delta = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Según el Teorema 2.0.34 para encontrar los escalares complejos $\lambda_1, \lambda_2, \lambda_3$ y λ_4 tales que:

$$g = \lambda_1 \cdot Id + \lambda_2 \cdot f$$

Hay que encontrar primero los escalares $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in \mathbb{R}$ tales que:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \alpha_{11}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \alpha_{12}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \alpha_{21}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + \alpha_{22}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Realizando los cálculos obtenemos:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha_{11} + \alpha_{12} & -\alpha_{21} + \alpha_{22} \\ \alpha_{21} + \alpha_{22} & \alpha_{11} - \alpha_{12} \end{pmatrix}$$

Tenemos pues un sistema de cuatro ecuaciones con cuatro incógnitas que hay que resolver en términos de a, b, c y d, haciendo aritmética obtenemos:

$$\begin{aligned} \alpha_{11} &= \frac{a+d}{2} \\ \alpha_{12} &= \frac{a-d}{2} \\ \alpha_{21} &= \frac{c-b}{2} \\ \alpha_{22} &= \frac{b+c}{2} \end{aligned}$$

De esto y debido a que $\lambda_j = \sum_{i=1}^{2} \alpha_{ij}\mu_i$ para $1 \leq j \leq 2$ obtenemos:

$$\begin{aligned} \lambda_1 &= \alpha_{11}\mu_1 + \alpha_{21}\mu_2 = \left(\frac{a+d}{2}\right) \cdot 1 + \left(\frac{c-b}{2}\right) \cdot i \\ \lambda_2 &= \alpha_{12}\mu_1 + \alpha_{22}\mu_2 = \left(\frac{a-d}{2}\right) \cdot 1 + \left(\frac{b+c}{2}\right) \cdot i \end{aligned}$$

Por tanto, dada una $\mathbb{R}$-base ordenada de $\mathbb{C}$ se obtienen los escalares deseados. En el caso de la base canónica los escalares para la ecuación (1) serán:

$$\lambda_1 = \frac{(a+d) + i(c-b)}{2}$$

$$\lambda_2 = \frac{(a-d) + i(b+c)}{2}.$$

Sea U un K-subespacio vectorial de L, y consideremos al subconjunto de todos los elementos τ de $\mathrm{End}_K L$ que satisfacen $\tau(U) = 0$

Observación 2.0.35. Sea $A = \{\tau \in \mathrm{End}_K(L) | \tau(U) = 0\}$ entonces:

i) $A \leq \mathrm{End}_K L$

ii) $\dim A = n(n - \dim_K U)$ donde $n = \dim_K L$.

Demostración. i) • Claramente $\tau_0 \in A$

- Si $\tau_1, \tau_2 \in A$, $(\tau_1 + \tau_2)[U] = \{(\tau_1 + \tau_2)(x) | x \in U\} = \{\tau_1(x) + \tau_2(x) | x \in U\} = \{0\}$; por otro lado $\tau_1[x] + \tau_2[x] = \{f(x) + g(x) | x \in U\} = \{0\}$, entonces $\tau_1 + \tau_2 \in A$.
- Si $\alpha \in K$ y $\tau \in A$, entonces $(\alpha\tau)[U] = \{(\alpha\tau)(x) | x \in U\} = \{0\}$, es decir, $\alpha\tau \in A$.

$$\therefore A \leq \mathrm{End}_L(K).$$

ii) Para obtener la dimensión de A, empecemos por notar que $\dim A \leq \dim(\mathrm{End}_K L) = n^2$. Consideremos una base para ${}_K U \leq_K L$, $\beta_1 = \{\mu_1, \ldots, \mu_k\} \hookrightarrow_K U$, y extendamos β_1 a una base $\beta \hookrightarrow \mathrm{End}_K L$ dada por $\beta = \{\mu_1, \ldots, \mu_k\} \cup \{\mu_{k+1}, \ldots, \mu_n\}$.

Sea $\tau \in A$ una función que anule al subespacio vectorial U, al obtener la matriz de representación respecto a β obtenemos que

$$[\tau]_\beta = ([\tau(\mu_1)]_\beta, \ldots, [\tau(\mu_k)]_\beta [\tau(\mu_k + 1)]_\beta [\tau(\mu_n)]_\beta)$$

Sin embargo

$$[\tau(\mu_1)]_\beta = \cdots = [\tau(\mu_k)]_\beta = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

entonces

$$[T]_\beta = \begin{pmatrix} 0 & 0 & \cdots & 0 & \alpha_{1(k+1)} & \cdots & \alpha_{1n} \\ 0 & 0 & \cdots & 0 & \alpha_{2(k+1)} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \alpha_{(n-1)(k+1)} & \cdots & \alpha_{(n-1)n} \\ 0 & 0 & \cdots & 0 & \alpha_{n(k+1)} & \cdots & \alpha_{nn} \end{pmatrix}$$

con esto es claro que $\dim A \leq n(n - k)$, con $k = \dim_K U$.

Como $\mathrm{End}_K L \cong M_{n\times n}(K)$ y $A \leq \mathrm{End}_K L$, entonces $A \cong W \leq M_{n\times n}(K)$.

Podemos construir una base para W con $n(n-1)$ matrices que tengan cero en todas sus entradas, salvo en una $\alpha_i j$ con $1 \leq i \leq n$, $k+1 \leq j \leq n$. Entonces $\dim W = n(n-k)$.

■

Observación 2.0.36. Si $\tau \in A$ entonces $\mathrm{ran}\tau \leq \dim A = |\beta_1| = n - \dim_K U$.

Demostración. Claramente $[\tau]_\beta$ es la matriz antes descrita, y τ tiene a lo más $n-k$ columnas linealmente independientes, de donde se sigue el resultado. ■

Lema 2.0.37. *Si H es un K-hiperplano en L, entonces cualquier hiperplano en L tiene la forma $a^{-1}H$ para algún elemento no cero $a \in L^*$.*

Demostración. Recordemos que L^* es el espacio dual de L compuesto por las funciones que van de ${}_K L$ en su campo K, mostraremos que todo K-hiperplano es el núcleo de alguna función en L^* distinta de la función cero.

Consideremos el siguiente diagrama:

$$\begin{array}{ccccc} L & \xrightarrow{\tau} & L & \xrightarrow{Tr} & K \\ {\scriptstyle i}\uparrow & & & & \\ H & & & & \end{array}$$

Donde:

- L es un espacio vectorial sobre el campo K de dimensión n con base $\{v_1, \ldots, v_n\}$, y H es K-hiperplano de dimensión $\dim H = \dim K - 1 = n-1$ con base $\beta' = \{v_1, \ldots, v_{n-1}\} \hookrightarrow H$;
- $i : H \longrightarrow L$ es la inclusión dada para toda $x \in H$ como $f(x) = x \in J$;
- Considerando la base ordenada $\beta = \beta' \cup \{v_n\} \hookrightarrow L$ tenemos que toda $x \in L$ se puede expresar como combinación lineal de elementos de β y escalares $\lambda \in K$, es decir $x = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Sea $\tau : L \longrightarrow L$ dada para toda $x \in L$ por $\tau(x) = \lambda_n v_n$; así podemos ver a τ como una proyección. Además τ es una de las funciones que aniquila a H, es decir, $\tau \in A = \{f \in \mathrm{End}_K L | f(H) = 0\}$;

- Finalmente $\mathrm{Tr} : L \longrightarrow K$ dada por $x = \lambda_1 v_1 + \cdots + \lambda_n v_n \mapsto \sum_{i=1}^{n} \lambda_i$, conocida como la *función trasa*.

Afirmamos que $g' = \mathrm{Tr} \circ \tau \circ i : H \longrightarrow K$ es una función con $\mathrm{Nuc}g' = H$. Sea $h \in H$, entonces $i(h) = h \in L$, donde $h = \lambda_1 v_1 + \cdots + \lambda_{n-1} v_{n-1} + 0v_n$, entonces $\tau(h) = 0v_n$, y por último $\mathrm{Tr}(0_L) = 0_K$. De esto se sigue que $g = \tau \circ \mathrm{Tr} : L \longrightarrow K$ es una función $g \in L^*$ con $g(v_n) \neq 0$ tal que $\mathrm{Nuc}(g) = H$.

Para $0 \neq a \in L$ definimos $g^a \in L^*$ con $g^a(x) = g(ax)$ para toda $x \in L$. Vamos a demostrar que

$$\mathrm{Nuc}(g^a) = a^{-1}H = a^{-1}\mathrm{Nuc}(g)$$

Véase que $\mathrm{Nuc}(g^a) = \{x \in L | g^a(x) = 0\}$, entonces $x \in \mathrm{Nuc}(g^a)$ si y solamente si $g^a(x) = 0$, es decir $g(ax) = 0$, que ocurre cuando $ax \in \mathrm{Nuc}(g)$, y como $\mathrm{Nuc}g = H$, si y sólo si $ax \in H$, esto es que exista $h \in H$ tal que $ax = h$ con $a \neq 0$ es decir $x = a^{-1}h$ con $h \in H$ que ocurre si y solamente si

$$\mathrm{Nuc}g^a = a^{-1}H$$

Ahora veamos que $\Psi : L \longrightarrow L^*$ dada por $\Psi(a) = g^a$ para toda $a \in L$ es un homomorfismo. Para cualquier $a, b \in L$, $\alpha \in K$, tenemos que $\Psi(a + \alpha b) = g^{a+\alpha b} = g((a + \alpha b)(x))$, donde $g \in L^*$, es decir $g :_K L \longrightarrow K$ y es lineal, entonces $g((a + \alpha b)(x)) = g(ax) + \alpha g(bx) = \Psi(a) + \alpha\Psi(b)$. Además, véase que $\mathrm{Nuc}\Psi = \{a \in L | \Psi(a) = 0_{L^*}\}$; es decir $a \in \mathrm{Nuc}\Psi$ si y sólo si $\Psi(a) = g^a = 0_{L^*}$, es decir, $\mathrm{Nuc}\Psi = \{0_{L^*}\}$, y entonces Ψ es inyectiva. Por otro lado, tenemos que $\dim_K L = n$, pero por álgebra lineal tenemos que $\dim L^* = \dim L \cdot \dim K = \dim L \cdot 1 = n$. De lo anterior se sigue que Ψ es un isomorfismo.

Dado que todo K-hiperplano es el núcleo de un homomorfismo no cero en L^*, entonces todo K-hiperplano tiene la forma $a^{-1}H$. ■

Ejemplo. Continuando con ${}_{\mathbb{R}}\mathbb{C}$, un $\mathbb{R}$-hiperplano es un subespacio de ${}_{\mathbb{R}}\mathbb{C}$ de dimensión 1, que son las rectas en ${}_{\mathbb{R}}\mathbb{C}$ que pasan por el origen.

De todas estos subespacios, consideremos a $U = \{a + bi \in_{\mathbb{R}} \mathbb{C} | a = 0\}$, el eje imaginario en ${}_{\mathbb{R}}\mathbb{C}$, para obtener el conjunto de todos las funciones en $\mathrm{End}_K L$ que aniquilan a U, empecemos por señalar que la función T_0 es una de ellas, y también está la proyección sobre el eje real, es decir $T(a+ib) = a$, sin embargo es fácil ver que $A = \{T \in \mathrm{End}_K L | T(a + ib) = \alpha a + \delta ai\}$.

Para mostrar que cualquier otro hiperplano se puede expresar en términos de U, consideremos el hiperplano $H = \{a+ib | a = bi\}$, y veamos que $H = zU$

para algúna $z \in \mathbb{C}$. Considerando $1+i \in H$ buscamos $x+iy \in \mathbb{C}$ tal que $1+i=(x+iy)(0+i)=-y+ix$, de donde tenemos que $-y=1$, $x=1$, mostraremos que $H=(1-i)U$

- Si $a \in (1-i)U$ entonces existe $u \in U$ tal que $a=(1-i)u$, y como $u \in U=\{x+iy|x=0\}$ entonces $a=(a-i)(iy)=y+iy$ que es un elemento de H.
- Si $b \in H$ entonces $b=y+iy$ con $y \in \mathbb{R}$, y es claro que $y+iy=(1-i)(iy)$ de donde $b \in (1-i)U$.

Un caso especial de un K-hiperplano en L, conocido como el *hiperplano de traza cero* H_0, que es el núcleo de la función traza $\mathrm{Tr}=\mathrm{Tr}_K^L \in L^*$, definida por

$$\mathrm{Tr}(x)=\sum_{i=1}^{n}\phi_i(x)$$

H_0 es un subespacio vectorial de L:

- $0 \in \mathrm{Nuc(Tr)}$ ya que $\sum_i \phi_i(0)=0_K$ por ser homomorfismos;
- si $x,y \in \mathrm{Nuc(Tr)}$ se tiene que $\sum_i \phi_i(x+y)=\sum \phi_i(x)+\phi_i(y)$ por ser homomorfismos, y además $\sum \phi_i(x)=\sum \phi_i(y)=0_K$, de donde $x+y \in \mathrm{Nuc(Tr)}$;
- para $\alpha \in k$ y $x \in L$ tenemos que $\mathrm{Tr}(\alpha x)=\sum_i \phi_i(\alpha x)$, donde ϕ_i son endomorfismos K-lineales, entonces $\mathrm{Tr}(\alpha x)=\alpha \mathrm{Tr}(x)$.

De esto se concluye que NucTr es un subespacio de L. Para demostrar que H_0 es efectivamente un hiperplano, observemos que Tr: $L \longrightarrow K$, es decir Tr$\in L^*$, y por el teorema de la dimensión de álgebra lineal tenemos que dim$L$ =dim(Im(Tr))+dim(Nuc(Tr)), por eso $n=1+$dim(Nuc(Tr)), de donde dim(Nuc(Tr))$= n-1$.

Si consideramos a

$$\pi=\phi_1+\cdots+\phi_n$$

claramente $\pi \in \mathrm{End}_K L$ por ser combinación lineal de elementos en $\phi \in \mathrm{End}_K L$, y por lo anterior $H_0=\mathrm{Nuc}\pi$.

Ejemplo. En nuestro ejemplo, tenemos que $\mathrm{Tr}(x+iy)=f_1(x+iy)+f_2(x+iy)=x+iy+x-iy=2x$ con $x \in \mathbb{R}$ de donde tenemos que Nuc(Tr$(x+iy)$)=$\{x+iy|x=0_{\mathbb{R}}\}$, es decir, $U=H_0$.

Por el lema anterior, tenemos que si H es un hiperplano, entonces $H = a^{-1}H_0$ para alguna $a \in L$, de donde se sigue

Lema 2.0.38. *Si H es un K-hiperplano $a^{-1}H_0$, entonces el elemento $\pi_a \in End_K L$ definido por $\pi_a = \phi_i(a)\phi_1 + \cdots + \phi_n(a)\phi_n$ aniquila a H, es decir $\pi_a[H] = 0$.*

Demostración. Para mostrar $\pi_a \in \mathrm{End}_K L$, recordemos que $\phi_i \in Gal(L/K) = \mathrm{Aut}_K L \leq \mathrm{End}_K L$, entonces $\phi(a) \in L$ para toda $1 \leq i \leq n$. Consideremos dos elementos $x, y \in L$ tales que $x = y$, entonces

$$\pi_a(x) = \phi_1(a)\phi(x) + \cdots + \phi_n(a)\phi_n(y)$$

y por otro lado

$$\pi_a(y) = \phi_1(a)\phi(y) + \cdots + \phi_n(a)\phi_n(y)$$

sin embargo ϕ_i es una función biyectiva, entonces $\phi_i(x) = \phi_i(y)$ para toda $1 \leq i \leq n$, así que $\pi_a(x) = \pi_a(y)$, y por eso π_a es una función bien definida.

Consideremos ahora $\alpha \in K$ y $x, y \in L$, y mostremos que π_a es una función lineal, tenemos que

$$\pi_a(\alpha x + y) = \phi_1(a)\phi_1(\alpha x + y) + \cdots + \phi_n(a)\phi_n(\alpha x + y)$$

donde ϕ_i es una función K-lineal para toda $1 \leq i \leq n$, entonces

$$\begin{aligned}
\pi_a(\alpha x + y) &= \phi_1(a)[\alpha\phi_1(x) + \phi_1(y)] + \cdots + \phi_n(a)[\alpha\phi_n(x) + \phi_n(y)] \\
&= \phi_1(a)\alpha\phi_1(x) + \cdots + \phi_n(a)\phi_n(x) + \\
&\quad + \phi_1(a)\alpha\phi_1(y) + \cdots + \phi_n(a)\phi_n(y) \\
&= \alpha(\phi_1(a)\phi_1(x) + \cdots + \phi_n(a)\phi_n(x)) + \\
&\quad + \phi_1(a)\phi_1(y) + \cdots + \phi_n(a)\phi_1(y) \\
&= \alpha\pi_a(x) + \pi_a(y).
\end{aligned}$$

entonces

$$\pi_a \in \mathrm{End}_K L$$

Para demostrar que $\pi_a[H] = 0_L$, tenemos que

$$\pi_a[H] = \pi_a[a^{-1}H_0] = \phi_1(a)\phi_1[a^{-1}H_0] + \cdots + \phi_n(a)\phi_n[a^{-1}H_0]$$

Es decir, con $h \in H$ arbitraria, tenemos que

$$\pi_a(h) = \phi_1(a)\phi_1(a^{-1}h_0) + \cdots + \phi_n(a)\phi_n(a^{-1}h_0)$$

pero ϕ_i es un automorfismo, entonces

$$\begin{aligned}\pi_a(h) =&\phi_1(a)\phi_1(a^{-1})\phi_1(h_0) + \cdots + \phi_n(a)\phi_n(a^{-1})\phi_n(h_0)\\ =&\phi_1(a)\phi_1(a)^{-1}\phi_1(h_0) + \cdots + \phi_n(a)\phi_n(a)^{-1}\phi_n(h_0)\\ =&\phi_1(h_0) + \cdots + \phi_n(h_0)\\ =&\mathrm{Tr}(h_0)\end{aligned}$$

así tenemos que

$$\pi_a[H] = \mathrm{Tr}[H_0] = \{0_K\}.\text{Entonces } \pi_a \text{ anula a } H.$$

■

Dado que π_a es generado por una combinación lineal de $\{\phi_1, \ldots, \phi_n\}$, y que un endomorfismo que aniquile a H es múltiplo de π_a, tenemos que estos forman un espacio vectorial de dimensión n.

Teorema 2.0.39. *Los elementos de rango* 1 *en* $End_K L$ *son aquellos de la forma*

$$\lambda\pi_a = \lambda\phi_1(a)\phi_1 + \cdots + \lambda\phi_n(a)\phi_n$$

donde $\lambda, a \in L$.

Demostración. Sean H el K-hiperplano $a^{-1}H_0$ para alguna $a \in L$, $\beta_0 = \{v_1, \ldots, v_{n-1}\} \hookrightarrow H_0$ y $\beta = \{v_1, \ldots, v_n\} \hookrightarrow L$ son bases para H_0 y L respectivamente.

Tenemos que la imagen $\mathrm{Im}\lambda\pi_a = \langle\lambda\pi_a(v_i)\rangle$ con $1 \leq i \leq n$ pero $\lambda\pi_a(v_i) = 0_K$ para toda $1 \leq i \leq n-1$, entonces $\mathrm{Im}\lambda\pi_a = \langle\{0, \pi_a(v_n)\}\rangle$; de aquí tenemos dos casos:

$$\pi_a(v_n)\begin{cases} = 0 & \Longrightarrow \mathrm{Im}\lambda\pi_a = \{0\} \Longrightarrow \mathrm{ran}(\lambda\pi_a) = 0\\ \neq 0 & \Longrightarrow \mathrm{Im}\lambda\pi_a = \langle\pi_a(v_n)\rangle \Longrightarrow \mathrm{ran}(\lambda\pi_a) = 1\end{cases}$$

Pero en el primer caso tenemos que $\pi_a = T_0$ la transformación que manda todo a 0_K así que todos los endormorfismos de rango 1 son de la forma $\lambda\pi_a$.
■

De lo anterior podemos afirmar que el producto de dos endomorfismos $\lambda\pi_a$ y $\mu\pi_b$ de rango 1 es de rango 1 o 0 ya que si $\beta_0 = \{v_1, \ldots, v_{n-1}\} \hookrightarrow H_0$ y $\beta = \{v_1, \ldots, v_n\} \hookrightarrow L$

$$\begin{aligned}\mathrm{Im}(\lambda\pi_a\mu\pi_b) &= \langle \lambda\pi_a \circ \mu\pi_b[\beta]\rangle \\ &= \langle (\lambda\pi_a \circ \mu\pi_b)(v_1), \cdots, (\lambda\pi_a \circ \mu\pi_b)(v_n)\rangle\end{aligned}$$

donde sin perdida de generalidad, $\mu\pi_b(v_1) = 0, \ldots, \mu\pi_b(v_{n-1}) = 0$, por eso $\lambda\pi_a \circ \mu\pi_b(v_1) = 0, \ldots, \lambda\pi_a \circ \mu\pi_b(v_{n-1}) = 0$, de donde tenemos tenemos que

$$\lambda\pi_a \circ \mu\pi_b(v_n) \begin{cases} = 0 & \Longrightarrow \mathrm{Im}(\lambda\pi_a \circ \mu\pi_b) = \{0\} \Longrightarrow \mathrm{ran}(\lambda\pi_a \circ \mu\pi_b) = 0 \\ \neq 0 & \Longrightarrow \mathrm{Im}(\lambda\pi_a \circ \mu\pi_b) = \langle \lambda\pi_a \circ \mu\pi_b(v_n)\rangle \Longrightarrow \mathrm{ran}(\lambda\pi_a) = 1 \end{cases}$$

Teorema 2.0.40. *Si λ, μ, a y b son elementos distintos de cero en L y $\lambda\pi_a$, $\mu\pi_b$ son los elementos correspondientes de rango 1 en $End_K L$ entonces*

$$(\lambda\pi_a)(\mu\pi_b) = \lambda Tr(a\mu)\pi_b.$$

Demostración. Recordemos que

$$\begin{aligned}(\lambda\pi_a)(\mu\pi_b) &= (\sum_{\phi_i \in G} \lambda\phi_i(a)\phi_i)(\sum_{\tau_i \in G} \mu\tau_i(b)\tau_i) \\ &= \sum_{\phi_i\tau_i \in G} \lambda\phi_i(a)\phi_i(\mu)\phi_i\tau_i(b)\phi_i\tau_i\end{aligned}$$

Si definimos $\rho(b) = \phi\tau(b)\phi\tau$ tenemos

$$\begin{aligned}&= \sum_{\phi_i \in G} \lambda\phi(a)\phi(\mu)\rho(b) \\ &= \sum_{\phi_i \in G} \lambda\phi(a\mu)\rho(b) \\ &= \lambda \sum_{\phi_i \in G} \phi(a\mu)\rho(b) \\ &= \lambda\mathrm{Tr}(a\mu)\rho(b)\end{aligned}$$

Además, de la definición de $\rho(b)$, vemos que si $\omega_i = \phi_i\tau_i$, $\omega_i \in G$, se puede obtener $\pi_b = \omega_1(b)\omega_1 + \cdots + \omega_n(b)\omega_n$ como un factor en la suma, es decir $(\lambda\pi_a)(\mu\pi_b) = \lambda\mathrm{Tr}(a\mu)\pi_b$. ■

Observación 2.0.41. $(\lambda\pi_a)(\mu\pi_b) = 0$ si y sólo si $\mathrm{Tr}(a\mu) = 0$

Demostración. Si $(\lambda\pi_a)(\mu\pi_b) = 0$ y $\mathrm{Tr}(a\mu) \neq 0$ tendriamos que $\pi_b = 0$, pero π_b es de rango 1, lo cual es una contradicción. La otra implicación es inmediata. ■

Observación 2.0.42. Aplicando el teorema para $\lambda\pi_a = \mu\pi_b$ con $\mathrm{Tr}(b\mu) = 1$ nos lleva a que

$$(\mu\pi_b)(\mu\pi_b) = \mu\mathrm{Tr}(b\mu)\pi_b = \mu\pi_b$$

es decir, $\mu\pi_b$ es *idempotente*

Observación 2.0.43. si consideramos un elemento τ de rango 1 en $\mathrm{End}_K L$, y denotamos por $\mathrm{tr}(\tau)$ la traza matricial de τ, tenemos que $\tau^2 = \mathrm{tr}(\tau)\tau$

Demostración.

- Por un lado, $\tau^2 = (\lambda\pi_a)(\lambda\pi_a) = \lambda\mathrm{Tr}(a\lambda)\pi_a$ para alguna $\lambda, a \in L$. Pero $\mathrm{Tr}(a\lambda) = \sum_{i=1}^{n} \phi_i(a\lambda)$, por eso

$$\lambda\mathrm{Tr}(a\lambda)\pi_a = \lambda(\sum_{i=1}^{n} \phi_i(a\lambda))(\sum_{i=1}^{n} \phi_i(a)\phi_i)$$

- Por otro lado, considerando la base $\beta = \{\phi_1, \ldots, \phi_n\} \hookrightarrow \mathrm{End}_K L$ tenemos que

$$[\tau]_\beta = \begin{pmatrix} \lambda\phi_1(a) & 0 & \ldots & 0 \\ 0 & \lambda\phi_2(a) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda\phi_n(a) \end{pmatrix}$$

de donde se se tiene que $\mathrm{tr}(\tau) = \sum_{i=1}^{n} \lambda\phi_i(a) = \lambda \sum_{i=1}^{n} \phi_i(a)$.

Además $\tau = \lambda\pi_a = \lambda(\phi_1(a)\phi_1 + \cdots + \phi_n(a)\phi_n)$, entonces $\mathrm{tr}(\tau)(\tau) = \lambda(\sum_{i=1}^{n} \phi_i(a))(\sum_{i=1}^{n})$ pero para toda $1 \leq i \leq n$ tenemos que $\phi_i(a)\phi_i(\lambda)\phi_i(a)\phi_i = \phi_i(a\lambda)\phi_i(a)\phi_i$. Así

$$\mathrm{tr}(\tau)(\tau) = \lambda(\sum_{i=1}^{n} \phi_i(a)\phi_i(\lambda))(\sum_{i=i}^{n} \phi_i(a)\phi_i) = \lambda(\sum_{i=1}^{n} \phi_i(a\lambda))(\sum_{i=1}^{n} \phi_i(a)\phi_i)$$

■

De todo lo anterior se desprende el siguiente

Corolario 2.0.44. *Si* $0 \neq \lambda \in L$ *y* $\lambda\pi_a$ *el elemento de rango* 1 *correspondiente en* $End_K L$ *entonces* $tr\lambda\pi_a = Tr(\lambda a)$

Demostración. Por la observación $(\lambda\pi_a)(\lambda\pi_a) = \mathrm{tr}(\lambda\pi_a)(\lambda\pi_a)$ y por el teorema anterior $(\lambda\pi_a)(\lambda\pi_a) = \lambda\mathrm{Tr}(\lambda a)\pi_a = \mathrm{Tr}(\lambda a)(\lambda\pi_a)$, entonces $\mathrm{tr}(\lambda\pi_a)(\lambda\pi_a) = \mathrm{Tr}(\lambda a)(\lambda\pi_a)$ de donde se sigue que

$$\mathrm{tr}(\lambda\pi_a) = \mathrm{Tr}(\lambda a)$$

■

Lema 2.0.45. *Sea* $\beta = \{x_1, \ldots, x_n\}$ *una* K*-base para* L*. Entonces la matriz de* $n \times n$

$$B = \begin{pmatrix} \phi_1(x_1) & \phi_2(x_1) & \ldots & \phi_n(x_1) \\ \phi_1(x_2) & \phi_2(x_2) & \ldots & \phi_n(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_1(x_n) & \phi_2(x_n) & \ldots & \phi_n(x_n) \end{pmatrix}$$

es invertible.

Demostración. Supongamos por contradicción que no es invertible, entonces por álgebra lineal, el rango $\mathrm{ran}B < n$, entonces existen $\lambda_1, \ldots, \lambda_n \in L$ no todos cero tales que

$$\lambda_1\phi_1(x_i) + \cdots + \lambda_n\phi_n(x_i) = 0$$

con $1 \leq i \leq n$, es decir, $\phi_j(x_i)$ es la j-esima columna de B.

Consideremos $x \in L$, como β es una base para L, entonces $x = \mu_1 x_1 + \cdots + \mu_n x_n$ con μ_i únicos en K. Si hacemos

$$\begin{array}{rc} & \mu_1(\lambda_1\phi_1(x_i) + \cdots + \lambda_n\phi_n(x_i)) = 0 \\ & \mu_2(\lambda_1\phi_1(x_i) + \cdots + \lambda_n\phi_n(x_i)) = 0 \\ + & \vdots \\ & \mu_n(\lambda_1\phi_1(x_i) + \cdots + \lambda_n\phi_n(x_i)) = 0 \end{array}$$

y factorizamos $\lambda_i\phi_i$, obtenemos

$$\lambda_1\phi_1(\mu_1 x_1 + \cdots + \mu_n x_n) + \cdots + \lambda_n\phi_n(\mu_1 x_1 + \cdots + \mu_n x_n) = 0$$

de donde

$$\lambda_1\phi_1(x) + \cdots + \lambda_n\phi_n(x) = 0$$

para toda $x \in L$, es decir:

$$\lambda_1\phi_1 + \cdots + \lambda_n\phi_n = 0$$

Pero $\{\phi_1, \ldots, \phi_n\}$ es un conjunto linealmente independiente, lo cual es una contradicción. Entonces $\text{ran}B = n$ y B es invertible. ■

Teorema 2.0.46. *Sea $\{x_1, \ldots, x_n\}$ una K-base para L, y π_i los elementos de $End_K L$ definidos anteriormente. Sea τ cualquier elemento de $End_K L$. Entonces existen μ_i elementos tales que*

$$\tau = \mu_1\pi_1 + \cdots + \mu_n\pi_n$$

Demostración. Por el teorema 2.0.34 escribimos a τ como $\tau = \lambda_1\phi_1 + \cdots + \lambda_n\phi_n$ con $\lambda_i \in L$. Ahora, usando que $\pi_i = \phi_1(x_i)\phi_1 + \cdots + \phi_n(x_i)\phi_n$ para $1 \leq i \leq n$ tenemos que encontrar μ_i tales que $\lambda_i = \mu_1\phi_i(x_1) + \cdots + \mu_n\phi_i(x_n)$.

Escribimos ahora

$$\begin{aligned}\tau =& \mu_1(\phi_1(x_1)\phi_1 + \cdots + \phi_n(x_1)\phi_n)\\ &+ \mu_2(\phi_1(x_2)\phi_1 + \cdots + \phi_n(x_2)\phi_n)\\ &+ \qquad\qquad \vdots\\ &+ \mu_n(\phi_1(x_n)\phi_1 + \cdots + \phi_n(x_n)\phi_n)\end{aligned}$$

es decir,

$$\tau = (\mu_1\phi_1(x_1) + \cdots + \mu_n\phi_1(x_n))\phi_1 + \cdots (\mu_1\phi_n(x_1) + \cdots + \mu_n\phi_n(x_n))\phi_n$$

así tenemos que

$$\lambda_1 = \mu_1\phi_1(x_1) + \cdots + \mu_n\phi_1(x_n)$$

y en general

$$\lambda_i = \mu_1\phi_i(x_1) + \cdots + \mu_n\phi_i(x_n)$$

Y así obtenemos el sistema de ecuaciones con incógnitas μ_i:

$$\begin{aligned}\lambda_1 &= \mu_1\phi_1(x_1) + \mu_2\phi_1(x_2) + \cdots + \mu_n\phi_1(x_n)\\ \lambda_2 &= \mu_1\phi_2(x_1) + \mu_2\phi_2(x_2) + \cdots + \mu_n\phi_2(x_n)\\ &\vdots\\ \lambda_n &= \mu_1\phi_n(x_1) + \mu_2\phi_n(x_2) + \cdots + \mu_n\phi_n(x_n)\end{aligned}$$

Traduciendo esto a matrices, si

$$\overline{\mu} = \begin{pmatrix}\mu_1\\ \vdots\\ \mu_n\end{pmatrix},\ \overline{b} = \begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_n\end{pmatrix},\ \text{y } C = \begin{pmatrix}\phi_1(x_1) & \phi_1(x_2) & \dots & \phi_1(x_n)\\ \phi_2(x_1) & \phi_2(x_2) & \dots & \phi_2(x_n)\\ \vdots & \vdots & \ddots & \vdots\\ \phi_n(x_1) & \phi_n(x_2) & \dots & \phi_n(x_n)\end{pmatrix}$$

entonces tenemos que $\overline{b} = C\overline{\mu}$, y para encontrar $\overline{\mu}$ tenemos que $\overline{\mu} = C^{-1}\overline{b}$, pero como $C = B^t$ y B es una matriz invertible, por álgebra lineal, C es también invertible, el sistema tiene una solución única, y efectivamente existen tales $\mu_1, \dots, \mu_n$. ■

Considerando, para toda $1 \leq i \leq n$, a $E_i = \{\tau | \tau \text{ es } L\text{-múltiplo de } \pi_i\} \leq \text{End}_K L$, es fácil ver que $\dim E_i = n$, y además, para toda $0 \neq \tau \in E_i$, tenemos que $\text{ran}\tau = 1$, así que $\text{End}_K L = \oplus_{i=1}^n E_i$, y como $\pi_i = \phi_1(x_i)\phi_1 + \cdots + \phi_n(x_i)\phi_n$, $\{\phi_1, \dots, \phi_n\}$ es una base para E_i, por eso $\dim(\text{End}_K L) = \sum_{i=1}^n \dim E_i = n \cdot n = n^2$

Teorema 2.0.47. *Sea $\tau = \lambda_1\phi_1 + \cdots + \lambda_n\phi_n$ con ϕ_1 la identidad, un elemento de $End_K L$, entonces $tr(\tau) = Tr(\lambda_1)$.*

Demostración. Consideremos las bases $\beta = \{\phi_1, \dots, \phi_n\} \hookrightarrow \text{End}_K L$ y $\beta_k = \{x_1, \dots, x_n\} \hookrightarrow_K L$. Si

$$\tau = \mu_1\pi_1 + \cdots + \mu_n\pi_n$$

y a su vez $\pi_i = \phi_1(x_i)\phi_1 + \cdots + \phi_n(x_i)\phi_n$ tenemos que

$$\tau = \mu_1(\phi_1(x_1)\phi_1 + \cdots + \phi_n(x_1)\phi_n) + \cdots + \mu_n(\phi_1(x_n)\phi_1 + \cdots + \phi_n(x_n)\phi_n)$$

Como $\mu_i\pi_i = \mu_i\phi_1(x_i)\phi_1 + \cdots + \mu_i\phi_n(x_i)\phi_n$,

$$\text{tr}(\tau) = \sum_{i=i}^{n} \text{tr}(\mu_i\pi_i).$$

Además $\mathrm{tr}\mu_i\pi_i = \mathrm{Tr}\mu_i x_i$, es decir,

$$\mathrm{tr}\tau = \sum_{i=1}^{n} \mathrm{Tr}\mu_i x_i = \mathrm{Tr}(\sum_{i=1}^{n} \mu_i x_i).$$

Como $\tau = [\mu_1\phi_1(x_1) + \mu_2\phi_1(x_2) + \cdots + \mu_n\phi_1(x_n)]\phi_1 + \cdots$ y por otro lado $\tau = \lambda_1\phi_1 + \cdots + \lambda_n\phi_n$, tenemos que

$$\lambda_1 = \mu_1\phi_1(x_1) + \cdots + \mu_n\phi_1(x_n)$$

de donde $\mathrm{Tr}(\lambda_1) = \sum_{i=1}^{n} \phi_i(\mu_1\phi_1(x_1) + \cdots + \mu_n\phi_1(x_n))$ y y se sigue el resultado. ■

Capítulo 3

Ejemplos y conclusiones.

Consideremos $f(x) = x^2 - p \in \mathbb{Q}[x]$. Claramente f no tiene raíces en $\mathbb{Q}$, y su campo de descomposición es

$$\mathbb{Q}(\sqrt{p}) = \{x + y\sqrt{p} | x, y \in \mathbb{Q} \text{ y } p \text{ es primo}\}$$

. De ahí que $\mathbb{Q}(\sqrt{q})$ sea una extensión de Galois de $\mathbb{Q}$, donde

$$Gal(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) = \text{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}) = \{\phi_1, \phi_2\}$$

con $\phi_1(x + y\sqrt{p}) = x + y\sqrt{p}$ la identidad, y $\phi_2(x + y\sqrt{p}) = x - y\sqrt{p}$ la conjugación. Por otro lado, visto como espacio vectorial sobre el campo $\mathbb{Q}$, la base canónica para $\mathbb{Q}(\sqrt{p})$ es $\beta = \{1, \sqrt{p}\} \hookrightarrow \mathbb{Q}(\sqrt{p})$. Así, una función en $\text{End}_{\mathbb{Q}}\mathbb{Q}(\sqrt{p})$, $T : \mathbb{Q}(\sqrt{p}) \longrightarrow \mathbb{Q}(\sqrt{p})$ tiene asociada una única matriz en $[T]_\beta \in M_{n\times n}(\mathbb{Q})$

Consideremos una función arbitraria con matriz de representación respecto a β

$$[T]_\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ con } a, b, c, d \in \mathbb{Q},$$

es decir, $T(1) = (a + c\sqrt{p})$ y $T(\sqrt{p}) = b + d\sqrt{p}$. Busquemos $\lambda_1, \lambda_2 \in \mathbb{Q}(\sqrt{p})$ tales que

$$T = \lambda_1\phi_1 + \lambda_2\phi_2.$$

Sean $\lambda_1 = x_1 + y_1\sqrt{p}$, $\lambda_2 = x_2 + y_2\sqrt{p}$ con $x_1, x_2, y_1, y_2 \in \mathbb{Q}$; evaluando T en

la base β tenemos que

$$\begin{aligned} T(1) &= \lambda_1\phi_1(1) + \lambda_2\phi_2(1) \\ &= (x_1 + y_1\sqrt{p})\phi_1(1) + (x_2 + y_2\sqrt{p})\phi_2(1) \\ &= (x_1 + y_1\sqrt{p})(1) + (x_2 + y_2\sqrt{p})(1) \\ &= (x_1 + x_2)(1) + (y_1 + y_2)(\sqrt{p}) \end{aligned}$$

$$\begin{aligned} T(\sqrt{p}) &= \lambda_1\phi_1(\sqrt{p}) + \lambda_2\phi_2(\sqrt{p}) \\ &= (x_1 + y_1\sqrt{p})\phi_1(\sqrt{p}) + (x_2 + y_2\sqrt{p})\phi_2(\sqrt{p}) \\ &= (x_1 + y_1\sqrt{p})(\sqrt{p}) + (x_2 + y_2\sqrt{p})(-\sqrt{p}) \\ &= x_1\sqrt{p} + y_1p - x_2\sqrt{p} - y_2p \\ &= (y_1p - y_2p)(1) + (x_1 - x_2)\sqrt{p} \end{aligned}$$

Comparando obtenemos que

$$\begin{array}{cc} x_1 + x_2 = a & y_1p - y_2p = b \\ y_1 + y_2 = c & x_1 - x_2 = d \end{array}$$

de donde

$$\begin{array}{cc} x_1 = \frac{a+d}{2} & y_1 = \frac{b+cp}{2p} \\ x_2 = \frac{a-d}{2} & y_2 = \frac{cp-b}{2p} \end{array}$$

Es decir:

$$\lambda_1 = \left(\frac{a+d}{2}\right) + \left(\frac{b+cp}{2}\right)\sqrt{p}, \;\; \lambda_2 = \left(\frac{a-d}{2}\right) + \left(\frac{cp-b}{2p}\right)\sqrt{p}.$$

Si $T : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ está dada por $T(x + y\sqrt{2}) = 2y\sqrt{2}$, entonces

$$[T]_\beta \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}.$$

Con esto, $\lambda_1 = 1$ y $\lambda_2 = -1$, entonces:

$$\begin{aligned} T(x + y\sqrt{2}) &= (1)\phi_1(x + y\sqrt{2}) + (-1)\phi_2(x + y\sqrt{2}) \\ &= (1)(x + y\sqrt{2}) + (-1)(x - y\sqrt{2}) \\ &= 2y\sqrt{2}. \end{aligned}$$

Por ser ambos espacios de dimensión 2, tenemos que $\mathbb{R}^2 \cong \mathbb{Q}(\sqrt{2})$. Como un hiperplano de $\mathbb{Q}(\sqrt{2})$ es un espacio vectorial de dimensión 1, los hiperplanos se identifican con las rectas que pasan por el origen. Un hiperplano en $\mathbb{Q}(\sqrt{p})$ es de la forma $x + ky\sqrt{p} = 0$ donde $k, x, y \in \mathbb{Q}$ y $x = ky$, o es el eje de los $x + y\sqrt{p}$ tal que $x = 0$.

Consideremos los hiperplanos de $\mathbb{Q}(\sqrt{p})$: $U = \{x + y\sqrt{p} \in \mathbb{Q}(\sqrt{p}) | x = 0\}$ y $H = \{x + y\sqrt{p} | x = y\}$, encontremos una $a \in \mathbb{Q}\sqrt{p}$ tal que

$$U = a^{-1}H$$

Consideremos $1 + \sqrt{p} \in H$ y $0 + \sqrt{p} \in U$, entonces:

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

De donde tenemos que $x = 1$ e $y = \frac{1}{p}$, es decir $a = 1 + \frac{\sqrt{p}}{p} = 1 + \frac{1}{\sqrt{p}}$.

Corroborando vemos que para $0 + y\sqrt{p} \in U$, el producto

$$(1 + \frac{\sqrt{p}}{p})(0 + y\sqrt{p}) = y + y\frac{\sqrt{p}}{p} \in H$$

Para encontrar a, el inverso de a^{-1}, definimos y denotamos al *conjugado* de $a = x + y\sqrt{p} \in \mathbb{Q}(\sqrt{p})$ como $\bar{a} = x - y\sqrt{p}$, y así tenemos que

$$a^{-1} = \frac{1}{a} = \frac{\bar{a}}{a\bar{a}}$$

En nuestro caso, $(a^{-1})^{-1} = a = \frac{p}{p-1} - \frac{\sqrt{p}}{p^2-1}$ si análogamente tomamos $x + x\sqrt{p} \in H$, tenemos que:

$$(x + x\sqrt{p})\left(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1}\right) = \left(\frac{xp - x}{p-1}\right)\sqrt{p} \in U$$

Respecto al hiperplano H_0, recordemos que $H_0 = \text{Nuc}(\text{Tr})$ donde $\text{Tr} = \phi_1 + \phi_2$, entonces para $x + y\sqrt{p} \in \mathbb{Q}(\sqrt{p})$

$$\begin{aligned} x + y\sqrt{p} \in \text{Nuc}Tr &\iff \text{Tr}(x + y\sqrt{p}) = 0 \\ &\iff \phi_1(x + y\sqrt{p}) + \phi_2(x + y\sqrt{p}) = 0 \\ &\iff 2x = 0 \\ &\iff x + y\sqrt{p} \in U \end{aligned}$$

Así que $H_0 = U$, y tenemos que si $a = \frac{p}{p-1} - \frac{\sqrt{p}}{p-1}$ entonces $a^{-1}H_0 = H$. Evaluemos ahora

$$\pi_a[H] = \phi_1(a)\phi_1[H] + \phi_2(a)\phi_2[H]$$

Sea $x + x\sqrt{p} \in H$, entonces

$$\begin{aligned}\pi_a(x + x\sqrt{p}) =& \phi_1(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1})\phi_1(x + x\sqrt{p}) \\ &+ \phi_2(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1})\phi_2(x + x\sqrt{p} \\ =& \left(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1}\right)(x + x\sqrt{p}) \\ &+ \left(\frac{p}{p-1} + \frac{\sqrt{p}}{p-1}\right)(x - x\sqrt{p}) = 0\end{aligned}$$

Consideremos ahora $\lambda = \sqrt{p} \in \mathbb{Q}(\sqrt{p})$, obtengamos la matriz de representación respecto a la base β de

$$\lambda\pi_a = \lambda\phi_1(a)\phi_1 + \lambda\phi_2(a)\phi_2$$

Recordando que $\beta = \{1, \sqrt{p}\}$,

$$\begin{aligned}\lambda\pi_a(1) =& \sqrt{p}\phi_1\left(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1}\right)\phi_1(1) + \sqrt{p}\phi_2\left(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1}\right)\phi_2(1) \\ =& \sqrt{p}\left(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1}\right) + \sqrt{p}\left(\frac{p}{p-1} + \frac{\sqrt{p}}{p-1}\right) \\ =& \left(\frac{2p}{p-1}\right)\sqrt{p}\end{aligned}$$

$$\begin{aligned}\lambda\pi_a(\sqrt{p}) =& \sqrt{p}\phi_1\left(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1}\right)\phi_1(\sqrt{p}) + \sqrt{p}\phi_2\left(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1}\right)\phi_2(\sqrt{p}) \\ =& \sqrt{p}\left(\frac{p}{p-1} - \frac{\sqrt{p}}{p-1}\right)(\sqrt{p}) + \sqrt{p}\left(\frac{p}{p-1} + \frac{\sqrt{p}}{p-1}\right)(\sqrt{p}) \\ =& \left(-\frac{2p}{p-1}\right)\sqrt{p}\end{aligned}$$

Así tenemos que

$$[\lambda\pi_a]_\beta = \begin{pmatrix} 0 & 0 \\ \frac{2p}{p-1} & -\frac{2p}{p-1} \end{pmatrix}$$

es una matriz de 2×2 con columnas linealmente dependientes, es decir, $\text{ran}\lambda\pi_a = 1$.

Continuando con los resultados, consideremos $\lambda = 1, \mu = \sqrt{p}$, $a = 1 + \sqrt{p}, b = 2\sqrt{p} \in \mathbb{Q}(\sqrt{p})$, así:

$$\begin{aligned} \lambda\pi_a =& (1)\phi_1(1+\sqrt{p})\phi_1 + (1)\phi_2(1+\sqrt{p})\phi_2 \\ =& (1+\sqrt{p})\phi_1 + (1-\sqrt{p})\phi_2 \\ =& \phi_1 + \sqrt{p}\phi_1 + \phi_2 - \sqrt{p}\phi_2 \end{aligned}$$

$$\begin{aligned} \mu\pi_b =& (\sqrt{p})\phi_1(2\sqrt{p})\phi_1 + (\sqrt{p})\phi_2(2\sqrt{p})\phi_2 \\ =& \sqrt{p}\sqrt{p}\phi_1 + \sqrt{p}(-\sqrt{p})\phi_2 \\ =& 2p\phi_1 - 2p\phi_2 \end{aligned}$$

Entonces

$$\begin{aligned} (\lambda\pi_a)(\mu\pi_b) =& 2p\phi_1\phi_1 - 2p\phi_1\phi_2 \\ & + 2p\sqrt{p}\phi_1\phi_1 - 2p\sqrt{p}\phi_1\phi_2 \\ & + 2p\phi_2\phi_1 - 2p\phi_2\phi_2 \\ & - 2p\sqrt{p}\phi_2\phi_1 + 2p\sqrt{p}\phi_2\phi_2 \\ =& 2p\phi_1 - 2p\phi_2 + 2p\sqrt{p}\phi_1 - 2p\sqrt{p}\phi_2 \\ & + 2p\phi_2 - 2p\phi_1 - 2p\sqrt{p}\phi_2 + 2p\sqrt{p}\phi_1 \\ =& 4p\sqrt{p}\phi_1 - 4p\sqrt{p}\phi_2 \end{aligned}$$

Por otro lado,

$$\begin{aligned} \lambda\text{Tr}(a\mu) =& (1)[\phi_1((1+\sqrt{p})\sqrt{p}) + \phi_2((1+\sqrt{p})\sqrt{p})] \\ =& \phi_1(p+\sqrt{p}) + \phi_2(1+\sqrt{p}) \\ =& p + \sqrt{p} + p - \sqrt{p} \\ =& 2p \end{aligned}$$

Entonces

$$\begin{aligned} \lambda\text{Tr}(a\mu)\pi_b =& 2p[\phi_1(2\sqrt{p})\phi_1 + \phi_2(\sqrt{p})\phi_2] \\ =& 2p[2\sqrt{p}\phi_1 - 2\sqrt{p}\phi_2] \\ =& 4p\sqrt{p}\phi_1 - 4p\sqrt{p}\phi_2 \end{aligned}$$

$$\therefore (\lambda\pi_a)(\mu\pi_b) = \lambda \mathrm{Tr}(a\mu)\pi_b$$

Usando la misma λ, a, tenemos también que

$$\mathrm{tr}(\lambda\pi_a) = 2 = \mathrm{Tr}(\lambda a)$$

Recordando que $\beta = \{1, \sqrt{p}\} \hookrightarrow \mathbb{Q}(\sqrt{p})$, tenemos que la matriz

$$B = \begin{pmatrix} \phi_1(1) & \phi_2(1) \\ \phi_1(\sqrt{p}) & \phi_2(\sqrt{p}) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{1}{\sqrt{p}} & -\frac{1}{\sqrt{p}} \end{pmatrix}$$

Es una matriz con $\det B = 0$, por lo tanto es una matriz invertible. Consideremos ahora a $\mathbb{C}$ como un $\mathbb{R}$-espacio vectorial, al igual que en los ejemplos anteriores el conjunto $Gal(\mathbb{C}/\mathbb{R}) = \{f_1, f_2\}$ donde f_1 es la identidad y f_2 es la conjucación compleja.

Sea la base $\beta = \{1, i\} \hookrightarrow_{\mathbb{R}} \mathbb{C}$, obtengamos $\pi_1(x)$ y $\pi_2(x)$;
sea $a + ib = x \in \mathbb{C}$, entonces:

$$\begin{aligned} \pi_1(x) &= f_1(1)f_1(x) + f_2(1)f_2(x) \\ &= 1f_1(a+ib) + 1f_2(a+ib) \\ &= a + ib + a - ib \\ &= 2a. \end{aligned}$$

$$\begin{aligned} \pi_i(x) &= f_1(i)f_1(x) + f_2(i)f_2(x) \\ &= if_1(a+ib) - if_2(a+ib) \\ &= ia - b - ia - b \\ &= -2b. \end{aligned}$$

Consideremos ahora la transformación lineal $T : \mathbb{C} \longrightarrow \mathbb{C}$ dada por $T(a+ib) = ra + sib$ donde $r, s \in \mathbb{C}$. Entonces tenemos que

$$\begin{aligned} T(a+ib) = ra + sib &= \mu_1\pi_1(a+ib) + \mu_2\pi_2(a+ib) \\ &= \mu_1(2a) + \mu_2(-2b). \end{aligned}$$

de donde tenemos que

$$\mu_1 = \frac{r}{2} \text{ y } \mu_2 = -\frac{s}{2}i.$$

Entonces tenemos efectivamente que

$$\begin{aligned}\mu_1\pi_1(x) + \mu_2\pi_2(x) &= \left(\frac{r}{2}\right) 2a + \left(-\frac{s}{2}i\right) 2b \\ &= ra + sib.\end{aligned}$$

Sea $T(a+ib) = 4a$; para ejemplificar el ultimo resultado de trabajo, hemos primero de expresar a T como combinación de funciones en $\mathrm{Aut}_{\mathbb{R}}\mathbb{C}$, tenemos que

$$T(a+ib) = 4a = \lambda_1 f_1(a+ib) + \lambda_2 f_2(a+ib)$$

De donde tenemos que $\lambda_1 = \lambda_2 = 2$, y por eso $\mathrm{Tr}(\lambda_1) = f_1(2) + f_2(2) = 4$..

Por otro lado $[T]_\beta = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$

Entonces la traza matricial también es efectivamente $\mathrm{tr}T = 4$.

A este punto hemos encontrado dos formas distintas para expresar a los automorfismos de una extensión de Galois, lo cual ofrece opciónes para representar a dichas funciones en términos de otras. Las aplicaciones de estos resultados a problemas concretos en matemáticas se continúan en [4]; las aplicaciones en la vida real de los mismos resultados, como en la mayoría de los casos: no son necesarias para garantizar la certeza del hecho.

Bibliografía

[1] Bhattacharya PB. et al. "Basic Abstract Algebra", segunda edición, Cambridge University Press (1994).

[2] Bloch Ethan. "Proofs and Fundamentals: A First Course in Abstract Mathematics" primera edición, Birkhauser (2000).

[3] Friedberg S.H. et al "Linear Algebra" cuarta edición, Prentice Hall, (2003).

[4] Gow Rod, Quinlan Rachel. "Galois Theory and linear Algebra" Linear Algebra an its Applications 430 (2009), 1778-1789.

[5] Hungerford T.W. "Abstract Algebra an introduction" 1a ed. Saunders College Publishing.

[6] Jacobson, N. "Basic Algebra I" segunda edición, San Francisco Freeman (1985).

[7] Papantonopoulou A. "Algebra: pure and applied" Prentice Hall, (2002).

[8] Rotman J. "An introduction to theory of groups", tercera edición. Prentice Hall (1995).