Capítulo

10

Cuerpos

10.1 Introducción

La estructura de cuerpo es una de las más completas dentro del álgebra. Por tener buenas propiedades de divisibilidad y factorización, los cuerpos son conjuntos adecuados para plantear y resolver ecuaciones.

En este capítulo se estudian las extensiones algebraicas de cuerpos y algunas de sus propiedades.

Existe una estrecha conexión entre la teoría de cuerpos y la teoría de los polinomios, como se verá en este capítulo. Ambas teorías tienen su origen común en uno de los problemas más antiguos de la matemática, como lo es la resolución de ecuaciones algebraicas de grado > 1 y el problema de las construcciones geométricas.

Desde la época de los babilonios, los matemáticos se plantean resolver ecuaciones cuadráticas, para lo cual comenzaron a utilizar raíces cuadradas. Los griegos resuelven algunos de estos problemas usando métodos geométricos. Uno de sus mayores logros fue demostrar que la ecuación

$$x^2 - 2 = 0$$

esa irresoluble en el cuerpo de los números racionales, pues $\sqrt{2}$ no se puede expresar como una fracción.

Además de este, los griegos plantearon otros problemas irresolubles, como la cuadratura del circulo, la trisección del ángulo y la duplicación del cubo, los cuales no se podrán resolver por fracciones, pero cuya demostración formal hubo de esperar varios siglos.

Durante la edad media y el renacimiento el álgebra se ocupa casi exclusivamente de la resolución de ecuaciones de 3^{er} grado y 4^{to} grado,

usando raíces. Vale destacar a **Escipión del Ferro** quien a comienzos del siglo XVI obtiene una solución por medio de radicales para la ecuación cúbica

$$x^3 + ax = b$$

También los matemáticos italianos del renacimiento Tartaglia, Cardano y Ludovico Ferrari, obtienen avances importantes al descubrir nuevas soluciones de estas ecuaciones mediante métodos ingeniosos de manipulación de raíces y cambios de variables.

El estudio general de las ecuaciones algebraicas de grado n, fue iniciado por Lagrange y Vandermonde en 1770. El método de Lagrange consiste en ir reduciendo de grado las ecuaciones, utilizando para ello el concepto de la resolvente de un polinomio.

Más tarde Carl F. Gauss en sus "*disquisitiones arithmethicae*" estudia el problema general de hallar las soluciones de una ecuación del tipo $x^n - 1 = 0$. Uno de los grandes logros de Gauss, es resolver el problema de la construcción geométrica con regla y compás de un poligono de n lados, lo cual se fundamenta en su estudio de esta ecuación.

El inicio de la teoría general de cuerpos se halla en la obra de los matemáticos, Ruffini, Abel y Galois, quienes demostraron que toda ecuación algebraica de grado mayor o igual que cinco no puede resolverse usando radicales.

Con Galois se inicia el estudio de las extensiones de cuerpos por adjunción de raíces. En sus trabajos se establece una conexión maravillosa entre las raíces de una ecuación polinómica, las extensiones de cuerpos que contienen estas raíces y el grupo de automorfismo de estos cuerpos. Esta teoría culmina en forma brillante uno de los capitulos más importantes de la matemática y que fue el objeto del álgebra durante varios siglos: la búsqueda de soluciones de una ecuación algebraica mediante radicales.

10.2 Cuerpos

Definición 10.2.1 *Un* **cuerpo** *es un conjunto $\mathbb{R}$, diferente del vacío, con dos operaciones llamadas suma y producto, denotadas por $+$ y $\cdot$*

tales que verifican

1) Para todo a, b en $\mathbb{R}$, se tiene:

$$a + b \in \mathbb{R} \quad y \quad a \cdot b \in \mathbb{R}$$

2) Para todos a, b, c en $\mathbb{R}$

$$\begin{aligned} a + (b + c) &= (a + b) + c \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \end{aligned}$$

3) Para todo a, b en $\mathbb{R}$ se tiene

$$a + b = b + a \quad y \quad a \cdot b = b \cdot a$$

4) Existen elementos 0 y 1 en $\mathbb{R}$ llamados cero y uno, tales que para todo a en $\mathbb{R}$

$$\begin{aligned} a + 0 &= 0 + a = a, \\ a \cdot 1 &= 1 \cdot a = a \end{aligned}$$

5) Para todo a en $\mathbb{R}$, existe un elemento $-a$ llamado el opuesto de a tal que

$$a + (-a) = (-a) + a = 0$$

6) Si a es diferente de cero, existe un elemento a^{-1} en $\mathbb{R}$ llamado el inverso de a, tal que

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

7) Para todos a, b, c en $\mathbb{R}$

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

Observación: De acuerdo a la definición anterior, se tiene que $\mathbb{R}$ es un cuerpo si y sólo si, $\mathbb{R}$ es un anillo conmutativo con unidad, en donde todo elemento distinto de cero es una unidad.

Ejemplo 1: El conjunto de los números reales $\mathbb{R}$ bajo la suma y el producto.

Ejemplo 2: Si p es un número primo, $\mathbb{Z}_p$ el conjunto de los enteros módulo p es un cuerpo con la suma y el producto módulo p.

Ejemplo 3: Sea K un cuerpo. Entonces $K(x)$, el conjunto de funciones racionales sobre K, cuyos elementos son funciones del tipo

$$f(x) = \frac{p(x)}{q(x)}$$

donde $p(x)$ y $q(x)$ son polinomios sobre K y $q(x) \neq 0$, es un cuerpo.

Definición 10.2.2 *Un* **espacio vectorial** *sobre un cuerpo K, es un conjunto no vacío V cuyos elementos llamaremos* **vectores** *(para diferenciarlos de los elementos de K que se llaman escalares) y un par de operaciones suma de vectores y producto por un escalar, denotadas por $+$ y $\cdot$ y que satisfacen*

1) V es un grupo abeliano bajo la suma de vectores.

2) Para un vector v y $\alpha \in K$, se tiene

$$\alpha \cdot v \in V$$

3) Para v_1, v_2 en V y $\alpha, \beta \in K$ se tiene

$$\begin{aligned} (\alpha + \beta) \cdot v_1 &= \alpha \cdot v_1 + \beta \cdot v_1 \\ \alpha(v_1 + v_2) &= \alpha \cdot v_1 + \alpha \cdot v_2 \end{aligned}$$

4) Para $v \in V$ y $\alpha, \beta \in K$ se tiene

$$\alpha(\beta \cdot v) = (\alpha \cdot \beta) \cdot v$$

5) Si 1 es el uno en K, entonces

$$1 \cdot v = v$$

para todo $v \in V$

Observación: Si V es un espacio vectorial sobre K, diremos que V es un K-espacio.

Observación: El vector cero de $(V, +)$ será denotado por 0.

Ejemplo 1: Todo cuerpo K es un espacio vectorial sobre si mismo.

Ejemplo 2: Sea $V = \mathbb{R} \times \mathbb{R}$ con la suma de vectores definida por

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

y el producto por un escalar $\lambda \in \mathbb{R}$

$$\lambda(v, u) = (\lambda v, \lambda u)$$

Entonces es fácil verificar que V con estas operaciones es un espacio vectorial sobre $\mathbb{R}$.

Definición 10.2.3 *Sean $\{v_1, \ldots, v_n\}$ un conjunto de vectores en un espacio vectorial V sobre K. Un elemento $v \in V$, se dice que es* **combinación lineal** *de $\{v_1, \ldots, v_n\}$ si existen escalares $\lambda_1, \ldots, \lambda_n$, tales que*

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

Definición 10.2.4 *Sea V un espacio vectorial y V' un subconjunto de V, de tal forma que V' es un espacio vectorial sobre K, con las mismas operaciones definidas en V. Entonces V' se dice un* **subespacio vectorial** *de V'.*

La siguiente proposición es un hecho bien conocido del álgebra lineal.

Proposición 10.2.1 *Sea $\{v_1, \ldots, v_n\}$ un conjunto de vectores de V. Entonces el conjunto de todas las combinaciones lineales de $\{v_1, \ldots, v_n\}$ genera un subespacio vectorial de V.*

Observación: El subespacio generado por $\{v_1, \ldots, v_n\}$ se denota por $\langle v_1, \ldots, v_n \rangle = W$. Los elementos $v_1, \ldots, v_n$ se llaman los **generadores de W**.

Observación: Si $V = \langle v_1, \ldots, v_n \rangle$, para algún conjunto de vectores $\{v_1, \ldots, v_n\}$ en V, entonces se dice que V es **finitamente generado**.

Definición 10.2.5 *Sea V un espacio vectorial. Un conjunto de vectores $\{v_1, \ldots, v_n\}$ se dicen* **linealmente dependientes**, *si existen escalares $\lambda_1, \ldots, \lambda_n$ no todos nulos, tales que*

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$$

Caso contrario, diremos que el conjunto $\{v_1, \ldots, v_n\}$ es **linealmente independientes**.

Definición 10.2.6 *Sea V un espacio vectorial. Un conjunto de vectores $\{v_1, \ldots, v_n\}$ se llama* **base** *del espacio V, si satisface*

i) $V = \langle v_1, \ldots, v_n \rangle$

ii) Los vectores $v_1, \ldots, v_n$ son linealmente independientes.

La siguiente proposición del álgebra lineal es bien conocida.

Proposición 10.2.2 *Sea V un espacio vectorial y*

$$B = \{v_1, \ldots, v_n\} \qquad C = \{u_1, \ldots, u_m\}$$

dos bases de V. Entonces $m = n$.

Observación: De acuerdo a la proposición anterior podemos asignar a cada espacio vectorial un entero no negativo n, el cual llamamos **la dimensión del espacio** y que es igual al número de vectores de una base cualquiera de V. Por supuesto, nuestra definición de dimensión, no dependerá de la base elegida.

Usaremos la notación $dim(V)$ para indicar la dimensión de V.

Definición 10.2.7 *Sean V y V' dos espacios vectoriales sobre K. Una aplicación $\phi : V \longrightarrow V'$ se llama* **homomorfismo** *entre espacios vectoriales, si satisface*

i) Para v_1, v_2 en V

$$\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$$

ii) Para $v \in V$ y $\lambda \in K$

$$\phi(\lambda v) = \lambda \phi(v)$$

Un homomorfismo entre espacios vectoriales, también se llama homomorfismo lineal o aplicación lineal.

Definición 10.2.8 *Dos espacios vectoriales V y V' se dicen* **isomorfos** *y lo denotamos por $V \approx V'$, si existen un homomorfismo $\phi : V \longrightarrow V'$, el cual es biyectivo.*

Definición 10.2.9 *Sean V y V' espacios vectoriales y $\phi : V \longrightarrow V'$ un homomorfismo. El conjunto de los elementos v de V tales que $\phi(v) = 0$, se denomina el* **Kernel o núcleo de** *ϕ y lo denotamos por* $\ker \phi$.

Observación: Es fácil verificar que $\ker \phi$ es un subespacio vectorial de V. Además ϕ es $1:1$ si y sólo si $\ker \phi = \{0\}$. Para hallar la dimensión del Kernel, usamos el siguiente teorema del álgebra lineal el cual es bien conocido.

Teorema 10.2.1 *Sea $\phi : V \longrightarrow V'$ un homomorfismo de espacios vectoriales. Entonces*

$$dim(\ker \phi) = \quad dimV - \quad dimV'$$

Ejercicios

1) Probar que el anillo $\mathbb{C}$ de los números complejos es un cuerpo.

2) Probar que todo cuerpo K es un espacio vectorial sobre K. ¿Cuál es la dimensión de este espacio?

3) Sea $V = \mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$ el conjunto de las n-uplas $(x_1, \ldots, x_n)$, con $x_i \in \mathbb{R}$. Definimos una suma en V, mediante

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

y el producto por un escalar $\lambda \in \mathbb{R}$:

$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$$

Probar que V con estas dos operaciones es un espacio vectorial sobre $\mathbb{R}$. Halle una base para este espacio y determine su dimensión. El espacio V se denomina **espacio n-dimensional sobre $\mathbb{R}$.**

4) Sea $n = 3$ como en el ejercicio anterior. Determine cuáles de los siguientes conjuntos de vectores son linealmente independientes.

a) $(1,1,1),\ (1,1,0),\ (0,1,0)$
b) $(1,2,3),\ (1,0,1),\ (0,0,2)$
c) $(1,1,1),\ (1,1,2),\ (1,0,1)$
d) $(1,2,1),\ (0,\frac{1}{2},1),\ (1,0,0)$

5) Determine el Kernel del homomorfismo

$$\begin{array}{rcl} \phi:\ \mathbb{R}^3 & \longrightarrow & \mathbb{R} \\ (x,y,z) & \longrightarrow & x+y+z \end{array}$$

6) Sea K un cuerpo. Probar que $K[x]$ es un K-espacio vectorial de dimensión infinita.

7) Si V_1 y V_2 son dos subespacios de V, entonces la suma de V y V' se define por

$$V_1 + V_1' = \{v_1 + v_2 \mid v_1 \in V,\ v_2 \in V'\}$$

Probar que $V_1 + V_2$ es un subespacio de V.

8) Demostrar que

$$dim(V_1 + V_2) = dimV_1 + dimV_2 - dim(V_1 \cap V_2)$$

9) Sea W el subconjunto de $\mathbb{R}^3$, formado por los vectores (x,y,z), tales que

$$3x - 2y - z = 0$$

Probar que W es un subespacio de $\mathbb{R}^3$ de dimensión 2.

10) Demuestre que a cada aplicación lineal $\phi:\ \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ se le puede asociar una matriz A_ϕ de orden 2×2 sobre $\mathbb{R}$.

11) Demuestre que la aplicación ϕ del ejercicio de arriba es inyectiva, si y sólo si la matriz A_ϕ es invertible.

12) Demuestre que el conjunto de aplicaciones lineales inyectivas de $\mathbb{R}^2$ en $\mathbb{R}^2$ es un grupo, el cual es isomorfo al grupo lineal $L_2(\mathbb{R})$ estudiado en el capítulo 1.

10.3 Extensiones de Cuerpos

Cuando estudiabamos las raíces de un polinomio $f(x)$ sobre un cuerpo $K[x]$, vimos que algunas de ellas estaban sobre otro cuerpo F, el cual contiene a K como subcuerpo. Esto sugiere entonces la necesidad de construir extensiones de cuerpos, como una técnica para poder resolver ciertas ecuaciones polinómicas.

El caso típico de una extensión del cuerpo $\mathcal{Q}$, consiste en un cuerpo de la forma $\mathcal{Q}(\alpha)$, donde α es raíz de un polinomio $p(x)$ irreducible en $\mathcal{Q}[x]$. Dichas extensiones son cuerpos que están dentro del cuerpo de los números complejos, y contienen a $\mathcal{Q}$ como subcuerpos. La forma de construirlos, depende del polinomio $p(x)$ y de la raíz α, y la extensión $\mathcal{Q}(\alpha)$ será un espacio vectorial sobre $\mathcal{Q}$.

Definición 10.3.1 *Un cuerpo F se dice una* **extensión** *de un cuerpo K, si $K \subseteq F$ y además K es un subcuerpo de F.*

Si F es una **extensión finita de** K, entonces se puede probar fácilmente que F es un espacio vectorial sobre K. Esto da origen a la siguiente

Definición 10.3.2 *Sea F una extensión de K. La dimensión de F como espacio vectorial sobre K, se denomina* **grado de la extensión** *de F sobre K, y se denota por $[F : K]$.*

Si el grado de la extensión F sobre K es finito, diremos que F es una **extensión** finita de K. Caso contrario diremos que F es una **extensión trascendente** de K.

Ejemplo 1: El cuerpo $\mathbb{C}$ de los números complejos es una extensión finita del cuerpo $\mathbb{R}$ de los números reales.

Ejemplo 2: El cuerpo $\mathbb{R}$ de los números reales es una extensión trascendente de $\mathcal{Q}$.

Definición 10.3.3 *Sea K un cuerpo y α un elemento en una extensión de K. Entonces el* **cuerpo engendrado por α sobre K,** *denotado por $K(\alpha)$, es igual a la intersección de todas las extensiones de K que contienen a α.*

Observación: Es claro que la definición de arriba tiene sentido, pues si α está en una extensión F, se tiene que $K(\alpha) \subseteq F$.

Por otro lado, es fácil probar que la intersección de cualquier número de cuerpos es un cuerpo.

Si K es un cuerpo, F una extensión de K y $\alpha \in F$, sea $K[\alpha]$ el subanillo de F formado por todas las expresiones polinomiales en K.

$$f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 \tag{10.1}$$

donde $a_i \in K$.

Entonces $K[\alpha]$ es un Dominio de Integridad que contiene a K y al elemento α.

El cuerpo de cociente de este Dominio de Integridad, formado por los cocientes de las expresiones del tipo (**??**), lo denotamos por U_α.

Es claro entonces que U_α es una extensión de K que contiene a α, y por lo tanto está contenido en $K(\alpha)$. Por otro lado, si L es una extensión de K que contiene a α, entonces debe contener todas las expresiones del tipo $a_n\alpha^n + \cdots + a_1\alpha + a_0$. Como L es un cuerpo, se tiene que L contiene todos los cocientes de dichas expresiones y por lo tanto L contiene a U_α. Luego U_α y $K(\alpha)$ son la misma cosa. Hemos demostrado entonces

Proposición 10.3.1 *Sea K un cuerpo y α un elemento en una extensión de K. Entonces $K(\alpha)$ consiste en todas las formas racionales*

$$\frac{f(\alpha)}{g(\alpha)}$$

donde $f(\alpha), g(\alpha)$ están en $K[\alpha]$ y $g(\alpha) \neq 0$

Definición 10.3.4 *Sea F una extensión de K. Un elemento $\alpha \in F$ se dice* **algebraico sobre** *K si α satisface una ecuación polinomial*

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

con $a_i \in K$.

Observación: Si α es algebraico sobre K, entonces α puede ser raíz de muchos polinomios con coeficientes en K, y entonces el polinomio f en la definición anterior no es único.

Sin embargo hay un polinomio especial, entre los polinomios que anulan a α, que merece particular antención.

Definición 10.3.5 *Sea α algebraico sobre K. Entonces el* **polinomo minimal de** *α, es el polinomio mónico, de grado mínimo que anula a α.*

Observación: Si $f(x)$ es el polinomio minimal de α, entonces $f(x)$ es irreducible sobre $\mathcal{Q}$. Si $f(x)$ es reducible entonces $f(x) = p(x)q(x)$, y entonces ambos polinomios $p(x)$ y $q(x)$ son mónicos. Además alguno de ellos anula a α y esto contradice la minimalidad de $f(x)$.

Ejemplo: Sea $\alpha = 1 + \sqrt{2}$, el cual es algebraico sobre $\mathcal{Q}$. El polinomio minimal de α viene dado por:

$$f(x) = x^2 - 2x - 1$$

Definición 10.3.6 *Sea α algebraico sobre K. Entonces diremos que α es* **algebraico de grado** *n, si el grado del polinomio minimal de α es n.*

Teorema 10.3.1 *Sea α algebraico sobre K de grado n. Entonces el grado de $K(\alpha)$ sobre K es n.*

Demostración: Sea $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ el polinomio minimal de α, el cual es irreducible, y consideremos el Dominio de Integridad $K[\alpha]$, formado por todas las expresiones del tipo:

$$b_m\alpha^m + \cdots + b_1\alpha + b_0$$

donde $b_i \in K$.

Notemos que α satisface el polinomio $f(x)$ y por lo tanto

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

Esta última expresión, nos permite reducir toda potencia de α de grado n o superior, a una combinación lineal de los elementos $\alpha^{n-1}, \ldots, \alpha, 1$. Luego

$$K[\alpha] = \{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 \cdot 1 \mid b_i \in K\}$$

Afirmamos además que $K[\alpha]$ es un cuerpo, para lo cual probaremos que todos los inversos de los elementos de $K[\alpha]$ están en $K[\alpha]$.

En efecto, sea $t = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$ un elemento en $K[\alpha]$ distinto de cero. Entonces el polinomio $g(x) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ es primo relativo con $f(x)$, pues $f(x)$ es irreducible y $f(x)$ no divide a $g(x)$. Luego existen polinomios $q(x)$ y $s(x)$ en $\mathcal{Q}[x]$, tales que

$$f(x)q(x) + g(x)s(x) = 1$$

Sustituyendo esta expresión en el valor de $x = \alpha$, tenemos

$$f(\alpha)q(\alpha) + g(\alpha)s(\alpha) = 1$$

Teniendo en cuenta que $f(\alpha) = 0$, se deduce

$$g(\alpha)s(\alpha) = 1$$

o sea

$$t \cdot s(\alpha) = 1$$

lo cual implica que $t^{-1} = s(\alpha) \in K[\alpha]$.

Por lo tanto, hemos probado que $k[\alpha]$ es un cuerpo y su cuerpo de cocientes es igual a si mismo. Por lo tanto $K(\alpha) = K[\alpha]$.

Para finalizar mostraremos que los elementos $1, \alpha, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)$ sobre K. Para probar esto, sólo nos falta verificar que estos elementos son linealmente independientes.

Supongamos que

$$C_{n-1}\alpha^{n-1} + \cdots + C_1\alpha + C_0 \cdot 1 = 0$$

para algunos elementos $C_i \in K$.

Luego el polinomio $f'(x) = C_{n-1}x^{n-1} + \cdots + C_1x + C_0$ es de grado menor que el grado de $f(x)$ y además anula a α. Esto contradice la minimalidad de $f(x)$ y por lo tanto $C_{n-1} = C_{n-2} = \cdots = C_1 = C_0 = 0$.

Los elementos $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forman una base de $K(\alpha)$ sobre K y por lo tanto

$$[K(\alpha) : K] = n$$

Con esto se da fin a la prueba.

♠

Teorema 10.3.2 *Sea K un cuerpo y $K(\alpha)$ una extensión finita de grado n. Entonces α es algebraico de grado n sobre K.*

Demostración: Consideremos los elementos $1, \alpha, \alpha^2, \ldots, \alpha^n$ en $F(\alpha)$. Puesto que la dimensión del espacio $K(\alpha)$ sobre K es n, estos $(n+1)$ elementos son linealmente independientes. Luego existen elementos $a_0, a_1, \ldots, a_n$ en K, no todos nulos, tales que

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 \cdot 1 = 0$$

Luego α es algebraico sobre K. El grado del polinomio minimal de α es menor o igual a n. Si suponemos que el grado de este polinomio es

$m < n$, entonces por el teorema anterior se deduce $[K(\alpha) : K] = m < n$, lo cual es una contradicción. Luego α es algebraico de grado n.

♠

Nuestro próximo paso será probar que el conjunto de los elementos algebraicos sobre un cuerpo K, es un cuerpo. Antes necesitamos el siguiente resultado.

Proposición 10.3.2 *Sea K un cuerpo y F una extensión finita de K. Sea L una extensión finita de F. Entonces L es una extensión finita de K y además: $[L : K] = [L : F][F : K]$.*

Demostración: Sea $[F : K] = n$ y $[L : F] = m$. Sean $\{x_1, \ldots, x_n\}$ una base de F sobre K, y $\{y_1, \ldots, y_m\}$ una base de L sobre F.

Probaremos que $\{x_i y_j\}$ $1 \leq i \leq n$, $1 \leq j \leq m$, es una base de L sobre K.

Sea $l \in L$. Entonces existen elementos $l_1, \ldots, l_m$ en F, tal que

$$l = l_1 y_1 + \cdots + l_m y_m \tag{10.2}$$

Como los l_i están en F, para cada l_i existen elementos $k_{ij} \in K$, tales que

$$l_i = k_{i1} x_1 + \cdots + k_{in} x_n, \quad \text{para todo} \quad 1 \leq i \leq m \tag{10.3}$$

Sustituyendo estos valores de l_i en la expresión (**??**) obtenemos

$$l = k_{11} x_1 y_1 + \cdots + k_{m1} x_1 y_m + \cdots + k_{1n} x_n y_1 + \cdots + k_{mn} x_m y_n$$

Luego los elementos $\{x_i y_j\}$ son un conjunto de generadores de L sobre K.

Supongamos que para algunos elementos a_{ij} en K, $1 \leq i \leq n$, $1 \leq j \leq m$, no todos nulos, se tiene

$$(a_{11} x_1 y_1 + \cdots + a_{1m} x_1 y_m) + \cdots + (a_{n1} x_n y_1 + \cdots + a_{nm} x_n y_m) = 0$$

Luego reagrupamos estos elementos para obtener

$$(a_{11}x_1 + a_{21}x_2 + \cdots + a_{n1}x_n)y_1 + \cdots + (a_{1m}x_1 + \cdots + a_{nm}x_n)y_m = 0$$

Como $x_i \in F$ para todo $1 \leq i \leq n$ y $a_{ij} \in K \subseteq F$, se tiene que los elementos

$$C_j = a_{1j}x_1 + \cdots + a_{nj}x_n, \qquad 1 \leq j \leq m$$

están todos en F, pues F es un cuerpo.

Luego se tendrá la combinación lineal

$$C_1y_1 + \cdots + C_my_m = 0$$

Como los $y_1, \ldots, y_m$ son linealmente independientes sobre F, se deben anular todos los C_i. Por lo tanto

$$C_k = 0, \quad \text{para todo} \quad 1 \leq k \leq m$$

o sea

$$a_{1j}x_1 + \cdots + a_{nj}x_n = 0, \qquad 1 \leq j \leq m$$

Nótese que los a_{ij} están en K y los elementos $x_1, \ldots, x_n$ son linealmente independientes sobre K. Luego se deduce de esto que $a_{ij} = 0$ para todo $1 \leq i \leq n$, $1 \leq j \leq m$.

En conclusión hemos probado que el conjunto $\{x_iy_j\}$ constituye una base de L sobre K, la cual tiene $m.n$ elementos. Luego $[L : K] = m.n$. Con esto queda probado la proposición.

♠

Teorema 10.3.3 *Sea K un cuerpo, y F una extensión de K. Entonces el conjunto de elementos de F que son algebraicos sobre K es un subcuerpo de F.*

Demostración: Sea $\mathcal{A}$ el conjunto de los elementos de F que son algebraicos sobre K. Para probar que $\mathcal{A}$ es un cuerpo basta tomar un par de elementos cualquiera a y b en $\mathcal{A}$, y demostrar

i) $a \pm b$ está en $\mathcal{A}$
ii) ab está en $\mathcal{A}$
ii) a/b está en $\mathcal{A}$, si $b \neq 0$

Sea $T = K(a)$ y $L = T(b)$. Entonces $a \in L$ y $b \in L$. Por ser L un cuerpo se tiene que $a \pm b \in L$, $ab \in L$ y $a/b \in L$, si $b \neq 0$.

Luego $[K(a+b) : K] \leq [L : K] = [L : T][T : K]$

Ahora bien, como b es algebraico sobre K, de grado n, digamos, entonces b es algebraico sobre $K(a)$, de grado $\leq n$. Luego

$$[L : T] = [T(b) : K(a)] \leq n$$

Sabemos también que a es algebraico sobre K, de grado m digamos. Luego

$$[T : K] = [K(a) : K] = m$$

Por lo tanto

$$[K(a+b) : K] \leq m.n$$

Luego $K(a+b)$ es una extensión finita de K, y por el teorema **??**, se tiene que $a+b$ es algebraico sobre K. De igual forma se prueba que los elementos $a-b$, ab y a/b son algebraicos sobre K.

♠

Definición 10.3.7 *Una extensión F de K se dice* **extensión algebraica**, *si todos los elementos de F son algebraicos sobre K.*

Definición 10.3.8 *Un número complejo c se dice* **número algebraico**, *si c es algebraico sobre $\mathcal{Q}$. Caso contrario diremos que c es un* **número trascendente**.

El teorema **??** establece entonces, en el caso $k = \mathcal{Q}$, que el conjunto de los números algebraicos es un cuerpo. Este cuerpo está contenido en $\mathcal{C}$, pero es diferente de $\mathcal{C}$, pues existen números reales que no son algebraicos como por ejemplo π y e.

Si α es un elemento algebraico sobre $\mathcal{C}$, entonces α es raíz de algún polinomio con coeficientes complejos, y por el Teorema Fundamental del Algebra, se tiene que $\alpha \in \mathcal{C}$. Luego el cuerpo de los elementos algebraicos sobre $\mathcal{C}$ es precisamente $\mathcal{C}$.

Definición 10.3.9 *Un cuerpo F se dice* **algebraicamente cerrado** *si todo elemento algebraico sobre F, está en F.*

Podemos establecer entonces el siguiente resultado.

Teorema 10.3.4 *El cuerpo de los números complejos es algebraicamente cerrado.*

Ejercicios

1) Sea r un número racional, y supongamos que $\sqrt{r} \notin \mathcal{Q}$. Probar que

$$\mathcal{Q}(\sqrt{r}) = \{a + b\sqrt{r} \mid a, b \in \mathcal{Q}\}$$

es una extensión algebraica de $\mathcal{Q}$, de grado 2.

$\mathcal{Q}(\sqrt{r})$ se llama **cuerpo cuadrático** generado por $\sqrt{r}$.

2) Probar que todo cuerpo cuadrático es de la forma $\mathcal{Q}(\sqrt{d})$, donde d es un entero libre de cuadrados.

3) Si $s = a+b\sqrt{d} \in \mathcal{Q}(\sqrt{d})$, entonces **la traza y la norma** del elemento x, se definen por

$$\begin{aligned} Tr(s) &= s + \overline{s} = 2a \\ N(s) &= s.\overline{s} = a^2 - db^2 \end{aligned}$$

Probar que para cualquier par de elementos s y t en $\mathcal{Q}(\sqrt{d})$ se tiene

i) $Tr(s+t) = Tr(s) + Tr(t)$
ii) $N(s.t) = N(s)N(t)$

4) Un elemento s en $\mathcal{Q}(\sqrt{d})$ se denomina **entero algebraico**, si satisface un polinomio mónico con coeficientes en $\mathcal{Q}$.

Demuestre que s es un entero algebraico, si y sólo si $Tr(s)$ y $N(s)$ son enteros.

5) Demuestre que el conjunto de los enteros algebraicos de $\mathcal{Q}(\sqrt{d})$ es un anillo.