UNIVERSIDAD DE GRANADA

Facultad de Ciencias. Grado en Matemáticas

Trabajo de fin de Grado

Operadores de dimensión

Autor: Marina Malagón Delgado
Tutor: Pascual Jara Martínez
Departamento de Álgebra

Curso académico 2021-2022

Operadores de dimensión

Marina Malagón Delgado

Marina Malagón Delgado. *Operadores de dimensión.*
Trabajo de fin de Grado. Curso académico 2021-2022.

Responsable de tutorización:
Pascual Jara Martínez. *Departamento de Álgebra.*

Grado en Matemáticas. Facultad de Ciencias. Universidad de Granada.

Declaración de originalidad.

Declaro la originalidad del Trabajo de Fin de Grado, en el cual se han citado debidamente las fuentes utilizadas para su elaboración.

En Granada, a 7 de junio de 2022.

Fdo: Marina Malagón Delgado.

A mi familia y a mis amigos
por su apoyo y ayuda para conseguir mi sueño,
por permanecer cuando otros se han marchado
y darme luz cuando más apagada estaba.
Dedicación especial a mi tutor, Pascual,
por su gran implicación en este trabajo
y la ayuda aportada para realizarlo.

Índice

Abstract

In this work we make an approach to the notion of dimension, and in particular to the transcendental dimension on Field Theory.

Dimension Theory is a useful tool in Mathematics, from the ancient times people need to compare size of different objects. They assume that a point and a rule have different size and the same happens with sections of the plane. This was the first approach to the dimension of geometrical objects made by the Greeks.

This notion of dimension was questioned after the work of G. Cantor on cardinally and Set Theory. Indeed, Cantor shows that a segment in the real line is equipotent with the unit square in the plane. This means that an object of dimension one is equipotent with an object of dimension two.

At the end of the XIX'th century this misunderstanding trouble was overcome introducing a new and different concept of equipotence. With this new geometrical and topological notion of dimension the next step was to give the algebraic counterpart. This coming through Algebraic Geometry take advantage of the Clasical Geometry. Thus the notion of dimension in Conmutative Algebra as the length of chains of prime ideal nuddenly appears.

We still need one more step to reach the transcendental dimension in field theory. The connection between dimension in Conmutative Algebra and Field Theory come from the hand of Noether's Normalizing Theorem. Thus an integral algebraic domain D, over a field K, has algebraic dimension d whenever the field of fraction of D has transcendental dimension d.

After this quick tour on the evolution of Dimension Theory and in order to establish a foundation of it, I focus the content of this memory in developing an abstract theory of dimension starting from the well known dimension theory of vector spaces and applying to the transcendental dimension of field extensions. New developes and applications on this abstract theory are actually been studied, see for instance [13, Cap.14], but these are out of our interests now.

This memory is divided in chapters. In chapter one I give a quick background on the develop and antecedents on Dimension Theory. I will make a summary of the beginnings and I will name the most influential mathematicians related to this theory.

In chapter two, I introduce an axiomatic approach to an abstract dimension theory and study the well known example of Lineal Algebra and vector spaces.

Chapters three to five are devolved to the study of field extension focusing on transcendental extensions; a subject which usually is not included in undergraduate courses in Algebra. We will begin by giving its definition and classifying depending on the elements between algebraic extensions and transcendental extensions. Our goal is to delve into the latter to give the concept of transcendence degree and relate it to the idea of vectorial dimension. Next, we are going to cover the definitions seen from another perspective, that of the dimension operators, to finally arrive at the same results obtained previously. Later, we will deal with a special class of extensions, the separable/inseparable ones. Prior to this, we will study certain closely bound element sets with separability, the linearly disjoint sets. After that, we will give results that will relate both concepts.

In chapter six I give some tapas on applications and related results involving transcendental extensions.

The memory finishes with a conclusions chapters, used references and a glossary or index on the terms used in it.

Introducción

En este trabajo realizamos una aproximación a la noción de dimensión, y en particular a la dimensión trascendente en la Teoría de Cuerpos.

La Teoría de la Dimensión es una herramienta útil en Matemáticas. Desde la antigüedad, las personas tienen necesidad de comparar el tamaño de diferentes objetos. Se sabe que un punto y una recta tienen distinto tamaño, y lo mismo ocurre con las secciones del plano. Este es el primer acercamiento a la dimensión de los objetos geométricos realizado por los griegos.

Esta noción de dimensión es cuestionada a partir del trabajo de G. Cantor sobre cardinalidad y Teoría de Conjuntos. De hecho, Cantor muestra que un segmento en la recta real es biyectivo al cuadrado unitario. Esto significa que un objeto unidimensional es equipotente con un objeto bidimensional.

A finales del siglo XIX se superó este malentendido introduciendo un nuevo concepto diferente al de equipotencia. Con una nueva noción geométrica y topológica de dimensión, el siguiente paso fue dar una noción algebraica. Esto proveniente de la Geometría Algebraica aprovecha la Geometría Clásica. Así, aparece la noción de dimensión en Álgebra Conmutativa definida como la longitud de cadenas de ideales primos.

Todavía necesitamos un paso más para tratar con la dimensión trascendental. La conexión entre dimensión en Álgebra Conmutativa y teoría de cuerpos viene de la mano del teorema de normalización de Noether. Un dominio algebraico integral D, sobre un cuerpo K, tiene dimensión algebraica d siempre que el cuerpo de fracciones de D tenga dimensión trascendente d.

Después de este rápido recorrido por la evolución de la Teoría de la Dimensión y con el fin de establecer un fundamento de la misma, enfoco el contenido de esta memoria en desarrollar una teoría abstracta de la dimensión partiendo de la conocida Teoría de la Dimensión en espacios vectoriales y desarrollando el concepto de dimensión trascendental de extensiones de cuerpos. Actualmente se están estudiando nuevos desarrollos y aplicaciones de esta teoría abstracta, ver por ejemplo [13, Cap.14], pero estos están fuera de nuestro interés ahora.

Este trabajo está dividido en capítulos. En el capítulo uno doy una breve introducción sobre el desarrollo y los antecedentes de la Teoría de la Dimensión.

En el capítulo dos presento un enfoque axiomático de una teoría de dimensión abstracta y estudio el conocido ejemplo de Álgebra Lineal y espacios vectoriales.

En los capítulos del tres al cinco me dedico al estudio de las extensiones de cuerpos y me centro en las extensiones trascendentes, un tema que generalmente no se incluye en los cursos de grado en Álgebra. Comenzamos dando la definición de extensión y clasificando, según los elementos, entre extensiones algebraicas y extensiones trascendentes. Nuestro objetivo es profundizar en estas últimas para dar el concepto de grado de trascendencia y relacionarlo con la idea de dimensión vectorial. A continuación, abarcaremos las definiciones vistas desde otra perspectiva, la de los operadores de dimensión, para llegar finalmente a los mismos resultados obtenidos anteriormente. Más adelante nos ocuparemos de una clase especial de extensiones, las separables. Antes de esto, estudiaremos ciertos conjuntos de elementos estrechamente ligados con la separabilidad, los conjuntos linealmente disjuntos. Después, daremos resultados que relacionarán ambos conceptos.

En el capítulo seis doy algunas tapas sobre aplicaciones y resultados relacionados que involucran extensiones trascendentales.

La memoria finaliza con capítulos de conclusiones, referencias utilizadas y un glosario o índice de los términos utilizados en el trabajo.

1. Teoría de la dimensión

Cuando se habla de dimensiones se hace referencia a las formas en que un objeto puede ser medido. También se hace alusión a las direcciones en las que es posible el movimiento.

Un habitante en un mundo formado por un punto no podría moverse de ninguna forma. No existe desplazamiento en ninguna dirección y no podemos medir. En cambio, sí tenemos una medida cuando estamos en un universo formado por una línea recta. Aquí hay una dirección en la que movernos, la determinada por la recta, y podemos medir a través de longitudes.

En el plano es posible el desplazamiento en infinitos sentidos, los cuales pueden ser interpretados como la suma de movimientos en dos direcciones. En este caso, el plano tiene dimensión dos y es posible la existencia de objetos que no son posibles en las dimensiones cero y uno (triángulos, cuadrados, círculos) que llamamos figuras planas. Aquí medimos longitud y anchura.

Añadiendo una dirección más pasamos al espacio tridimensional, donde es posible la existencia de figuras que llamaremos sólidos (cubo, cilindro, pirámide) que en las anteriores no tenían cabida. Aquí añadimos la profundidad.

¿Existen más de tres dimensiones? ¿Qué entendemos verdaderamente por dimensión? ¿Dirección del movimiento posible de un objeto? Vamos a hacer un estudio conciso, con ayuda de las referencias [6] y [7], que trate de dar respuesta al origen de toda una teoría de la dimensión y nos aproxime al concepto de dimensión.

1.1. Cardinalidad

Las primeras menciones al concepto de dimensión surgen con los antiguos griegos, con el problema cosmológico de explicar la perspectiva física del espacio. Estos sabios no hicieron un estudio detallado sobre la Teoría de la Dimensión, aunque ya empezaron a involucrarse con problemas conceptuales relacionados con tal magnitud, ideas y teorías despreocupadas.

Los primeros pitagóricos plantearon explicar las figuras geométricas que ellos podían percibir (puntos, líneas, superficies y sólidos) a través de números. Así, el punto lo describieron con el 1, la línea con el 2, el 3 lo usaron para el triángulo y el 4 para la pirámide, estableciendo que toda figura se podía conseguir a partir de estas.

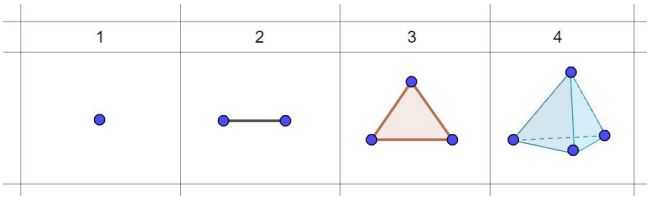

Figura 1: Dimensión para los griegos

Pitagóricos más tardíos, como Nicomachus, nombraron explícitamente la idea de dimensión. Consideraron el 1 adimensional porque no suponía aporte cuando se añadía un punto a un punto. El 2 lo dotaron de dimensión uno, dado que una línea se puede extender en una dirección. Bidimensionales serían las superficies, las cuales se extienden en dos direcciones. Finalmente, los sólidos que se extienden en tres direcciones serían tridimensionales.

En el libro de Euclides se enuncia que un punto es lo que no tiene parte, una línea es de longitud sin anchura, una superficie es lo que tiene largo y ancho, y un sólido es lo que tiene largo, ancho y profundidad. Aditivamente, los extremos de una recta son puntos, los de una superficie son líneas y los de un sólido son superficies. Euclides nombra la dimensión de figuras geométricas.

Aristóteles, no muy conforme con los conceptos dimensionales de Euclides, propuso su propia teoría de la dimensión basada en divisibilidad y continuidad. Con una nueva visión pitagórica, concibe la naturaleza como magnitudes y cuerpos, divisibles en todos los sentidos. La magnitud que se extiende en un sentido es la línea, y la que lo hace en dos es el plano. Por la percepción del ambiente tridimensional, Aristóteles asegura que no hay más magnitudes que las dichas.

La teoría de Euclides y la de Aristóteles ofrecen pocos detalles sobre la dimensión, pero nos dan una conexión entre tal concepto y las figuras geométricas. Éstas, junto con otras teorías griegas, llamaron la atención de matemáticos como Bolzano o Riemman y fueron punto de partida del estudio de otros que buscaron el origen de las ideas de dimensión, como Poincaré o Menger.

1.2. Dimensión geométrica

Sobre mediados del siglo XIX empiezan a desarrollarse teorías de dimensión más abstractas de la mano Grassmann, Cayley, Riemann y otros. Se consideraban espacios de más de tres dimensiones, hecho escapable de la percepción cotidiana, y que por tanto inducía a un cambio de la Geometría.

Ya había en la Antigua Grecia pensamiento sobre mayores dimensiones detrás de trabajos como los de Heron y Diofanto, quienes introdujeron incógnitas de dimensiones superiores. Sin embargo, no se atrevieron a ir más allá de la tradición. Siguiendo sus pasos, árabes y occidentales algebristas hablaron de espacios de más de tres dimensiones sin intención de introducirlos.

Fue Oresme, a mediados del siglo XIV, quien por primera vez describía una imagen tridimensional de un sólido cuatridimensional . Sobre el siglo XVI, M. Stifel señaló la incapacidad de la Geometría para progresar más allá de un sólido tridimensional mientras que al Álgebra no le ocurría esto. Así, con esta rama se podía establecer una nueva formulación geométrica del tema.

A partir del siglo XVIII se intensificó la idea de considerar hiperespacios. I. Kant consideró espacios de dimensiones superiores y examinó el problema tridimensional de la cosmología para explicar la naturaleza. Para abordar el tema que siglo antes ya trataron Galileo y Leibniz, Kant especuló con una ciencia de n-espacios. Sin embargo, fue D'Alembert quien insertó una idea más concreta de espacio de más de tres dimensiones unos años después.

Años más tarde, Lagrange siguió con el concepto de hiperespacio para explicar la mecánica como una geometría de cuatro dimensiones añadiendo el tiempo como la cuarta dimensión. A pesar de todas estas tomas de contacto multidimensional, nadie formuló ninguna teoría formal que ayudara a la comprensión de estos objetos impensables.

Gauss se interesó en el tema dimensional y quiso relacionar geometría abstracta (la que se ocupa de variedades n-dimensionales) con geometría concreta (la espacial tridimensional). Su actitud ante la Geometría es el principio de la nueva visión filosófica desarrollada en el siglo XIX de tal rama, por la cual comienzan a separarse Física y Geometría. Sus publicaciones sobre hiperespacios y problemas algebraicos, analíticos y geométricos atrajo a matemáticos al ámbito de la dimensión, entre ellos Grassmann y Riemann.

Grassmann veía que la Geometría, como rama de unas Matemáticas puras, no podía tener limitaciones dimensionales. En consecuencia, el pensamiento de Grassmann trascendía la Geometría cotidiana tridimensional y se inclinaba al estudio de espacios abstractos de dimensiones superiores. Con el mismo pensamiento filosófico, Riemman también hizo un estudio de hiperespacios; en 1868, introdujo el concepto topológico de variedad n-dimensional.

1.3. Cantor

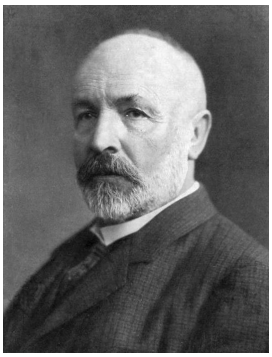

Figura 2: G.Cantor

La Teoría de la Dimensión adquirió novedad y relevancia cuando Cantor en 1877 puso en correspondencia biyectiva un segmento con un cuadrado. Con ello, surgió el problema de invarianza dimensional. Se quería desarrollar una teoría que justificara la posibilidad o imposibilidad de invarianza de dimensión respecto algún tipo de aplicaciones.

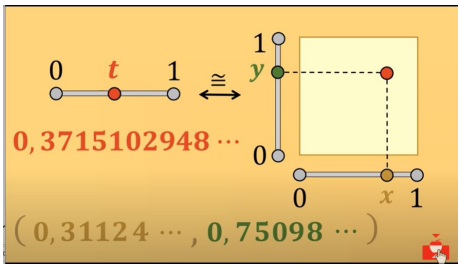

Figura 3: Biyección de Cantor (ver [15])

Cantor dio paso a un nuevo problema: visto que una biyección no era suficiente para mantener la dimensión, era preciso considerar más invariantes que la cardinalidad para tener la permanencia dimensional. Esta cuestión atrajo la atención de matemáticos y fue clave para el desarrollo de toda una teoría de la dimensión, formalización de conceptos y novedosos resultados.

El escaso conocimiento que se tenía de Topología aumentaba la dificultad del asunto, por entonces las demostraciones se sustentaban de métodos analíticos reales y Geometría básica. A pesar de ello, matemáticos contemporáneos a Cantor como J. Lüroth, J. Thomae, E. Netto o E. Jürgen consiguieron algunos avances para el problema.

Jürgen sobresalió por ser el primer matemático en aclarar la relación entre invarianza dimensional e invarianza del dominio. Este matemático dio la prueba en el caso plano, de dos dimensiones, de la invarianza dimensional.

Netto completó una prueba general de la invarianza dimensional en el ámbito topológico, mejorando la aportada por Thomae. Esta cuestión fue tratada al mismo tiempo por Cantor en sus correspondencias con Dedekind.

1.4. Dimensión topológica

El hecho de tener que considerar otros invariantes para conseguir resolver el problema de invarianza dio origen a una nueva materia: la Topología. Todos los intentos de 1878 y 1879 para probar la invarianza dimensional fueron fallidos porque se estaban usando métodos inadecuados debido a la falta de conocimientos topológicos. Sin embargo, la generalidad de matemáticos del momento no veían las deficiencias que presentaban las demostraciones realizadas y dieron por válida la prueba presentada por Netto dejando establecido el concepto de dimensión y conservación por aplicaciones.

1.4.1. Topología analítica

Cantor dio comienzo a la Teoría de Conjuntos de puntos, la cual provocó un progreso en la Topología a través de una nueva perspectiva del pensamiento y supuso un pilar fundamental para el desarrollo de la Topología analítica. El objetivo de Cantor era analizar el conjunto de puntos en el n-espacio euclidiano y sus características. Así, su teoría del continuo se convierte en base de la Topología de Conjuntos de puntos y establece conceptos como la conectividad y el conjunto cerrado.

Los analistas fueron los primeros en percatarse de que el pensamiento cantoriano provocó un desarrollo profundo de las Matemáticas. La Teoría de Conjuntos de puntos fue clave para el estudio y desarrollo de funciones reales y complejas a partir de las nuevas herramientas del análisis funcional.

En 1905, F. Riesz recurre a la dimensión de funciones para dar su noción de dimensión en espacios euclídeos. Además, postula que se conserva la dimensión entre conjuntos a partir de aplicaciones biyectivas continuas. En contraposición, parece que sus definiciones eran difíciles de aplicar para establecer el número dimensional.

Baire estableció teoremas sobre la invarianza dimensional y redujo tal cuestión al problema de demostrar una generalización del Teorema de separación de Jordan para el caso n-dimensinal, el cual no alcanzó a probar. Sus aportes al ámbito dimensional a través de límites y sucesiones tuvo gran repercusión matemática. Fue importante su presentación de que lo que llama el espacio de dimensión cero, formado por las sucesiones de números enteros, y la demostración de que tal espacio es homeomorfo al conjunto de los números irracionales. Es más, probó la homeomorfía de tal espacio con el conjunto de coordenadas irracionales en el espacio n-dimensional euclideano.

En 1910, M. Fréchet se incorporó al estudio de la dimensión introduciendo conceptos como el de homeomorfismo o el de espacio de Fréchet. Su teoría, parecida a la Teoría de Cardinales de Cantor y al estilo de Riesz, es apropiada para las comparaciones de espacios euclídeos y otros espacios. Fréchet dio ejemplo de espacio infinito-dimensional, aunque no se adentró en el estudio de estos espacios. Su aportación más relevante fue considerar dimensiones fraccionarias.

1.4.2. Topología geométrica

Las ideas de Cantor también tuvieron una gran repercusión en la Geometría, puestas en relevancia por G. Peano y C. Jordan. En el Teorema de la curva de Jordan aparece una sección dedicada a la Teoría de Conjuntos. Tal teorema adquirió importancia por ser visto por matemáticos como una vía para la solución del problema de la invarianza dimensional.

Peano, al igual que su rival Jordan, consideró la teoría cantoriana para sus ideas geométricas sobre el estudio de curvas y magnitudes geométricas como son lo que llama medida interior y exterior. Con la curva de Peano se produjo otro choque con la noción de dimensión, pues se estableció un aplicación continua (no biyectiva) entre un objeto de dimensión uno y otro de dimensión dos. Esto dio comienzo a lo que se conoce como Teoría de la curva topológica, la cual tiene una conexión estrecha con la Teoría de la Dimensión.

Jügens presentó de una forma más amena los problemas de la dimensión y acondicionó el camino para el desarrollo de los topólogos del siglo XX. A. Schoenflies dedujo más tarde, al igual que Jügens, la invarianza dimensional del dominio del plano usando el Teorema de Cantor. Este resultado lo quiso generalizar a cualquier espacio, pero se encontró con dificultades. Schoenflies se convirtió en un pionero del desarrollo de la Topología, a pesar de que sus ideas fueron refutadas por Brouwer y otros.

1.4.3. Topología algebraica

Los nuevos aportes de Topología y la dificultad de resolver el problema de invarianza llamaba a sabios a encontrar la solución a tal cuestión a partir de nuevos enfoques. Entre estos, destacan los de H. Poincaré.

Figura 4: Henri Poincaré

Poincaré se convirtió en promotor de la Topología algebraica que conocemos persiguiendo el análisis sobre las dimensiones. Su desarrollo surgió debido al estudio epistemológico de la naturaleza y origen geométrico, el cual veía íntegramente relacionado con el espacio. En 1890 expuso su primera teoría de la dimensión, la cual se basaba en Teoría de Grupos, y posteriormente lanzó su segunda teoría, esta vez basada en la Topología.

La primera de sus teorías usaba el grupo de transformaciones y sus subgrupos. Poincaré delató en uno de sus artículos las imperfecciones de la definición de dimensión a partir de la Teoría de Grupos, entre ellas la falta de atracción intuitiva. En consecuencia, Poincaré cambió a un enfoque topológico para dar el concepto dimensional a partir de lo que él denominó corte. En esta cree dar solución a la paradoja de Cantor, pues se añade que la continuidad es condición necesaria de la aplicación para la invarianza dimensional.

El concepto de dimensión que emplea Poincaré, a partir de los cortes, es mediante recursividad. Así, se dirá que un continuo es n-dimensional cuando se puede fragmentar en partes por cortes $(n-1)$-dimensionales continuos.

1.5. El problema de invarianza dimensional

1.5.1. Brouwer

Tras los fallidos intentos de los numerosos matemáticos anteriormente nombrados, L.E.J. Brouwer logró dar en 1911 la primera demostración generalizada de la estabilidad dimensional aceptable. Brouwer conocía de los invariantes punto límite, conexión, dominio, frontera, curvas y arcos. Además, consideró el grado de una función y el concepto de homotopía en esferas. También proporcionó una prueba para el Teorema de la curva de Jordan.

Figura 5: L.E.J. Brouwer

En el mismo año de la prueba de Brouwer, Lebesgue lanzó su demostración de la invarianza. Brouwer, lleno de ambición por la superioridad y popularidad matemática, buscó errores y tachó la prueba de inadecuada. Esto fue el principio de la confrontación entre ambos matemáticos por conseguir la primicia de la solución del problema dimensional.

Brouwer quiso seguir los pasos de Poincaré para su teoría de la dimensión. Reforzó el concepto de continuo en dimensión arbitraria y la noción de corte, pero encontró dificultades y fallos que lo obligaron a abandonar el camino de Poincaré y formar el suyo propio. Su definición pasaba a basarse en el concepto de separación y se presentaba de un modo inductivo, lo que suponía una mejora de la informal definición de Poincaré con los cortes.

Tres matemáticos fueron los que tuvieron influencia en Brouwer. El primero era Schoenflies, por el cual Brouwer se introdujo al ámbito topológico para solventar sus deficiencias. El segundo influyente fue Hadamard, quien ofreció a Brouwer el grado de una aplicación continua. Finalmente, el tercer contribuyente fue Lebesgue a partir del cual tomó ideas, críticas y mejoras.

1.5.2. Urysohn y Menger

Tras la repercusión de Brouwer se dejó a un lado el interés por el concepto de dimensión. Es en 1921 cuando empieza de nuevo a adquirir importancia con los aportes de P. Urysohn y K. Menger. También en esa fecha consiguió Lebesgue publicar la correcta prueba de su principio del mosaico, con la invarianza dimensional como una de sus consecuencias.

Previo a 1921 podemos encontrar resultados destacables como la caracterización de forma teórica de la medida de la dimensión, realizada por F. Hausdorff en 1919. Este matemático mostró una teoría menos topológica y más métrica. También es relevante la fundación en 1920 de un escuela polaca de Teoría de Conjuntos y Topología que trajo avances en cuestiones topológicas que serían luego importantes para el estudio dimensional. En ese mismo año se hizo un refuerzo en la teoría de curvas, que fue determinante para las investigaciones de Urysohn y Menger sobre la dimensión.

Figura 6: Pavel Urysohn

Urysohn se centró en la definición de dimensión a partir de problemas de curvas y superficies. Dio una definición inductiva en términos métricos que mostraba que era un invariante topológico. Obtuvo grandes resultados para el espacio de dos y tres dimensiones y para tratar con dimensiones superiores recurrió al principio del mosaico de Lebesgue.

No satisfecho, demostró resultados como es la dimensión de la unión de espacios y definió conceptos como variedad cantoriana de dimensión dada. Su trabajo significó una indagación y elevación de la teoría abstracta en espacios métricos y topológicos. Junto con Alexandroff, contribuyó relevantemente a la Topología general.

Figura 7: Karl Menger

En el mismo año, al igual que Urysohn e independientemente, Menger se preocupó por dar una definición correcta de curva y estableció relación con la noción de dimensión. Definió esta última a partir de la corrección de la dada por Poincaré en su artículo de 1912. Para los teoremas dimensionales usó el método de modificación de un barrio en la vecindad de sus límites.

Menger sigue un camino similar a Urysohn y obtiene resultados y nociones similares a tal matemático (noción de curvas, superficies, uso del mosaico de Lebesgue, variedad cantoriana, teorema de la suma).

Tenemos que destacar que tanto Brouwer como Urysohn y Menger definen adecuadamente, de manera inductiva, el concepto de dimensión y emplean para ello las últimas herramientas topológicas descubiertas. Las definiciones dadas por estos matemáticos son equivalentes para espacios métricos separables, sin embargo divergen más allá de tales espacios. Actualmente, se toma la definición de Urysohn-Menger por su aproximación a la idea intuitiva dimensional y los elegantes teoremas que encierra.

La divergencia del concepto de dimensión dependiendo del espacio considerado demuestra que no hay una definición universal ni teoría única general válida para todos los ámbitos. Se toman aquellos conceptos y resultados correctamente formulados que tienen mayor repercusión en otras áreas de las Matemáticas. Todos ellos conforman la Teoría de la Dimensión.

1.6. Dimensión algebraica

Más allá de las definiciones de dimensión dadas y argumentadas por matemáticos en Geometría y Topología, podemos dar la versión algebraica de la misma sirviendo como puente la Geometría Algebraica y su relación con el Álgebra Conmutativa. Para ello, vamos a ver cómo influye el número de indeterminadas.

Sea K cuerpo y $K[X]$ el anillo de polinomios, notaremos por $P(K)$ al conjunto de partes de K (familia de subconjuntos de K) y por $\mathrm{Id}(K[X])$ al conjunto formado por los ideales de $K[X]$. Con esta notación, consideramos la aplicación $\phi : \mathrm{Id}(K[X]) \longrightarrow P(K)$ tal que a cada ideal maximal de $K[X]$ le hace corresponder sus raíces en K. Se tiene que $\phi(X - \alpha) = \alpha$ y si $\mathcal{P} \subseteq K[X]$ tenemos $\phi(\mathcal{P}) = \{x \in K |\ p(X) = 0, \forall p \in \mathcal{P}\}$ conjunto de ceros de $\mathcal{P}$ (o conjunto algebraico definido por $\mathcal{P}$). Si consideramos $K = \mathbb{R}$ entonces ϕ no establece una buena relación dado que, por ejemplo, $1, (X^2 + 1) \in \phi^{-1}(\emptyset)$. Sin embargo, tomando $K = \mathbb{C}$ no tendremos problema. En efecto, los ideales primos de $\mathbb{C}$ son de la forma $X - \alpha$ y para cada uno tendremos por correspondencia biyectiva vía ϕ al elemento α de $\mathbb{C}$ y viceversa. Esto que ocurre con $\mathbb{C}$ es válido para cualquier otro cuerpo algebraicamente cerrado.

Podemos extender esta situación a dimensiones mayores. Seguiremos considerando el cuerpo de los complejos para una comprensión más amena. Sea ahora $\Phi : \mathrm{Id}(\mathbb{C}[X_1, \ldots, X_n]) \longrightarrow P(\mathbb{C}^n)$ definida utilizando los conjuntos de ceros. A un conjunto $\mathcal{P} \subseteq \mathbb{C}[X]$ le hacemos corresponder $\Phi(\mathcal{P}) = \{x \in \mathbb{C} |\ p(X) = 0, \forall p \in \mathcal{P}\}$ conjunto de ceros de $\mathcal{P}$. Tenemos una biyección entre los ideales radicales y los conjuntos algebraicos (o variedades). Parece razonable considerar la dimensión de $\mathbb{C}[X_1, \ldots, X_n]$ como el número de indeterminadas, n. Esto es así ya que al ideal $\{0\}$ le corresponde el conjunto algebraico $\mathbb{C}^n$ y al ideal $\mathbb{C}[X_1, \ldots, X_n]$ el conjunto algebraico $\emptyset$, y desde el punto de vista geométrico $\mathbb{C}^n$ tiene dimensión n.

Dado un conjunto irreducible $V \subseteq \mathbb{C}$, el ideal $I(V) \subseteq \mathbb{C}[X_1, \ldots, X_n]$ es un ideal primo. En consecuencia, el anillo cociente $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I(V)}$ es un dominio de integridad, llamado anillo de coordenadas de V. Este anillo refleja lo que le pasa a V, por lo que se verifica que $\dim(\frac{\mathbb{C}[X_1,\ldots,X_n]}{I(V)})$ equivale a $\dim(V)$. Estamos relacionando dimensión algebraica con geométrica. La dimensión algebraica de $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I(V)}$ es la longitud máxima de las cadenas de ideales primos. Este número podemos obtenerlo también utilizando la Teoría de Cuerpos, ya que es la dimensión trascendente de la extensión del cuerpo de fracciones de $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I(V)}$ sobre $\mathbb{C}$.

2. Espacios vectoriales

Comenzamos con un breve repaso de los conceptos básicos y de los resultados más relevantes del Álgebra Lineal. Nos ayudaremos de [11] y [12] para la exposición de esta sección, en la cual nos limitamos a lo más básico y notorio sobre espacios vectoriales para luego hacer comparación con la teoría que pretendemos desarrollar.

2.1. Teoría de la dimensión abstracta de Steinitz

Definición 2.1. Sea V un conjunto no vacío y K un cuerpo, se dice que V es un **espacio vectorial sobre** K si existen dos operaciones $+ : V \times V \longrightarrow V$ y $\cdot :\ K \times V \longrightarrow\ V$ tales que para todo $u, v, w \in V$ y para todo $\lambda, \mu \in K$:

(1) Propiedad asociativa: $u + (v + w) = (u + v) + w$.
(2) La operación $+$ tiene **elemento neutro** $0 \in V$, elemento que verifica las relaciones $u + 0 = u = u + 0$.
(3) La operación $+$ tiene **elemento opuesto** para cada elemento u de V, a saber, $-u \in V$ que verifica las relaciones $u + (-u) = 0 = (-u) + u$.
(4) Propiedad conmutativa: $u + v = v + u$.
(5) Propiedad pseudodistributiva $\lambda(u + v) = \lambda u + \mu v$.
(6) Propiedad pseudodistributiva $(\lambda + \mu)u = \lambda u + \mu u$.
(7) Propiedad pseudoasociativa $\lambda(\mu u) = (\lambda\mu)u$.
(8) Existe un elemento neutro para la acción: $1 \in K$ que verifica las relaciones $1u = u = u1$.

Definición 2.2. Llamaremos **vectores** a los elementos de V y **escalares** a los elementos de K.

Ejemplo 2.3. Sea $n \in \mathbb{N}$ y K cuerpo, se tiene que $K^n = K \times \overset{n)}{\cdots} \times K$ es un espacio vectorial con las operaciones suma $(u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1+v_1, \ldots, u_n+v_n)$ y producto por un escalar $\lambda(v_1, \ldots, v_n) = (\lambda v_1, \ldots, \lambda v_n)$, siendo $(u_1, \ldots, u_n), (v_1, \ldots, v_n) \in K^n$ y $\lambda \in K$.

Ejemplo 2.4. Sea K un cuerpo, entonces el anillo de polinomios $K[X]$ es un espacio vectorial sobre K con las operaciones suma $(p+g)(x) = p(x)+g(x)$ y producto por un escalar $(\lambda p)(x) = \lambda p(x)$, donde $p(x), g(x) \in K[X]$ y $\lambda \in K$.

Desde este momento, en toda esta sección V será un espacio vectorial sobre un cuerpo K.

Definición 2.5. Llamamos **combinación lineal** de vectores $v_1, \ldots, v_r$ de V a una expresión de la forma: $\lambda_1 v_1 + \cdots + \lambda_r v_r$ con $\lambda_1, \ldots, \lambda_r \in K$ escalares.

Definición 2.6. Sea $S = \{u_1, \ldots, u_r\} \subseteq V$ una familia de vectores, definimos el **subespacio generado** por S como el conjunto de todas las combinaciones lineales que pueden formarse con los elementos de S, a saber, $L(S) = \{\sum_{k=1}^{r} \lambda_i u_i |\ u_i \in S \text{ y } \lambda_i \in K\}$. Dicho conjunto es el mínimo subespacio vectorial de V que contiene a S.

Ejemplos 2.7. (A) Sea $v \in V$, entonces $L(v) = \{\lambda v |\ \lambda \in K\}$ consta de copias de v a diferentes escalas, esto es, múltiplos escalares de v.

(B) Considerando $e_1 = (1, 0, 0), e_2 = (0, 1, 0) \in \mathbb{R}^3$, se tiene que $L(\{e_1, e_2\}) = \{(\lambda_1, \lambda_2, 0) |\ \lambda_i \in \mathbb{R}\}$ es el plano $z = 0$ de $\mathbb{R}^3$.

Definición 2.8. Llamamos **sistema de generadores** de un subespacio $W \subseteq V$ a un subconjunto no vacío $S \subseteq W$ tal que $W = L(S)$. Esto es, todo elemento de W puede expresarse como combinación lineal de vectores de S.

Consideramos los siguientes ejemplos tomados de [12].

Ejemplo 2.9. Sea K un cuerpo y $n \in \mathbb{N}$, se tiene que $C = \{e_1, \ldots, e_n\} \subseteq K^n$ con $e_i = (0, \ldots, 0, \overset{(i)}{1}, 0, \ldots, 0)$ es un sistema de generadores de K^n. En efecto, todo elemento $(v_1, \ldots, v_n) \in K^n$ se puede escribir de la forma $\sum_{i=1}^{n} e_i v_i$ con $v_1, \ldots, v_n \in K$.

Ejemplo 2.10. Sea K un cuerpo, se tiene que $S = \{X^i |\ i \in \mathbb{N} \cup \{0\}\} \subseteq K[X]$ es un sistema de generadores de $K[X]$, pues cada polinomio $p(X) \in K[X]$ se puede escribir de la forma $p(X) = a_n X^n + \cdots + a_1 X + a_0$, con $a_n, \ldots, a_0 \in K$.

Definición 2.11. Se dice que un conjunto de elementos no nulos $S \subseteq V$ es **linealmente independiente** cuando para cualquier subcolección finita $\{u_1, \ldots, u_r\} \subseteq S$ la expresión $\lambda_1 u_1 + \cdots + \lambda_r u_r = 0$ implica $\lambda_1 = \cdots = \lambda_r = 0$. Lo que es igual, ningún vector de S es combinación lineal de otros vectores de S. En otro caso, se dice que el conjunto es **linealmente dependiente**.

Ejemplo 2.12. Se sigue que el conjunto C del Ejemplo (2.9.) es linealmente independiente, pues si $\lambda_1, \ldots, \lambda_n \in K$ son tales que $\sum_{i=1}^{n} e_i \lambda_i = 0$ necesariamente $\lambda_i = 0$ para todo $i \in \{1, \ldots, n\}$.

Ejemplo 2.13. Del Ejemplo (2.10.), se deduce que la familia infinita numerable $S = \{X^i |\ i \in \mathbb{N} \cup \{0\}\}$ es linealmente independiente. En efecto, si usamos la notación $p_i(X) = X^i$ y tomamos cualquier subconjunto finito $S' = \{p_{i_1}(X), \ldots, p_{i_m}(X)\} \subseteq S$, entonces la igualdad $a_1 p_{i_1}(X) + \cdots + a_m p_{i_m}(X) = 0$ conduce a que $a_1 = \cdots = a_m = 0$.

Teorema 2.14. *Sea S un subconjunto linealmente independiente de V y sea u un elemento de $V - L(S)$. Entonces, $S \cup \{u\}$ es linealmente independiente.*

DEMOSTRACIÓN. Dado $\{u_1, \ldots, u_n\} \subseteq S \cup \{u\}$ tal que $\sum_{i=1}^{n} \lambda_i u_i = 0$. Si $u \neq u_i$ para $i = 1, \ldots, n$, entonces $\lambda_1 = \cdots = \lambda_n = 0$. Si $u = u_1$, entonces $\sum_{i=1}^{n} \lambda_i u_i = 0$ con $\lambda_1 \neq 0$ nos lleva a que $u_1 = \sum_{i=2}^{n} \frac{\lambda_i}{\lambda_1} u_i \in L(S)$ en contradicción con la elección de u. □

Proposición 2.15. *Sea $\{S_i\}_{i \in I} \subseteq V$ familia filtrada no vacía formada por conjuntos linealmente independientes. Entonces, $\bigcup_{i \in I} S_i$ es linealmente independiente.*

DEMOSTRACIÓN. Dado un conjunto finito $\{u_1, \ldots, u_n\} \subseteq \bigcup_{i \in I} S_i$, existe un índice $j \in I$ tal que $\{u_1, \ldots, u_n\} \subseteq S_j$. En consecuencia, $\{u_1, \ldots, u_n\}$ es linealmente independiente y la arbitrariedad del subconjunto finito tomado implica que $\bigcup_{i \in I} S_i$ es linealmente independiente. □

Definición 2.16. Llamamos **base de un espacio vectorial** a un sistema de generadores de V sobre K que sea linealmente independiente.

Ejemplo 2.17. $C = \{e_1, \ldots, e_n\} \subseteq K^n$ es una base de K^n sobre K.

Ejemplo 2.18. $S = \{X^i |\ i \in \mathbb{N} \cup \{0\}\}$ es una base de $K[X]$ sobre K.

Teorema 2.19. (Teorema de Steinitz.) *Todo espacio vectorial tiene una base.*

DEMOSTRACIÓN. Sea V espacio vectorial no nulo, entonces existe $S \subseteq V$ subconjunto linealmente independiente. Si $L(S) = V$, entonces S es una base. Si $L(S) \neq V$ existe $x \in V - L(S)$ y, por el Teorema (2.14.), $S \cup \{x\}$ es linealmente independiente. Sea la familia $\Gamma = \{S \subseteq V |\ S$ es linealmente independiente$\}$ en la que se considera el orden por inclusión. Dado que Γ es no nula y para cada cadena $\{S_i |\ i \in I\} \subseteq \Gamma$ tenemos una cota superior $\cup_{i \in I} S_i$ justificada por la Proposición (2.15.), estamos en condiciones de aplicar el Lema de Zorn para garantizar la existencia de un elemento maximal T en Γ. Además T es sistema generador y lo razonamos por reducción al absurdo. Supongamos que $T = \{u_j |\ j \in J\}$ no fuera sistema generador, razonando como al principio tendremos la existencia de $u \in V - L(T)$ tal que $T \cup \{u\}$ es linealmente independiente. Entonces, $T \cup \{u\} \in \Gamma$ y llegamos a una contradicción con la maximalidad de T. □

Observación 2.20. En este trabajo tratamos el teorema anterior con un espacio vectorial de dimensión arbitraria. El caso finito ha sido estudiado en la carrera y puede verse en [11, Proposición 1.16] o [12, Teorema 3.22].

Corolario 2.21. *Sea $S \subseteq V$ linealmente independiente. Entonces, existe una base B de V tal que $S \subseteq B$.*

DEMOSTRACIÓN. Consideramos la familia $\Gamma = \{R \subseteq V |\ R$ es linealmente independiente y $S \subseteq R\}$. Razonando de forma análoga al Teorema, llegamos a la existencia de un elemento maximal B de Γ que resulta ser sistema generador. Ese conjunto B es por tanto base tal que $S \subseteq B$. □

Teorema 2.22. *Sean B y B' bases de V. Entonces, $|B| = |B'|$.*

DEMOSTRACIÓN. Si B es finita, entonces B' es también finita verificando $|B| = |B'|$. Si las bases no son finitas, escribimos $B = \{b_i |\ i \in I\}$ y $B' = \{b'_j |\ j \in J\}$. Observamos que dado $i \in I$, tenemos que $b_i \in < b'_{j_1}, \ldots, b'_{j_{t_i}} >$ por ser B' una base. Con esto llegamos a que todo elemento $i \in I$ está asociado a un conjunto finito $\{j_1, \ldots, j_{t_i}\} \subseteq J$, por lo cual $|B| \leq |B'|$. Razonando de forma análoga para los elementos de B' tenemos $|B'| \leq |B|$, así que $|B| = |B'|$. □

Como consecuencia de este teorema, tenemos que el cardinal de un conjunto de vectores que constituyen una base de un espacio vectorial V es un invariante, lo que conlleva la buena definición del siguiente concepto.

Definición 2.23. Se define la **dimensión del espacio vectorial** V como el número de vectores que tiene una base de V. Se denota $\dim_K(V)$, aunque por abreviar se suele usar la notación $\dim(V)$ obviando el cuerpo base K.

Ejemplo 2.24. Sea K cuerpo y $n \in \mathbb{N}$, se tiene que K^n es un espacio vectorial con $\dim_k(K^n) = n$, mientras que $K[X]$ tiene dimensión infinita.

Teorema 2.25. *Todo espacio vectorial V sobre K es isomorfo a una suma directa de copias del cuerpo K indizada en un conjunto de cardinal $\dim(V)$.*

DEMOSTRACIÓN. Supongamos que $\dim(V) = c$, entonces existe una base $B = \{b_i |\ i \in I\}$ de cardinal c. Cada elemento $v \in V$ se escribe de forma única como $v = \sum_{i \in I} k_i b_i$ con $k_i \in K$ casi todos nulos. Éstos están en correspondencia con las aplicaciones de I en K de soporte finito, que forman la suma directa $K^{(I)}$ de c-copias del cuerpo K. □

Corolario 2.26. *Dos espacios vectoriales de igual dimensión son isomorfos.*

3. Extensiones de cuerpos

En este apartado vamos a extender los conocimientos del Álgebra Lineal al área de las extensiones de cuerpos. Para ello, haremos un estudio previo de las nociones que tendremos que tener presentes en nuestro propósito de abordar las bases de trascendencia y definir el grado de una extensión trascendente.

Definición 3.1. Sean K y F cuerpos, se dice que F es una **extensión** de K cuando K es un subcuerpo de F, esto es, K es un cuerpo con las operaciones definidas en F que le dan su estructura algebraica restringidas a K. En tal caso, se denota F/K.

Proposición 3.2. *Sea F/K una extensión de cuerpos. Entonces, F es un espacio vectorial sobre K con las operaciones producto $\cdot\colon K \times F \longrightarrow F$, definida $(\lambda, u) \longmapsto \lambda u$, y suma $+ : F \times F \longrightarrow F$, definida $(u, v) \longmapsto u + v$.*

Demostración. Se verifican trivialmente los axiomas de espacio vectorial por el hecho de que F es un cuerpo y $K \subseteq F$. □

A partir de ahora, trabajaremos con una extensión de cuerpos F/K.

Definición 3.3. Sea $A \subseteq F$ un subconjunto, se define $K(A)$ el **subcuerpo generado** por A sobre K como el menor subcuerpo que contiene a A, por lo tanto es la intersección de todos los subcuerpos que contienen a A. Se tiene que $K(A)$ contiene al conjunto $K[A] = \{\sum k_{i_1 \dots i_t} a_{i_1}^{e_{i_1}} \cdots a_{i_t}^{e_{i_t}} |\ a_{i_j} \in A, e_{i_j} \in \mathbb{N}, k_{i_1 \dots i_t} \in K\} \subseteq F$, que es un dominio de integridad y verifica que $K(A)$ es su cuerpo de fracciones.

Definición 3.4. Diremos que $\alpha \in F$ es **elemento algebraico** sobre K cuando exista un polinomio no nulo $f \in K[X]$ tal que $f(\alpha) = 0$, en tal caso se denota $Irr(\alpha, K)$ al polinomio irreducible que tiene por raíz a α. Si no existe, se dirá que α es **trascendente** sobre K.

Definición 3.5. Se dice que F/K es una **extensión algebraica** cuando todo elemento $\alpha \in F$ es algebraico. En otro caso, si existe algún elemento $\beta \in F$ trascendente, se dice que F/K es una **extensión trascendente**.

Sabemos que un espacio vectorial V sobre un cuerpo K está determinado, salvo isomorfismo, por su dimensión. Queremos llevar la terminología de dimensión al terreno de las extensiones y, a raíz de ahí, ver si ocurre algo similar a los espacios vectoriales.

Definición 3.6. Llamamos **grado de la extensión** F/K a la dimensión de F como espacio vectorial sobre K. Se denotará $[F : K]$.

Ejemplo 3.7. El conjunto de los números complejos $\mathbb{C}$ es una extensión de $\mathbb{R}$ y una $\mathbb{R}$-base de $\mathbb{C}$ es $\{1, i\}$, pues todo número complejo puede expresarse de la forma $a+ib$ con $a, b \in \mathbb{R}$. Se tiene entonces que $[\mathbb{C} : \mathbb{R}] = 2$. Sin embargo, considerando $\mathbb{C}$ como extensión de $\mathbb{Q}$ se tiene que $[\mathbb{C} : \mathbb{Q}]$ es infinito.

3.1. Bases de trascendencia y grado de trascendencia

El concepto de grado de extensión no nos aporta información relevante cuando tratamos con casos de extensiones trascendentes, como son por ejemplo $\mathbb{R}/\mathbb{Q}$ o $K(X)/K$ con X indeterminada, donde el grado es infinito. Vamos, con ayuda de [10] y [8], en busca de dar otro concepto: el grado de trascendencia.

Definición 3.8. Sea una extensión de cuerpos F/K, diremos que los elementos $\alpha_1, \ldots, \alpha_n \in F$ son **algebraicamente dependientes** sobre K si existe un polinomio no nulo $f \in K[X_1, \ldots, X_n]$ tal que $f(\alpha_1, \ldots, \alpha_n) = 0$. Serán **algebraicamente independientes** en caso de no existencia de tal polinomio, o lo que es igual, la combinación $\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n} = 0$ con $a_{i_1,\ldots,i_n} \in K$ implica que $a_{i_1,\ldots,i_n} = 0$ para todos los índices $i_1, \ldots, i_n$.

Observación 3.9. Tendremos independencia algebraica de $\alpha_1, \ldots, \alpha_n \in F$ cuando el homomorfismo evaluación $\Phi_{\alpha_1,\ldots,\alpha_n} : K[X_1, \ldots, X_n] \longrightarrow F$, definido $\Phi_{\alpha_1,\ldots,\alpha_n}(f) = f(\alpha_1, \ldots, \alpha_n)$, sea inyectivo ($\mathrm{Ker}\Phi_{\alpha_1,\ldots,\alpha_n} = 0$). En este caso, se tiene que $K[X_1, \ldots, X_n] \cong K[\alpha_1, \ldots, \alpha_n] = \mathrm{Im}(\Phi_{\alpha_1,\ldots,\alpha_n})$. Tal isomorfismo extiende a los cuerpos de fracciones a través de la aplicación $\Phi_{ext} : K(X_1, \ldots, X_n) \longrightarrow K(\alpha_1, \ldots, \alpha_n)$ definida $\Phi_{ext}(X_i) = \alpha_i$.

Definición 3.10. Sea F/K una extensión de cuerpos y $\alpha_1, \ldots, \alpha_n \in F$ elementos algebraicamente independientes sobre K, llamamos **extensión trascendente pura** de K al cuerpo $K(\alpha_1, \ldots, \alpha_n)$.

Definición 3.11. Denominamos **base de trascendencia** de F sobre K a un conjunto S algebraicamente independiente tal que $F/K(S)$ es una extensión algebraica.

Proposición 3.12. *Sea F/K y $A \subseteq F$ un conjunto minimal que verifica que $F/K(A)$ es extensión algebraica. Entonces, A es una base de trascendencia de F sobre K.*

Demostración. Supongamos que A no es algebraicamente independiente, entonces existe $\alpha \in A$ que es algebraicamente dependiente en $A - \{\alpha\}$. Por la transitividad de la dependencia algebraica se tendría que $F/K(A - \{\alpha\})$ es algebraica, en contradicción con la minimalidad de A respecto a la propiedad. □

Proposición 3.13. *Sea F/K y $S \subseteq F$ maximal algebraicamente independiente. Entonces, S es una base de trascendencia de F sobre K.*

DEMOSTRACIÓN. Si $\alpha \in S$ es claro que es algebraico sobre $K(S)$, pues $f(x) = x - \alpha \in K(S)[X]$ es polinomio no nulo verificando $f(\alpha) = 0$. Si $\alpha \in F - S$, por maximalidad de S se tiene que $S \cup \{\alpha\}$ es algebraicamente dependiente, así que α es algebraico sobre $K(S)$. □

Teorema 3.14. *Sea F/K extensión de cuerpos y $S \subseteq F$ algebraicamente independiente sobre K. Entonces, S está contenido en una base de trascendencia de F sobre K.*

DEMOSTRACIÓN. Consideramos la familia $\Omega = \{C \subseteq F |\ C$ es algebraicamente independiente sobre K y $S \subseteq C\}$, la cual podemos ordenar parcialmente por inclusión. Sea $T \subseteq \Omega$ totalmente ordenado, veamos que $B = \cup_{A \in T} A$ está en T. Es claro que $S \subseteq B$ por definición de T y B, ahora para ver que B es algebraicamente independiente razonamos por contradicción. Supongamos que existe $B' \subseteq B$ finito algebraicamente dependiente sobre K, necesariamente B' debe estar contenido en uno de los subconjuntos de T. En consecuencia, tal subconjunto es algebraicamente dependiente, lo cual es una contradicción con que los elementos de T son algebraicamente independientes. Visto que $B \in T$ y notando que es cota superior para tal cadena arbitraria, estamos en condiciones de aplicar el Lema de Zorn. Éste nos garantiza la existencia de un conjunto maximal algebraicamente independiente conteniendo a S, que resulta ser una base de trascendencia de F/K por la Proposición (3.13.). □

Observación 3.15. (Existencia de bases de trascendencia.) Tomando cualquier subconjunto algebraicamente independiente S de una extensión F/K tendremos probada, por el teorema anterior, la existencia de una base de trascendencia de F/K (la cual contendrá a S).

Teorema 3.16. *Sea F/K extensión de cuerpos, $S = \{x_1, \ldots, x_m\}$ base de trascendencia de F sobre K con m minimal y $C = \{w_1, \ldots, w_n\}$ un conjunto de elementos de F algebraicamente independientes sobre K. Entonces $n \leq m$.*

DEMOSTRACIÓN. Dado que $S = \{x_1, \ldots, x_m\}$ es base de trascendencia, se tiene por definición que $w_1 \in F$ es algebraico sobre $K(x_1, \ldots, x_m)$ y podemos considerar el irreducible $\mathrm{Irr}(w_1, K(x_1, \ldots, x_m)) \in K(x_1, \ldots, x_m)[X_0]$. Por la independencia algebraica del conjunto $C = \{w_1, \ldots, w_n\}$, tenemos que $w_1 \in C$ no es algebraico sobre K. En consecuencia, el polinomio irreducible $\mathrm{Irr}(w_1, K(x_1, \ldots, x_m)) \notin K[X_0]$ y es así que debe tener a alguno de los x_i, pongamos x_1.

Como $w_1, x_1, \ldots, x_m$ son algebraicamente dependientes, existe un polinomio no nulo $F_1 \in K[X_0, X_1, \ldots, X_m]$ tal que $F_1(w_1, x_1, \ldots, x_m) = 0$. Reordenado en x_1, llegamos a la expresión $\sum G_{1_j}(w_1, x_2, \ldots, x_m)x_1^j = 0$, donde $G_{1_j} \in K[X_0, X_2, \ldots, X_m]$. Si todos los G_{1_j} fuesen nulos, se tendría que w_1 es raíz de $G_{1_j}(X_0, X_2, \ldots, X_m)$ y por ello $\mathrm{Irr}(w_1, K(x_1, \ldots, x_m))|G_{1_j}$. En consecuencia, x_1 no aparecería en $\mathrm{Irr}(w_1, K(x_1, \ldots, x_m))$ en contradicción con lo razonado anteriormente. Existe pues algún $G_{1_j} \neq 0$ y x_1 es algebraicamente dependiente sobre $K(w_1, x_2, \ldots, x_m)$.

Consideramos ahora w_2, que será algebraico sobre $K(w_1, x_2, \ldots, x_m)$. Tomamos $\mathrm{Irr}(w_2, K(w_1, x_2, \ldots, x_m))$, en el cual aparecerá alguno de los elementos $\{w_1, x_2, \ldots, x_m\}$. No puede aparecer solo w_1, porque de ser así se contradice la independencia algebraica de $\{w_1, w_2\}$. Aparecerá entonces algún x_i, pongamos x_2. Como $w_1, w_2, x_2, \ldots, x_m$ son algebraicamente dependientes, existe un polinomio no nulo $F_2 \in K[X_0, X_1, \ldots, X_m]$ tal que $F_2(w_1, w_2, x_2, \ldots, x_m) = 0$. Reordenado en x_2, llegamos a la expresión $\sum G_{2_j}(w_1, w_2, x_3, \ldots, x_m)x_2^j = 0$, donde $G_{2_j} \in K[X_0, X_2, \ldots, X_m]$. Si todos los G_{2_j} fuesen nulos, se tendría que w_2 es raíz de $G_{2_j}(X_0, X_2, \ldots, X_m)$ y por ello estaríamos en la situación de que $\mathrm{Irr}(w_2, K(w_1, x_2, \ldots, x_m))|G_{2_j}$. En consecuencia, x_2 no aparecería en $\mathrm{Irr}(w_1, K(w_1, x_2, \ldots, x_m))$ en contradicción con lo razonado anteriormente. Existe pues algún $G_{2_j} \neq 0$ y x_2 es algebraico sobre $K(w_1, w_2, x_3, \ldots, x_m)$.

Mediante un proceso de inducción y reenumerando si es necesario, encontramos $\{w_1, \ldots, w_r\}$ con $r < n$ tales que F es algebraico sobre la extensión $K(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m)$. Por ello, existe $F_{r+1} \in K[X_0, X_1, \ldots, X_m]$ tal que $F_{r+1}(w_1, \ldots, w_r, w_{r+1}, x_{r+1}, \ldots, x_m) = 0$. Como C es K-algebraicamente independiente, podemos encontrar x_j, supongamos x_{r+1}, algebraico sobre $K(w_1, \ldots, w_r, w_{r+1}, x_{r+2}, \ldots, x_m)$. Dado que toda torre de extensiones algebraicas es algebraica, F es algebraica sobre $K(w_1, \ldots, w_r, w_{r+1}, x_{r+2}, \ldots, x_m)$. Repitiendo el proceso, si $m \leq n$ podemos cambiar los x_i por w_j y llegar a que $F/K(C)$ es algebraica, así C es base de trascendencia de F/K. Esto muestra que $m \leq n$ implica $n = m$.

□

Corolario 3.17. *Cualesquiera dos bases de trascendencia de la misma extensión trascendente tienen igual cardinal.*

Demostración. Si las bases son finitas, hacemos aplicación doble del Teorema. En caso de bases no finitas escribimos $B = \{b_i |\ i \in I\}$ y $B' = \{b'_j |\ j \in J\}$. Observamos que dado $i \in I$, tenemos que $b_i \in < b'_{j_1}, \ldots, b'_{j_{t_i}} >$ por ser B' una base.

Así, todo elemento $i \in I$ está asociado a un conjunto finito $\{j_1, \ldots, j_{t_i}\} \subseteq J$, por lo cual $|B| \leq |B'|$. Razonando de forma análoga para los elementos de B' tenemos $|B'| \leq |B|$, por lo cual $|B| = |B'|$. □

Análogo a lo que ocurría en espacios vectoriales, el hecho de que bases de trascendencia para una misma extensión tengan igual cardinal va a dar luz verde al concepto que describimos a continuación.

Definición 3.18. Definimos el **grado de trascendencia** de una extensión de cuerpos F/K como el cardinal de una de las bases de trascendencia de F sobre K. Usaremos la notación $\text{tr.deg}(F/K)$.

Observación 3.19. Una extensión de cuerpos F/K algebraica tiene grado de trascendencia cero. En efecto, $S = \emptyset$ de cardinal nulo es base de trascendencia de F/K por ser un conjunto algebraicamente independiente verificando que $F/K(\emptyset) = F/K$ es extensión algebraica.

Proposición 3.20. *Sean F/K y L/K extensiones algebraicamente cerradas y con igual grado de trascendencia sobre K. Entonces, F y L son K-isomorfas.*

Demostración. Sean B_F y B_L respectivas bases de trascendencia para F/K y L/K. Ambas bases tienen igual cardinal, dado que por hipótesis tenemos coincidencia en el grado de trascendencia por parte de las distintas extensiones. Podemos entonces definir una biyección $G : B_F \to B_L$, la cual extiende a un único K-isomorfismo $G_{ext} : K[B_F] \to K[B_L]$. Por ello, existe un único K-isomorfismo entre los cuerpos de fracciones $E : K(B_F) \to K(B_L)$ que me permite identificar $K(B_F)$ con $K(B_L)$. Se tiene que estos cuerpos son clausuras algebraicas del mismo cuerpo y por ello son isomorfos. □

Observación 3.21. Dos cuerpos algebraicamente cerrados con el mismo cardinal incontable y la misma característica son isomorfos. En efecto, sean K y K' los cuerpos primos de F y F', respectivamente. Podemos identificar K con K' y notar que cuando F es incontable su cardinalidad es la misma que la cardinalidad de una base de trascendencia sobre K. Finalmente, se aplica la Proposición (3.20.).

Vemos que las nociones que acabamos de dar en esta sección guardan similitud con las que dimos en la Sección (2):

ÁLGEBRA LINEAL	TRASCENDENCIA
linealmente independiente	algebraicamente independiente
base	base de trascendencia
dimensión	grado de trascendencia

3.2. Operadores de dimensión

Nos disponemos ahora a redefinir los conceptos de la Sección (3.1) como una aplicación de lo que vamos a introducir como operadores de dimensión. Vamos a desarrollar una teoría general de tales operadores y relacionarla con las extensiones de cuerpos a partir de la información aportada por [2].

Definición 3.22. Dado un conjunto E, y considerando $P(E)$ el conjunto de partes de E, llamamos **operador dimensional** en E a una aplicación $d : P(E) \longrightarrow P(E)$ tal que:

(I) Si $S \subseteq T \subseteq E$, entonces $S \subseteq d(S) = d(d(S)) \subseteq d(T)$.

(II) Si $S \subseteq E$ y $\Omega = \{M \subseteq S |\ M \text{ es finito}\}$, entonces $d(S) = \bigcup_{M\in\Omega} d(M)$.

(III) Si $S \subseteq E$, $x \in E$ y $\widetilde{x} \in d(S \cup \{x\}) - d(S)$, entonces $x \in d(S \cup \{\widetilde{x}\})$.

Veamos algunos ejemplos para asimilar este concepto.

Ejemplo 3.23. Sea E un conjunto, las siguientes aplicaciones son operadores dimensionales porque verifican las condiciones dadas en la definición:

(a) La identidad en $P(E)$, esta es la aplicación $Id_{P(E)} : P(E) \longrightarrow P(E)$ definida $Id_{P(E)}(S) = S$ para todo $S \subseteq E$.

(b) La aplicación total $d_E : P(E) \longrightarrow P(E)$ definida $d_E(S) = E$.

(c) La aplicación $p_F : P(E) \longrightarrow P(E)$ definida $p_F(S) = FS$ para todo $S \subseteq E$, siendo F un cuerpo y E un espacio vectorial.

A partir de este momento, y durante toda la sección, vamos a tener presente en cada definición y resultado que estamos trabajando con un operador dimensional d en un conjunto E.

Definición 3.24. Sea $S \subseteq E$, se dice que S es:

- Un **conjunto d-libre** si para cualquier $x \in S$ se cumple $x \notin d(S - \{x\})$.
- Un **conjunto d-denso** cuando $d(S) = E$.
- Una **d-base** si S es d-denso y d-libre.

Observación 3.25. Está claro con esta definición que el conjunto vacío $\emptyset$ es d-libre y el total E es d-denso. En efecto, como $\emptyset$ no tiene ningún elemento verifica $x \notin d(S - \{x\}), \forall x \in \emptyset$. Por otro lado, por definición tenemos que $E \subseteq d(E) \in P(E)$, lo que implica que $d(E) = E$, esto es, E es d-denso.

Ejemplo 3.26. Volviendo al Ejemplo (3.23.)

(a) Todo subconjunto de E es d-libre y solo E es d-denso, por lo que la única d-base para $Id_{P(E)}$ es E.

(b) Al revés que antes, ahora hay un único subconjunto de E que es d-libre, el vacío, y todo subconjunto de E es d-denso. En consecuencia, $\emptyset$ es la única d-base para d_E.

(c) Para este caso, los conjuntos d-libres son aquellos que son linealmente independientes y los conjuntos d-densos son los subconjuntos que son sistema generador. Así pues, las d-bases son las bases del F-espacio vectorial E.

Proposición 3.27. *Sean T y S subconjuntos de E tales que $S \subseteq T \subseteq E$.*
(1) Si T es d-libre, entonces S es d-libre.
(2) Si S es d-denso, entonces T es d-denso.
(3) Si $S \subseteq E$, entonces S es d-denso si y solo si $d(S)$ es d-denso.

Demostración.

(1) Dado $x \in S$, por la condición de inclusión $S \subseteq T$, tenemos que $x \in T$. Usando que T es d-libre, $x \notin d(T - \{x\}) \supseteq d(S - \{x\})$. Por ello, $x \notin d(S - \{x\})$ y S es d-libre.

(2) Por definición de operador dimensional y usando la hipótesis de que S es d-denso, tenemos que $S \subseteq d(S) = E \subseteq d(T) \in P(E)$. En consecuencia, $d(T) = E$ y T es d-denso.

(3) Usando de nuevo la definición de operador dimensional, tenemos la igualdad $d(S) = d(d(S))$, la cual me garantiza que si S o $d(S)$ es d-denso entonces también lo es el otro dado que $E = d(S) = d(d(S))$.

□

Proposición 3.28. *Sea $\{S_i\}_{i\in I} \subseteq P(E)$ familia filtrada no vacía formada por conjuntos d-libres. Entonces, $\bigcup_{i\in I} S_i$ es d-libre.*

Demostración. Razonemos por reducción al absurdo, si $\bigcup_{i\in I} S_i$ no es d-libre, entonces existe $x \in \bigcup_{i\in I} S_i$ tal que $x \in d((\bigcup_{i\in I} S_i) - \{x\})$. Por ello existe un conjunto finito $A \subseteq (\bigcup_{i\in I} S_i) - \{x\}$ verificando que $x \in d(A)$. Tenemos pues que $A \cup \{x\}$ es un subconjunto finito de $\bigcup_{i\in I} S_i$, así que por hipótesis debe existir $j \in I$ tal que $A \cup \{x\} \subseteq S_j$. En consecuencia, $A \subseteq S_j - \{x\}$ y, por definición de operador dimensional, $x \in d(A) \subseteq d(S_j - \{x\})$, lo que contradice que S_j es d-libre. □

Proposición 3.29. *Sean $S \subseteq E$ conjunto d-libre, $y \in E - d(S)$. Entonces, $S \cup \{y\}$ es d-libre.*

Demostración. Por contrarrecíproco, si $S \cup \{y\}$ no es d-libre, entonces existe $x \in S \cup \{y\}$ tal que $x \in d(S \cup \{y\} - \{x\})$ $(*)^1$. Si $x = y$ tendríamos que $x \in d(S \cup \{x\} - \{x\}) = d(S)$, en contradicción con la hipótesis de que $y \in E - d(S)$. Así, $x \neq y$ y por ello $x \in S$, lo cual implica que $x \notin d(S - \{x\})$ $(*)^2$ por ser S un conjunto d-libre. De $(*)^1$ y $(*)^2$ tenemos que $x \in d(S \cup \{y\} - \{x\}) - d(S - \{x\}) = d((S - \{x\}) \cup \{y\}) - d(S - \{x\})$, luego $y \in d((S - \{x\}) \cup \{x\}) = d(S)$ por definición de operador diferencial, lo que contradice la hipótesis. □

Proposición 3.30. *Sea B subconjunto de E. Entonces, equivalen:*

(i) B es d-base.
(ii) B=mín$\{T \subseteq E |\ T$ es d-denso$\}$.
(iii) B=máx$\{S \subseteq E |\ S$ es d-libre$\}$.

Demostración. (I⇒ II). Consideramos S un subconjunto propio de B, entonces existe $x \in B$ tal que $S \subseteq B - \{x\}$. Por hipótesis de que B es d-base, en particular es d-libre, se tiene que $x \notin d(B - \{x\}) \supseteq d(S)$. Esto conlleva a que $d(S) \neq E$ dado que $x \notin d(S)$, así que S no puede ser d-denso. En consecuencia, no existe ningún subconjunto propio de B que sea d-denso.

(II⇒ III). Supongamos que existe $x \in B$ tal que $x \in d(B - \{x\})$, entonces $B = (B - \{x\}) \cup \{x\} \subseteq d(B - \{x\})$. Usando que B es d-denso tenemos también que $d(B - \{x\})$ es d-denso por la Proposición (3.27.), llegando así a una contradicción con la hipótesis de minimalidad de B. Tenemos probado que B es d-libre. Ahora, consideramos un conjunto S tal que $B \subset S \subseteq E$, por lo que debe existir $x \in S$ verificando que $B \subseteq S - \{x\}$. De nuevo, usando que B es d-denso y la Proposición (3.27.), tenemos que $S - \{x\}$ es d-denso. Esto implica que $x \in d(S - \{x\})$ y así S no es d-libre. Llegamos pues a B es el máximo conjunto d-libre.

(III⇒ I). Veamos que B es d-denso razonando por absurdo. Si no lo fuera, $d(B) \subset E$ y existiría $x \in E - d(B)$. Se tendría entonces, por la Proposición (3.29.), que $B \cup \{x\}$ es d-libre, en contradicción con la hipótesis de maximalidad de B como conjunto d-libre. □

Teorema 3.31. *Sea $S \subseteq E$ un conjunto d-libre y $T \subseteq E$ d-denso. Entonces, existe $C \subseteq T$ tal que $S \cup C$ es d-base y $S \cap C = \emptyset$.*

Demostración. Sea $\Omega = \{A \subseteq T |\ A \cup S$ es d-libre y $A \cap S = \emptyset\}$ familia de subconjuntos de T dotada con la relación de orden parcial por inclusión. Como $\emptyset \in \Omega$, se tiene que Ω es no vacío e inductivo por la Proposición (3.28.).

Aplicando el Lema de Zorn, tenemos probada la existencia de C elemento maximal en Ω. En particular, $C \cup S$ es d-libre. Para ver que es d-denso razonamos por reducción al absurdo. Suponemos que no lo es, entonces se sigue que $T \nsubseteq d(S \cup C)$ por hipótesis de que T es d-denso y por la Proposición (3.27.). Tomamos $x \in T - d(S \cup C) \subseteq T - (S \cup C)$. Ahora, dado que $S \cup C$ es d-libre y $x \notin d(S \cup C)$ tenemos por la Proposición (3.29.) que $(S \cup C) \cup \{x\} = S \cup (C \cup \{x\})$ es d-libre, y por ello también lo es $C \cup \{x\}$ en virtud de (3.27.). Como $x \notin S \cup C$, se tiene que $C \subset C \cup \{x\}$ en contradicción con la maximalidad de C en Ω. □

Corolario 3.32. *Sea $S \subseteq E$ un conjunto d-libre y $T \subseteq E$ d-denso tal que $S \subseteq T$. Entonces, existe B d-base tal que $S \subseteq B \subseteq T$.*

Demostración. Considerar el C del teorema anterior para definir $B = S \cup C$ que verifica ser d-base y $B \subseteq T$ dado que $S, C \subseteq T$. □

Corolario 3.33. *Sea E conjunto y d operador dimensional en E.*
(1) Si $L \subseteq E$ es d-libre, entonces existe B d-base tal que $L \subseteq B$.
(2) Si $D \subseteq E$ es d-denso, entonces existe B d-base tal que $B \subseteq D$.
(3) Hay existencia de una d-base.

Demostración. Es consecuencia del Corolario (3.32.) teniendo presente la Observación (3.25.)

(1) Dado que L es d-libre y E es d-denso tal que $L \subseteq E$, entonces aplicando el corolario, tenemos probada la existencia de B d-base tal que $L \subseteq B \subseteq E$.

(2) Esta vez aplicamos el corolario a $\emptyset$ que es d-libre y a D que es d-denso tales que $\emptyset \subseteq D$ y tendremos pues que existe B d-base tal que $\emptyset \subseteq B \subseteq D$.

(3) Aplicación del corolario a $\emptyset$ d-libre y E d-denso, para probar la existencia de B d-base tal que $\emptyset \subseteq B \subseteq E$.

□

Teorema 3.34. *Sea $S \subseteq E$ conjunto d-libre y $T \subseteq E$ conjunto d-denso. Entonces las d-bases son equipotentes dos a dos.*

Demostración. Distinguimos casos:

(C1).Existencia de una d-base finita.

Razonemos por inducción que dadas B y C d-bases tal que C es finita y $\mathrm{Card}(C - B) = n$, entonces B y C son equipotentes. Para $n = 0$ se verifica dado que $\mathrm{Card}(C - B) = 0$ implica que $C - B = \emptyset$. En consecuencia $C \subseteq B$ y por la Proposición (3.30.) tenemos la igualdad.

Supongamos cierta la hipótesis para n y veamos el caso de que B y C son d-bases tal que C es finita y $\mathrm{Card}(C-B)=n+1$. Dado que $C-B\neq\emptyset$, escogemos $x\in C-B$. Entonces, por la Proposición (3.30.) $C-\{x\}\subset C$ no es un conjunto d-denso y por ello tampoco lo es $d(C-\{x\})$. Se tiene pues que $B\nsubseteq d(C-\{x\})$ y podemos tomar $y\in B-d(C-\{x\})$. Dado que $C-\{x\}$ es d-libre por serlo C, por la Proposición (3.29.) llegamos a que $(C-\{x\})\cup\{y\}$ es d-libre. Además, como $y\in d(C)$ llegamos a que $y\in d((C-\{x\})\cup\{x\})-d(C-\{x\})$ y por definición de operador dimensional, $x\in d((C-\{x\})\cup\{y\})$. Entonces, $x\in C=(C-\{x\})\cup\{x\}\subseteq d((C-\{x\})\cup\{y\})$, lo que conlleva que $d((C-\{x\})\cup\{y\})$ sea d-denso y por ello también lo sea $(C-\{x\})\cup\{y\}\equiv\widetilde{C}$. Como consecuencia, $\widetilde{C}$ es d-base. Dado que $x\in C$ y $y\notin C-\{x\}$, se tiene que C y $\widetilde{C}$ son equipotentes. En particular $\widetilde{C}$ es finito tal que $\widetilde{C}-B=((C-\{x\})\cup\{y\})-B=(C-B)-\{x\}$, ya que $y\in B$ y $x\in C-B$. Consecuentemente, $\mathrm{Card}(\widetilde{C}-B)=Car(C-B)-1=n$ y es aplicable la hipótesis de inducción, por la cual tenemos que B y $\widetilde{C}$ son equipotentes y ello lleva a que también lo sean B y C.

(C2).Todas las d-bases son infinitas.

Dado que B es d-denso, tenemos que $C\subseteq d(B)$. Ahora, para cada $x\in C$ podemos escoger un subconjunto finito $B_X\subseteq B$ para el cual $x\in d(B_x)$. Sea $\widetilde{B}=\bigcup_{x\in C}B_x$, se tiene que $C\subseteq d(\widetilde{B})$ dado que $x\in C$ implica $x\in d(B_x)\subseteq d(\widetilde{B})$. Esto conduce a que $d(\widetilde{B})$ es d-denso y consecuentemente también $\widetilde{B}\subseteq B$. Por la Proposición (3.30.), $\widetilde{B}=B$ y tenemos entonces que $\mathrm{Card}(B)=\mathrm{Card}(\widetilde{B})=\mathrm{Card}(\bigcup_{x\in C}B_x)\leq\sum_{x\in C}\mathrm{Card}(B_x)\leq\aleph\mathrm{Card}(C)=\mathrm{Card}(C)$. □

Esta particularidad de las d-bases, que guarda cierta analogía con las bases en espacios vectoriales, nos garantiza una buena definición del análogo en espacios vectoriales a dimensión.

Definición 3.35. Sea E conjunto, d operador dimensional en E, llamamos **d-dimensión** de E al cardinal de una d-base.

3.2.1. Bases y grado de trascendencia

Vamos a ver en este apartado cómo se relacionan los operadores de dimensión con las extensiones de cuerpos a través de distintos resultados.

Definición 3.36. Dada una extensión de cuerpos L/K, llamamos **clausura algebraica** del subconjunto $F\subseteq L$ a una extensión algebraica de F que sea algebraicamente cerrada. Usaremos la notación $\overline{F}^L$.

Proposición 3.37. *Sea K cuerpo y L/K una extensión de cuerpos. Entonces $d : P(L) \longrightarrow P(L)$ tal que $d(S) = \overline{K(S)}^L$ es un operador dimensional. Además, si $S \subseteq L$:*
(1) S es d-denso si y solo si $L/K(S)$ es una extensión algebraica.
(2) S es d-libre si y solo si S es K-algebraicamente independiente.

Demostración. Veamos que d es un operador dimensional dado que verifica las condiciones para serlo:

(i) Sea $S \subseteq T \subseteq L$, entonces $S \subseteq \overline{K(S)}^L = d(S)$ dado que todo elemento $x \in S$ es algebraico sobre $K(S)$. Además, $d(S) = \overline{K(S)}^L \subseteq \overline{K(T)}^L = d(T)$ puesto que todo elemento $x \in L$ algebraico sobre $K(S)$ también lo es sobre $K(T)$, ya que $K(S) \subseteq K(T)$. Por otro lado, se verifica $d(d(S)) = d(S)$ por doble inclusión. En efecto, por lo anterior tenemos que $S \subseteq d(S)$ y esto implica $d(S) \subseteq d(d(S))$. Sea ahora $\alpha \in d(d(S)) = d(\overline{K(S)}^L) = \overline{(\overline{K(S)}^L)}^L$, entonces α es algebraico sobre $\overline{K(S)}^L$. Por ello, α es algebraico sobre $K(S)$ y $\alpha \in \overline{K(S)}^L = d(S)$.

(ii) Sean $S \subseteq L$ y $\Omega = \{M \subseteq S |\ M \text{ es finito}\}$, queremos ver que $d(S) = \cup_{M\in\Omega} d(M)$. Por un lado, observamos que $M \subseteq S$ implica $d(M) = \overline{K(M)}^L \subseteq \overline{K(S)}^L = d(S)$, por lo cual $\cup_{M\in\Omega} d(M) \subseteq d(S)$. Por otro lado, dado $\alpha \in d(S) = \overline{K(S)}^L$ se tiene que α es algebraico sobre $K(S)$. En consecuencia, existe $M \subseteq S$ finito tal que α es algebraico sobre $K(M)$ y por ello $\alpha \in \overline{K(M)}^L = d(M)$ y $\alpha \in \cup_{M\in\Omega} d(M)$.

(iii) Sean $S \subseteq L$, $\alpha \in L$ y $\beta \in d(S \cup \{\alpha\}) - d(S)$, veamos que $\beta \in d(S \cup \{\beta\})$. La elección de $\beta \in \overline{K(S \cup \{\alpha\})}^L - \overline{K(S)}^L$ implica que β es trascendente sobre $K(S)$ y algebraico sobre $K(S)(\alpha)$, por lo cual existe $M = \{s_1, \ldots, s_t\} \subseteq S$ finito tal que β es algebraico sobre $K(M \cup \{\alpha\})$ y es trascendente sobre $K(M)$. En consecuencia, existe $F \in K[X, Y, X_1, \ldots, X_t]$ tal que $F(\alpha, \beta, s_1, \ldots, s_t) = 0$. Reescribimos de tal forma que llegamos a la expresión $\sum G_j(\alpha, s_1, \ldots, s_t)\beta^j = 0$ con los $G_j(\alpha, s_1, \ldots, s_t)$ no todos nulos. Reordenando en α, tenemos la expresión $\sum H_k(\beta, s_1, \ldots, s_t)\alpha^k = 0$ con los $H_k(\beta, s_1, \ldots, s_t)$ no todos nulos, pues en otro caso se llegaría a que β es algebraico sobre $K(M)$, contradicción. En consecuencia, algún H_i es no nulo y por ello α es algebraico sobre $K(\beta, s_1, \ldots, s_t)$ y algebraico sobre $K(S \cup \{\beta\})$.

Pasemos ahora a demostrar (1) y (2):

(1) Un conjunto $S \subseteq L$ es d-denso si $L = d(L) = \overline{K(S)}^L$, esto es, L es algebraica sobre $K(S)$.

(2) Razonamos las dos implicaciones por contrarrecíproco. Para la primera, suponemos que $S \subseteq L$ es algebraicamente dependiente sobre K. Consideramos $A = \{\alpha_1, \ldots, \alpha_n\} \subseteq S$ subconjunto finito algebraicamente dependiente sobre K con menor cardinal, a saber $\mathrm{Card}(A) = n$. Tomamos $f \in K[X_1, \ldots, X_n]$ no nulo tal que $f(\alpha_1, \ldots, \alpha_n) = 0$. Si $n = 1$, se tiene que α_1 es algebraico sobre K y $A - \{\alpha_1\} = \emptyset$, por lo que $\alpha_1 \in d(A - \{\alpha_1\}) = d(\emptyset) = \overline{K}^L$. Para $n > 1$, escribimos $f(X_1, \ldots, X_n) = \sum_{i=0}^m f_i(X_1, \ldots, X_{n-1}) X_n^i$, con $f_i \in K[X_1, \ldots, X_{n-1}]$ y $f_m \neq 0$. De la minimalidad cardinal de A se sigue que $f_m(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Sea $g \in K(A - \{\alpha_n\})[Y]$ tal que $g(Y) = \sum_{i=0}^m f_i(\alpha_1, \ldots, \alpha_{n-1}) Y^i$ no nulo. Evaluando, $g(\alpha_n) = \sum_{i=0}^m f_i(\alpha_1, \ldots, \alpha_{n-1}) \alpha_n^i = f(\alpha_1, \ldots, \alpha_n) = 0$. Se tiene pues que α_n es algebraico sobre $K(A - \{\alpha_n\})$, lo que se traduce en que $\alpha_n \in d(A - \{\alpha_n\})$. Hemos probado que para $n \geq 1$ se verifica $\alpha_n \in d(A - \{\alpha_n\})$, lo que implica que A no es d-libre y en consecuencia tampoco lo es S.

Veamos ahora la otra implicación. Supongamos que $S \subseteq L$ no es d-libre, entonces existe $A \subseteq S$ finito que no es d-libre. Sea $\alpha \in A$ tal que $\alpha \in d(A - \{\alpha\})$, entonces α es algebraico sobre $K(A - \{\alpha\})$ y por ello existen $\gamma_0, \ldots, \gamma_m \in K(A - \{\alpha\})$ tal que $\sum_{i=0}^m \gamma_i \alpha^i = 0$ con $\gamma_m \neq 0$. Podemos tomar los coeficientes $\gamma_0, \ldots, \gamma_m \in K[A - \{\alpha\}]$. Si $A = \{\alpha\}$, tenemos que $A - \{\alpha\} = \emptyset$, por lo que $\alpha_n \in d(A - \{\alpha\}) = d(\emptyset) = \overline{K}^L$ y α es algebraico sobre K y por ello A es algebraicamente dependiente sobre K. Si $A = \{\alpha_1, \ldots, \alpha_n\}$, tomamos $\gamma_i = f_i(\alpha_1, \ldots, \alpha_{n-1})$ con $f_i \in K[X_1, \ldots, X_{n-1}]$ siendo $f_m \neq 0$ dado que $\gamma_m \neq 0$. Sea $f \in K[X_1, \ldots, X_n]$ tal que $f(X_1, \ldots, X_n) = \sum_{i=0}^m f_i(X_1, \ldots, X_{n-1}) X_n^i$ no nulo. Evaluando, $f(\alpha_1, \ldots, \alpha_n) = \sum_{i=0}^m f_i(\alpha_1, \ldots, \alpha_{n-1}) \alpha_n^i = \sum_{i=0}^m \gamma_i \alpha^i = 0$, lo que implica que A es algebraicamente dependiente sobre K. Consecuentemente también lo es S.

□

Definición 3.38. Sea K cuerpo y L/K una extensión de cuerpos, llamaremos **operador dimensional asociado a la extensión** al operador definido en la Proposición (3.37.) .

Con la vigencia de la Proposición (3.37.), podemos dar una definición alternativa a la vista en la Definición (3.11.) para base de trascendencia y grado de trascendencia en un nuevo contexto, el de operadores dimensionales.

Definición 3.39. Definimos **base de trascendencia** de una extensión de cuerpos L/K como una base del operador asociado a la extensión.

Definición 3.40. Llamamos **grado de trascendencia** de L/K a la dimensión del operador asociado a la extensión. Se denotará $\text{tr.deg}(L/K)$.

Observación 3.41. Una extensión de cuerpos algebraica tiene grado de trascendencia nulo dado que $\emptyset$ es una base para el operador dimensional asociado a la extensión.

Observación 3.42. Dos bases de trascendencia B y C de la misma extensión de cuerpos L/K son equipotentes y las extensiones $L/K(B)$ y $L/K(C)$ son ambas algebraicas con igual grado de trascendencia. Sin embargo, puede ocurrir que el grado lineal de las extensiones $L/K(B)$ y $L/K(C)$ sea distinto.

Ejemplo 3.43. Sea $\alpha \in \mathbb{R}$ elemento $\mathbb{Q}$-trascendente, se verifica que las extensiones $\mathbb{Q}(\alpha)$ y $\mathbb{Q}(\alpha, \sqrt{2})$ tienen ambas grado de trascendencia 1. Sin embargo, $\mathbb{Q}(\alpha)$ tiene grado lineal 2 por admitir como $\mathbb{Q}$-base a $\{1, \alpha\}$ mientras que $\mathbb{Q}(\alpha, \sqrt{2})$ tiene grado lineal 3 por aceptar como $\mathbb{Q}$-base a $\{1, \alpha, \sqrt{2}\}$.

Proposición 3.44. *Sea K cuerpo y L/K una extensión finitamente generada. Entonces, $\text{tr.deg}(L/K(S))$ es finito. Además, para B base de trascendencia se tiene que $L/K(B)$ es finito.*

Demostración. Dado que L/K es finitamente generada, existe $S \subset L$ tal que $K(S) = L$, luego $L/K(S)$ es algebraica y por ello existe una base de L sobre K contenida en S, que es finita por serlo S. De consecuencia tenemos que $\text{tr.deg}(L/K)$ es finito.

Por otro lado, si consideramos B base de trascendencia de L/K se tiene que $L/K(B)$ es algebraica, lo cual sumado a que es finitamente generada por serlo por hipótesis L/K, llegamos a que $L/K(B)$ es finita. □

Corolario 3.45. *Sea L/K extensión de cuerpos finitamente generada, B base de trascendencia y $T \subseteq L$ tal que $L = K(T)$. Entonces, existe $S \subseteq T$ finito tal que $B \cap S = \emptyset$ y $L = K(B \cup S)$.*

Demostración. De la proposición anterior se sigue que $L/K(B)$ es finita, así para cada subconjunto finito $S \subseteq T - B$ tenemos que $[K(B)(S) : K(B)] \leq [L : K(B)]$. Consideramos S tal que $[K(B)(S) : K(B)]$ tiene la mayor longitud posible y vamos a ver que $L = K(B)(S)$. Supongamos por reducción al absurdo que $L \supset K(B)(S)$, entonces $T - B \nsubseteq K(B)(S)$ dado que de no ser así tendríamos que $L = K(T) = K(B)(T - B) \subseteq K(B)(S) \subset L$.

Escogemos pues $\alpha \in T - B$ tal que $\alpha \notin K(B)(S)$. Tenemos que $S \cup \{\alpha\} \subseteq T - B$ es finito y verifica $[K(B)(S \cup \{\alpha\}) : K(B)] = [K(B)(S)(\alpha) : K(B)] = [K(B)(S)(\alpha) : K(B)(S)][K(B)(S) : K(B)] > [K(B)(S) : K(B)]$ en contradicción con la elección de S. Así pues, hemos demostrado que $L = K(B)(S)$ y podemos concluir que $S \subseteq T$ es finito verificando $B \cap S = \emptyset$ y $L = K(B \cup S)$. □

Definición 3.46. Una extensión de cuerpos trascendente L/K es **cuerpo de función algebraica** sobre K si es finitamente generada. Si $\text{tr.deg}(L/K) = n$ se dirá cuerpo de función algebraica sobre K en n variables.

Ejemplo 3.47. $\mathbb{Q}(e, \pi, \sqrt{5})$ es cuerpo de función algebraica sobre $\mathbb{Q}$ en dos variables. En efecto, $\mathbb{Q}(e, \pi, \sqrt{5})/\mathbb{Q}$ es finitamente generada por $\{e, \pi, \sqrt{5}\}$ y $\text{tr.deg}(\mathbb{Q}(e, \pi, \sqrt{5})/\mathbb{Q}) = 2$.

Proposición 3.48. *Sean L/K y M/L extensiones de cuerpos.*
(1) Si B es base de trascendencia de L/K y C es base de trascendencia de M/L, entonces $B \cap C = \emptyset$ y $B \cup C$ es base de trascendencia de M/K.
(2) $tr.deg(M/K) = tr.deg(M/L) + tr.deg(L/K)$.

Demostración. Por definición de base de trascendencia, tenemos que $B \subseteq L$ es algebraicamente independiente sobre K y $C \subseteq M$ lo es sobre L. Entonces, $B \cup C$ es algebraicamente independiente sobre K y $B \cap C = \emptyset$.

Falta ver que $M/K(B \cup C)$ es algebraica. Dado que $L/K(B)$ es algebraica por ser B una base, tenemos que $L/K(B \cup C)$ es algebraica. Entonces, como $L(C) = K(B \cup C)(L)$, tenemos que $L(C)/K(B \cup C)$ es algebraica. Ahora, dado que $M/L(C)$ es algebraica por definición de base, tenemos una torre de extensiones algebraicas que me llevan a que $M/K(B \cup C)$ también sea algebraica. □

Definición 3.49. Sean F/K y F'/K' extensiones de cuerpos y $\tau : F \longrightarrow F'$ y $\sigma : K \longrightarrow K'$ morfismos. Diremos que τ es **morfismo extensión** de σ si $\tau(\alpha) = \sigma(\alpha)$ para todo $\alpha \in K$. Si además $\sigma = Id_K$, esto es, σ es la identidad en K se dice que τ es K-morfismo.

Proposición 3.50. *Sean L_1/K_1, L_2/K_2 extensiones de cuerpos algebraicamente cerradas tal que $tr.deg(L_2/K_2) = tr.deg(L_1/K_1)$. Entonces, todo isomorfismo $h : K_1 \longrightarrow K_2$ es extensible a un isomorfismo $h_{ext} : L_1 \longrightarrow L_2$.*

Demostración. Sea B_1 una base de trascendencia de L_1/K_1 y sea B_2 una de L_2/K_2. Dado que por hipótesis el grado de trascendencia es igual para ambas extensiones, se tiene que B_1 y B_2 son equipotentes.

En consecuencia, podemos encontrar una biyección $b : B_1 \to B_2$. Por independencia algebraica de B_1 sobre K_1 y de B_2 sobre K_2, tenemos la existencia de un isomorfismo $\gamma : K_1[B_1] \to K_2[B_2]$ que extiende a b y h, y que puede ser extendido al isomorfismo $\gamma_{ext} : K_1(B_1) \to K_2(B_2)$. Como L_1 es clausura algebraica de $K_1(B_1)$ y L_2 lo es de $K_2(B_2)$, llegamos a que γ_{ext} extiende a un isomorfismo h_{ext} que extiende a h. □

Corolario 3.51. *Sean L_1/K_1 y L_2/K_2 extensiones de cuerpos algebraicamente cerradas tales que tr.deg(L_2/K_2) = tr.deg(L_1/K_1). Entonces, L_1 y L_2 son K-isomorfas.*

Corolario 3.52. *Sea L/K extensión de cuerpos algebraicamente cerrada. Entonces, todo K-isomorfismo es extensible a un L-isomorfismo.*

Proposición 3.53. *Sean L/K y M/L extensiones de cuerpos tales que M/L es algebraicamente cerrada y tr.deg(L/K) es finito. Entonces, cualquier K-monomorfismo $u : L \to M$ es extensible a un K-automorfismo de M.*

Demostración. Por la Proposición (3.48.) tenemos que $\text{tr.deg}(M/L) + \text{tr.deg}(L/K) = \text{tr.deg}(M/K) = \text{tr.deg}(M/u(L)) + \text{tr.deg}(u(L)/K)$ y, observando que por inyectividad $\text{tr.deg}(L/K) = \text{tr.deg}(u(L)/K)$, llegamos a que $\text{tr.deg}(M/L) = \text{tr.deg}(M/u(L))$. La extensión de u a un K-automorfismo de M se sigue de la Proposición (3.50.). □

Corolario 3.54. *Sea L/K extensión de cuerpos algebraicamente cerrada con grado de trascendencia finito. Entonces, todo K-endomorfismo es K-automorfismo.*

Definición 3.55. Sea K cuerpo, definimos el **grado de un elemento** $u(x) = \frac{v(x)}{w(x)} \in K(X)$ como $\deg(u) = \max\{\deg(v), \deg(w)\}$.

Lema 3.56. *Sean K cuerpo y $u \in K(X) - K$. Entonces, u es K-trascendente, X es $K(u)$-algebraico y $[K(X) : K(u)] = \deg(u)$.*

Demostración. Sea $u(X) = \frac{v(X)}{w(X)}$ con $v(X)$ y $w(X)$ primos relativos, entonces X es $K(u)$-algebraico dado que $v(T) - w(T)u \in K(u)[T]$ es polinomio no nulo que tiene por raíz a X. Además, u es K-trascendente porque de no ser así se tendría que X sería K-algebraico. Consideramos el irreducible $v(T) - w(T)Z \in K[Z,T]$. Por trascendencia de u tenemos una biyección $h : K[Z,T] \longrightarrow K[u,T]$ definida $h(Z,T) = (u,T)$ y, en consecuencia, $v(T) - w(T)u$ es irreducible en $K[u,T]$ y por el Lema de Gauss también en $K(u)[T]$. Se tiene entonces que $[K(X) : K(u)] = \deg(\text{Irr}(X, K(u))) = \deg(v(T) - w(T)u) = \deg(u)$. □

Teorema 3.57. (Lüroth) *Sea K cuerpo y $K(\alpha)/K$ extensión trascendente simple. Entonces, todo subcuerpo propio E entre $K(\alpha)$ y K es una extensión trascendente de K.*

Demostración. Por el Lema (3.56.) se tiene que $[K(X) : E] \leq [K(X) : K(\alpha)] = \deg(\alpha)$. Entonces $K(X)/E$ es algebraica por ser finita y podemos considerar $f = \mathrm{Irr}(\alpha, E) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n \in E[X]$. Observamos que $\{a_0, \ldots, a_{n-1}\} \nsubseteq K$ dado que α es K-trascendente. Tomamos pues $a_j \in E - K$ y queremos probar que $E = K(a_j)$.

Sea $d(X)$ un polinomio de grado mínimo verificando $d(X)a_i(X) \in K[X]$ para todo $i \subseteq \{1, \ldots, n\}$ y sea $g(X, Y) = d(X)f(Y) = d(X)Y^n + d(X)a_1Y^{n-1} + \ldots + d(X)a_n \in K[X, Y]$. Se tiene que g es primitivo como polinomio en Y, esto es, $mcd(d, da_1, \ldots, da_n) = 1 \in K[X]$. El grado de g en X es $m = \text{máx}_i \deg(da_i)$. Escribiendo $a_i = \frac{b}{c}$ con $b, c \in K[X]$ primos relativos, llegamos a que $b(T) - c(T)a_i(X) \in E[T]$ tiene a X por raíz y es divisible por f. Entonces, $f(Y)q(Y) = b(Y) - c(Y)a_i(X)$ con $q(Y) \in E[Y]$. Multiplicando por $c(X)$, llegamos a la igualdad $c(X)f(Y)q(Y) = c(X)b(Y) - c(Y)b(X)$.

Como g difiere de f por $d \in K(X)$, se tiene que g divide a $c(X)b(Y) - c(Y)b(X)$ en $K(X)[Y]$ y, por ser g primitivo, también en $K[X, Y]$. Así, existe $h \in K[X, Y]$ tal que $g(X, Y)h(X, Y) = c(X)b(Y) - c(Y)b(X)$. Dado que $c(X)b(Y) - c(Y)b(X)$ tiene grado a lo sumo m en X y m es el grado de g en X, se sigue que $c(X)b(Y) - c(Y)b(X)$ tiene grado m y h tiene grado 0 en X, esto es, $h \in K[Y]$. Entonces, $c(X)b(Y) - c(Y)b(X)$ no es divisible por ningún elemento no constante de $K[X]$.

Usando la simetría de $c(X)b(Y) - c(Y)b(X)$ en X y en Y, tenemos que $c(X)b(Y) - c(Y)b(X)$ tiene grado m en Y y es indivisible por cualquier elemento no constante de $K[Y]$. De ello, h es indivisible por cualquier elemento no constante de $K[Y]$ y es pues que $h \in K^\times$. En conclusión, g es múltiplo constante de $c(X)b(Y) - c(Y)b(X)$.

Comparando grados en Y de nuestra igualdad, observamos que $n = m$. Aplicando el Lema (3.56.), se tiene $[K(X) : K(a_i)] = \deg(a_i) \leq \deg(da_i) = m = n = [K(X) : E] \leq [K(X) : K(a_i)]$, y por ello $E = K[a_i]$.

Por la elección de $a_j \notin K$, tenemos $[K(X) : E] \leq [K(X) : K(a_j)] = \deg(a_j) \leq \deg(da_j) \leq \deg(da_i) = m = n = [K(X) : E]$ y así $E = K(a_j)$. □

Para la demostración de este teorema y del lema previo hemos tomado las ideas de [10].

Observación 3.58. El teorema no se verifica si la extensión no es simple.

Definición 3.59. Diremos que una base de trascendencia B de una extensión de cuerpos L/K es una **base pura** cuando $K(B) = L$. En tal caso, se dice que L/K es una **extensión puramente trascendente**.

Ejemplo 3.60. Sea K cuerpo y sea I un conjunto no vacío. Se tiene que $K(X_i)_{i\in I}$, con $\{X_i\}_{i\in I}$ indeterminadas, es extensión puramente trascendente sobre K verificando que $\text{tr.deg}(K(X_i)_{i\in I}/K) = \text{Card}(I)$.

Observación 3.61. Existen extensiones que no son puramente trascendentes.

Ejemplos 3.62. (A)Un ejemplo de extensión no puramente trascendente es L/K con K cuerpo tal que $Car(K) \neq 3$, $K(\alpha)/K$ y $K(\alpha, \beta)/K(\alpha)$ son simples donde $\alpha \in L$ y β es raíz cúbica de $1 - \alpha^3$.

(B)Otro caso es el Ejemplo (4.15.).

Observación 3.63. Toda extensión puramente trascendente admite una base de trascendencia no pura.

Ejemplos 3.64. (A) Sea B base de trascendencia de una extensión puramente trascendente L/K. Entonces $C = \{\alpha^{k_\alpha} \in L |\ \alpha \in B\}$ es base de trascendencia no pura.

(B) Otro caso es $\{\alpha^n\}$ base de $K(\alpha)/K$ trascendente con $[K(\alpha)/K(\alpha^n)] = n$.

Observación 3.65. Sea L/K extensión de cuerpos pura y $K \subset M \subset L$.

(1) Si $\text{tr.deg}(L/K) = 1$, entonces M es puramente trascendente por el Teorema (3.57.).

(2) Si $\text{tr.deg}(L/K) = 2$ y K es algebraicamente cerrado, entonces M es puramente trascendente (Teorema de Castelnuovo).

(3) Existen extensiones L/K con $\text{tr.deg}(L/K) > 2$ que no son trascendentes puras.

4. Extensiones separables

Definición 4.1. Sea F/K una extensión de cuerpos y sean A y B dominios intermedios de la extensión. Se dice que A y B son **linealmente disjuntos** si cualesquiera familias K-linealmente independientes $(\alpha_i)_{i\in I} \subseteq A$ y $(\beta_j)_{j\in J} \subseteq B$ verifican que $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ es también K-linealmente independiente.

Proposición 4.2. *Sea F/K y sean A y B dos dominios intermedios entre K y F que son linealmente disjuntos sobre K.*

(1) Si $(\alpha_i)_{i\in I} \subseteq A$ es base del K-espacio A y $(\beta_j)_{j\in J} \subseteq B$ lo es de B. Entonces, $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ es base del K-espacio AB.

(2) $[AB : K] = [A : K][B : K]$.

(3) $A \cap B = K$.

(4) $K(A)$ y $K(B)$ son linealmente disjuntos sobre K.

Demostración.

(1) Por hipótesis y definición de linealidad disjunta de A y B, tenemos que $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ es K-linealmente independiente. Por otro lado, también tenemos que $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ es sistema generador del K-espacio AB.

(2) Consecuencia del item anterior.

(3) Como A y B son cuerpos intermedios entre F y K tenemos que $A\cap B \subseteq K$. Supongamos por reducción al absurdo que $A \cap B \subset K$ y escogemos $\alpha \in (A\cap B)-K$. Entonces $\{1, \alpha\} \in A\cap B$ es familia en A y B linealmente independiente sobre K, y por definición $\{1, \alpha, \alpha, \alpha^2\}$ sería K-linealmente independiente. Sin embargo, esta familia es K-linealmente dependiente porque hay un elemento repetido y llegamos pues a una contradicción.

(4) Supongamos por reducción al absurdo que $K(A)$ y $K(B)$ no son linealmente disjuntos sobre K. Entonces, existen familias $(\alpha_i)_{i\in I} \subseteq K(A)$ y $(\beta_j)_{j\in J} \subseteq K(B)$ linealmente independientes sobre K verificando que $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ es conjunto linealmente dependiente sobre K. Podemos escoger $(\lambda_{ij})_{(i,j)\in I\times J} \in K$ no todos nulos tales que $\sum_{(i,j)\in I\times J} \lambda_{ij}\alpha_i\beta_j = 0$. Tomamos $\alpha \in A$ y $\beta \in B$ no nulos que satisfagan que $\alpha\alpha_i \in A$ para todo $i \in I$ y $\beta\beta_j \in B$ para todo $j \in J$. Como $\sum_{(i,j)\in I\times J} \lambda_{ij}(\alpha\alpha_i)(\beta\beta_j) = 0$, se tiene que $((\alpha\alpha_i)(\beta\beta_j))_{(i,j)\in I\times J}$ es K-linealmente dependiente, en contradicción con la hipótesis de linealidad disjunta de A y B.

□

Proposición 4.3. *Sea F/K extensión de cuerpos, A un dominio intermedio entre K y F y sea M un cuerpo intermedio entre K y F. Suponemos que A y M son linealmente disjuntos sobre K. Entonces:*

(1) Si $(\alpha_i)_{i\in I} \subseteq A$ es linealmente independiente sobre K, lo es sobre M.

(2) Toda base del K-espacio A es una base del M-espacio AM.

(3) $[A : K] = [AM : M]$.

Demostración.

(1) Sea una combinación M-lineal finita nula, $\sum_{i\in I} \alpha_i m_i = 0$ con $(m_i)_{i\in I} \subseteq M$ casi todos nulos. Tomamos $(\beta_j)_{j\in J} \subseteq M$ base lineal de M sobre K, entonces $m_i = \sum_{j\in J} \lambda_{ij}\beta_j$ con $(\lambda_{ij})_{j\in J} \in K$ casi todos nulos para cada $i \in I$. Se tiene pues una matriz $L = (\lambda_{ij})_{ij}$ cuyas columnas vienen indizadas por i. Como hay un número finito de m_i, entonces hay un número finito de columnas no nulas. En consecuencia, los λ_{ij} son casi todos nulos. Se tiene que $0 = \sum_{i\in I} m_i\alpha_i = \sum_{i\in I}(\sum_{j\in J} \lambda_{ij}\beta_j)\alpha_i = \sum_{i,j} \lambda_{ij}\beta_j\alpha_i$, una expresión imposible por ser M y A linealmente disjuntos sobre K salvo que cada λ_{ij} sea nulo y por tanto cada m_i nulo.

(2) Resultado del item anterior y del hecho de que un sistema generador del K-espacio A es sistema generador del M-espacio AM.

(3) Consecuencia del item anterior.

□

Proposición 4.4. *Sea F/K extensión de cuerpos y sean A y B dos dominios intermedios entre K y F. Si existe $(\alpha_i)_{i\in I} \subseteq A$ base del K-espacio A y $(\beta_j)_{j\in J} \subseteq B$ base del K-espacio B tal que $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ es linealmente independiente sobre K. Entonces, A y B son linealmente disjuntos sobre K.*

Demostración. Sean $(a_z)_{1\le z\le m} \subseteq A$ y $(b_y)_{1\le y\le n} \subseteq B$ conjuntos K-linealmente independientes. Existen subconjuntos finitos $\widetilde{I} \subseteq I$ y $\widetilde{J} \subseteq J$ tales que $(a_z)_{1\le z\le m} \subseteq \sum_{i\in\widetilde{I}} K\alpha_i$ y $(b_y)_{1\le y\le n} \subseteq \sum_{j\in\widetilde{J}} K\beta_j$. Dado que se verifica $[\sum_{i\in\widetilde{I}} K\alpha_i \colon K] = \mathrm{Card}(\widetilde{I}) = r$ y $[\sum_{j\in\widetilde{J}} K\beta_j \colon K] = \mathrm{Card}(\widetilde{J}) = s$, se tiene que $m \le r$ y $n \le s$ y podemos escoger $(a_z)_{m+1\le z\le r} \subseteq A$ y $(b_y)_{n+1\le y\le s} \subseteq B$ tales que $(a_z)_{1\le z\le r} \subseteq A$ es base del K-espacio $\sum_{i\in\widetilde{I}} K\alpha_i$ y $(b_y)_{1\le y\le s} \subseteq B$ base del K-espacio $\sum_{j\in\widetilde{J}} K\beta_j$. Como $\sum_{i\in\widetilde{I}} K\alpha_i = \sum_{1\le z\le r} Ka_z$ y $\sum_{j\in\widetilde{J}} K\beta_j = \sum_{1\le y\le s} Kb_y$ se tiene que $\sum_{(i,j)\in\widetilde{I}\times\widetilde{J}} K\alpha_i\beta_j = \sum_{1\le z\le r,1\le y\le s} Ka_zb_y$. Por ello, $(a_zb_y)_{1\le z\le r,1\le y\le s}$ es sistema generador del K-espacio $\sum_{(i,j)\in\widetilde{I}\times\widetilde{J}} K\alpha_i\beta_j$. Es más, es base por nuestra suposición que implica que es rs-dimensional. Esto implica que $(a_zb_y)_{1\le z\le m,1\le y\le n}$ es linealmente independiente sobre K. □

Proposición 4.5. *Sea F/K extensión de cuerpos, A un dominio intermedio entre K y F y sea M un cuerpo intermedio entre K y F. Si existe $(\alpha_i)_{i\in I} \subseteq A$ base del K-espacio A que es linealmente independiente sobre M, entonces A y M son linealmente disjuntos sobre K.*

Demostración. Dado que $(\alpha_i)_{i\in I} \subseteq A$ es K-base de A, es también un sistema generador del M-espacio AM. Es más, es base por hipótesis de que es una familia M-linealmente independiente. Sea $(m_j)_{j\in J}$ una K-base lineal de M, se tiene que $(\alpha_i m_j)_{(i,j)\in I\times J}$ es base del K-espacio AM, en particular es K-linealmente independiente. Por la Proposición (4.4.) podemos concluir que A y M son linealmente disjuntos sobre K. □

Proposición 4.6. *Sean L/K y M/L extensiones de cuerpos y sea $S \subseteq M$ algebraicamente independiente sobre L. Entonces, $K(S)$ y L son linealmente disjuntos sobre K.*

Demostración. Sea $D = \{\alpha_1, \ldots, \alpha_n\} \subseteq S$. Por hipótesis de independencia algebraica de S sobre L, tenemos que $(\prod_{i=1}^{n} \alpha_i^{k_z})_{k_1,\ldots,k_n\in N}$ es linealmente independiente sobre L, por lo que es base del K-espacio $K[D]$. Por la Proposición (4.5.), se tiene que $K[D]$ y L son linealmente disjuntos sobre K. Sea $\Omega = \{F \subseteq S |\ F \text{ es finito}\}$, se verifica que $(K[D])_{D\in\Omega}$ es filtrado con $K[S] = \cup_{D\in\Omega} K[D]$. En consecuencia, $K[S]$ y L son linealmente disjuntos sobre K. Concluimos la demostración como resultado de la Proposición (4.2.) aplicado a $K(S)$, que es el cuerpo de fracciones de $K[S]$ en M. □

Proposición 4.7. *Sean L/K y M/L extensiones de cuerpos con M finitamente generado sobre K. Entonces, L es finitamente generado sobre K.*

Demostración. Sea S base de trascendencia de L/K y T base de trascendencia de M/L. Entonces, $S\cup T$ es base de trascendencia de M/K y, por hipótesis de que M es finitamente generado sobre K, tenemos la finitud de S y T y que M es finito sobre $K(S\cup T) = K(S)(T)$. De la independencia algebraica de T sobre L y usando la Proposición (4.6.), se sigue que $K(S\cup T)$ y L son linealmente disjuntos sobre $K(S)$. Por la Proposición (4.3.), toda base lineal de L sobre $K(S)$ es linealmente independiente sobre $K(S\cup T)$. En consecuencia, dado que hemos visto que M es finito sobre $K(S\cup T)$, tenemos que toda base lineal de L sobre $K(S)$ es finita. Esto implica que L es finito sobre $K(S)$ y, al ser S finito, L es finitamente generado sobre K. □

Proposición 4.8. *Sea F/K extensión de cuerpos tal que K tiene de característica un primo p.*

(1) Si K y L^p son linealmente disjuntos sobre K^p y $(\alpha_i)_{i\in I} \subseteq L$ es linealmente independiente sobre K. Entonces, $(\alpha_i^{p^n})_{i\in I} \subseteq L$ es linealmente independiente sobre K.

(2) Si existe $(\alpha_i)_{i\in I} \subseteq L$ base lineal de L sobre K tal que $(\alpha_i^{p^n})_{i\in I} \subseteq L$ es linealmente independiente sobre K, entonces K y L^p son linealmente disjuntos sobre K^p.

Demostración. Una familia $(l_j)_{j\in J}$ de elementos de L es base lineal de L/K si y solo si $(l_j^p)_{j\in J}$ es base lineal de L^p/K^p. De la Proposición (4.3.) probamos (1) para el caso $n = 1$ y el caso general se demuestra aplicando inducción. Por otro lado, tenemos probado (2) haciendo uso de la Proposición (4.5.). □

Definición 4.9. Sea K cuerpo, se dice que $f \in K[X]$ es **K-separable** cuando sus factores K-irreducibles tienen ceros simples.
Una extensión de cuerpos L/K algebraica será **extensión separable** cuando $\mathrm{Irr}(\alpha, K)$ es K-separable para todo elemento $\alpha \in L$.

Ahora vamos a relacionar el concepto de separabilidad con el de linealidad disjunta para extender la definición de extensión separable al área de las extensiones trascendentes. Para ello, vamos a ver dos resultados en los que intervendrá el subgrupo generado por la unión de dos conjuntos. Dados H y G conjuntos, notaremos por $H \vee G$ al subgrupo generado por $H \cup G$.

Proposición 4.10. *Sea F/K extensión de cuerpos tal que K tiene de característica un primo p.*

(1) Si L/K es separable, entonces $L = K \vee L^p$.

(2) Si $L = K \vee L^p$ y L/K es finita, entonces L/K es separable.

Demostración.

(1) Empezamos notando que $L^p \subseteq K \vee L^p$, lo que lleva a que $L/K \vee L^p$ sea puramente inseparable. Si L/K es separable tendremos que también lo es $L/K \vee L^p$, por lo que $L = K \vee L^p$.

(2) Sea $[L : K] = n$ y $(l_i)_{1\leq i\leq m} \subseteq L$ linealmente independiente. Se tiene que $m \leq n$ y podemos considerar la extensión de $(l_i)_{1\leq i\leq m}$ a una base lineal $(l_i)_{1\leq i\leq n}$ de L/K. Como $L = \sum_{i=1}^n Kl_i$, se tiene que $L^p = \sum_{i=1}^n K^p l_i^p$. Dado que L/K es finita, es algebraica y se tiene que $L = K \vee L^p = KL^p = \sum_{i=1}^n Kl_i^p$. En consecuencia, $(l_i^p)_{1\leq i\leq n}$ es sistema generador del K-espacio L. Es más, es base de L/K al ser n-dimensional.

Se sigue pues que $(l_i^p)_{1\leq i\leq m}$ es K-linealmente independiente. Sea $\alpha \in L$ y f el polinomio minimal de α sobre K con $\deg(f) = n$. Entonces, $(\alpha^i)_{0\leq i\leq n-1}$ es K-linealmente independiente y $(\alpha^{ip})_{0\leq i\leq n-1}$ lo es también. Si f no fuera separable, se tendría que $f \in K[X^p]$. Entonces, $f(X) = g(X^p)$ con $g \in K[X]$ tal que $\deg(g) = m$. Se sigue de $g(\alpha^p) = f(\alpha) = 0$ que $(\alpha^{ip})_{0\leq i\leq m}$ es K-linealmente dependiente, en contradicción con que $n = \deg(f) = p\deg(g) = pm > m$. En conclusión, f es separable y por ello α es K-separable.

□

Proposición 4.11. *Sea F/K extensión algebraica de cuerpos tal que K tiene de característica un primo p. Entonces, L es separable sobre K si y solo si K y L^p son linealmente disjuntos sobre K^p.*

Demostración. Para la implicación directa consideramos $(\alpha_i)_{1\leq i\leq n} \subseteq L$ linealmente independiente sobre K. Entonces, $K(\alpha_1, \ldots, \alpha_n)/K$ es separable. Por uso de la Proposición (4.10.) tenemos que $K(\alpha_1, \ldots, \alpha_n) = K \vee K(\alpha_1, \ldots, \alpha_n)^p$ y que, por finitud de $K(\alpha_1, \ldots, \alpha_n)/K$, el conjunto $(\alpha_i)_{1\leq i\leq n}$ es K-linealmente independiente.
La implicación inversa de sigue de la parte final de la demostración de la Proposición (4.10.). □

Definición 4.12. Se dirá que F/K es **extensión separable** si $\mathrm{Car}(K) = 0$ o $\mathrm{Car}(K) = p$ con p primo y K y L^p son linealmente disjuntos sobre K^p.

Proposición 4.13. *Sea F/K tal que K tiene de característica un primo p.*

(1) Si L/K es extensión separable y M/L es extensión de cuerpos. Entonces, L y $P(M/K) = \{m \in M |\ m$ es puramente inseparable sobre $K\}$ son linealmente disjuntos sobre K.

(2) Si existe M/L extensión perfecta tal que L y $\mathcal{A} = \{\alpha \in M |\ \alpha^p \in K\}$ son linealmente disjuntos sobre K. Entonces, L/K es extensión separable.

Demostración.

(1) Sea $(\alpha_i)_{i\in I} \subseteq L$ tal que $\sum_{i\in I} \alpha_i\beta_i = 0$, con $\beta_i \in P(M/K)$. Para cada $i \in I$ existe n_i entero positivo tal que $\beta_i^{p^{n_i}} \in K$. Sea $n = sup_{i\in I} n_i$, entonces $\beta_i^{p^n} \in K$ para todo $i \in I$. Por la Proposición (4.8.), tenemos que $(\alpha_i^{p^n})_{i\in I}$ es K-linealmente independiente. Como $\sum_{i\in I} \alpha_i^{p^n}\beta_i^{p^n} = (\sum_{i\in I} \alpha_i\beta_i)^{p^n} = 0$ se sigue que $\beta_i^{p^n} = 0$ para cada $i \in I$. En consecuencia, toda familia finita no vacía de elementos de L que es K-linealmente independiente es linealmente independiente sobre $P(M/K)$, y por la Proposición (4.5.) tenemos que L y $P(M/K)$ son linealmente disjuntos sobre K.

(2) Consideramos ϕ el endomorfismo de Frobenius de M, que es un automorfismo por la hipótesis de que M es perfecto. Dado que $\phi(\mathcal{A}) = K$, $\phi(L) = L^p$ y $\phi(K) = K^p$, la linealidad disjunta de K y L^p sobre K^p equivale a la de $\mathcal{A}$ y L sobre K.

□

Proposición 4.14. *Sea L/K extensión de cuerpos puramente trascendental. Entonces, L/K es extensión separable.*

Demostración. Sea S una base pura de L/K y $T = \phi(S)$ con ϕ el endomorfismo de Frobenius de L. Entonces, $L^p = K(S)^p = K^p(T)$ y T es K-algebraicamente independiente. Ahora, la Proposición (4.6.) implica que K y L^p son K^p-linealmente disjuntos. □

Ejemplo 4.15. (Extensión trascendente no separable) Sea K cuerpo de característica p primo, por ejemplo $\mathbb{F}^p$. Consideramos la extensión $K(a, b, c)$ puramente trascendente. Sea ξ raíz p-ésima de $ac^p + b$, esto es, $\xi^p = ac^p + b$ $(*^1)$. Se tiene que $K(a, b, c, \xi)/K(a, b)$ es trascendente por ser c trascendente sobre $K(a, b)$. Sin embargo, vamos a ver que es una extensión no separable.

Por definición de ξ, tenemos que $ac^p + b - \xi^p = 0$. En consecuencia, $\{1, c^p, \xi^p\}$ es un conjunto linealmente dependiente sobre $K(a, b)$. Para ver que la extensión $K(a, b, c, \xi)/K(a, b)$ no es separable vamos a ver que $\{1, c, \xi\}$ es un conjunto linealmente independiente sobre $K(a, b)$, condición dada por (4.8.).

Supongamos que existen $\alpha, \beta, \gamma \in K(a, b)$ tales que $\alpha + c\beta + \xi\gamma = 0$, queremos ver que $\alpha = \beta = \gamma = 0$. Como tales elementos están en el cuerpo de fracciones, podemos multiplicarlos por el mínimo común múltiplo de manera que existen $f_0, f_1, f_2 \in K[a, b]$ tales que $f_0 + cf_1 + \xi f_2 = 0$ $(*^2)$.

Consideramos el endomorfismo de Frobenius $\phi : K[a, b] \longrightarrow K[a, b]$ definida $\phi(x) = x^p$ para $x \in K$. Usando la notación $\overline{f} = \phi(f)$ y aplicando ϕ a nuestra relación $(*^2)$ llegamos a que $\overline{f}_0 + c\overline{f}_0 + \xi\overline{f}_2 = 0$.

Tomamos el endomorfismo de Frobenius $\Phi : K(a, b, c, \xi) \longrightarrow K(a, b, c, \xi)$ definida $\Phi(x) = x^p$ para $x \in K(a, b, c, \xi)$. Análogamente, aplicando Φ a $(*^2)$ y usando la misma notación para la imagen, tenemos que $\overline{f}_0 + c^p\overline{f}_0 + \xi^p\overline{f}_2 = 0$ (ahora hemos elevado a p todos los coeficientes de f_i, $\overline{f}_i(a^p, b^p)$, mientras que antes los que se elevaban a p eran únicamente los pertenecientes a K, $\overline{f}_i(a, b)$).

Intercambiando en la última expresión obtenida ξ^p por la relación dada en $(*^1)$ obtenemos $0 = \overline{f}_0 + c^p\overline{f}_0 + (ac^p + b)\overline{f}_2 = (\overline{f}_0 + b\overline{f}_2) + (\overline{f}_1 + a\overline{f}_2)c^p$ (polinomio en a, b, c), de lo que se sigue por un lado que $0 = \overline{f}_0 + b\overline{f}_2$ y por otro que $0 = \overline{f}_1 + a\overline{f}_2$ (polinomios en a, b, c). Entonces, $\overline{f}_0 = \overline{f}_1 = \overline{f}_2 = 0$. En consecuencia, $\alpha = \beta = \gamma = 0$.

Proposición 4.16. *Sean L/K y M/L extensiones de cuerpos.*

(1) Si L/K y M/L son separables, entonces M/K es extensión separable.

(2) Si M/K es extensión separable, entonces L/K es separable.

Demostración.

(1) Sea $(\alpha_i)_{i\in I}$ base lineal de L/K y $(\beta_j)_{j\in J}$ base lineal de M/L. Por hipótesis de separabilidad de L/K tenemos, haciendo uso de la Proposición (4.8.), que $(\alpha_i^p)_{i\in I}$ es K-linealmente independiente y $(\beta_j^p)_{j\in J}$ es L-linealmente independiente. Además, notamos que $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ es base lineal de M/K, así como también $(\alpha_i^p\beta_j^p)_{(i,j)\in I\times J}$ es K-linealmente independiente. Usando otra vez la Proposición (4.8.), tenemos probada la separabilidad de M/K por la existencia de una base lineal.

(2) Dado que por un lado $K^p \subseteq L^p \subseteq M^p$ y por otro M^p y K son K^p-linealmente disjuntos, tenemos que L^p y K son K^p-linealmente disjuntos. □

Observación 4.17. El recíproco de (1) en la proposición anterior no es cierto y lo vemos con un contraejemplo. Consideramos K cuerpo de característica p primo y α trascendente sobre K, entonces $K(\alpha)/K$ es extensión trascendente simple. De la Proposición (4.14.) se sigue que $K(\alpha)/K$ es separable. Sin embargo, $K(\alpha)/K(\alpha^p)$ no es extensión separable al ser puramente inseparable ($\mathrm{Irr}(\alpha, K(\alpha^p)) = X^p - \alpha^p = (X-\alpha)^p$) verificando $K(\alpha) \neq K(\alpha^p)$.

Proposición 4.18. *Sea L/K extensión separable de cuerpos tal que K tiene de característica un primo p. Si $(\alpha_i)_{i\in I} \subseteq L$ es base lineal de L sobre K, entonces $(\alpha_i^{p^n})_{i\in I}$ es base del K-espacio KL^p.*

Demostración. Por hipótesis y usando la Proposición (4.8.), tenemos que $(\alpha_i^p)_{i\in I}$ es K-linealmente independiente. Además, por el hecho de que $L = \sum_{i\in I} K\alpha_i$ se sigue que $L^p = \sum_{i\in I} K^p\alpha_i^p$. En consecuencia, $KL^p = \sum_{i\in I} K\alpha_i^p$ y por ello $(\alpha_i^p)_{i\in I}$ es también sistema generador del K-espacio KL^p. □

Corolario 4.19. *Sea L/K extensión separable algebraica de cuerpos tal que K tiene de característica un primo p. Si $(\alpha_i)_{i\in I} \subseteq L$ es base lineal de L sobre K, entonces $(\alpha_i^{p^n})_{i\in I}$ es base de K.*

Demostración. Consideramos la Proposición (4.10.) y la igualdad $KL = K \vee L$, resultado de ser L/K algebraica. Tenemos que $L = K \vee L^p = KL^p$. □

Proposición 4.20. *Sean L/K y M/L extensiones de cuerpos tal que L/K es algebraica y M/K es separable. Entonces, M/L es extensión separable.*

Demostración. Sea $(\alpha_i)_{i\in I}$ base lineal de L/K y sea $(\beta_j)_{j\in J}$ base lineal de M/L, tenemos que $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ es base lineal de M/K. Dado que esta extensión es separable, por la Proposición (4.8.) tenemos que $(\alpha_i^p\beta_j^p)_{(i,j)\in I\times J}$ es K-linealmente independiente. Usando la Proposición (4.16.) tenemos la separabilidad de L/K. Dado que L/K es algebraica y separable, aplicando el corolario (4.19.) tenemos que $(\alpha_i^p)_{i\in I}$ es base lineal de L/K. Consideramos ahora $(\beta_j^p)_{j\in J}$ tal que $\sum_{j\in J}\lambda_j\beta_j^p = 0$, con $(\lambda_j)_{j\in J} \subseteq L$ casi todos nulos. Como $(\alpha_i^p)_{i\in I}$ es base lineal de L/K, podemos expresar $\lambda_i = \sum_{i\in I} k_{ij}\alpha_i^p$ donde $(k_{ij})_{i\in I} \subseteq K$ son casi todos nulos. Entonces, $k_{ij} = 0$ para casi todo $(i,j) \in I\times J$ y $\sum_{(i,j)\in I\times J} k_{ij}\alpha_i\beta_j = \sum_{j\in J}\lambda_j\beta_j^p = 0$. Por la independencia lineal de $(\alpha_i^p\beta_j^p)_{(i,j)\in I\times J}$ sobre K llegamos a que $k_{ij} = 0$ para todo $(i,j) \in I\times J$, lo cual implica que $\lambda_j = 0$ para todo $j \in J$. Concluimos entonces que $(\beta_j^p)_{j\in J}$ es L-linealmente independiente y por la Proposición (4.8.) tenemos que M/L es separable. □

Proposición 4.21. *Sean L/K extensión de cuerpos tal que K es perfecto. Entonces, L/K es extensión separable.*

Demostración. Si $\mathrm{Car}(K) = p$, entonces $K^p = K$. En consecuencia, cualquier extensión de cuerpos L/K verifica que K y L^p son linealmente disjuntos sobre K^p. □

5. Derivaciones de cuerpos

Vamos ahora a presentar una clase especial de aplicaciones para estudiar la separabilidad de cuerpos desde otro contexto.

Definición 5.1. Sea F cuerpo y A subdominio suyo, llamamos **derivación de A en F** a una aplicación $D : A \longrightarrow F$ tal que $D(\alpha+\beta) = D(\alpha) + D(\beta)$ y $D(\alpha\beta) = \beta D(\alpha) + \alpha D(\beta)$.

Particularmente, llamamos derivación de F a una derivación de F en F.

Ejemplos 5.2.

(A) Sea F cuerpo y A subdominio suyo, la aplicación $D : A \longrightarrow F$ tal que $D(\alpha) = 0$ para todo $\alpha \in A$ es una derivación de A en F, derivación trivial.

(B) Sea K un cuerpo, la aplicación $D : K[X] \longrightarrow K(X)$ tal que $D(f) = f'$ es una derivación de $K[X]$ en $K(X)$. Más general y considerando un conjunto I, la aplicación $D_l : K[X_i]_{i\in I} \longrightarrow K(X_i)_{i\in I}$ definida $D_l(f) = \frac{\partial f}{\partial X_l}$ para cada $l \in I$ es una derivación de $K[X_i]_{i\in I}$ en $K(X_i)_{i\in I}$.

Proposición 5.3. *Sean F cuerpo, A subdominio suyo y $D : A \longrightarrow F$ derivación. Entonces:*
(1) $D(1) = 0$.
(2) $D(\alpha) = n\alpha^{n-1}D(\alpha)$.
(3) $D(\frac{\alpha}{\beta}) = \frac{\beta D(\alpha) - \alpha D(\beta)}{\beta^2}$.

Demostración.

(1) $D(1) = D(1\cdot 1) = 1D(1) + 1D(1)$, por lo que $D(1) = 0$.

(2) Lo probamos para $n > 0$ por inducción sobre n. Para $n = 1$ tenemos probada la igualdad de forma trivial. Supongamos que se verifica $D(\alpha) = n\alpha^{n-1}D(\alpha)$ para n entero positivo. Veamos que se verifica también para $n+1$: $D(\alpha^{n+1}) = D(\alpha\alpha^n) = \alpha^n D(\alpha) + \alpha D(\alpha^n) \overset{hip}{=} \alpha^n D(\alpha) + \alpha(n\alpha^{n-1}D(\alpha)) = \alpha^n D(\alpha) + n\alpha^n D(\alpha) = (n+1)\alpha^n D(\alpha)$. Vamos a ver ahora que se cumple la hipótesis también para $n < 0$ observando que: $0 = D(1) = D(\alpha^n\alpha^{-n}) = \alpha^{-n}D(\alpha^n) + \alpha^n D(\alpha^{-n}) \overset{hip.-n>0}{=} \alpha^{-n}D(\alpha^n) + \alpha^n(-n\alpha^{-n-1}D(\alpha)) = \alpha^{-n}D(\alpha^n) - n\alpha^{-1}D(\alpha)$.

(3) $D(\alpha) = D(\beta(\beta^{-1}\alpha)) = (\beta^{-1}\alpha)D(\beta) + \beta D(\beta^{-1}\alpha)$, por lo que tenemos $D(\frac{\alpha}{\beta}) = D(\beta^{-1}\alpha) = \beta^{-2}(\beta D(\alpha) - \alpha D(\beta)) = \frac{\beta D(\alpha) - \alpha D(\beta)}{\beta^2}$.

□

Proposición 5.4. *Sea A dominio con K su cuerpo de fracciones, L/K extensión de cuerpos y D derivación de A en L. Entonces, existe una única extensión a K que sea derivación, a saber, $D_{ext} : K \longrightarrow L$ definida $D_{ext}(\frac{\alpha}{\beta}) = \frac{\beta D(\alpha)-\alpha D(\beta)}{\beta^2}$.*

Demostración. Por la Proposición (5.3.), si buscamos D_{ext} derivación de K en L extensión de D se tiene que verificar que $D_{ext}(\frac{\alpha}{\beta}) = \frac{\beta D_{ext}(\alpha)-\alpha D_{ext}(\beta)}{\beta^2} = \frac{\beta D(\alpha)-\alpha D(\beta)}{\beta^2}$ para todo $\alpha, \beta \in A$ con $\beta \neq 0$. Voy a considerar entonces la aplicación $D_{ext} : K \longrightarrow L$ tal que $\frac{\alpha}{\beta} \to \frac{\beta D(\alpha)-\alpha D(\beta)}{\beta^2}$.
Veamos que está bien definida. Sean $\alpha, \beta, \lambda, \mu \in A$ tales que $\beta, \mu \neq 0$ y $\frac{\alpha}{\beta} = \frac{\lambda}{\mu}$. Entonces $\alpha\mu = \lambda\beta$ y $\mu D(\alpha) + \alpha D(\mu) = D(\alpha\mu) = D(\lambda\beta) = \beta D(\lambda) + \lambda D(\beta)$. De tales igualdades obtenemos que $\mu D(\alpha) - (\frac{\alpha\mu}{\beta})D(\beta) = \beta D(\lambda) - (\frac{\beta\lambda}{\mu})D(\mu)$. Dividiendo entre $\beta\mu$ llegamos a que $\frac{\beta D(\alpha)-\alpha D(\beta)}{\beta^2} = \frac{\mu D(\lambda)-\lambda D(\mu)}{\mu^2}$, lo cual prueba que nuestra aplicación está bien definida.
Veamos que es derivación. Sean $\frac{\alpha}{\beta}, \frac{\lambda}{\mu} \in K$, tenemos $D(\frac{\alpha}{\beta} + \frac{\lambda}{\mu}) = D(\frac{\alpha\mu+\lambda\beta}{\beta\mu}) = \frac{\beta\mu D(\alpha\mu+\lambda\beta)-(\alpha\mu+\lambda\beta)D(\beta\mu)}{(\beta\mu)^2} = \frac{\beta\mu[\mu D(\alpha)+\alpha D(\mu)+\beta D(\lambda)+\lambda D(\beta)]-(\alpha\mu+\lambda\beta)[\mu D(\beta)+\beta D(\mu)]}{(\beta\mu)^2} = \frac{\beta\mu^2 D(\alpha)+\beta^2\mu D(\lambda)-(\alpha\mu^2 D(\beta)+\beta^2\lambda D(\mu))}{(\beta\mu)^2} = \frac{\beta D(\alpha)-\alpha D(\beta)}{\beta^2} + \frac{\mu D(\lambda)-\lambda D(\mu)}{\mu^2} = D(\frac{\alpha}{\beta}) + D(\frac{\lambda}{\mu})$.
Por otro lado, vemos que se verifica $D(\frac{\alpha}{\beta}\frac{\lambda}{\mu}) = D(\frac{\alpha\lambda}{\beta\mu}) = \frac{\beta\mu D(\alpha\lambda)-\alpha\lambda D(\beta\mu)}{(\beta\mu)^2} = \frac{\beta\mu[\lambda D(\alpha)+\alpha D(\lambda)]-\alpha\lambda[\mu D(\beta)+\beta D(\mu)]}{(\beta\mu)^2} = \frac{\mu\lambda[\beta D(\alpha)-\alpha D(\beta)]+\alpha\beta[\mu D(\lambda)-\lambda D(\mu)]}{(\beta\mu)^2} = \frac{\lambda}{\mu}\frac{\beta D(\alpha)-\alpha D(\beta)}{\beta^2}$
$+ \frac{\alpha}{\beta}\frac{\mu D(\lambda)-\lambda D(\mu)}{\mu^2} = \frac{\lambda}{\mu}D(\frac{\alpha}{\beta}) + \frac{\alpha}{\beta}D(\frac{\lambda}{\mu})$.

□

Proposición 5.5. *Sea K cuerpo, L/K extensión y sean D y E derivaciones de K en L. Entonces:*
(1) $\Omega = \{\alpha \in K |\ D(\alpha) = E(\alpha)\} \subseteq K$ es un subcuerpo.
(2) Si $S \subseteq K$ es tal que $D = E$ en S, entonces $D = E$ en $K(S)$.
(3) $D = E$ en el cuerpo primo de K.

Demostración.

(1) Se sigue de la definición de derivación y de la Proposición (5.3.). Observamos que $0, 1 \in \Omega$, dado que $D(0) = 0 = E(0)$ y $D(1) = 0 = E(1)$. Además, para $\alpha, \beta \in \Omega$ se verifica que $D(\alpha-\beta) = D(\alpha)-D(\beta) = E(\alpha)-E(\beta) = E(\alpha-\beta)$ y $D(\alpha\beta^{-1}) = \frac{\beta D(\alpha)-\alpha D(\beta)}{\beta^2} = \frac{\beta E(\alpha)-\alpha E(\beta)}{\beta^2} = E(\alpha\beta^{-1})$, por lo que $\alpha-\beta, \alpha\beta^{-1} \in \Omega$.

(2) Consecuencia del item anterior teniendo en cuenta que $S \subseteq \Omega$, por lo que $K(S) \subseteq \Omega$ por ser $K(S)$ el menor subcuerpo que contiene a S.

(3) Dado que P el subcuerpo primo de K es la intersección de subcuerpos de K, tenemos $P \subseteq \Omega$ y por ello $D = E$ en tal.

□

Observación 5.6. Sea L/K extensión de cuerpos y sea D derivación de K en L:

(1) $\{\alpha \in K |\ D(\alpha) = 0\} \subseteq K$ es un subcuerpo.

(2) Si K es cuerpo primo, D es necesariamente la derivación trivial.

Definición 5.7. Sea K cuerpo, L/K y M/L extensiones y sea D derivación de L en M. Diremos que D es K**-derivación** si $D(\alpha) = 0$ para todo $\alpha \in K$.

Ejemplos 5.8. Sea K un cuerpo e I un conjunto:

(A) Existe una K-derivación $D_{ext} : K(X) \longrightarrow K(X)$ definida $D(\frac{f}{g}) = \frac{gf' - fg'}{g^2}$, la cual es la única derivación de $K(X)$ extensión de la derivación D definida en el Ejemplo (5.2.) (B).

(B) Para cada $l \in I$, existe una K-derivación $D_{l_{ext}} : K(X_i)_{i\in I} \longrightarrow K(X_i)_{i\in I}$ definida $D_{l_{ext}}(\frac{f}{g}) = \frac{g\frac{\partial f}{\partial X_l} - f\frac{\partial g}{\partial X_l}}{g^2}$, la cual es la única derivación de $K(X_i)_{i\in I}$ extensión de la derivación D_l definida en el Ejemplo (5.2.) (B).

Proposición 5.9. *Sea K cuerpo y L/K extensión.*

(1) Si P es el subcuerpo primo de K y D es derivación de K en L, entonces D es P-derivación.

(2) Si K tiene característica p primo, entonces toda derivación D de K en L es una K^p-derivación.

Demostración.

(1) Como P es el subcuerpo primo de K, es tal que verifica $P \subseteq \{\alpha \in K |\ D(\alpha) = 0\} \subseteq K$. Por ello, D es una P-derivación.

(2) Dado que $\mathrm{Car}(K) = p$, tenemos $p\alpha^{p-1}D(\alpha) = D(\alpha^p) = D(1) = 0$ para toda $\alpha \in K$. Entonces, D es una K^p-derivación.

□

Proposición 5.10. *Sean L/K y M/L extensiones de cuerpos.*

(1) Una derivación D de L en M es K-derivación si y solo si es K-lineal.

(2) Si K tiene característica p primo y D es una K-derivación de L en M, entonces D es una $K \vee L^p$-derivación.

Demostración.

(1) Supongamos que D es K-derivación, entonces para toda $\alpha \in K$ y $\beta \in L$ tenemos que $D(\alpha\beta) = \beta D(\alpha) + \alpha D(\beta) = \alpha D(\beta)$, por lo que D es K-lineal. Recíprocamente, supongamos que D es K-lineal, entonces para todo $\alpha \in K$ se tiene $D(\alpha) = D(\alpha \cdot 1) = \alpha D(1) = 0$, de lo que se sigue que D es K-derivación.

(2) Por la Proposición (5.9.), tenemos que D es una L^p-derivación. En consecuencia, $D(\alpha) = 0$ para toda $\alpha \in K \cup L^p$. Como $K \vee L^p$ es subcuerpo de L generado por $K \cup L^p$, por la Proposición (5.5.) tenemos $D(\alpha) = 0$ para todo $\alpha \in K \vee L^p$.

□

Definición 5.11. Sea L/K extensión de cuerpos y sea D derivación de K en L. Para cada $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, denotamos $f^D = \sum_{i=0}^{n} D(a_i)X^i \in L[X]$.

Proposición 5.12. *Sea L/K extensión de cuerpos y D una derivación de K en L.*

(1) $A : K[X] \longrightarrow L[X]$ definida $f \to f^D$ es una derivación.

(2) Si $\alpha \in K$ y $f \in K[X]$, entonces $D(f(\alpha)) = f^D(\alpha) + f'(\alpha)D(\alpha)$.

Demostración.

(1) Sean $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ y $g = \sum_{i=0}^{m} b_i X^i \in K[X]$.

Observamos que:

$$\begin{aligned} A(f+g) &= (f+g)^D \\ &= (\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i)^D = \sum_{i=0}^{n} D(a_i)X^i + \sum_{i=0}^{m} D(b_i)X^i \\ &= f^D + g^D = A(f) + A(g). \end{aligned}$$

Por otro lado,

$$\begin{aligned} A(fg) = (fg)^D &= \left(\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{i=0}^{m} b_i X^i\right)\right)^D \\ &= \left(\sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_i b_{k-i}\right)X^k\right)^D = \sum_{k=0}^{n+m}\sum_{i=0}^{k} D(a_i b_{k-i})X^k \\ &= \sum_{k=0}^{n+m}\sum_{i=0}^{k}(a_i D(b_{k-i}) + D(a_i)b_{k-i})X^k \\ &= \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_i D(b_{k-i})\right)X^k + \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} D(a_i)b_{k-i}\right)X^k \\ &= f(g^D) + g(f^D) = fA(g) + gA(f). \end{aligned}$$

(2) Sea $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ y sea $\alpha \in K$, entonces desarrollando tenemos que $D(f(\alpha)) = D(\sum_{i=0}^{n} a_i\alpha^i) = \sum_{i=0}^{n} D(a_i\alpha^i) = \sum_{i=0}^{n} D(a_i)\alpha^i + \sum_{i=0}^{n} a_i D(\alpha^i) = \sum_{i=0}^{n} D(a_i)\alpha^i + \sum_{i=0}^{n} i a_i \alpha^{i-1} D(\alpha) = f^D(\alpha) + f'(\alpha)D(\alpha)$. □

Proposición 5.13. *Sea K cuerpo, L/K extensión, $\alpha, \beta \in L$ y J ideal de relaciones algebraicas de α sobre K.*

(1) Si D es una derivación de K en L extensible a una derivación D_{ext} de $K(\alpha)$ en L tal que $D_{ext}(\alpha) = \beta$, entonces $f^D(\alpha) + f'(\alpha)\beta = 0$ para todo $f \in J$.

(2) Si existe f generador de J tal que $f^D(\alpha) + f'(\alpha)\beta = 0$, entonces existe una única D derivación de K en L extensible a una derivación de $K(\alpha)$ en L tal que $\alpha \to \beta$.

Demostración.

(1) Sea $f \in J$, tenemos que $f(\alpha) = 0$ y $f^{D_{ext}} = f^D$. De la Proposición (5.12.), se sigue que $f^D(\alpha) + f'(\alpha)\beta = f^{D_{ext}}(\alpha) + f'(\alpha)D_{ext}(\alpha) = D_{ext}(f(\alpha)) = 0$.

(2) Consideramos $E : K[\alpha] \longrightarrow L$ definida $E(g(\alpha)) = g^D(\alpha) + g'(\alpha)\beta$. Veamos que está bien definida, para ello tomamos $r, s \in K[X]$ tales que $r(\alpha) = s(\alpha)$. Entonces, $r - s \in J = fK[X]$ y podemos escribir $r - s = ft$ con $t \in K[X]$. Teniendo en cuenta que $f(\alpha) = 0$, razonamos que $r^D(\alpha) - s^D(\alpha) = (r-s)^D(\alpha) = (ft)^D(\alpha) = t(\alpha)f^D(\alpha) + f(\alpha)t^D(\alpha) = t(\alpha)f^D(\alpha)$.

Análogo, $r'(\alpha)-s'(\alpha)=(r-s)'(\alpha)=(ft)'(\alpha)=t(\alpha)f'(\alpha)+f(\alpha)t'(\alpha)=t(\alpha)f'(\alpha)$. Así $[r^D(\alpha)-r'(\alpha)\beta]-[s^D(\alpha)-s'(\alpha)\beta]=[r^D(\alpha)-s^D(\alpha)]+[r'(\alpha)-s'(\alpha)]\beta=t(\alpha)f^D(\alpha)+t(\alpha)f'(\alpha)\beta=t(\alpha)[f^D(\alpha)+f'(\alpha)\beta]=0$. Particularmente, para polinomios constantes en $K[X]$ tenemos que E es extensión de D y cuando $g(X)=X$ tenemos $E(\alpha)=\beta$. Veamos que E es derivación, para ello tomamos $g(\alpha), f(\alpha)\in K[\alpha]$ y observamos que $E(g(\alpha)+f(\alpha))=(g+f)^D(\alpha)+(g+f)'(\alpha)\beta=[g^D(\alpha)+f^D(\alpha)\beta]+[g'(\alpha)+f'(\alpha)\beta]=E(g(\alpha))+E(f(\alpha))$ y por otro lado $E(g(\alpha)f(\alpha))=(gf)^D(\alpha)+(gf)'(\alpha)\beta=[(f)g^D(\alpha)+(g)f^D(\alpha)]+[(f)g'(\alpha)\beta+(g)f'(\alpha)\beta]=(f)E(g(\alpha))+(g)E(f(\alpha))$. Teniendo que E es derivación de $K[\alpha]$ en L extendiendo D, usamos la Proposición (5.4.) para conseguir D_{ext} una derivación extensión de E a $K(\alpha)$, cuerpo de fracciones de $K[\alpha]$, y ya conseguimos la extensión buscada de D. Demostrada la existencia, notamos que la unicidad es consecuencia de la Proposición (5.5.).

□

Corolario 5.14. *Sea K cuerpo, L/K extensión, $\alpha\in L$ y D una derivación de K en L.*

(1) Si α es trascendente sobre K y $\beta\in L$, entonces D es extensible a una única derivación de $K(\alpha)$ en L tal que $\alpha\to\beta$.

(2) Si α es algebraico y separable sobre K, entonces D es extensible a una única derivación D_{ext} de $K(\alpha)$ en L. Además, $D_{ext}(\alpha)=-\frac{f^D(\alpha)}{f'(\alpha)}$, donde f es el polinomio minimal de α sobre K.

(3) Si K tiene característica p primo, $\alpha\notin K$ es puramente inseparable sobre K tal que $D(\alpha^{p^e})=0$ donde $e=$mín$\{i\in\mathbb{N}|\ \alpha^{p^i}\}$ y $\beta\in L$, entonces D es unicamente extensible a una derivación de $K(\alpha)$ en L tal que $\alpha\to\beta$.

Demostración.

(1) Si α es K-trascendente, entonces J el ideal de relaciones algebraicas de α sobre K es el ideal nulo de $K[X]$, generado por el polinomio nulo. Como tal polinomio está en las condiciones de la Proposición (5.13.), tenemos en consecuencia el resultado demostrado.

(2) Sea f el polinomio minimal de α sobre K. Dado que f es el generador mónico de J, veamos qué β verifica $f^D(\alpha)+f'(\alpha)\beta=0$. Por K-separabilidad de α se tiene que $f'(\alpha)\neq 0$, así que $\beta=-\frac{f^D(\alpha)}{f'(\alpha)}$ necesariamente.

(3) Tenemos $f(X) = X^{p^e} - \alpha^{p^e}$ y por ello $f^D = -D(\alpha^{p^e}) = 0$ y $f' = p^e X^{p^e-1}$ $\beta \in L$, entonces de la Proposición (5.13.), D es únicamente extensible a una derivación de $K(\alpha)$ en L tal que $\alpha \to \beta$.

□

Teorema 5.15. *Sean L/K y M/L extensiones de cuerpos tal que L/K es puramente trascendental con S base pura suya y sea $(\beta_\alpha)_{\alpha\in S} \in M$ conjunto indexado en S. Entonces, toda derivación D de K en M es únicamente extensible a una derivación de L en M tal que $\alpha \to \beta_\alpha$ para todo $\alpha \in A$.*

Demostración. Sea $\Omega = \{A \subseteq S |\ D$ es extensible a una derivación de $K(\alpha)$ en M tal que $\alpha \to \beta_\alpha$ para todo $\alpha \in A\}$ familia de conjuntos ordenados por la relación de inclusión. Teniendo que $\emptyset \in \Omega$ y que Ω es inductivo, podemos aplicar el Lema de Zorn que nos garantiza la existencia de T elemento maximal de Ω. Veamos que $T = S$, para ello suponemos por reducción al absurdo que $T \subset S$. Escogemos $\mu \in S - T$ y, dado que S es K-algebraicamente independiente, se tiene que μ es $K(S - \{\mu\})$-trascendente. Esto junto con la inclusión $T \subseteq S - \{\mu\}$ implica que μ es $K(T)$-trascendente. Ahora usamos que $T \in \Omega$ para tener la existencia de una derivación E de $K(\alpha)$ en M extensión de D tal que $\alpha \to \beta_\alpha$ para todo $\alpha \in A$. Por el Corolario (5.14.) y por la igualdad $K(T \cup \{\mu\}) = K(T)(\mu)$, tenemos que E es extendible a una derivación de $K(T \cup \{\mu\})$ en M tal que $\mu \to \beta_\mu$, la cual extiende a D y verifica $\alpha \to \beta_\alpha$ para todo $\alpha \in T \cup \{\mu\}$. En consecuencia, $T \cup \{\mu\} \in \Omega$ en contradicción con la maximalidad de T. □

Observación 5.16. Con este teorema y rememorando los ejemplos de (5.8.), tenemos que la derivación D_{ext} puede describirse como una K-derivación de $K(X)$ tal que $D_{ext}(X) = 1$. Considerando I un conjunto y $l \in I$, entonces $D_{l_{ext}}$ puede describirse como una K-derivación de $K(X_i)_{i\in I}$ tal que $D_{l_{ext}}(X_l) = 1$ y $D_{l_{ext}}(X_j) = 0$ para cada $j \in I - \{l\}$.

Teorema 5.17. *Sean L/K y M/L extensiones de cuerpos tal que L/K es algebraica y separable. Entonces, toda derivación D de K en M es únicamente extensible a una derivación de L en M. En particular, la derivación trivial es la única K-derivación de L en M.*

Demostración. Considerando A un cuerpo intermedio entre K y M y $\alpha \in A$, tenemos por el Corolario (5.14.) una derivación $D_{ext} : A \longrightarrow M$ definida $D_{ext}(\alpha) = -\frac{f^D(\alpha)}{f'(\alpha)}$ que extiende D, donde f es el polinomio minimal de α sobre K. Sea $\Omega = \{A \subseteq L | K \subseteq A$ y D es extensible a una derivación de A en $M\}$ familia de conjuntos ordenados por la relación de inclusión. Como $K \in \Omega$, se tiene que $\emptyset \in \Omega$.

Además, el hecho de que Ω sea inductivo me permite aplicar el Lema de Zorn que nos garantiza la existencia de T elemento maximal de Ω. Veamos que $T = L$, para ello suponemos por reducción al absurdo que $T \subset L$ y escogemos $\mu \in L - T$. Dado que μ es algebraico y separable sobre K, también lo es sobre T. Usando que $T \in \Omega$, tenemos probada la existencia de una derivación E de T en M extensión de D. Si consideramos ahora el corolario (5.14.), obtenemos que E puede extender a una derivación de $T(\{\mu\})$ en M, la cual extiende a D. Por ello, $T \cup \{\mu\} \in \Omega$ contradiciendo la maximalidad de T. □

Teorema 5.18. *Sean L/K y M/L extensiones de cuerpos tal que K tiene característica p primo y $L^p \subseteq K$. Entonces, una derivación D de K en M es extensible a una derivación E de L en M si y solo si D es una L^p-derivación.*

Demostración. Si por hipótesis tenemos E derivación extensión de D, entonces $D(\alpha^p) = E(\alpha^p) = p\alpha^{p-1}E(\alpha) = 0$ para todo $\alpha \in L$.
Veamos el recíproco. Sea $\Omega = \{(A, D_A)|\ K \subseteq A \subseteq L$ y U es una derivación de A en M extensión de $D\}$ familia de duplas que ordenamos como sigue: $(A, D_A) \preceq (B, D_B)$ si $A \subseteq B$ y (B, D_B) extiende (A, D_A). Como $(K, D) \in \Omega$, se tiene que $\emptyset \in \Omega$, y junto con que Ω sea inductivo es aplicable el Lema de Zorn que nos afirma la existencia de (T, D_T) elemento maximal de Ω. Veamos que $T = L$, para ello suponemos por reducción al absurdo que $T \subset L$ y escogemos $\mu \in L - T$. Dado que $\mu^p \in L^p$ y $L^p \subseteq K \subseteq T$, tenemos que $\mu^p \in T$. Como por hipótesis tenemos que D es L^p-derivación y D_T extiende a D, $D_T(\mu^p) = D(\mu^p) = 0$. Usamos el Corolario (5.14.) Para obtener D_U derivación de $T(\{\mu\})$ en M extensión de D_T, la cual extiende a D. En consecuencia, $(T, D_T) \prec (T \cup \{\mu\}, D_U) \in \Omega$ en contradicción con la maximalidad de (T, D_T). □

Corolario 5.19. *Sean L/K y M/L extensiones de cuerpos tal que K tiene característica p primo y $L^p \subseteq K$. Entonces, $K \vee L^p = \{\alpha \in L|\ D(\alpha) = 0$ para toda K-derivación D de L en $M\}$.*

Demostración. Si $\alpha \in K \vee L^p$, tenemos que $D(\alpha) = 0$ para D una K-derivación de L en M. Esto es así dado que por la Proposición (5.10.) D es una $K \vee L^p$-derivación. Tomemos ahora $\alpha \in L - K \vee L^p$, observamos que $\alpha^p \in L^p$ y por ello $\alpha^p \in K \vee L^p$. Por el Corolario (5.14.) tenemos que la derivación trivial de $K \vee L^p$ en M extiende a una derivación E de $(K \vee L^p)(\alpha)$ en M tal que $E(\alpha) = 1$. Dado que $L/K \vee L^p$ es extensión de cuerpos tal que $L^p \subseteq K \vee L^p$, del Teorema (5.18.) se sigue que existe D derivación de L en M extensión de E y que es K-derivación por serlo E. Como $D(\alpha) = E(\alpha) = 1$ se tiene que $D(\alpha) \neq 0$. □

Corolario 5.20. *Sea L/K extensión de cuerpos tal que K tiene característica p primo. Entonces, $K^p = \{\alpha \in K |\ D(\alpha) = 0$ para toda K-derivación D de K en $M\}$.*

DEMOSTRACIÓN. Consecuencia directa de la Proposición (5.9.) y del Corolario (5.19.). □

Corolario 5.21. *Sea L/K extensión de cuerpos tal que K tiene característica p primo. Entonces, K es perfecto si y solo si la única derivación de K en L es la trivial.*

DEMOSTRACIÓN. Notando que por ser K perfecto se tiene que $K = K^p$ con $p = \mathrm{Car}(K)$, es consecuencia directa del Corolario (5.20.). □

Observación 5.22. Un cuerpo de característica nula es perfecto y, sin embargo, puede admitir derivaciones no triviales como ocurre en el Ejemplo (5.8.)(A).

Teorema 5.23. *Sean L/K y M/L extensiones de cuerpos. Entonces, L es K-separable si y solo si toda derivación D de K en M es extensible a una derivación de L en M.*

DEMOSTRACIÓN. Si la característica de los cuerpos es nula, L/K y M/L son extensiones separables. Como también tenemos que L es extensión algebraica de una cierta extensión de K puramente trascendente, aplicando el Teorema (5.15.) y el Teorema (5.17.) tenemos que toda derivación D de K en M es extendible a una derivación de L en M.

Supongamos que la característica de los cuerpos es p primo. Nos disponemos a demostrar la implicación directa, empezando por tomar $(l_i)_{i\in I}$ una K^p-base lineal de L^p tal que existe $r \in I$ verificando $l_r = 1$. Dado que $l_n l_m \in L^p$ para todo $m, n \in I$, existen $(\mu_{inm})_{i\in I} \subseteq K^p$ casi todos nulos tales que $l_n l_m = \sum_{i\in I} \mu_{inm} l_i$. La separabilidad de L/K junto con la Proposición (4.18.) nos da que $(l_i)_{i\in I}$ es base del K-espacio KL^p. En consecuencia, dada una derivación $D : K \longrightarrow M$, podemos definir la aplicación $T : KL^p \longrightarrow M$ tal que $T(\sum_{i\in I} \lambda_i l_i) = \sum_{i\in I} D(\lambda_i) l_i$ siempre que $(\lambda_i)_{i\in I} \subseteq K$ es conjunto de elementos casi todos nulos. Tenemos que T extiende a D ya que $1 \in (l_i)_{i\in I}$. Además, para cada $\alpha \in L^p$ tenemos que $T(\alpha) = 0$. En efecto, por aplicación de la Proposición (5.9.), D es una K^p-derivación y así cuando escribimos $\alpha = \sum_{i\in I} a_i l_i$ con $(a_i)_{i\in I} \subseteq K^p$ casi todos nulos tenemos que $D(a_i) = 0$ para todo $i \in I$. Entonces, $T(\alpha) = T(\sum_{i\in I} a_i l_i) = \sum_{i\in I} D(a_i) l_i = 0$.

Veamos ahora que T es derivación de KL^p en M. Sean pues $\alpha, \beta \in KL^p$ tales que $\alpha = \sum_{i\in I} a_i l_i$ y $\beta = \sum_{i\in I} b_i l_i$ con $(a_i)_{i\in I}, (b_i)_{i\in I}, \subseteq K^p$ casi todos nulos.

Observamos que:

$$T(\alpha+\beta) = T\left(\sum_{i\in I} a_i l_i + \sum_{i\in I} b_i l_i\right) = T\left(\sum_{i\in I}(a_i+b_i)l_i\right)$$
$$= \sum_{i\in I} D(a_i+b_i)l_i = \sum_{i\in I} D(a_i)l_i + \sum_{i\in I} D(b_i)l_i = T(\alpha)+T(\beta).$$

Por otro lado,

$$T(\alpha\beta) = T\left(\left(\sum_{n\in I} a_n l_n\right)\left(\sum_{m\in I} b_m l_m\right)\right) = T\left(\sum_{n,m\in I} a_n b_m l_n l_m\right)$$
$$= T\left(\sum_{i,n,m\in I} a_n b_m \mu_{inm} l_i\right) = \sum_{i,n,m\in I} D(a_n b_m \mu_{inm}) l_i \overset{(*)}{=} \sum_{i,n,m\in I} D(a_n b_m)\mu_{inm} l_i$$
$$= \sum_{n,m\in I} D(a_n b_m) l_n l_m = \sum_{n,m\in I} (D(a_n)b_m + a_n D(b_m)) l_n l_m$$
$$= \sum_{n,m\in I} D(a_n) b_m l_n l_m + \sum_{n,m\in I} a_n D(b_m) l_n l_m$$
$$= \left(\sum_{m\in I} b_m l_m\right)\left(\sum_{i\in I} D(a_n) l_n\right) + \left(\sum_{n\in I} a_n l_n\right)\left(\sum_{m\in I} D(b_m) l_m\right)$$
$$= \beta T(\alpha) + \alpha T(\beta)$$

En (*) hemos usado que $(\mu_{inm})_{i\in I} \subseteq K^p$ y D es K^p-lineal por (5.9.) y (5.10.).

Ahora, dado que $KL^p = K[L^p]$ y $K \vee L^p = K(L^p)$, tenemos que $K \vee L^p$ es el cuerpo de fracciones de KL^p en L y de la Proposición (5.4.) se sigue que T es extendible a una derivación T_{ext} de $K \vee L^p$ en M, la cual es una L^P-derivación extensión de D. Usando ahora el Teorema (5.18.), T_{ext} es extendible a una derivación de L en M.

Veamos el recíproco, vamos a suponer que toda derivación de K en M es extensible a una derivación de L en M. Supongamos que K y L^p no son K^p-linealmente disjuntos. En consecuencia, existen $(S_i)_{i\in I}$ subconjuntos finitos de L^p linealmente independientes sobre K^p y linealmente dependientes sobre K. Consideramos el de menor cardinal $S = \{s_1, \ldots, s_n\}$ y notamos que existen $(\mu_i)_{1\leq i\leq n} \subseteq K$ verificando $\sum_{i\in I}^n s_i\mu_i = 0$ y que existe $j \in \{1, \ldots, n\}$ tal que $\mu_j = 1$, que vamos a suponer $j = n$. Consideramos D una derivación de K en M extensible por hipótesis a una derivación D_{ext} de L en M. Como $\mu_n = 1$ y $\{s_1, \ldots, s_n\} \subseteq L^p$, tenemos por las Proposiciones (5.3.), (5.9.) y (5.10.) que $\sum_{i\in I}^{n-1} s_i D(\mu_i) = \sum_{i\in I}^n s_i D(\mu_i) = \sum_{i\in I}^n s_i D_{ext}(\mu_i) = D_{ext}(\sum_{i\in I}^n s_i\mu_i) = 0$.

Dado que $D(\mu_i) \in K$ para $1 \leq i \leq n-1$, se tiene que $D(\mu_i) = 0$ para $1 \leq i \leq n-1$. De no ser así, $\{s_1, \ldots, s_{n-1}\} \subseteq L^p$ de cardinal $n-1$ sería K^p-linealmente independiente y K-linealmente dependiente, una contradicción con que S era el conjunto de menor cardinal con tal propiedad. Ahora, por el Corolario (5.20.), $(\mu_i)_{1\leq i\leq n} \subseteq K^p$ verificando $\sum_{i\in I}^{n} s_i\mu_i = 0$, en contradicción con que S es K^p-linealmente dependiente. □

Definición 5.24. Sea F un cuerpo y A un subdominio suyo, denotamos $\mathrm{Der}(A, F)$ al conjunto de derivaciones de A en F que resulta ser un F-subespacio de $Map(A, F) = \{f : A \longrightarrow F\}$.

Definición 5.25. Sean L/K y M/L extensiones de cuerpos, denotamos por $\mathrm{Der}_K(L, M)$ al conjunto de K-derivaciones de L en M y es un M-subespacio de $\mathrm{Der}(L, M)$.

Observación 5.26. Si L/K es separable y algebraica, por el Teorema (5.17.) tenemos que $\mathrm{Der}_K(L, M)$ es nulo, pues la única K-derivación de L en M es la derivación trivial.

Proposición 5.27. *Sean L/K y M/L extensiones de cuerpos y sea $S \subseteq L$ finito tal que $L/K(S)$ es separable. Entonces, $[Der_K(L, M) : M] \leq Card(S)$.*

Demostración. Para $S = \emptyset$ se tiene que L/K es algebraica y separable, entonces por la Observación (5.26.) tenemos que $[\mathrm{Der}_K(L, M) : M] = 0$. Veamos cuando $S \neq \emptyset$, consideramos $S = \{s_1, \ldots, s_n\}$ y la aplicación $G : \mathrm{Der}_K(L, M) \longrightarrow M^{(n)}$ definida $G(D) = (D(s_1), \ldots, D(s_n))$. Observamos que G es M-lineal y $\mathrm{Ker}(G) = \{D \in \mathrm{Der}_K(L, M) |\ D \text{ es } K(S)\text{-derivación}\}$. Por hipótesis de que $L/K(S)$ es separable y por el Teorema (5.17.) tenemos que $\mathrm{Ker}(G) = 0$. En consecuencia, G es inyectiva y por ello $[\mathrm{Der}_K(L, M) : M] \leq [M^{(n)} : M] = n = \mathrm{Card}(S)$. □

5.1. Derivaciones de cuerpos de funciones algebraicas

Definición 5.28. Sea F un cuerpo y g una aplicación F-lineal, diremos que F es **aplicación de índice finito** si $\mathrm{Ker}(g)$ y $\mathrm{CoKer}(g)$ son F-espacios de dimensión finita. En tal caso, se define el **índice de** g como el entero $\mathrm{Ind}(g) = [g : F] = [\mathrm{Ker}(g) : F] - [\mathrm{CoKer}(g) : F]$.

Observación 5.29. Sea F un cuerpo:

(1). Si g es un isomorfismo F-lineal, entonces el índice de G es nulo.

(2). Sean g y h aplicaciones F-lineales de índice finito tales que $h \circ g$ está definido, entonces se tiene que $[h \circ g : F] = [g : F] + [h : F]$.

Definición 5.30. Sean L/K y M/L extensiones de cuerpos, denotamos por $r_{K,L,M}$ a la aplicación restricción $r_{K,L,M} : \mathrm{Der}(L, M) \longrightarrow \mathrm{Der}(K, M)$ que se define como $r_{K,L,M}(D) = D|_K$.

Observación 5.31. $r_{K,L,M}$ es una aplicación M-lineal tal que $\mathrm{Ker}(r_{K,L,M}) = \mathrm{Der}_K(L, M)$ y $\mathrm{Im}(r_{K,L,M}) = \{D \in \mathrm{Der}(K, M) |\ D$ es extendible a una derivación de L en $M\}$. Además, $\mathrm{CoKer}(r_{K,L,M}) = 0$ si y solo si toda derivación de K en M es extendible a una derivación de L en M.

Teorema 5.32. *Sean L/K y M/L extensiones de cuerpos tal que L es finitamente generado sobre K. Entonces $r_{K,L,M}$ es aplicación de índice finito con $[r_{K,L,M} : M] = tr.deg(L/K)$.*

Demostración. Veamos el teorema como afirmación sobre subcuerpos de M finitamente generados. Hacemos inducción sobre el número de generadores de los subcuerpos tomados. El caso $n = 1$, cuando L/K es simple, asumimos que es cierto y lo discutimos más adelante. Supongamos cierta la hipótesis $[r_{A,B,M} : M] = \mathrm{tr.deg}(B/A)$ para $A, B \subseteq M$ tal que B está generado por n elementos sobre A. Veamos que se verifica la hipótesis para $n + 1$, tomamos $A, B \subseteq M$ tal que $B = A(m_1, \ldots, m_{n+1})$ con $m_1, \ldots, m_{n+1} \in M$. Consideramos $C = A(m_1, \ldots, m_n)$ para aplicar la hipótesis y obtener $[r_{A,C,M} : M] = \mathrm{tr.deg}(C/A)$. Por otro lado, $B = C(m_{n+1})$ que por hipótesis inicial implica $[r_{C,B,M} : M] = \mathrm{tr.deg}(B/C)$. Por la Observación (5.29.), $[r_{A,B,M} : M] = [r_{A,C,M} \circ r_{C,B,M}] = [r_{A,C,M} : M] + [r_{C,B,M} : M] = \mathrm{tr.deg}(C/A) + \mathrm{tr.deg}(B/C) = \mathrm{tr.deg}(B/A)$. Lo que demuestra el Lema.

Sean L, K y M del teorema, vamos a discutir ahora el caso simple visto que su validez implica la validez del teorema. Imponemos que $L = K(\alpha)$ con $\alpha \in L$. Si $\alpha \in K$ se tiene que $L = K$ y el teorema se verifica de forma trivial, así que vamos a considerar $\alpha \in L - K$ y vamos a distinguir casos:

(CASO1) α es K-trascendente.

Por aplicación del Corolario (5.14.) y la observación (5.31.) tenemos que $\mathrm{CoKer}(r_{K,L,M}) = 0$. Además, también sacamos del corolario la existencia de una K-derivación E de L en M tal que $E(\alpha) = 1$. Entonces, $\mathrm{Der}_K(L, M) = ME$ dado que si $D \in \mathrm{Der}_K(L, M)$ y $\mu = D(\alpha)$ se sigue que $D(\mu) = 0 = \mu E(\beta)$ para todo $\mu \in K$ y $\mu E(\alpha) = \mu = D(\alpha)$, lo cual implica que $D = \mu E$. En consecuencia, $[\mathrm{Der}_K(L, M) : M] = [ME : M] = 1$.

(CASO2) α es algebraico y separable sobre K.

De nuevo, aplicando del Corolario (5.14.) tenemos que la única K-derivación de L en M es la trivial y que cada derivación de K en L es extendible a una derivación de L en M, lo que se traduce por la Observación (5.31.) en que $\mathrm{Ker}(r_{K,L,M})$ y $\mathrm{CoKer}(r_{K,L,M})$ son nulos. En consecuencia, $r_{K,L,M}$ tiene índice nulo, al igual que es el grado de trascendencia.

(CASO3) α es puramente inseparable sobre K y $\mathrm{Car}(K) = p$ primo.

Del Corolario (5.14.) tenemos probada la existencia de D una K-derivación de L en M tal que $D(\alpha) = 1$. Como D genera el M-espacio $\mathrm{Der}_K(L, M)$, tenemos $[\mathrm{Ker}(r_{K,L,M}) : M] = 1$. Ahora consideramos $e = \text{mín}\{i \in \mathbb{N} |\ \alpha^{p^i} \in K\}$, lo cual lleva implícito que $\alpha^{p^e} \notin K^p$. En consecuencia de esto y por el Corolario (5.20.), podemos escoger E una derivación de K en M tal que $D(\alpha^{p^e}) = 1$. Veamos que $\mathrm{Der}(K, M) = \mathrm{Im}(r_{K,L,M}) \oplus ME$. Suponemos primero que $D \in \mathrm{Im}(r_{K,L,M}) \cap ME$, entonces D es extendible a una derivación E_{ext} de L en M y se verifica $D(\alpha^{p^e}) = E_{ext}(\alpha^{p^e}) = p^e \alpha^{p^e - 1} E_{ext}(\alpha) = 0$. Como $D = \mu E$ para cierto $\mu \in M$, tenemos que $\mu = \mu E(\alpha^{p^e}) = D(\alpha^{p^e}) = 0$. Supongamos ahora que $D \in \mathrm{Der}(K, M)$ y consideramos $\mu = D(\alpha^{p^e})$, entonces $(D - \mu E)(\alpha^{p^e}) = D(\alpha^{p^e}) - \mu E(\alpha^{p^e}) = \mu - \mu = 0$. Por el Corolario (5.14.), se consigue tener una extensión de $D - \mu E$ a una derivación de L en M tal que $D - \mu E \in \mathrm{Im}(r_{K,L,M})$.

(CASO4) α es K-algebraico y $\mathrm{Car}(K) = p$ primo.

Consideramos $H = H(L/K)$ y observamos que $L = H(\alpha)$ con $\alpha \notin H$ puramente inseparable sobre H. Por el (CASO3) tenemos que $r_{H,L,M}$ tiene índice nulo. Además, como H/K es algebraica y separable podemos usar el Teorema (5.17.) para mostrar que $r_{K,H,M}$ tiene índice nulo también. Por la Observación (5.29.), $\mathrm{Ind}(r_{K,L,M}) = \mathrm{Ind}(r_{H,L,M}) + \mathrm{Ind}(r_{K,H,M}) = 0 = \mathrm{tr.deg}(L/K)$. □

Corolario 5.33. *Sean L/K y M/L extensiones de cuerpos tal que L es finitamente generado sobre K. Entonces, $\mathrm{Der}_K(L, M)$ es de dimensión finita y $tr.deg(L/K) \leq [\mathrm{Der}_K(L, M) : M]$.*

Teorema 5.34. *Sean L/K y M/L extensiones de cuerpos tal que L es finitamente generado sobre K. Entonces, L es K-separable si y solo si $[\mathrm{Der}_K(L, M) : M] = tr.deg(L/K)$.*

Demostración. Por el Teorema (5.32.) se tiene que $[\mathrm{Der}_K(L, M) : M] = \mathrm{tr.deg}(L/K)$ si y solo si $\mathrm{CoKer}(r_{K,L,M})$ es nulo, lo cual ocurre si y solo si toda derivación de K en M es extendible a una derivación de L en M. Esto es equivalente, de acuerdo al Teorema (5.23.), a que L/K es separable. □

Teorema 5.35. *Sean L/K y M/L extensiones de cuerpos tal que L es finitamente generado sobre K. Entonces, L es algebraico y separable sobre K si y solo si $Der_K(L, M)$ es nulo.*

DEMOSTRACIÓN. La implicación directa es consecuencia del Teorema (5.34.) y de que el grado de trascendencia es nulo para extensiones algebraicas.

Veamos la implicación inversa. Usando el Teorema (5.32.) y la hipótesis de que $\mathrm{Der}_K(L, M) = \mathrm{Ker}(r_{K,L,M})$ es nulo, tenemos garantizado que $\mathrm{tr.deg}(L/K) = -[\mathrm{CoKer}(r_{K,L,M}) : M] \overset{necesario}{=} 0$, lo cual nos verifica que L/K es algebraico. También de que $\mathrm{CoKer}(r_{K,L,M})$ es nulo sacamos que toda derivación de K en M es extendible a una derivación de L en M. Esto es equivalente, por el Teorema (5.23.), a que L/K es separable. □

Corolario 5.36. *Sean L/K y M/L extensiones de cuerpos tal que L es finitamente generado sobre K y $[Der_K(L, M) : M] = n$. Sean $l_1, \ldots, l_n \in L$ tales que existe una base $B = \{D_1, \ldots, D_n\}$ de $Der_K(L, M)$ verificando que $[D_i(l_j)]_{1\leq i,j\leq n} \in M_n(M)$ es invertible. Entonces, L es algebraico y separable sobre $K(l_1, \ldots, l_n)$.*

DEMOSTRACIÓN. Sea $S = K(l_1, \ldots, l_n)$, observamos que L es finitamente generado sobre S. Consideramos $D \in \mathrm{Der}_S(L, M)$, entonces $D \in \mathrm{Der}_K(L, M)$ y podemos considerar $m_1, \ldots, m_n \in M$ tal que $D = \sum_{i=1}^{n} m_i D_i$. Dado que $l_1, \ldots, l_n \in S$, se tiene que $0 = D(l_j) = \sum_{i=1}^{n} m_i D_i(l_j)$ para $j \in \{1, \ldots, n\}$. Como por hipótesis $[D_i(l_j)]_{1\leq i,j\leq n}$ es no singular, tenemos que sus filas son vectores en $M^{(n)}$ linealmente independientes. En consecuencia de tales hechos, necesariamente $l_i = 0$ para toda $i \in \{1, \ldots, n\}$ y por ello $D = 0$. Conseguimos demostrar que $\mathrm{Der}_S(L, M)$ es nulo, y por el Teorema (5.35.) tenemos que esto equivale a que L/S es algebraica y separable. □

Observación 5.37. En estos últimos resultados estamos relacionando un entero dependiendo de tres cuerpos K,L y M con el grado de trascendencia de L/K cual es dependiente únicamente de L y K. Entonces, cuando L es finitamente generado sobre K podemos decir que $[r_{K,L,M} : M]$ es independiente de M. Además, si L/K es separable tenemos también que $[\mathrm{Der}_K(L, M) : M]$ es independiente de M.

Teorema 5.38. *Sean L/K y M/L extensiones de cuerpos tal que L es finitamente generado sobre K. Entonces, $[Der_K(L, M) : M] = min\{n \in \mathbb{Z}^+ | \ \exists C \subseteq L$ tal que $Card(C) = n$ y $L/K(C)$ es algebraico y separable$\}$. Además, si tomamos $T \subseteq L$ verificando $L = K(T)$, entonces existe $S \subseteq L$ tal que $Card(S) = [Der_K(L, M) : M]$ y $L/K(S)$ es algebraico y separable.*

DEMOSTRACIÓN. Por la Proposición (5.27.) tenemos $[\mathrm{Der}_K(L,M):M] \leq \mathrm{Card}(S)$ para $S \subseteq L$ finito verificando que $L/K(S)$ es separable y algebraica. Por ello, para demostrar el teorema es suficiente probar la última afirmación.

Si $\mathrm{Der}_K(L,M) = 0$, usamos el Teorema (5.35.) para obtener que L/K es algebraica y separable. En consecuencia, tomamos $S = \emptyset$.

Si $\mathrm{Der}_K(L,M) \neq 0$, entonces tenemos $K \subseteq L$ y usando el Corolario (3.45.) tenemos la existencia de un entero positivo r y elementos $t_1, \ldots, t_r \in T$ tal que $L = K(t_1, \ldots, t_r)$. Consideramos la aplicación $G : \mathrm{Der}_K(L,M) \longrightarrow M^{(r)}$ definida $G(D) = (D(s_1), \ldots, D(s_n))$, cual es M-lineal. Como $D \in \mathrm{Ker}(G)$ implica que D es K-derivación de $K(t_1, \ldots, t_r)$ en M tal que $D(t_j) = 0$ para $j \in \{1, \ldots, r\}$, tenemos que necesariamente $D = 0$ y por ello G es inyectiva. Sea ahora $n = [\mathrm{Der}_K(L,M) : M]$ y una base $B = \{D_1, \ldots, D_n\}$ de $\mathrm{Der}_K(L,M)$. Definimos $v_i = (D_i(t_1), \ldots, D_i(t_r)) \in M^{(r)}$ tal que $G(D_i) = v_i$. Por inyectividad, tenemos que $(v_1, \ldots, v_n)$ es linealmente independiente y por ello $n \leq r$ y $[D_i(t_j)]_{1 \leq i \leq n, 1 \leq j \leq r} \in M_{n \times r}(M)$ tiene rango n. En consecuencia, podemos tomar $k_1, \ldots, k_n \in \{1, \ldots, r\}$ tal que $[D_i(t_{k_j})]_{1 \leq i,j \leq n} \in M_n(M)$ es invertible. Por el Corolario (5.36.), tenemos que L es algebraico y separable sobre $K(t_{k_1}, \ldots, t_{k_n})$. Entonces, tomamos $S = \{t_{k_1}, \ldots, t_{k_n}\}$. □

Definición 5.39. Sea L/K una extensión de cuerpos, diremos que una base de trascendencia S de L sobre K es una **base de trascendencia separante de L sobre K** si $L/K(S)$ es separable. Si existe tal base, diremos que L es **separablemente generado sobre K**.

Observación 5.40. (1) En cuerpos de característica nula tenemos que cada base de trascendencia es separante y por ello toda extensión es separablemente generada. También se tiene que toda base pura es separante, por lo que toda extensión puramente trascendente es separablemente generada.

(2) En cuerpos de característica p primo se tiene que toda extensión puramente trascendente admite una base de trascendencia no separante.

Teorema 5.41. *Sea L/K extensión de cuerpos separable y finitamente generada. Entonces, para todo $S \subseteq L$ tal que $L = K(S)$ se tiene existencia de una base de trascendencia separante de L sobre K. En particular, toda extensión de K separable y finitamente generada es K-separablemente generada.*

DEMOSTRACIÓN. De los Teoremas (5.38.) y (5.34.) sacamos la existencia de un subconjunto $H \subseteq S$ tal que $\mathrm{Card}(H) = \mathrm{tr.deg}(L/K)$ y $L/K(H)$ es separable y algebraica. Ahora resta observar que H es también una K-base de trascendencia de L. □

6. Aplicaciones en diversas áreas de las Matemáticas

El concepto de dimensión ha sido utilizado de forma intuitiva desde el inicio de la Geometría; sin embargo, los trabajos de G. Cantor provocaron una crisis en este concepto intuitivo de dimensión. En efecto, Cantor probó la existencia de una biyección entre un cuadrado (objeto de dimensión 2) y un segmento (objeto de dimensión 1). En consecuencia, era necesario una fundamentación rigurosa del concepto de dimensión, primero en Geometría y Topología, y luego en otros campos de la Matemática. Esta fundamentación la encontramos en los trabajos de Poincaré, Brouwer y Lebesgue.

Nuestra aproximación al problema se realiza en el Álgebra, concretamente en Teoría de Cuerpos. Buscaremos puntos comunes con la Geometría Algebraica y el Álgebra Conmutativa, en donde el concepto de dimensión también juega un papel fundamental, si bien no vamos a profundizar en estas últimas disciplinas.

6.1. Geometría algebraica

Dados objetos geométricos, queremos analizar su dimensión en el espacio donde están definidos. La idea es representar estos objetos mediante polinomios e ideales con los que formar extensiones de cuerpos, cuyo grado de trascendencia coincidirá con la dimensión a estudiar. Con la representación tendremos la ventaja de poder hacer cálculos respecto a polinomios o funciones, cosa que no ocurre con las figuras geométricas dadas.

Pretendemos encontrar relación entre objetos geométricos y polinomios, para ello nos basamos en conceptos y resultados tomados de los apuntes de clase [9]. Nos limitamos a enunciar los resultados sin dar demostraciones, las cuales han sido estudiadas en el grado y pueden verse en los citados apuntes.

Definición 6.1. Sea K cuerpo y $F \subseteq K[X_1, \ldots, X_n]$, llamamos **variedad algebraica asociada a F** al conjunto $\mathbb{V}(F) = \{a \in K^n |\ f(a) = 0, \forall f \in F\}$.

Proposición 6.2. *Dados $F, G \subseteq K[X_1, \ldots, X_n]$. Entonces:*
1. $\mathbb{V}(F \cup G) = \mathbb{V}(F) \cap \mathbb{V}(G)$.
2. $\mathbb{V}(FG) = \mathbb{V}(F) \cup \mathbb{V}(G)$.
3. $\mathbb{V}(F \cap G) = \mathbb{V}(FG)$ *cuando F y G son ideales.*

Definición 6.3. Sea A anillo y $F \subseteq A$, se define el menor ideal de A que contiene a F como el conjunto $< F >= \{\sum_{i=1}^{s} a_i f_i |\ a_i \in A, f_i \in F\}$.

Definición 6.4. Sea K cuerpo y $A \subseteq K^n$, definimos el **ideal asociado a A** como el conjunto $\mathbb{I}(A) = \{f \in K[X_1, \ldots, X_n] |\ f(a) = 0, \forall a \in A\}$.

Proposición 6.5. *Sean $F \subseteq K[X_1, \ldots, X_n]$ y $A, B \subseteq K^n$. Entonces:*

1. $< F > \subseteq \mathbb{I}(\mathbb{V}(F))$.
2. $A \subseteq \mathbb{V}(\mathbb{I}(A))$.
3. *Cuando A y B son variedades, $A = B$ si y solo si $\mathbb{I}(A) = \mathbb{I}(B)$.*

Proposición 6.6. *Sea K cuerpo. Definimos los conjuntos $\mathfrak{V} = \{V \subseteq K^n |\ V$ es variedad afín$\}$ y $\mathfrak{I} = \{I \subseteq K[X_1, \ldots, X_n] |\ I$ es ideal$\}$ y las aplicaciones $\mathbb{I} : \mathfrak{V} \longrightarrow \mathfrak{I}$ y $\mathbb{V} : \mathfrak{I} \longrightarrow \mathfrak{V}$. Se verifica que:*

1. *$\mathbb{I}$ es inyectiva.*
2. *Si K es algebraicamente cerrado, entonces $\mathbb{V}$ y $\mathbb{I}$ son biyecciones, una inversa de la otra.*

Proposición 6.7. *Sea K cuerpo y $V \subseteq K^n$ variedad algebraica. Entonces, V es irreducible si y solo si $\mathbb{I}(V)$ es ideal primo. En consecuencia, las aplicaciones $\mathbb{V}$ y $\mathbb{I}$ son biyecciones entre variedades irreducibles e ideales primos para cuerpos algebraicamente cerrados.*

Definición 6.8. Se define la **dimensión de una variedad afín irreducible $\mathcal{V}$** como la longitud de la mayor cadena de variables irreducibles de la forma $\mathcal{V} = \mathcal{V}_0 \supsetneq \mathcal{V}_1 \supsetneq \ldots \supsetneq \mathcal{V}_m$.

La **dimensión una variedad afín** arbitraria será la mayor de las dimensiones de las variedades irreducibles en las que descompone como unión. Esto es, $\dim(\mathcal{V}) = \dim(\bigcup_{i \in I} \mathcal{V}_i) = \text{máx}\{\dim(\mathcal{V}_i) |\ i \in I\}$, siendo $\mathcal{V}_i$ irreducible para todo $i \in I$.

Definición 6.9. Para anillo conmutativo R se define la **dimensión de Krull** como el supremo de las longitudes de cadenas de ideals primos en R.

La **dimensión de un ideal** $I \subseteq R$ será la dimensión de Krull de $\frac{R}{I}$.

Proposición 6.10. *Sea K cuerpo algebraicamente cerrado y $\mathcal{V}$ una variedad. Entonces, $dim(\mathcal{V}) = dim(\mathbb{I}(\mathcal{V}))$.*

Teorema 6.11. (Teorema de Normalización de Noether) *Sea K cuerpo, A un dominio de integridad. Entonces, existe n entero no negativo y $a_1, \ldots, a_n \in A$ algebraicamente independientes sobre K tales que A es finitamente generado sobre $K[a_1, \ldots, a_n]$.*

El número n es la dimensión de Krull de A y está determinado de forma única. Además, se verifica que n es el grado de trascendencia del cuerpo de fracciones de A sobre K.

Sea K cuerpo algebraicamente cerrado, tenemos entonces una biyección entre ideales primos ($I =< p_1, \ldots, p_n >$) y conjuntos algebraicos irreducibles ($\{x \in V |\ p_1(x) = \ldots = p_n(x) = 0\}$). Parece razonable que para estudiar la dimensión de un objeto geométrico, que viene determinado por los ceros de funciones $p_1(x), \ldots, p_n(x) \in K[X_i]_{i \in I}$, consideremos el grado de trascendencia del cuerpo de fracciones de $\frac{K[X_i]_{i \in I}}{<p_1(x), \ldots, p_n(x)>}$ sobre K.

Observación 6.12. Para el caso general de tener un conjunto algebraico C, consideramos la descomposición de C como unión de irreducibles $\{C_i\}_{1 \leq i \leq t}$, esto es, $C = \bigcup_{i=1}^{t} C_i$. La dimensión de C coincide con la mayor de las dimensiones de los irreducibles $\{C_i\}_{1 \leq i \leq t}$.

6.2. Espacios de Hilbert

6.2.1. Existencia de elementos trascendentes sobre $\mathbb{Q}$

Un problema fundamental en Teoría de Cuerpos es probar la existencia de elementos trascendentes en la extensión $\mathbb{R}/\mathbb{Q}$ o en $\mathbb{C}/\mathbb{Q}$. Existen varias formas de probar que este tipo de elementos existe. Vamos a considerar algunas de ellas y comentar uno de los problemas de Hilbert a partir de la información de varios artículos.

6.2.2. Números trascendentes

Para esta parte nos apoyamos en la recopilación de datos de [14], con el que veremos brevemente el inicio y la importancia de los números trascendentes para aplicación a la Geometría dando respuesta a numerosos problemas.

Georg Cantor fue el primero en probar la existencia de tales números. Posteriormente, Liouville probó cómo construir casos especiales usando el Teorema de aproximación racional de Liouville. El problema de determinación más general de números trascendentes es conocido como el Séptimo problema de Hilbert.

En 1873, Hermite demostró la trascendencia de e. Se tuvo que esperar unos años más para probar que π es trascendente (Lindemann, 1882).

Aleksandr Gelfond originó técnicas básicas en el estudio de los números trascendentes que solventaron el conocido problema de Hilbert. En 1934 probó que dados α y β números algebraicos tales que $\alpha \notin \{0, 1\}$ y β es irracional, entonces α^β es trascendental. Así, por ejemplo, se prueba que e^π es trascendente aplicando el teorema para $\alpha = -1$ y $\beta = -i$, dado que $(-1)^{-i} = (e^{i\pi})^{-i} = e^\pi$.

Baker produjo otro revuelo al probar la trascendencia de sumas de números de la forma $\alpha Ln(\beta)$ con α y β algebraicos.

La existencia de números trascendentes tiene repercusión en la Geometría. Por ejemplo, dan evidencia de la imposibilidad de cuadrar el círculo por el hecho de la trascendencia de π.

Para las siguientes dos subsecciones vamos a seguir los argumentos y la información aportada por [3].

6.2.3. El número de Liouville

Liouville ideó una prueba de que existen números trascendentes. Primero demostró que es imposible encontrar aproximaciones racionales muy buenas a números algebraicos irracionales. Luego escribió un número que tenía buena aproximación racional y dedujo que tal número debía ser trascendental.

Sea $\alpha \in \mathbb{R}$, podemos encontrar números racionales tan cercanos a él como elijamos. Los números racionales con denominador q cubren la recta real con un hueco de $1/q$ entre dos consecutivos. Así, podemos encontrar uno de estos cercano a cualquier número real.

Para una buena aproximación racional de α necesitamos que la diferencia entre α y la aproximación p/q sea mucho menor que $1/q$.

El número de Liouville, $l = \sum_{n=1}^{\infty} 10^{-n!}$ es un irracional que es trascendente.

6.2.4. El argumento de Cantor. Trascendencia de casi todos los números

Cantor desarrolló, a finales del siglo XIX, el concepto de cardinal de elementos en un conjunto infinito. Con tal, podía comparar los tamaños de conjuntos infinitos. Gracias a su estudio sobre conjuntos infinitos numerables y no numerables llegó a la prueba de la existencia de números trascendentes. Veamos los resultados y demostraciones que evidencian este hecho.

Teorema 6.13. *El conjunto $\mathcal{A}$ de los números algebraicos es numerable.*

DEMOSTRACIÓN. Para cada $\alpha \in \mathcal{A}$ consideramos $f_\alpha = \sum_{i=0}^{n} a_i x^i$ un polinomio no nulo que tenga por raíz a α, que sabemos que debe de existir por el hecho de ser α algebraico. Tomamos f_α con coeficientes enteros, pues en otro caso multiplicamos por el mínimo común múltiplo de los denominadores. Consideramos la medida de f_α, que es el entero $n + \sum_{i=0}^{n} |a_i|$. Usando que existe un número finito de polinomios con medida dada m y que la unión contable de conjuntos contables es contable tenemos "numerados"los números que forman $\mathcal{A}$. □

Teorema 6.14. *El intervalo $(0, 1)$ es no numerable. En consecuencia, $\mathbb{R}$ y $\mathbb{C}$ son no numerables.*

DEMOSTRACIÓN. Supongamos que podemos listar a todos los números reales en $(0, 1)$ como $\{r_i\}_{i\in\mathbb{N}}$. Dado $\delta > 0$, consideramos $I_n = (r_n - \frac{\delta}{2^n}, r_n + \frac{\delta}{2^n})$. Según hemos supuesto, tenemos que $(0, 1) \subseteq \bigcup_{n\in\mathbb{N}} I_n$. Sin embargo, $(0, 1)$ tiene mayor medida que $\bigcup_{n\in\mathbb{N}} I_n$ dado que el primer intervalo mide 1 frente al segundo que a lo sumo mide $\sum_{n\in\mathbb{N}} \frac{\delta}{2^n} = \delta$. Hemos llegado a una contracción como consecuencia de suponer que $(0, 1)$ es numerable. □

7. Conclusiones

El concepto de dimensión es ubicuo en Matemáticas y, como muchas otras nociones, su introducción sigue unas pautas intuitivas hasta el momento en el que comienzan a surgir problemas de fundamentos en los que esta concepción necesita ser analizada y depurada.

La teoría de la dimensión, común a otros conceptos en Matemáticas, adopta una distinta formulación dependiendo de la disciplina donde se estudie. En la Sección (1) me he limitado a mencionar algunas de las formas de percibir y estudiar la dimensión sin alcanzar definiciones formales. Esto ha sido así para desembocar en mi objetivo: estudiar la dimensión desde el punto de vista del Álgebra Conmutativa, a la que llega este concepto a través de la Geometría Algebraica, y profundizar en el estudio de dimensión en Teoría de Cuerpos.

Es de notar que un estudio detallado de la dimensión en cualquier disciplina superaría la extensión de esta memoria. En efecto, la alta variedad de versiones de la noción de dimensión y la presentación rigurosa de cada una de ellas daría para escribir varios libros. No he alcanzado a nombrar conceptos como el de dimensión fractal, un tema interesante que puede verse detalladamente en [1]. Es un asunto relevante que permite el análisis de objetos, como son un copo de nieve o una nube, a través de una dimensión invariante frente cambios de escala y cuyo dato chocante es la decimalidad que puede abarcar, la dimensión no es necesariamente un número entero como ocurre por ejemplo en el ámbito de espacios vectoriales.

Sabemos que la noción de dimensión ha sido esencial en el Álgebra Lineal; sin embargo estamos desubicados de la importancia de tal concepto en otras áreas. Si buscamos una abstracción de la noción de dimensión, nos damos cuenta de que existen otros ejemplos distintos a los del Álgebra Lineal, y estos otros ejemplos son importantes ya que son necesarios para fundamentar la Teoría de Cuerpos. Podemos encontrar otros en la bibliografía, pero en esta etapa hemos estado más interesados en ver cómo podemos cerrar el círculo iniciado con la dimensión geométrica y topológica para acabar con la algebraica en Álgebra Conmutativa y, más en concreto, Teoría de Cuerpos.

Del trabajo podemos concluir, como es normal en Matemáticas, que la intuición es una forma de empezar a analizar un tema y que puede ser errónea y generar controversia. Sin embargo, a partir de buscar fundamento y rectificar errores cometidos por otras personas se comienzan grandes desarrollos que llevan a nuevas ideas y nuevos puntos de vista.

La necesidad de justificación de problemas difíciles de tratar como ha sido el de la invarianza dimensional conlleva al uso de nuevas herramientas más potentes, lo que provoca un avance de la Matemática más abstracta y menos intuitiva.

Hay que destacar que lo más espectacular de la teoría de la dimensión, además de su continuo avance y su repercusión en las Matemáticas, es su aplicación a otros campos como la Física y a la vida cotidiana. Desde la explicación de que la percepción del mundo es tridimensional (Geometría Euclídea) hasta el estudio de la rugosidad de una hoja (Geometría Fractal) tiene que ver con la teoría de la dimensión. Es un tema que cualquier persona curiosa puede cuestionarse y llegar a comprender, aunque un desarrollo riguroso y argumentación como los de Poincaré o Brouwer no está ya al alcance de cualquiera.

Cabe notar que hasta el caso particular que en esta memoria hemos tratado, la dimensión algebraica, admite diferentes definiciones: aquí la hemos visto a través de la Teoría de Cuerpos por un lado y a partir de los operadores dimensionales por otro. Sin embargo, cualquier versión deja observar la similitud con el Álgebra Lineal como he ido señalando a lo largo del desarrollo del trabajo.

El estudio algebraico profundo y detallado que he presentado ha servido para suplir un asunto que usualmente se deja de lado y no llega a impartirse en el grado, este es el de las extensiones trascendentes. He de decir que he relacionado brevemente tal contenido con el Álgebra Conmutativa y he eludido profundizar en resultados como el Teorema de Normalización de Noether, porque han sido estudiados en la optativa de Álgebra Conmutativa y Computacional y pueden verse en los apuntes de clase [9].

Para finalizar con las conclusiones, destacamos que el asunto de la trascendencia algebraica es un tema que se sigue desarrollando y que tiene relevantes problemas abiertos como el citado Séptimo problema de Hilbert. Con mi trabajo he querido hacer una introducción al contenido y un estudio riguroso, comparativo y relacionado con varias ramas de la Matemática y otros campos y problemas conocidos para llamar la atención sobre tal cuestión.

La grandeza de las Matemáticas radica en su rigidez, exactitud y abstracción. Es un área donde los errores pueden desembocar en el desarrollo de nuevas ramas y las ideas más alocadas pueden llegar a ser las más acertadas. Con esto termino mi memoria, la cual espero que haya servido para un acercamiento al tema dimensional y una apertura a la curiosidad por el Álgebra.

Referencias

[1] Alejandro Afonso, Medida, dimensión y fractales, TFG Universidad de La Laguna, (2018). (Enlace)

[2] Julio R. Bastida, Field Extensions and Galois Theory, (1984), págs. 212-278. (MR0747137)

[3] Peter J. Cameron, Introduction to algebra. Second edition. Oxford University Press, Oxford, (2008), págs. 223-228. (MR2378429)

[4] Sabrina Garbin y Miriam Mirelles, Un estudio sobre la noción de dimensión en la enseñanza–aprendizaje de las Matemáticas, Investigación Didáctica, 27(2) (2009), págs. 223-240. (Enlace)

[5] Robert Gray, Georg Cantor and trascendental numbers. Amer. Math. Monthly 101 (1994), no. 9, págs. 819–832. (MR1300488)

[6] Dale M. Johnson, The problem of the invariance of dimension in the growth of modern topology. I. Arch. Hist. Exact Sci. 20 (1979), no. 2, págs. 97–188. (MR0535148)

[7] Dale M. Johnson, The problem of the invariance of dimension in the growth of modern topology. II. Arch. Hist. Exact Sci. 25 (1981), no. 2-3, págs. 85–267. (MR0641730)

[8] Serge Lang, Algebra, (2002), págs. 355-375. (MR1878556)

[9] Francisco Javier Lobillo, Álgebra Conmutativa Computacional, (2019), págs. 30-32, 92-93. (Enlace)

[10] J.S.Milne, Field and Galois Theory, (2015), págs. 109-118. (Enlace)

[11] Manuel Ritoré, Espacios vectoriales, (2018), págs. 1-19.

[12] César Rosales, Bases, dimensión y coordenadas en un espacio vectorial, (2015), págs. 18-35. (Enlace).

[13] Philipp Rothmaler, Introduction to model theory. Gordon and Breach Science Publishers, Amsterdam, (2000), Cap.14. (MR1800596)

[14] Eric W. Weisstein, CRC concise encyclopedia of mathematics. CRC Press, Boca Raton, FL, (1999), págs. 1826-1827. (MR1660242)

[15] Vídeo explicativo de la Biyección de Cantor. YouTube. (Enlace)

Enlaces de la fotos vistas en la Sección (1)

- Foto de Cantor (Enlace).
- Foto del vídeo explicativo de la Biyección de Cantor.(Enlace).
- Foto de Poincaré.(Enlace).
- Foto de Brouwer.(Enlace).
- Foto de Urysohn.(Enlace).
- Foto de Menger.(Enlace).

Índice alfabético