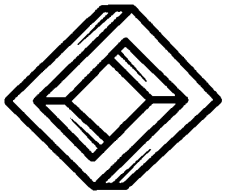
Publicaciones Electrónicas
Sociedad Matemática Mexicana

Teoría de Galois, un primer curso.
(Tercera Edición)

Flor de María Aceff
Emilio Lluis-Puebla

www.smm.org.mx

Serie: Textos. Vol. 14 (2016)



Teoría de Galois, un primer curso.
Tercera Edición

Flor de María Aceff
y
Emilio Lluis-Puebla

Universidad Nacional Autónoma de México

Publicaciones Electrónicas
Sociedad Matemática Mexicana

Índice General

Prefacio **5**

Introducción **7**

I Teoría de Anillos **9**
I.1 Anillos 9
I.2 Propiedades elementales y Teoremas de Isomorfismo 16
I.3 Polinomios y Campo de Cocientes 25

II Teoría de Campos y Teoría de Galois **37**
II.1 Extensiones de Campos 37
II.2 Automorfismos y más sobre extensiones 49
II.3 Teoría de Galois 58

Bibliografía y Referencias **67**

Lista de Símbolos **69**

Índice Analítico **71**

Prefacio

La teoría general de las estructuras es una herramienta muy poderosa. Siempre que alguien pruebe que sus objetos de estudio satisfacen los axiomas de cierta estructura, obtiene, de inmediato para sus objetos, todos los resultados válidos para esa teoría. Ya no tiene que comprobar cada uno de ellos particularmente. Actualmente, podría decirse que las estructuras permiten clasificar las diversas ramas de la Matemática.

Este texto contiene el trabajo escrito a lo largo de varios años del material correspondiente a nuestro curso sobre la materia (Álgebra Moderna II) que hemos impartido en la Facultad de Ciencias de la Universidad Nacional Autónoma de México. Después de haber ofrecido por muchos años el curso con excelentes textos, algunos citados en la Bibliografía, y de los cuales hemos sido inspirados, decidimos escribir uno que siga el enfoque de los libros [Ll1] [Ll2] y [Ll3]. Es decir, escogimos una presentación moderna donde introducimos el lenguaje de diagramas conmutativos y propiedades universales, tan requerido en la Matemática actual así como en la Física y en la Ciencia de la Computación, entre otras disciplinas.

Ha sido nuestra intención la de llegar al Teorema Principal de la Teoría de Galois de la manera más corta y elegante posible. Hemos visto que el exponer demasiado material hace muy tedioso el curso a los alumnos y al profesor, además de que algunos alumnos pierden de vista el objetivo dentro de un mar de definiciones y proposiciones. Creemos haber logrado este propósito.

El texto consta de dos capítulos con tres secciones cada uno. Cada sección contiene una serie de problemas que se resuelven con creatividad utilizando el material expuesto, mismos que constituyen una parte fundamental del texto. Tienen también como finalidad, la de permitirle al estudiante redactar matemática. El libro está diseñado para un primer curso sobre la Teoría de

Galois el cual se cubre en su totalidad en cuarenta horas de clase. La primera edición salió publicada en el 2011, la segunda en el 2013 y la presente en el 2016 conservando la estructura original con pequeños cambios y correcciones tipográficas que siempre aparecen a pesar de múltiples revisiones.

Deseamos agradecer a nuestros alumnos y a los árbitros revisores el haber hecho oportunas y acertadas sugerencias para mejorar este texto. Cualquier falta u omisión que aún permanezca es de nuestra exclusiva responsabilidad. En particular, el segundo autor de este libro agradece y aprecia el enorme esfuerzo y dedicación de su esposa, la Dra. Flor de Ma. Aceff quien a pesar de su delicado estado de salud por varios años, siempre mostró el profesionalismo y amor a la Matemática trabajando en el presente texto con todo su entusiasmo.

Finalmente, comentamos que hemos decidido incluir este texto dentro de las Publicaciones Electrónicas de la Sociedad Matemática Mexicana con el ánimo de predicar con el ejemplo y mostrar la confianza en este tipo de publicaciones.

Mayo de 2016.

Introducción

Como es frecuente en la Matemática, los intentos por resolver un problema específico dan lugar a una Teoría Matemática. En este caso, los intentos por encontrar soluciones por radicales de ecuaciones algebraicas dan como resultado varias de las ramas de la Matemática: la Teoría de Grupos, la Teoría de Anillos y la Teoría de Galois entre otras. En [A-Ll1] y [A-Ll2] el lector puede encontrar otros ejemplos de esta situación. La Teoría de Galois es una interacción entre grupos, campos y polinomios, entre el Álgebra Lineal y la Teoría de Grupos.

Se sabe de la escuela secundaria cómo encontrar por el método de radicales las soluciones de un polinomio cuadrático, con coeficientes en $\mathbb{R}$, de la forma $f(t) = at^2 + bt + c$, con $a \neq 0$. Esto lo sabían los antiguos babilonios alrededor del año 1600 A.C. Las raíces están dadas mediante la fórmula $(-b \pm \sqrt[2]{b^2 - 4ac})/2a$. Esta solución está en una tableta de barro que sobrevive hasta la fecha. Este método es válido para cualquier polinomio con coeficientes en un campo de característica diferente de 2 cuyas raíces están en la cerradura algebraica de ese campo. Lo mismo sucede para polinomios de grado 3 y 4 (del Ferro, Tartaglia, Ferrari y Cardano en 1545) sobre los números racionales. Los matemáticos trataron por cientos de años de encontrar una fórmula por radicales para polinomios de grado 5 (Lagrange en 1770 y Ruffini en 1799 probaron que los métodos para grados 3 y 4 fallan para grado 5). Fue Abel en 1824 y 1826 quien probó que esto no puede necesariamente resolverse por radicales. En fin, la solución de ecuaciones polinomiales ha sido un problema matemático por más de 3500 años.

Galois asoció a cada ecuación un grupo, llamado ahora, de Galois en honor a él. Este grupo consiste de un subconjunto de permutaciones de las soluciones. A partir de las propiedades del grupo de Galois se pueden deducir propiedades de una ecuación, sin hacer mención de ella. Vagamente, la idea

principal de la Teoría de Galois es la de considerar las permutaciones de las raíces de un polinomio que tienen la característica de que permutadas siguen satisfaciendo cualquier ecuación algebraica que satisfagan originalmente. Estas permutaciones de las raíces forman un grupo, el grupo de Galois.

El concepto que abarca a los polinomios y a los campos es el de anillo conmutativo. Comenzamos el Capítulo I estudiando el sistema algebraico de los anillos. La palabra anillo fue introducida por David Hilbert. Alrededor del año 1921, Emmy Noether fundamenta la Teoría de Anillos Conmutativos. También estudiamos dos tipos de anillos importantes, los dominios enteros y los campos. El concepto de campo (o cuerpo) fue considerado por Dedekind en 1871, por Kronecker en 1881, y por ambos alrededor de 1850 en sus clases. Pero fue Weber en 1893 quien proveyó de una definición como la que actualmente usamos. El concepto de ideal fue introducido por Kummer alrededor de 1850 y utilizado como ahora lo conocemos por Dedekind.

En 1881 Leopold Kronecker proveyó una extensión de un campo adjuntado una raíz de un polinomio irreducible. En 1894 Dedekind fue el primer matemático en desarrollar el concepto de automorfismo de campos, lo llamó permutaciones del campo. Fue Emil Artin en 1926 quien desarrolló la relación entre campos y grupos con mucho detalle y enfatizó que la Teoría de Galois no debería tener como meta la de determinar las condiciones de solubilidad de ecuaciones algebraicas sino la de explorar las relaciones entre las extensiones de campos y los grupos de automorfismos y es esta última intención la que se sigue en el presente texto.

Con respecto a la notación para una extensión de campos hemos preferido denotar con $K' \rightarrowtail K$ una extensión imitando una torre rotada 90 grados a la derecha, es decir, una torre acostada de campos ya que esto facilita visualizar específicamente los campos y su respectiva inclusión en otros.

Capítulo I

Teoría de Anillos

I.1 Anillos

En esta sección definiremos varias estructuras algebraicas que son los objetos de estudio de la Teoría de Anillos. Para un breve panorama de algunas estructuras algebraicas incluyendo las de los anillos véase [Ll3]. Supondremos que el lector ya conoce los fundamentos de la Teoría de Grupos como en [Ll3] y utilizaremos la notación que ahí se expone.

1.1 Definición. Un **anillo** es una terna $(\Lambda, +, \cdot)$ donde Λ es un conjunto no vacío, $+$ y $\cdot$ son operaciones binarias tales que
(i) $(\Lambda, +)$ es un grupo conmutativo
(ii) $(\Lambda, \cdot)$ es un semigrupo
(iii) $u(v+w) = uv + uw$ y $(u+v)w = uw + vw$

La propiedad (iii) se llama **ley distributiva**.

Nótese que se ha suprimido el símbolo $\cdot$, en uv, como es usual en la notación utilizada en la Teoría de Grupos.

1.2 Ejemplos. El lector podrá comprobar que $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(M_n K, +, \cdot)$, $(K, +, \cdot)$, $(K[x], +, \cdot)$, $(\mathbb{C}, +, \cdot)$ son anillos, (Problema 1.1).

Si un anillo $(\Lambda, +, \cdot)$ satisface

(iv) $(\Lambda, \cdot)$ es un semigrupo conmutativo, entonces $(\Lambda, +, \cdot)$ se llamará **anillo conmutativo**.

Si $(\Lambda, \cdot)$ es un monoide, diremos que $(\Lambda, +, \cdot)$ es un **anillo con identidad** o **con uno**. Denotaremos con 1 a este único elemento neutro del monoide.

Si consideramos un anillo Λ con multiplicación dada por $(u, v) \longmapsto uv$ pero definimos su multiplicación como $(u, v) \longmapsto vu$, obtendremos un anillo llamado **opuesto de** Λ, denotado ${}^o\Lambda$, que tiene el mismo elemento cero y uno de Λ. Dicho anillo coincide con Λ solamente cuando Λ es conmutativo.

Si el producto de dos elementos distintos de cero de un anillo Λ es el elemento cero del anillo, entonces esos dos elementos se dice que son **divisores de cero.** Si un anillo conmutativo $(\Delta, +, \cdot)$ con $1 \neq 0$ no posee divisores de cero, se llamará **dominio entero**. Si un dominio entero posee un inverso multiplicativo para cada elemento no nulo, se dice que es un **anillo con división**.

Observe que un anillo con uno es un anillo con división, sí, y sólo si, los elementos distintos de cero forman un grupo bajo la multiplicación (Problema 1.2). Los cuaternios $\mathbb{H}$ constituyen un ejemplo de anillo (no conmutativo) con división (Problema 1.3).

Finalmente, un **campo** es un anillo conmutativo con división.

1.3 Ejemplos. $\mathbb{Z}$ es un dominio entero, $2\mathbb{Z}$ es un anillo conmutativo sin elemento de identidad para la multiplicación; $\mathbb{Z}_n$ no es dominio entero para toda n, solamente cuando n es primo. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son campos bajo las operaciones binarias usuales en cada uno. Las matrices cuadradas sobre cualquiera de los tres campos mencionados son un anillo no conmutativo con uno. Los enteros módulo n son anillos conmutativos con uno y cuando n es primo, son campos. Los divisores de cero del anillo $\mathbb{Z}_n$ son los elementos distintos de cero que no son primos relativos con n, por lo tanto, $\mathbb{Z}_p$ no posee divisores de cero para p primo.

1.4 Definición. Diremos que un subconjunto Γ de un anillo $(\Lambda, +, \cdot)$ es un **subanillo** de Λ si Γ es, a la vez, un anillo estable o cerrado [Ll3, I.1.6] bajo las operaciónes binarias inducidas. Lo denotaremos $\Gamma < \Lambda$. Si el subanillo Γ de un anillo Λ es un dominio entero, entonces diremos que Γ es

un **subdominio** de Λ. Si el subanillo Γ de un anillo Λ es un campo, entonces diremos que Γ es un **subcampo** de Λ.

De la definición de subanillo es inmediato el siguiente resultado que proporciona una manera de comprobar si un subconjunto de un anillo es un subanillo de él.

1.5 Proposición. Un subconjunto Γ de un anillo $(\Lambda, +, \cdot)$ es un subanillo de Λ si, y sólo si, Γ es estable o cerrado bajo $+$ y $\cdot$, i.e., si $x - y \in \Gamma$ y $xy \in \Gamma$ para cualesquiera x, $y \in \Gamma$.

Demostración. Véase el Problema 1.4.♦

1.6 Ejemplos. Para todo entero $n \in \mathbb{Z}$, $n\mathbb{Z} < \mathbb{Z}$. $\mathbb{Z} < \mathbb{R} < \mathbb{C}$. Pero como dominios enteros, $\mathbb{Z}$ es un subdominio de $\mathbb{R}$ y $n\mathbb{Z}$ no es un subdominio de $\mathbb{Z}$ para n distinto de 1 y -1. $\mathbb{Q}$ es un subcampo de $\mathbb{R}$, pero $\mathbb{Z}$ no es un subcampo de $\mathbb{R}$.

Es fácil ver que un subanillo no trivial Γ de un dominio entero Λ es un subdominio de Λ sí, y sólo si, Γ contiene al elemento de identidad de Λ (Problema 1.7). Asímismo, es fácil ver que un subanillo Γ de un campo Λ es un subcampo de Λ sí, y sólo si, para todo elemento $x \in \Gamma$, su inverso $x^{-1} \in \Gamma$ (Problema 1.8).

A continuación, veamos un concepto que hace el papel para la Teoría de Anillos equivalente a la de subgrupo normal para la Teoría de Grupos.

1.7 Definición. Un subanillo I de un anillo Λ se llamará **ideal izquierdo de** Λ si para toda $x \in \Lambda$ y para toda $a \in I$ se tiene que $xa \in I$, es decir, $\Lambda I \subset I$. Un subanillo I de un anillo Λ se llamará **ideal derecho de** Λ si para toda $x \in \Lambda$ y para toda $a \in I$ se tiene que $ax \in I$, es decir, $I\Lambda \subset I$. Un subanillo I de un anillo Λ se llamará **ideal de** Λ si es ideal izquierdo e ideal derecho a la vez.

1.8 Ejemplos. El subanillo $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$. Los subanillos Λ y 0 son los **ideales triviales** de Λ. Los ideales izquierdos de Λ son los ideales derechos de ${}^{o}\Lambda$.

Observe que si Λ es un anillo e I un ideal de Λ, la parte aditiva de Λ constituye un grupo abeliano y, por lo tanto, I es un subgrupo normal de Λ.

Los ideales de un anillo distintos de los triviales se llamarán **ideales propios no triviales**.

1.9 Proposición. Sea Λ un anillo con división. Entonces Λ solamente posee ideales triviales.

Demostración: Sea I un ideal no trivial cualquiera de Λ. Como I es no trivial, posee un elemento $a \in I$ diferente de cero. Por ser I ideal, $1 = aa^{-1} \in I$. Por lo tanto, $\Lambda = 1\Lambda \subset I\Lambda \subset I$. Luego, $I = \Lambda$.♦

Observe que debido a esta proposición, un campo no puede poseer ideales propios no triviales.

¿Cómo se relacionan dos anillos? Mediante funciones que preserven la estructura de anillos.

1.10 Definición. Si $(\Lambda, \diamond, \star)$ y $(\Lambda', +, \cdot)$ son anillos, un **homomorfismo de anillos** es una función que es un homomorfismo del grupo conmutativo de Λ en el grupo conmutativo de Λ' y que también es un homomorfismo del semigrupo de Λ en el semigrupo de Λ', es decir,

$$f(x \diamond y) = f(x) + f(y) \text{ y } f(x \star y) = f(x) \cdot f(y).$$

Usualmente utilizaremos, por abuso, la notación $+$ y $\cdot$ para denotar las (posibles) diferentes operaciones binarias de dos anillos relacionados mediante un homomorfismo, quedando la notación imprecisa, pero usual

$$f(x + y) = f(x) + f(y) \text{ y } f(x \cdot y) = f(x) \cdot f(y).$$

o peor aún,

$$f(x + y) = f(x) + f(y) \text{ y } f(xy) = f(x)f(y).$$

Imitando lo correspondiente para grupos [Ll3] tenemos la siguiente

1.11 Proposición. La composición de dos homomorfismos de anillos es un homomorfismo de anillos.

Demostración. Sean $f : \Lambda' \to \Lambda$ y $g : \Lambda \to \Lambda''$ homomorfismos de anillos. Luego $(g \circ f)(x + y) = g(f(x + y)) = g(f(x) + f(y)) = g(f(x)) + g(f(y)) = (g \circ f)(x) + (g \circ f)(y)$. Análogamente, $(g \circ f)(xy) = g(f(xy)) =$

$g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$. Por lo tanto $(g \circ f)$ es un homomorfismo de anillos.♦

1.12 Definición. Sea $f : \Lambda \to \Lambda'$ un homomorfismo de anillos. Diremos que f es un **isomorfismo**, y escribiremos $f : \Lambda \xrightarrow{\cong} \Lambda'$ si existe un homomorfismo $g : \Lambda' \to \Lambda$ tal que $g \circ f = 1_\Lambda$ y $f \circ g = 1_{\Lambda'}$.

Es fácil comprobar (Problema 1.11) que, si g existe está determinada en forma única; lo denotaremos con f^{-1} y se llama **inverso** de f. Diremos que dos anillos Λ y Λ' son **isomorfos** si existe un isomorfismo $f : \Lambda \xrightarrow{\cong} \Lambda'$ y escribiremos $\Lambda \cong \Lambda'$.

1.13 Definición. Sea $f : \Lambda \to \Lambda'$ un homomorfismo de anillos. El **núcleo** de f, denotado $\ker f$, es el conjunto de todos los elementos $x \in \Lambda$ tales que $f(x) = 0$ donde 0 denota la identidad aditiva de Λ'. La **imagen** de f, denotada $im\ f$, es el conjunto de $f(x)$ con $x \in \Lambda$.

Observe que solamente vemos el concepto de núcleo de un homomorfismo de anillos como núcleo de la parte de grupo aditivo de los anillos. Aún cuando los anillos sean con uno, no pediremos que la imagen del uno del anillo del dominio vaya a dar al uno del anillo codominio (Problema 1.12).

Si en la definición de homomorfismo se tiene que $\ker f = \{0\}$, diremos que f es un **monomorfismo** y lo denotamos $f : \Lambda \rightarrowtail \Lambda'$; si $im\ f = \Lambda'$, diremos que f es un **epimorfismo** y lo denotamos $f : \Lambda \twoheadrightarrow \Lambda'$ y si f es tal que $\ker f = \{0\}$ e $im\ f = \Lambda'$, entonces diremos que f es un **isomorfismo**. De otra manera, f es un monomorfismo cuando es inyectiva; es un epimorfismo cuando es suprayectiva y es un isomorfismo cuando es biyectiva. Llamaremos **endomorfismo** a un homomorfismo $f : \Lambda \to \Lambda$ y diremos que es **automorfismo** si dicha f es biyectiva.

Observe que, como grupos conmutativos, $2.\_ : \mathbb{Z} \longrightarrow 2\mathbb{Z}$ dado por $x \longmapsto 2x$ establece un isomorfismo de grupos abelianos pero, como anillos no se tiene un isomorfismo.

Diremos que un homomorfismo $f\colon \Lambda \to \Lambda'$ es **trivial** si $f(x) = 0$ para todo $x \in \Lambda$. Es decir, $im\ f = \{0\}$. Equivalentemente, $f = 0$ si, y sólo si, $\ker f = \Lambda$.

Recuérde que si A es un subconjunto de B, la función $\iota : A \longrightarrow B$ dada por $\iota(a) = a \in B$ para toda $a \in A$ se llama **inclusión** de A en B. La función identidad de un anillo Λ en sí mismo es un homomorfismo llamado **homomorfismo de identidad**.

1.14 Proposición. Sean $f\colon \Lambda' \to \Lambda$, $g\colon \Lambda \to \Lambda''$ dos homomorfismos de anillos y $h = g \circ f$ la composición. Entonces, (i) si h es monomorfismo, f es monomorfismo, y (ii) si h es epimorfismo, g es epimorfismo.

Demostración. (i) Supongamos que h es monomorfismo. Si $f(x) = f(y)$ luego $h(x) = g(f(x)) = g(f(y)) = h(y)$. Como h es monomorfismo, $x = y$. Por lo tanto, f es monomorfismo. (ii) Supongamos que h es epimorfismo. Entonces $h(\Lambda') = \Lambda''$. Luego, $\Lambda'' = h(\Lambda') = g(f(\Lambda')) \subset g(\Lambda) \subset \Lambda''$. Por lo tanto, $g(\Lambda) = \Lambda''$.♦

Problemas.

1.1 (i) Compruebe que los conjuntos con sus operaciones binarias respectivas en el Ejemplo 1.2 son efectivamente anillos.
(ii) Defina operaciones binarias de suma y producto en nZ y pruebe que nZ es un anillo, n entero positivo.

1.2 Pruebe que un anillo con uno es un anillo con división, sí, y sólo si, los elementos distintos de cero forman un grupo bajo la multiplicación.

1.3 Verifique que los cuaternios $\mathbb{H}$ forman un anillo (no conmutativo) con división.

1.4 Pruebe que un subconjunto Γ de un anillo $(\Lambda, +, \cdot)$ es un subanillo de Λ si, y sólo si, Γ es estable o cerrado bajo $+$ y $\cdot$.

1.5 Compruebe que si G es un grupo abeliano, entonces el conjunto de endomorfismos $End(G, G)$ con la composición es un anillo.

1.6 Compruebe que los anillos $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ son conmutativos y que $End(G, G)$ del Problema 1.5 no lo es.

1.7 Pruebe que un subanillo no trivial Γ de un dominio entero Λ es un subdominio de Λ sí, y sólo si, Γ contiene al elemento de identidad de Λ.

1.8 Pruebe que un subanillo Γ de un campo Λ es un subcampo de Λ sí, y sólo si, para todo elemento $x \in \Gamma$, su inverso $x^{-1} \in \Gamma$.

1.9 Sea Λ un anillo. Pruebe que el conjunto $I = \{x \in \Lambda \mid nx = 0, n \in \mathbb{Z}\}$ es un ideal de Λ.

1.10 Pruebe que $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ dado por $x \longmapsto r$, donde r es el residuo módulo n es un homomorfismo de anillos.

1.11 En la notación la Definición 1.12 pruebe que, si g existe, está determinada en forma única, el cual es denotado con f^{-1} y se llama inverso de f.

1.12 Proporcione un ejemplo en donde bajo un homomorfismo de anillos, $f : \Lambda \to \Lambda'$, $f(1_\Lambda) \neq 1_{\Lambda'}$.

Pruebe que, como anillos, $\mathbb{Z}_i \times \mathbb{Z}_j$ es isomorfo a $\mathbb{Z}_{i\times j}$ cuando el máximo común divisor $(i, j) = 1$.

1.14 Encuentre las raíces de la ecuación $x^2 - 7x + 12$ en $\mathbb{Z}_8$.

1.15 Pruebe que los inversos izquierdo y derecho de una unidad en un anillo con uno coinciden.

1.16 Demuestre que los divisores de cero del anillo $\mathbb{Z}_n$ son los elementos distintos de cero que no son primos relativos con n, por lo tanto, $\mathbb{Z}_p$ no posee divisores de cero para p primo.

1.17 Demuestre que si Δ es un dominio entero finito, entonces Δ es campo.

I.2 Propiedades elementales y Teoremas de Isomorfismo

Veamos algunas propiedades de los anillos.

2.1 Proposición. Sea Λ un anillo. Entonces

(i) $0x = 0 = x0$ para toda $x \in \Lambda$.

(ii) En un anillo Λ vale la ley de cancelación para todo elemento distinto de cero sí, y sólo si, Λ no posee divisores de cero.

(iii) $(-x)y = x(-y) = -(xy)$, para toda x,$y \in \Lambda$.

(iv) $(-x)(-y) = xy$ para toda x,$y \in \Lambda$.

Demostración. (i) Como $0 = 0 + 0$, $0x = (0 + 0)x = 0x + 0x$. Luego, $0x = 0$. Análogamente, $x0 = 0$.

(ii) Supongamos que en Λ vale la ley de la cancelación para todo elemento distinto de cero. Veamos que Λ no tiene divisores de cero. Tomemos el producto de dos elementos distintos de cero tal que su producto sea cero, es decir, $xy = 0$. Por la parte (i), $x0 = 0$. Luego $xy = x0$. Como $x \neq 0$, entonces $y = 0$. Esto contradice el hecho de que $y \neq 0$.

Ahora, supongamos que Λ no tiene divisores de cero. Supongamos que $xa = ya$ para $a \neq 0$. Luego, por la distributividad, $(x - y)a = xa - ya = 0$. Como $a \neq 0$ y Λ no posee divisores de cero, $x - y = 0$. Así, $x = y$.

(iii) Como $xy + (-x)y = (x + (-x))y = 0y = 0$ luego $(-x)y = -(xy)$ pues el inverso es único. Análogamente $xy + x(-y) = x(y + (-y)) = x0 = 0$, luego $x(-y) = -(xy)$.

(iv) Por (iii) $-(x(-y)) = (-x)(-y)$. También, por (iii), $-(x(-y)) = -(-(xy))$. Luego, $-(-(xy)) + (-xy) = 0$. Luego, $-(-(xy)) = xy$. Así, $(-x)(-y) = xy$ para toda x,$y \in \Lambda$.

Sea $(\Lambda, +, \cdot)$ un anillo con uno. Un elemento $x \in \Lambda$ se llama **inverso izquierdo** de un **elemento invertible por la izquierda** $y \in \Lambda$ si $xy = 1$. Análogamente, un elemento $x \in \Lambda$ se llama **inverso derecho** de un **elemento invertible por la derecha** $z \in \Lambda$ si $zx = 1$. Diremos que $y \in \Lambda$ es **invertible** o **unidad** si es a la vez invertible por la izquierda y la derecha.

Es fácil comprobar que los inversos izquierdo y derecho de una unidad en un anillo con uno coinciden y que el conjunto de unidades es un grupo bajo la multiplicación (Problema 2.6).

Observe que si I es un ideal con uno de un anillo conmutativo con uno Λ, se tiene que $\Lambda I \subset I$, es decir $xI \subset I$ para toda $x \in \Lambda$. Si tomamos $y \in I$ una unidad de Λ, entonces consideremos $x = y^{-1}$. Luego, $y^{-1}y = 1 \in I$. Así, $xI \subset I$, para toda $x \in \Lambda$ y $x1 = x \in \Lambda$. Entonces $I = \Lambda$. Además si Λ es un anillo no necesariamente conmutativo con uno e I un ideal que contiene también al uno de Λ, entonces $I = \Lambda$.

2.2 Proposición. Sea $f : \Lambda \longrightarrow \Lambda'$ un homomorfismo de anillos. Entonces $\ker f$ es un ideal de Λ e $im\, f$ es un subanillo de Λ'.

Demostración. Por [Ll3, I.3.20] $\ker f$ e $im\, f$ son subrupos de la parte abeliana aditiva de Λ y Λ' respectivamente y fácilmente se puede ver que son subsemigrupos de la parte multiplicativa de Λ y Λ' respectivamente. Para ver que $\ker f$ es un ideal de Λ, sea $x \in \ker f$ y $a \in \Lambda$. Entonces $f(ax) = f(a)f(x) = f(a)0 = 0$. Por lo tanto, $ax \in \ker f$. Análogamente, $xa \in \ker f$. Luego, $\ker f$ es un ideal.♦

Una consecuencia inmediata es la siguiente: sea $f : \Lambda \longrightarrow \Lambda'$ un homomorfismo no trivial donde Λ es un campo y Λ' un anillo. Por la proposición anterior, $\ker f$ es un ideal de Λ y por 1.9, como Λ es campo, no posee ideales no triviales, es decir, solamente posee al 0 y a Λ como ideales. Como f no es trivial, $\ker f = 0$ y por lo tanto, f es monomorfismo.

Es inmediato comprobar que todo dominio entero finito es un anillo con división (Problema 2.1) y que todo dominio entero conmutativo finito es un campo (Problema 1.17). Observe que todo dominio entero y anillo con

división poseen al menos los elementos de identidad bajo la suma y multiplicación. Por ejemplo, el dominio entero $\mathbb{Z}$ no es un campo pues todo entero distinto de ± 1 no posee inverso.

De manera semejante a [Ll3, I.3.18] se tiene la siguiente

2.3 Proposición. La intersección de subanillos de un anillo es un subanillo.

Demostración. Véase el Problema 2.5.♦

Imitando la definición de [Ll2, I.2.17] para espacios vectoriales, tenemos

2.4 Definición. Sea S un subconjunto de un anillo Λ. La intersección de todos los subanillos de Λ que contienen a S se llama **subanillo de Λ generado por** S.

Definiciones semejantes se tienen de **subdominio** o **subcampo generado por un subconjunto** S.

2.5 Definición. Diremos que un anillo Λ es de **característica 0** (denotada $car(\Lambda) = 0$) si $n = 0$ es el único entero tal que $nx = 0$ para toda $x \in \Lambda$. Si Λ no es de característica 0, el menor entero positivo n tal que $nx = 0$ para toda $x \in \Lambda$ se llama **característica** del anillo Λ (denotada $car(\Lambda) = n$).

2.6 Ejemplos Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen característica 0. El anillo $\mathbb{Z}_n$ tiene característica n.

2.7 Proposición.

(i) Sea Λ un anillo con 1. La característica de Λ es igual al orden del elemento 1. De no ser así, Λ es de característica **0** si el grupo aditivo de Λ es de orden infinito.

(ii) Si Λ no posee divisores de 0, todos los elementos distintos de cero tienen el mismo orden.

(iii) Si Λ es un anillo no trivial sin divisores de cero tal que $car(\Lambda) \neq 0$, entonces Λ es de característica igual a un número primo.

Demostración. (i) Sea n el orden del 1, es decir, n veces $1+1+\cdots+1 = 0$. Entonces, $nx = n(1x) = (n1)x = 0$ para toda $x \in \Lambda$. Así, Λ es de

característica n. Es claro que Λ es de característica 0 si el 1 es de orden infinito.

(ii) Sean x,y cualesquiera dos elementos distintos de cero del anillo Λ y supongamos que x es de orden n. Luego, $x(ny) = n(xy) = (nx)y = 0y = 0$. Por hipótesis, Λ no posee divisores de cero y como x es distinto de cero, se tiene que $ny = 0$. Como y es arbitrario, cualquier elemento distinto de cero tiene orden n.

(iii) Sea $n = car(\Lambda)$. Como $\Lambda \neq 0$, podemos escoger un elemento $x \neq 0$. Luego, por (ii), x es de orden n. Veamos que n debe ser un número primo. Supongamos que n se factoriza como producto de dos primos $n = pq$. Entonces, $(px)(qx) = pqxx = nxx = 0$. Como Λ no posee divisores de cero, px ó qx debe ser 0. Como x es de orden n, ó p ó q es n y el que queda es 1. Por lo tanto, n es primo.♦

Por la proposición anterior podemos decir que un anillo no trivial Λ sin divisores de cero es de característica 0 sí, y sólo si, todo elemento distinto de cero es de orden infinito. De otra manera, la característica $car(\Lambda)$ es un número primo y todo elemento distinto del cero es de orden p.

Recordando el concepto de espacio vectorial cociente estudiado en el curso de Álgebra Lineal como en [Ll2, II.4] o en la Teoría de Grupos como en [Ll3, II.2] y considerando la parte aditiva, se tenía que, para el caso en que Λ es un grupo conmutativo e I un subgrupo de Λ con $x \in \Lambda$, denotábamos con $x + I$ el conjunto $\{x + y | y \in I\}$. Dichos elementos $x + I$ los llamamos **clases laterales** de I en Λ. Como $0 \in I$ y $x = x + 0 \in x + I$, cada $x \in \Lambda$ pertenece a una clase lateral.

Se comprobó que cualesquiera dos clases laterales o son ajenas o son iguales. Se denotó con Λ/I el conjunto de todas las clases laterales de I en Λ y se le dio a Λ/I una estructura de grupo mediante

$$+ : \Lambda/I \times \Lambda/I \to \Lambda/I$$

dada por

$$((x + I), (y + I)) \longmapsto ((x + y) + I).$$

También se comprobó que la operación binaria anterior está bien definida y que define una estructura de grupo abeliano (la parte aditiva de espacio vectorial) en Λ/I. Llamamos a Λ/I, **grupo cociente** de Λ módulo I.

También, se vio que si I es un subgrupo del grupo Λ y si $y \in x + I$, entonces existe $w \in I$ tal que $y = x + w$. Así $y - x = w \in I$. Luego, $y - x \in I \iff -(y - x) = x - y \in I \iff x \in y + I$. En resumen,

$$y \in x + I \iff y - x \in I \iff x \in y + I$$

Finalmente, se consideró $p\colon \Lambda \to \Lambda/I$ dada por $x \longmapsto x + I$. Si x,$w \in \Lambda$, entonces

$$p(x + w) = (x + w) + I = (x + I) + (w + I) = p(x) + p(w).$$

Por lo tanto, p es un homomorfismo de grupos llamado **proyección canónica**.

Todo esto se realizó para espacios vectoriales sobre un campo K. Recuérdese de nuevo que la parte aditiva es un grupo conmutativo. Lo mismo sucede para la parte abeliana aditiva de los anillos. Si Λ es un anillo e I un ideal de Λ, la parte aditiva de Λ constituye un grupo abeliano y, por lo tanto, I es un subgrupo normal de Λ.

Ahora, para Λ un anillo e I un ideal de Λ, definamos en el grupo cociente Λ/I una multiplicación

$$\cdot\colon \Lambda/I \times \Lambda/I \to \Lambda/I$$

dada por

$$((x + I), (y + I)) \longmapsto ((x \cdot y) + I)$$

Si tomamos elementos cualesquiera x,$y \in \Lambda$ y a,$b \in I$ entonces,

$$(x + a)(y + b) = xy + xb + ay + ab \in xy + I$$

por la distributividad e I ser un ideal. Luego

$$(x + I)(y + I) \subset xy + I.$$

Así, la clase lateral $xy + I$ no depende de los elementos x e y y únicamente sí depende de las clases laterales $(x + I)$ y $(y + I)$ lo cual nos dice que la multiplicación anterior está bien definida haciendo por lo tanto de Λ/I un anillo. Llamaremos a Λ/I **anillo cociente de Λ sobre su ideal** I. Si Λ

posee elemento de identidad 1, entonces $1+I$ es la identidad en Λ/I. Observe que si Λ es conmutativo, también Λ/I lo es.

Considere $p\colon \Lambda \to \Lambda/I$ dada por $x \longmapsto x+I$. Si x,$y \in \Lambda$, entonces

$$p(xy) = (xy) + I = (x+I)(y+I) = p(x)p(y).$$

Luego, p es un epimorfismo de anillos, denotado $p : \Lambda \twoheadrightarrow \Lambda/I$, con núcleo $I = \ker p$. Así tenemos una sucesión exacta corta [Ll3, II.1]:

$$0 \longrightarrow I \xrightarrow{\ i\ } \Lambda \xrightarrow{\ p\ } \Lambda/I \longrightarrow 0.$$

Por lo tanto, hemos visto que un subanillo I de un anillo Λ es un ideal de Λ si, y sólo si, existe un homomorfismo de anillos $f : \Lambda \to \Lambda'$ con núcleo $\ker f = I$.

Sea $f : \Lambda \to \Lambda'$ un homomorfismo de anillos con ideales $I \subset \Lambda$ e $I' \subset \Lambda'$ tales que $f(I) \subset I'$, entonces $f^* : \Lambda/I \longrightarrow \Lambda'/I'$ dado por $f^*(x+I) = f(x)+I'$ es el homomorfismo inducido por f en los grupos abelianos cociente [Ll3, II.3]. Como

$$\begin{aligned} f^*((x+I)(y+I)) &= f^*(xy+I) \\ &= f(xy)+I' \\ &= f(x)f(y)+I' \\ &= (f(x)+I')(f(y)+I') \\ &= f^*(x+I)f^*(y+I) \end{aligned}$$

para toda x,$y \in \Lambda$, el homomorfismo de anillos $f^* : \Lambda/I \longrightarrow \Lambda'/I'$ se llama **homomorfismo inducido por** f.

Análogamente a [Ll3, II.3.2], se tiene

2.8 Proposición. Sea $f : \Lambda \to \Lambda'$ un homomorfismo de anillos con ideales $I \subset \Lambda$ e $I' \subset \Lambda'$ tales que $f(I) \subset I'$. Considérense las proyecciones canónicas a los cocientes correspondientes $p : \Lambda \longrightarrow \Lambda/I$ y $p' : \Lambda' \longrightarrow \Lambda'/I'$. Entonces $f^* : \Lambda/I \longrightarrow \Lambda'/I'$ es el homomorfismo inducido por f, el siguiente cuadrado es conmutativo

$$\begin{array}{ccc} \Lambda & \xrightarrow{\ f\ } & \Lambda' \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p'} \\ \Lambda/I & \xrightarrow{\ f^*\ } & \Lambda'/I' \end{array}$$

e $im\, f^* = p'(im\, f)$ y $\ker f^* = p(f^{-1}(I'))$.♦

Análogamente a [Ll3, II.3.3], se tiene

2.9 Teorema. Bajo las mismas hipótesis de la proposición anterior, en particular, si f es un epimorfismo con $I' = e$ e $I = \ker f$ entonces $\Lambda'/I' \cong \Lambda'$ y f^* es un isomorfismo en el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \Lambda & \overset{f}{\twoheadrightarrow} & \Lambda' \\ \downarrow{\scriptstyle p} & & \cong\downarrow I_{\Lambda'} \\ \Lambda/\ker f & \overset{f^*}{\longrightarrow} & \Lambda' \end{array}$$

♦

Análogamente a [Ll3, II.3.4], se tiene

2.10 Teorema. Sea $f : \Lambda \to \Lambda'$ un homomorfismo de anillos con ideales $I \subset \Lambda$ e $I' \subset \Lambda'$ tales que $f(I) \subset I'$ y como caso particular del teorema anterior, $e = I' \subset \Lambda'$ con $I \subset \ker f$. Entonces existe un homomorfismo único $f^* : \Lambda/I \longrightarrow \Lambda'$ dado por $x + I \mapsto f^*(x + I) = f(x) + I' = f(x)$. Además, $\ker f^* = \ker f/I$ e $imf = imf^*$. El homomorfismo f^* es un isomorfismo si, y sólo si, f es un epimorfismo e $I = \ker f$.♦

Análogamente a [Ll3, II.3.5], se tiene

2.11 Corolario. (Primer Teorema de Isomorfismo). Bajo las mismas hipótesis del teorema anterior $\Lambda/\ker f \cong im\, f$.

Demostración. Como f es epimorfismo, $im\, f = \Lambda'$, luego $\Lambda/\ker f \cong im\, f$.♦

En otras palabras, si $f : \Lambda \twoheadrightarrow \Lambda'$ es un epimorfismo de anillos con núcleo $\ker f$, entonces existe un isomorfismo único $f^* : \Lambda/\ker f \cong \Lambda'$, tal que $f = f^* \circ p$, es decir, cualquier homomorfismo de Λ con núcleo $\ker f$ tiene imagen isomórfica a $\Lambda/\ker f$. Aún más, nos dice cuál isomorfismo: aquel tal que $im\, f = im\, f^*$. Este resultado, $\Lambda/\ker f \cong im\, f$ se conoce como el **Primer Teorema de Isomorfismo**. Uno puede "determinar" cuál es el anillo cociente de dos anillos sin necesidad de establecer las clases laterales como veremos en más adelante.

2.12 Ejemplo. Sea I un ideal de un anillo Λ. Consideremos el anillo cociente Λ/I. Sea $\iota\colon I \longrightarrow \Lambda$ el monomorfismo de inclusión y $p\colon \Lambda \longrightarrow \Lambda/I$ el epimorfismo de proyección. Entonces $im\,\iota = I = \ker p$ y, por lo tanto,

$$0 \longrightarrow I \xrightarrow{\iota} \Lambda \xrightarrow{p} \Lambda/I \longrightarrow 0$$

es una sucesión exacta corta. Consideremos ahora una sucesión exacta corta

$$0 \xrightarrow{h} \Lambda' \xrightarrow{f'} \Lambda \xrightarrow{f} \Lambda'' \xrightarrow{k} 0.$$

Recordemos entonces que $im\,f' = \ker f$, y f' es monomorfismo, pues $0 = im\,h = \ker f$ y, además, f es epimorfismo porque $im\,f = \ker k = \Lambda''$. Sea $I = im\,f' = \ker f$ el cual es un ideal de Λ, entonces f' establece un isomorfismo $I \xrightarrow{\cong} \Lambda'$ y f establece otro isomorfismo $\Lambda/I \xrightarrow{\cong} \Lambda''$ por el primer teorema de isomorfismo. Por lo tanto, una sucesión exacta corta es una sucesión con un ideal y el anillo cociente de un anillo.

2.13 Ejemplo. $f : \Lambda \twoheadrightarrow \Lambda''$ donde $\Lambda = \mathbb{Z}$ y $\Lambda'' = \mathbb{Z}_n$ es un epimorfismo con núcleo el subgrupo $n\mathbb{Z}$, es decir,

$$0 \longrightarrow n\mathbb{Z} \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}_n \longrightarrow 0$$

es un sucesión exacta corta. Luego, por el teorema anterior $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Análogamente a [Ll3, II.3.11], se tiene

2.14 Teorema. (**Segundo Teorema de Isomorfismo**). Sean I,J ideales de Λ. Entonces $(I + J)/J \cong I/(I \cap J)$.♦

Análogamente a [Ll3, II.3.13], se tiene

2.15 Teorema. (**Tercer Teorema de Isomorfismo**). Sean I,J ideales de Λ con $J \subset I$. Entonces, $\Lambda/I \cong (\Lambda/J)/(I/J)$.♦

2.16 Teorema.
(i) Si Δ es un dominio entero de característica 0, entonces el subgrupo aditivo de Δ generado por el 1 es isomorfo a $\mathbb{Z}$.
(ii) Si Δ es un dominio entero de característica $p \neq 2$, entonces el subgrupo aditivo de Δ generado por el 1 es un subcampo isomorfo a $\mathbb{Z}_p$.

Demostración. (i) Sea $f : \mathbb{Z} \longrightarrow \Delta$ dada por $n \longrightarrow f(n) = n1$. Como $f(n + n') = (n + n')1 = n1 + n'1 = f(n) + f(n')$ y $f(nn') = (nn')1 = (n1)(n'1) = f(n)f(n')$. Luego f es un homomorfismo. Como Δ es de característica 0, el 1 es de orden infinito. Así que el núcleo de f consiste solamente del 0 y por lo tanto, f es monomorfismo. Claramente, la imagen de $\mathbb{Z}$ bajo f es el subgrupo de Δ.

(ii) Si Δ no es de característica 0 entonces la característica de Δ es un número primo p y el 1 es de orden p. Por lo tanto, el núcleo de f es el ideal $p\mathbb{Z}$. Luego f induce un monomofismo $f^* : \mathbb{Z}/p\mathbb{Z} \longrightarrow \Delta$.♦

Problemas.

2.1 Compruebe que todo dominio entero finito es un anillo con división.

2.2 Compruebe que el dominio entero $\mathbb{Z}$ no es un campo.

2.3 Compruebe que $\mathbb{Z}_n$ es campo sí, y sólo si, n es un número primo.

2.4 Compruebe que los dominios enteros $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son campos.

2.5 (i) Pruebe que la intersección de subanillos de un anillo es un subanillo.

(ii) Pruebe lo correspondiente a la parte (i) para subdominios y subcampos.

2.6 Demuestre que los inversos izquierdo y derecho de una unidad en un anillo con uno Λ coinciden y que el conjunto de unidades es un grupo bajo la multiplicación, denotado Λ^*.

2.7 Compruebe que $\Lambda/\{0\} \cong \Lambda$ y que $\Lambda/\Lambda \cong \{0\}$.

2.8 Escriba detalladamente la demostración de 2.8.

2.9 Escriba detalladamente la demostración de 2.9.

2.10 Escriba detalladamente la demostración de 2.10.

2.11 Escriba detalladamente la demostración de 2.14.

2.12 Escriba detalladamente la demostración de 2.15.

I.3 Polinomios y Campo de Cocientes

En los cursos usuales de Álgebra Superior (como en CLl) se estudia el anillo de polinomios. Ahí se definen, se le da una estructura de anillo al conjunto de polinomios, se estudia lo referente a divisibilidad y factorización, etc. En este curso damos por estudiado tales temas y únicamente haremos mención de los resultados que requerimos para nuestro estudio posterior.

A continuación definiremos, siguiendo el estilo de [Ll3], el anillo de polinomios $\Lambda[t]$ de un anillo Λ.

3.1 Definición. Sea Λ un anillo con uno. Un **anillo de polinomios de** Λ es una terna,

$$(\Pi, f, t)$$

donde Π es un anillo, $f : \Lambda \rightarrowtail \Pi$ es un monomorfismo con $f(1)$ como identidad de Π, $t \in \Pi$ un elemento que conmuta con $f(x)$ para toda $x \in \Lambda$, tal que (cumple la siguiente *propiedad* llamada *universal*) para todo monomorfismo $g : \Lambda \rightarrowtail \Lambda'$ con $g(1)$ como identidad de Λ' y todo elemento $y \in \Lambda'$ que conmuta con $g(x)$ para toda $x \in \Lambda$, existe un homomorfismo único $h : \Pi \to \Lambda'$ tal que $h(t) = y$ y $h \circ f = g$, es decir, el siguiente diagrama conmuta:

$$\begin{array}{ccc} \Lambda & \xrightarrow{f} & \Pi \\ & {\scriptstyle g}\searrow & \downarrow{\scriptstyle h} \\ & & \Lambda' \end{array}$$

3.2 Teorema. Sea (Π, f, t) un anillo de polinomios de Λ. Entonces el conjunto $f(\Lambda) \cup \{t\}$ genera Π. Además, si (Π', f', t') es otro anillo de polinomios de Λ, entonces existe un isomorfismo único $k : \Pi \to \Pi'$ tal que $k(t) = t'$ y $k \circ f = f'$.

Demostración. La demostración es análoga a las de [Ll3, III.3] y la dejamos como ejercicio para el lector (Problema 3.1).♦

Considérese $\mathbb{Z}^+ \cup \{0\}$ el conjunto de enteros no negativos, Λ un anillo con uno, y sea $\Pi = \{\varphi : \mathbb{Z}^+ \cup \{0\} \longrightarrow \Lambda \mid \varphi(n) = 0 \text{ para casi toda } n \in \mathbb{Z}^+ \cup \{0\}\}$. Démosle a Π una estructura de anillo (Problema 3.2 (i)) definiendo dos operaciones binarias

$$\begin{aligned} + \quad &: \quad \Pi \times \Pi \longrightarrow \Pi \\ (\varphi, \xi) \quad &\mapsto \quad (\varphi + \xi)(n) = \varphi(n) + \xi(n) \\ \cdot \quad &: \quad \Pi \times \Pi \longrightarrow \Pi \\ (\varphi, \xi) \quad &\mapsto \quad (\varphi\xi)(n) = \sum_{j=0}^{n} \varphi(j)\xi(n-j). \end{aligned}$$

Ahora, para cada $x \in \Lambda$, definamos una función que depende de x denotada f_x mediante

$$f_x(n) = x \text{ si } n = 0 \text{ ó } 0 \text{ si } n > 0.$$

Así, $f_x \in \Pi$ y la asignación dada por $x \mapsto f_x$ define una función $f : \Lambda \to \Pi$. Es fácil comprobar que f es un monomorfismo y que $f(1)$ es la identidad de Π (Problema 3.2 (ii)).

Definamos $t \in \Pi$ dado por $t(n) = 1$ si $n = 1$ o 0 si $n \neq 1$. Claramente t conmuta con f_x para toda $x \in \Lambda$. Veamos que (Π, f, t) es un anillo de polinomios de Λ : sea $g : \Lambda \to \Lambda'$ un monomorfismo con $g(1)$ como identidad tal que cualquier elemento $y \in \Lambda'$ conmute con $g(x)$ para toda $x \in \Lambda$. Definamos $h : \Pi \to \Lambda'$ mediante

$$\varphi \longmapsto h(\varphi) = g(\varphi(0)) + \sum_{n=1}^{\infty} g(\varphi(n))y^n.$$

Como $\varphi(n) = 0$ para casi toda n, la sumatoria es finita. Es fácil ver que h es homomorfismo, $h(t) = y$, $h \circ f = g$ y que es única (Problema 3.2 (iii)). De aquí que cualquier elemento de Π puede escribirse de manera única como $\varphi = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$, donde $\lambda_i \in \Lambda$ y $\lambda_i = \varphi(i)$ para $i = 0, \ldots, n$. Así tenemos el siguiente

3.3 Teorema. Para cualquier anillo con uno Λ, existe un anillo de polinomios de Λ.♦

Identificaremos Λ con su imagen $f(\Lambda)$ dentro de Π. Así, Λ se puede ver como un subanillo de Π bajo la inclusión f. Llamaremos a Π, **anillo de polinomios de** Λ y a t **indeterminada**. Usualmente denotamos a Π como $\Lambda[t]$ y sus elementos los llamaremos **polinomios en la indeterminada** t **con coeficientes en el anillo** Λ. Los elementos de Λ los llamaremos **constantes**. Los elementos de Λ se llaman **coeficientes del polinomio** φ, λ_n **coeficiente inicial** y λ_0 **término constante**. El **grado**, $gr(\varphi)$, de un elemento distinto de cero $\varphi \in \Lambda[t]$ es el mayor entero n tal que $\varphi(n) \neq 0$.

Sea Λ un anillo conmutativo. Si $\Lambda[t]$ es un anillo de polinomios del anillo Λ, podemos considerar el anillo de polinomios en la indeterminada t' del anillo de $\Lambda[t]$, es decir, $(\Lambda[t])[t']$, el cual se puede probar que es isomorfo a $(\Lambda[t'])[t]$. Usando esta identificación lo denotaremos simplemente con $\Lambda[t, t']$ y diremos que es el anillo de polinomios en las indeterminadas t y t' con coeficientes en Λ. Generalizando esto podemos definir el anillo de polinomios $\Lambda[t_1,...,t_s]$ en las indeterminadas $t_1,...,t_s$ con coeficientes en Λ.

Consideremos $\Lambda'[t]$ un anillo de polinomios de un subanillo Λ' de un anillo conmutativo Λ y $a \in \Lambda$. Por la propiedad universal de los anillos de polinomios aplicada como en el siguiente diagrama

$$\begin{array}{ccc} \Lambda' & \xrightarrow{\ i\ } & \Lambda'[t] \\ & \iota \searrow & \downarrow_{E_a} \\ & & \Lambda \end{array}$$

existe un homomorfismo

$$E_a : \Lambda'[t] \longrightarrow \Lambda$$

dado por

$$\begin{array}{rcl} \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 & \longmapsto & E_a(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) \\ & = & \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0 \end{array}$$

tal que para $b \in \Lambda'$, $E_a(b) = b$ y $E_a(t) = a$ llamado **homomorfismo de evaluación o sustitución**. Resulta que a cada polinomio $f = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$ le asociamos el elemento de un anillo $E_a(f) = E_a(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0$. Ésto es válido para anillos conmutativos y no necesariamente para no conmutativos. $E_a(f)$ significa

evaluar el polinomio f en $t = a$. La asignación $a \mapsto E_a(f)$ determina una función $f^{@} : \Lambda \longrightarrow \Lambda$ tal que $f^{@}a = E_a(f)$, es decir: si

$$f = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$$

entonces

$$f^{@}a = E_a(f) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0.$$

Cualquier función de Λ en Λ que pueda escribirse como una función del tipo $f^{@}$ se llama **función polinomial**.

Como observamos, cada polinomio $f \in \Lambda'[t]$ determina una función de Λ en Λ. Formalmente, podríamos resumir que la asignación $f \mapsto f^{@}$ determina un homomorfismo de anillos $\Phi : \Lambda'[t] \to \Lambda^{\Lambda}$ (Problema 3.16), (el cual no siempre es inyectivo, a menos que Λ' sea dominio entero infinito).

Los elementos de $\Lambda[t]$ los denotaremos con letras como f. El uso tradicional de escribirlos como $f(t)$ sólo indicará que la indeterminada es t. Esta notación tradicional hace aparentar a f como si fuera una función con variable t.

Si Δ es un dominio entero, se estudió en un curso de Álgebra Superior que existe el algoritmo de la división para polinomios sobre Δ. Recordemos que un elemento $a \in \Delta$ es un **cero** o **raíz** del polinomio f si $f^{@}(a) = 0$.

Recuerde (2.4) que si S es un subconjunto de un anillo Λ, la intersección de todos los subanillos de Λ que contienen a S se llama **subanillo de Λ generado por** S. De manera similar, si S un subconjunto de un anillo Λ, la intersección de todos los ideales de Λ que contienen a S es un ideal de Λ (Problema 3.13) y se llama **ideal de Λ generado por** S denotado $\langle S \rangle$. Los elementos de S se llaman **generadores** del ideal $\langle S \rangle$. Si S consiste de elementos $t_1,...,t_n$ denotaremos el ideal $\langle S \rangle$ con $\langle t_1, ..., t_n \rangle$ y diremos que es **finitamente generado**. Si $\langle S \rangle$ está generado por un solo elemento t diremos que $\langle t \rangle$ es un **ideal principal**. Un dominio entero en el cual todo ideal es principal lo llamaremos **dominio de ideales principales.**

Observe que el ideal $\langle t_1, ..., t_n \rangle$, al contener los elementos $t_1,...,t_n$ implica que debe contener a todos los elementos ("combinaciones lineales") de la forma $\lambda_1 t_1 + \cdots + \lambda_n t_n$ donde $\lambda_i \in \Lambda$. Los elementos $t_1,...,t_n$ constituyen una "base" del ideal. Se tiene el siguiente resultado: si K es un campo, el anillo

de polinomios $K[t]$ es un dominio de ideales principales. También, $\mathbb{Z}$ es un dominio de ideales principales (Problema 3.10). Observe también que este concepto de generadores difiere del definido en Álgebra Lineal para espacios vectoriales.

Sea Λ un anillo. Diremos que un ideal m es **máximo** si los únicos ideales que lo contienen son m y Λ. Es decir, m es un ideal máximo de Λ, si para cualquier ideal n de Λ tal que $m \subset n \subset \Lambda$ se tiene que $n = m$ o $n = \Lambda$. Diremos que un ideal p es **primo** si para cualesquiera elementos x,$y \in \Lambda$, tales que si $xy \in p$ entonces $x \in p$ ó $y \in p$. Es fácil comprobar que si Λ es un anillo conmutativo con uno entonces Λ/m es un campo si, y sólo si, m es un ideal máximo. Además, p es un ideal primo si, y sólo si Λ/p es dominio entero (Problema 3.12).

Como un ejemplo de lo anterior, considere el caso en que $\Lambda' = \mathbb{Q}$, luego $\Lambda'[t] = \mathbb{Q}[t]$ es el anillo de polinomios de un subanillo $\Lambda' = \mathbb{Q}$ de un anillo $\Lambda = \mathbb{C}$ e $i \in \Lambda = \mathbb{C}$. Por la propiedad universal de los anillos de polinomios aplicada como en el siguiente diagrama

$$\begin{array}{ccc} \Lambda' = \mathbb{Q} & \xrightarrow{f} & \Lambda'[t] = \mathbb{Q}[t] \\ & {\scriptstyle \iota} \searrow & \downarrow_{E_i} \\ & & \Lambda = \mathbb{C} \end{array}$$

existe un homomorfismo

$$E_i : \Lambda'[t] = \mathbb{Q}[t] \longrightarrow \Lambda = \mathbb{C}$$

dado por

$$\begin{array}{rcl} \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 & \longmapsto & E_i(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) \\ & = & \lambda_n i^n + \cdots + \lambda_2 i^2 + \lambda_1 i^1 + \lambda_0 \end{array}$$

tal que para $a \in \Lambda' = \mathbb{Q}$, $E_i(t) = i$ y $E_i(a) = a$. Denotamos $E_i(\mathbb{Q}[t])$ con $\mathbb{Q}[i]$ el cual consta de números complejos de la forma $a + bi$ con a,$b \in \mathbb{Q}$. Sabemos que el núcleo de E_i es el ideal de $\mathbb{Q}[t]$ generado por $t^2 + 1$ y por 2.11 considerando el siguiente diagrama

$$\begin{array}{ccccc} \ker E_i & \rightarrowtail & \mathbb{Q}[t] & \twoheadrightarrow & \mathbb{Q}[t]/\ker E_i \\ & & & \searrow & \downarrow \cong \\ & & & & E_i(\mathbb{Q}[t]) = \mathbb{Q}[i] \end{array}$$

que $\mathbb{Q}[t]/\ker E_i \cong E_i(\mathbb{Q}[t]) = \mathbb{Q}[i]$. Como $\ker E_i$ es un ideal máximo, $\mathbb{Q}[i]$ es un subcampo de $\mathbb{C}$ el cual denotaremos $\mathbb{Q}(i)$.

A continuación, veamos que todo dominio entero puede verse contenido en un campo que llamaremos campo de cocientes. Para que la ecuación $mx = n$, con m,$n \in \mathbb{Z}$, tenga solución nos vemos forzados a considerar el campo $\mathbb{Q}$ de números racionales.

3.4 Definición. Sea Δ un dominio entero conmutativo no trivial. Un **campo de cocientes de** Δ es una pareja (K, f) donde K es un campo y $f : \Delta \longrightarrow K$ es un monomorfismo de anillos tal que para cualquier monomorfismo $g : \Delta \longrightarrow \Delta'$ con Δ' un anillo con división, existe un homomorfismo de anillos único $h : K \longrightarrow \Delta'$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \Delta & \xrightarrow{f} & K \\ & {\scriptstyle g}\searrow & \downarrow{\scriptstyle h} \\ & & \Delta' \end{array}$$

3.5 Teorema. Sea (K, f) un campo de cocientes de Δ. Entonces, $f(\Delta)$ genera a K. Además, si (K', f') es otro campo de cocientes de Δ, entonces existe un isomorfismo único $k : K \longrightarrow K'$ tal que $k \circ f = f'$.

Demostración. La demostración es análoga a las de [Ll3, III.3] y la dejamos como ejercicio para el lector (Problema 3.3).♦

Para probar la existencia de un campo de cocientes, imitemos la construcción de los números racionales a partir de los números enteros pero para un dominio entero.

Consideremos el conjunto Δ^* de los elementos distintos de cero de Δ y denotemos con $\Xi = \Delta \times \Delta^*$. Definamos en Ξ una relación mediante $(a_1, b_1) \sim (a_2, b_2)$ sí y sólo si $a_1 b_2 = a_2 b_1$ en Δ. Es fácil verificar que $\sim$ es una relación de equivalencia (Problema 3.4).

Sea $K = \Xi/\sim$ y denotemos con a/b la clase de equivalencia de (a, b). Definamos la suma y multiplicación de clases como en los números racionales, es

decir, $(a_1/b_1)+(a_2/b_2) = (a_1b_2+a_2b_1)/b_1b_2$ y $(a_1/b_1)\cdot(a_2/b_2) = (a_1a_2)/(b_1b_2)$. Es fácil comprobar que estas operaciones están bien definidas y que hacen de K un anillo conmutativo con uno, cuyo elemento cero es la clase de equivalencia de la forma $0/b$ y su uno la clase de la forma a/b con $a = b$. (Problema 3.5).

Como el inverso de un elemento diferente de cero a/b es b/a pues $a \neq 0$, $(a/b)\cdot(b/a) = 1$ luego, K es un campo. Veamos que $(K, f : \Delta \longrightarrow K)$ es un campo de cocientes de Δ. Definamos $f : \Delta \longrightarrow K$ mediante $f(a) = a/1$. Es inmediato comprobar que f es un monomorfismo. Consideremos cualquier monomorfismo $g : \Delta \longrightarrow \Delta'$ con Δ' un anillo con división. Como $g(b) \neq 0$ si $b \neq 0$ en Δ, podemos definir $h' : \Xi \longrightarrow \Delta'$ mediante $h'(a, b) = g(a)/g(b)$. Es fácil comprobar que h' está bien definida (Problema 3.6).

Así, $h'(a, b)$ depende solamente de la clase de equivalencia a/b, por lo tanto podemos definir una función $h : K \longrightarrow \Delta'$. Es fácil comprobar que h es un homomorfismo tal que $h \circ f = g$ (Problema 3.6). Veamos que h es única: sea $k : K \longrightarrow \Delta'$ cualquier otro homomorfismo tal que $k \circ f = g$. Sea $a/b \in K$. Luego $a/b = f(a)f(b)^{-1}$ y por lo tanto $k(a/b) = g(a)g(b)^{-1} = h(a/b)$. Así, $k = h$. Hemos probado el siguiente

3.6 Teorema. Para cualquier dominio entero conmutativo no trivial Δ existe un campo de cocientes.♦

3.7 Ejemplos. Si Δ es el dominio entero conmutativo no trivial $\mathbb{Z}$, entonces su campo de cocientes es $\mathbb{Q}$. Si consideramos el campo K, el anillo de polinomios $K[t]$ de K es un dominio entero y no un campo. Sin embargo por el teorema 3.6 podemos construir su campo de cocientes $K(t)$, donde cada elemento puede escribirse de la forma f/g donde f y g son polinomios en $K[t]$ con $g \neq 0$. Análogamente, para $K[t_1,...,t_s]$ podemos construir $K(t_1,...,t_s)$ el cual se llama **campo de cocientes o de funciones racionales con** s **indeterminadas sobre** K.

3.8 Teorema. Sea K un campo de característica 0. El subcampo de K generado por el uno de K es isomorfo a $\mathbb{Q}$.

Demostración. Sea $x = m/n \in \mathbb{Q}$ con m un entero y n un entero positivo. Si $x \neq 0$ podemos considerar m y n con solamente ± 1 como divisor común. Si $x = 0$, podemos tomar $m = 0$ y $n = 1$. Así, la expresión para x es única. Definamos $f : \mathbb{Q} \longrightarrow K$ mediante $f(x) = m1/n1$, para toda $x =$

m/n. Es fácil ver que f es un homomorfismo (Problema 3.11). Consideremos el ideal $\ker f$ de $\mathbb{Q}$. Como $f(1) = 1$, $\ker f \neq \mathbb{Q}$. Pero como un anillo con división no puede tener ideales propios no triviales (1.9), $\ker f = 0$. Luego, f es monomorfismo. Como $im\, f$ es un subcampo de K generado por el 1 hemos terminado.♦

Por la proposición anterior y 2.16 (ii) todo campo contiene un subcampo isomorfo a $\mathbb{Z}_p$ para algún primo p o un subcampo isomorfo a $\mathbb{Q}$. Llamaremos a $\mathbb{Z}_p$ y a $\mathbb{Q}$ **campos primos**. Ellos serán fundamentales para nuestro estudio posterior de campos.

Existe una manera, que no demostraremos, de probar cuando un polinomio

$$f(t) = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 \in \mathbb{Q}[t]$$

es irreducible llamado **Criterio de Einsenstein**. Dice que si p es un número primo y $f \in \mathbb{Z}[t]$, entonces f es irreducible sobre $\mathbb{Q}$ si λ_n no es congruente con 0 módulo p, $\lambda_i \not\equiv 0 \ (mod\ p)$ para $i < n$, y λ_0 no es congruente con 0 módulo p^2.

Problemas.

3.1 Pruebe que si (Π, f, t) es un anillo de polinomios de Λ, entonces el conjunto $f(\Lambda) \cup \{t\}$ genera Π. También, pruebe que si (Π', f', t') es otro anillo de polinomios de Λ, entonces existe un isomorfismo único $k : \Pi \longrightarrow \Pi'$ tal que $k(t) = t'$ y $k \circ f = f'$.

3.2 (i) Sea $\mathbb{Z}^+ \cup \{0\}$ el conjunto de enteros no negativos y Λ un anillo con uno. Compruebe que el conjunto $\Pi = \{\varphi : \mathbb{Z}^+ \cup \{0\} \longrightarrow \Lambda \mid \varphi(n) = 0$ para casi toda $n \in \mathbb{Z}^+ \cup \{0\}$ posee una estructura de anillo definiendo dos operaciones binarias mediante

$$\begin{aligned} n &\mapsto (\varphi + \xi)(n) = \varphi(n) + \xi(n) \\ n &\mapsto (\varphi\xi)(n) = \sum_{j=0}^{n} \varphi(j)\xi(n-j). \end{aligned}$$

(ii) Sea $f_x \in \Pi$ y considere la asignación dada por $x \mapsto f_x$ la cual define una función $f : \Lambda \to \Pi$. Compruebe que f es un monomorfismo y que $f(1)$ es la identidad de Π.

(iii) En el Teorema 3.2 compruebe que: h es homomorfismo, $h(t) = y$, $h \circ f = g$ y que h es única. Establezca que cualquier elemento de Π puede escribirse de manera única como $\varphi = \lambda_0 + \lambda_1 t^1 + \lambda_2 t^2 + \cdots + \lambda_n t^n$, donde $\lambda_i \in \Lambda$ y $\lambda_i = \varphi(n)$ para $i = 0, \ldots, n$.

3.3 Pruebe que si (K, f) es un campo de cocientes de Δ, entonces, $f(\Delta)$ genera K. También, pruebe que si (K', f') es otro campo de cocientes de Δ, entonces existe un isomorfismo único $k : K \longrightarrow K'$ tal que $k \circ f = f'$.

3.4 Considere el conjunto Δ^* de los elementos distintos de cero de Δ y denote con $\Xi = \Delta \times \Delta^*$. Defina en Ξ una relación mediante $(a_1, b_1) \sim (a_2, b_2)$ sí y sólo si $a_1 b_2 = a_2 b_1$ en Δ. Compruebe que $\sim$ es una relación de equivalencia.

3.5 Sea $K = \Xi/\sim$ y denote con a/b la clase de equivalencia de (a, b). Defina la suma y multiplicación de clases como en los números racionales, es decir, $(a_1/b_1)+(a_2/b_2) = (a_1 b_2 + a_2 b_1)/b_1 b_2$ y $(a_1/b_1)\cdot(a_2/b_2) = (a_1 a_2)/(b_1 b_2)$. Compruebe que estas operaciones están bien definidas y que hacen de K un anillo conmutativo con uno cuyo elemento cero es la clase de equivalencia de la forma $0/b$ y con uno la clase de la forma a/b con $a = b$.

3.6 (i) Defina $h' : \Xi \longrightarrow \Delta'$ mediante $h'(a, b) = g(a)/g(b)$. Compruebe que h' está bien definida. **(ii)** Por la parte (i) $h'(a, b)$ depende solamente de la clase de equivalencia a/b, por lo tanto defina una función $h : K \longrightarrow \Delta'$. Pruebe que h es un homomorfismo tal que $h \circ f = g$.

3.7 Pruebe que si Δ' es un anillo con división que contiene a un subdominio Δ entonces la función inclusión $\iota : \Delta \longrightarrow \Delta'$ se extiende a un monomorfismo único $h : K \longrightarrow \Delta'$ donde K es el campo de cocientes.

3.8 Pruebe que el campo de cocientes de un campo cualquiera K es K mismo.

3.9 Pruebe que en un anillo Λ el ideal $\langle 0 \rangle = 0$ donde $\langle 0 \rangle$ denota el ideal generado por el elemento de identidad aditivo 0. También, pruebe que si Λ tiene uno, entonces $\langle 1 \rangle = \Lambda$.

3.10 Pruebe que (i) $\mathbb{Z}$ es un dominio de ideales principales. (ii) Demuestre que si K es un campo, el anillo de polinimios $K[t]$ es un dominio de ideales

principales. (iii) Pruebe que si Δ es un dominio entero finito, entonces $\Delta[t]$ es un dominio entero.

3.11 Pruebe que, en el Teorema 3.8, f es un homomorfismo.

3.12 Sea Λ es un anillo conmutativo con uno. Pruebe que Λ/m es un campo si, y sólo si, m es un ideal máximo y que p es un ideal primo si, y sólo si Λ/p es un dominio entero.

3.13 Pruebe que si S un subconjunto de un anillo Λ, la intersección de todos los ideales de Λ que contienen a S es un ideal de Λ.

3.14 Sea K un campo. Pruebe que un polinomio en $K[t]$ es irreducible si, y sólo si, el ideal generado por él es máximo.

3.15 Considere $\Lambda'[t]$ un anillo de polinomios de un campo Λ', Λ' un subanillo de un anillo Λ y $a \in \Lambda$. Pruebe que la función

$$E_a : \Lambda'[t] \longrightarrow \Lambda$$

dada por

$$\begin{aligned} \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 &\longmapsto E_a(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) \\ &= \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + a_0 \end{aligned}$$

es un homomorfismo tal que para $b \in \Lambda'$, $E_a(b) = b$ y $E_a(t) = a$.

3.16 Pruebe que la asignación $f \mapsto f^{@}$ determina un homomorfismo de anillos $\Phi : \Lambda'[t] \to \Lambda^{\Lambda}$.

3.17 Pruebe el algoritmo de la división para polinomios, es decir, pruebe que si $f(t) = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$ y $g(t) = \mu_m t^m + \cdots + \mu_2 t^2 + \mu_1 t^1 + \mu_0$ son polinomios en $K[t]$ con $\lambda_n, \mu_m \neq 0$ en K y $m > 0$ entonces existen polinomios únicos $q(t)$ y $r(t)$ en $K[t]$ tal que $f(t) = g(t)q(t) + r(t)$, con $r(t) = 0$ o bien el grado de $r(t)$ menor que el grado de $g(t)$.

3.18 Pruebe que (i) $(t - a)$ es un factor de un polinomio $f(t) \in K[t]$ si, y sólo si, a es una raíz de $f(t)$, $a \in K$.

(ii) Pruebe que cualquier polinomio no trivial de grado m en $K[t]$ tiene a lo más m raíces en K.

3.19 Recuerde que un polinomio es irreducible si no puede expresarse como producto de dos polinomios de menor grado. Pruebe que todo polinomio no trivial en $K[t]$ puede factorizarse en forma única como producto de polinomios irreducibles salvo el orden y constantes de los mismos.

3.20 Para un primo p considere el polinomio

$$\Phi_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

Pruebe que es irreducible en $\mathbb{Q}[t]$ y por tanto en $\mathbb{Z}[t]$. Sugerencia: pruebe que $\Phi_p(t)(t-1) \equiv (t-1)^p \ (mod\ p)$ y que $\Phi_p(t) \equiv (t-1)^{p-1}$ y utilice el Criterio de Einsenstein.

3.21 Los **polinomios ciclotómicos** $\Phi_n(t) \in \mathbb{Z}[t]$, $n \geq 1$ están definidos mediante

$$t^n - 1 = \Pi_{d|n} \Phi_d(t).$$

Escriba los polinomios ciclotómicos para $n \leq 20$ y establezca la fórmula recursiva

$$\Phi_n(t) = \frac{t^n - 1}{\Pi_{d|n, d<n} \Phi_d(t)}$$

para calcular $\Phi_n(t)$ a partir de $\Phi_i(t)$ para $i < n$. Las raíces del polinomio $t^n - 1$ se llaman **raíces n-ésimas de la unidad**. Los polinomios ciclotómicos aparecen en la Teoría Matemática de la Música, véase [Am] y artículos en [Ll-M-N].

Capítulo II

Teoría de Campos y Teoría de Galois

II.1 Extensiones de Campos

Los objetos de estudio de la Teoría de Campos son precisamente éstos, sin embargo dicha teoría se concentra principalmente en el estudio de las extensiones de ellos.

Los campos que usaremos son: el de los números racionales denotado con $\mathbb{Q}$, el de los números reales denotado con $\mathbb{R}$, el de los números complejos denotado con $\mathbb{C}$, el de los enteros módulo un primo p denotado $\mathbb{Z}_p$. Recuerde también el campo de cocientes de un dominio entero del ejemplo I.3.7 $K(t)$ y $K(t_1,...,t_s)$.

Recuerde que todo homomorfismo de campos es inyectivo.

1.1 Definición. Consideremos dos campos K' y K. Diremos que K es una **extensión** de K' si la siguiente sucesión de homomorfismos es exacta:

$$0 \longrightarrow K' \xrightarrow{\iota} K$$

es decir, ι es un monomorfismo e identificamos K' con $\iota(K')$ dentro de K cuando esto sea posible. Decimos que K' es el **campo base** de la extensión. Vemos entonces a $K' \cong \iota(K')$ como un subcampo de K. Denotamos la

extensión K **de** K' o **extensión de** K' **en** K con $K' \rightarrowtail K$ o bien $K' \leq K$, o bien $K : K'$, o bien $K' < K$ cuando $K' \neq K$, o también K/K', o

$$\begin{array}{c} K \\ | \\ K' \end{array}$$

También escribiremos simplemente **extensión** por abuso cuando esté implícito el contexto correspondiente.

1.2 Ejemplos.

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{R} \\ 0 & \longrightarrow & \mathbb{R} & \longrightarrow & \mathbb{C} \\ 0 & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{C} \end{array}$$

son extensiones. Con las demás notaciones se verían así:

$$\begin{array}{ccc} \mathbb{Q} & \rightarrowtail & \mathbb{R} \\ \mathbb{R} & \rightarrowtail & \mathbb{C} \\ \mathbb{Q} & \rightarrowtail & \mathbb{C} \end{array}$$

$$\begin{array}{ccc} \mathbb{R} & : & \mathbb{Q} \\ \mathbb{C} & : & \mathbb{R} \\ \mathbb{C} & : & \mathbb{Q} \end{array}$$

$$\begin{array}{c} \mathbb{R}/\mathbb{Q} \\ \mathbb{C}/\mathbb{R} \\ \mathbb{C}/\mathbb{Q} \end{array}$$

$$\begin{array}{c} \mathbb{R} \\ | \\ \mathbb{Q} \end{array}$$

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array}$$

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{Q} \end{array}$$

Este tipo de "torres de campos" son uno de los principales temas de estudio de la Teoría de Campos. Preferiremos la notación $K' \rightarrowtail K$ para denotar una extensión imitando una torre rotada 90 grados a la derecha, es decir, una torre o "condominio horizontal" de campos ya que esto facilita visualizar específicamente los campos y su respectiva inclusión en otros.

1.3 Definiciones. (i) Si $K' \rightarrowtail K$ y $K \rightarrowtail K''$ son extensiones, diremos que $K' \rightarrowtail K$ es una **subextensión de** $K' \rightarrowtail K''$ y se acostumbra escribir $(K' \rightarrowtail K) \leq (K' \rightarrowtail K'')$.

(ii) Diremos que dos extensiones

$$K' \overset{\iota}{\rightarrowtail} K$$

y

$$L' \overset{\iota'}{\rightarrowtail} L$$

son **isomorfas** si existen homomorfismos de campos $\alpha : K' \longrightarrow L'$ y $\beta : K \longrightarrow L$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} K' & \overset{\iota}{\rightarrowtail} & K \\ \downarrow^{\alpha} & & \downarrow^{\beta} \\ L' & \overset{\iota'}{\rightarrowtail} & L \end{array}$$

Podemos identificar $K' \cong \iota(K')$, $L' \cong \iota'(L')$ y $\beta \mid_{K'} = \alpha$.

Ahora introduciremos el Álgebra Lineal en el estudio de las extensiones de campos. Considere una extensión $K' \rightarrowtail K$. Como K' puede verse dentro de K, podemos considerar el espacio vectorial K sobre K', denotar $\dim_{K'} K$ como $[K' \rightarrowtail K]$ y llamarla **grado de** K **sobre** K', el cual puede ser infinito.

Si el grado de K sobre K' es finito (infinito), entonces diremos que la extensión $K' \rightarrowtail K$ es **finita** (**infinita**). El grado de una extensión es el invariante más importante de una extensión.

1.4 Teorema. Si $K' \rightarrowtail K$ y $K \rightarrowtail K''$ son extensiones finitas entonces $K' \rightarrowtail K''$ es una extensión finita y

$$[K' \rightarrowtail K][K \rightarrowtail K''] = [K' \rightarrowtail K''].$$

Demostración. Consideremos $\{u_i\}_{i=1}^n$ y $\{v_j\}_{j=1}^m$ bases para las extensiones $K' \rightarrowtail K$ y $K \rightarrowtail K''$, es decir para K como espacio vectorial sobre K' y para K'' como espacio vectorial sobre K. Veamos que los nm elementos $\{u_i v_j\}$ forman una base para $0 \longrightarrow K' \longrightarrow K''$, es decir, una base para K'' sobre K'.

Sea w cualquier elemento de K''. Entonces $w = \sum_{j=1}^m \mu_j v_j$ con $\mu_j \in K$. Pero como $\mu_j \in K$ y K es un espacio sobre K', $\mu_j = \sum_{i=1}^n \lambda_{ij} u_i$ con $\lambda_{ij} \in K'$. Sustituyendo, $w = \sum_{j=1}^m (\sum_{i=1}^n \lambda_{ij} u_i) v_j = \sum_{i,j} \lambda_{ij}(u_i v_j)$. Luego, los elementos $u_i v_j$ generan el espacio K'' sobre K'.

Consideremos una combinación lineal $\sum_{i,j} \eta_{ij}(u_i v_j) = 0$ con $\eta_{ij} \in K'$. Entonces, $\sum_{j=1}^m (\sum_{i=1}^n \eta_{ij} u_i) v_j = 0$ con $\sum_{i=1}^n \eta_{ij} u_i \in K$. Como $\{v_j\}_{j=1}^m$ es base del espacio K'' sobre K, $\sum_{i=1}^n \eta_{ij} u_i = 0$ para toda j. Como a la vez, $\{u_i\}_{i=1}^n$ es una base para K sobre K', $\sum_{i=1}^n \eta_{ij} u_i = 0$ implica que $\eta_{ij} = 0$ para toda i,j. Luego, los elementos $\{u_i v_j\}$ son linealmente independientes. Así, $\{u_i v_j\}$ es una base para K'' sobre K'.♦

En esta situación, decimos que K es un **campo intermedio de** K' **y** K''. Nótese que si $K' \rightarrowtail K''$ es una extensión infinita, también lo serán $K' \rightarrowtail K$ y $K \rightarrowtail K''$. También observe que si $K' \rightarrowtail K''$ es una extensión finita, como corolario se tiene que la dimensión de K sobre K' o la de K'' sobre K divide a la dimensión de K'' sobre K', es decir $[K' \rightarrowtail K] \mid [K' \rightarrowtail K'']$ o $[K \rightarrowtail K''] \mid [K \rightarrowtail K'']$. Dicho de otra manera, el grado de K sobre K' divide al grado de K''sobre K'o bien que el grado de K'' sobre K divide al grado de K'' sobre K'.

1.5 Corolario. Consideremos una familia de campos $\{K_i\}$ para $i = 1,..., s$ tal que cada K_{i+1} es una extensión finita de K_i. Entonces K_s es una extensión finita de K_1 y

$$[K_1 \rightarrowtail K_2][K_2 \rightarrowtail K_3] \cdots [K_{s-1} \rightarrowtail K_s] = [K_1 \rightarrowtail K_s].$$

Demostración. Problema 1.1.♦

1.6 Ejemplos. Considere la extensión $\mathbb{R} \rightarrowtail \mathbb{C}$ donde $\mathbb{C} = \{a1+bi \mid a,b \in \mathbb{R}\}$. Entonces 1 e i generan a $\mathbb{C}$ como espacio vectorial sobre $\mathbb{R}$. Como $i \notin \mathbb{R}$, $\{1, i\}$ es linealmente independiente sobre $\mathbb{C}$. Luego, $\{1, i\}$ es una base para $\mathbb{C}$ sobre $\mathbb{R}$ y por lo tanto $\dim_{\mathbb{R}} \mathbb{C} = [\mathbb{R} \rightarrowtail \mathbb{C}] = 2$. Sea $\mathbb{R}(i)$ el subcampo que contiene a los elementos de la forma $x + iy$, con x,$y \in \mathbb{R}$. Luego, $\mathbb{C} = \mathbb{R}(i)$, (Problema 1.2).

1.7 Ejemplo. Sea $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Al definir así $\mathbb{Q}(\sqrt{2})$, cualquier elemento es de la forma $a + b\sqrt{2}$ y por lo tanto $\{1, \sqrt{2}\}$ genera el espacio vectorial $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Veamos que es linealmente independiente: supongamos que es linealmente dependiente, es decir, que existe una combinación lineal de ellos $c+d\sqrt{2} = 0$ con c,$d \in \mathbb{Q}$ no ambos cero. Si $d = 0$, entonces $c1 = 0$ lo cual implica que ambos c,d serían cero contra lo supuesto. También, si $c = 0$, entonces $d\sqrt{2} = 0$ lo cual implica que ambos c,d sean cero contra lo supuesto. La única posibilidad es que ambos c y d sean distintos de cero y por lo tanto se tendría que $d\sqrt{2} = -c1$ y así $\sqrt{2} = -\frac{c}{d} \in \mathbb{Q}$ lo cual es imposible. Por lo tanto $\{1, \sqrt{2}\}$ es linealmente independiente y constituye una base para el espacio vectorial $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Luego $[\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})] = 2$.

Recordemos de (I.3) el homomorfismo de evaluación o sustitución adaptado a campos: consideremos $K'[t]$ el anillo de polinomios de un subcampo K' de un campo K'' y $a \in K''$. El homomorfismo

$$E_a : K'[t] \longrightarrow K''$$

dado por

$$\begin{aligned} \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0 &\longmapsto E_a(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) \\ &= \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0 \end{aligned}$$

tal que para $b \in K'$, $E_a(b) = b$ y $E_a(t) = a$ se llama **homomorfismo de evaluación o sustitución**. Es decir, a cada polinomio $f = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$ le asociamos el elemento del campo $E_a(f) = E_a(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0$. $E_a(f)$ significa evaluar el polinomio f en $t = a$. La asignación $a \mapsto E_a(f)$ determina una función $f^{@} : K'' \longrightarrow K''$ tal que $f^{@}a = E_a(f)$, es decir: si

$$f = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$$

entonces

$$f^{@}a = E_a(f) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0.$$

Cualquier función de K'' en K'' que pueda escribirse como una función del tipo $f^{@}$ se llama **función polinomial**.

Como observamos, cada polinomio $f \in K'[t]$ determina una función de K'' en K''. Formalmente, decimos que la asignación $f \mapsto f^{@}$ determina un homomorfismo de anillos $\Phi : K'[t] \to K''^{K''}$, (el cual no siempre es inyectivo, a menos que K' sea dominio entero infinito). Los elementos de $K'[t]$ los denotaremos con letras como f, g, h. El uso tradicional de escribirlos como $f(t)$ sólo indicará que la indeterminada es t. Esta notación tradicional hace aparentar a f como si fuera una función con variable t y no debe causar confusión alguna. Como $K'[t]$ es un dominio entero, existe un algoritmo de la división para polinomios sobre K' (Problema I.3.17).

Nos interesa considerar campos que estén entre K' y K''. Considere el subcampo de K'' generado por un subconjunto X de K'' (I.2.4 y P.I.2.6 ii).

1.8 Definición. Sea X un subconjunto de K'' y $K' \rightarrowtail K''$ una extensión. El subcampo de K'' generado por $K' \cup X$ denotado con $K'(X)$, se llama **subcampo obtenido por la adjunción de X a K'**.

Obsérvese que el subcampo $K'(X)$ puede ser mucho más grande que $K' \cup X$. $K'(\{x, y, z\})$ se denota $K'(x, y, z)$. Consideremos la extensión $K' \rightarrowtail K''$con $X = \{a_1,..., a_j \mid a_i \in K''$ para $i = 1,..., j\}$. Denotamos con $K'(a_1,..., a_j)$ el mínimo subcampo de K'' que contiene a K' y a los elementos $a_1,..., a_j$.

La extensión $K' \rightarrowtail K'(a_1,..., a_j)$ se dice que está **generada** por $a_1,..., a_j$ y también decimos que es una extensión **finitamente generada** de K'. La extensión $K' \rightarrowtail K'(a)$ se llama **extensión simple** de K' por a. El reordenar las $a_i \in K''$ para $i = 1,..., j$, no cambia $K'(a_1,..., a_j)$ y se tiene que $K'(a_1,..., a_n) = K'(a_1,..., a_{n-1})(a_n)$.

1.9 Ejemplo. Por 1.7 sabemos que $[\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})] = 2$. Adjuntemos $\sqrt{3}$ a $\mathbb{Q}(\sqrt{2})$, es decir, consideremos $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Entonces sus elementos son de la forma $a = c + d\sqrt{3}$ con c,$d \in \mathbb{Q}(\sqrt{2})$. Luego, 1,$\sqrt{3}$ generan $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Es fácil ver que son linealmente independientes sobre $\mathbb{Q}(\sqrt{2})$. Por lo tanto son una base de $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$. Así, $[\mathbb{Q}(\sqrt{2}) \rightarrowtail (\mathbb{Q}(\sqrt{2}))(\sqrt{3})] = 2$.

Por 1.4, se tiene que $[\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})(\sqrt{3})] = 4$. Por la demostración de 1.4, $\{\sqrt{6},\sqrt{3},\sqrt{2},1\}$ es base de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ sobre $\mathbb{Q}$.

1.10 Ejemplo. Como vimos en 1.7 $[\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})] = 2$. Sabemos que $\mathbb{Q}(\sqrt{2})$ es subcampo de $\mathbb{R}$ y que $i \notin \mathbb{Q}(\sqrt{2})$ pues $i \notin \mathbb{R}$. Como $i^2 + 1 = 0$, $\mathbb{Q}(\sqrt{2})(i) = \mathbb{Q}(\sqrt{2}, i)$ y $[\mathbb{Q}(\sqrt{2}) \rightarrowtail \mathbb{Q}(\sqrt{2}, i)] = 2$. Luego

$$[\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) \rightarrowtail \mathbb{Q}(\sqrt{2}, i)] = [\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2}, i)] = 4$$

Observe que $K'[t]$ puede verse como un espacio vectorial sobre K' donde los elementos a^n con $n \geq 0$ generan $K'[t]$ sobre K' y que $K'[t]$ no es de dimensión finita pues los polinomios pueden tener un grado muy grande y no ser combinaciones lineales de un conjunto finito de polinomios.

Podemos hacer equivalente el problema de "encontrar las soluciones" de una ecuación polinomial

$$f = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$$

al problema de encontrar las raíces o ceros de

$$f^{@}a = E_a(f) = \lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0.$$

Es decir, resolveremos el problema original traducido a un problema equivalente usando homomorfismos, ideales, cocientes, etc. Nos preguntamos si existe una extensión $K' \rightarrowtail K$ tal que $f(t) \in K'[t]$ posea una raíz en K. Veremos que todo polinomio de grado mayor o igual a 1 con coeficientes en cualquier campo K' posee una raíz en algún subcampo K de K'' que lo contenga. ¿Existirá una extensión K de K' tal que un polinomio $f(t) \in K'[t]$ tenga una raíz en K?

Consideremos la extensión $K' \rightarrowtail K''$, $a \in K''$ y t la indeterminada. Entonces el homomorfismo de evaluación $E_a : K'[t] \longrightarrow K''$ envía K' isomórficamente en sí mismo tal que para $b \in K'$, $E_a(b) = b$ y $E_a(t) = a$. Como todo polinomio f se factoriza en $K'[t]$ en polinomios irreducibles sobre K', si q denota uno de tales polinomios irreducibles, el ideal I generado por q es máximo en $K'[t]$. Luego el cociente $K'[t]/I$ es campo. Considérese

$$\varphi : K' \longrightarrow K'[t]/I$$

dada por

$$x \longmapsto x + I$$

Es fácil ver que φ envía a K' isomórficamente en sí mismo dentro de $K'[t]/I$ (Problema 1.4). Así, podemos considerar $K = K'[t]/I$ como una extensión de K'. Sea $a = t + I$, $a \in K$. Consideremos $E_a : K'[t] \longrightarrow K$. Si

$$q(t) = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0, \lambda_i \in K'$$

entonces

$$q^{@}a = E_a(q(t)) = (\lambda_n(t+I)^n + \cdots + \lambda_2(t+I)^2 + \lambda_1(t+I)^1 + \lambda_0) + I \in K.$$

Como t es un representante de la clase lateral $a = t + I$, $q(a) = (\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) + I = q(t) + I = I$ en K. Luego, a es tal que $q(a) = 0$ y, por lo tanto, $f(a) = 0$. Hemos probado el siguiente

1.11 Teorema. (Kronecker) Si $f(t)$ es un polinomio no trivial en $K'[t]$ donde K' es un campo, entonces existe una extensión K de K' y un elemento $a \in K$ tal que $f(a) = 0$.♦

1.12 Ejemplo. El polinomio $f(t) = t^2 + t + 1 \in \mathbb{Z}_2[t]$ es irreducible sobre $\mathbb{Z}_2$, (Problema 1.5). Por el Teorema 1.11 existe un campo $K = \mathbb{Z}_2(a)$ que contiene una raíz a de f. Luego, $\mathbb{Z}_2(a)$ posee los elementos de la forma

$$\begin{array}{cccc} 0+0a & 1+0a & 0+1a & 1+1a \\ \| & \| & \| & \| \\ 0 & 1 & a & 1+a \end{array}$$

lo cual nos proporciona un campo con cuatro elementos.

1.13 Ejemplo. Considere $K' = \mathbb{R}$ y $f(t) = t^2 + 1$ un polinomio irreducible en $\mathbb{R}[t]$. Luego, el ideal $I = \langle t^2 + 1 \rangle$ generado por este polinomio irreducible es máximo y por lo tanto el cociente $\mathbb{R}[t]/I$ es campo. Podemos ver a $\mathbb{R}$ como un subcampo de $\mathbb{R}[t]/I$. Sea $a = t + I$. Entonces $a^2 + 1 = (t+I)^2 + (1+I) = (t^2+1) + I = 0_{\mathbb{R}[t]/I}$. Así, a es una raíz de $t^2 + 1$.

Nos interesarán las extensiones $K' \rightarrowtail K$ para las cuales cualquier elemento $a \in K$ sea raíz de una ecuación polinomial sobre K'.

1.14 Definición. Sea $K' \rightarrowtail K$ una extensión. Diremos que un elemento $a \in K$ es **algebraico sobre** K' si existe un polinomio no nulo $f \in K'[t]$

tal que a es raíz de f. Si a no es raíz de algún polinomio no nulo $f \in K'[t]$ diremos que es **trascendente sobre** K'. Diremos que K es una **extensión algebraica de** K' si todo elemento de K es algebraico sobre K'. Diremos que K es una **extensión trascendente de** K' si al menos un elemento de K es trascendente sobre K'.

Se acostumbra llamar **número algebraico** a un elemento de $\mathbb{C}$ el cual es algebraico sobre $\mathbb{Q}$ y **número trascendente** si es trascendente sobre $\mathbb{Q}$.

1.15 Ejemplos. Considere la extensión $\mathbb{Q} \rightarrowtail \mathbb{R}$. $\sqrt{2}$ es un elemento algebraico sobre $\mathbb{Q}$ pues es raíz del polinomio $t^2 - 2 \in \mathbb{Q}[t]$. También, si consideramos la extensión $\mathbb{Q} \rightarrowtail \mathbb{C}$, $\sqrt{2}$ e $i = \sqrt{-1}$ son elementos algebraicos sobre $\mathbb{Q}$ pues son raíces de los polinomios $t^2-2 \in \mathbb{Q}[t]$ y $t^2+1 \in \mathbb{Q}[t]$ respectivamente. Cualquier elemento $a \in K'$ es raíz del polinomio $t-a \in K'[t]$ y por lo tanto es algebraico sobre K'. Se puede probar que $\pi, e \in \mathbb{R}$ son trascendentes sobre $\mathbb{Q}$. Pero π es algebraico sobre $\mathbb{R}$ al ser raíz de $t - \pi \in \mathbb{R}[t]$. Observe que $\sqrt{2}$ también es raíz de muchos polinomios más, propónga usted algunos.

Considere la extensión $K' \rightarrowtail K''$, y $a \in K''$ algebraico sobre K'. El **polinomio mínimo para** a **sobre** K', denotado $m_{a,K'}$, es el polinomio mónico irreducible único de grado mínimo $m(t) \in K'[t]$ tal que $m(a) = 0$ el cual divide a cualquier otro polinomio que tenga a a como raíz (Problema 1.7). El grado del polinomio $m_{a,K'}$ lo llamaremos **grado de** a **sobre** K' y lo denotaremos $gr(a, K')$. A continuación veamos que si $a \in K''$ es algebraico sobre K' entonces $[K' \rightarrowtail K'(a)] = gr(a, K')$: considérese la extensión simple $K'(a)$ de K' tal que el núcleo $\ker E_a$ del homomorfismo de evaluación

$$E_a : K'[t] \longrightarrow K'(a)$$

sea no trivial. Si suponemos que a es algebraico sobre K', el núcleo de E_a es un ideal, el cual es principal (P I.3.10) generado por $m_{a,K'}$ el cual es máximo (P I.3.14) i.e. $\ker E_a = \langle m_{a,K'} \rangle$ es un ideal máximo. Luego, $K'[t]/\langle m_{a,K'} \rangle$ es un campo el cual es isomorfo a $E_a(K'[t])$ el cual es un subcampo de $K'(a)$ que contiene a a, i.e. $K'(a)$. Todo elemento de $K'[t]/\langle m_{a,K'} \rangle$ es de la forma $f(t) + I$ donde $I = \langle m_{a,K'} \rangle$ con el grado de $f(t) < gr(m_{a,K'})$. Luego, cualquier elemento de $K'[t]/\langle m_{a,K'} \rangle$ puede escribirse como combinación lineal de n clases laterales $1+I, t+I, t^2+I, ..., t^{n-1}+I$ donde $n = gr(m_{a,K'})$. Como

$t^i + I \to a^i$, vemos que los elementos $1, a, ..., a^{n-1}$ son base para $K'(a)$ sobre K'. Así, $[K' \rightarrowtail K'(a)] = gr(m_{a,K'})$. (Véase el Problema 1.8)

Si consideramos la misma extensión simple $K'(a)$ de K' tal que el núcleo $\ker E_a$ del homomorfismo de evaluación $E_a : K'[t] \longrightarrow K'(a)$ sea trivial. Entonces E_a es un monomorfismo. Luego $E_a(K'[t])$ no es un campo pero es un dominio entero y podemos considerar el campo de cocientes $K'(t)$ y se tiene un monomorfismo $K'(t) \longrightarrow K'(a)$ el cual también es suprayectivo pues a está en la imagen. (a es trascendente sobre K').

1.16 Ejemplos. Considere la extensión $\mathbb{Q} \rightarrowtail \mathbb{C}$, el polinomio $f(t) = t^2 - 2$ y el homomorfismo de evaluación $E_{\sqrt{2}} : \mathbb{Q}[t] \longrightarrow \mathbb{C}$. Entonces $E_{\sqrt{2}}(f(t)) = f(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$. Luego, $f(t) = t^2 - 2 \in \ker E_{\sqrt{2}}$. Así $[\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})] = 2 = gr(\sqrt{2}, \mathbb{Q})$, luego $m_{\sqrt{2},\mathbb{Q}}(t) = t^2 - 2$.

Considere la extensión $\mathbb{Q} \rightarrowtail \mathbb{C}$, el polinomio $f(t) = t^2 + 1$ y el homomorfismo de evaluación $E_i(f(t)) = f(i) = i^2 + 1 = 0$. Luego, $f(t) = t^2 + 1 \in \ker E_i$. Así $[\mathbb{Q} \rightarrowtail \mathbb{Q}(i)] = 2 = gr(i, \mathbb{Q})$, luego $m_{i,\mathbb{Q}}(t) = t^2 + 1$. No es trivial el obtener el polinomio mínimo en general.

1.17 Proposición. Si una extensión $K' \rightarrowtail K$ es finita, entonces es algebraica sobre K'.

Demostración. Sea $a \in K$. Veamos que a es algebraico sobre K'. El conjunto $\{a^n, a^{n-1}, \ldots, a^2, a^1, 1\}$ no es linealmente independiente, es decir, existe una combinación lineal

$$\lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0 = 0$$

con no toda $\lambda_i = 0$. Luego $f(t) = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$ es un polinomio no trivial en $K'[t]$ con $f(a) = 0$. Luego, a es algebraico sobre K'.♦

El inverso de 1.17 es falso pues hay extensiones algebraicas de grado infinito.

1.18 Teorema. Considere la extensión algebraica $K' \rightarrowtail K$. Entonces, $K = K'(a_1, ..., a_n)$ para $a_1, ..., a_n \in K$ sí, y sólo si K es una extensión finita sobre K'.

Demostración. Si $K = K'(a_1, ..., a_n)$, a_i es algebraico sobre K' y por lo tanto es algebraico sobre cualquier extensión de K'. Luego, el campo $K'(a_1)$ es algebraico sobre K' y generalizando $K'(a_1, ..., a_k)$ es algebraico sobre

$K'(a_1,...,a_{k-1})$ para $k = 2,...,n$. Luego $K = K'(a_1,...,a_n)$ es una extensión finita de K'. La parte, sólo si, se deja como ejercicio, ver Problema 1.10.♦

1.19 Definición. Considere la extensión algebraica $K' \rightarrowtail K$. La **cerradura algebraica de** K' **en** K es el conjunto $\{a \in K \mid a$ es algebraico sobre $K'\}$ y lo denotaremos con $\overline{K'_K}$ o simplemente, por abuso, $\overline{K'}$.

1.20 Proposición. Si $K' \rightarrowtail K$ es una extensión y $\overline{K'_K}$ la cerradura algebraica de K' en K entonces $\overline{K'_K}$ es un campo y es la extensión más grande de K' en K.

Demostración. Si a,$b \in K$ son algebraicos sobre K' entonces $a \pm b$, ab y a/b con $b \neq 0$ son algebraicos sobre K'. Si a,$b \in \overline{K'_K}$ entonces $K'(a,b)$ es una extensión finita y sus elementos son algebraicos sobre K'. Es decir, $K'(a,b) \subset \overline{K'_K}$. Luego, $\overline{K'_K}$ contiene a todo elemento de K que es algebraico sobre K', y así, $\overline{K'_K}$ es la extensión más grande de K'contenida en K.♦

Problemas.

1.1 Considere una familia de campos $\{K_i\}$ para $i = 1,...,s$ tal que cada K_{i+1} es una extensión finita de K_i. Pruebe que K_s es una extensión finita de K_1 y que

$$[K_1 \rightarrowtail K_s] = [K_1 \rightarrowtail K_2][K_2 \rightarrowtail K_3] \cdots [K_{s-1} \rightarrowtail K_s].$$

1.2 Sea $\mathbb{R}(i)$ el subcampo que contiene a los elementos de la forma $x+iy$, con x,$y \in \mathbb{R}$. Pruebe que $\mathbb{C} = \mathbb{R}(i)$.

1.3 Pruebe que $\mathbb{Q} \rightarrowtail \mathbb{R}$ y $\mathbb{Q} \rightarrowtail \mathbb{C}$ son extensiones infinitas y que $[\mathbb{Q} \rightarrowtail \mathbb{Q}(i)] = 2$.

1.4 Considérese

$$\varphi : K' \longrightarrow K'[t]/I$$

dada por

$$t \longmapsto t + I$$

Verifique que φ envía a K' isomórficamente en sí mismo dentro de $K'[t]/I$.

1.5 Pruebe que si f es un polinomio en $K'[t]$ de grado 2 ó 3, entonces f tiene una raíz en K' si, y sólo si, f es reducible sobre K'.

1.6 Escriba las tablas de sumar y multiplicar del campo con cuatro elementos del Ejemplo 1.12.

1.7 Pruebe que el polinomio mínimo para a sobre K', denotado $m_{a,K'}$, divide a cualquier otro polinomio que tenga a a como raíz.

1.8 Pruebe que si $a \in K$ entonces son equivalentes las siguientes: (i) a es algebraico sobre K', (ii) el homomorfismo de evaluación posee un núcleo no trivial y (iii) la extensión $K' \rightarrowtail K'(a)$ es finita.

1.9 Compruebe que $m_{\sqrt{2},\mathbb{Q}}(t) = t^2 - 2$, que $m_{\sqrt{2},\mathbb{R}}(t) = t^2 - \sqrt{2}$, y por lo tanto, $\sqrt{2}$ es algebraico de grado 2 sobre $\mathbb{Q}$ y es algebraico de grado 1 sobre $\mathbb{R}$. También compruebe que $m_{i,\mathbb{C}}(t) = t - i$.

1.10 Pruebe la parte "sólo si" de 1.18.

1.11 Compruebe que $K'[t]$ puede verse como un espacio vectorial sobre K' donde los elementos a^n con $n \geq 0$ generan $K'[t]$ sobre K'.

1.12 Considere la extensión $\mathbb{Q} \rightarrowtail \mathbb{C}$. Encuentre el polinomio mínimo para $\sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$.

1.13 Compruebe que $\mathbb{Q}\left(\sqrt[6]{2})\right) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Sugerencia: Verifique que

$$[\mathbb{Q}\left(\sqrt[6]{2})\right) \rightarrowtail \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})] = 1.$$

II.2 Automorfismos y más sobre extensiones

2.1 Definición. Sea Λ un anillo. Un **automorfismo** de Λ es un isomorfismo de anillos $\sigma : \Lambda \to \Lambda$. Denotaremos con $Aut(\Lambda)$ el conjunto de automorfismos de Λ.

2.2 Definición. Sea Γ un subanillo de Λ. Un **automorfismo de Λ sobre Γ** es un isomorfismo de anillos $\sigma : \Lambda \to \Lambda$ tal que $\sigma(a) = a$ para toda $a \in \Gamma$. Denotaremos con $Aut_\Gamma(\Lambda)$ el conjunto de automorfismos de Λ sobre Γ.

2.3 Proposición. $Aut(\Lambda)$ y $Aut_\Gamma(\Lambda)$ son grupos bajo la composición de funciones.

Demostración. Como la composición de automorfismos es automorfismo, como vale la asociatividad de funciones bajo la composición, como el inverso de un automorfismo también es un automorfismo y la identidad también lo es, el conjunto $Aut(\Lambda)$ es un grupo bajo la composición. Análogamente para $Aut_\Gamma(\Lambda)$.♦

2.4 Ejemplo. Considere $\Lambda = \mathbb{Z}$. Entonces todo $m \in \mathbb{Z}$ es de la forma $m1$ para $m \in \mathbb{Z}$. Claramente $\sigma(m1) = m1$. Por lo tanto $\sigma = I_\mathbb{Z}$. Luego, $Aut(\mathbb{Z}) = \{I_\mathbb{Z}\}$.

2.5 Proposición. Sea Δ un dominio entero, (K, f) su campo de cocientes y $\sigma : \Delta \to \Delta$ un automorfismo. Entonces el homomorfismo inducido $\sigma_* : K \to K$ es un automorfismo.

Demostración. Por I.3.4, existe $\sigma_* : K \to K$. Veamos que posee inverso. Como $\sigma : \Delta \to \Delta$ induce $\sigma_*^{-1} : K \to K$ y $\sigma^{-1}\sigma = \sigma\sigma^{-1} = I$. Por el Problema 2.3 (i), $\sigma_*^{-1}\sigma_* = \sigma_*\sigma_*^{-1} = I_K$. Luego, σ_* posee a σ_*^{-1} como inverso.♦

2.6 Definición. Sea $K' \rightarrowtail K$ una extensión y $f \in K'[t]$. Diremos que f **se descompone en** $K' \rightarrowtail K$ o **sobre** K si se factoriza en factores lineales en $K[t]$.

Observe que si se tiene un campo K'' tal que $f \in K'[t]$ se descompone sobre K'', entonces las distintas raíces a_1, ..., a_j de $f(t)$ en K'' generan el subcampo $K'(a_1, ..., a_j)$ de K'' que es el campo mínimo de K'' en el cual f se factoriza en factores lineales en $K''[t]$.

2.7 Definición. La extensión mínima de K' que cumple lo anterior se llama **campo de descomposición** de f sobre K' y lo denotaremos K'_f.

Nos preguntamos si existe una extensión $K' \rightarrowtail K''$ tal que un polinomio f se factorice en factores lineales. Para contestar esta pregunta, supongamos que a_1 es una raíz en $K' \rightarrowtail K^1$ y omitimos el factor $(t - a_1)$ considerando el polinomio $f_1(t) = f(t)/(t - a_1) \in K^1[t]$. Luego hacemos lo mismo encontrando una extensión $K' \rightarrowtail K^2$ que contenga una raíz de $f_1(t)$, etc. Así tenemos el siguiente

2.8 Teorema. Sea $f \in K'[t]$ un polinomio. Entonces existe una extensión finita $K' \rightarrowtail K''$ que es un campo de descomposición de f sobre K'.♦

2.9 Ejemplo. Considere el polinomio $f(t) = t^4 - 4$ en $\mathbb{Q}[t]$. Como $f(t) = (t^2 - 2)(t^2 + 2)$ podemos adjuntar las raíces $-\sqrt{2}$ y $\sqrt{2}$ de $t^2 - 2$ obteniendo $\mathbb{Q}(-\sqrt{2},\ \sqrt{2}) = \mathbb{Q}(\sqrt{2})$ el cual es una extensión $\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})$ de grado 2. Nos fijamos en $(t^2+2) \in \mathbb{Q}(\sqrt{2})[t]$. Las raíces $-\sqrt{2}i$ y $\sqrt{2}i$ son complejas, no en $\mathbb{R}$, luego $(t^2 + 2)$ es irreducible en $\mathbb{Q}(\sqrt{2})[t]$. Ahora consideramos $\mathbb{Q}(\sqrt{2}, \sqrt{2}i) = \mathbb{Q}(\sqrt{2}, i)$ y la extensión $\mathbb{Q}(\sqrt{2}) \rightarrowtail \mathbb{Q}(\sqrt{2}, i)$ la cual es de grado 2. Considere la torre acostada de campos $\mathbb{Q} \overset{2}{\rightarrowtail} \mathbb{Q}(\sqrt{2}) \overset{2}{\rightarrowtail} \mathbb{Q}(\sqrt{2},\ i) \rightarrowtail \cdots \rightarrowtail \mathbb{C}$. Luego el campo de descomposición de f sobre $\mathbb{Q}$ en $\mathbb{C}$ es $\mathbb{Q}(\sqrt{2},\ i)$ y por lo tanto $[\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2},\ i)] = 4$.

Suponga que $a_1, ..., a_j \in K$ son las distintas raíces de $f \in K'[t]$. $K'(a_1, ..., a_j)$ es el mínimo subcampo que contiene a K' y a las a_i. Pero $K'(a_1,\ \ldots,\ a_j)$ está contenido en cualquiera o todo subcampo de descomposición. Por lo tanto tenemos la siguiente

2.10 Proposición. Sea $K' \rightarrowtail K''$ una extensión y $f \in K''[t]$. Si K^1 y K^2 son subcampos de descomposición para f sobre K' entonces $K^1 = K^2$.♦

Notación. (i) Para las extensiones $K' \rightarrowtail K$ y $K' \rightarrowtail K''$ denotaremos con $hom_{K'}(K,\ K'')$ el conjunto de homomorfismos (inyectivos) de K en K'' que dejan fijo a K'. Considere la extensión finita $K' \rightarrowtail K''$, entonces $hom_{K'}(K'',\ K'') = Aut_{K'}(K'',\ K'')$ es un grupo. (ii) Sea $K' \rightarrowtail K''$ una extensión y $f \in K'[t]$. Denotaremos con $R(f,\ K'')$ el conjunto de las raíces de f en K''.

2.11 Proposición. Sea $K' \rightarrowtail K''$ una extensión y $f \in K'[t]$ un polinomio irreducible. Sea $a_i \in K''$ una raíz de f. Entonces los conjuntos

$$hom_{K'}(K'(a_i), K'') \text{ y } R(f, K'')$$

poseen la misma cardinalidad.

Demostración. Considere el diagrama

$$\begin{array}{ccccc} K' & \longrightarrow & K'[t] & \xrightarrow{\varphi} & K'[t]/\langle f\rangle \\ & \searrow & E_a \downarrow & \varphi_a \swarrow & \cong\downarrow \varphi_{a_i} \\ & & K'' & \dashleftarrow & K'(a_i) \end{array}$$

donde $E_a : K'[t] \longrightarrow K''$ es el homomorfismo de evaluación, el cual se factoriza mediante $\varphi_a : K'[t]/\langle f\rangle \rightarrow K''$. Para cada raíz a_i existe un φ_{a_i}. Entonces, cada raíz a_i da lugar a un homomorfismo $\psi_a = \varphi_a \circ (\varphi_{a_i})^{-1}$ para el cual $\psi_a(a_i) = a_i$.♦

2.12 Ejemplo. Como $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[t]/\langle t^2-2\rangle$ donde t^2-2 es irreducible sobre $\mathbb{Q}$, hay dos homomorfismos que dejan fijo a $\mathbb{Q}$ que envían $\sqrt{2}$ en $\pm\sqrt{2}$, que son raíces complejas de t^2-2. Estas dos raíces nos dan los homomorfismos

$$\begin{array}{lccl} 1,\ \delta: & \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{C} \\ & a+b\sqrt{2} & \longmapsto & 1(a+b\sqrt{2}) = \quad a+b\sqrt{2} \\ & a+b\sqrt{2} & \longmapsto & \delta(a+b\sqrt{2}) = \quad a-b\sqrt{2} \end{array}$$

Si ponemos $\mathbb{Q}(\sqrt{2})$ en lugar de $\mathbb{C}$ obtenemos

$$hom_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C}) = hom_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2})) = Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}).$$

Luego $|hom_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}),\ \mathbb{C})| = 2$.

La siguiente proposición es clave para comprender el grupo de automorfismos para el caso de extensiones algebraicas.

2.13 Proposición. Considere las extensiones $K' \rightarrowtail K$ y $K' \rightarrowtail K''$. Entonces

(i) para $f \in K[t]$, cada $\delta \in hom_{K'}(K,\ K'')$ se restringe a una función inyectiva $\delta_f : R(f,\ K) \longrightarrow R(f,\ K'')$.

(ii) si $\delta \in hom_{K'}(K,\ K)$ entonces $\delta_f : R(f,K) \longrightarrow R(f,K)$ es biyectiva.

Demostración. (i) Para $a \in R(f,K)$ se tiene que $f(\delta(a)) = \delta(f(a)) = \delta(0) = 0$, por lo tanto δ envía $R(f,K)$ en $R(f,K'')$. Como δ es inyectiva, su restricción a $R(f,K) \subseteq K$ es una inyección también.

(ii) De (i), $\delta_f : R(f,K) \longrightarrow R(f,K)$ es inyectiva y como es de un conjunto finito en sí mismo es suprayectiva.♦

Observe que (ii) dice que cualquier automorfismo de K permuta el conjunto de raíces de K de un polinomio $f \in K[t]$.

2.14 Definición. Considere la extensión $K' \rightarrowtail K''$. Diremos que los elementos $a,\ b \in K''$ son **conjugados sobre** K' si son raíces del mismo polinomio mínimo sobre K', es decir, $m_{a,K'} = m_{b,K'}$.

2.15 Ejemplos. Considere la extensión $\mathbb{Q} \rightarrowtail \mathbb{C}$, i y $-i$ son conjugados sobre $\mathbb{Q}$ pues son raíces del mismo polinomio mínimo sobre $\mathbb{Q}$, $m_{i,\mathbb{Q}}(t) = t^2 + 1 = m_{-i,\mathbb{Q}}(t)$. Si se considera la extensión $\mathbb{Q} \rightarrowtail \mathbb{C}$, $\sqrt{2}$ y $-\sqrt{2}$ son conjugados sobre $\mathbb{Q}$ pues son raíces del mismo polinomio mínimo sobre $\mathbb{Q}$, $m_{\sqrt{2},\mathbb{Q}}(t) = t^2 - 2 = m_{-\sqrt{2},\mathbb{Q}}(t)$. También, para $\mathbb{Q} \rightarrowtail \mathbb{C}$, $\sqrt[3]{2}$, $\sqrt[3]{2}e^{2\pi i/3}$, $\sqrt[3]{2}e^{4\pi i/3}$ son conjugados sobre $\mathbb{Q}$ pues son raíces del mismo polinomio mínimo sobre $\mathbb{Q}$, $m_{\_,\mathbb{Q}}(t) = t^3 - 2$.

2.16 Teorema. Sea K' un campo, a, b elementos algebraicos sobre K', $n = gr(m_{a,K})$. Entonces a y b son conjugados sobre K' si, y sólo si, la función

$$\varphi_{a,b} : K'(a) \longrightarrow K'(b)$$

dada por

$$\lambda_{n-1}a^{n-1} + \cdots + \lambda_1 a^1 + \lambda_0 \longmapsto \lambda_{n-1}b^{n-1} + \cdots + \lambda_1 b^1 + \lambda_0$$

es un isomorfismo de campos.

Demostración. Supongamos que a y b son conjugados, es decir, $m_{a,K'} = m_{b,K'}$. Consideremos el siguiente diagrama

$$\begin{array}{ccccccc} \langle m_{a,K'}\rangle & \longrightarrow & K'[t] & \longrightarrow & K'[t]/\langle m_{a,K'}\rangle & = & K'[t]/\langle m_{b,K'}\rangle \\ & E_a \searrow & & \downarrow\cong \varphi_a & & & \downarrow\cong \varphi_b \\ & & & K'(a) & \overrightarrow{\varphi_{a,b}} & & K'(b) \end{array}$$

Definimos $\varphi_{a,b} = \varphi_b \circ \varphi_a^{-1}$ el cual es un isomorfismo tal que

$$\begin{aligned} \varphi_{a,b}(\lambda_{n-1}a^{n-1} + \cdots + \lambda_1 a^1 + \lambda_0) &= \varphi_b \circ \varphi_a^{-1}(\lambda_{n-1}a^{n-1} + \cdots + \lambda_1 a^1 + \lambda_0) \\ &= \varphi_b[(\lambda_{n-1}a^{n-1} + \cdots + \lambda_1 a^1 + \lambda_0) + \langle m_{a,K'}\rangle] \\ &= \lambda_{n-1}b^{n-1} + \cdots + \lambda_1 b^1 + \lambda_0. \end{aligned}$$

Ahora veamos que si $\varphi_{a,b}$ es isomorfismo entonces a y b serán conjugados. Considere $m_{a,K'}(t) = \lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$. Entonces $\lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0 = 0$. Por lo tanto $\varphi_{a,b}(\lambda_n a^n + \cdots + \lambda_2 a^2 + \lambda_1 a^1 + \lambda_0) = \lambda_n b^n + \cdots + \lambda_2 b^2 + \lambda_1 b^1 + \lambda_0 = 0$. Luego $m_{b,K'} | m_{a,K'}$. Análogamente $m_{a,K'} | m_{b,K'}$ y así, a y b son conjugados.♦

2.17 Ejemplo. Considere la extensión $\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})$ y el polinomio $m_{\sqrt{2},\mathbb{Q}}(t) = t^2 - 2$. Sus raíces son $-\sqrt{2}$ y $\sqrt{2}$ y por definición, son conjugadas sobre $\mathbb{Q}$. Por el teorema anterior, $\varphi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ dada por $a + b\sqrt{2} \longmapsto \varphi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ es un automorfismo de $\mathbb{Q}(\sqrt{2})$.

2.18 Definiciones. Sea $f \in K'[t]$ un polinomio irreducible. Diremos que el polinomio f es **separable sobre** K'' si toda raíz de f es simple en la extensión $K' \rightarrowtail K''$. Un elemento algebraico $a \in K''$ en una extensión $K' \rightarrowtail K''$ es **separable** si su polinomio mínimo $m_{a,K'} \in K'[t]$ es separable. Si $K' \rightarrowtail K''$ es una extensión finita, el **grado de separabilidad,** denotado $\{K' \rightarrowtail K''\}$, de la extensión $K' \rightarrowtail K''$, es el orden de $hom_{K'}(K'', \overline{K'})$. Si $K' \rightarrowtail K''$ es una extensión finita, se dice que es **separable** si $\{K' \rightarrowtail K''\} = [K' \rightarrowtail K'']$.

Observe que si $K' \rightarrowtail K'(a)$ es una extensión finita simple, por 2.11 aplicado a $K'' = \overline{K'}$ se tiene que $\{K' \rightarrowtail K'(a)\} = |R(m_{a,K'}, \overline{K'})|$.

2.19 Proposición. Si $K' \rightarrowtail K$ y $K \rightarrowtail K''$ son extensiones finitas, entonces $\{K' \rightarrowtail K\}\{K \rightarrowtail K''\} = \{K' \rightarrowtail K''\}$.

Demostración. Problema 2.6.♦

2.20 Definición. Considere $K' \rightarrowtail K''$ una extensión finita. Diremos que es una **extensión normal** si K'' es el campo de descomposición sobre K' de algún polinomio $f \in K'[t]$.

Recuérdese que $hom_{K'}(K,\ K'')$ denota el conjunto de homomorfismos de K en K'' que dejan fijo a K'. Así, $hom_{K'}(K'', K'') = Aut_{K'}(K'')$ pues todo homomorfismo inyectivo es suprayectivo y por lo tanto invertible. Por el Problema 2.8, una extensión $K' \rightarrowtail K''$ es normal si para toda $\psi \in hom_{K'}(K'',\ \overline{K'})$ se tiene que $\psi(K'') = K''$. Obsérvese que si $K' \rightarrowtail K''$ es una extensión normal, entonces, siempre que se tenga un polinomio irreducible $f \in K'[t]$ el cual posea una raíz en K'', se separa en K'' puesto que cada par de raíces de f son conjugadas sobre K' y una va a dar a la otra mediante un homomorfismo $\overline{K'} \rightarrow \overline{K'}$ que envía a K'' en sí mismo.

2.21 Teorema. Sea $K' \rightarrowtail K''$ una extensión algebraica y $K' \rightarrowtail K \rightarrowtail K''$ una torre de campos. Si $\psi_{_0} : K \rightarrow \overline{K'}$ es un homorfismo que fija los elementos de K', entonces existe un homomorfismo $\psi : K'' \longrightarrow \overline{K'}$ que "extiende" a ψ_0.

$$\begin{array}{ccc} K'' & \overset{\psi}{\dashrightarrow} & \overline{K'} \\ | & \nearrow_{\psi_0} & | \\ K & & | \\ | & & | \\ K' & = & K' \end{array}$$

Demostración. Sea A el conjunto de las parejas $(C,\ \varphi)$ donde $(K \rightarrowtail C) \leq (K \rightarrowtail K'')$ y $\varphi : C \rightarrow \overline{K'}$ extiende a ψ_0. Ordenemos A mediante la relación $\lll$ para la cual $(C_1,\ \varphi_1) \lll (C_2,\ \varphi_2)$ siempre que $C_1 \leq C_2$ y φ_2 extiende a φ_1. Luego $(A, \lll)$es un conjunto parcialmente ordenado. Supóngase que $B \subseteq A$ es un subconjunto totalmente ordenado. Sea $\mathcal{C} = \cup_{(C,\varphi)\in Y} C$. Entonces $(K \rightarrowtail \mathcal{C}) \leq (K \rightarrowtail K'')$. También existe una función $\overline{\varphi} : \mathcal{C} \rightarrow \overline{K'}$ dada por $\overline{\varphi}(a) = \varphi(a)$ cuando $a \in C$ para $(C, \varphi) \in B$. Es claro que si $a \in C'$ para $(C', \varphi') \in B$ entonces $\varphi'(a) = \varphi(a)$ y por lo tanto $\overline{\varphi}$ está bien definida. Entonces para toda pareja $(C, \varphi) \in B$ tenemos que $(C, \varphi) \lll (\mathcal{C}, \overline{\varphi})$ y así $(\mathcal{C}, \overline{\varphi})$ es una cota superior de B. Por el Lema de Zorn, debe de haber un elemento máximo de A, a saber, (K_0'', φ_0).

Supongamos que $K_0'' \neq K''$, entonces existe un elemento $a \in K''$ para el cual $a \notin K_0''$. Como K'' es algebraico sobre K', también es algebraico sobre K_0'' pues a es algebraico sobre K_0''. Si $m_{a,K_0''}(t) = t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0$, entonces el polinomio $f(t) = t^n + \cdots + \varphi_0(\lambda_2)t^2 + \varphi_0(\lambda_1)t^1 + \varphi_0(\lambda_0) \in (\varphi_0(K_0''))[t]$ es también irreducible y por lo tanto tiene una raíz b en $\overline{K'}$ el cual es también la cerradura algebraica de $\varphi_0(K_0'')$. Por la propiedad universal del anillo de polinomios $K_0''[t]$, φ_0 da lugar a φ_0'' como en el siguiente diagrama

$$\begin{array}{ccccc} K_0'' & \longrightarrow & K_0''[t] & \longrightarrow & K_0''[t]/\left\langle m_{a,K_0''}(t)\right\rangle \cong K_0''(a) \\ & \searrow_{\varphi_0} & \downarrow_{\varphi_0'} & \swarrow_{\varphi_0''} & \\ & & \overline{K'} & & \end{array}$$

Pero $(K_0'',\ \varphi_0) \lll (K_0''(a),\ \varphi_0'')$ y $(K_0'',\ \varphi_0) \neq (K_0''(a),\ \varphi_0'')$ contradiciendo la maximalidad de $(K_0'',\ \varphi_0)$. Por lo tanto, $K_0'' = K''$ y podemos tomar $\psi = \varphi_0$.♦

2.22 Definición. Considere $K' \rightarrowtail K''$ una extensión finita simple. Diremos que $a \in K''$ es un **elemento primitivo** de la extensión si $K'' = K'(a)$.

El siguiente teorema se conoce como el teorema del elemento primitivo.

2.23 Teorema. Sea $K' \rightarrowtail K''$ una extensión separable. Entonces K'' posee un elemento primitivo.

Demostración. Supongamos que K''es un campo infinito. Como K'' se construye a partir de una sucesión de extensiones simples, basta considerar el caso $K'' = K'(a,\ b)$. Sean $f,\ g \in K'[t]$ los polinomios mínimos de a y b sobre K' respectivamente. Considere $a = a_1,\ ...,\ a_r$ y $b = b_1,\ ...,\ b_s$ las distintas raíces de f y g respectivamente en K'. Como $K' \rightarrowtail K''$ es separable, $r = gr\,(f)$ y $s = gr\,(g)$. Para $j \neq 1$ se tiene que $b = b_1 \neq b_j$ y por lo tanto la ecuación $a + xb = a_i + xb_j$ tiene solamente una solución, a saber, $a - a_i = xb_j - xb = x(b_j - b)$ y $x = \frac{a-a_i}{b_j-b}$. Si escogemos una $x \in K'$ diferente de estas soluciones (pues K' es infinito), entonces $a + xb \neq a_i + xb_j$, excepto cuando $i = j = 1$.

Sea $c = a + xb$. Entonces los polinomios $g(t)$ y $f(c - xt)$ tienen coeficientes en $K'(c)[t]$ y poseen a b como raíz, es decir, $g(b) = 0$ y $f(c - xb) = f(a) = 0$. De hecho, b es su única raíz común pues escogimos x tal que $c \neq a_i + xb_j$, es decir, $a_i \neq c - xb_j$ a menos que $1 = i = j$.

Por lo tanto, el $m.c.d.(g(t),\ f(c-xt)) = t-b$. Se sabe que el máximo común divisor de dos polinomios tiene coeficientes en el mismo campo que los coeficientes de los polinomios. Luego $b \in K'(c)$ y esto implica que $a = c - xb$ también está en $K'(c)$. Por lo tanto, $K'(a,\ b) = K'(c)$. Para el caso en que K'' sea un campo finito, ver el Problema 3.5 en la siguiente sección.♦

Problemas.

2.1 Pruebe que $Aut(\mathbb{Z}_n) = \{I_{\mathbb{Z}_n}\}$.

2.2 Suponga que un anillo Λ contiene a $\Gamma = \mathbb{Z}$ ó $\mathbb{Z}_n$ y $\sigma \in Aut(\Lambda)$. Pruebe que σ se restringe a la identidad en Λ y por lo tanto $Aut(\Lambda) = Aut_\Gamma(\Lambda)$.

2.3 Sean Δ' y Δ dominios enteros, K' y K sus campos de cocientes respectivamente y $\sigma : \Delta' \to \Delta$ un monomorfismo. (i) Pruebe que existe un único homomorfismo inducido $\sigma_* : K' \to K$ tal que $\sigma_*(a) = \sigma(a)$ para $a \in \Delta' \subset K'$. (ii) Pruebe que $I_{\Delta'} : \Delta' \to \Delta'$ induce $I_* = I : K' \to K'$ y que si $\Delta' \xrightarrow{\sigma} \Delta \xrightarrow{\mu} \Delta''$ son monomorfismos de dominios enteros, entonces $\mu_*\sigma_* = (\mu\sigma)_* : K' \to K'$.

2.4 (i) Pruebe que $(\ )_* : Aut(\Delta') \to Aut(K')$ es un monomorfismo. (ii) Pruebe que $(\ )_* : Aut(\mathbb{Z}) \to Aut(\mathbb{Q})$ es un isomorfismo y por lo tanto $Aut(\mathbb{Q}) = \{I_{\mathbb{Q}}\}$.

2.5 Pruebe que las raíces de polinomios con coeficientes en $\mathbb{R}$ son conjugadas. Sugerencia: considere $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(-i)$.

2.6 Pruebe la Proposición 2.19: si $K' \rightarrowtail K$ y $K \rightarrowtail K''$ son extensiones finitas, entonces $\{K' \rightarrowtail K\}\{K \rightarrowtail K''\} = \{K' \rightarrowtail K''\}$.

2.7 Pruebe que si $K' \rightarrowtail K$ y $K \rightarrowtail K''$ son extensiones finitas, entonces $K' \rightarrowtail K$ y $K \rightarrowtail K''$ son separables si, y sólo si $K' \rightarrowtail K''$ es separable.

2.8 Pruebe que K'' es el campo de descomposición sobre K' de algún polinomio $f \in K'[t]$ (es decir $K' \rightarrowtail K''$ es una extensión normal) si, y sólo si, $\psi(K'') = K''$ para todo $\psi \in hom_{K'}(K'',\ \overline{K'})$.

2.9 Considere las extensiones finitas $K' \rightarrowtail K$ y $K \rightarrowtail K''$. Pruebe que si la extensión $K' \rightarrowtail K''$ es normal, entonces la extensión $K \rightarrowtail K''$ es normal.

2.10 Sea f un polinomio en $K'[t]$. Un elemento $a \in \overline{K'}$ tal que $f(a) = 0$ es una **raíz de multiplicidad** n si n es el mayor entero tal que $(t-a)^n$ es un factor de f en $\overline{K'}[t]$. Pruebe que si f es irreducible en $K'[t]$ entonces todas las raíces de f en $\overline{K'}$ tienen la misma multiplicidad. Sugerencia: Use los Teoremas 2.16 y 2.21.

II.3 Teoría de Galois

Recordemos que hemos estado estudiando la estructura de una extensión algebraica $K' \rightarrowtail K''$ analizando los automorfismos de K'' que dejan fijo a K', es decir, analizando $Aut_{K'}(K'')$.

3.1 Definición. Una extensión finita $K' \rightarrowtail K''$ se llama **extensión de Galois** si es normal y separable.

Por el teorema 2.21, todo automorfismo $K' \longrightarrow K'$ se extiende a un homomorfismo de $K'' \longrightarrow \overline{K'}$ manteniendo fijos a los elementos de K'. Luego tenemos la biyección $hom_{K'}(K'', \overline{K'}) \longleftrightarrow Aut_{K'}(K'')$ y por lo tanto

$$|Aut_{K'}(K'')| = \{K' \rightarrowtail K''\} = [K' \rightarrowtail K''].$$

3.2 Definición. El **grupo de Galois de la extensión** $K' \rightarrowtail K''$ es el grupo $Aut_{K'}(K'')$ denotado $Gal(K' \rightarrowtail K'')$. Sus elementos se llaman **automorfismos de Galois** de $K' \rightarrowtail K''$.

Así, $|Gal(K' \rightarrowtail K'')| = \{K' \rightarrowtail K''\} = [K' \rightarrowtail K'']$.

3.3 Ejemplo. Por 1.9 sabemos que $[\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 4$. Consideremos $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. El isomorfismo $\varphi_{\sqrt{3},-\sqrt{3}} : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ dado por $c + d\sqrt{3} \mapsto c - d\sqrt{3}$, con c,$d \in \mathbb{Q}(\sqrt{2})$ es un automorfismo que tiene a $\mathbb{Q}(\sqrt{2})$ como campo fijo. Análogamente, $\varphi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ tiene a $\mathbb{Q}(\sqrt{3})$ como campo fijo. Como la composición de automorfismos es un automorfismo, vemos que $\varphi_{\sqrt{3},-\sqrt{3}} \circ \varphi_{\sqrt{2},-\sqrt{2}}$ no deja fijo ni a $\sqrt{2}$, ni a $\sqrt{3}$. Consideremos el grupo $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$. Sabemos que $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ es una base para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$. Consideremos $\iota = 1_{Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2},\sqrt{3}))}$, $\alpha_1 = \varphi_{\sqrt{2},-\sqrt{2}}$, $\alpha_2 = \varphi_{\sqrt{3},-\sqrt{3}}$ y $\alpha_3 = \varphi_{\sqrt{3},-\sqrt{3}} \circ \varphi_{\sqrt{2},-\sqrt{2}}$.

Como $\alpha_1(\sqrt{2}) = -\sqrt{2}$, $\alpha_1(\sqrt{6}) = -\sqrt{6}$ y $\alpha_2(\sqrt{3}) = -\sqrt{3}$, $\mathbb{Q}$ es el campo fijo de $\{\iota,\alpha_1,\alpha_2,\alpha_3\}$.

Sea $K' \rightarrowtail K''$ una extensión de Galois y H un subgrupo de $Gal(K' \rightarrowtail K'')$. Denotemos con

$$(K'')^H = \{a \in K'' | \alpha(a) = a, \text{ para toda } \alpha \in H\}.$$

Entonces $(K'')^H$ es un subcampo de K'' que contiene a K' pues si $a,b \in (K'')^H$ y $\alpha \in H$, $\alpha(a+b) = \alpha(a) + \alpha(b) = a + b$, $\alpha(ab) = \alpha(a)\alpha(b) = ab$, $\alpha(a^{-1}) = \alpha(a)^{-1}$ si $a \neq 0$ y si $c \in K'$, entonces $\alpha(c) = c$, es decir $K' \leq (K'')^H$. Llamaremos a $(K'')^H$ **subcampo fijo de** H. Si H denota una familia $\{\varphi_i\}$ de automorfismos de K'' que dejan fijo a K', denotamos con $(K'')^{\{\varphi_i\}}$ al subcampo fijo de la familia $\{\varphi_i\}$.

3.4 Ejemplo. Considere la extensión $\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})$ y el polinomio $m_{\sqrt{2},\mathbb{Q}}(t) = t^2 - 2$. Sus raíces son $-\sqrt{2}$ y $\sqrt{2}$ y son conjugadas sobre $\mathbb{Q}$. Como vimos en el Ejemplo 2.17, $\varphi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ dada por $a + b\sqrt{2} \longmapsto \varphi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ es un automorfismo de $\mathbb{Q}(\sqrt{2})$. Pero $a + b\sqrt{2} = a - b\sqrt{2}$ cuando $b = 0$. Luego, el subcampo fijo de $\{\varphi_{\sqrt{2},-\sqrt{2}}\}$ es $\mathbb{Q}(\sqrt{2})^{\{\varphi_{\sqrt{2},-\sqrt{2}}\}} = \mathbb{Q}$.

Por el Problema 2.7, si $K' \rightarrowtail K''$ es una extensión de Galois entonces las extensiones $K' \rightarrowtail (K'')^H$ y $(K'')^H \rightarrowtail K''$ son separables y también $(K'')^H \rightarrowtail K''$ es normal y por lo tanto es una extensión de Galois. Recuerde que $|Gal((K'')^H \rightarrowtail K'')| = \{(K'')^H \rightarrowtail K''\} = [(K'')^H \rightarrowtail K'']$. Todo automorfismo de $Gal((K'')^H \rightarrowtail K'')$ es un automorfismo de $Gal(K' \rightarrowtail K'')$, luego $Gal((K'')^H \rightarrowtail K'')$ es un subgrupo de $Gal(K' \rightarrowtail K'')$. Observe que, por definición, $H \leq Gal((K'')^H \rightarrowtail K'')$ y por el Teorema de Lagrange, $o(H)|o(Gal((K'')^H \rightarrowtail K'')$.

3.5 Proposición. Si H es un subgrupo de $Gal(K' \rightarrowtail K'')$ entonces $Gal((K'')^H \rightarrowtail K'') = H$.

Demostración. Como la extensión $(K'')^H \rightarrowtail K''$ es separable, por el teorema 2.23, es una extensión simple, es decir, $K'' = (K'')^H(a)$. Considere los distintos elementos de $H = \{1_H = \beta_1, \beta_2, ..., \beta_n\}$. Considere el polinomio de grado n

$$f(t) = (t - a)(t - \beta_2(a)) \cdots (t - \beta_n(a)) \in K''[t].$$

Observe que $f(t)$ no cambia al aplicar β_j a sus coeficientes puesto que las raíces $\beta_k(a)$ son permutadas por β_j. Por lo tanto, $f(t) \in (K'')^H[t]$. Así, $[(K'')^H \rightarrowtail K''] = [(K'')^H \rightarrowtail ((K'')^H)(a)] \leq n = o(H)$. Por otro lado, como $H \leq (Gal((K'')^H \rightarrowtail K''))$,tenemos que $n = o(H) \leq o(Gal((K'')^H \rightarrowtail K'')) = [(K'')^H \rightarrowtail K'')]$. Por las dos desigualdades anteriores se tiene que $o(H) = n = o(Gal((K'')^H \rightarrowtail K'')) = [(K'')^H \rightarrowtail K'')]$ y por lo tanto $Gal((K'')^H \rightarrowtail K'') = H$♦

Sea $K' \rightarrowtail K''$ una extensión de Galois y $(K' \rightarrowtail K) \leq (K' \rightarrowtail K'')$. Entonces la extensión $K \rightarrowtail K''$ también es de Galois cuyo grupo de Galois lo denotamos $Gal(K \rightarrowtail K'')$.

3.6 Definición. El grupo de Galois $Gal(K \rightarrowtail K'')$ anterior se llamará **grupo de Galois relativo de las extensiones** $(K' \rightarrowtail K)$ y $(K' \rightarrowtail K'')$.

3.7 Proposición. Considere $(K' \rightarrowtail K) \leq (K' \rightarrowtail K'')$. Entonces $(K'')^{Gal(K \rightarrowtail K'')} = K$.

Demostración. Es claro que $K \leq (K'')^{Gal(K \rightarrowtail K'')}$. Por otro lado, sea $a \in K'' - K$. Por el Problema 3.3, existe un automorfismo $\sigma \in Gal(K \rightarrowtail K'')$ tal que $\sigma(a) \neq a$ y por lo tanto $a \notin (K'')^{Gal(K \rightarrowtail K'')}$. Así, $(K'')^{Gal(K \rightarrowtail K'')} \leq K$. Por lo tanto, $(K'')^{Gal(K \rightarrowtail K'')} = K$.♦

Consideremos una extensión de Galois finita $K' \rightarrowtail K''$. Denotemos con $Subgr(K' \rightarrowtail K'')$ el conjunto de todos los subgrupos de $Gal(K' \rightarrowtail K'')$ y $Subext(K' \rightarrowtail K'')$ el conjunto de todas las subextensiones $K' \rightarrowtail K$ de $K' \rightarrowtail K''$, es decir, donde K es un campo intermedio $K' \leq K \leq K''$. Ordenemos estos conjuntos por inclusiones. Claramente $Subgr(K' \rightarrowtail K'')$ es un conjunto finito.

Los siguientes resultados constituyen los principales de la Teoría de Galois.

3.8 Teorema . Sea $K' \rightarrowtail K''$ una extensión de Galois finita. Definamos las siguientes funciones

$$\begin{array}{rccl} g: & Subgr(K' \rightarrowtail K'') & \longrightarrow & Subext(K' \rightarrowtail K'') \text{ dada por} \\ & H & \longmapsto & g(H) = ((K'')^H \rightarrowtail K'') \end{array}$$

y

$$\begin{array}{rccl} f: & Subext(K' \rightarrowtail K'') & \longrightarrow & Subgr(K' \rightarrowtail K'') \text{ dada por} \\ & (K' \rightarrowtail K'') & \longmapsto & f(K' \rightarrowtail K'') = Gal(K' \rightarrowtail K'') \end{array}$$

Entonces las funciones f y g son biyecciones mutuamente inversas que preservan el orden de contención inverso.

Demostración. Utilizando los resultados anteriores, considere las composiciones siguientes

$$\begin{array}{ccccc} Subgr(K' \rightarrowtail K'') & \xrightarrow{g} Subext(K' \rightarrowtail K'') & \xrightarrow{f} & Subgr(K' \rightarrowtail K'') \\ & & & f(g(H)) = \\ H \longmapsto & g(H) = ((K'')^H \rightarrowtail K'') & \longmapsto & = f((K'')^H \rightarrowtail K'') \\ & & & = Gal((K'')^H \rightarrowtail K'') \\ & & & = H \end{array}$$

$$\begin{array}{ccccc} Subext(K' \rightarrowtail K'') & \xrightarrow{f} Subgr(K' \rightarrowtail K'') & \xrightarrow{g} & Subext(K' \rightarrowtail K'') \\ & f(K' \rightarrowtail K) & & \\ (K' \rightarrowtail K) & \longmapsto \quad \| \quad & \longmapsto & (K'')^{Gal(K' \rightarrowtail K)} \rightarrowtail K'' = \\ & Gal(K' \rightarrowtail K) & & = (K' \rightarrowtail K) \end{array}$$

i.e., $f \circ g = 1_{Subgr(K' \rightarrowtail K'')}$ y $g \circ f = 1_{Subext(K' \rightarrowtail K'')}$. Luego, f y g son inversos uno del otro. Si H_1 y H_2 son elementos del conjunto $Subgr(K' \rightarrowtail K'')$ tal que $H_1 \leq H_2$ entonces $(K' \rightarrowtail (K'')^{H_2}) \leq (K' \rightarrowtail (K'')^{H_1})$ pues si $b \in (K'')^{H_2}$ entonces permanece fijo por todo elemento de H_1 pues H_1 es un subconjunto de H_2. Por lo tanto, g también invierte el orden. También, si $(K' \rightarrowtail K_1) \leq (K' \rightarrowtail K_2)$ son elementos de $Subext(K' \rightarrowtail K'')$, entonces como $K_1 \leq K_2$, $Gal(K_2 \rightarrowtail K'') \leq Gal(K_1 \rightarrowtail K'')$ y si $\sigma \in Gal(K_2 \rightarrowtail K'')$ entonces σ fija todo elemento de K_1. Por lo tanto $f(K' \rightarrowtail K_2) \leq f(K' \rightarrowtail K_1)$ y f invierte el orden de contención.♦

Es de mencionarse que este fenómeno no se estudia solamente en la Teoría de Galois, sino en general en la Teoría de Conjuntos Parcialmente Ordenados. Tal par de biyecciones son, de hecho, funtores y se les conoce como una conexión de Galois. Esto tiene mucha importancia en la Teoría de la Computación y en la Teoría Matemática de la Música.

3.9 Proposición. Sea $K' \rightarrowtail K''$ una extensión de Galois y $(K' \rightarrowtail K) \leq (K' \rightarrowtail K'')$. Entonces el grupo de Galois relativo $Gal(K \rightarrowtail K'')$ de las extensiones $(K' \rightarrowtail K)$ y $(K' \rightarrowtail K'')$ es un subgrupo normal de $Gal(K' \rightarrowtail K'')$ si, y sólo si $(K' \rightarrowtail K)$ es una extensión normal.

Demostración. Supongamos que $Gal(K \rightarrowtail K'') \lhd Gal(K' \rightarrowtail K'')$, es decir, para toda $\alpha \in Gal(K \rightarrowtail K'')$ y $\beta \in Gal(K' \rightarrowtail K'')$ tenemos que

$\beta\alpha\beta^{-1} \in Gal(K \rightarrowtail K'')$. Si $k \in K$, entonces para cualquier $\kappa \in Gal(K' \rightarrowtail K'')$ y $\alpha \in Gal(K \rightarrowtail K'')$, $\kappa(k) \in K''$ satisface $\alpha\kappa(k) = \kappa(\kappa^{-1}\alpha\kappa(k)) = \kappa(k)$ puesto que $\kappa^{-1}\alpha\kappa \in Gal(K \rightarrowtail K'')$; luego $\kappa(k) \in (K'')^{Gal(K \rightarrowtail K'')} = K$. Por el Teorema 2.21, todo homomorfismo $K \to \overline{K'}$ que deja fijo a K' se extiende a un homomorfismo $K'' \to \overline{K'}$ el cual debe tener imagen K''. Por lo tanto, $K' \rightarrowtail K''$ es una extensión normal.

Ahora supongamos que $K' \rightarrowtail K''$ es una extensión normal. Entonces, para cada $\alpha \in Gal(K \rightarrowtail K'')$ y $k \in K$, $\alpha(k) \in K$. También, para cada $\beta \in Gal(K' \rightarrowtail K'')$, $\beta(\alpha(k)) = \alpha(k)$ y por lo tanto $\alpha^{-1}\beta\alpha(k) = k$. Así que $\alpha^{-1}\beta\alpha \in Gal(K \rightarrowtail K'')$. Luego, para toda $\alpha \in Gal(K' \rightarrowtail K'')$, $\alpha Gal(K \rightarrowtail K'')\alpha^{-1} = Gal(K \rightarrowtail K'')$ y por lo tanto $Gal(K \rightarrowtail K'') \lhd Gal(K' \rightarrowtail K'')$.♦

3.10 Proposición. Sea $K' \rightarrowtail K$ una extensión de Galois. Entonces existe un isomorfismo de grupos

$$Gal(K' \rightarrowtail K'')/Gal(K \rightarrowtail K'') \cong Gal(K' \rightarrowtail K)$$

dado por $\alpha Gal(K \rightarrowtail K'') \longmapsto \alpha|_K$.

Demostración. Como $K' \rightarrowtail K$ es una extensión normal, si $\alpha \in Gal(K' \rightarrowtail K'')$ entonces $\alpha K = K$. Así es que podemos restringir α a un automorfismo de K, $\alpha|_K : K \longrightarrow K$. Entonces $\alpha|_K$ es la identidad en K sí, y sólo si , $\alpha \in Gal(K \rightarrowtail K'')$. Es inmediato comprobar que la función

$$\begin{array}{ccc} Gal(K' \rightarrowtail K'') & \longrightarrow & Gal(K' \rightarrowtail K) \\ \alpha & \longmapsto & \alpha|_K \end{array}$$

es un homomorfismo de grupos con núcleo $Gal(K \rightarrowtail K'')$. Así que obtenemos un monomorfismo

$$Gal(K' \rightarrowtail K'')/Gal(K \rightarrowtail K'') \rightarrowtail Gal(K' \rightarrowtail K)$$

tal que

$$\begin{array}{rcl} o(Gal(K' & \rightarrowtail & K'')/Gal(K \rightarrowtail K'')) = [K' \rightarrowtail K'']/[K \rightarrowtail K''] \\ & = & [K' \rightarrowtail K] = o(Gal(K' \rightarrowtail K)) \end{array}$$

y por lo tanto es un isomorfismo.♦

3.11 Ejemplo. El problema 3.1 y el ejemplo 3.3 nos dicen que

$$Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong V$$

y que los cuatro automorfismos ι,α_1,α_2,α_3 dejan fijo a $\mathbb{Q}$. Los diagramas siguientes ilustran la correspondencia de Galois para la extensión $\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2}, \sqrt{3})$:

$$\begin{array}{ccccc} & & \mathbb{Q}(\sqrt{2}, \sqrt{3}) & & \\ & & | & & \\ \mathbb{Q}(\sqrt{3}) & & \mathbb{Q}(\sqrt{2}) & & \mathbb{Q}(\sqrt{6}) \\ & & | & & \\ & & \mathbb{Q} & & \end{array}$$

$$\begin{array}{ccccc} & & Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2}, \sqrt{3})) & & \\ & & | & & \\ \{\iota, \alpha_1\} & & \{\iota, \alpha_2\} & & \{\iota, \alpha_3\} \\ & & | & & \\ & & \{\iota\} & & \end{array}$$

Consideremos una extensión finita $K' \rightarrowtail K''$ de grado l. Veamos a K'' como espacio vectorial sobre K'. Supongamos que K' tiene q elementos. Luego, cualquier elemento u de K'' puede escribirse en forma única como $u = \lambda_1 v_1 + \cdots + \lambda_l v_l$ para $\{\lambda_i\}_{i=1}^{l} \in K'$ y $\{v_i\}_{i=1}^{l}$ una base de K''. Hay q^l expresiones para u pues cada λ_i puede ser cualquiera de los q elementos de K'. Luego K'' tiene q^l elementos.

Observe que si K'' es un campo finito de característica p, entonces se tiene una extensión $K' \rightarrowtail K''$ donde $K' \cong \mathbb{Z}_p$. Luego K'' tiene p^l elementos, para l un entero positivo, es decir, $|K''| = p^{[\mathbb{Z}_p \rightarrowtail K'']}$.

Ahora, si consideramos el grupo multiplicativo $(K'')^*$ de los elementos distintos de cero de K'', recordemos que tiene orden $p^l - 1$. Si tomamos un elemento $a \in K''$, el orden de a, $o(a)|o((K'')^*) = p^l - 1$. Luego $a^{p^l-1} = 1$ y $a^{p^l} = a$. Por lo tanto, cualquier elemento de K'' es raíz del polinomio $t^{p^l} - t$, el cual tiene a lo más p^l raíces. Así, si K'' está contenido en $\overline{\mathbb{Z}_p}$, los elementos de K'' son las raíces en $\overline{\mathbb{Z}_p}$ del polinomio $t^{p^l} - t \in \mathbb{Z}_p[t]$.

Considere el polinomio $f(t) = t^{p^l} - t \in \mathbb{Z}_p[t]$. Su derivada es $f'(t) = p^l t^{p^l-1} - 1 = -1$. Por el problema 3.4 todas las raíces de $f(t)$ en $\overline{\mathbb{Z}_p}$ son simples. Luego, f posee p^l raíces distintas en $\overline{\mathbb{Z}_p}$. Si $\{0, a_1, ..., a_{p^l-1}\}$ son las

distintas raíces, entonces en $\overline{\mathbb{Z}_p}[t]$, $t^{p^l} - t = t(t-a_1)\cdots(t-a_{p^l-1})$ y cada raíz es simple sobre $\mathbb{Z}_p$.

Denotemos con $\mathbb{F}_{p^l} = \{a \in \overline{\mathbb{Z}_p} \mid f(a) = 0\} \subseteq \overline{\mathbb{Z}_p}$.

3.12 Teorema. $\mathbb{F}_{p^l}$ es un subcampo de $\overline{\mathbb{Z}_p}$ con p^l elementos, $l \geq 1$.

Demostración. Si a,$b \in \mathbb{F}_{p^l}$ entonces $(a+b)^{p^l} - (a+b) = (a^{p^l} + b^{p^l}) - (a+b) = (a^{p^l} - a) + (b^{p^l} - b) = 0$ y $(ab)^{p^l} - (ab) = (a^{p^l} b^{p^l}) - (ab) = ab - ab = 0$. Claramente 0,1 son raíces de $t^{p^l} - t$. Si $a \neq 0$, $a^{p^l} = a$ y $(1/a)^{p^l} = 1/a$. Por lo tanto, $\mathbb{F}_{p^l}$ es un subcampo de $\overline{\mathbb{Z}_p}$.♦

Observe que $\mathbb{Z}_p \leq \mathbb{F}_{p^l}$ y que $\mathbb{Z}_p \rightarrowtail \mathbb{F}_{p^l}$ es una extensión finita. El subcampo $\mathbb{F}_{p^l}$ se llama **campo de Galois** de orden p^l. Se acostumbra denotar a $\mathbb{Z}_p$ con $\mathbb{F}_p$. También se usa la notación $GF(p^l)$ para $\mathbb{F}_{p^l}$ en la literatura sobre este tema. Es claro que $[\mathbb{F}_p \rightarrowtail \mathbb{F}_{p^l}] = l$.

Problemas.

3.1 Compruebe que $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2},\sqrt{3})) = Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2},\sqrt{3})) \cong V$ (el grupo 4 de Klein).

3.2 Pruebe que el grupo de Galois $Gal(K \rightarrowtail K'')$ relativo de las extensiones $(K' \rightarrowtail K)$ y $(K' \rightarrowtail K'')$ es un subgrupo de $Gal(K' \rightarrowtail K'')$, es decir, $Gal(K \rightarrowtail K'') \leq Gal(K \rightarrowtail K'')$ cuyo orden $o(Gal(K \rightarrowtail K'')) = [K' \rightarrowtail K'']$.

3.3 Recuerde que [A-D-Ll-M p.107] una acción de un grupo G en un conjunto X es **transitiva** si para cualesquiera x,$y \in X$ existe $g \in G$ tal que $gx = y$. También decimos que la acción es **libre** si solamente para $g = e \in G$ se tiene que $gx = x$, de otra manera, si para cuando $g \neq e \in G$, $gx \neq x$. Pruebe que si $K' \rightarrowtail K''$ es una extensión de Galois finita donde K'' es el campo de descomposición de un polinomio irreducible $f \in K'[t]$ de grado n entonces el grupo $Gal(K' \rightarrowtail K'')$ actúa transitiva y libremente en $R(f, K'')$.

3.4 Considere el anillo de polinomios $K[t]$ para un campo K. Se define la **derivada** $\partial : K[t] \longrightarrow K[t]$ dada por $\partial(f(t)) = \partial(\lambda_n t^n + \cdots + \lambda_2 t^2 + \lambda_1 t^1 + \lambda_0) = n\lambda_n t^{n-1} + \cdots + 2\lambda_2 t^1 + \lambda_1 = f'(t)$; $\lambda_i \in K$. Pruebe que si $f \in K[t]$

posee una raíz $a \in K''$ para una extensión $K \rightarrowtail K''$, entonces a es una raíz múltiple de f si, y sólo si, f y f' poseen un factor lineal común en $K[t]$ que se anula en a.

3.5 Pruebe el teorema del elemento primitivo para el caso en que K'' sea finito.

3.6 Pruebe que $\mathbb{F}_{p^l} \leq \overline{\mathbb{F}_p}$ es el subcampo de descomposición para los polinomios $t^{p^l} - t$ y $t^{p^l-1} - 1$ sobre $\mathbb{F}_p$.

3.7 Pruebe que $\mathbb{F}_{p^l}$ es el único subcampo (salvo isomorfismo) con p^l elementos.

3.8 Considere $\mathbb{F}_{p^k}$ y $\mathbb{F}_{p^l}$ dos campos de Galois de característica p. Pruebe que $\mathbb{F}_{p^k}$ es subcampo de $\mathbb{F}_{p^l}$ si, y sólo si, k divide a l.

3.9 Dibuje un diagrama de los subcampos de $\mathbb{F}_{p^{60}}$ ordenados via la divisibilidad por $l = 60$.

Bibliografía y Referencias

[Am] Amiot, E. Rhythmic Canons and Galois Theory. H. Fripertinger, L. Reich (Eds.). Colloquium on Mathematical Music Theory. Grazer Math. Ber. Bericht Nr. 347. (2005).

[A-D-Ll-M] Agustín-Aquino, O., du Plessis, J., Lluis-Puebla, E., Montiel, M. Una introducción a la Teoría de Grupos con aplicaciones en la Teoría Matemática de la Música. Pub. Electr. Sociedad Matemática Mexicana. Serie textos. Vol. 10 (2009).

[A-Ll1] Aceff, F., Lluis-Puebla, E. Matemática en la Matemática, Música, Medicina y Aeronáutica. Pub. Electr. Sociedad Matemática Mexicana. Serie Divulgación. Vol. 1 (2006).

[A-Ll2] Aceff, F., Lluis-Puebla, E. Matemática en la Matemática II, Música II, Naturaleza y Nuestro Cuerpo. Pub. Electr. Sociedad Matemática Mexicana. Serie Divulgación. Vol. 2 (2007).

Artin E. Galois Theory. (1944 Segunda Ed.) Dover. (1998).

Baker, A. An Introduction to Galois Theory. www.maths.gla.ac.uk/~ajb/dvi-ps/Galois.pdf (2007).

Bewersdorff, J. Galois Theory for Beginners. Student Math. Library. Vol. 35. American Mathematical Society. (2006).

Birkhoff, G. MacLane, S. Algebra.Macmillan. (1968).

Bourbaki, N. Algebra I. Addison Wesley. (1973).

[F] Fraleigh, J.B. Abstract Algebra. Seventh Edition. Addison Wesley. (2003).

Hu, S-T. Elements of Modern Algebra. Holden-Day. (1965).

Hungerford, T.W. Algebra. Springer. (1980).

Lang, S. Algebra. Addison Wesley. (1965).

[Ll1] Lluis-Puebla, E. Álgebra Homológica. Addison Wesley Ib. (1990).

[Ll2] Lluis-Puebla, E. Álgebra Lineal. Sitesa. (1997).

[Ll3] Lluis-Puebla, E. Teoría de Grupos, un primer curso. Pub. Electr. Sociedad Matemática Mexicana. Vol. 6 (2006).

[Ll-M-N] Lluis-Puebla, E., Mazzola, G. and Noll, T. (Eds.). Perspectives in Mathematical and Computational Music Theory. EpOs, 149–164, Universität Osnabrück. (2004).

Milne, J.S. Fields and Galois Theory. www.jmilne.org/math/CourseNotes/ft.html. (2003).

Morandi, P. Field and Galois Theory. Graduate Texts in Mathematics Vol. 167. Springer. (1996).

Rotman, J.J. Galois Theory. Second Edition. Universitext, Springer. (2001)

Snaith, V.P. Groups, Rings and Galois Theory. World Scientific. (2003).

Stewart, I. Galois Theory. Chapman & Hall. (2004).

Lista de Símbolos

$(\Lambda, +, \cdot)$	9
1	10
$^{o}\Lambda$	10
$\Gamma < \Lambda$	10
$\ker\, f$	13
f^{-1}	13
$f : \Lambda \overset{\cong}{\to} \Lambda'$	13
$\Lambda \cong \Lambda'$	13
$im\ f$	13
$f : \Lambda \rightarrowtail \Lambda'$	13
$f : \Lambda \twoheadrightarrow \Lambda'$	13
ι	14
$End(G, G)$	14
f^{-1}	15
$car\,(\Lambda) = 0$	18
$car\,(\Lambda) = n$	18
$x + I$	19
Λ / I	20
p	20
(Π, f, t)	25
f_x	26
$\Lambda\,[t]$	27
$gr\,(\varphi)$	27
E_a	27
$f^{@}$	28
$\langle S \rangle$	28
$\langle t_1, ..., t_n \rangle$	28
Ξ	30
(K, f)	30
$t^n - 1 = \Pi_{d\mid n} \Phi_d(t)$	35
$K' \rightarrowtail K$	38
$K' \leq K$	38
$K : K'$	38
$K' < K$	38
$\begin{matrix} K \\ \mid \\ K' \end{matrix}$	38
$(K' \rightarrowtail K) \leq (K' \rightarrowtail K'')$	39
$[K' \rightarrowtail K]$	39
$K'\,(X)$	42
$K'\,(a_1, ..., a_j)$	42
$K' \rightarrowtail K'\,(a_1, ..., a_j)$	42
$\underline{gr\,(a, K')}$	45
$\overline{K'_K}$	47
$\overline{K'}$	47
$Aut\,(\Lambda)$	49
$Aut_\Gamma\,(\Lambda)$	49
K'_f	50
$\hom_{K'}(K, K'')$	51
$Aut_{K'}\,(K'', K'')$	51
$R\,(f, K'')$	51
$\{K' \rightarrowtail K''\}$	53
$Gal\,(K' \rightarrowtail K'')$	58
$(K'')^H$	59
$(K'')^{\{\varphi_i\}}$	59

$Subgr\,(K' \rightarrowtail K'')$	60	$GF(p^l)$	64
$Subext\,(K' \rightarrowtail K'')$	60	∂	64
$\mathbb{F}_p$	64		

Índice Analítico

A

acción
- libre 64
- transitiva 64

algebraica(o)
- cerradura 47
- elemento 44
- número 45
- extensión 45

anillo 9
- característica de un 18
- cociente sobre su ideal I 20
- con uno 10
- con división 10
- con identidad 10
- conmutativo 10
- de característica 0 18
- de polinomios de Λ 25
- opuesto 10

anillos
- homomorfismo de 12
- ismorfismo de 13
- isomorfos 13

automorfismo 13, 49
- de Λ sobre Γ 49
- de Galois 58

B

base 28

C

campo 10
- base de una extensión 37
- de cocientes con s indeterminadas 31
- de cocientes de Δ 30
- de descomposición 50
- de funciones racionales con s indeterminadas 31
- de Galois 64
- extensión de un 37
- intermedio 40

campos primos 32

característica
- 0 18
- de un anillo 18

cero de un polinomio 28

cerradura algebraica 47

clases laterales 19

cociente de
- anillo sobre su ideal 20
- grupos 19

coeficiente inicial 27

coeficientes del polinomio 27

combinaciones lineales 28

constantes 27
criterio de Einsenstein 32

D
derivada 64
divisores de cero 10
dominio de ideales principales 28
dominio entero 10

E
elemento
  algebraico 44
  grado de un 45
  invertible por la derecha 17
  invertible por la izquierda 17
  primitivo 55
  separable 53
  trascendente 45
elementos conjugados 52
endomorfismo 13
epimorfismo 13
extensión
  algebraica 45
  de Galois 58
  de K de K' 38
  de K' en K 38
  de un campo 37
  elemento primitivo de una 55
  finita 40
  finita separable 53
  finitamente generada 42
  generada por 42
  infinita 40
  K de K' 38
  normal 54
  simple 42
  trascendente 45
extensiones isomorfas 39

F
finita
  extensión 40
    separable 53
finitamente generada(o)
  extensión 42
  ideal 28
función polinomial 28

G
Galois
  campo de 64
  extensión 58
  grupo 58, 60
generadores del ideal 28
grado
  de K sobre K' 39
  de separabilidad de una extensión 53
  de un elemento sobre K' 45
  de un polinomio 27
grupo
  cociente 19
  de Galois de una extensión 58
  de Galois relativo a las extensiones 60

H
homomorfismo
  de anillos 12
  de evaluación o sustitución 27
  de identidad 14
  inducido por f 21
  trivial 13

I
ideal 11
  base del 28

de Λ generado por S 28
derecho 11
finitamente generado 28
izquierdo 11
maximo 29
primo 29
principal 28
ideales
propios no triviales 12
triviales 11
imagen de f 13
inclusión 14
indeterminada 27
inverso
de f 13
derecho 17
izquierdo 17
invertible 17
por la derecha 17
por la izquierda 17
isomorfas(os)
anillos 13
extensiones 39
isomorfismo 13
isomorfismo de anillos 13

L
ley distributiva 9

M
monomorfismo 13

N
núcleo de f 13
número
algebraico 45
trascendente 45

P
polinomio
cero de un 28
mínimo 45
raíz de un 28
separable sobre K 53
polinomios
ciclotómicos 35
en la indeterminada t con coeficientes en el anillo Λ 27
Primer teorema de isomorfismo 22
proyección canónica 20

R
raíces n-ésimas de la unidad 35
raíz
de multiplicidad n 57
de un polinomio 28

S
Segundo teorema de isomorfismo 23
separable
elemento 53
extensión finita 53
polinomio 53
subanillo 10
de Λ generado por S 28
de Λ generado por S 28
subcampo 11
fijo 59
fijo de una familia 59
generado por S 18
obtenido por adjunción de un conjunto 42
subdominio 11
generado por S 18
subextensión de campos 39

T

Teorema
  de isomorfismo
    Primer 22
    Segundo 23
    Tercer 23
  de Kronecker 44
  del elemento primitivo 55
Tercer teorema de isomorfismo 23
término constante 27
trascendente
  elemento 45
  extensión 45
  número 45

U
unidad 17