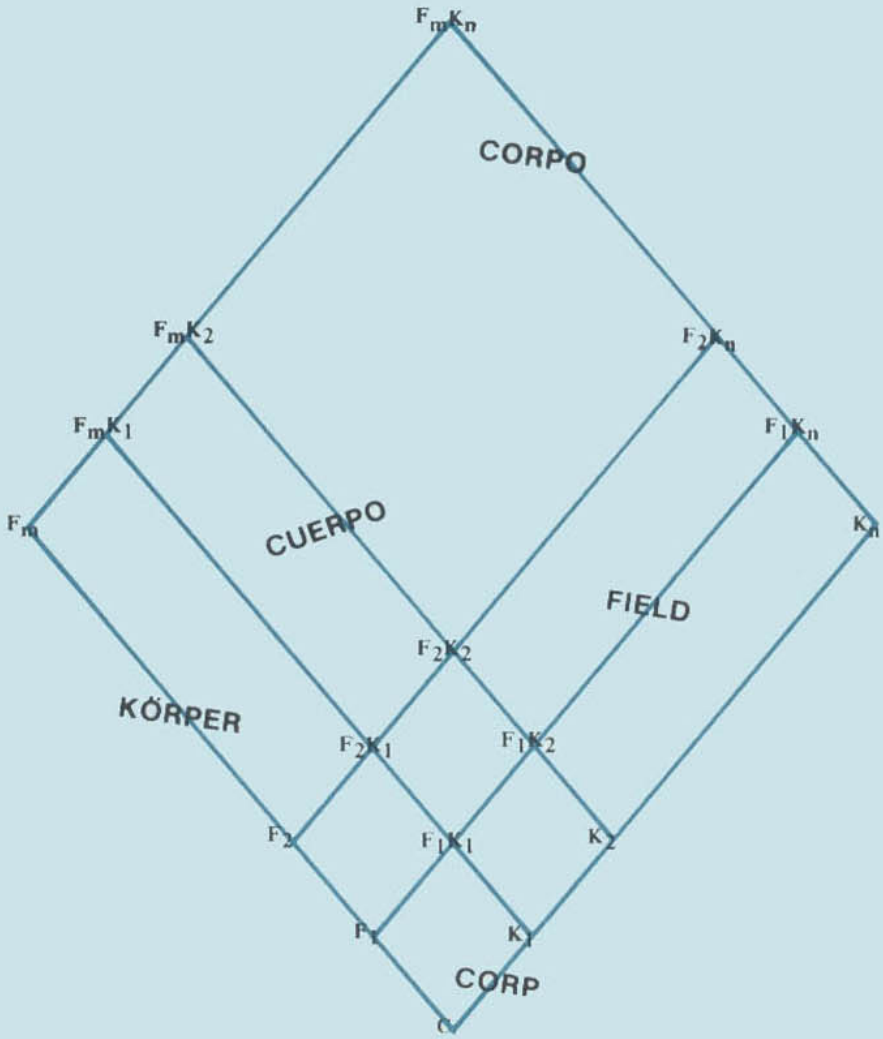
serie de matemática

monografía no. 22

ESTRUCTURAS ALGEBRAICAS V (TEORIA DE CUERPOS)

Secretaría General de la
Organización de los Estados Americanos
Programa Regional de Desarrollo Científico y Tecnológico



ESTRUCTURAS ALGEBRAICAS V
(TEORIA DE CUERPOS)

por

Héctor A. Merklen
Instituto de Matemática e Estatística
Universidade de São Paulo
São Paulo, BRASIL

Secretaría General de la
Organización de los Estados Americanos
Programa Regional de Desarrollo Científico y Tecnológico
Washington, D.C. - 1979

Esta monografía ha sido preparada para su publicación en el Departamento de Asuntos Científicos de la Secretaría General de la Organización de los Estados Americanos

Editora: Eva V. Chesneau

Asesor Técnico: Dr. Francisco Mario Piscoya H.
Lima, Perú

A los lectores

El programa de monografías científicas es una faceta de la vasta labor de la Organización de los Estados Americanos, a cargo del Departamento de Asuntos Científicos de la Secretaría General de dicha Organización, a cuyo financiamiento contribuye en forma importante el Programa Regional de Desarrollo Científico y Tecnológico.

Concebido por los Jefes de Estado Americanos en su Reunión celebrada en Punta del Este, Uruguay, en 1967, y cristalizado en las deliberaciones y mandatos de la Quinta Reunión del Consejo Interamericano Cultural, llevado a cabo en Maracay, Venezuela, en 1968, el Programa Regional de Desarrollo Científico y Tecnológico es la expresión de las aspiraciones preconizadas por los Jefes de Estado Americanos en el sentido de poner la ciencia y la tecnología al servicio de los pueblos latinoamericanos.

Demostrando gran visión, dichos dignatarios reconocieron que la ciencia y la tecnología están transformando la estructura económica y social de muchas naciones y que, en esta hora, por ser instrumento indispensable de progreso en América Latina, necesitan un impulso sin precedentes.

El Programa Regional de Desarrollo Científico y Tecnológico es un complemento de los esfuerzos nacionales de los países latinoamericanos y se orienta hacia la adopción de medidas que permitan el fomento de la investigación, la enseñanza y la difusión de la ciencia y la tecnología; la formación y perfeccionamiento de personal científico; el intercambio de informaciones, y la transferencia y adaptación a los países latinoamericanos del conocimiento y las tecnologías generadas en otras regiones.

En el cumplimiento de estas premisas fundamentales, el programa de monografías representa una contribución directa a la enseñanza de las ciencias en niveles educativos que abarcan importantísimos sectores de la población y, al mismo tiempo, propugna la difusión del saber científico.

La colección de monografías científicas consta de cuatro series, en español y portugués, sobre temas de física, química, biología y matemática. Desde sus comienzos, estas obras se destinaron a profesores y alumnos de ciencias de los primeros años de la universidad; de estos se tiene ya testimonio de su buena acogida.

Esta introducción brinda al Programa Regional de Desarrollo Científico y Tecnológico de la Secretaría General de la Organización de los Estados Americanos la ocasión de agradecer al doctor Héctor A. Merklen, autor de esta monografía, y a quienes tengan el interés y buena voluntad de contribuir a su divulgación.

Marzo de 1979

ÍNDICE

Página

1

POLINOMIOS

1. CONSTRUCCIÓN Y PRIMERAS PROPIEDADES

Introducción

Intuitivamente, los *polinomios* son *símbolos* construidos con letras y números ligados por las operaciones de adición, sustracción y multiplicación. Por ejemplo:

$$X^2 + Y^2 + Z^2 \quad \text{o} \quad X^3 + 2X^2 + 4X + 8.$$

Aparecen con frecuencia al simbolizar términos algebraicos que implican variables lógicas. Su importancia es tal que justifica el desarrollo de una teoría matemática sobre ellos.

La teoría matemática de los polinomios es un modelo matemático de aquellos símbolos, mediante el cual se pretende captar sus características esenciales y obtener las propiedades que de éstas se deduzcan. No puede esperarse que el ente matemático "polinomio" sea el ente intuitivo "polinomio". El polinomio matemático es apenas un objeto convenientemente definido para reflejar en sus propiedades el contenido semántico del polinomio intuitivo.

Vamos a construir este modelo. En primer lugar, es preciso delimitar el dominio de los coeficientes numéricos, los cuales deben formar un conjunto dotado de operaciones de adición, sustracción y multiplicación caracterizadas por las propiedades usuales. Es decir, el conjunto de los coeficientes debe ser un anillo. Para simplificar, se supondrá que los coeficientes forman un anillo R, conmutativo y de identidad 1.

En segundo lugar, hay que especificar las letras o variables que se usarán. Para nuestros propósitos será suficiente suponer que las letras forman el conjunto finito: $\mathcal{X} = \{X_1, X_2, \ldots, X_n\}$. Los casos más importantes corresponden a $n = 1, 2, 3$ y para ellos se usará, respectivamente, la notación $\mathcal{X} = \{X\}, \{X, Y\}, \{X, Y, Z\}$.

En tercer lugar, cabe mencionar la conveniencia de hacer la construcción en dos etapas, primero introduciendo los *monomios* que son los términos con que se construyen, después los polinomios. Se piensa aquí en monomios sin coeficientes:

$$M = X_1^{e_1} X_2^{e_2} \ldots X_n^{e_n} \quad (e_i \in \mathbb{N})$$

pues así se puede concentrar la atención en la parte literal, lo que permite captar mejor el papel que desempeñan las letras.

Es claro que cada monomio, M, puede ser perfectamente representado por la familia de exponentes: $(e_1, e_2, \ldots, e_n) \in \mathbb{N}^n$. Pero una adopción precipitada de esta idea llevaría a perder totalmente las letras. Tratando de nuevo, se ve que también se puede representar por una función $\mathcal{X} \to \mathbf{N}$:

$$X_1 \to e_1$$

$$X_2 \to e_2$$

$$\vdots$$

$$X_n \to e_n$$

Esta representación es preferible porque permite dar cuenta fácilmente tanto de la estructura algebraica de los monomios como del papel que las letras desempeñan.

Intuitivamente un polinomio es una combinación lineal de monomios, de coeficientes en R. Por ejemplo,

$P = 3XYZ - 2X^2Y + 4XZ$ se escribe: $P = 3M_1 - 2M_2 + 4M_3$, donde

$M_1 = XYZ$, $M_2 = X^2Y$, $M_3 = XZ$.

Si se procede por analogía con el caso de los monomios, considerando que cada polinomio está determinado si se conoce el coeficiente de cada uno de los monomios que lo forman, tentaríamos representar cada polinomio por una función cuyo dominio es un conjunto finito de monomios y que tienen sus valores en R. Así, se representaría el polinomio P por la función:

$$P : \{M_1, M_2, M_3\} \to R$$

$$M_1 \to 3$$

$$M_2 \to -2$$

$$M_3 \to 4$$

Pero esto introduciría dificultades innecesarias debidas a la heterogeneidad de los objetos (funciones con una infinidad de dominios diferentes). La manera obvia de superarlas consiste en llamar polinomios, no a las funciones de la forma $P : D \to R$, donde D es un conjunto finito de monomios, sino a las funciones $P : \mathcal{M} \to R$ (con dominio en el conjunto $\mathcal{M}$ de todos los monomios) que tienen soporte finito, es decir tales que existe un subconjunto finito, D, de $\mathcal{M}$, tal que $P(M) = 0$ para todo M que no pertenece a D.

Éste es el modelo que desarrollaremos. Cabe al lector atento percibir cómo se traducen en el modelo las propiedades algebraicas y cómo se da cabida al papel que desempeñan las letras, incluyendo la posibilidad de sustituir éstas por objetos de una estructura algebraica en que el enunciado polinomial tenga sentido.

Monomios

Sea $\mathcal{X} = \{X_1, \ldots, X_n\}$ un conjunto cualquiera, a cuyos elementos llamaremos *letras*.

Sea $\mathcal{M}$ el semigrupo conmutativo de las funciones de $\mathcal{X}$ en $\mathbb{N}$, denotado en forma multiplicativa. Es decir, si M y N, son dos de tales funciones, MN es la función que a cada X_i hace corresponder $M(X_i) + N(X_i)$; y 1 es la función idénticamente igual a 0.

Sea $\iota: \mathcal{X} \to \mathcal{M}$ la aplicación que a cada X_i asocia la función $X_j \mapsto \delta_{ij} (j = 1, \ldots n)$ (donde δ_{ij} es el "delta de Kronecker", un símbolo que vale 1 cuando $j = i$ y 0 cuando $j \neq i$). La aplicación ι es inyectiva.

Se tiene la importante identidad siguiente:

$$\forall M \in \mathcal{M} : \quad M = \prod_{i=1}^{n} (\iota_{X_i})^{M(X_i)} \qquad [1]$$

es decir: $\mathcal{M}$ es generado por la imagen de ι. Y, más aún, [1] es la única forma (salvo el orden de los factores) de expresar M como producto de monomios de la forma ι_{X_i}. Esto es:

$$\forall M \in \mathcal{M} : \quad M = \prod_{i=1}^{n} (\iota_{X_i})^{e_i} \text{ implica}$$

$$e_i = M(X_i) (\forall i = 1, \ldots, n) \qquad [2]$$

La igualdad [1] se demuestra calculando el valor de la función de la derecha en un X_j arbitrario:

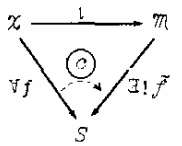
$$\left(\prod_{i=1}^{n} (\iota_{X_i})^{M(X_i)}\right)(X_j) = \sum_{i=1}^{n} M(X_i)\delta_{ij} = M(X_j)$$

La proposición [2] resulta inmediatamente de un cálculo similar.

La función ι tiene la propiedad fundamental siguiente:

> Dado un semigrupo conmutativo cualquiera, S, y una aplicación $f: \mathcal{X} \to S$, existe un único homomorfismo $\tilde{f}: \mathcal{M} \to S$, tal que $f = \tilde{f}\iota$. [3]

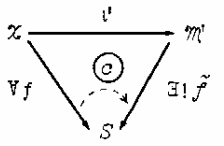
En símbolos:



[4]

En efecto, la condición exigida determina $\tilde{f}$ pues ella implica que $\tilde{f}(\iota_{X_i}) = f(X_i)$, y la imagen de ι genera $\mathcal{M}$. Por otra parte, basta definir $\tilde{f}(\prod_{i=1}^{n} (\iota_{X_i})^{e_i}) = \prod_{i=1}^{n} (f(X_i))^{e_i}$ (lo que es legítimo por [2]) para tener una función que verifica [4] y que es un homomorfismo de semigrupos.

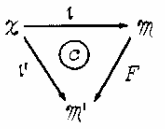
Véase ahora que la propiedad fundamental [3] determina ι salvo isomorfismo. Esto es: si $\iota' : \mathcal{X} \to \mathcal{M}'$ es una aplicación de $\mathcal{X}$ en un semigrupo $\mathcal{M}'$ que verifica

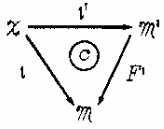


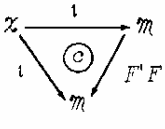
[5]

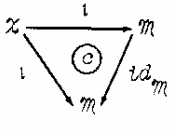
entonces existe un isomorfismo F de $\mathcal{M}$ sobre $\mathcal{M}'$ tal que $\iota' = F\iota$.

En efecto, si valen [4] y [5], se tiene:









lo que implica $F'F = id_{\mathcal{M}}$. Análogamente se ve que $FF' = id_{\mathcal{M}'}$, y, por lo tanto, F y F' son isomorfismos inversos entre sí.

Definición 1. *Cada función* ι de $\mathcal{X}$ *en un semigrupo* $\mathcal{M}$ *que verifica* [3] *se llama,* por abuso de lenguaje, *semigrupo de los monomios en las letras de* $\mathcal{X}$.

Salvo isomorfismo, existe un único semigrupo de monomios en $X_1, X_2, \ldots, X_n$. Por eso se habla de *el* semigrupo de los monomios en $X_1, \ldots, X_n$. Si no hay posibilidades de confusión se adoptarán las convenciones siguientes:

$\mathcal{M}$ es el semigrupo de los monomios en $X_1, \ldots X_n$:

los elementos de $\mathcal{M}$ se llaman monomios;

los monomios ι_{X_i} se denotan, respectivamente, X_i (así, cada letra es también un monomio);

con esta identificación, ι es la inclusión $\mathcal{X} \hookrightarrow \mathcal{M}$;

cada monomio, M, tiene una expresión única de la forma:

$$M = X_1^{e_1} X_2^{e_2} \ldots X_n^{e_n} (e_i \in \mathbb{N})$$

Nota. La definición 1 se aplica también si $\mathcal{X}$ es infinito. El semigrupo $\mathcal{M}$ se construye como antes, excepto que no todas las funciones M de $\mathcal{X}$ en $\mathbb{N}$ son monomios, sino solamente las que tienen como máximo un número finito de valores distintos de 0 (o sea: sólo las que tienen so-

porte finito). Las restantes consideraciones se extienden sin dificultad al caso en que $\mathcal{X}$ es infinito.

La propiedad [3], fundamental de los monomios, tiene una interpretación interesante. Dar una función f de $\mathcal{X}$ en S equivale a dar elementos $x_1, x_2, \ldots, x_n$ de S en correspondencia con las letras $X_1, X_2, \ldots, X_n$. Entonces [3] significa que, dados los x_i, existe un único homomorfismo, $\bar{f}$, que lleva X_i en x_i ($\forall i = 1, \ldots, n$). Este homomorfismo está dado por:

$$X_1^{e_1} \ldots X_n^{e_n} \mapsto x_1^{e_1} \ldots x_n^{e_n}$$

es decir, consiste en sustituir cada letra por el elemento correspondiente de S. Por eso, $\bar{f}$ se llama la *función de evaluación* de los monomios en los x_i. *Notación:* $\mathrm{ev}_{(x_1, \ldots, x_n)}$.

Además, la unicidad de $\bar{f}$ permite asociar a cada monomio M una función de $\underbrace{Sx\,Sx \ldots xS}_{n}$ en S:

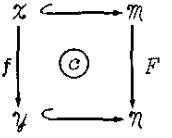
$$\bar{M} : \underbrace{Sx\,Sx \ldots xS}_{n} \to S$$

$$(x_1, \ldots, x_n) \mapsto \mathrm{ev}_{(x_1, \ldots, x_n)}(M)$$

Por ejemplo, si $M = X_1^{e_1} \ldots X_n^{e_n}$, la función $\hat{M}$ está dada por:

$$(x_1, \ldots, x_n) \mapsto x_1^{e_1} \ldots x_n^{e_n}$$

Observación 1. Si $\mathcal{X} \hookrightarrow \mathcal{M}$, $\mathcal{Y} \hookrightarrow \mathcal{N}$ son dos semigrupos de monomios, cada aplicación conjuntística $f : \mathcal{X} \to \mathcal{Y}$ induce un homomorfismo $F : \mathcal{M} \to \mathcal{N}$, el único tal que:



F es el homomorfismo que, por [3], corresponde a la aplicación compuesta $\mathcal{X} \xrightarrow{f} \mathcal{Y} \hookrightarrow \mathcal{N}$.

En esta forma el homomorfismo que corresponde a la aplicación identidad de $\mathcal{X}$, es la identidad de $\mathcal{M}$. Si $f : \mathcal{X} \to \mathcal{Y}$ induce $F : \mathcal{M} \to \mathcal{N}$ y si $g : \mathcal{Y} \to \mathcal{Z}$ induce $G : \mathcal{N} \to \mathcal{O}$, entonces $gf : \mathcal{X} \to \mathcal{Z}$ induce $GF : \mathcal{M} \to \mathcal{O}$. Por lo tanto:

si f es inyectiva, F es inyectiva;

si f es epiyectiva, F es epiyectiva;

si f es biyectiva, F es biyectiva.

Álgebras

Para simplificar la exposición convendremos que, salvo mención expresa de lo contrario, "anillo" significa "anillo con identidad 1";

"homomorfismo de anillos" significa "homomorfismo de anillos que lleva 1 en 1".

Definición 2. *Sea R un anillo conmutativo. Llámase R-álgebra a todo homomorfismo α de R en el centro de un anillo A.*

Cuando no hay posibilidades de confusión se llama R-álgebra al anillo A.

Sea $\alpha : R \to A$ una R-álgebra. La aplicación

$$(r, a) \mapsto \alpha(r)a \quad (r \in R,\ a \in A)$$

define en A una estructura de R-módulo (que se dice asociada al álgebra) y es costumbre escribir ra en vez de $\alpha(r)a$. También, con un poco de negligencia, se suele hablar del elemento "r" de A, y se quiere decir el elemento "$r \cdot 1$" (o el elemento $\alpha(r)$) de A. O se dice que r es un elemento de R (un escalar de R) pensado como elemento de A.

Por ejemplo, todo anillo A es una $\mathbb{Z}$-álgebra a través del homomorfismo que aplica el 1 de $\mathbb{Z}$ en el 1 de A (y que lleva cada entero n en el elemento $n \cdot 1$). El núcleo de este homomorfismo es un ideal de $\mathbb{Z}$ cuyo generador en $\mathbb{N}$ se llama la *característica* de A. *Notación:* $\chi(A)$.

Decir que A tiene característica 0 es lo mismo que decir que los
6 múltiplos de 1 y sus opuestos forman un subanillo de A isomorfo a $\mathbb{Z}$: los anillos de característica 0 contienen a $\mathbb{Z}$. Por consiguiente, los cuerpos de característica 0 contienen a $\mathbb{Q}$.

Decir que A tiene característica $h > 0$ equivale a decir que:

$$\forall n \in \mathbb{N} : n \cdot 1 = 0 \text{ (en } A) \Leftrightarrow h \mid n \text{ (en } \mathbb{Z})$$

O sea que los múltiplos de h, considerados como elementos de A, son iguales a 0. En este caso, la característica h se puede definir como el mínimo número de veces que es necesario repetir el sumando 1 para obtener 0 en A.

Si A es *íntegro* (es decir, no tiene divisores de 0) $\mathbb{Z} \cdot 1 \subset A$ es íntegro y, por lo tanto, el ideal generado por la característica de A es primo en $\mathbb{Z}$. Quiere decir que la característica de un anillo íntegro es 0 o es un número primo. En particular, la característica de un cuerpo es 0 o es un número primo.

Si R es un cuerpo y A una R-álgebra, entonces A, como R-módulo, es un R-espacio vectorial. Quiere decir que la terminología usual de espacios vectoriales es aplicable a A. Por ejemplo, tiene sentido hablar de la *dimensión* de A.

Si R es un cuerpo y $\dim_R A < \infty$, se dice que A es una *R-álgebra finita*.

El ejemplo 1 muestra cómo puede efectuarse el proceso inverso de definir el álgebra a partir de la estructura de módulo.

Ejemplo 1. Sea A un R-módulo libre con base B. Sea $m : B \times B \to A$ una función cualquiera, denotada por $m(b, b') = bb'$, con la siguiente propiedad de asociatividad:

$$(bb')b'' = b(b'b'') \quad (\forall b, b', b'' \in B)$$

En tal caso existe en A una estructura de anillo, tal vez sin elemento 1, cuya multiplicación coincide con m en $B \times B$.

En efecto, definamos una multiplicación en A mediante:

$$\left(\sum_i r_i b_i\right)\left(\sum_j s_j b'_j\right) = \sum_{i,j} r_i s_j b_i b'_j$$

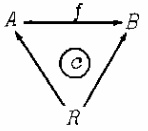
(donde r_i y s_j están en R, y b_i y b'_j están en B).

Esto es posible, pues cada elemento de A es una combinación lineal única de B con coeficientes en R.

Un cálculo directo muestra que esta multiplicación es asociativa y doblemente distributiva con relación a la suma de A. Si esta multiplicación tiene elemento neutro, 1, A es un anillo en nuestro sentido y existe una única estructura de R-álgebra $R \to A$ que induce en A su estructura original de R-módulo.

Nótese que para que esta R-álgebra sea conmutativa es necesario y suficiente que m sea conmutativa, es decir, que $bb' = b'b$ para todo par de elementos de la base B. 7

Definición 3. *Sean R un anillo conmutativo y $R \to A$ y $R \to B$ dos R-álgebras. Una aplicación $f : A \to B$ es un homomorfismo de R-álgebras cuando es un homomorfismo de anillos tal que*



Esta condición equivale a que $f(r \cdot 1_A) = r \cdot 1_B$ para todo r de R. En otras palabras, para que f sea un homomorfismo de R-álgebras es necesario y suficiente que sea, a la vez, un homomorfismo de anillos y un homomorfismo de R-módulos.

Polinomios

Sea R un anillo conmutativo y sea $\mathcal{X} \hookrightarrow \mathcal{M}$ un semigrupo de monomios ($\mathcal{X} = \{X_1, X_2, \ldots X_n\}$). En[4], cap. 4, ejemplo 2', se mostró que existe un R-módulo libre, $\mathcal{P}$, y una inyección $\mu : \mathcal{M} \to \mathcal{P}$ cuya imagen es una base de $\mathcal{P}$. Usemos las consideraciones del ejemplo 1 para definir una estructura de R-álgebra en $\mathcal{P}$. Definimos:

$$m : \operatorname{Im}\mu \times \operatorname{Im}\mu \to \mathcal{P}$$

por

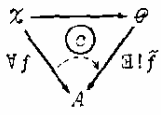
$$\mu(M) \cdot \mu(N) = \mu(MN)$$

Entonces esta función induce en $\mathcal{O}$ una estructura de álgebra conmutativa que tiene como identidad 1 el elemento neutro $\mu(1)$, imagen del elemento 1 de los monomios. La aplicación $r \to r \cdot 1$ que define el R-álgebra $\mathcal{O}$ es inyectiva (porque $\mathcal{O}$ es R-libre). La restricción de μ a $\mathcal{X}$ es también una inyección que se denota por $\iota : \mathcal{X} \to \mathcal{O}$.

La función ι tiene la propiedad fundamental siguiente:

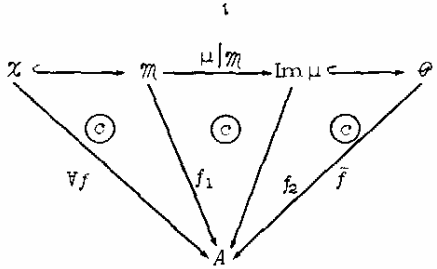
Dada una R-álgebra conmutativa, A, y una aplicación $f : \mathcal{X} \to A$, existe un único homomorfismo de R-álgebras $\tilde{f} : \mathcal{O} \to A$ tal que $f = \tilde{f}\iota$. [6]

En símbolos:



[7]

La demostración se basa en la propiedad [3] de los monomios y, en líneas generales, es semejante a la demostración de [3]. Dada f, existe una única forma de completar el siguiente diagrama con morfismos f_1, f_2, $\tilde{f}$:



[8]

El homomorfismo de semigrupos, f_1, se determina por f, por [3]; el homomorfismo de semigrupos, f_2, está determinado por la conmutatividad de ese triángulo, porque $\mu|\mathcal{M}$ es un isomorfismo; la aplicación R-lineal, $\tilde{f}$, está determinada por la conmutatividad del último triángulo por ser Im μ una base de $\mathcal{O}$. Ahora, esta $\tilde{f}$ que, en principio, sólo es un homomorfismo de R-módulos, resulta ser también, por la definición de la multiplicación en $\mathcal{O}$, un homomorfismo de anillos. Luego, $\tilde{f}$ es un homomorfismo de R-álgebras, y de [8] se deduce que $f = \tilde{f}\iota$.

La unicidad de $\tilde{f}$ se prueba así. Si $\tilde{f}'$ verifica [7] en vez de $\tilde{f}$, su restricción a Im μ, compuesta con la inversa de $\mu|\mathcal{M}$, hace conmutar el primer triángulo de [8]. Luego, esta función coincide con f_1 (por [3]) y, por lo tanto, la restricción de $\tilde{f}'$ a Im μ coincide con f_2. Entonces, dado que $\tilde{f}'$ es una aplicación R-lineal que coincide con $\tilde{f}$ en una base de su dominio, resulta que $\tilde{f}'$ es igual a $\tilde{f}$.

Procediendo como en el caso de los monomios, se demuestra fácilmente que la propiedad [6] determina la R-álgebra $\mathcal{X} \xrightarrow{\iota} \mathcal{P}$, salvo isomorfismo. Esto es: si $\mathcal{X} \xrightarrow{\iota'} \mathcal{P}'$ es un R-álgebra que verifica [6], entonces existe un isomorfismo F de $\mathcal{P}$ sobre $\mathcal{P}'$ tal que $\iota' = F\iota$.

Definición 4. *Cada R-álgebra $\mathcal{P}$, junto con una aplicación $\iota : \mathcal{X} \to \mathcal{P}$ que verifica* [6], *se llama una R-álgebra de polinomios en las letras de $\mathcal{X}$.*

Salvo isomorfismo hay una única R-álgebra de polinomios en $X_1, X_2, \ldots, X_n$. Por eso se habla de *el* álgebra de polinomios en X_1, $X_2, \ldots, X_n$ con coeficientes en R. *Notación:* $R[X_1, X_2, \ldots, X_n]$.

Como μ es inyectiva, identificamos cada monomio M con $\mu(M)$ y, en particular, cada letra X_i con el polinomio $\mu(X_i)$. Entonces ι simplemente una inclusión: $\mathcal{X} \hookrightarrow \mathcal{P}$.

Cada polinomio, es decir cada elemento de $\mathcal{P}$, es una combinación lineal de monomios con coeficientes en R. Como $\mathcal{M}$ es una base de $\mathcal{P}$, dos polinomios son iguales si, y sólo si, tienen coeficientes iguales para monomios iguales.

Si $P \in R[X_1, X_2, \ldots, X_n]$, es conveniente adoptar la notación $P(X_1, X_2, \ldots, X_n)$ para indicar el símbolo que expresa P como combinación lineal de monomios en las letras $X_1, X_2, \ldots, X_n$.

La propiedad fundamental de los polinomios, [6], tiene la interesante interpretación siguiente:

Para definir un homomorfismo, f, de la R-álgebra $R[X_1, X_2, \ldots, X_n]$ en una R-álgebra conmutativa A basta escoger una familia de elementos de A en correspondencia con las letras: $X_i \mapsto x_i$, $x_i \in A$. Entonces existe un único f que lleva cada X_i en x_i.

El homomorfismo así definido se llama la *evaluación* en $x_1, x_2, \ldots, x_n$. *Notación:* $\mathrm{ev}_{(x_1, x_2, \ldots, x_n)}$. Consiste en sustituir en P cada letra X_i por el elemento x_i:

$$\mathrm{ev}_{(x_1, \ldots, x_n)} : P(X_1, \ldots, X_n) \mapsto P(x_1, \ldots, x_n)$$

Cada polinomio, P, define una función de $\underbrace{A \times A \times \ldots \times A}_{n}$ en A, denotada por $\hat{P}$:

$$\hat{P} : (x_1, \ldots, x_n) \mapsto \mathrm{ev}_{(x_1, \ldots, x_n)}(P)$$
$$= P(x_1, \ldots, x_n)$$

El elemento $P(x_1, \ldots, x_n)$ llámase el *valor* de P en $(x_1, \ldots, x_n)$. Se dice que $(x_1, \ldots x_n)$ es un *cero* de P (o una *raíz* de P cuando P tiene sólo una variable) cuando $P(x_1, \ldots, x_n) = 0$ (cuando P se anula en $(x_1, \ldots, x_n)$).

Definición 5. *Sean $\mathcal{X} \hookrightarrow \mathcal{P}$ una R-algebra de polinomios y A una R-algebra conmutativa. Sean $x_1, x_2, \ldots, x_n$ elementos de A. El nucleo de la función de evaluacion $\mathrm{ev}_{(x_1, \ldots, x_n)}$ es un ideal de $\mathcal{P}$, denotado por $R(x_1, \ldots, x_n)$, que se llama el ideal de las relaciones algebraicas entre los x_i.*

Este ideal se caracteriza por la propiedad siguiente:

$$P \in R(x_1, \ldots, x_n) \Leftrightarrow P(x_1, \ldots, x_n) = 0$$

Este ideal no depende en esencia de las letras $X_1, \ldots, X_n$. Si se le calcula para otro anillo de polinomios en el mismo número de variables, $R[Y_1, \ldots, Y_n]$, el nuevo ideal de relaciones algebraicas se obtiene del anterior por el simple reemplazo de cada X_i por Y_i.

Observación 2. Si $\mathcal{X} \to \mathcal{P}$, $\mathcal{Y} \to \mathcal{Q}$ son dos R-álgebras de polinomios, cada aplicación $f : \mathcal{X} \to \mathcal{Y}$ induce un homomorfismo $F : \mathcal{P} \to \mathcal{Q}$. Como en el caso de los monomios, si $f : \mathcal{X} \to \mathcal{Y}$, $g : \mathcal{Y} \to \mathcal{Z}$ inducen, respectivamente, $F : \mathcal{P} \to \mathcal{Q}$ y $G : \mathcal{Q} \to \mathcal{Z}$, entonces gf induce GF. La identidad induce la identidad. F es inyectiva, epiyectiva, biyectiva si, y sólo si, f es, respectivamente, inyectiva, epiyectiva, biyectiva.

Ejemplo 2. $R[X_1, \ldots, X_n] \cong R[Y_1, \ldots, Y_n]$.

Ejemplo 3. *Acción del grupo simétrico en los polinomios*

Cada permutación de las letras: $\sigma : X_i \to X_{\sigma(i)}$ induce un automorfismo de $R[X_1, \ldots, X_n]$, que se denota por el mismo símbolo, σ:

$$(\sigma P)(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

10 Por ejemplo, el ciclo $(1, 2, 3)$ lleva el polinomio $X^2Y - 3Z - X$ al polinomio $Y^2Z - 3X - Y$.

Así se tiene una acción del grupo simétrico S_n en $R[X_1, \ldots, X_n]$, por automorfismos. (Véase[6], cap. 2, en especial el ejemplo 8.) Esta acción se usa para definir el *signo* de una permutación. Sea R un anillo con característica distinta de 2 y sea P el polinomio

$$\prod_{i<j}^{n} (X_i - X_j)$$

Se demuestra que la órbita de P, bajo la acción de S_n, es $\{P, -P\}$ y, por lo tanto, el estabilizador de P es un subgrupo de índice 2 en S_n. Es el subgrupo *alternado*, A_n. Las permutaciones de A_n tienen signo 1, y las otras, signo -1. Se verifica entonces

$$\sigma(P) = \operatorname{sign}(\sigma) \cdot P \quad (\forall \sigma \in S_n)$$

Los polinomios que son puntos fijos para esta acción de S_n se llaman *simétricos*. He aquí algunos ejemplos:

$$\prod_{i,j=1}^{n} (X_i - X_j), \quad X_1 + X_2 + \ldots + X_n, \quad X_1 X_2 \ldots X_n,$$

$$\sum_{i=1}^{n} X_i^2$$

Ejemplo 4. Sean $\mathcal{X}$ e $\mathcal{Y}$ dos conjuntos disjuntos y sea $\mathcal{Z}$ su unión. Consideremos sus respectivas álgebras de polinomios con coeficientes en R: $R[\mathcal{X}]$, $R[\mathcal{Y}]$ y $R[\mathcal{Z}]$. Se tiene que

$$R[Z] \cong R[\chi][\gamma]$$

(donde, a la derecha, se tiene el álgebra de polinomios en γ con coeficientes en el anillo $R[\chi]$), siendo éste un isomorfismo de R-álgebras que se reduce a la identidad en las letras.

En efecto, la inclusión $\chi \hookrightarrow R[Z]$ tiene una única extensión $R[\chi] \to R[Z]$ (homomorfismo de R-álgebras) y, por lo tanto, $R[Z]$ es una $R[\chi]$-álgebra. Entonces, la inclusión $\gamma \hookrightarrow R[Z]$ tiene una única extensión $R[\chi][\gamma] \xrightarrow{F} R[Z]$ (homomorfismo de $R[\chi]$-álgebras). Por otro lado, la inclusión $Z \hookrightarrow R[\chi][\gamma]$ tiene una única extensión $R[Z] \xrightarrow{G} R[\chi][\gamma]$ (homomorfismo de R-álgebras). Es inmediato que FG es la identidad de $R[Z]$, y GF la de $R[\chi][\gamma]$ (ambas aplicaciones son la identidad en los coeficientes y en las letras). Por lo tanto, considerados como morfismos de R-álgebras, F y G son isomorfismos inversos entre sí.

Estos ejemplos ilustran la enorme versatilidad de los polinomios y muestran cómo un anillo de polinomios puede ser presentado de diversas maneras. Basándose en el ejemplo 4 es fácil probar por inducción que:

$$R[X_1, X_2, \ldots, X_n] \cong R[X_1][X_2]\ldots[X_n]$$

Cuando se aplica el isomorfismo $R[Z] \to R[\chi][\gamma]$ estudiado en el ejemplo 4, se dice que se reagrupan las letras considerando los polinomios como polinomios en γ con coeficientes en $R[\chi]$. 11

Sea A una R-álgebra. Si S es un subconjunto de A, la intersección de todas las subálgebras que contienen a S es una subálgebra, que se denota por $R[S]$. Es la mínima subálgebra que contiene a S. Se dice que $R[S]$ es la subálgebra *generada* por S. Si $R[S] = A$, se dice que S es un conjunto de generadores de A. Si A posee un conjunto finito de generadores se dice que A es de *tipo finito* o que A es *finitamente generada* (en abreviatura: f. g.).

Teorema 1. *Teorema fundamental de las álgebras conmutativas. Sean R y S anillos conmutativos; sea $A = R[x_1, \ldots, x_n]$ una R-álgebra conmutativa de tipo finito; sea B una S-álgebra conmutativa y sean $y_1, \ldots, y_n$ elementos de B. Sea, finalmente, $\lambda : R \to S$ un homomorfismo. Entonces:*

1) *Existe un único homomorfismo de anillos*

$$\Phi : R[X_1, \ldots, X_n] \to S[Y_1, \ldots, Y_n]$$

que coincide con λ en R y lleva cada X_i en Y_i.

2) *Para que exista un homomorfismo de anillos $f : A \to B$ que coincida con λ en R y lleve cada x_i en y_i es necesario y suficiente que $\Phi(P(x_1, \ldots, x_n)) \subset P(y_1, \ldots, y_n)$.*

Demostración

1) Si Φ debe llevar X_i en Y_i y $\Phi|_R = \lambda$, resulta

$$\Phi\Big(\sum_i a_i M_i(X_1,\ldots,X_n)\Big) = \sum_i \mathcal{Z}(a_i) M_i(Y_1,\ldots,Y_n)$$

o sea que Φ, si existe, está unívocamente determinada por las condiciones.

Ahora, si se define Φ por aquella relación, lo que es posible pues cada polinomio es combinación lineal única de monomios con coeficientes en R, se comprueba de inmediato que Φ verifica las condiciones del teorema.

2) Consideremos el diagrama siguiente:

$$\begin{array}{ccccc} \mathcal{R}(x_1,\ldots,x_n) & \hookrightarrow & R[X_1,\ldots,X_n] & \xrightarrow{\mathrm{ev}_{(x_1,\ldots,x_n)}} & A \\ \downarrow \Phi & & \downarrow \Phi & & \downarrow f \\ \mathcal{R}(y_1,\ldots,y_n) & \hookrightarrow & S[Y_1,\ldots,Y_n] & \xrightarrow{\mathrm{ev}_{(y_1,\ldots,y_n)}} & B \end{array}$$

Si f tiene las propiedades indicadas, el cuadrado de la derecha es conmutativo y, por lo tanto, Φ lleva el ideal de las relaciones algebraicas entre los x_i en el ideal de las relaciones algebraicas entre los y_i. Recíprocamente, si Φ tiene esta propiedad, se tiene conmutatividad en el cuadrado de la izquierda y, por lo tanto, Φ pasa a los cocientes $R[x_1, \ldots, x_n] = A$ y $S[y_1,\ldots,y_n] \subset B$ llevando x_i en y_i y reduciéndose a $\mathcal{Z}$ en R. Este pasaje a los cocientes es la función f buscada.

Observación 3. La parte 1) de este teorema es de aplicación corriente en álgebra: todo morfismo de anillos conmutativos tiene una única prolongación en los polinomios. Por esta razón y para simplificar las notaciones, por lo general se usa la misma letra, $\mathcal{Z}$, tanto para el morfismo de R en S como para su prolongación en los polinomios.

Observación 4. La condición necesaria y suficiente para la existencia de la prolongación f (parte 2) del teorema) se puede expresar en otra forma equivalente en la que no se hace uso explícito de los ideales de relaciones algebraicas. En efecto, basta emplear la indicación anotada después de la definición 5 para obtener:

La condición $\Phi(\mathcal{R}(x_1,\ldots,x_n)) \subset \mathcal{R}(y_1,\ldots,y_n)$ es equivalente a:

$$\forall P \in R[X_1,\ldots,X_n],\quad P(x_1,\ldots,x_n) = 0 \Rightarrow \Phi(P)(y_1,\ldots,y_n) = 0$$

o también, por la observación 3:

$$\forall P \in R[X_1,\ldots,X_n],\quad P(x_1,\ldots,x_n) = 0 \Rightarrow \mathcal{Z}(P)(y_1,\ldots,y_n) = 0$$

Con frecuencia el ideal $\mathcal{R}(x_1,\ldots,x_n)$ viene dado por un conjunto de generadores: $\mathcal{R}(x_1,\ldots,x_n) = (P_i,\ i \in I)$. En tal caso, como se comprueba fácilmente, la condición de existencia de la prolongación f se escribe así:

$$\forall i \in I : P_i(x_1,\ldots,x_n) = 0 \Rightarrow \mathcal{Z}(P_i)(y_1,\ldots,y_n) = 0$$

Ejemplo 5. Toda R-álgebra de tipo finito, $A = R[x_1,\ldots,x_n]$, es un cociente de $R[X_1,\ldots,X_n]$:

$$A[x_1,\ldots,x_n] \cong \frac{R[X_1,\ldots,X_n]}{\mathcal{R}(x_1,\ldots,x_n)}$$

Esto da una nueva pauta de la importancia de los polinomios.

Ejemplo 6. Sean I un ideal de R, $S = R/I$ y $\mathcal{L} : R \to S$ la aplicación canónica. El homomorfismo Φ del teorema:

$$\Phi : R[X_1,\ldots,X_n] \to S[X_1,\ldots,X_n]$$

se llama el pasaje a polinomios módulo I. Si P es un polinomio con coeficientes en R, su imagen se suele denotar por $\bar{P}$, y se obtiene sustituyendo cada coeficiente a de P por su imagen módulo I, que se suele denotar por $\bar{a}$. Este homomorfismo es un epimorfismo.

Ejemplo 7. Si R es un subanillo de S, la inclusión $R \hookrightarrow S$ (considerada como $\mathcal{L}$) define una inyección $R[X_1,\ldots,X_n] \to S[X_1,\ldots,X_n]$ y puede considerarse el primero como un subanillo del segundo. Por ejemplo, $\mathbb{Z}[X_1,\ldots,X_n]$ puede entenderse como un subanillo de $\mathbb{Q}[X_1,\ldots,X_n]$.

Grado

Sea $G = \mathbb{N} \cup \{\omega\} (\omega \notin \mathbb{N})$ un conjunto ordenado por el orden de $\mathbb{N}$ y la condición $\omega \leq n$ $(\forall n \in \mathbb{N})$. Defínase en G una estructura (denotada aditivamente) de semigrupo mediante la condición de que $(\mathbb{N}, +)$ sea un subsemigrupo de G y las condiciones: $\omega + g = g + \omega = \omega$ $(\forall g \in G)$.

Definición 6. *Sea $X_1^{e_1}\ldots X_n^{e_n} = M$ un monomio en las letras $X_1,\ldots,X_n$. Se llama grado de M* (notación: $\mathrm{gr}(M)$) *a $e_1 + \ldots + e_n \in G$. Si $P = \sum_i r_i M_i \in R[X_1, \ldots, X_n]$, $P \neq 0$ (donde r_i son elementos no nulos de R y M_i son monomios), se llama grado de P a:*

$$\mathrm{gr}(P) = \max\{\mathrm{gr}(M_i)/i\} \in G$$

Se llama grado del polinomio 0 a $\omega \in G$

Los polinomios cuyos monomios tienen todos el mismo grado se llaman *homogéneos*

La función gr tiene las siguientes propiedades de demostración inmediata:

1. $\mathrm{gr}(P + Q) \leq \max(\mathrm{gr}(P), \mathrm{gr}(Q))$
2. Si $\mathrm{gr}(P) \neq \mathrm{gr}(Q)$, $\mathrm{gr}(P + Q) = \max(\mathrm{gr}(P), \mathrm{gr}(Q))$
3. $\mathrm{gr}(PQ) \leq \mathrm{gr}(P) + \mathrm{gr}(Q)$
4. Si R es íntegro, $\mathrm{gr}(PQ) = \mathrm{gr}(P) + \mathrm{gr}(Q)$
5. $\mathrm{gr}(P) = 0$ si, y sólo si, P es un elemento no nulo de R.

Nota. No hay dificultad alguna en considerar polinomios en un conjunto infinito de variables. Basta construir primero los monomios en la

forma indicada antes y seguir después, sin cambios, el proceso aquí presentado.

2. POLINOMIOS SOBRE UN ANILLO FACTORIAL

Divisibilidad

Sea R un anillo conmutativo, con 1, sin divisores de 0, es decir: un *anillo íntegro*. Sea $U(R)$, o simplemente U, el grupo de unidades del semigrupo $(R, .)$.

Dados $a, b \in R$ se dice que a *divide* b *(notación:* $a|b$) cuando existe $c \in R$ tal que $ac = b$. O sea: $a|b \Rightarrow b \in (a)$. La relación $|$ es reflexiva y transitiva, pero no es simétrica en general. En efecto, la relación "$a|b$ y $b|a$" equivale a $(a) = (b)$, o a $aU = bU$, y se expresa verbalmente diciendo "a está asociado con b" *(notación:* $a \sim b$. La relación "ser asociados" es una relación de equivalencia: es la congruencia módulo U.

Si se considera el semigrupo cociente $\bar{R} = R/U$, la relación de divisibilidad induce en $\bar{R}$ un orden parcial que tiene a U, la clase de 1, como elemento mínimo y a $\{0\}$, la clase de 0, como elemento máximo. Los elementos minimales de $\bar{R}$ se llaman *primos*. Por abuso de lenguaje se llaman también primos a los elementos p de R tales que pU es un elemento primo de $\bar{R}$. Por lo tanto, son primos los elementos p de R que no pertenecen a U y que poseen la propiedad de minimalidad siguiente:

$$\forall x \in R, \quad x|p \Rightarrow \begin{matrix} x \sim 1 \\ \text{o} \\ x \sim p \end{matrix}$$

Es claro que $\bar{R}$, con el orden $|$ y la multiplicación heredada de R es isomorfo al conjunto $\mathcal{Y}_0$ de los ideales principales de R, con el orden $\supset$ y la multiplicación usual de ideales. Por lo tanto, $p \in R$ es primo si, y sólo si, (p) es un elemento maximal de $\mathcal{Y}_0$.

Ejemplo 1. En $R[X]$, $(X - x)|P$ si, y sólo si, $P(x) = 0$, o sea si, y sólo si, x es una raíz de P. Si R es un cuerpo, todo polinomio de primer grado de $R[X]$ es primo en $R[X]$.

Anillos Factoriales

Sea R un anillo íntegro y sea $\mathcal{Y}$ el semigrupo de los ideales principales no nulos de R ($\mathcal{Y}$ es un subsemigrupo de $\mathcal{Y}_0$). Sea $\mathcal{P}$ el conjunto de los ideales principales generados por elementos primos de R.

Definición 1. A. *Se dice que R es principal cuando todo ideal de R es principal* (o sea cuando $\mathcal{Y}_0$ es el conjunto de todos los ideales de R).

B. *Se dice que R es factorial cuando la inclusión $\mathcal{P} \hookrightarrow \mathcal{Y}$ es un semigrupo de monomios en las letras de $\mathcal{P}$.*

O sea, R es factorial si, y sólo si, (demuestrése!) cada ideal principal no nulo de R es un producto único (salvo el orden de los factores) de ideales generados por primos:

$$\forall x \in R, \quad x \neq 0, \quad (x) = (p_1)^{e_1} \dots (p_r)^{e_r} \quad \text{(expresión única)}$$

$$(e_i \in \mathbb{N} - 0, \quad p_i \text{ primos no asociados})$$

De modo equivalente, R es factorial si, y sólo si, cada elemento no nulo de R, a, que no esté en U, se escribe en la forma:

$$a = p_1^{e_1} \dots p_r^{e_r} \quad \begin{pmatrix} p_i \text{ primos no asociados,} \\ e_i \text{ naturales no nulos} \end{pmatrix}$$

y esta descomposición es única en el sentido de que si, además,

$$a = p_1'^{e_1'} \dots p_{r'}'^{e_{r'}'} \quad \begin{pmatrix} p_i' \text{ primos no asociados,} \\ e_i' \text{ naturales no nulos} \end{pmatrix}$$

entonces $r = r'$, y existe una permutación $\sigma \in S_r$ tal que para todo $i = 1, \dots, r$: $p_i \sim p'_{\sigma(i)}$ y $e_i = e'_{\sigma(i)}$.

Ejemplo 2. $\mathbb{Z}$ es un anillo factorial.

Ejemplo 3. Si R es principal, R es factorial.

Para demostrarlo, comencemos mostrando la unicidad de la descomposición en factores primos. Razonamos por inducción en mín(r, r') (y podemos suponer, sin pérdida de generalidad, que $r = \text{mín}(r, r')$).

Si $r = 1$ se debe mostrar que una igualdad de la forma

$$P^e = P_1'^{e_1'} \dots P_{r'}'^{e_{r'}'}$$

(donde P es generado por el primo p y P_1' por el primo p_1') implica $r' = 1$, $P_1' = P$ y $e_1' = e$. Esa igualdad significa que $p_1'^{e_1'} \dots p_{r'}'^{e_{r'}'}$ es congruente con 0 módulo P y, como R es principal, P es maximal (véase la afirmación que antecede al ejemplo 1) y R/P es un cuerpo. Por lo tanto, algún p_i' es 0 módulo P. Se puede suponer, sin pérdida de generalidad, que p_1' es 0 módulo P, o sea que $p \mid p_1'$, lo que implica $p_1' \sim p$.

Ahora, si fuera $e \leq e_1'$, simplificando P^e, se tendría que $R = (1)$ es un producto de primos. Por lo tanto se deduce que $r' = 1$ y $e_1' = e$. Si fuera $e > e_1'$ se tendría, simplificando ahora $P_1'^{e_1'}$, que una potencia de P es un producto de ideales (p_i') con p_i' no asociado con p, cosa imposible por el argumento hecho más arriba.

Si $r > 1$, se parte del hecho de que $P_1'^{e_1'} \dots P_{r'}'^{e_{r'}'} \subset P$ para deducir, por el mismo argumento ya citado, que, por ejemplo, $P_1' = P_1$, $e_1' = e_1$. Simplificando, la demostración se completa fácilmente a partir de la hipótesis de recurrencia.

Para mostrar la existencia de la descomposición en factores primos se necesitan algunas propiedades de los ideales del anillo principal R.

En primer lugar, observemos que toda sucesión creciente de ideales: $I_1 \subset I_2 \subset \ldots$ llega a ser constante a partir de un cierto lugar. En efecto, si I es la unión de todos ellos, I es un ideal principal: $I = (a)$ y hay un n tal que $a \in I_n$. Por lo tanto, todo ideal I_m con $m \geq n$ es igual a $I_n = I$.

Esto implica que (en el semigrupo $\mathcal{Y}$) todo I tiene sólo un número finito de divisores. En caso contrario, tomando divisores sucesivos, se podría construir una sucesión estrictamente creciente de ideales. De aquí se deduce, a su vez, que todo $a \in R$, $a \neq 0$ y $a \notin U$ tienen un divisor primo.

Para probar que $I = (a)$ es un producto de factores de la forma (p), con p primo, se razona por inducción en el número n de divisores de I. Si $n = 1$, $I = R$ y es un producto vacío de ideales de la forma indicada. Si $n > 1$, I tiene un divisor de la forma (p) (pues a tiene un divisor primo) y se puede considerar un producto $J = (p_1) \ldots (p_s)$ (p_i primos) tal que $J \mid I$ y tal que s sea máximo. Si K es el ideal tal que $JK = I$, K tiene un divisor de la forma (p) y $J \cdot (p) \mid I$, lo que contradice la elección de J. Esto termina la demostración.

Ejemplo 4. Sean K un cuerpo y X una letra. Entonces $K[X]$ es un anillo principal y, por tanto, factorial. La demostración (igual a la correspondiente al anillo $\mathbb{Z}$) es muy conocida. Se basa en el algoritmo de división entera.

16 Si $P \in K[X]$ es un polinomio no nulo, se llama *coeficiente principal* de P al coeficiente del monomio de mayor grado que aparece con coeficiente no nulo en la expresión de P. Si el coeficiente principal es 1, el polinomio se llama *mónico*.

Dos polinomios $P, Q \in K[X]$ son asociados si, y sólo si, existe $a \in K$, $a \neq 0$, tal que $Q = aP$. Por lo tanto, todo polinomio es asociado de un polinomio mónico, y éste es único, pues dos polinomios mónicos asociados son necesariamente iguales.

Esto significa que si R es de la forma $K[X]$, K un cuerpo, puede representarse $\tilde{R}$ por el conjunto de los polinomios mónicos de $K[X]$, más el polinomio 0. Esta representación consiste en elegir, para cada clase $P \cdot U$ de $\tilde{R}$, el único polinomio mónico que pertenece a $P \cdot U$. La correspondencia así obtenida es un isomorfismo para la multiplicación y para la relación de divisibilidad.

Algo semejante ocurre cuando $R = \mathbb{Z}$. En este caso, cada elemento to de $\tilde{R}$ es de la forma $\{n, -n\}$ y cada clase no nula tiene un único representante positivo. Así, $\tilde{R}$ puede representarse por N, y esta correspondencia es también un isomorfismo para la multiplicación y para la relación de divisibilidad.

A juzgar por los ejemplos presentados, sólo los anillos principales son factoriales. Sin embargo, el ejemplo 5 mostrará, más adelante, que esto no es así.

Máximo Divisor Común y Mínimo Múltiplo Común

Definición 2. *Sea $(a_i)_i \in I$ una familia no vacía de elementos de R, y sean $\tilde{a}_i$ los elementos correspondientes de $\tilde{R}$.*

tiene, por definición, que $d \mid d'$. Pero la relación que define Dd implica que $Rd = Ra + Rb$, que implica $d' \mid d$. Luego, $d' \sim d$.

El Lema de Gauss

Definición 3. *Sean R un anillo factorial y X una letra. Un polinomio $P \in R[X]$, de grado mayor que 0, se llama irreducible si la relación $P_1P_2 = P$ implica $\mathrm{gr}(P_1) = 0$ o $\mathrm{gr}(P_2) = 0$.*

Por ejemplo, todo polinomio de grado 1 es irreducible en $R[X]$ (o, como suele decirse, sobre R).

Los polinomios que son primos de $R[X]$ son irreducibles, pero el recíproco no es necesariamente verdadero. Por ejemplo, $2X \in \mathbb{Z}[X]$ es irreducible, pero no es primo.

Si R es un cuerpo, un polinomio es irreducible si, y sólo si, es primo.

Definición 4. *Sean R un anillo factorial, X una letra y P un polinomio de $R[X]$. Se llama contenido de P al mdc de los coeficientes de P. Notación: $c(P)$. Se dice que P es primitivo cuando $c(P) = 1$.*

Proposición 1. *Sean R un anillo factorial, X una letra y $P \in R[X]$, $P \neq 0$.*

A. *Existen un polinomio primitivo $P' \in R[X]$ y un elemento $a \in R$ tales que $P = aP'$. Esta descomposición es única (salvo asociados, en el sentido de que si $P = a_1P_1'$, $P_1' \in R[X]$, primitivo, y $a_1 \in R$, entonces $a \sim a_1$ y $P' \sim P_1'$). Se tiene además que $\bar{a} = c(P)$.*

B. *Sean K el cuerpo de cocientes de R y $P \in K[X]$, $P \neq 0$. Entonces existen $P' \in R[X]$, primitivo, y $\alpha \in K$ tales que $P = \alpha P'$. Esta descomposición es única en el sentido de que si $P = \alpha_1P_1'$ ($P_1' \in R[X]$, primitivo, y $\alpha_1 \in K$), entonces $P' \sim P_1'$ y existe $u \in U(R)$ tal que $\alpha = u\alpha_1$.*

C. *Si P es un polinomio irreducible y primitivo de $R[X]$, P es un primo de $R[X]$, y recíprocamente.*

Demostración

A. Sea $a \in R$ tal que $\bar{a} = c(P)$. Entonces $a \mid P$ y $P = aP'$, $c(P') = 1$. Si $aP' = a_1P_1'$, a divide los coeficientes de P_1' y, por lo tanto, $a \mid a_1$. Por la misma razón, $a_1 \mid a$. Simplificando se obtiene $P' \sim P_1'$.

B. Los coeficientes de P pueden escribirse en la forma a_1/d ($a_1, d \in R$) y entonces $dP \in R[X]$. Aplicando A., tenemos: $dP = aP'$ ($a \in R$, $P' \in R[X]$, primitivo) y $P = \frac{a}{d}P'$. Si se verifica $\frac{a}{d}P' = \frac{a_1}{d_1}P_1'$, se deduce $ad_1P' = a_1dP_1'$, que implica, por A., $ad \sim a_1d$ y $P' \sim P_1'$.

C. La demostración es inmediata.

Proposición 2. *Lema de Gauss. Sean R un anillo factorial y $P, P' \in R[X]$, primitivos. Entonces PP' es primitivo.*

Demostración. Sean $P(X) = a_0 + a_1X + \ldots$ y $P'(X) = a'_0 + a'_1X + \ldots$. Razonando por reducción al absurdo, sea p un primo de R que divide a todos los coeficientes de PP'. Sean a_i y a'_j, respectivamente, el primer coeficiente de P y P', que no es divisible por p. Entonces el coeficiente de lugar $i + j$ de PP' es $a_{i+j}a'_0 + a_{i+j-1}a'_1 + \ldots + a_ia'_j + \ldots + a_0a'_{i+j}$ y no es divisible por p contra lo supuesto.

Corolario. *La función contenido: $P \to c(P)$ es un homomorfismo respecto de la multiplicación: $c(PP_1) = c(P)c(P_1)$.*

Demostración. Se aplica la proposición 1: $P = aP'$, $P_1 = a_1P'_1$, $PP_1 = cP''$ (con P', P'_1 y P'' primitivos) y se tiene, por el lema de Gauss: $P'P'_1 = (aa_1)(P''P'_1)$, con $P'P'_1$ primitivo. Por lo tanto por la proposición 1, A, $aa_1 \sim c$.

Proposición 3. *Si R es factorial, $R[X]$ es factorial.*

Demostración. Sea P un polinomio no nulo de $R[X]$. Considerándolo como elemento de $K[X]$ (donde K es el cuerpo de cocientes de R), se puede escribir P como un producto de polinomios primos de $K[X]$ (cf. el ejemplo 4). Basándose en la proposición 1 se puede escribir cada uno de esos factores como producto de un elemento de K por un polinomio primitivo, el cual es entonces un primo de $R[X]$ por la proposición 1, C. Así se consigue expresar P como un producto de un elemento de K, a, por un producto de primos de $R[X]$ y la proposición 1, B implica que $a \in R$. Finalmente, si se descompone a en factores primos (de R) se tiene P descompuesto en factores primos de $R[X]$. La unicidad de esta descomposición resulta de la unicidad de la descomposición en factores primos en $K[X]$. En efecto, los divisores irreducibles de P son los divisores primos de P en $K[X]$.

Corolario. *Si R es factorial y n es un número natural no nulo, el anillo de polinomios $R[X_1, \ldots, X_n]$ es factorial.*

Demostración. Inducción en n teniendo presente que $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$.

Ejemplo 5. Existen anillos factoriales que no son principales. Veamos que $\mathbf{Z}[X]$ no es principal. En efecto, 2 es un primo de $\mathbf{Z}[X]$, pero (2) no es un ideal maximal, pues el cociente $\mathbf{Z}[X]/(2)$ es isomorfo a $\frac{\mathbf{Z}}{2\mathbf{Z}}[X]$, que no es un cuerpo.

Uno de los problemas básicos del estudio de los polinomios sobre un cuerpo K es el de decidir si un polinomio es irreducible o no.

Uno de los métodos que se pueden aplicar es el de partir de un anillo factorial R cuyo cuerpo de cocientes sea K. La proposición 1 indica que el problema de hallar los polinomios irreducibles de $K[X]$ es en esencia equivalente al de hallar los polinomios irreducibles de $R[X]$. Para decidir si $P \in R[X]$ es irreducible hay dos teoremas importantes.

Proposición 4. *Sea R un anillo factorial e I un ideal de R. Sea $\mathcal{Q}$ el epimorfismo natural de $R[X]$ sobre $(R/I)[X]$* (véase 1, ejemplo 6) *y sea $P \in R[X]$, mónico. Si $\mathcal{Q}(P)$ es irreducible, P es irreducible.*

Demostración: Si P no es irreducible es un producto P_1P_2 de polinomios mónicos de grados positivos. Entonces $\mathcal{Z}(P) = \mathcal{Z}(P_1)\mathcal{Z}(P_2)$ es reducible, pues $\mathcal{Z}(P_1)$ y $\mathcal{Z}(P_2)$ son mónicos del mismo grado, respectivamente, que P_1 y P_2

Ejemplo 6. $X^2 + X + 1$ es irreducible en $\mathbb{Q}[X]$, pues $X^2 + X + 1$ pertenece a $\mathbb{Z}[X]$ y es irreducible módulo 2.

Proposición 5. *Criterio de Eisenstein. Sean R un anillo factorial y p un primo de R. Sea $P \in R[X]$ tal que*

$$P(X) = a_0 + a_1X + \ldots + a_nX^n; \quad p \nmid a_n;$$

$$p \mid a_i \ (i = 0, 1, \ldots, n-1); \quad p^2 \nmid a_0$$

Entonces P es irreducible.

Demostración. Por reducción al absurdo. Sea $P = QT$ una factorización no trivial de P, y sean: $Q = b_0 + b_1X + \ldots$, $T = c_0 + c_1X + \ldots$. Como p divide a b_0c_0 y p^2 no, se puede suponer sin pérdida de generalidad que $p \mid b_0$ y $p \nmid c_0$. Sea t el primer lugar que p no divide b_t (t tiene que ser menor que n, pues $\mathrm{gr}(P) > \mathrm{gr}(Q)$). Entonces: $a_t = b_tc_0 + b_{t-1}c_1 + \ldots + b_0c_t$ no es divisible por p. Absurdo.

Ejemplo 7. Si p es un número primo, $X^n - p$ es irreducible sobre $\mathbb{Q}$. Esto implica, en particular, que $\sqrt{2}$ no es un número racional.

3. DESCOMPOSICIÓN FACTORIAL Y RELACIONES ENTRE COEFICIENTES Y RAÍCES

Si R es un anillo factorial y $P \in R[X]$ es un polinomio mónico de grado $n > 0$ que tiene n raíces distintas en R, se sigue que la descomposición de P en factores primos es:

$$P(X) = \prod_{i=1}^{n} (X - x_i)$$

Más generalmente, si R es sólo un anillo íntegro y P no necesariamente mónico, se tiene también una factorización: $P(X) = a\prod_{i=1}^{n}(X - x_i)$, donde a es el coeficiente principal de P.

Esta relación permite decidir hasta qué punto las funciones polinómicas determinan el polinomio que las define: Si P y Q, son polinomios en $R[X]$ y si $P(x_i) = Q(x_i)$ para un conjunto $\{x_1, \ldots, x_m\} \subset R$ que tiene más elementos que el mayor de los grados de P y Q, se verifica $P = Q$. En efecto, si $P - Q$ no fuera 0, tendría más raíces que su grado, lo que es absurdo, pues si $P - Q$ tiene grado n es $n < m$ y $P - Q = a(X - x_1) \ldots (X - x_n)$ (con $a \in R$, $a \neq 0$, $x_1, \ldots, x_n$ distintos) y es imposible que $(P - Q)(x) = 0$ para un x diferente de $x_1, \ldots, x_n$, pues R es íntegro.

Proposición 1. *Si R es un anillo íntegro con infinitos elementos, la aplicación $P \mapsto \hat{P}$ que a cada polinomio $P \in R[X]$ asocia su función polinómica, es inyectiva.*

Demostración. Es inmediata, por lo observado anteriormente.

Sean R un anillo íntegro y $X, X_1, \ldots, X_n$, letras. Sean $S = R[X_1, \ldots, X_n]$ y $\tilde{P}(X) = \prod_{i=1}^{n}(X - X_i) = \tilde{a}_0 + \tilde{a}_1 X + \ldots + \tilde{a}_{n-1}X^{n-1} + X^n \in S[X]$.

El grupo simétrico S_n opera naturalmente en S (véase 1, ejemplo 3) y define un grupo de automorfismos de $S[X]$ que deja fija la letra X. Es claro entonces que

$$\forall \sigma \in S_n : \sigma(\tilde{a}_i) = \tilde{a}_i \quad (i = 0, 1, \ldots, n-1)$$

lo que significa que cada $\tilde{a}_i$ es un polinomio simétrico (véase 1, ejemplo 3).

Cada $\tilde{a}_i$ se obtiene de la siguiente manera: Se considera el conjunto de los términos del desarrollo de $\prod_{i=1}^{n}(X - x_i)$ que tienen $n - i$ veces el factor X, se suman estos términos y se saca el factor común X^{n-i}. El coeficiente así obtenido para X^{n-i} es, precisamente, $\tilde{a}_i$. Por lo tanto, $\tilde{a}_i$ se obtiene eligiendo todos los subconjuntos de $\{X_1, \ldots, X_n\}$ que tienen i elementos: $\{X_{j_1}, \ldots, X_{j_i}\}$, y sumando los productos correspondientes (con el signo) : $(-X_{j_1})(-X_{j_2})\ldots(-X_{j_i}) = (-1)^i X_{j_1}\ldots X_{j_i}$. Es decir:

$$\tilde{a}_i = (-1)^i \sum_{\substack{J \subset \{1, \ldots, n\} \\ |J| = i}} \left(\prod_{j \in J} X_j \right) \qquad [1]$$

Definición 1. *Dado el anillo de polinomios $R[X_1, \ldots, X_n]$ se llaman funciones simétricas elementales* (en las X_i) *a los polinomios $s_0, s_1, \ldots, s_n$ definidos por:*

$$s_i(X_1, \ldots, X_n) = \sum_{\substack{J \subset \{1, \ldots, n\} \\ |J| = i}} \left(\prod_{j \in J} X_j \right) \qquad [2]$$

Por ejemplo:

$$s_0 = 1,$$

$$s_1 = X_1 + X_2 + \ldots + X_n,$$

$$s_n = X_1 X_2 \ldots X_n.$$

Como consecuencia de lo anterior, si $P \in R[X]$ tiene todas sus raíces distintas en R, o, más generalmente, si P tiene la descomposición factorial $a\prod_{i=1}^{n}(X - x_i)$ en $R[X]$, entonces los coeficientes a_i de P están dados por:

RELACIONES ENTRE COEFICIENTES Y RAÍCES

$$a_i = (-1)^i \cdot a \cdot s_i(x_1, \ldots, x_n) \quad (i = 0, 1, \ldots, n) \qquad [3]$$

Por ejemplo (como, por otra parte, es ampliamente conocido):

Si $P(X) = X^2 + bX + c = (X - x_1)(X - x_2)$, entonces $b = -(x_1 + x_2)$, $c = x_1x_2$;

Si $P(X) = X^3 + bX^2 + cX + d = (X - x_1)(X - x_2)(X - x_3)$,

$$b = -(x_1 + x_2 + x_3)$$

$$c = x_1x_2 + x_2x_3 + x_3x_1$$

$$d = -x_1x_2x_3.$$

Se puede demostrar (véase más adelante 2. 4, teorema 3) que todo polinomio simétrico es un polinomio de las funciones simétricas elementales s_i.

2

EXTENSIONES DE DIMENSIÓN FINITA

1. MOTIVACIÓN

Uno de los problemas centrales del álgebra es la resolución de ecuaciones de la forma

$$P(X) = 0, \quad (P \in R[X]) \qquad [1]$$

es decir, hallar los elementos de R, a, tales que $P(a) = 0$. Este problema, en extremo difícil, no tiene una solución satisfactoria, como sería disponer de un algoritmo para obtener las raíces de P. Esto ni siquiera es posible en el caso más simple en que R es un cuerpo.

Una buena aproximación teórica a la solución de este problema consiste en estudiar el "grado de dificultad" que presenta la resolución de la ecuación [1]. Precisemos lo que se entiende por "grado de dificultad".

Partamos del caso más simple, en que R es un cuerpo que contiene todas las raíces de P, es decir tal que $P(X) = a \prod_{i=1}^{n} (X - x_i)$ para ciertos elementos $a, x_1, \ldots, x_n$ de R. Aceptemos que las cuatro operaciones elementales (adición, sustracción, multiplicación y división) son algo simple, con el mínimo grado de dificultad. Es decir, concuérdese en que hallar las raíces $x_1, \ldots, x_n$ de P es fácil cuando se conocen ciertos elementos $y_1, \ldots, y_m$ y se sabe que los x_i son funciones racionales de los y_i y de los coeficientes de P (o sea: los x_i se obtienen a partir de los y_i y de los coeficientes de P mediante una sucesión finita de las cuatro operaciones elementales).

Esta situación se puede caracterizar así: Dado P, sea K un cuerpo conocido (por ejemplo, el cuerpo generado por los coeficientes de P) tal que $P \in K[X]$. Admitimos que la ecuación [1] puede ser fácilmente resuelta cuando se conocen elementos $y_1, \ldots, y_m$ tales que el mínimo cuerpo, E, que contiene a K y a los y_i contiene también a las raíces de P. Se conviene entonces que si $E = K$, la resolución de [1] presenta el mínimo grado de dificultad.

Así, la resolución [1] depende en esencia del salto de K a E. Si E es generado por $\{y_1, \ldots, y_m\}$ sobre K, podemos considerar los cuerpos generados, respectivamente, por $\{y_1\}$, $\{y_1, y_2\}$, $\{y_1, y_2, y_3\}$, ... como un camino para llegar, paso a paso, de K a E. Pero, es claro, sólo un análisis que permitiera decidir cuál es la mejor elección de los y_i proporcionaría una buena idea del grado de complejidad del paso de K a E, que, a su vez, sería una buena indicación del grado de dificultad de la resolución de [1].

Así pasamos a estudiar las extensiones de cuerpos:

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

es decir, sistemas formados por un cuerpo E y un subcuerpo, K, de E.

Ejemplo 1. Sea $P(X) = X^2 + bX + c \in R[X]$ un polinomio que tiene las raíces $x_1, x_2 \in R$ y sea K el cuerpo generado por b y c, $P \in K[X]$. Como $b = -(x_1 + x_2)$, la ecuación está resuelta si se conoce $\delta = x_1 - x_2$. El cuerpo de las raíces, E, es generado por δ. Para hallar δ, observemos que $\Delta = \delta^2 = (x_1 - x_2)^2$ es una función simétrica de x_1 y x_2, y, por lo tanto, es un polinomio de b y c. En efecto, $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4c$.

Llegamos así a la conocida solución de $P(X) = 0$: Si K no tiene característica 2, $x_1, x_2 = (-b \pm \sqrt{b^2 - 4c})/2$.

Ejemplo 2. Para resolver en $\mathbb{C}$ la ecuación

$$P(X) = X^6 - X^3 - 1 = 0$$

basta conocer las raíces de $Y^2 - Y - 1 = 0$, que son $y_1, y_2 = (1 \pm \sqrt{5})/2$. Si F es el cuerpo generado por y_1, y_2, se tiene una torre:

$$\begin{array}{c} E \\ | \\ F \\ | \\ K \end{array}$$

y las raíces de P son las raíces cúbicas de y_1 e y_2.

Ejemplo 3. Consideremos la siguiente ecuación con coeficientes racionales:

$$P(X) = X^5 - 2X^4 + 3X^3 + 3X^2 - 2X + 1 = 0 \qquad [2]$$

y busquemos sus soluciones en $\mathbb{C}$.

En primer lugar se observa que P tiene la raíz -1 y, dividiendo por $X + 1$, se halla:

$$P(X) = (X + 1)(X^4 - 3X^3 + 6X^2 - 3X + 1),$$

de modo que el problema se reduce a resolver:

$$Q(X) = X^4 - 3X^3 + 6X^2 - 3X + 1 = 0$$

Lógicamente sería interesante aquí poder decidir si Q puede también descomponerse en factores. Ello simplificaría aún más la situación. Sin embargo esta discusión nos apartaría demasiado del asunto principal.

Un cálculo fácil muestra que $Q(X) = X^4 \cdot Q\left(\frac{1}{X}\right)$, de donde se deduce que $Q(X) = 0$ implica $Q(1/X) = 0$. Lo que muestra que las raíces de Q se agrupan en pares de la forma $\{x, 1/x\}$ y Q es divisible por polinomios de la forma

$$(X - x)(X - 1/x) = X^2 + X - (x + 1/x)$$

Si se escribe $Y = X + \frac{1}{X}$ se obtiene que $Q(X) = X^2(Y^2 - 3Y + 4)$ y el problema se reduce a resolver

$$Y^2 - 3Y + 4 = 0$$

Este análisis muestra que el cuerpo E generado por las raíces de [2], x_1, x_2, x_3, x_4, tiene el subcuerpo F generado por $y_1 = x_1 + 1/x_1$ e $y_2 = x_2 + 1/x_2$ (suponiendo que $x_3 = 1/x_1$ y que $x_4 = 1/x_2$), y se tiene

$$\begin{array}{c} E \\ | \\ F \\ | \\ K \end{array}$$

Si se conoce F, se conoce E, pues los x_i son las raíces de las ecuaciones de segundo grado $X^2 - y_i X + 1 = 0$ $(i = 1, 2)$. Y F se conoce, pues y_1, y_2 son las raíces de $Y^2 - 3Y + 4 = 0$.

Ejemplo 4. *Construcciones con regla y compás*

Puesto que se sabe resolver fácilmente ecuaciones de segundo grado, el problema de resolver una ecuación $P(X) = 0$ se simplifica al máximo cuando hay una torre de cuerpos de la forma:

$$\begin{array}{ccc} E & = & F_n \\ & & | \\ & & F_{n-1} \\ & & | \\ & & \vdots \\ & & | \\ & & F_1 \\ & & | \\ K & = & F_0 \end{array}$$

que conecta el cuerpo de base K con el cuerpo de las raíces, E, en la cual el paso de cada F_i a F_{i+1} consiste en resolver una ecuación de segundo grado. (Los saltos correspondientes a ecuaciones de segundo grado son los más simples, pues los que corresponden a ecuaciones de primer grado son triviales y no permiten ningún progreso: Si F es el cuerpo generado sobre K por la raíz de $aX + b = 0$ $(a \neq 0)$, entonces $F = K$).

Ésta es precisamente la situación a que conduce el estudio de uno de los famosos problemas matemáticos heredados de la Grecia clásica:

decidir si un problema geométrico dado es resoluble mediante construcciones con regla y compás.

Un problema geométrico se reduce a, dada una figura Φ formada por puntos, rectas, polígonos, etc., hallar otra figura Ψ que verifique ciertas condiciones. Resolver el problema por construcciones con regla y compás significa determinar Ψ a partir de Φ mediante un número finito de operaciones de los tipos siguientes:

1. trazar la recta determinada por dos puntos conocidos;

2. hallar el punto común (si lo hay) a dos rectas conocidas;

3. trazar la circunferencia cuyo centro y radio son conocidos;

4. hallar los puntos de intersección (si existen) de una recta y una circunferencia dadas;

5. hallar los puntos de intersección (si existen) de dos circunferencias dadas.

Se observa que cada figura geométrica se puede determinar por un conjunto de puntos y esto permite describir los problemas geométricos en los siguientes términos: Hallar un conjunto de puntos Δ, que satisface ciertas condiciones, a partir de un conjunto de puntos Γ. El problema es resoluble con regla y compás si Δ se puede obtener a partir de un número finito de operaciones del tipo siguiente:

i. dados dos pares de puntos, hallar los puntos de intersección de las rectas que determinan;

ii. dados puntos que determinan una circunferencia y una recta, hallar sus puntos de intersección;

iii. dados puntos que determinan dos circunferencias, hallar sus puntos de intersección.

Para estudiar este problema se introduce un modelo algebraico. Mediante un sistema de coordenadas (elegido de modo que el segmento unidad de cada eje sea construible con regla y compás) se representa cada punto del plano por un número complejo (no se precisa estudiar expresamente problemas de geometría espacial, pues cada construcción se realiza dentro de un cierto plano), y cada conjunto de puntos del plano por un subcuerpo de $\mathbb{C}$ (el cuerpo generado por los representantes de tales puntos).

Si F es el cuerpo generado por el conjunto D, cada elemento de F se obtiene a partir de los elementos de D por medio de una sucesión finita de las cuatro operaciones elementales. Cada una de estas operaciones corresponde, en el plano, a una sucesión finita de las operaciones elementales i, ii, iii. Por lo tanto, si D corresponde a un conjunto de puntos Δ, cada elemento de F corresponde a un punto que puede construirse con regla y compás a partir de Δ. Más generalmente, si a es solución de una ecuación de segundo grado de coeficientes en F, como la extrac-

ción de raíces cuadradas también puede realizarse en el plano con regla y compás, se tiene que a representa también un punto que puede obtenerse por regla y compás a partir de Δ.

Inversamente, dado el conjunto de puntos Δ, que corresponde al cuerpo F, cada punto obtenido por una de las operaciones i, ii, iii, corresponde a un número complejo que es solución de una ecuación de primer o segundo grado con coeficientes en F.

Dar un conjunto de puntos, Γ, equivale a dar un cuerpo K de números complejos. Construir Δ con regla y compás a partir de Γ, significa hallar una sucesión de conjuntos de puntos: $\Delta_0 = \Gamma$, $\Delta_1, \ldots, \Delta_n = \Delta$ tales que cada Δ_{i+1} se obtiene de Δ_i, agregándole los puntos obtenidos por una de las operaciones i, ii, iii. En el modelo, esto corresponde a una torre de cuerpos:

$$\begin{array}{c} F_n = E \\ | \\ F_{n-1} \\ | \\ \vdots \\ | \\ F_1 \\ | \\ F_0 = K \end{array} \qquad [3]$$

tales que cada F_{i+1} se obtiene a partir de F_i, agregando las raíces de una ecuación de segundo grado sobre F_i.

Recíprocamente, si se tiene una torre [3] en que cada F_{i+1} es generado sobre F_i por las raíces de una ecuación de segundo grado, entonces F_n es generado por un conjunto D correspondiente a un conjunto de puntos Δ, que puede ser construido por regla y compás a partir de Γ.

En conclusión, decidir si un cierto problema geométrico puede ser resuelto con regla y compás equivale a decidir si una cierta extensión de cuerpos puede presentarse como una torre del tipo [3] con las propiedades indicadas.

Ejemplo 5. *Resolución de ecuaciones por radicales.*

Una ecuación

$$P(X) = 0 \quad (P \in R[X]) \qquad [4]$$

es resoluble por radicales si es posible expresar sus raíces a partir de los coeficientes de P mediante una sucesión finita de las cuatro operaciones elementales y la operación de extracción de una raíz. En otras palabras, para cada raíz x de P debe haber una sucesión $x_0, x_1, \ldots, x_n = x$ en que x_0 es uno de los coeficientes de P y o bien x_{i+1} está en el cuerpo generado por $x_0, \ldots, x_i$ y los coeficientes de P, o bien x_{i+1} es una raíz de un polinomio de la forma $X^k - b$, con b perteneciente al cuerpo generado por $x_0, \ldots, x_i$ y los coeficientes de P.

Denotemos por K el cuerpo generado por los coeficientes de P, y por E el cuerpo generado por K y las raíces de P. Para que [4] sea resoluble por radicales es necesario y suficiente que haya una torre de la forma [3] en la cual cada F_{i+1} se obtiene de F_i agregando una raíz de una ecuación de la forma $X^k - b = 0$ con $b \in F_i$.

Los ejemplos que anteceden justifican el estudio de las extensiones de cuerpos. Para el tipo de problemas considerados hasta ahora, el estudio puede limitarse a las extensiones de dimensión finita. Ese es el objeto del presente capítulo.

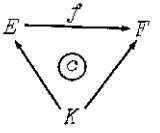
2. ALGEBRICIDAD Y TRASCENDENCIA

En esta sección, K es un cuerpo conmutativo y χ es la característica de K.

Definición 1. *Llámase extensión de K a toda K-álgebra $\iota : K \to E$ en que E es un cuerpo* (conmutativo).

Todo homomorfismo de anillos, ι, cuyo dominio es un cuerpo, es inyectivo. Luego, toda K-álgebra, E, contiene una copia de K que es un subanillo de E. Quiere decir que dar una extensión de K es equivalente a dar un cuerpo E y una manera de identificar K con un subcuerpo de E. Recíprocamente, si K es un subcuerpo de E, entonces la inclusión $K \hookrightarrow E$ define una extensión de K. Es costumbre hablar de la extensión E de K, en vez de decir la extensión $K \to E$. También es frecuente decir: "K está contenido en E" para indicar que K es un subcuerpo de E y que, por lo tanto, E es una extensión de K.

De acuerdo con 1. 1, definición 3, un morfismo de la extensión $K \to E$ en la extensión $K \to F$ es un homomorfismo de anillos $f : E \to F$ tal que



Si K es un subcuerpo de E y F, para que f sea un K-morfismo es necesario y suficiente que su restricción a K sea la identidad de K. Es costumbre decir: f es un K-morfismo de extensiones de cuerpos si, y sólo si, deja fijo cada elemento de K.

Notaciones

1. E/K denota la extensión $K \to E$.

2. $\mathrm{Hom}(E/K, F/K)$ es el conjunto de los morfismos de E/K en F/K. Análogamente se definen $\mathrm{End}(E/K)$ y $\mathrm{Aut}(E/K)$.

3. Si R es un anillo, $\mathrm{Aut}\,(R)$ es el grupo de los automorfismos de R.

4. Si E y F son espacios vectoriales, $\mathrm{Hom}_K(E, F)$, $\mathrm{End}_K(E)$ y $\mathrm{Aut}_K(E)$ son son los respectivos conjuntos de aplicaciones lineales.

5. Si E es una K-álgebra y S una parte de E, $K[S]$ es la subálgebra generada por S, y $K(S)$ (si existe) el subcuerpo generado por S (es decir, la intersección de todos los subcuerpos de E que contienen a K). $K(S)$ es el cuerpo de cocientes de $K[S]$.

6. Si $K[\chi]$ es un anillo de polinomios, $K(\chi)$ es el cuerpo de cocientes de $K[\chi]$, llamado *cuerpo de las funciones racionales en las letras de* χ.

7. Si q es un número natural, $\mathbb{F}_q$ denota, si existe, un cuerpo finito con q elementos (se verá en 4, ejemplo 2, que todos ellos son isomorfos). Por ejemplo, si q es un número primo, $\mathbb{F}_q = \mathbb{Z}/(q)$.

8. Según se vio en 1. 1, toda K-álgebra es un K-espacio vectorial. Dada la extensión E/K, $(E : K)$ denota la dimensión de E como K-espacio vectorial (este símbolo se usa de preferencia cuando esta dimensión es finita).

Uno de los objetivos básicos de la teoría de cuerpos es brindar información sobre el reticulado formado por los cuerpos F intermedios entre K y E. Cada vez que se consideran varios de estos cuerpos es útil representarlos por diagramas de Hasse: Para indicar que F_1 está contenido en F_2 se dispone la letra F_1 en un nivel más bajo que la letra F_2 y se las une por un trazo. Por ejemplo, para decir que E es una extensión de K se usa el diagrama

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

Interesan especialmente las siguientes configuraciones elementales:

Torres

Son las familias totalmente ordenadas de subextensiones de E/K:

$$\begin{array}{c} E \\ \vdots \\ | \\ F_n \\ | \\ F_{n-1} \\ | \\ \vdots \\ | \\ K \end{array}$$

Se dice que E/K es la torre y que cada F_n/F_{n-1} es un piso de la torre.

Nos interesan en especial las torres finitas, es decir las que tienen un número finito de pisos.

Compuestos

Si F y G son cuerpos intermedios entre K y E (o, más generalmente, si son sólo subcuerpos de E) se llama *compuesto* de F y G (*notación:* FG) al subcuerpo generado por F y G. Por lo tanto, $FG = F(G) = G(F) = GF$. Si $F = K(S)$ y G contiene a K, $FG = G(S)$. Puede definirse también el compuesto para una familia arbitraria de subcuerpos de E (es el cuerpo generado por todos ellos dentro de E).

Lema. *Sea E una K-álgebra de dimensión finita que es un anillo íntegro. Entonces E es una extensión de K.*

Demostración. Si a es un elemento no nulo de E, la aplicación $x \to xa$ es lineal e inyectiva y, por consiguiente, es un isomorfismo. Es decir, existe a' en E tal que $a' \cdot a = 1$.

Sean E un cuerpo y F y G subcuerpos de E que contienen a K (o, más generalmente, sean F y G dos subálgebras de la K-álgebra conmutativa E). La aplicación

$$F \times G \to E$$

$$(x, y) \to xy$$

es K-bilineal y, por lo tanto, define una aplicación lineal de $F \otimes_K G$ en E, α. La imagen de α es la subálgebra $K[F \cup G]$ generada por F y G.

Proposición 1. *Con las notaciones anteriores, si $(F : K)$ o $(G : K)$ es finita, entonces* $\operatorname{Im} \alpha = K[F \cup G] = FG$.

Demostración. Supóngase que $(F : K)$ es finita. Entonces, $\operatorname{Im} \alpha$ es un anillo íntegro que es a su vez una G-álgebra finita.

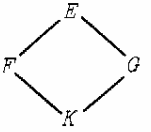
Esta proposición muestra que cuando $(F : K)$ y $(G : K)$ son finitas, entonces el compuesto FG es el conjunto de los elementos de la forma $\sum_i x_i y_i$ $(x_i \in F,\ y_i \in G)$. En el caso general, el compuesto FG es el cuerpo de cocientes de $K[F \cup G]$ y, por lo tanto, es el conjunto de los elementos de la forma $(\sum_i x_i y_i)(\sum_j x'_j y'_j)^{-1}$ $(x_i, x'_j \in F,\ y_i, y'_j \in G)$.

Definición 2. *Sea E una extensión de K y sean F y G cuerpos intermedios. Se dice que F y G son linealmente disjuntos sobre K* (notación: L. D. $/K$) *cuando la aplicación natural $\alpha : F \otimes_K G \to K[F \cup G]$ es un isomorfismo.* (Esta definición se aplica también a dos subálgebras F y G de una álgebra conmutativa E.)

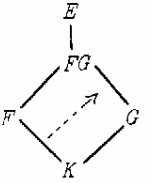
Para que F y G sean L. D. $/K$ es necesario y suficiente que toda familia de elementos de G que es linealmente independiente sobre K (*notación:* l. i. $/K$) sea también l. i. $/F$. O, en forma análoga, que toda familia de elementos de F que es l. i. $/K$ sea también l. i. $/G$.

Traslaciones

Dadas las extensiones



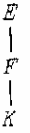
se llama *traslación* de F/K a G a la extensión FG/G:



El comportamiento de la dimensión o grado de una extensión con respecto a las configuraciones elementales se describe en la proposición siguiente:

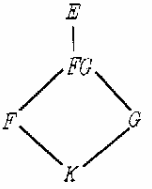
Proposición 2.

A. *Dada la torre*



$(E : K)$ *es finita si, y sólo si,* $(E : F)$ *y* $(F : K)$ *son finitas. En este caso,* $(E : K) = (E : F)(F : K)$.

B. *Dadas las extensiones*



$(FG : K)$ *es finita si, y sólo si,* $(F : K)$ y $(G : K)$ *son finitas. En este caso,* $(FG : K) \leq (F : K)(G : K)$ *y son iguales si, y sólo si,* F y G *son* L. D. $/K$.

C. *En la situación de* B, *si* $(F : K)$ *es finita* $(FG : G)$ *es finita y menor o igual que* $(F : K)$. *Son iguales si, y solo si,* F *y* G *son* L. D. $/K$. *Hay casos en que* $(FG : G)$ *es finita y* $(F : K)$ *es infinita.*

Demostración

A. Sea $(e_i)_i$ una K-base de F, y $(e'_j)_j$ una F-base de E. Entonces $(e_i e'_j)_{i,j}$ es una K-base de E.

En efecto, si $\sum \alpha_{ij} e_i e'_j = 0$ ($\alpha_{ij} \in K$), se deduce, por ser los e'_j l. i. /F, que cada $\sum \alpha_{ij} e_i = 0$, lo que implica $\alpha_{ij} = 0$ para todo i y para todo j. Por otro lado, dado $x \in E$, existen $y_j \in F$ tales que $x = \sum y_j e'_j$, y, para cada j, existen $\alpha_{ij} \in K$ tales que $y_j = \sum \alpha_{ij} e_i$. Por lo tanto, $x = \sum \alpha_{ij} e_i e'_j$.

B. Es consecuencia inmediata de la proposición 1 y de las propiedades del producto tensorial.

C. La primera parte es también consecuencia inmediata de la proposición 1. Si $(F : K)$ es infinita y si $G = F$, $(GF : G) = 1$.

Sea E una extensión de K y x un elemento de E. Como se vio en 1. 1, ejemplo 5, existe un epimorfismo $K[X] \to K[x]$ que lleva X en x y tiene por núcleo el ideal de las relaciones algebraicas de x, $\mathcal{R}(x)$. Como $K[x]$ es íntegro, $\mathcal{R}(x)$ es un ideal primo de $K[X]$ y caben sólo dos posibilidades: $\mathcal{R}(x) = 0$ ó $\mathcal{R}(x)$ es un ideal maximal de $K[X]$ (generado por un primo de $K[X]$, cf. 1. 2, ejemplo 4). En el primer caso, $K[X] \cong K[x]$ y $K(x)$ es isomorfo al cuerpo de funciones racionales en X, $K(X)$. En el segundo caso, si $\mathcal{R}(x) = (P)$, $K[x]$ es un cuerpo: $K[x] = K(x) \cong K[X]/(P)$ y $(K(x) : K)$ es finita e igual al grado de P.

Definición 3. A. *Sea x un elemento de una extensión de K. Se dice que x es algebraico sobre K* (notación: alg/K) *cuando $\mathcal{R}(x) \neq 0$; se dice que x es trascendente sobre K* (notación: tras/K) *cuando $\mathcal{R}(x) = 0$.*

B. *E/K es algebraica cuando todo x de E es* alg/K. *En caso contrario se dice que E/K es trascendente.*

Definición 4. *Sea x un elemento algebraico sobre K. Se llama polinomio irreducible de x sobre K* (notación: Irr(x/K)) *al único polinomio mónico que genera el ideal $\mathcal{R}(x)$.*

Por lo tanto, para que $P = \text{Irr}(x/K)$ es necesario y suficiente que sea mónico y que $Q(x) = 0$ si, y sólo si, $P|Q$. Debe observarse que si F es una extensión de K tal que x y F están contenidos en un mismo cuerpo, entonces x es también alg/F y, más aún, $\text{Irr}(x/F)|\text{Irr}(x/K)$.

Las extensiones de la forma $K(x)$ (es decir, que son generadas por un solo elemento) se llaman *simples*, y pueden ser finitas o infinitas. Se dice que x es un *elemento primitivo* de $K(x)$.

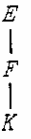
Cuando x es tras/K, $K[x]$ es isomorfo al anillo de los polinomios de $\{x\}$ y tiene como base el conjunto infinito de todas las potencias de x con exponente natural. En este caso, $K(x)/K$ es infinita y $K(x)$ es el cuerpo de cocientes de $K[x]$.

Si x es alg/K y si $P = \mathrm{Irr}(x/K)$ tiene grado n, entonces $K(x) = K[x]$ y $K(x)/K$ es finita. Una K-base de $K(x)$ es $\{1, x, \ldots, x^{n-1}\}$. El grado de P es igual al grado, o dimensión de la extensión. Es frecuente llamar *grado de x sobre K* (notación: $\mathrm{gr}(x/K)$), al grado de $\mathrm{Irr}(x/K)$.

El comportamiento de la idea de algebricidad con relación a las configuraciones elementales es el siguiente:

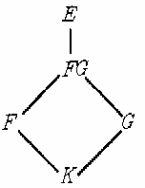
Proposición 3.

A. *Dada la torre*



E/K es algebraica si, y sólo si E/F y F/K son algebraicas.

B. *Dadas las extensiones*



FG/K es algebraica si, y sólo si F/K y G/K son algebraicas.

C. *En la situación de B, si F/K es algebraica, FG/G también lo es. El recíproco no es necesariamente verdadero.*

Demostración

A. Si E/K es algebraica es obvio que tanto E/F como F/K lo son. Recíprocamente, si E/F y F/K son algebraicas, sea x un elemento de E y $P = \mathrm{Irr}(x/F)$. Si $a_1, \ldots, a_n \in F$ son los coeficientes de P, entonces x es algebraico sobre $K(a_1, \ldots, a_n)$. Por la proposición 2, B, $K(a_1, \ldots, a_n)/K$ es finita y por la proposición 2, A, $K(x)/K$ también lo es. Luego, x es alg/K.

B. La parte A implica que si S es un conjunto finito de elementos de una extensión de K, entonces $K(S)/K$ es finita y, *a fortiori*, algebraica. Los elementos de FG son de la forma $(\sum x_i y_i)\,(\sum x'_j y'_j)^{-1}$ (con $x_i x'_j \in F$ e $y_i, y'_j \in G$). Luego, si F y G son algebraicos sobre K, FG también lo es. El recíproco es obvio.

C. Si F/K es algebraica cada elemento de F es algebraico sobre G (véase el comentario a continuación de la definición 4) y, por lo observado

anteriormente, FG/G es también algebraica. Finalmente, si $F = K(X)$ es un cuerpo de funciones racionales, y si $G = K(X^2)$, entonces F/K es trascendente, pero $FG = F$ es algebraica de grado 2 sobre G.

Corolario. *E/K es algebraica si, y sólo si, E es generado, sobre K, por un conjunto de elementos* alg$/K$.

Hasta este momento hemos clasificado las extensiones de las siguientes maneras:

-finitas o infinitas, según que la dimensión lo sea;

-finitamente generadas o no, según que exista o no un conjunto finito de generadores;

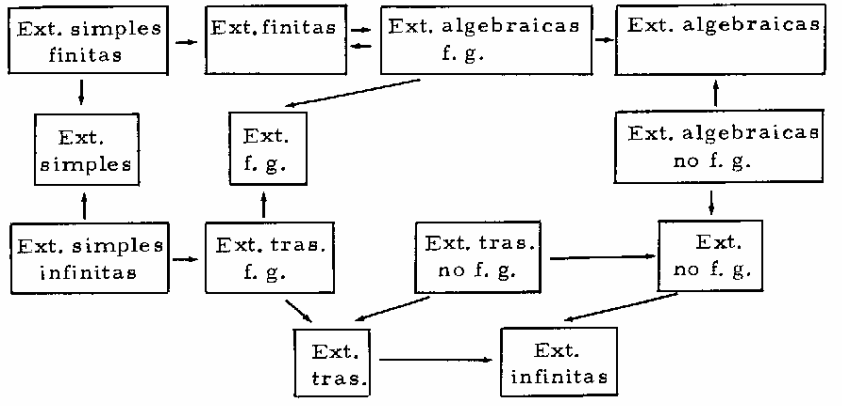
-trascendentes o algebraicas, según existan o no elementos trascendentes.

El criterio de Eisenstein (véase 1. 2, proposición 5) muestra que existen polinomios irreducibles de todos los grados sobre $\mathbb{Q}$. Como todo polinomio de grado impar sobre $\mathbb{Q}$ tiene una raíz en $\mathbb{R}$, existen subextensiones de grado arbitrariamente grande en $\mathbb{R}/\mathbb{Q}$. Por la proposición 3, el conjunto de los elementos de $\mathbb{C}$ que son alg$/\mathbb{Q}$ es una extensión algebraica de $\mathbb{Q}$, denotada por $\hat{\mathbb{Q}}$. $\hat{\mathbb{Q}}$ se llama el *cuerpo de los números algebraicos*. $\hat{\mathbb{Q}}/\mathbb{Q}$ es entonces un ejemplo de una extensión algebraica de dimensión infinita.

Puede demostrarse que el conjunto $\hat{\mathbb{Q}}$ es un conjunto enumerable (véase 4. 2, proposición 1). Esto implica que $\mathbb{R}/\mathbb{Q}$ es una extensión trascendente. Más en concreto es demostrable que las conocidas constantes e y π son trascendentes sobre $\mathbb{Q}$.

Por las proposiciones 3 y 2, E/K es finita si, y sólo si, es algebraica y finitamente generada.

Las relaciones entre los tipos de extensiones consideradas hasta aquí aparecen esquematizadas en el diagrama siguiente:



Ext. = extensiones; f. g. = finitamente generadas; tras. = trascendentes.

Ejemplo 1. *Cuerpos primos.* Todo cuerpo contiene un subcuerpo mínimo, que está determinado, salvo isomorfismo, por la característica. En efecto, al estudiar el concepto de característica (cf. I. 1) se observa que si K es un cuerpo de característica 0 entonces 1 genera un subcuerpo isoformo a $\mathbb{Q}$; y, si la característica de K es un número primo p, entonces $\mathbb{Z}1$ es un cuerpo isoformo a $\mathbb{Z}/(p)$, denotado por $\mathbb{F}_p$.

Estos cuerpos minimales se llaman *cuerpos primos*. $\mathbb{Q}$ es el cuerpo primo de característica 0; $\mathbb{F}_p$ es el cuerpo primo de característica p.

Todo cuerpo K es una extensión de su cuerpo primo P. Todo automorfismo de K, por dejar fijo 1, deja fijo cada elemento de P. Por lo tanto, $\mathrm{Aut}(K) = \mathrm{Aut}(K/P)$.

Si $\chi = p > 0$, K posee un automorfismo de particular importancia, llamado *automorfismo de Frobenius*, y se denota por F (o, si es necesario, por F_p). Es la aplicación "potencia de exponente p": $x \mapsto x^p$. Esta función es inyectiva y preserva la multiplicación. Pero también preserva la suma, pues cada número combinatorio de la forma $\binom{p}{i}$ $(i \neq 0, p)$ es múltiplo de p y, por lo tanto, se anula en K. Entonces:

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} \cdot x^{p-i} \cdot y^i = x^p + y^p$$

Lema. *Sea K un cuerpo y G un subgrupo finito de $(K - \{0\}, \cdot)$. Entonces G es cíclico.*

Demostración. Sean $x, y \in G$ de órdenes m y n, respectivamente, y sea $s = \mathrm{mmc}(m, n)$. Veamos que $\exists z \in G$ tal que $|z| = s$. Para cada primo p que divide s, sea z_p el elemento de $\langle x \rangle$ o de $\langle y \rangle$ cuyo orden es la potencia de p que divide s. Como los z_p conmutan y tienen órdenes relativamente primos, su producto, z, tiene orden s.

Entonces si N es el máximo de los órdenes de los elementos de G, resulta $x^N = 1$ para todo x de G. En efecto, si $|y| = N$ y $|x| = n$, existe z con orden $\mathrm{mmc}(n, N)$ y, como N es máximo, $\mathrm{mmc}(n, N) = N$ y resulta que $n \mid N$.

Esto implica que G está contenido en el conjunto de las raíces en K del polinomio $X^N - 1$. Por consiguiente, $|G| \leq N$, lo cual implica que $G = \langle y \rangle$.

Ejemplo 2. *Cuerpos finitos.* Todo cuerpo finito tiene característica positiva. Si K es un cuerpo finito con q elementos y con característica p, K es una extensión finita, de dimensión, digamos, n, de $\mathbb{F}_p$. Por lo tanto, $|K| = |\mathbb{F}_p|^n$, o sea $q = p^n$:

El número de elementos de un cuerpo finito es una potencia de un número primo.

Por el lema, $(K - \{0\}, .)$ es un grupo cíclico de orden $q - 1$ y, por lo tanto, todo elemento de K es una raíz del polinomio

$$X^q - X = X^{p^n} - X \in \mathbb{F}_p[X]$$

Como este polinomio tiene como máximo q raíces, resulta que K es igual al conjunto de todas sus raíces. Este polinomio no tiene raíces múltiples.

Sea E una extensión finita de un cuerpo finito K. Entonces E es finito y, por el lema, $E - \{0\}$ es un grupo cíclico generado por un cierto elemento a. Esto implica que $E = K(a)$:

Toda extensión finita de un cuerpo finito es simple.

Veamos ahora un ejemplo concreto. El polinomio $X^2 + X + 1$ no tiene raíces en $\mathbb{F}_2$ y, por consiguiente, es irreducible. Entonces $\mathbb{F}_2[X]/(X^2 + X + 1)$ es una extensión de grado 2 de $\mathbb{F}_2$ y por lo tanto es un cuerpo de 4 elementos. Si llamamos a este cuerpo K, tenemos que $(K, +)$ es un producto de dos grupos de 2 elementos: $(K, +)$ es isomorfo al 4-grupo de Klein. Si se representa K en la forma $K = \{0, 1, x, x + 1\}$, su tabla de multiplicación, obtenida con ayuda de la relación $x^2 = x + 1$, es:

x	0	1	x	$1 + x$
0	0	0	0	0
1	0	1	x	$1 + x$
x	0	x	$1 + x$	1
$1 + x$	0	$1 + x$	1	x

Ejemplo 3. Sea x el número real $2\sqrt{2} - \sqrt[3]{3}$. Por el criterio de Eisenstein, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es algebraica de grado 2 y $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ es algebraica de grado 3. Como $x \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, $\mathrm{gr}(x) \mid 6$ (cf. la proposición 2). $\mathrm{Irr}(x/\mathbb{Q})$ se obtiene buscando una combinación lineal nula de las primeras 6 potencias de x, con coeficientes racionales. Tenemos:

$$(x - 2\sqrt{2})^3 = x^3 - 6x^2\sqrt{2} + 24x - 16\sqrt{2} = 3$$

de donde

$$2\sqrt{2}(3x^2 + 8) = x^3 + 24x - 3$$

y, elevando al cuadrado:

$$x^6 - 24x^4 - 6x^3 + 192x^2 - 144x - 503 = 0$$

Deducimos que $\mathrm{Irr}(x/\mathbb{Q})$ es un divisor de $X^6 - 24X^4 - 6X^3 + 192X^2 - 144X - 503 =_{\mathrm{def}} P(X)$.

A las claras, para hallar $\mathrm{Irr}(x/\mathbb{Q})$ debiéramos factorizar P y ver cuál de sus divisores primos tiene a x como raíz. Esta tarea promete

ser larga y tediosa. Veamos que se puede evitar aplicando lo sabido sobre extensiones.

En primer lugar observamos que $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt[3]{3})$ es una extensión de $\mathbb{Q}$ cuya dimensión debe ser un divisor de 2 y de 3 (cf. la proposición 2, A). Esto implica que $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt[3]{3}) = \mathbb{Q}$.

Si fuera $gr(x/\mathbb{Q}) = 3$, como 9 no divide a 6, $(\mathbb{Q}(x, \sqrt[3]{3}) : \mathbb{Q}) = 3$, que implica $x \in \mathbb{Q}(\sqrt[3]{3})$ y $\sqrt{2} \in \mathbb{Q}(\sqrt[3]{3})$, lo cual es absurdo. Si fuera $gr(x/\mathbb{Q}) = 2$, como 4 no divide a 6, $(\mathbb{Q}(x, \sqrt{2}) : \mathbb{Q}) = 2$, y resulta nuevamente el absurdo que $\sqrt[3]{3} \in \mathbb{Q}(\sqrt{2})$. Por un razonamiento análogo tampoco puede ser $gr(x/\mathbb{Q}) = 1$, y se tiene finalmente que $gr(x/\mathbb{Q}) = 6$ y que $P = \mathrm{Irr}(x/\mathbb{Q})$.

Ejemplo 4. Considérese ahora el número real $x = \sqrt{2} + \sqrt{3}$. Procediendo como en el ejemplo 3, se ve que x es una raíz del polinomio entero $Q(X) = X^4 - 10X^2 + 19$.

Es inmediato que Q no tiene raíces racionales, de modo que, si no es irreducible sobre $\mathbb{Q}$, se factoriza en $\mathbb{Z}[X]$ en la forma $Q = A \cdot B$, con con A y B mónicos y de segundo grado:

$$A = X^2 + bX + c, \qquad B = X^2 + cX + d$$

La relación $Q = AB$ conduce a las ecuaciones:

$$a + c = 0$$

$$b + d + ac = -10$$

$$ad + bc = 0$$

$$bd = 19$$

Si $a = 0$, b y d son las raíces de $X^2 + 10X + 19$, que no tiene raíces enteras. Si $a \neq 0$, se deduce $b = d$, $bd = 19$, lo que es imposible en números enteros. Esto prueba que Q es irreducible sobre $\mathbb{Q}$ y, por lo tanto, $\mathrm{Irr}(x/\mathbb{Q}) = Q$. Como consecuencia, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(x)$, una extensión simple que tiene a x como elemento primitivo.

3. MORFISMOS, NORMALIDAD Y CUERPOS DE DESCOMPOSICIÓN

Para poder profundizar más en el estudio de las extensiones, se deben estudiar los morfismos.

Definición 1. *Sean E/K y F/K extensiones cualesquiera, y sea x un elemento de E. Se dice que y es un conjugado de x en F, sobre K (notación: $x \underset{K}{\sim} y$ o, simplemente, $x \sim y$), si existe $f \in \mathrm{Hom}(K(x)/K, F/K)$ tal que $f(x) = y$.*

La relación $\underset{K}{\sim}$ (ser conjugados sobre K) es una relación de equivalencia. De acuerdo con el teorema fundamental (1. 1, teorema 1) $x \sim y$ si, y sólo si, $P(x) = P(y)$. Por lo tanto,

$$x \underset{K}{\sim} y \Leftrightarrow \begin{cases} y \text{ es tras}/K \text{ (cuando } x \text{ es tras}/K) \\ \operatorname{Irr}(x/K) = \operatorname{Irr}(y/K) \text{ (cuando } x \text{ es alg}/K) \end{cases}$$

Cualquiera que sea el cuerpo F, un elemento alg/K tiene un número finito de conjugados en F, siempre menor que o igual al grado de dicho elemento.

Para facilitar la exposición, se usarán las locuciones siguientes:

Si $P \in K[X]$ y F es un cuerpo extensión de K, se dirá que P *se descompone (o factoriza) totalmente en* F *(o sobre* F*)* si $P(X) = a\prod_i (X - x_i)$ (con $a, x_i \in F$). También se dirá para significar lo mismo que P tiene todas sus raíces en F.

Decir que x *tiene todos sus conjugados en* F significa que $\operatorname{Irr}(x/K)$ se descompone totalmente en F.

Obsérvese que si P se descompone totalmente en K, entonces también se descompone totalmente en cualquier extensión de K. Obsérvese también que si P se descompone totalmente en K y si Q divide a P, entonces Q también se descompone totalmente en K.

El problema de hallar morfismos de una extensión en otra puede siempre encararse como caso particular del problema de prolongar un

morfismo a una extensión mayor. En efecto, f es un morfismo de E/K en G/K si, y sólo si, f extiende a E la inyección canónica $K \hookrightarrow G$. Como ya se ha dicho varias veces, las condiciones generales que rigen la prolongación de morfismos están implícitas en el teorema fundamental (l. 1, teorema 1) y dependen del ideal de las relaciones algebraicas de un conjunto de generadores de E sobre K.

Primer caso: extensiones simples. Por lo ya visto, el morfismo $K \hookrightarrow G$ puede prolongarse a $E = K(x)$ si, y sólo si, $\operatorname{Irr}(x/K)$ tiene una raíz x' en G (o sea, si, y sólo si, x tiene un conjugado en G sobre K). Cada uno de tales elementos x' determina la extensión, que es el único K-morfismo que lleva x en x'.

Más generalmente, sea $f \in \operatorname{Hom}(F/K, G/K)$ y $E = F(x)$. Denótese por P el polinomio $\operatorname{Irr}(x/F)$ y supóngase que sea $P(X) = X^n + a_1X^{n-1} + \ldots + a_n$. Para que f pueda prolongarse a un K-morfismo de E en G es necesario y suficiente que $f(P) = X^n + f(a_1)X^{n-1} + \ldots + f(a_n)$ (véase l. 1, Obs. 3) tenga una raíz x' en G. En tal caso, la prolongación, f', está determinada por la condición $f'(x) = x'$. Como $P \mid \operatorname{Irr}(x/K)$ y como f deja fijo $\operatorname{Irr}(x/K)$, se tiene que $f(P)$ también divide a $\operatorname{Irr}(x/K)$. Por lo tanto, una condición *suficiente* para la existencia de la prolongación f' es que $\operatorname{Irr}(x/K)$ se descomponga totalmente en G. En tal caso, el número de prolongaciones f' es igual al número de raíces de $f(P)$ en G, o sea menor que o igual a $\operatorname{gr}(f(P)) = \operatorname{gr}(P) = (E : F)$.

Segundo caso: extensiones finitas. Consideremos la torre

$$\begin{array}{c} E \\ | \\ F \\ | \\ K \end{array}$$

y sea $f \in \mathrm{Hom}(F/K, G/K)$. Mostremos que también en este caso, si E/F es finita, para que f pueda prolongarse a E es suficiente que $\forall x \in E$, $\mathrm{Irr}(x/K)$ se descomponga totalmente en G y que, en tal caso, el número total de prolongaciones sea menor que o igual a $(E : F)$.

Como toda extensión finita es finitamente generada, se puede escribir $E = F(x_1, \ldots, x_n)$ (x_1 alg/F) y razonar por inducción en m. Por el primer caso, este teorema es cierto para $m = 1$. Si el teorema es cierto para $m - 1$, f tiene un cierto número n_1, de prolongaciones f_i a $F(x_1, \ldots, x_{m-1})$ y $n_1 \leq (F(x_1, \ldots, x_{m-1}) : F)$. Por el primer caso, cada f_i tiene un cierto número n_i' de prolongaciones a $E = F(x_1, \ldots, x_{m-1})(x_m)$, y todos estos n_i' son menores que o iguales a $n_2 = (E : F(x_1, \ldots, x_{m-1}))$. Contando, se obtiene que f tiene $\sum_{i=1}^{n_1} n_i' \leq n_1 n_2 \leq (F(x_1, \ldots, x_{m-1}) : F)$. $(E : F(x_1, \ldots, x_{m-1}) = (E : F)$ (véase 2, proposición 2).

Proposición 1. *Sea E/K una extensión finita. Son equivalentes:*

1) $\forall x \in E$, x *tiene todos sus conjugados en* E;

2) *Si un polinomio $P \in K[X]$ es irreducible y tiene una raíz en E, entonces P se descompone totalmente en E;*

3) *Dadas las extensiones*

$$\begin{array}{c} G \\ | \\ E \\ | \\ F \\ | \\ K \end{array}$$

todo $f \in \mathrm{Hom}(F/K, G/K)$ tiene su imagen en E y puede prolongarse a un automorfismo de E/K.

En (3), *el número de prolongaciones de f a E sólo depende de E/F (y no de f) y es menor que o igual a $(E : F)$. En particular,* $\mathrm{Aut}(E/K)$ *es un grupo finito, de orden menor que o igual a $(E : K)$ cualquiera que sea la extensión finita E/K.*

Demostración. Es claro que (1) es equivalente a (2) y, por lo visto anteriormente, (2) implica que todo morfismo f de F/K en G/K puede prolongarse a E, siendo el número de estas prolongaciones menor que o igual a $(E : F)$. El mismo análisis anterior muestra que las imágenes de estas prolongaciones están en E y son, por lo tanto, automorfismos de E/K.

Para completar la prueba de que (2) implica (3) basta mostrar que el número de prolongaciones de f no depende de f. Si g es otro morfismo de F/K en G/K considérese el conjunto $H = \{h \in \mathrm{Aut}(E/K)/hf = g\}$ (es decir, H es el conjunto de las prolongaciones de gf^{-1} de $f(F) \subset E$ a E). Entonces es inmediato comprobar que $f' \mapsto hf'$ define una biyección del conjunto de las prolongaciones de f sobre el conjunto de las prolongaciones de g.

Para terminar, demostremos que (3) implica (2). Sea P un polinomio irreducible sobre K que tiene una raíz, x, en E, y sea Q un divisor primo de P sobre E. Sea $G = E[X]/(Q)$, de modo que G es una extensión de la forma $E(y)$ con y una raíz de Q en G, El morfismo de $K(x)$ en $K(y)$ que lleva x en y debe tener, por (3), su imagen en E. Esto implica que $y \in E$, de donde $G = E$ y $\mathrm{gr}(Q) = 1$.

Definición 2. *Una extensión finita E/K se llama normal cuando cumple una de las condiciones equivalentes de la proposición* 1.

Definición 3. *Se llama cuerpo de descomposición sobre K (o cuerpo de las raíces sobre K) de un polinomio $P \in K[X]$ a toda extensión E/K tal que:*

1) *P se factoriza totalmente sobre E;*

2) *Si F es una subextensión de E y P se factoriza totalmente sobre F, entonces $F = E$.*

Obsérvese que si un cuerpo L contiene un cuerpo de descomposición de P sobre K, resulta que éste es único. En efecto, L contiene todas las raíces de P y el cuerpo de descomposición de P es el generado por estas raíces sobre K.

Obsérvese también que si E/K es normal y si P es un polinomio irreducible que tiene una raíz en E, resulta que E contiene un cuerpo de descomposición de P. Más aún, si E es generada sobre K por $x_1, \ldots, x_m$, y si $P_i = \mathrm{Irr}(x_i/K)$, entonces E es el cuerpo de descomposición sobre K del polinomio $P = P_1 P_2 \ldots P_m$:

Toda extensión normal (finita) es el cuerpo de descomposición de un polinomio.

Proposición 2. *Sea $P \in K[X]$ un polinomio de grado positivo n.*

A. *Existe un cuerpo de descomposición L de P sobre K.*

B. *L/K es finita de grado menor que o igual a $n!$.*

C. *L/K es normal.*

D. *Si L/K y L'/K son cuerpos de descomposición de P, son isomorfos.*

Demostración

A. Consideremos los divisores primos de P sobre una extensión finita F de K, y sea m el mayor de sus grados. Elíjase F de modo que m sea

mínimo y, entre ellas, de modo que el número de divisores primos de P con grado m sea también mínimo. Sea Q un divisor primo de P sobre F con grado m y sea E la extensión $F[X]/(Q)$. Si m fuera mayor que 1, P tendría en E menos divisores primos de grado m, lo que contradice la elección de F. Luego, $m = 1$ y P se factoriza totalmente en F. Luego, F contiene un cuerpo de descomposición de P sobre K, L.

B. Si $x_1, \ldots, x_n$ son las raíces de P en L, n es menor que o igual a n y se tiene una torre:

$$\begin{array}{ll} F_n = L & \\ \vert & \\ F_{n-1} & \\ \vert & \\ \vdots & \text{donde } F_i = K(x_1, \ldots, x_i) \\ \vert & \\ F_1 & \\ \vert & \\ F_0 = K & \end{array}$$

Bastará probar que $(F_{i+1} : F_i) \leq n - i$. Como $P(X) = (X - x_1)(X - x_2)\ldots$ $\ldots (X - x_i) \cdot Q$, $\mathrm{gr}(Q) = n - i$ y $\mathrm{Irr}(x_{i+1}/F_i) : Q$.

C. Conservemos las notaciones de B y demostremos que L/K verifica la condición (3) de la proposición 1. Si $F = L$ y si f es un morfismo de L/K en otra extensión G/K (donde G contiene L), como L es generado por los x_i sobre K y como $f(x_i)$ es una raíz de P, $f(L) = L$. Si $F \neq L$, existe un i tal que $F_i \subset F \subsetneq F_{i+1}$, de modo que $F_{i+1} = F(x_{i+1})$. Sea $Q = \mathrm{Irr}(x_{i+1}/F) = X^k + a_1 X^{k-1} + \ldots + a_k$. Como $Q \mid P$, $f(Q)$ también divide a P y por lo tanto tiene sus raíces en L. Eso implica que f puede prolongarse a F_{i+1}. Repitiendo este argumento un número finito de veces tenemos que f se prolonga a un automorfismo de L. 41

D. El mismo argumento anterior muestra que la inclusión $K \hookrightarrow L'$ se prolonga a un K-morfismo de L en L'. Entonces su imagen es un cuerpo de descomposición de P y, por consiguiente, es igual a L'.

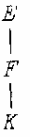
Así hemos demostrado que los conceptos "extensión normal finita" y "cuerpo de descomposición de un polinomio" son equivalentes. También resulta que toda extensión finita E/K está contenida en una mínima extensión normal, N/K, que diremos es generada por E sobre K. En efecto, si $x_1, \ldots, x_n$ generan E/K, y si P es el producto de sus polinomios irreducibles sobre K, entonces el cuerpo de descomposición de P sobre E es la mínima extensión de E que es normal sobre K.

Sigue también de la proposición (1) que la intersección de una familia de extensiones normales es una extensión normal.

El comportamiento de la normalidad con relación a las configuraciones elementales es el siguiente:

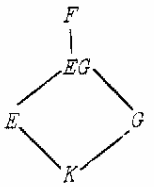
Proposición 3. *Sea E/K una extensión finita.*

A. *Dada la torre:*



si E/K es normal, E/F también lo es, pero es posible que F/K no lo sea. Hay ejemplos en que E/F y F/K son normales, mientras que E/K no lo es.

B. *Dadas las extensiones:*



si E/K y G/K son normales, EG/K también lo es. Es posible que EG/K sea normal sin que E/K o G/K (o ambas) lo sean.

C. *En la situación anterior, si E/K es normal, EG/G también lo es, pero el recíproco no es necesariamente verdadero.*

Demostración

A. Como todo F-conjugado de x es un K-conjugado de x, E/K normal implica E/F normal.

Sea $P(X) = X^3 - 2 \in \mathbb{Q}[X]$, y sea E su cuerpo de descomposición sobre $\mathbb{Q}$. Si w es una raíz cúbica compleja de 1 y si $\sqrt[3]{2}$ es la raíz cúbica real de 2, entonces $E = \mathbb{Q}(\sqrt[3]{2}, w)$. La extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal pues $\sqrt[3]{2} \cdot w$ es un conjugado de $\sqrt[3]{2}$ que (por no ser real) no está en $\mathbb{Q}(\sqrt[3]{2})$.

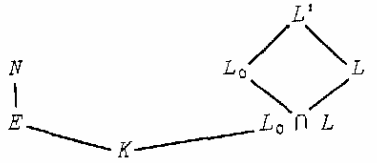
Toda extensión de grado 2 es normal, pues es igual al cuerpo de descomposición de un polinomio de segundo grado (si un polinomio de segundo grado tiene una raíz en un cuerpo, tiene las dos). Sea r la raíz cuarta real positiva de 2 y sea s la raíz cuadrada positiva de 2. Entonces $\mathbb{Q}(r)$ no es normal (pues r tiene conjugados no reales), pero las dos extensiones: $\mathbb{Q}(r)/\mathbb{Q}(s)$ y $\mathbb{Q}(s)/\mathbb{Q}$, por ser de dimensión 2, son normales.

B. Si E es el cuerpo de descomposición de P y G es el cuerpo de descomposición de Q, entonces EG es el cuerpo de descomposición de PQ. La extensión $\mathbb{Q}(\sqrt[3]{2}, w)/\mathbb{Q}$ estudiada en A es el compuesto de $\mathbb{Q}(\sqrt[3]{2})$ y $\mathbb{Q}(\sqrt[3]{2} \cdot w)$, que no son normales.

C. Si E es el cuerpo de descomposición de P sobre K, EG es el cuerpo de descomposición de P sobre G. $\mathbb{Q}(\sqrt[3]{2}, w)$ es el cuerpo de descomposición de $X^3 - 2$ sobre $\mathbb{Q}(w)$, pero $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal.

Grado de Separabilidad

Consideremos el conjunto finito $\mathrm{Hom}(E/K, L/K)$, donde E/K es finita y L/K arbitraria. Sea N la mínima extensión de E que es normal sobre K (véase la observación que precede a la proposición 3): N es el cuerpo de descomposición de un cierto polinomio P sobre K. Sean L' el cuerpo de descomposición de P sobre L y L_0 el cuerpo de descomposición de P sobre K que está contenido en L'. Se tiene la configuración siguiente:



y se sabe que existe un K-morfismo, $\mathcal{Q}$, de N sobre L_0.

Cada $f \in \mathrm{Hom}(E/K, L/K)$ está determinada por los valores que toma en las raíces de P en E. Por lo ya observado, estos valores pertenecen a $L_0 \cap L$. En este sentido, $\mathrm{Hom}(E/K, L/K) \subset \mathrm{Hom}(E/K, L_0 \cap L/K)$.

Por otra parte, mediante $\mathcal{Q}$, se puede definir una inyección de $\mathrm{Hom}(E/K, L/K)$ en $\mathrm{Hom}(E/K, N/K)$:

$$f \rightarrow \mathcal{Q}^{-1} f \qquad [1]$$

Para que ésta sea una biyección, es decir para que sea sobre $\mathrm{Hom}(E/K, N/K)$, es necesario y suficiente que $L_0 \subset L$ (o sea, que L contenga una copia de N).

En efecto, si $L_0 \subset L$, cada $g \in \mathrm{Hom}(E/K, N/K)$ es imagen por [1] de $\mathcal{Q} g \in \mathrm{Hom}(E/K, L/K)$. Recíprocamente, si [1] es sobre, $L_0 \subset L$. Pues, en primer lugar, [1] sobre implica que $E \hookrightarrow N$ es de la forma $\mathcal{Q}^{-1} f$ para algún $f : E \rightarrow L$, y se deduce que $f = \mathcal{Q}|_E$ y, por lo tanto, $\mathcal{Q}(E) \subset L$. Si fuera ahora $L_0 \not\subset L$ deduciríamos un absurdo. Pues si L_0 no está contenido en L, existe una raíz de P, x' en L_0 y fuera de L. Elijamos $x \in L_0 \cap L$, $x \sim x'$, imagen por $\mathcal{Q}$ de una raíz de P en E y sea f' un morfismo que prolonga $K(x) \rightarrow K(x')$. Entonces $\mathcal{Q}^{-1} f' \mathcal{Q} : E \rightarrow N$ debe ser de la forma $\mathcal{Q}^{-1} f$ para algún $f : E \rightarrow L$. Esto implica que $f' \mathcal{Q} = f$ y, por lo tanto, que $\mathrm{Im}(f') \subset L$, lo que es absurdo.

Este análisis muestra que para describir $\mathrm{Hom}(E/K, L/K)$ es suficiente conocer $\mathrm{Hom}(E/K, N/K)$: los morfismos de E en una extensión que es normal y finita sobre K. También se ve que $\mathrm{Hom}(E/K, N/K)$ es en esencia el mismo, cualquiera que sea la extensión normal N/K que contiene a E, pues el caso en que L/K es normal y contiene una copia de E, conduce a $L_0 \subset L$ y a que hay una biyección entre $\mathrm{Hom}(E/K, N/K)$ y $\mathrm{Hom}(E/K, L/K)$.

Definición 4. A. *Dada la extensión finita E/K, se llama grado de separabilidad de E sobre K* (notación: $(E:K)_s$) *al número de K-morfismos de E en una extensión de E que sea normal sobre K.*

B. *Si x es alg/K, se llama grado de separabilidad de x sobre K* (notación $\mathrm{grs}(x/K)$) *a* $(K(x) : K)_s$.

C. *Si $P \in K[X]$ es irreducible, se llama grado de separabilidad de P* (notación: $\mathrm{grs}(P)$) a $((K[X]/(P)) : K)_s$.

Obsérvese que, cualquiera sea L/K, se tiene:

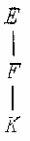
$$|\,\mathrm{Hom}(E/K, L/K)\,| \leq (E : K)_s \leq (E : K)$$

Ejemplo 1. Si $E = K(x)$ es finita sobre K, entonces $(E : K)_s$ es igual al número de conjugados distintos de x.

El comportamiento del grado de separabilidad con relación a las configuraciones elementales es el siguiente:

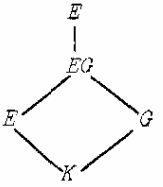
Proposición 4. *Sea E/K una extensión finita*

A. *Dada la torre*



se tiene que $(E : K)_s = (E : F)_s \cdot (F : K)_s$.

B. *Dada la configuración*



$(EG : G)_s \leq (E : K)_s$.

C. *En la situación anterior, si G/K es también finita,*

$$(EG : K)_s \leq (E : K)_s \cdot (G : K)_s .$$

Demostración

A. Sea N una extensión normal de K que contiene a E.

Tenemos:

$$(F : K)_s = |\mathrm{Hom}(F/K, N/K)|$$

$$(E : F)_s = |\mathrm{Hom}(E/F, N/F)|$$

$$(E : K)_s = |\mathrm{Hom}(E/K, N/K)|$$

$\mathrm{Hom}(E/K, N/K)$ se obtiene prolongando a E, de todas las maneras posibles, todos los elementos de $\mathrm{Hom}(F/K, N/K)$ y todos ellos tienen el mismo número de prolongaciones que es igual a $|\mathrm{Hom}(E/F, N/F)|$ (véase la proposición 1).

B. NG es una extensión normal de G que contiene a EG (véase la proposición 3). Cada $f \in \mathrm{Hom}(EG/G, NG/G)$ define, por restricción, un elemento de $\mathrm{Hom}(E/K, N/K)$, y esta aplicación es inyectiva, pues cada G-morfismo, siendo la identidad sobre G, está determinado por su restricción a E.

C. $(EG : K)_s = (EG : G)_s \cdot (G : K)_s \leq (E : K)_s \cdot (G : K)_s$.

Observación. Como el cuerpo de descomposición de un polinomio P sobre K es esencialmente único, se usará, si no hay posibilidad de confusión, la notación P/K para representar a uno cualquiera de ellos.

Ejemplo 2. El ejemplo 2 de 2 indica que todo cuerpo finito es una extensión normal de su cuerpo primo. Por consiguiente, toda extensión E/K en que E es un cuerpo finito, es normal.

Ejemplo 3. Sea w una raíz compleja de 1. El grupo multiplicativo generado por w tiene un cierto orden finito, n, y es el conjunto de las raíces de $X^n - 1$ en $\mathbb{C}$.

Por lo tanto, $\mathbb{Q}(w)$ es el cuerpo de descomposición de $X^n - 1$ y es una extensión normal de $\mathbb{Q}$.

4. LA TEORIA DE GALOIS

El matemático francés Evaristo Galois (1811-32) pasó a la inmortalidad por haber resuelto en forma satisfactoria el problema de cuáles son las ecuaciones polinómicas resolubles por radicales. No obstante, la contribución más significativa de Galois fue mostrar la importancia que tienen los automorfismos de un cuerpo en el estudio de ese cuerpo como extensión de uno de sus subcuerpos.

Muchos textos pasan por alto que, para la teoría de Galois, la manera natural de definir una extensión E/K es a partir del cuerpo mayor, E. Es al adoptar este punto de vista cuando la teoría se presenta en la forma más simple, destacándose mejor el papel de los morfismos. Comenzaremos, pues, de esta manera, dejando para después el problema de presentar las extensiones de Galois, E/K, a partir del cuerpo de base, K.

Observación

Sean E un cuerpo y A un conjunto de sus automorfismos. El conjunto $\{x \in E / f(x) = x (\forall f \in A)\}$ es un subcuerpo de E, llamado *el cuerpo fijo* de A (*notación*: E^A). Este cuerpo es también el cuerpo fijo del grupo de automorfismos generado por A.

Dado un conjunto S de elementos de E, el conjunto $\{f \in \mathrm{Aut}(E)/f(s) = s (\forall s \in S)\}$ es un grupo, el *grupo de los S-automorfismos de E (nota-*

ción: $\mathrm{Aut}(E/S)$). Si K es el subcuerpo generado por S, este grupo coincide con el grupo de los K-automorfismos de E.

Definición 1. *Se dice que E/K es de Galois con grupo G si existe un subgrupo finito de* $\mathrm{Aut}(E)$, G, *tal que* $E^G = K$.

Teorema 1. *Sea E/K de Galois con grupo G de orden n.*

A. *Todo elemento x de E es alg/K de grado $\leq n$.*

B. $\forall x \in E$, $\mathrm{Irr}(x/K)$ *se descompone totalmente en E y no tiene raíces múltiples* (por tanto, E/K es normal).

C. *E/K es una extensión simple, y por lo tanto, finita.*

D. $(E : K) = |G| = n$.

E. $\mathrm{Aut}(E/K) = G$.

F. *Si H es un grupo de automorfismos de E tal que $E^H = K$, entonces $H = G$. Por lo tanto G es único, y se lo puede denotar por* $\mathrm{gal}(E/K)$.

Demostración

A y B. Sea $\{x_1, \ldots, x_r\} = \{f(x)/f \in G\}$ y sea $P(X) = \prod_{i=1}^{r}(X - x_i)$. Entonces $f(P) = P$ para todo $f \in G$, de modo que P tiene sus coeficientes en K. Como $P(x) = 0$, $\mathrm{Irr}(x/K) \mid P$ y como todos los x_i son K-conjugados de x, $\mathrm{Irr}(x/K) = P$. Se deduce que $\mathrm{gr}(x) = r \leq n$.

C. Supongamos primero que K es un cuerpo finito y sea y un elemento de E de grado máximo. Si $E \neq K(y)$ existe z tal que $K(y, z) \supsetneq K(y)$, y existe x tal que $K(z, y) = K(x)$ (véase 2, ejemplo 2), lo que contradice la elección de y. Supongamos, en segundo lugar, que K es infinito y, razonando por reducción al absurdo, elijamos y y z, como en el argumento precedente. Sea $M = \mathrm{Hom}(K(y, z)/K, E/K)$. Como z no está en $K(y)$ y tiene todos sus conjugados distintos (es decir, $\mathrm{Irr}(z/K)$ no tiene raíces múltiples), cada morfismo de $K(y)$ en E tiene más de una prolongación a $K(y, z)$ (véase 3, proposición 1), de modo que $|M| > \mathrm{gr}(y)$.

Considérense las ecuaciones:

$$f(y) + Xf(z) = g(y) + Xg(z)$$

una para cada par de morfismos distintos $f, g \in M$. Si $f(z) = g(z)$, como $f \neq g$, $f(y) \neq g(y)$ y la ecuación no tiene solución. Por lo tanto existe un número finito de elementos de K que son solución de alguna de aquellas ecuaciones y, siendo K infinito, existe $a \in K$ tal que $f, g \in M$, $f \neq g$ implica $f(y + az) \neq g(y + az)$. Como consecuencia, $\mathrm{gr}(y + az) > \mathrm{gr}(y)$, lo que es una contradicción.

D y E. Sea $E = K(x)$. Entonces, por A, $(E : K) = \mathrm{gr}(x) \leq |G|$. Por otra parte, $G < \mathrm{Aut}(E/K)$ y, siendo E/K simple, $|\mathrm{Aut}(E/K)| \leq \mathrm{gr}(x)$.

F. Todo lo anterior es consecuencia de la hipótesis $E^G = K$. Por lo tanto, si $E^H = K$ se tiene también $H = \mathrm{Aut}(E/K) = G$.

Teorema 2. *Teorema fundamental de la teoría de Galois. Sea E/K de Galois con grupo G.*

A. *Las aplicaciones $H \mapsto E^H$ y $F \mapsto \mathrm{Aut}(E/F)$ definen biyecciones inversas entre sí entre el conjunto de los subgrupos de G y el conjunto de los cuerpos intermedios entre K y E.*

B. *Esta correspondencia es un isomorfismo de orden (decreciente) para las relaciones de inclusión*

C. *Si F es un cuerpo intermedio, E/F es de Galois.*

D. *Si F es un cuerpo intermedio y $f \in G$,*

$$\mathrm{gal}(E/f(F)) = f \cdot \mathrm{gal}(E/F) \cdot f^{-1}$$

E. *Si F es un cuerpo intermedio, para que F/K sea de Galois es necesario y suficiente que* $\mathrm{gal}(E/F) \lhd \mathrm{gal}(E/K) = G$, *y en tal caso* $\mathrm{gal}(F/K) \cong \dfrac{\mathrm{gal}(E/K)}{\mathrm{gal}(E/F)}$.

Demostración

A y B. Por definición, E/E^H es de Galois con grupo H. Luego, por el teorema 1, $\mathrm{Aut}(E/E^H) = H$, lo que significa que la composición de la primera y la segunda aplicaciones es la identidad en el conjunto de los subgrupos de G. Ahora, si F es un cuerpo intermedio, la compuesta en el otro orden asocia F con $E^{\mathrm{Aut}(E/F)}$. Si denotamos $\mathrm{Aut}(E/F)$ por H debemos demostrar entonces que $E^H = F$. Si $E = K(x)$, $E = F(x)$ y, como x tiene todos sus K-conjugados distintos, existen $(E : F)$ automorfismos de E/F, lo que prueba que H tiene $(E : F)$ elementos. Pero el teorema 1 dice que $|H| = (E : E^H)$ y entonces deducimos que, como se quería demostrar $E^H = F$ (pues es claro que $E^H \supset F$).

C. Se sigue de lo demostrado en A.

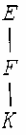
D. $g \in \mathrm{gal}(E/f(E))$ si, y sólo si, para todo $x \in F$, $g(f(x)) = f(x)$, o sea si, y sólo si, $f^{-1}gf(x) = x$, que equivale a $f^{-1}gf \in \mathrm{gal}(E/F)$.

E. Si F/K es de Galois, es normal y, por consiguiente, $f(F) = F$ para todo f de G. Entonces D implica que $\mathrm{gal}(E/F)$ es normal en G. Recíprocamente, si esta condición se cumple, D implica que $f(F) = F$ para todo f de G. Quiere decir que la aplicación $f \mapsto f|_F$ define un epimorfismo de G sobre $\mathrm{Aut}(F/K)$, lo que implica que G y $\mathrm{Aut}(F/K)$ tienen el mismo cuerpo fijo, K. Resulta que F/K es de Galois. Como el núcleo de aquella aplicación de restricción es precisamente el conjunto de los f de G que se reducen a la identidad en F, es decir $\mathrm{gal}(E/F)$, la demostración está completa (aplíquese el teorema del epimorfismo para grupos).

El comportamiento de las extensiones de Galois con relación a las configuraciones elementales es el siguiente:

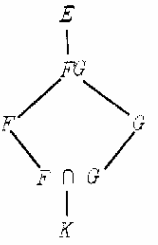
Proposición 1.

A. *Dada la torre*



si E/K es de Galois, E/F también lo es, pero F/K puede no ser de Galois.

B. *Dada la configuración*



si F/K y G/K son de Galois, entonces FG/K y $(F \cap G)/K$ son de Galois y $\mathrm{gal}(FG/(F \cap G)) \cong \mathrm{gal}(FG/F) \times \mathrm{gal}(FG/G) \cong \mathrm{gal}(F/(F \cap G)) \times \mathrm{gal}(G/(F \cap G))$. *Es posible que FG/K sea de Galois sin que ni F/K ni G/K lo sean.*

C. *En la situación de* B, *si F/K es de Galois con grupo H, entonces cualquiera que sea G/K, FG/G es de Galois con grupo isomorfo a* $\mathrm{gal}(F/F \cap G) < H$. *En tal caso, además, F y G son* L. D. *sobre $F \cap G$.*

Es posible que sea FG/G de Galois sin que F/K lo sea.

Demostración

A. Ya se demostró en el teorema 2.

B. Sean F/K y G/K de Galois y, por lo tanto, normales. Entonces FG/K es normal (véase 3, proposición 3, B) y las operaciones de restricción definen sendos epimorfismos de $\mathrm{Aut}(FG/K)$ sobre $\mathrm{gal}(F/K)$ y $\mathrm{gal}(G/K)$, respectivamente. Esto implica que el cuerpo fijo de $\mathrm{Aut}(FG/K)$ es K y, por lo tanto, FG/K es de Galois. Un argumento similar, observando además que $(F \cap G)/K$ es normal por ser intersección de extensiones normales, prueba también que $(F \cap G)/K$ es de Galois.

Sean ahora $H = \mathrm{gal}(FG/(F \cap G))$, $H_1 = \mathrm{gal}(FG/F)$ y $H_2 = \mathrm{gal}(FG/G)$. Las operaciones de restricción definen, respectivamente, sendos epimorfismos de H_1 sobre $\mathrm{gal}(G/G \cap F))$ y de H_2 sobre $\mathrm{gal}(F/(F \cap G))$. Estos son, de hecho, isomorfimos pues, por ejemplo, el núcleo del primero está

formado por todos los f de $\mathrm{gal}(FG/F)$ que se reducen a la identidad en G, y sólo la identidad satisface esta condición.

Por otro lado, las operaciones de restricción definen sendos epimorfismos de H sobre $\mathrm{gal}(F/(G \cap F))$, con núcleo H_1, y sobre $\mathrm{gal}(G/(G \cap F))$, con núcleo H_2.

El teorema fundamental (teorema 2, A y B) implica, finalmente, que $H_1H_2 = H$ y que $H_1 \cap H_2 = 1$.

El mismo ejemplo dado al demostrar la proposición 3, B de 3 muestra que puede ser FG/K de Galois, sin que F/K y G/K lo sean.

C. Sigue de 3, proposición 3, C que FG/G es normal. Si $F = K(x)$, $FG = G(x)$ y $\mathrm{Irr}(x/G) \mid \mathrm{Irr}(x/K)$. Como los coeficientes de $\mathrm{Irr}(x/G)$ son las funciones simétricas de los conjugados de x (cf. 1.3,3), están en F. Esto prueba que $\mathrm{Irr}(x/G) = \mathrm{Irr}(x/(G \cap F))$, que implica $(FG : G) = (F : (F \cap G))$. Luego, F y G son L. D. sobre $(F \cap G)$ (véase la indicación a continuación de 2, definición 2).

Por otro lado, la normalidad de FG/G implica que $\mathrm{Aut}(FG/G)$ tiene tantos elementos como conjugados tiene x sobre G, o sea tantos como $(FG : G)$, y esto implica que FG/G es de Galois. Como vimos en la demostración de B la operación de restricción define un isomorfismo de $\mathrm{gal}(FG/G)$ sobre $\mathrm{gal}(F/(F \cap G))$.

El mismo ejemplo dado en la demostración de 3, proposición 3, C muestra que puede ser FG/G de Galois sin que F/K lo sea.

Ejemplo 1. *La ecuación general de grado n.*

Sea $\mathcal{X} = \{X_1, \ldots, X_n\}$ un conjunto de letras y $E = K(X_1, \ldots, X_n)$ el cuerpo de las funciones racionales en las X_i sobre K. Sean $s_1, \ldots, s_n$ las funciones simétricas elementales de las X_i (véase 1.3, definición 1) y sea $F = K(s_1, \ldots, s_n)$.

Como se vio ya, el grupo simétrico S_n opera fielmente en E y puede ser identificado con un subgrupo de $\mathrm{Aut}(E/F)$. Por otro lado, E es un cuerpo de descomposición sobre F del polinomio $X^n - s_1X^{n-1} + s_2X^{n-2} + \ldots + (-1)^n s_n$, de modo que $(E : F) \leq n!$ (véase 3, proposición 2, B). Si F' es el cuerpo fijo de S_n, F' contiene a F y E/F' es de Galois con grupo S_n y, por consiguiente, $(E : F') = |S_n| = n!$ Esto prueba que $F' = F$, o sea: E/F es de Galois con grupo S_n.

Se demostrará ahora que los s_i son algebraicamente independientes, es decir que el ideal de sus relaciones algebraicas es 0 o, lo que es equivalente, que $K[s_1, \ldots, s_n]$ es el anillo de los polinomios en las s_i.

Se razonará por inducción en n ya que la afirmación es trivial si $n = 1$. Si se llama $s_1', \ldots, s_{n-1}'$ a las funciones simétricas elementales de $X_1, \ldots, X_{n-1}$, es inmediato que $s_i'(X_1, \ldots, X_{n-1}) = s_i(X_1, \ldots, X_{n-1}, 0)$. Sea P un polinomio no nulo de grado mínimo que se anula en las s_i. Considerando P como polinomio en X_n con coeficientes en $K[X_1, \ldots, X_{n-1}]$, se ve que al hacer $X_n = 0$ resulta un polinomio en $X_1, \ldots, X_{n-1}$ que, como

polinomio en $s'_1, \ldots, s'_{n-1}$, debe ser igual a 0 (por la hipótesis de inducción). Esto prueba que P es divisible por X_n. De la misma manera se demuestra que cada X_i divide a P y, por lo tanto, s_n divide a $P : P = s_n \cdot P'$. Se deduce que P', como polinomio en $s_1, \ldots, s_n$, es 0 en contradicción con la elección de P.

Sean $A_1, \ldots, A_n, X$ letras y sea K un cuerpo. Se llama *ecuación general de grado n sobre K* a la ecuación:

$$P(X) = X^n + A_1 X^{n-1} + \ldots + A_n = 0$$

donde $P \in K(A_1, \ldots, A_n)[X]$.

Sea L un cuerpo de descomposición de P sobre $K(A_1, \ldots, A_n)$. Si a cada A_i se asocia $(-1)^i s_i$ se obtiene un isomorfismo de $K(A_1, \ldots, A_n)$ sobre $K(s_1, \ldots, s_n)$ que transforma P en el polinomio $X^n - s_1 X^{n-1} + \ldots + (-1)^n s_n$, cuyo cuerpo de descomposición es E. Esto implica que $L/K(A_1, \ldots, A_n)$ es una extensión de Galois isomorfa con E/F y tiene como grupo de Galois el grupo simétrico S_n:

El cuerpo de las raíces de la ecuación general de grado n es una extensión de Galois del cuerpo de los coeficientes cuyo grupo es el grupo simétrico S_n.

Como aplicación de los resultados anteriores se puede demostrar el siguiente:

Teorema 3. *Teorema fundamental de las funciones simétricas. Todo polinomio simétrico en las letras $X_1, \ldots, X_n$ es un polinomio en las funciones simétricas elementales $s_1, \ldots, s_n$.*

Demostración. Si un polinomio $f \in K[X_1, \ldots, X_n]$ es simétrico, es invariante para S_n y, por lo tanto, pertenece a $F = K(s_1, \ldots, s_n)$. O sea: f es una función racional de las s_i.

Para el lector que conoce los elementos de la teoría de enteros algebraicos, la demostración se completa así: como $K[X_1, \ldots, X_n]$ es entero sobre $K[s_1, \ldots, s_n]$, y como éste es un anillo factorial (y, por consiguiente, integralmente cerrado), entonces $f \in K[s_1, \ldots, s_n]$.

Una demostración más explícita es la siguiente. Sea B el conjunto de todos los monomios en las X_i cuyo grado, con relación a cada una de las X_i, es menor que n. Como cada X_i es una solución de $X^n - s_1 X^{n-1} + \ldots + (-1)^n s_n = 0$, cada producto $X_i b$ (con $b \in B$) es una combinación lineal, con coeficientes en $K[s_1, \ldots, s_n]$, de los elementos de B.

Razonando por inducción a partir de aquí se puede probar que, cualquiera que sea el polinomio f, fb ($b \in B$) es una combinación lineal de los elementos de B con coeficientes en $K[s_1, \ldots, s_n]$. Ordenemos los elementos de B en la forma: $B = \{b_1, \ldots, b_n\}$. Entonces tenemos relaciones de la forma:

$$fb_i = \sum_j a_{ij} b_j \quad (a_{ij} \in K[s_1, \ldots, s_n])$$

lo que significa que el sistema de ecuaciones lineales homogéneas con matriz

$$A = \begin{pmatrix} f - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & f - a_{22} & \cdots & -a_{2n} \\ \vdots & & & \\ -a_{n1} & -a_{n2} & \cdots & f - a_{nn} \end{pmatrix}$$

tiene la solución no nula $b_1, \ldots, b_n$. Por lo tanto, el determinante de A es 0. Esto, a su vez, significa que f es una raíz del polinomio mónico con coeficientes en $K[s_1, \ldots, s_n]$:

$$P(X) = \det \begin{pmatrix} X - a_{11} & \cdots\cdots & -a_{1n} \\ \vdots & & \\ -a_{n1} & \cdots\cdots & X - a_{nn} \end{pmatrix}$$

Resumiendo la información obtenida, se puede decir que f es una fracción a/b que verifica una ecuación de la forma:

$$X^n + a_1 X^{n-1} + \ldots + a_n = 0 \qquad [1]$$

donde tanto a como b y como los a_i están en el anillo factorial $K[s_1, \ldots, s_n]$. Puede suponerse además que $\text{mdc}(a, b) = 1$.

Veamos que esto implica que $b = 1$, o sea $f = a \in K[s_1, \ldots, s_n]$, como se quería demostrar. En efecto, si p es un primo que divide a b, basta sustituir $f = a/b$ en [1] para deducir que p también divide a a. Lo que es una contradicción.

Podemos agregar que la expresión de f como polinomio de las s_i es única debido a que las s_i son algebraicamente independientes.

Ejemplo 2. *Cuerpos finitos*

Ya se vio (cf. 2, ejemplo 2) que si E es un cuerpo finito tiene característica $p > 0$ y es una extensión finita de $\mathbb{F}_p$, de una cierta dimensión n. Entonces $|E| = p^n$ y E es el cuerpo de descomposición sobre $\mathbb{F}_p$ del polinomio $X^{p^n} - X$. Por lo tanto, todos los cuerpos finitos de q elementos son isomorfos entre sí.

Recíprocamente, dado un número q, potencia de un primo: $q = p^n$, llamemos E al cuerpo de descomposición sobre $\mathbb{F}_p$ del polinomio $X^{p^n} - X$. Se deduce inmediatamente que E es igual al conjunto de las raíces de este polinomio y, como veremos, tiene q elementos. Esto probará que para cada potencia de un primo existe un cuerpo con ese número de elementos.

Si E tiene $r = p^n$ elementos, E es generado por un elemento de orden $p^n - 1$, a. Como a es raíz de $X^{p^n-1} - 1$, resulta que $p^n - 1$ divide $p^n - 1$. Si el cociente es $k > 1$ se deduce, por una de las conocidas identidades de álgebra elemental, que

$$X^{(p^m-1)(k-1)} + X^{(p^m-1)(k-2)} + \ldots + X^{p^m-1} + 1 \qquad [2]$$

divide a $X^{p^n-1} - 1$. Entonces hay un elemento de E, a^i, que es raíz de [2]. Sustituyendo se tiene

$$\underbrace{1 + 1 + \ldots + 1}_{k} = 0$$

lo que significa que p divide a k, y, por lo tanto, que p divide a $p^n - 1$, lo cual es absurdo.

Consideremos ahora el grupo cíclico de automorfismos de E generado por el automorfismo de Frobenius, F. Si $0 < m < n$, $a^{p^m} \neq a$, pero $a^{p^n} = a$. Luego, $|F| = n$ y la extensión de Galois correspondiente a $\langle F \rangle = G$ tiene, necesariamente, como cuerpo fijo a $\mathbb{F}_p$:

Si E es un cuerpo finito con p^n elementos, $E/\mathbb{F}_p$ es de Galois con grupo cíclico $\langle F \rangle$.

Más generalmente, si K es un cuerpo finito cualquiera y si E/K es una extensión finita, tenemos una torre de la forma:

$$\begin{array}{c} E \\ | \\ K \\ | \\ \mathbb{F}_p \end{array}$$

Por el teorema fundamental de la teoría de Galois, E/K es de Galois y tiene grupo cíclico subgrupo de $\langle F \rangle$.

5. SEPARABILIDAD

Los elementos de una extensión de Galois E/K tienen dos propiedades principales: en primer lugar, tienen todos sus conjugados en E (E es normal sobre K) y, en segundo lugar, sus conjugados son todos distintos (es decir, su polinomio irreducible no tiene raíces múltiples) (véase 4, teorema 1).

Tenemos entonces dos factores que pueden hacer que E/K no sea de Galois: que E no sea normal sobre K y que haya elementos en E cuyo polinomio irreducible posea raíces múltiples. El primero de estos ya se analizó en 3. Ocupémonos ahora del segundo.

La cuestión puede hacerse bien precisa: dado $P \in K[X]$, irreducible, P se descompone totalmente sobre ciertas extensiones de K: las que contienen un cuerpo de descomposición de P. Ahora bien, la descomposición de P en factores de primer grado es esencialmente independiente

de la extensión, pues todos los cuerpos de descomposición de P sobre K son isomorfos entre sí. Por lo tanto, el hecho de que P tenga o no raíces múltiples sólo depende de P y de K, y no de la extensión en que estas raíces se encuentran.

En el caso de los polinomios con raíces reales que pueden expresarse fielmente como funciones de una variable real, es fácil demostrar que un polinomio tiene raíces reales múltiples si, y sólo si, tiene alguna raíz real que es también raíz de su derivada. Esto motiva la teoría siguiente.

Derivadas

Sean K un cuerpo cualquiera y X una letra. Llámase *función derivada* a la aplicación K-lineal D de $K[X]$ en $K[X]$ que lleva cada monomio X^n en nX^{n-1} (entendiéndose que, en el caso $n = 0$, $X^n = 1$, esto significa que 1 va en 0). Si $M = X^m$ y $N = X^n$ son dos monomios, se tiene:

$$D(MN) = D(X^{m+n}) = (m+n)X^{n+m-1} = mX^{m-1}X^n + X^m \cdot nX^{n-1} =$$

$$= D(M) \cdot N + M \cdot D(N)$$

Esta relación, la familiar fórmula de derivación de un producto, se extiende al caso de dos polinomios cualesquiera $P = \sum_i a_i M_i$ y $Q = \sum_j b_j N_j$, pues:

$$D(PQ) = D(\sum_{i,j} a_i b_j M_i N_j) = \sum_{i,j} a_i b_j (D(M_i)N_j + M_i D(N_j))$$

$$= D(\sum_i a_i D(M_i))(\sum_j b_j N_j) + (\sum_i a_i M_i)(\sum_j b_j D(N_j))$$

$$= D(P) \cdot Q + P \cdot D(Q)$$

Proposición 1. *Para que un polinomio P tenga raíces múltiples es necesario y suficiente que $mdc(P, D(P)) \neq 1$.*

Demostración. Si, sobre un cierto cuerpo L, P se escribe en la forma $P(X) = (X - a)^2 \cdot Q(X)$, entonces $D(P) = 2(X - a)Q + (X - a)^2 D(Q)$ y resulta que $(X - a)$ divide tanto a P como a $D(P)$. *(Nota:* En este argumento se usa la derivada D como aplicación lineal de $L[X]$ en $L[X]$, y que, por tener P sus coeficientes en un cuerpo menor, K, entonces $D(P)$ coincide con la derivada de P como aplicación lineal de $K[X]$ en $K[X]$. Este hecho es de verificación inmediata y se deja a cargo del lector.)

Recíprocamente, si P no tiene raíces múltiples en un cuerpo de descomposición P, se escribe así:

$$P(X) = a(X - a_1)(X - a_2) \dots (X - a_n)$$

(a_i todos distintos) y se tiene:

$$D(P)(X) = \sum_i a \cdot (X - a_1) \dots (X - a_{i-1})(X - a_{i+1}) \dots (X - a_n)$$

y ningún divisor primo de P divide $D(P)$. (Este argumento, desarrollado dentro de un cuerpo de descomposición de P, subsiste también para K en virtud de 1. 2, observación 1.)

Definición 1. *Sea K un cuerpo cualquiera. Se llama exponente característico de K al número definido así:*

si la característica de K es 0, es el número 1;

si $\chi(K)$ es un numero primo, es ese número primo.

En todo lo que sigue de esta sección, K es un cuerpo y p es el exponente característico de K.

Proposición 2

A. *Para que $P \in K[X]$, irreducible, tenga raíces múltiples es necesario que $p > 1$.*

B. *Para cada polinomio irreducible $P \in K[X]$ existe un polinomio irreducible $Q \in K[X]$, sin raíces múltiples, y un número p^k tales que*

$$P(X) = Q(X^{p^k}) \qquad [1]$$

Q está determinado por P (y, por lo tanto, también p^k y, cuando $p > 1$,
también k) y $p^k = \mathrm{gr}(P)/\mathrm{grs}(P)$.

C. *Para que P no tenga raíces múltiples es necesario y suficiente que* $\mathrm{gr}(P) = \mathrm{grs}(P)$.

Demostración

A. Si P es irreducible y tiene raíces múltiples, la proposición 1 implica que $D(P)$ es divisible por P, lo que es imposible a menos que $D(P) = 0$. Si $\mathrm{gr}(P) > 0$, $D(P)$ no puede ser 0 en característica 0. Luego $p > 1$.

B. Si $\chi(K) = 0$ (o sea si $p = 1$) esto es evidente en virtud de A. Si $p > 1$, sea k el mayor número natural para el cual existe un polinomio Q que verifica [1] ($k = 0$ siempre es válido). Como toda factorización de Q conduce a una factorización de P, Q es irreducible. Si $k \geq 1$, todos los exponentes de X en P son múltiplos de p y $D(P) = 0$, que implica que P tiene raíces múltiples.

Habiéndose elegido k en la forma indicada, Q no puede tener raíces múltiples, pues sería $D(Q) = 0$ y todos los exponentes de X en Q serían múltiplos de p, lo que implicaría que Q es un polinomio de X^p y k no sería el máximo posible.

Sea, en un cuerpo de descomposición, $Q(X) = a(X - a_1) \ldots (X - a_n)$, que implica: $P(X) = a(X^{p^k} - a_1) \ldots (X^{p^k} - a_n)$. Para cada i existe una raíz de P, b_i, tal que $b_i^{p^k} = a_i$ y resulta: $X^{p^k} - a_i = X^{p^k} - b_i^{p^k} = (X - b_i)^{p^k}$ y $P(X) = a \cdot (X - b_1)^{p^k}(X - b_2)^{p^k} \ldots (X - b_n)^{p^k}$. Por lo tanto, todas las raíces de

P tienen la misma multiplicidad, p^k, y hay tantas raíces como el grado de Q. La demostración está completa (véase 3, definición 4 y ejemplo 1).

C. Consecuencia inmediata de lo anterior.

Extensiones Separables, Inseparables y Puramente Inseparables

Definición 2. A. *Un polinomio irreducible de* $K[X]$ *se llama separable sobre* K *(notación* sep/K*) cuando no tiene raíces múltiples. Es decir,* P *es* sep/K *si, y sólo si,* $\mathrm{gr}(P) = \mathrm{grs}(P)$. *Un polinomio cualquiera se llama separable sobre* K *cuando sus divisores primos lo son.*

B. *Un elemento* alg/K *es* sep/K *cuando su polinomio irreducible* (sobre K) *lo es.*

Una extensión algebraica E/K *es separable* (se dice E *es* sep/K) *cuando sus elementos son* sep/K.

C. *Los polinomios, elementos* alg/K, *extensiones* alg/K, *que no son* sep/K *se llaman inseparables sobre* K.

Obsérvese que si x es un elemento sep/K y si F es una extensión cualquiera de K contenida en un mismo cuerpo con x, entonces x también es sep/F.

Ejemplo 1. Sean K un cuerpo de característica positiva p y X una letra. Por el criterio de Eisenstein, $Y^p - X^p$ es irreducible en $K(X^p)[Y]$ y, por lo tanto, un polinomio inseparable. Esto implica que $K(X)/K(X^p)$ es inseparable.

Ejemplo 2. Toda extensión de Galois es separable.

Definición 3. Un cuerpo K es perfecto cuando toda extensión algebraica E/K es separable.

Ejemplo 3. Todo cuerpo finito es perfecto.

Ejemplo 4. Todo cuerpo de característica 0 es perfecto.

Observación 1. Sea E/K una extensión simple finita: $E = K(x)$ y sea $P = \mathrm{Irr}(x/K)$. La expresión [1] significa que P puede escribirse como un polinomio separable en X^{p^k}.

Además tenemos que, a partir de $\mathrm{gr}(P) = \mathrm{grs}(P) \cdot p^k$, $(E : K) = (E : K)_s \cdot p^k$:

Si E/K *es una extensión simple,* $(E : K)_s$ *divide a* $(E : K)$ *y el cociente es una potencia de* p.

Definición 4. A. *Si* $P \in K[X]$, *irreducible, se llama grado de inseparabilidad de* P *(notación:* $\mathrm{gri}(P)$*) a* $\mathrm{gr}(P)/\mathrm{grs}(P)$. $\mathrm{gri}(P)$ *es una potencia del exponente característico* p.

B. *Si* x *es* alg$/K$, *se llama grado de inseparabilidad de* x *(notación:* gri(x/K) *a* gri(Irr(x/K)). *Se dice que* x *es puramente inseparable sobre* K *(notación:* p. i. $/K$*) cuando* gri(x/K) = gr(x/K).

C. *Una extensión algebraica* E/K *es puramente inseparable* (se dice: E *es* p. i. $/K$) *si todos sus elementos lo son.*

De acuerdo con esta definición los elementos p. i. $/K$ se pueden caracterizar así: sea N una extensión de E que es normal sobre K. Entonces, $x \in E$ es p. i. $/K$ si, y sólo si, $f(x) = x$ para todo $f \in$ Hom$(K(x)/K, N/K)$.

Proposición 3. *Sea* E/K *una extensión finita.*

A. $(E : K)_s \mid (E : K)$. *El cociente es una potencia de* p.

B. E/K *es separable si, y sólo si,* $(E : K)_s = (E : K)$.

C. E/K *es p. i. si, y sólo si,* $(E : K)_s = 1$.

Demostración

A. Basándose en la observación 1, se razona por inducción en el número de generadores de E/K. Sea $E = K(x_1, \ldots, x_m)$ y $F = K(x_1, \ldots, x_{m-1})$. Entonces $(E : F)_s \mid (E : F)$ y, por la hipótesis de recurrencia, $(F : K)_s \mid (F : K)$, y ambos cocientes son potencias de p. Utilícese ahora 2, proposición 2, A y 3, proposición 4, A.

B. Sea primero el caso de una extensión simple: $E = K(x)$. Sea $y \in K(x)$. Si E/K es separable, y es sep$/K$ y, por definición, $(K(y) : K)_s = (K(y) : K)$ y $(K(x) : K(y))_s = (K(x) : K(y))$, de donde $(E : K)_s = (E : K)$. Recíprocamente, si $(E : K)_s = (E : K)$, resultan las dos igualdades anteriores y la primera implica que y es sep$/K$. En el caso general se razona por inducción en el número de generadores utilizando el mismo tipo de argumento que se empleó para la parte A.

C. Demostración totalmente análoga a la de B.

Corolario. *Sean* E/K *una extensión separable finita y* N *una extensión de* E *que es normal sobre* K. *Un elemento* x *de* E *pertenece al cuerpo de base* K *si, y sólo si,* $f(x) = x$ *para todo* $f \in$ Hom$(E/K, N/K)$.

Demostración. $x \in K$ si, y sólo si, $(K(x) : K) = 1$, o sea si, y sólo si, $(K(x) : K)_s = 1$, que equivale a la condición indicada.

El comportamiento de la separabilidad con relación a las configuraciones elementales es el siguiente:

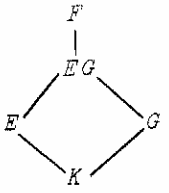
Proposición 4. *Sea* E/K *una extensión algebraica.*

A. *Dada la torre*

$$\begin{array}{c} E \\ | \\ F \\ | \\ K \end{array}$$

E es sep/K *si, y sólo si, E/F y F/K son separables.*

B. *Dada la configuración:*



si E/K es separable, también lo es EG/G.

C. *En la situación de B, EG/K es separable si, y sólo si, ambas: $E/_{\cap}$ y G/K son separables.*

D. *E/K es separable si, y sólo si, es generada por un conjunto de elementos separables.*

La demostración es inmediata.

El comportamiento de la inseparabilidad pura con relación a las configuraciones elementales es exactamente el mismo que el de la separabilidad. Esto se demuestra también mediante los mismos argumentos.

Elementos Primitivos

Proposición 5. *Toda extensión separable finita tiene un elemento primitivo.*

Demostración. La misma del 4, teorema 1, C.

Estructura de Una Extensión Finita

Según la proposición 4, toda extensión algebraica tiene una máxima subextensión separable: es la subextensión generada por el conjunto de todos los elementos separables.

Sea E/K una extensión algebraica cualquiera y sea E_s/K la máxima subextensión separable. Por la proposición 2, B, todo elemento x de E verifica $x^{p^k} \in E_s$, para algún k. Esto prueba que E/E_s es p. i. (véase la definición 4). Por lo tanto, toda extensión algebraica tiene la estructura siguiente:

$$\begin{array}{l} E \\ | \quad \text{p. i.} \\ E_s \\ | \quad \text{sep} \\ K \end{array}$$

Supóngase ahora que E/K es finita y sea N una extensión de E normal sobre K. Como E/E_s es p. i., $(E : E_s)_s = 1$ y, por consiguiente, $(E : K)_s =$

$= (E_s : K)$, y $(E : E_s)$ es una potencia de p (se le llama el grado de inseparabilidad de E/K, *notación:* $(E : K)_i$).

De la misma manera también se demuestra que toda extensión algebraica, E/K, tiene una máxima subextensión puramente inseparable, E_i, que es generada por todos los elementos p. i./K. No obstante, la semejanza no es completa pues en general E/E_i no es separable. Más aún, existen extensiones inseparables en las cuales $E_i = K$:

Ejemplo 5. Sea $K = \mathbb{F}_2(X)$, donde X es una letra, y sea $E = K(y, z)$, donde y es una raíz del polinomio irreducible $Y^2 + Y + X \in K[Y]$ y donde z es una raíz del polinomio $Z^2 - y$ que es irreducible sobre $K(y)$. Es fácil probar que no existe en E ningún elemento x tal que $x^2 \in K$. Luego, no existe en E ningún elemento p. i./K. Sin embargo, E/K es inseparable y $E_s = K(y)$.

Este ejemplo muestra también la falsedad del recíproco del corolario de la proposición 3. En efecto, si N es una extensión de E normal sobre K y si $x \in E$, resulta

$$x \in K \Leftrightarrow f(x) = x \quad (\forall f \in \mathrm{Hom}(K(x)/K(x)/K, N/K)$$

y sin embargo E/K no es separable.

La estructura general de una extensión finita se puede describir en forma mucho más explícita cuando la extensión es normal.

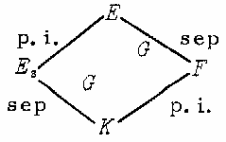
Proposición 6. *Sean E/K una extensión normal finita, $G = \mathrm{Aut}(E/K)$ y F el cuerpo fijo de G: $F = E^G$.*

A. *E/F es de Galois con grupo G. $(E : F) = (E : K)_s$.*

B. *F/K es p.i. y $(F : K) = (E : K)_i$ y $F = E_i$.*

C. *E_s/K es de Galois con grupo isomorfo a G.*

D. *E_s y F son* L. D./K.



Demostración

A. Obvio, por definición. $(E : F) = |\mathrm{Aut}(E/F)| = |G| = (E : K)_s$.

B. Obvio por A y por las definiciones de grado de separabilidad y grado de inseparabilidad.

C. Es claro que E_s es invariante para todos los morfismos de G y, por el corolario de la proposición 3, el cuerpo fijo de $G|_{E_s}$, es K. Luego, E_s/K es de Galois y tiene grupo $G|_{E_s}$, isomorfo a G.

D. Sigue de 4, proposición 2,C, porque, evidentemente, $E_s \cap F = K$.

Corolario 1. *Una extensión finita E/K es de Galois si, y sólo si, es normal y separable.*

Demostración. Por 4, teorema 1, B, toda extensión de Galois es normal y separable. Recíprocamente, si la extensión finita E/K es normal y separable, es de Galois por la proposición 6, A y B.

Corolario 2. *E/K es de Galois si, y sólo si, E es el cuerpo de descomposición de un polinomio separable sobre K.*

Aplicaciones

1. El teorema fundamental del álgebra

Definición 6. *Un cuerpo E es algebraicamente cerrado si, y sólo si, todo polinomio $P \in E[X]$, de grado ≥ 1, tiene una raíz (y, por lo tanto, todas) en E.*

De modo equivalente, E es algebraicamente cerrado si, y sólo si, la única extensión algebraica de E es E/E.

Teorema 1. *Teorema fundamental del álgebra.*

$\mathbb{C}$ es algebraicamente cerrado.

Demostración. Como todo polinomio de grado impar de $\mathbb{R}[X]$ tiene una raíz en $\mathbb{R}$, si $E/\mathbb{R}$ es algebraica finita de grado mayor que 1, $(E : \mathbb{R})$ es par. Si $E/\mathbb{R}$ es de Galois con grupo G y $E \neq \mathbb{R}$, entonces $(E : \mathbb{R})$ es de la forma $2^k n$, con n impar y $k \geq 1$. Si H es un 2-grupo de Sylow de G y si F es el cuerpo fijo de H, entonces $(F : \mathbb{R}) = n$. Por lo tanto, $n = 1$ y G es un 2-grupo. Entonces G posee una serie de composición: $G = G_0 \rhd G_1 \rhd \rhd \ldots \rhd G_r = 1$ tal que, para todo i, $G_{i+1} \rhd G_i$ de índice 2. Esto implica que E es una torre: $E = F_r/F_{r-1}/ \ldots /F_1/F_0 = \mathbb{R}$ tal que para todo i, $(F_{i+1} : F_i) = 2$. Como todo polinomio de segundo grado con coeficientes en $\mathbb{C}$ tiene raíces en $\mathbb{C}$, se tiene que F_1 es isomorfo a $\mathbb{C}$ y $r = 1$. Así se ha demostrado que $\mathbb{R}$ tiene sólo dos extensiones de Galois: $\mathbb{R}/\mathbb{R}$ y $\mathbb{C}/\mathbb{R}$.

Como toda extensión algebraica de $\mathbb{R}$ está contenida en una de Galois, ambas son también las únicas extensiones algebraicas de $\mathbb{R}$. Por lo tanto, la única extensión algebraica de $\mathbb{C}$ es $\mathbb{C}/\mathbb{C}$ y esto completa la demostración.

2. Problemas resolubles con regla y compás (continuación)

En 2. 1, ejemplo 4 se vio que los problemas geométricos resolubles con regla y compás son los que corresponden a extensiones finitas de la forma $E = F_r/F_{r-1}/ \ldots /F_1/F_0 = K$ donde $(F_{i+1} : F_i) = 2$. Para esto es necesario que $(E : K)$ sea una potencia de 2.

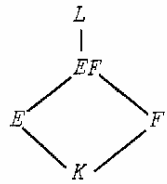
Ahora estamos en condiciones de dar una condición necesaria y suficiente para que se dé esta situación.

Teorema 2. *Sean E/K la extensión que corresponde a un cierto problema geométrico y N la mínima extensión de E que es normal sobre K. Para que el problema geométrico sea resoluble por regla y compás es necesario y suficiente que $(N : K)$ sea una potencia de 2.*

Demostración. La condición es suficiente, pues en tal caso, N/K es de Galois y su grupo es un 2-grupo. Por lo visto en la demostración del teorema 1, N/K es una torre finita con pisos de dimensión 2 y, por consiguiente, todos los elementos de N (en particular los de E) corresponden a puntos que se pueden construir con regla y compás. Se necesitará el lema siguiente:

Lema. *Todo compuesto de un número finito de extensiones de grado 2 tiene por grado una potencia de 2.*

Demostración del lema. Puede razonarse por inducción. Considérese la configuración.



donde $(E : K) = 2$ y $(F : K)$ es una potencia de 2. Si E está contenido en F, no hay nada que demostrar. Si E no está contenido en F, $E \cap F = K$ y, como E/K es de Galois, E y F son L. D. $/K$. Por lo tanto $(EF : K) = (E : K)(F : K)$ es una potencia de 2.

Fin de la demostración del teorema. Manteniendo las notaciones, basta probar que si E/K es una torre con pisos de dimensión 2, entonces $(N : K)$ es una potencia de 2. Razonamos por inducción en r. Se puede suponer que si $N' \subset N$ es la mínima extensión de F_{r-1} que es normal sobre K, se sigue que $(N' : K)$ es una potencia de 2. Si $N = N'$, no hay nada que demostrar. En caso contrario $(EN' : N') = 2$ y, si $E = K(x)$, $\mathrm{gr}(x/N') = 2$. N es generada por los conjugados de x sobre K y, como N'/K es normal, cada conjugado de x tiene grado 2 sobre N'. Luego, N/N' es un compuesto de cuerpos de grado 2 y, por el lema, $(N : N')$ también es una potencia de 2. Esto completa la demostración.

Ejemplo 6. No todo ángulo puede dividirse en tres partes iguales con regla y compás. En efecto, si α es $\frac{1}{3}$ del ángulo de un triángulo equilátero, α no es construible. Si lo fuera, también lo sería $\cos \alpha$. La relación $(\cos \alpha + i \cdot \mathrm{sen}\, \alpha)^3 = (1 + i\sqrt{3})/2$ implica que $\cos^3 \alpha - 3 \cos \alpha \cdot \mathrm{sen}^2 \alpha = \frac{1}{2}$, de donde se deduce que $\cos \alpha$ es una raíz del polinomio $8X^3 - 6X - 1$, que es irreducible sobre $\mathbb{Q}$ pues no tiene raíces racionales. Entonces $\mathrm{gr}(\cos \alpha/\mathbb{Q}) = 3$, que no es una potencia de 2. Lo que implica que el supuesto es absurdo.

Ejemplo 7. Dado un cubo de arista a, es imposible construir con regla y compás un cubo cuyo volumen sea el doble del primero. Si fuera posible, se podría construir un segmento de longitud $\sqrt[3]{2}$, lo que es absurdo pues $\mathrm{gr}(\sqrt[3]{2}/\mathbb{Q})$ no es una potencia de 2.

Ejemplo 8. Es imposible rectificar una circunferencia con regla y compás, es decir, no se puede construir, a partir de la longitud de r, la longitud $2\pi r$. Lo contrario implicaría que π es construible, es decir que $gr(\pi/\mathbb{Q})$ es una potencia de 2, lo cual es absurdo, pues se puede demostrar que π es trascendente sobre $\mathbb{Q}$.

3

ECUACIONES

1. RAÍCES DE LA UNIDAD

Si w es una raíz de la unidad en E/K, $\langle w \rangle$ es un subgrupo cíclico finito de $(E,.)$. Si el orden de w en este grupo es n, se dice que w es una *n-raíz primitiva* sobre K (Nota: de hecho esto no depende de K, sino del cuerpo primo de K.)

Si K tiene característica positiva, p, los órdenes de las raíces de 1 sobre K son siempre números primos respecto de p. En efecto, $w^{p^k} = 1$ implica $w^k = 1$, pues el automorfismo de Frobenius es inyectivo.

Si m entero positivo es de la forma $p^k n$ (donde p es el exponente característico de K y $\text{mdc}(p, n) = 1$), el polinomio $X^m - 1$ tiene derivada nula si, y sólo si, $p^k > 1$, y sus raíces son las raíces de $X^n - 1$. Por otra parte $X^n - 1$ tiene derivada $nX^{n-1} \neq 0$ y por lo tanto $\text{mdc}(X^n - 1, D(X^n - 1)) = 1$, lo que implica que $X^n - 1$ es separable sobre K.

O sea, cualquiera que sea m, las raíces m-ésimas de 1 son las raíces n-ésimas de 1 (siendo todas ellas distintas). Una n-raíz primitiva genera el cuerpo de descomposición de $X^m - 1$, o de $X^n - 1$, sobre K que es una extensión normal y separable (es decir, de Galois).

Definición 1. *Sean p el exponente característico de K y $n \geq 1$ primos relativos* (en característica 0, $p = 1$ y todos los números son primos respecto de p). *El cuerpo de descomposición de $X^n - 1$ sobre K se llama el cuerpo ciclotómico de orden n sobre K* que se denota $K(\sqrt[n]{1})$.

El grupo formado por las raíces de $X^n - 1$ (grupo de las n-raíces de 1) es un grupo cíclico de orden n y, por lo tanto, tiene $\varphi(n)$ (función de Euler de n) generadores o raíces primitivas. El polinomio cuyas raíces son las n-raíces primitivas: $w_1, \ldots, w_{\varphi(n)}$,

$$\Phi_n(X) = \prod_i (X - w_i)$$

se llama el enésimo polinomio ciclotómico (en exponente p o, si χ es la característica de K, en característica χ). Si K_0 es el cuerpo primo de K, $\Phi_n(X) \in K_0[x]$, porque es fijo para todo automorfismo de K (un tal automorfismo sólo puede permutar las w_i). Más adelante (cf. la proposición 1) se probará que, en característica 0, $\Phi_n \in \mathbb{Z}[X]$.

Es claro que $K(\sqrt[n]{1})$ es también el cuerpo de descomposición de Φ_n.

Las diferentes n-raíces de 1 pueden clasificarse según su orden y correspondiente a cada orden queda definido un polinomio ciclotómico Φ_d con $d \mid n$. Se deduce de inmediato que

$$X^n - 1 = \prod_{d|n} \Phi_d$$

Esta relación permite el cálculo de Φ_n por un proceso de recurrencia: si se conocen todos los Φ_n correspondientes a los divisores d de n menores que n, entonces Φ_n se puede obtener por:

$$\Phi_n = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d}$$

Por ejemplo, de este modo se puede obtener:

$$\Phi_1 = X - 1$$

$$\Phi_2 = \frac{X^2 - 1}{X - 1} = X + 1$$

$$\Phi_3 = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$$

$$\Phi_4 = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1$$

$$\Phi_5 = \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1$$

.
.
.

$$\Phi_{12} = \frac{X^{12} - 1}{(X^4 - 1)(X^2 + X + 1)} = X^6 - X^5 + X^3 - X + 1$$

En general, si q es un número primo

$$\Phi_q = \frac{X^q - 1}{X - 1} = X^{q-1} + X^{q-2} + \ldots + X + 1$$

y

$$\Phi_{q^k} = \frac{X^{q^k} - 1}{X^{q^{k-1}} - 1} = X^{q^{k-1}(q-1)} + X^{q^{k-1}(q-2)} + \ldots + X^{q^{k-1}} + 1$$

Sean $G = \mathrm{gal}(K(\sqrt[n]{1})/K)$ y w una n-raíz primitiva. Cada $f \in G$ está determinado por $f(w) = w^i$, donde i es un número menor que n y primo con n (es decir, una unidad del anillo Z_n de los enteros módulo n). Si f corresponde a i y $g \in G$ corresponde a j, se sigue $(fg)(w) = f(w^j) = w^{ij}$. Se deduce que la correspondencia $f \mapsto i$ define un monomorfismo de G en el grupo U_n de las unidades de Z_n. Se ha demostrado que:

$\mathrm{gal}(K(\sqrt[n]{1})/K)$ *es un grupo conmutativo isomorfo a un subgrupo de* U_n.

Si Φ_n es irreducible sobre K, como $|G| = \mathrm{gr}(\Phi_n) = \varphi(n) = |U_n|$, resulta $G \cong U_n$.

Sea p un número primo. Como se sabe $\mathbf{F}_p(\sqrt[n]{1})/\mathbf{F}_p$ (al igual que cualquier extensión finita de un cuerpo finito) es una extensión de Galois cíclica, de grupo generado por el automorfismo de Frobenius, F. Si

w es una n-raíz primitiva, el orden de F es el primer exponente no nulo, k, tal que $F^k(w) = w$, o sea, el primer k no nulo tal que $w^{p^k} = w$ o $w^{p^k-1} = 1$. Como $|w| = n$ el orden de F es el primer k no nulo tal que n divide $p^k - 1$, o el primer k no nulo tal que $p^k \equiv 1 \pmod{n}$.

En otras palabras, la dimensión de la extensión $\mathbb{F}_p(\sqrt[n]{1})$ sobre $\mathbb{F}_p$ es el primer natural no nulo, k, tal que p^k es congruente con 1 módulo n. Si $k < \varphi(n)$, Φ_n no es irreducible sobre $\mathbb{F}_p$: se descompone en $\varphi(n)/k$ factores de grado k correspondientes a las órbitas de F operando en el conjunto de las n-raíces primitivas.

Por ejemplo, $(\mathbb{F}_2(\sqrt[7]{1}) : \mathbb{F}_2) = 3$ y, en característica 2:

$$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = (X^3 + X + 1)(X^3 + X^2 + 1)$$

En cambio, $(\mathbb{F}_3(\sqrt[5]{1}) : \mathbb{F}_3) = 4$ y, por consiguiente, Φ_5 es irreducible sobre $\mathbb{F}_3$.

El caso de característica 0 se resuelve por la siguiente:

Proposición 1. *En característica 0, Φ_n es irreducible sobre $\mathbb{Q}$. (Para todo $n \geq 1$).*

Demostración. Sean $P \in \mathbf{Z}[X]$ un divisor irreducible de Φ_n y Q tal que $PQ = X^n - 1$. Puede suponerse que tanto P como Q son mónicos. Sea w una n-raíz primitiva que anula P y demostremos que si p es un primo que no divide n, entonces w^p también es raíz de P. Para ello pasamos al cociente módulo p (véase 1. 1, ejemplo 6). Si fuera $P(w^p) \neq 0$, sería $Q(w^p) = 0$ y P dividiría $Q(X^p)$ (por ser $P = \mathrm{Irr}(w/\mathbb{Q})$). Entonces, módulo p, $\bar{P}(X) \mid \bar{Q}(X^p) = (\bar{Q}(X))^p$, y se deduce que si $\bar{T}$ es un divisor primo de $\bar{P}$ resulta $\bar{T}^2 \mid (X^n - 1)$, o sea una contradicción porque, como $p \nmid n$, $X^n - 1$ no tiene raíces múltiples en característica p.

Ahora basta observar que toda raíz primitiva se obtiene a partir de w por sucesiva elevación a exponentes primos y primos con n. Esto implica que todas las n-raíces primitivas son raíces de P y, por consiguiente, $\Phi_n = P$.

Incidentalmente, hemos demostrado además que Φ_n tiene sus coeficientes en $\mathbf{Z}$.

Ejemplo 1. Sea $n = ab$ con $\mathrm{mdc}(a, b) = 1$. Además sean:

$$E = \mathbb{Q}(\sqrt[n]{1}), \quad F = \mathbb{Q}(\sqrt[a]{1}), \quad G = \mathbb{Q}(\sqrt[b]{1})$$

Demostremos que $E = FG$ y que F y G son L. D. $/\mathbb{Q}$. Lo primero es obvio, pues si u es una a-raíz primitiva y v una b-raíz primitiva, entonces $w = uv$ es una n-raíz primitiva.

Sean $M = \mathrm{gal}(E/\mathbb{Q})$, $H = \mathrm{gal}(F/\mathbb{Q})$ y $K = \mathrm{gal}(G/\mathbb{Q})$. Por la proposición 1, H puede identificarse al conjunto de los enteros menores que a y primos con a. Si t es uno de ellos, el automorfismo correspondiente se

define por la condición $u \mapsto u^t$. En tal caso t también define un elemento de M mediante la condición $uv \mapsto u^t v$. Esto prueba también que H es isomorfo a gal(E/G). De modo similar, K es isomorfo a gal(E/F). Ahora basta recurrir a 2.4, proposición 2, B.

Incidentalmente, se ha probado además la siguiente propiedad de la función de Euler:

$$\text{mdc}(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a) \cdot \varphi(b)$$

Ejemplo 2. *Polígonos regulares construibles con regla y compás.*

Usando el modelo algebraico para estudiar los problemas geométricos, es claro que el problema de construir un polígono regular de $n \geq 3$ lados con regla y compás se corresponde con el problema de expresar $\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}$ como una torre de pisos de dimensión 2. Como la extensión es normal, es condición necesaria y suficiente para ello que su grado sea una potencia de 2.

En otras palabras, el polígono regular de n lados es construible si, y sólo si, $\varphi(n)$ es una potencia de 2.

Si $n = p_1^{k_1} \ldots p_r^{k_r}$ es la descomposición de n en factores primos, entonces $\varphi(n) = \prod_i \varphi(p_i^{k_i}) = \prod_i p_i^{k_i - 1}(p_i - 1)$. Por lo tanto, $\varphi(n)$ es una potencia de 2 si, y sólo si, para cada $p_i \neq 2$, es $k_i = 1$ y $p_i - 1$ es una potencia de 2.

Los primos p que satisfacen esta condición se llaman *primos de Fermat* y se caracterizan por la expresión:

$$p = 2^h + 1$$

Se observa inmediatamente que h también tiene que ser una potencia de 2. En efecto, si fuera $h = st$ con $s > 1$ impar, tendríamos

$$p = 2^{st} + 1 = (2^{t(s-1)} - 2^{t(s-2)} + \ldots + (-1)^{s-1} 2^t)(2^t + 1)$$

y p no sería primo. Luego los primos de Fermat son de la forma:

$$p = 2^{2^k} + 1$$

Para los primeros valores de k se obtienen los números primos siguientes: 3, 5, 17, 257, 65537. $2^{2^5} + 1$ es divisible por 641.

Resumiendo, son construibles exactamente aquellos polígonos regulares cuyo número de lados es de la forma $2^n p_1 \ldots p_r$, donde los p_i son primos de Fermat distintos.

2. ECUACIONES RESOLUBLES POR RADICALES

En esta sección K es un cuerpo de exponente característico p.

Proposición 1. *Sea n un número primo con p y supóngase que K contiene las n-raíces de 1. Entonces las proposiciones que siguen son equivalentes:*

1) *E/K es de Galois con grupo cíclico de orden n;*

2) *E es el cuerpo de descomposición sobre K de un polinomio irreducible de la forma $X^n - a$ (se dice que E se obtiene adjuntando a K el radical $\sqrt[n]{a}$.)*

Demostración

(1) implica (2). Sea $\mathrm{gal}(E/K) = \langle f \rangle$, un grupo cíclico de orden n, y sea w una n-raíz primitiva. El elemento $y = \sum_{i=0}^{n-1} w^i f^i(x)$, donde x es un elemento primitivo de E/K, tiene la propiedad de que $f(y) = w^{-1}y$. Por lo tanto, y tiene todos sus conjugados distintos y es otro elemento primitivo de E/K. Si escribimos $a = y^n$ esa misma propiedad implica, que $f(a) = a$, o sea $a \in K$ (véase 2.5, corolario de la proposición 3). Luego y es una raíz de $X^n - a$ que es entonces irreducible sobre K.

(2) implica (1). Si x es una raíz de $X^n - a$, las otras raíces son xw^i $(i = 1, \ldots, n-1)$ y, por lo tanto, $E = K(x)$.

Para cada $i = 0, 1, \ldots, n-1$, $x \mapsto xw^i$ define un elemento de $\mathrm{gal}(E/K)$ que resulta ser isomorfo con el grupo cíclico Z_n de los enteros módulo n.

Observación 1. Con las notaciones anteriores, si n es primo, o bien $X^n - a$ tiene todas sus raíces en K, o bien es irreducible sobre K. En efecto, si $b \notin K$ es una raíz de $X^n - a$ y si $P = \mathrm{Irr}(b/K)$, entonces $E = K(b)$ y $(E:K) = \mathrm{gr}(P)$. Si b_1 es otra raíz de P, $b_1 = bw^i$ $(1 \leq i < n)$ y, siendo n primo, w^i es otra n-raíz primitiva. Se puede suponer sin pérdida de generalidad que $b_1 = bw$. Entonces $b \mapsto b_1$ define un automorfismo f de E/K tal que $n = |f| \leq (E:K) = \mathrm{gr}(P) \leq n$. Esto implica que $\mathrm{gr}(P) = n$ y, por lo tanto, que $P = X^n - a$.

Proposición 2. *Sea $P \in K[X]$ un polinomio separable y sea E el cuerpo de descomposición de P sobre K. Supongamos que $G = \mathrm{gal}(E/K)$ es un grupo resoluble.*

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = 1 \qquad G_i/G_{i+1} \cong Z_{p_i} \quad (p_i \text{ primos})$$

tal que todos los p_i son diferentes de p. Supongamos también que K contiene todas las p_i-raíces de 1 (para todo i). Entonces la ecuación $P(X) = 0$ es resoluble por radicales sobre K (véase 2.1, ejemplo 5).

Demostración. Por el teorema fundamental de la teoría de Galois, E/K es una torre con pisos F_{i+1}/F_i de Galois, con grupos cíclicos G_i/G_{i+1} de órdenes p_i. Se sigue de la proposición 1 que F_{i+1} es de la forma $F_i(\sqrt[p_i]{a_i})$.

Nota: Los primos p_i son exactamente los que dividen $|G|$.

Corolario. *Si $p = 1$ o si $p > n$, todas las n-raíces de 1 son expresables por radicales sobre K.*

Demostración. Se puede razonar por inducción sobre los números menores que n. Si K contiene las m raíces de 1 para todos los números m menores que n, como $\mathrm{gal}(K(\sqrt[n]{1})/K)$ es isomorfo a un subgrupo de U_n, grupo conmutativo cuyo exponente divide $\varphi(n)$, se puede aplicar la proposición 2.

Observación 2. Sean $P \in K[X]$ y E el cuerpo de descomposición de P sobre K. La ecuación $P(X) = 0$ es resoluble por radicales sobre K si, y sólo si, E/K es una torre con pisos de la forma F_{i+1}/F_i, $F_{i+1} = F_i(\sqrt[n_i]{a_i})$. Conviene observar que, sin pérdida de generalidad, puede suponerse que cada n_i es un número primo. En efecto, si n_i no es primo, el piso F_{i+1}/F_i se puede sustituir por una torre en que cada piso tiene la misma forma, pero con un radical de índice primo. Para comprenderlo basta ver que si $n = hk$, la extensión $F(\sqrt[n]{a})/F$ se puede sustituir por la torre con pisos $F_1(\sqrt[k]{b})/F_1$ y $F_1 = F(\sqrt[k]{a})/F$, $b = \sqrt[k]{a}$. Pues la notación $F(\sqrt[n]{a})$ representa una extensión $F(c)$, donde c es una raíz de $X^n - a$. Basta entonces escribir $b = c^h$, para tener que c es una raíz del polinomio $X^h - b$ sobre el cuerpo $F(b)$, y que b es una raíz de $X^k - a$ sobre F.

Teorema 1. *Teorema de Galois. Sea $P \in K[X]$ un polinomio separable.* 68 *Sea E el cuerpo de descomposición de P sobre K y sea $G = \mathrm{gal}(E/K)$. Entonces:*

A. *Si G es resoluble y $p = 1$ o $p > p_i$ (donde p_i son los primos que dividen el orden de G), entonces $P(X) = 0$ es resoluble por radicales sobre K.*

B. *Si $P(X) = 0$ es resoluble por radicales sobre K: E/K es una torre con pisos de la forma $F_{i+1} = F_i(\sqrt[p_i]{a_i})$, donde los p_i son numerosos primos; entonces $p = 1$ o $p \neq p_i$ para todo i y G es resoluble.*

C. *Si $p = 1$ (o sea, si $\chi(K) = 0$), $P(X) = 0$ es resoluble por radicales si, y sólo si, G es resoluble.*

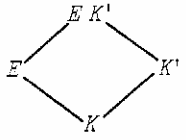
Demostración

A. Por la proposición 2, corolario, todas las p_i-raíces de 1 son expresables por radicales sobre K. Si K' es el cuerpo obtenido agregando a K todas estas raíces, $P(X) = 0$ es resoluble por radicales sobre K' (y, por consiguiente, sobre K) por la proposición 2.

B. Sea $K' = K(\sqrt[m]{1})$, donde $m = \mathrm{mmc}(p_i/i = 1, \ldots)$, y sea $E' = E(\sqrt[m]{1}) = EK'$. Finalmente, sean $F'_i = F_iK' \subset E'$ $(i = 1 \ldots)$.

Entonces K'/K es de Galois con grupo conmutativo y F'_{i+1} es el cuerpo de descomposición sobre F'_i del polinomio $X^{p_i} - a_i$. Por la observación 1, o bien $F'_{i+1} = F'_i$ o bien dicho polinomio es irreducible y, por la proposición 1, F'_{i+1}/F'_i es de Galois con grupo cíclico de orden p_i.

Aplicando a la torre formada por los F'_i el teorema fundamental de la teoría de Galois, deducimos que $\mathrm{gal}(E'/K')$ es un grupo resoluble. Considerando la configuración:



por 2.4, proposición 2, tenemos que E'/K es de Galois y, como $\mathrm{gal}(K'/K) \cong \mathrm{gal}(E'/K)/\mathrm{gal}(E'/K')$, $\mathrm{gal}(E'/K)$ es un grupo resoluble. Finalmente, como $G \cong \mathrm{gal}(E'/K)/\mathrm{gal}(E'/E)$, G es resoluble.

Observación 3. Ya se vio (cf. 2.4, ejemplo 1) que el grupo de Galois del cuerpo de descomposición de la ecuación general de grado n es isomorfo al grupo simétrico S_n.

Como S_1, S_2, S_3 y S_4 son resolubles, las ecuaciones de primero, segundo, tercer y cuarto grado son resolubles por radicales sobre cualquier cuerpo de característica 0 (o sobre cuerpos de característica $\neq 2, 3$).

Como S_n no es resoluble si $n \geq 5$, la ecuación general de grado mayor que 4 no es resoluble por radicales.

Debe observarse que, cuando p es un número primo que divide n, hay ecuaciones muy simples (por ejemplo la $X^2 + X + 1 = 0$ sobre $\mathbb{F}_2$) que no son resolubles por radicales.

3. DETERMINACIÓN DEL GRUPO DE GALOIS Y RESOLUCIÓN DE ECUACIONES

Se reanuda aquí el estudio del problema con que se inició el capítulo 2: la resolución de ecuaciones polinómicas. El estudio algebraico de las ecuaciones polinómicas se basa en el análisis de la extensión definida por el cuerpo de descomposición del polinomio sobre el cuerpo de base (que por lo general es el cuerpo generado por los coeficientes del polinomio). El caso más simple, y el único que se tratará, corresponde a las extensiones de Galois (o sea cuando el polinomio es separable sobre el cuerpo de base).

Si se tiene una extensión de Galois resoluble (es decir con grupo resoluble), los teoremas ya estudiados permiten construir, paso a paso, la torre de raíces que define el cuerpo de descomposición del polinomio en cuestión y, en un sentido esencialmente teórico, se consigue la resolución de la ecuación considerada. Para poder proceder así es preciso determinar el grupo de Galois y hallar una sucesión de Jordan-Hölder que proporcione sus sucesivos factores de composición, pues a partir de esta sucesión se va contruyendo la torre.

Nos ocuparemos de la situación siguiente: Se da un cuerpo K y un polinomio separable, F, con coeficientes en K. El cuerpo de descom-

posición de P sobre K, E, define una extensión de Galois, E/K, cuyo grupo, G, se llama el *grupo de Galois de P sobre K*. *Notación:* $\mathrm{gal}(P/K)$.

Sea $P = P_1^{k_1} \dots P_r^{k_r}$ la descomposición de P en factores primos sobre K. Entonces $Q = P_1 \dots P_r$ tiene las mismas raíces que P y el mismo cuerpo de descomposición, E. Por lo tanto, sin pérdida de generalidad (sustituyendo P por Q) se puede suponer que P no tiene raíces múltiples.

Se introduce el conjunto de las raíces de P: $x_1, \dots, x_n$. Si x es una de estas raíces, x es raíz de uno solo de los P_i y, cualquiera que sea el morfismo f, $f(x)$ es otra raíz del mismo P_i. Esto significa, por una parte, que G opera por permutaciones en el conjunto de las raíces de P: G puede considerarse como un conjunto de permutaciones de $R = \{x_1, \dots, x_n\}$ y, si se fija un orden en este conjunto, G puede identificarse a un subgrupo de S_n. Por otra parte, G opera también por permutaciones en las raíces de cada divisor primo P_i: los subconjuntos de R formados por las raíces de cada P_i son precisamente las órbitas de R bajo la acción de G. En particular, se tiene:

P es irreducible sobre K si, y sólo si, G es transitivo en R.

En efecto, si x e y son raíces de P_i, son conjugados sobre K y el morfismo $K(x) \to K(y)$ se puede prolongar a un automorfismo de E/K, es decir existe un f en G tal que $f(x) = y$.

Ejemplo 1. *Extensiones de cuerpos finitos.*

Sea K un cuerpo finito de característica p. Se sabe que E/K es una extensión de Galois con grupo cíclico. Si P es irreducible de grado n, G puede identificarse con un subgrupo cíclico transitivo de S_n. Las únicas permutaciones f que generan un grupo transitivo en S_n son los n-ciclos: $f = (a_1, \dots, a_n)$. Esto significa que, para una cierta ordenación de las raíces de P, se puede suponer $f = (1, 2, \dots, n)$ (interpretación: si x es una raíz de P, las otras son $x^p, x^{p^2}, \dots, x^{p^{n-1}}$). Resulta también que basta una raíz, x, de P para generar la extensión: $E = K(x)$.

Si P es un producto de polinomios irreducibles diferentes: $P = P_1 \dots P_r$, de grados $n_1, \dots, n_r$, entonces G es generado por una permutación de la forma:

$$(1, \dots, n_1)(n_1 + 1, \dots, n_1 + n_2) \dots (n_1 + \dots + n_{r-1} + 1, \dots, n)$$

Conviene observar que en nuestro caso es muy fácil calcular el grado $(E : K)$. Basta usar la relación $P(x) = 0$ para calcular las diferentes potencias $x^p, x^{p^2}, \dots, x^{p^k}, \dots$ y determinar el mínimo k tal que $x^{p^k} = x$. Entonces $p^k - 1$ es el mmc de los órdenes de las raíces de P en el grupo multiplicativo de E. Como todos estos grupos son cíclicos, se deduce que $(E, .)$ tiene orden $p^k - 1$ y, por lo tanto, $(E : K) = k$. En ciertos casos esta información es útil para hallar la descomposición de P en factores primos.

Por ejemplo, sea $P = X^6 + X^5 + X^4 + X^3 + 1$ sobre $\mathbb{F}_2$. Obtenemos sucesivamente:

$$x^7 = x^3 + x + 1, \quad x^8 = x^4 + x^2 + x, \quad x^{16} = x,$$

de donde se infiere que el orden de las raíces divide 15: $|x| = 1, 3, 5, 15$. Como $|x| + 1$ debe ser una potencia de 2, $|x| = 1, 3, 15$. La relación $x = 1$, junto con $P(x) = 0$ lleva al absurdo $1 + 1 + 1 + 1 + 1 = 0$. La relación $x^3 = 1$ conduce a $1 + x^2 + x + 1 + 1 = 0$, o sea $x^2 + x + 1 = 0$.

Así se llega a la conclusión de que o bien P es divisible por $X^2 + X + 1$, o bien P es un producto de polinomios irreducibles de orden 4 (pues todas sus raíces tendrían orden 15). Como esto es imposible, sólo subsiste la primera posibilidad. Efectuando la división se obtiene $P = (X^2 + X + 1)(X^4 + X + 1)$. Como $X^4 + X + 1$ no es divisible por $X^2 + X + 1$ (que era el único polinomio que podía anular las raíces de P, aparte de los irreducibles de cuarto grado), se deduce que $X^4 + X + 1$ es irreducible sobre $\mathbf{F}_2$ y que aquélla es la descomposición de P en factores primos. E/K tiene en nuestro ejemplo dimensión 4 y, para una cierta ordenación de las raíces de P, el grupo de Galois de E/K es generado por la permutación (1, 2) (3, 4, 5, 6).

Hay dos métodos importantes para determinar el grupo de Galois, el de utilizar la acción de S_n en el cuerpo de funciones racionales en n letras y el de reducción a un cuerpo residual.

Aprovechamiento de la Acción de S_n en $K(X_1, \ldots, X_n)$

Sean $X_1, \ldots, X_n$ letras y sea L el cuerpo de las funciones racionales en las X_i sobre K. Sean $s_1, \ldots, s_n$ las funciones simétricas elementales en las X_i y S el subcuerpo generado por ellas: $S = K(s_1, \ldots, s_n)$ = cuerpo de las funciones simétricas. Se sabe ya que L/S es de Galois con grupo S_n. 71

El epimorfismo de K-álgebras que lleva $K[X_1, \ldots, X_n]$ sobre E (dado por $X_i \mapsto x_i$) aplica s_i en $(-1)^i a_i$, donde a_i son los coeficientes de P: $P(X) = X^n + a_1 X^{n-1} + \ldots$ El grupo de Galois, G, es precisamente el subgrupo de S_n que deja invariante el ideal de las relaciones algebraicas, $\mathcal{R}(x_1, \ldots, x_n)$.

De acuerdo con la teoría de Galois, elegido un conjunto cualquiera de polinomios: $Q_i (i \in I)$ queda determinado un subgrupo de S_n, H: el conjunto de las permutaciones que dejan fijos cada uno de los Q_i (véase 2.4, proposición 1, B). H es el grupo de Galois de la extensión $L/K((Q_i)_{i \in I})$.

Sea $y_i = Q_i(x_1, \ldots, x_n) \in E$. La extensión $E/K((y_i)_{i \in I})$ es de Galois y su grupo está formado por todas las permutaciones de G que dejan fijos cada uno de los y_i. Para que G sea un subgrupo de H es necesario y suficiente que cada permutación de G deje fijos todos los y_j (pues entonces G, operando en las letras X_i deja fijos todos los Q_j). En otras palabras: $G < H$ si, y sólo si, todos los y_j están en K.

En general se tiene que $\mathrm{gal}(E/K((y_i)_{i \in I}) = G \cap H$, pues cada f de $G \cap H$, por dejar fijos los Q_j, deja fijos también los y_j, y recíprocamente.

Ejemplo 2. *El discriminante.*

Como vimos en 1. 1, ejemplo 3, si $p = \mathcal{X}(K) \neq 2$, el grupo de las permutaciones que dejan fijo el polinomio $\prod_{i<j}(X_i - X_j)$ es el grupo alternado, A_n. Por lo tanto, el elemento $\delta = \delta(E/K) = \prod_{i<j}(x_i - x_j) \in E$ es el que decide si $G < A_n$ o no. Más precisamente, en característica distinta de 2, $\mathrm{gal}(E/K(\delta)) = G \cap A_n$.

El polinomio $(\prod_{i<j}(X_i - X_j))^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(X_i - X_j)$ es simétrico y, por lo tanto, pertenece al cuerpo S. Eso implica que el elemento $\delta^2 = \Delta = \Delta(E/K) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(x_i - x_j)$ pertenece a K (y es un polinomio en los coeficientes de P, véase 2. 4, teorema 3). Este elemento Δ se llama *discriminante de* P y también se dice que es uno de los discriminantes de E/K. Se puede calcular basándose en las observaciones siguientes: La definición de δ indica que es el valor del determinante de van der Monde en los x_i:

$$\delta = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & & \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix}$$

de donde se deduce que:

$$\Delta = \delta^2 = \left| \begin{pmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_n \\ \vdots & & \\ x_1^{n-1} & \dots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ 1 & x_n & \dots & x_n^{n-1} \end{pmatrix} \right| = \begin{vmatrix} n & s_1' & s_2' & \dots & s_{n-1}' \\ s_1' & s_2' & \dots & & \\ \vdots & & & & \\ s_{n-1}' & s_n' & \dots & & s_{2n-2}' \end{vmatrix}$$

donde, para cada $i = 1, \dots$ s_i' es el polinomio simétrico homogéneo $\sum_{j=1}^{n} x_j^i$.

Por el teorema de las funciones simétricas, cada s_i' es un polinomio de los coeficientes de P. De hecho hay fórmulas de recurrencia, las fórmulas de Newton, que permiten expresar los polinomios s_i' como polinomios de las s_i. Luego, Δ es fácilmente calculable a partir de P.

En resumen, se tiene un método eficiente de decidir si G es parte del grupo alternado o no. Basta calcular el discriminante y ver si es o no el cuadrado de un elemento de K.

Por ejemplo, en el caso de la ecuación de segundo grado: $P(X) = X^2 + bX + c = 0$, el discriminante es $\Delta = (x_1 - x_2)^2 = s_1^2 - 4s_2 = b - 4c$. Si Δ es un cuadrado, $G \subset A_2 = 1$ y $E = K$, o sea P tiene sus dos raíces en K. Si Δ no es un cuadrado, G no está contenido en A_2 y, por lo tanto, $G \cong S_2 = \langle (1,2) \rangle$.

Entonces $\delta = x_1 - x_2$ (-1 es la 2-raíz primitiva), junto con $-b = x_1 + x_2$, permiten calcular las dos raíces en la forma usual.

Nota: No interesa aquí dedicar atención especial a los diversos métodos de cálculo aplicables a la resolución efectiva de ciertas ecuaciones. Por esta razón no se presta ninguna atención especial a fórmulas (como las de Newton) ni a algoritmos generales. Tampoco preocupa, al tratar, por ejemplo, de las ecuaciones de tercero y cuarto grados, dar el camino teórico más eficiente para resolverlas en el caso general. Nos limitaremos a las consideraciones necesarias para evidenciar la posibilidad práctica de resolver dichas ecuaciones.

Al proceder así pudiera parecer que se desconoce la importancia y el mérito de diversos estudios ya realizados tendientes a describir el mejor método general de resolución. No es éste el caso, sino que se prefiere dejar de lado tales caminos teóricos generales y rígidos a fin de estimular al lector a enfocar de modo independiente cada problema particular. Esto estimula la imaginación, afianza los conocimientos y debe ser una norma más eficiente, pues sin duda el camino óptimo para resolver cada problema particular no coincide en general con el camino óptimo teórico, válido para todos los casos.

Ejemplo 3. *Ecuaciones de tercer grado.*

En esta sección se supone que $p = \chi(K) \neq 2, 3$. Sea P un polinomio de tercer grado sobre K. Ya sea directamente o por medio de las fórmulas de Newton se deducen las siguientes expresiones de los s_i' en función de los s_i:

$$s_1' = s_1, \quad s_2' = s_1^2 - 2s_2, \quad s_3' = s_2's_1 - s_1's_2 + 3s_3,$$

$$s_4' = s_3's_1 - s_2's_2 + s_1's_3$$

que permiten calcular fácilmente Δ, el discriminante de P.

Si Δ es el cuadrado de un elemento de K, o sea si $\delta \in K$, $G < A_3 \cong Z_3$ y E/K tiene grados 1 ó 3. En el primer caso, P es reducible y tiene tres raíces en K. En el segundo caso, P es irreducible sobre K pues G opera transitivamente sobre las tres raíces.

Si Δ no es el cuadrado de ningún elemento de K, $G \not< A_3$ y $G = S_3$ o (para una cierta ordenación de las raíces) $G = \langle (1, 2) \rangle$. Si se da esto último, P es reducible: tiene una raíz en K y las otras dos fuera de K.

Sea w una 3-raíz primitiva (es decir una raíz de $X^2 + X + 1$), y sea $F = K(w)$. En tal caso $E(w)$ es de Galois sobre $F(\delta)$, con grupo H contenido en A_3. Si $E(w) = F(\delta)$, $(E : K)$ es igual a 2 o a 4, pero no puede ser 4, pues S_3 no tiene subgrupos de orden 4. Luego, en este caso, P es reducible sobre K.

Por lo tanto, si P es irreducible sobre K, $(E(w) : F(\delta)) = 3$ y $E(w)/F(\delta)$ es de Galois con grupo cíclico A_3. De 3, proposición 1 se obtiene una manera de generar E. Según lo visto allí, si escribimos $y = x_1 + wx_2 + w^2x_3$, entonces $y^3 = a \in F(\delta)$ y $E(w) = F(\delta, y) = K(w, \delta, \sqrt[3]{a})$. El sistema de ecuaciones

$$x_1 + x_2 + x_3 = s_1$$

$$x_1 + wx_2 + w^2x_3 = y$$

$$x_1x_2 + x_2x_3 + x_3x_1 = s_2$$

es de segundo grado y permite el cálculo de las raíces x_i.

Ejemplo 4. *Ecuaciones de cuarto grado.*

En esta sección sean $p = \chi(K) \neq 2, 3$ y P un polinomio de cuarto grado sobre K. Para abreviar la discusión se supondrá también que P es irreducible sobre K (en caso contrario, el problema conduce a ecuaciones de primero, segundo y tercer grado).

G es un subgrupo transitivo de S_4 y, por lo tanto, para una cierta ordenación de las raíces, G es uno de los grupos siguientes:

$$\langle (1,2,3,4) \rangle \cong Z_4;$$

$$V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\};$$

$$H = \langle V_4, (1,2,3,4) \rangle \in \mathrm{Syl}_2(S_4);$$

$$A_4;$$

$$S_4.$$

Procediendo de acuerdo con el método general presentado al comienzo de esta sección, se introducen ciertos polinomios

$$Q_1 = X_1X_2 + X_3X_4, \quad Q_2 = X_1X_3 + X_2X_4, \quad Q_3 = X_1X_4 + X_2X_3$$

y vemos que el subgrupo de S_4 que deja fijos estos polinomios es V_4. La aplicación natural de $K[X_1, \ldots, X_4]$ sobre $E = K(x_1, \ldots, x_4)$ lleva Q_i sobre $y_i \in E$ $(i = 1, 2, 3)$: $y_1 = x_1x_2 + x_3x_4$, $y_2 = x_1x_3 + x_2x_4$, $y_3 = x_1x_4 + x_2x_3$. Corresponde ahora analizar las extensiones $E/K(y_1, y_2, y_3)$ y $(K(y_1, y_2, y_3)/K$. Para ello sea $Q \in K[X]$ el polinomio de raíces y_1, y_2, y_3. Su discriminante es:

$$(x_1x_2 + x_3x_4 - x_1x_3 - x_2x_4)^2 (x_1x_2 + x_3x_4 - x_1x_4 - x_2x_3)^2 \cdot (x_1x_3 + x_2x_4 -$$

$$- x_1x_4 - x_2x_3)^2 = ((x_1 - x_4)(x_2 - x_3))^2 ((x_1 - x_3)(x_2 - x_4))^2 ((x_1 -$$

$$- x_2)(x_3 - x_4))^2 = \Delta$$

o sea, Q y P tienen el mismo discriminante.

El problema de resolver $P(X) = 0$ es teóricamente fácil: se resuelve $Q(X) = 0$ como se indicó en el ejemplo 3 y después, usando por ejemplo $x_1x_2 + x_3x_4 = y_1$, $(x_1x_2)(x_3x_4) = s_4$, se obtienen (por una ecuación de segundo grado) x_1x_2 y x_3x_4. Análogamente, de $(x_1 + x_2) + (x_3 + x_4) = s_1$ y $(x_1 + x_2) + (x_3 + x_4) = y_2 + y_3$, se obtienen $x_1 + x_2$ y $x_3 + x_4$. Estos valo-

res y los precedentes permiten calcular x_1, x_2, x_3, x_4. (El lector atento mostrará que, haciendo un pequeño cambio en el procedimiento, es posible hallar las cuatro raíces resolviendo dos ecuaciones de segundo grado y un sistema de ecuaciones de primer grado; con esto se prueba que la dimensión de E sobre $K(y_1, y_2, y_3)$ es menor que o igual a 4.)

Veamos ahora las diversas posibilidades de la extensión E/K.

1. Δ *es el cuadrado de un elemento de* K. Por tanto $G < A_4$.

1. a. Q *es irreducible sobre* K.

En este caso, $\text{gal}(K(y_1, y_2, y_3)/K) \cong \text{gal}(E/K)/\text{gal}(K(y_1, y_2, y_3)/K) \cong A_3$ (aplíquese el estudio del ejemplo 3 y el hecho de que el discriminante de Q es igual a Δ). De acuerdo con las posibilidades que se tienen para G, se deduce que $G = S_4$ o $G = A_4$ y como $G < A_4$ sólo resta $G = A_4$. Esto implica, a su vez, que $\text{gal}(E/K(y_1, y_2, y_3)) \cong V_4$.

1. b. Q *es reducible sobre* K.

Valiéndose de lo visto en el ejemplo 3, se deduce que aquí, necesariamente, $\text{gal}(K(y_1, y_2, y_3)/K) = 1$, o sea que los y_i están en K. Examinando la lista de posibilidades de E, se deduce que $G = V_4$. (Nótese que $(1, 2, 3, 4) \notin A_4$.)

2. Δ *no es el cuadrado de ningún elemento de* K. $G \not< A_4$.

Se tiene la torre:

$$\begin{array}{l} E = K(x_1, \ldots, x_4) \\ | \\ F = K(y_1, y_2, y_3) \\ | \\ K(\delta) \\ | \\ K \end{array}$$

2. a. Q *es irreducible sobre* K.

Entonces $\text{gal}(F/K) \cong S_3$, lo que implica $G = S_4$.

2. b. Q *es reducible sobre* K.

Entonces Q tiene exactamente una raíz en K y se debe tener $F = K(\delta)$ y $\text{gal}(F/K) \cong S_2$. Como G no está contenido en A_4 y la dimensión de E sobre F no supera 4, se tiene (de acuerdo con la lista de posibilidades) que $G \cong \langle (1, 2, 3, 4) \rangle$ o $G \cong H$. Lo primero ocurre si $(E : F) = 2$ (cuando, por ejemplo, x_1x_3 y x_2x_4 están en F) y lo segundo, si $(E : F) = 4$.

Paso a Un Cuerpo Residual

Pasemos ahora a tratar de un segundo método para determinar el grupo de Galois de la ecuación $P(X) = 0$. La idea se aplica cuando P es un polinomio de coeficientes en un anillo R cuyo cuerpo de cocientes es

K. Bajo ciertas condiciones, si M es un ideal maximal de R y se considera P módulo M: $\bar{P}$, entonces el cuerpo de descomposición de $\bar{P}$ sobre el cuerpo $\bar{K} = R/M$ define una extensión de Galois cuyo grupo es isomorfo a un subgrupo de G. Más aún: si se identifican tanto el grupo de Galois de P como el de $\bar{P}$ con sendos subgrupos de S_n (mediante adecuada ordenación de las raíces) puede resultar que el grupo de Galois de $\bar{P}$ sea *igual* a un subgrupo de G. Entonces, variando M, es posible determinar diferentes subgrupos de G y obtener así información suficiente para caracterizar G por completo.

Este resultado depende de la posibilidad de dar una caracterización especial del grupo de Galois de un polinomio. Para presentarla, se seguirán usando las notaciones K, P, E, G, etc., pero es claro que los argumentos se aplican también a $\bar{K}$, $\bar{P}$, etc.

Como antes, se supondrá que P tiene todas sus raíces distintas y dadas en un cierto orden $x_1, \ldots, x_n$. Entonces G resulta identificado a un subgrupo de S_n. Así, si se habla del automorfismo $\sigma \in S_n$ de E/K es que nos referimos al automorfismo determinado por las condiciones $x_i \mapsto x_{\sigma(i)}$ $(i = 1, \ldots, n)$. La caracterización que se busca de G consiste en dar un criterio para que una permutación σ defina un automorfismo de G.

Introducimos n letras $X_1, \ldots, X_n$ y los cuerpos $L = E(X_1, \ldots, X_n)$ y $F = K(X_1, \ldots, X_n)$. Aplicando 2.4, proposición 2, C y el hecho de que

$F \cap E = K$, se deduce que L/F es una extensión de Galois con grupo isomorfo a G. Este isomorfismo se obtiene asociando cada f de G con su única prolongación a L que deja fijos los elementos de F, es decir, las letras X_i.

Sea x el elemento $\sum_i x_i X_i$ de L. Cada permutación $\sigma \in G < S_n$ se extiende a L dando origen a $\sigma(x) = \sum_i x_{\sigma(i)} X_i = \sum_i x_i X_{\sigma^{-1}(i)}$. O sea que la acción de cada permutación de G en el elemento especial x coincide con la acción de la permutación inversa *actuando en los letras* X_i. Para no caer en confusiones se van a especializar un poco más las notaciones.

Los elementos de $L = E(X_1, \ldots, X_n)$ son cocientes de polinomios en las letras X_i con coeficientes en $E = K(x_1, \ldots, x_n)$. Es decir, los elementos de L son cocientes de polinomios en las X_i cuyos coeficientes son polinomios en las x_i. Las permutaciones de G actúan en estos elementos de L por permutación de los x_i. Por otro lado, como en toda álgebra de funciones racionales, las permutaciones de S_n actúan en los elementos de L por permutación de las letras X_i. Para distinguir las dos acciones se convendrá en lo siguiente: si $z \in L$ y $\sigma \in G$, se escribirá $\sigma(z)$ para indicar la acción de σ en z, pero si se piensa σ como una permutación que actúa en las letras X_i, se escribirá $\tilde{\sigma}(z)$.

Entonces, repetimos, para el elemento $x \in L$ introducido más arriba, se tiene $\sigma(x) = \tilde{\sigma}^{-1}(x)$, $\forall \sigma \in G$. La definición de x muestra además que la correspondencia $\sigma \in S_n \mapsto \tilde{\sigma}(x) \in L$ es inyectiva, lo que implica, en particular, que x tiene todos sus F-conjugados distintos. Por con-

siguiente, $E = F(x)$ y cada $\sigma \in G$ está determinada por $\sigma(x) = \tilde{\sigma}^{-1}(x)$. Se tiene además que

$$\mathrm{Irr}(x/F) \underset{\text{def}}{=} P_1(X) = \prod_{\sigma \in G} (X - \sigma(x))$$

Llamaremos *polinomio genérico asociado a* $P \in K[X]$ el polinomio $\hat{P}$ definido por:

$$\hat{P}(X) = \prod_{\sigma \in S_n} (X - \tilde{\sigma}(x))$$

Este polinomio es simétrico tanto en relación con las letras X_i como en relación con las raíces x_i de P. Por lo tanto, sus coeficientes sólo dependen de los coeficientes de P y de las funciones simétricas elementales de las X_i.

El grupo de Galois de P, G, permuta las raíces de $\hat{P}$ y cada órbita para esta acción define un divisor de $\hat{P}$ con todos los coeficientes fijos para G, es decir con coeficientes en F. Se tiene entonces: $\hat{P} = P_1 \ldots P_r$, donde cada $P_i \in F[X]$ y tiene sus raíces permutadas transitivamente por G. Se deduce que cada P_i es irreducible sobre F y que $P_1 \ldots P_r$ es la descomposición de $\hat{P}$ en factores primos sobre F.

Esta caracterización de G está contenida en el teorema:

El grupo de Galois de P es el conjunto de todas las permutaciones de S_n que, operando en las letras X_i, dejan invariante uno de los divisores primos del polinomio genérico de P (y, por lo tanto, todos).

En efecto, como se acaba de ver, cada $\sigma \in G$ deja fijo cada P_i, lo que implica que $\tilde{\sigma}(P_i) = \sigma^{-1}(P_i) = P_i$. Por otro lado, si $\sigma \notin G$, $\sigma(x)$ no es un conjugado de x sobre F y, por consiguiente, $\sigma(x)$ es una raíz de un P_i diferente de P_1. Entonces, $\tilde{\sigma}^{-1}(P_1) \neq P_1$, que implica $\tilde{\sigma}(P_1) \neq P_1$.

Para enunciar el resultado en relación con grupos de Galois debemos fijar algunas otras notaciones.

Sea R un anillo íntegro con cuerpo de cocientes K y sea P un polinomio mónico con coeficientes en R y sin raíces múltiples. Sean M un ideal maximal de R, $\bar{K}$ el cuerpo cociente R/M y Q el epimorfismo natural de R sobre $\bar{K}$, que consideramos prolongado a un epimorfismo de $R[X]$ sobre $\bar{K}[X]$ (véase 1.1, observación 3 y ejemplo 6). Sean $\bar{P} = Q(P)$, E el cuerpo de descomposición de P sobre K y $\bar{E}$ el cuerpo de descomposición de $\bar{P}$ sobre $\bar{K}$. Se supondrá como antes que las raíces de P están dadas en un cierto orden $x_1, \ldots, x_n$ para poder usar las notaciones y la caracterización que vimos más arriba. Sea $S = R[x_1, \ldots, x_n]$ la R-subálgebra de E generada por los x_i. Es claro que para todo f de G, $f(S) = S$.

Proposición 1. *Con las notaciones anteriores, si $\bar{P}$ no tiene raíces múltiples, se sigue que:*

A. *Q puede prolongarse a un epimorfismo de S sobre $\bar{E}$ que lleva las raíces de P a las raíces de $\bar{P}$.*

B. *Sea* $\mathfrak{M}$ *el núcleo de esta prolongación de* $\mathfrak{L}$ *a* S *y, suponiendo* $G < S_n$, *sea* $\bar{G}$ *el subgrupo de* G *formado por las permutaciones que dejan* $\mathfrak{M}$ *invariante. La correspondencia* $\sigma \in \bar{G} \to \bar{\sigma}$, *donde* $\bar{\sigma}(\mathfrak{L}(x_1)) = \mathfrak{L}(x_{\sigma(1)})$ *define un isomorfismo de* $\bar{G}$ *sobre* $\mathrm{gal}(\bar{E}/\bar{K})$. *Más aún, si para las raíces de* $\bar{P}$ *se adopta el orden* $\bar{x}_1 = \mathfrak{L}(x_1), \ldots \bar{x}_n = \mathfrak{L}(x_n)$, *resulta que* $\mathrm{gal}(\bar{E}/\bar{K})$, *como subgrupo de* S_n, *es igual a* $\bar{G}$.

Demostración

A. Considérese la prolongación de $\mathfrak{L}$ a los polinomios y sea $\mathfrak{R}_0$ el ideal de las relaciones algebraicas de los x_i en S (un ideal de $R[X_1, \ldots, X_n]$). Sea $\bar{\mathfrak{R}}$ un ideal maximal de $\bar{K}[X_1, \ldots, X_n]$ que contiene a $\mathfrak{L}(\mathfrak{R}_0)$. Si llamamos $\bar{E}'$ al cuerpo cociente $\bar{K}[X_1, \ldots, X_n]/\bar{\mathfrak{R}}$ se tiene que, como $\mathfrak{L}(\mathfrak{R}_0) \subset \bar{\mathfrak{R}}$, $\mathfrak{L}$ induce un epimorfismo del cociente $S \cong R[X_1, \ldots, X_n]/\mathfrak{R}_0$ sobre el cociente $\bar{E}'$, el cual se seguirá denotando por $\mathfrak{L}$. Este $\mathfrak{L}$ se prolonga naturalmente al álgebra de polinomios $S[X]$. Como $P = (X - x_1) \ldots (X - x_n)$ en $S[X]$, se tiene que $\bar{P} = \mathfrak{L}(P) = (X - \mathfrak{L}(x_1)) \ldots (X - \mathfrak{L}(x_n))$ en $\bar{E}'[X]$. Esto prueba que $\bar{E}'$ contiene todas las raíces de $\bar{P}$ y, como es generado por ellas sobre $\bar{K}$, es isomorfo a $\bar{E}$.

B. Sean $\hat{P}$ y $\hat{\bar{P}}$ los respectivos polinomios genéricos asociados a P y $\bar{P}$, y sean $\hat{P} = P_1 \ldots P_r$, $\hat{\bar{P}} = \bar{P}_1 \ldots \bar{P}_s$ las respectivas descomposiciones en factores primos en $F[X]$ y $\bar{F}[X]$ (donde, como antes, $F = K(X_1, \ldots, X_n)$ y $\bar{F}$ es $\bar{K}(X_1, \ldots, X_n)$). Observemos que $\hat{P}$ tiene sus coeficientes en $R[X_1, \ldots, X_n]$ y se deduce de la definición del polinomio genérico que $\mathfrak{L}(\hat{P}) = \hat{\bar{P}}$. Por lo tanto, $\mathfrak{L}(P_1)$ es el producto de algunos de los factores primos de $\hat{\bar{P}}$.

De acuerdo con la caracterización del grupo de Galois a partir del polinomio genérico, $\mathrm{gal}(\bar{E}/\bar{K})$ es el conjunto de las permutaciones σ tales que $\bar{\sigma}(\bar{P}_1) = \bar{P}_1$. Pero esto implica $\bar{\sigma}(P_1) = P_1$, pues en caso contrario $\sigma(x)$ sería raíz de otro P_i y $\sigma(\mathfrak{L}(x))$ sería raíz de $\mathfrak{L}(P_1)$, lo que implica una contradicción.

Así queda demostrado que $\mathrm{gal}(\bar{E}/\bar{K})$, como subgrupo de S_n, es un subgrupo de G, y es claro que $\bar{G}$ está contenido en $\mathrm{gal}(\bar{E}/\bar{K})$. Para ver que son iguales, se razona así: Si $\sigma \in G$, $\sigma \notin \bar{G}$, existe $y \in \mathfrak{M}$ tal que $\sigma(y) \notin \mathfrak{M}$. Esto significa que $\sigma \notin \mathrm{gal}(\bar{E}/\bar{K})$, pues si fuera una permutación de este grupo se tendría: $0 = \sigma(0) = \sigma(\mathfrak{L}(y))$, que implicaría, sucesivamente, $\mathfrak{L}(y) = 0$ y $y \in \mathfrak{M}$.

Este teorema puede aplicarse fácilmente en la determinación del grupo de Galois de un cuerpo de números, es decir, una extensión de Galois de $\mathbb{Q}$. Si E es la extensión de $\mathbb{Q}$ definida como cuerpo de descomposición del polinomio $Q \in \mathbb{Q}[X]$, existe un entero d tal que dQ es de la forma $a_0X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$. Multiplicando por a_0^{n-1} y reemplazando X por a_0X se obtiene un polinomio mónico con coeficientes enteros, P, cuyas raíces se obtienen dividiendo las raíces de Q por a_0. Por lo tanto, E es también el cuerpo de descomposición de P.

También, sin pérdida de generalidad, puede suponerse que el cuerpo E es el cuerpo de descomposición de un polinomio mónico con coeficientes enteros, P, y sin raíces múltiples. Entonces puede intentarse

aplicar la proposición 1 con $R = \mathbb{Z}$ y M igual al ideal generado por un número primo cualquiera p. En tal caso, $\bar{K}$ es el cuerpo finito de p elementos y $\bar{P}$ es el polinomio P con sus coeficientes considerados módulo p. Si $\bar{P}$ no tiene raíces múltiples, la proposición 1 prueba que $\mathrm{gal}(\bar{P}/\bar{K})$ es un subgrupo de $G = \mathrm{gal}(E/K)$.

Como se vio en el ejemplo 1, es relativamente fácil descomponer $\bar{P}$ en factores primos y decidir si tiene o no raíces múltiples. Después, resulta trivial el determinar la forma del grupo de Galois de $\bar{P}$.

Considerando diferentes primos p se consigue determinar la forma de varias permutaciones de G y, en algunos casos, esto basta para determinar G.

Ejemplo 5. Hallar el grupo de Galois sobre $\mathbb{Q}$ de $X^5 - 3X^2 + 1$.

Considérese primero el polinomio módulo 2: $X^5 + X^2 + 1$. Si x es una raíz cualquiera se tiene:

$$x^5 = x^2 + 1, \quad x^8 = x^3 + x^2 + 1, \quad x^{16} = x^4 + x^3 + x + 1, \quad x^{32} = x$$

y se deduce que el orden de x es un divisor de 31. Como $x = 1$ no es raíz, se deduce que el orden de x es 31 y que dicho polinomio es irreducible (y separable) módulo 2.

La aplicación de la proposición 1 muestra que G contiene un ciclo de la forma (1, 2, 3, 4, 5).

Módulo 3, el polinomio se escribe: $(X^5 + 1) = (X + 1)(X^4 - X^3 + X^2 - X + 1)$. Vemos que el segundo factor es el polinomio ciclotómico de orden 10, y el grado de su cuerpo de descomposición sobre $\mathbb{F}_3$ es el mínimo k tal que 3^k es congruente con 1 módulo 10. Se obtiene que este grado es 4 y por lo tanto dicho polinomio es irreducible. $X^5 + 1$ no tiene raíces múltiples módulo 3 y, por lo establecido, su grupo de Galois es cíclico y generado por una permutación de la forma (1, 2, 3, 4).

Así hemos establecido que nuestro grupo G contiene un 5-ciclo y un 4-ciclo. Finalmente, considerando el polinomio módulo 7, se tiene $X^5 - 3X^2 + 1 = (X - 2)(X - 3)(X^3 - 2X^2 - 2X - 1)$ (descomposición en factores irreducibles). Esto muestra que G contiene también un 3-ciclo. Por lo tanto, G tiene por lo menos 60 elementos y no está contenido en A_5. Deducimos que $G \cong S_5$. El cuerpo de descomposición de nuestro polinomio tiene dimensión 120 sobre $\mathbb{Q}$, y la ecuación $X^5 - 3X^2 + 1 = 0$ no es resoluble por radicales.

Ejemplo 6. Hallar el grupo de Galois sobre $\mathbb{Q}$ de $X^5 + 2X + 9$.

Módulo 2, es $X^5 + 1$. Deducimos que G contiene un 4-ciclo.

Módulo 3, es $X^5 + 2X = (X - 1) \cdot X \cdot (X^2 + 1)$. Deducimos que G contiene una trasposición. Si el polinomio fuera reducible, como no tiene raíces racionales, sería producto de uno de segundo grado por uno de tercer grado y $(E : K)$ sería un divisor de $2!3! = 12$. Como 8 no divide 12, esto no es posible. Como G permuta transitivamente las raíces, $5 \mid\mid G \mid$ y deducimos que $G \cong S_5$.

4

EXTENSIONES INFINITAS

1. EL LEMA DE ZORN

Uno de los axiomas de la matemática que ha provocado más discusiones es el siguiente:

Axioma de elección. Todo producto cartesiano de una familia no vacía de conjuntos no vacíos, es no vacío.

El análisis lógico ha permitido establecer, en primer lugar, que el axioma de elección es independiente de los axiomas usuales de la matemática. En segundo lugar, que el axioma de elección es lógicamente equivalente a otras numerosas proposiciones pertenecientes a diversas teorías. Si bien algunas de ellas no son intuitivas, su importancia es enorme. Como consecuencia, hay una diferencia tremenda entre la matemática no-Zermeliana (que no acepta el axioma de elección) y la matemática Zermeliana (que sí lo acepta). La matemática Zermeliana constituye, en exceso, la mayor parte de la matemática actual.

Dos de las proposiciones equivalentes al axioma de elección son las siguientes:

Teorema de la buena ordenación (Zermelo). *Si A es un conjunto no vacío, existe una relación sobre A que es un buen orden.* (i.e., todo subconjunto no vacío de A tiene un elemento mínimo para dicha relación.)

Lema de Zorn. Sea $(D, \leq)$, $D \neq \phi$, un conjunto ordenado inductivo (i.e., si C es una parte no vacía de D que es totalmente ordenada por el orden de D, entonces C tiene una cota superior en D), *entonces D tiene un elemento maximal.*

Muchos teoremas importantes dependen esencialmente del lema de Zorn. Y hay muchos otros que sólo se saben demostrar con cierta facilidad usando directa o indirectamente este resultado. En este capítulo trataremos de cuestiones para cuyo desarrollo se necesita del lema de Zorn.

Frecuentemente se aplicará el lema de Zorn en la forma siguiente:

Sea D una familia de partes de un conjunto E y considérense las proposiciones siguientes:

1) Si C es una parte no vacía de D, totalmente ordenada por inclusión, la unión de C pertenece a D.

2) Si C es una parte no vacía de D, totalmente ordenada por inclusión, la intersección de C pertenece a D.

Proposición 1.

A. *Si $D \neq \phi$ verifica* (1), *D tiene un elemento maximal para la relación de inclusión.*

B. *Si $D \neq \phi$ verifica* (2), *D tiene un elemento minimal para la relación de inclusión.*

Ejemplo 1. Sean R un anillo y a un elemento inversible de R (a la izquierda, por ejemplo). Entonces existe un ideal maximal (a la izquierda) de R que contiene a a.

En efecto, sea $\mathcal{B}$ el conjunto de todos los ideales propios de R (a la izquierda) que contienen a a. $\mathcal{B} \neq \phi$ porque $Ra \in \mathcal{B}$. Si $\mathcal{C}$ es una familia totalmente ordenada de elementos de $\mathcal{B}$, $\cup\, \mathcal{C}$ es también un ideal en $\mathcal{B}$. Luego, $\mathcal{B}$ verifica (1) y tiene un elemento maximal, M. Si M no fuera un ideal maximal de R, existiría un ideal N tal que $M \subsetneq N \subsetneq R$ y se deduciría que $N \in \mathcal{B}$, lo que implica una contradicción.

De modo análogo se prueba que todo ideal propio (a la izquierda, por ejemplo) está contenido en un ideal maximal (a la izquierda).

2. CLAUSURA ALGEBRAICA

Proposición 1. *Sea E/K una extensión algebraica.*

A. *Si K es finito, E es enumerable.*

B. *Si K es infinito, $|E| = |K|$.*

Demostración. Sea $\mathcal{P}_n \subset K[X]$ el conjunto de los polinomios mónicos de grado mayor que o igual a 1, de modo que su unión es disjunta. Cada elemento x de E determina $\mathrm{Irr}(x/K)$ que pertenece a esa unión y esto permite definir una inyección de E en $\bigcup_n (J_n \times \mathcal{P}_n)$ (donde $J_n = \{1, 2, \ldots n\}$), pues cada polinomio irreducible de grado n tiene como máximo n raíces. Como $|J_n \times \mathcal{P}_n| = n \cdot |K|^n$, tenemos que, si K es finito, $\cup J_n \times \mathcal{P}_n$ es enumerable; si K es infinito, $|J_n \times \mathcal{P}_n| = |K|$ y se deduce B.

Teorema 1. *Todo cuerpo K tiene una clausura algebraica.* Es decir, dado K existe Ω/K, algebraica, tal que Ω es algebraicamente cerrado (cf. 2.5, definición 6).

Demostración. Sea C un conjunto cuyo cardinal es mayor que $|\mathbb{N}|$ y que $|K|$. Por la proposición 1, si E/K es algebraica existe una inyección de E en C. Sea $\mathcal{E}$ el conjunto de todas las estructuras de extensión algegraica de K: $(E, +, .\,; K \to E)$ que se pueden definir sobre un conjunto parte de C (con las diferentes definiciones posibles de suma, multiplicación, etc.). Considérese $\mathcal{E}$ ordenado por la relación "ser subcuerpo de". Es claro que $\mathcal{E}$ verifica 1, proposición 1, A y, por lo tanto, tiene un elemento maximal $(E, +, .\,; K \to E)$. Si E no fuera algebraicamente cerrado existiría una extensión algebraica propia, F, de E. Por la elección de C existe una inyección $I : F \to C$ que se reduce a la identidad en E. Si se define en $i(F)$ la estructura de cuerpo que hace de i un isomorfismo,

tenemos que $t(F) \in \mathfrak{s}$, y se contradice la maximalidad de E. Luego E es algebraicamente cerrado.

Observación 1. Toda clausura algebraica de K es normal/K.

Teorema 2. *Extensión de morfismos.*

Sea E/K una extensión algebraica y L/K una extensión cualquiera tal que L es algebraicamente cerrado.

A. *Todo $f \in \mathrm{Hom}(F/K, L/K)$ de una subextensión F de E se prolonga a un morfismo de E en L.*

B. *Si Ω_1/E, Ω_2/E son dos clausuras algebraicas de E, entonces son E-isomorfas y, por lo tanto, K-isomorfas.*

C. *Sea $E \hookrightarrow \Omega$, donde Ω es una clausura algebraica de E. Entonces, todo K-morfismo de E en Ω se prolonga a un K-automorfismo de Ω.*

Demostración.

A. Consideremos un K-morfismo f de F en L y la familia de sus prolongaciones a subextensiones de E (véase 2.3, proposición 1 y definición 2). Si $g : E_1 \to L$ es una prolongación maximal (que existe en virtud del lema de Zorn), entonces $E_1 = E$. Pues si existiera un x en E que no está en E_1, g podría prolongarse a $E_1(x)$.

B. Por A, el morfismo $E \hookrightarrow \Omega_2$ se prolonga a Ω_1. Su imagen es entonces una subextensión de Ω_2 tal que Ω_2 es algebraica sobre ella y tal que ella es algebraicamente cerrada. Esto implica que esa imagen es igual a Ω_2.

C. Consecuencia trivial de B.

3. GRADO DE TRASCENDENCIA

Definición 1. *Sea E/K una extensión cualquiera y $A \subset E$.*

A. *Si $A = \{x_1, \ldots, x_n\}$, A es algebraicamente libre sobre K* (notación: a.i./K) *cuando $K[x_1, \ldots, x_n]$ es el álgebra de los polinomios en las letras x_i con coeficientes en K* (o sea cuando $P(x_1, \ldots, x_n) = 0$).

B. *Si A es infinito, A es* a.i./K *cuando todo subconjunto finito de A es* a.i./K.

C. *E/K es trascendente pura si existe una parte S,* a.i./K, *tal que $E = K(S)$* (es decir, cuando S es finito, E es el álgebra de las funciones racionales en las letras de S).

Proposición 1. *Toda extensión E/K contiene un conjunto B que es* a.i./K *maximal. $E/K(B)$ es algebraica y $K(B)/K$ es trascendente pura.*

Demostración. La existencia de B es consecuencia del lema de Zorn. Si fuera $E/K(B)$ trascendente, habría un elemento x en E trascendente

sobre $K(B)$. Entonces $B \cup \{x\}$ sería a.i./K, lo que implica una contradicción.

Definición 2. *Los conjuntos B que verifican las propiedades de la proposición 1 se llaman bases de trascendencia de E/K.*

Sean E una extensión de K y S una parte de E. *Se dirá que S es a-generador de E* sobre K si $E/K(S)$ es algebraica. Si E/K tiene un conjunto a-generador finito, se dirá que E tiene *grado de trascendencia* finito sobre K.

Proposición 2. *Sea S un conjunto a-generador de E/K.*

A. *Si $A \subset E$ es un conjunto finito y* a.i./K, $|A| \leq |S|$.

B. *Si E/K tiene grado de trascendencia finito y B_1 y B_2 son bases de trascendencia de E/K, entonces* $|B_1| = |B_2|$.

Demostración

A. Sea $a \in A$. Como a es alg/$K(S)$ existe un polinomio con coeficientes en $K(S)$ que tiene a como raíz. Considerando que sólo un número finito de elementos de S pueden figurar en los coeficientes de este polinomio, se deduce que, para un cierto n, existe $P \in K[X, X_1, \ldots, X_n]$ y elementos $s_1, \ldots, s_n \in S$ tales que $P(a, s_1, \ldots, s_n) = 0$. Como a es a.i./K (es decir, trascendente sobre K), si consideramos a P como polinomio en X con coeficientes en $K[X_1, \ldots, X_n]$, debe haber por lo menos un coeficiente de P que tenga grado positivo en las X_i. Si llamamos Q a ese polinomio coeficiente y si X_i es una letra que aparece en un monomio de Q con coeficiente no nulo, se deduce que s_i es algebraico sobre $K(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n, a)$. Por lo tanto, $(S - \{s_i\}) \cup \{a\}$ es un nuevo conjunto a-generador de E/K.

Razonando por inducción, sea $A_1 \subset A$ con r elementos, tal que existe $S_1 \subset S$, con r elementos, tal que $S' = (S - S_1) \cup A_1$ es un conjunto a-generador de E/K. Si $A_1 = A$ la existencia de S_1 significa $|A| \leq |S|$. Si existe un elemento a en $A - A_1$, como a es alg/$K(S')$, existe $P' \in K[X_1, \ldots, X_r, Y_1, \ldots, Y_{n-r}][X]$ tal que $P(a_1, \ldots, a_r, s_1, \ldots, s_{n-r})(a) = 0$ (donde los a_i son los elementos de A_1 y los s_i son ciertos elementos de $S - S_1$). Considerando ahora P' como polinomio en $X_1, \ldots, X_r, X$ con coeficientes en $K[Y_1, \ldots, Y_{n-r}]$ se deduce que, como $\{a_1, \ldots, a_r, a\}$ es a.i./K, hay por lo menos un coeficiente Q' de P' que tiene grado positivo en $Y_1, \ldots, Y_{n-r}$. Razonando como antes resulta entonces que hay un $s_i \in S - S_1$ que es algebraico sobre $K(a, a_1, \ldots, a_r, s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_{n-r})$. Por lo tanto $S - S_1$ no puede ser vacío y escribiendo $A' = A_1 \cup \{a\}$ y $S'' = S_1 \cup \{s_i\}$ (ambos con $r + 1$ elementos), se tiene que $A' \cup (S - S'')$ es un nuevo conjunto a-generador de E/K.

Este procedimiento de inducción finita termina cuando se tiene un conjunto $S_0 \subset S$, con el mismo número de elementos que A, tal que $A \cup (S - S_0)$ es a-generador de E/K. Luego $|A| \leq |S|$.

B. Trivial, porque tanto B_1 como B_2 son a.i./K y a-generadores de E/K. Basta aplicar dos veces lo anterior tomando primero B_1 como conjunto A y B_2 como S, y después B_2 como A y B_1 como S.

Corolario. *Si E/K tiene grado de trascendencia infinito todo conjunto a-generador es infinito.*

Nota. También en el caso de grado de trascendencia infinito se puede demostrar que dos bases de trascendencia tienen siempre el mismo cardinal.

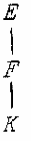
Definición 3. *Si E/K tiene grado de trascendencia finito, se llama grado de trascendencia de E/K* (notación grtr(E/K)) *al número de elementos de una base de trascendencia de E/K.*

Por ejemplo, si $X_1, \ldots, X_n$ son letras, entonces grtr$_K(X_1, \ldots, X_n)/K = n$.

El comportamiento del grado de trascendencia con relación a las configuraciones elementales es el siguiente:

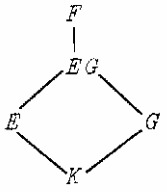
Proposición 3.

A. *Dada la torre*



grtr (E/K) *es infinito si, y sólo si,* grtr (E/F) y grtr (F/K) *son finitos. En tal caso,* grtr(E/K) = grtr(E/F) + grtr(F/K).

B. *Dada la configuración:*



si grtr(E/K) *es finito,* grtr$(EG/G) \leq$ grtr(E/K). *Para que sean iguales, es necesario y suficiente que toda parte de E* a.i./K *sea también* a.i./G.

C. *En el caso anterior,* grtr(EG/K) *es finito si, y sólo si,* grtr(E/K) *y* grtr(G/K) *son finitos. Si esto es así,* grtr$(EG/K) \leq$ grtr(E/K) + grtr(G/K) *y para que sean iguales es necesario y suficiente que toda parte de E* (resp. de G), *que es* a.i./K, *sea también* a.i./G (resp./E).

Demostración

A. Sea grtr(E/K) finito. Si $B \subset F$ es a.i./K, entonces $|B| \leq$ grtr(E/K) (por la proposición 2) y grtr(F/K) es finito. Si C es a.i./F, también lo es sobre K y por lo tanto también grtr(E/F) es finito.

Sean ahora B y C bases de trascendencia de F/K y E/F, respectivamente. Como $B \cap C = \phi$, es suficiente mostrar que $B \cup C$ es una base de trascendencia de E/K. Escribamos $B = \{x_1, \ldots, x_n\}$, $C = \{y_1, \ldots, y_m\}$. Si existiera un polinomio Q tal que $Q(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$, considerándolo como polinomio en $Y_1, \ldots, Y_m$ con coeficientes en $K(x_1, \ldots, x_n) \subset \subset F$, tendríamos que cada uno de sus coeficientes es 0 (porque los y_i son a.i./F). O sea, los coeficientes de Q en $K[X_1, \ldots, X_n]$ se anulan para los x_i. Como los x_i son a.i./K se deduce que $Q = 0$. Esto prueba que $B \cup C$ es a.i./K, y sólo falta mostrar que E es algebraico sobre $K(B \cup C)$. Si $x \in E$, x es alg/$F(C)$. Esto significa que existe un polinomio $P \in \in F[y_1, \ldots, y_m][X]$ que se anula en x. Si $a_1, \ldots, a_r$ son los coeficientes de P en F, se tiene que $P \in K[a_1, \ldots, a_r, y_1, \ldots, y_m][X]$. O sea, x es algebraico sobre $K(a_1, \ldots, a_r, y_1, \ldots, y_m)$ y, como $K(a_1, \ldots, a_r, y_1, \ldots, y_m)$ es algebraico sobre $K(x_1, \ldots, x_n, y_1, \ldots, y_m)$, entonces x es algebraico sobre $K(B \cup C)$.

B. Sea B, de cardinal n, una base de trascendencia de E/K y sea s tal que $E = K(B)(S)$. Entonces $EG = G(B)(S)$ y, como S es algebraico sobre K, S es algebraico sobre G. Luego, si B' es una parte a.i./G maximal de B, resulta que B' es una base de trascendencia de EG/G. Esto prueba que $\mathrm{grtr}(EG/G) \leq \mathrm{grtr}(E/K)$. Para que sean iguales es necesario y suficiente que $B' = B$, lo que equivale al enunciado.

C. Como EG/K es una torre con pisos EG/G y G/K (o EG/E y E/K), esta proposición es consecuencia de A y B.

4. SEPARABILIDAD

Sea p el exponente característico de K y sea Ω una clausura algebraica de K. Para cada subextensión E de Ω sea $E^{p^{-1}} \underset{\text{def}}{=} F^{-1}(E)$, donde, si $p = 1$, $F = id_\Omega$, y, si $p > 1$, F es el automorfismo de Frobenius de Ω. Es claro que E es un subcuerpo de $E^{p^{-1}}$.

Se define, por recurrencia, la sucesión:

$$E_0 = E, \quad E_{n+1} = (E_n)^{p^{-1}} \underset{\text{def}}{=} E^{p^{-(n+1)}}$$

que es una sucesión creciente. Entonces

$$E^{p^{-\infty}} \underset{\text{def}}{=} \bigcup_n E_n$$

es un subcuerpo de Ω.

Nótese que los conceptos aquí adoptados sólo tienen interés cuando K tiene característica positiva.

Proposición 1. *$K^{p^{-\infty}}/K$ es la mínima subextensión de Ω/K que es un cuerpo perfecto.*

Demostración. Sea E/K una subextensión de Ω/K tal que E es un cuerpo perfecto. Como no existen elementos p.i./E, si x es un elemento arbitrario de Ω tal que, para algún natural k, $x^{p^k} \in E$, entonces $x \in E$. Esto significa que $E \supset E^{p^{-\infty}} \supset K^{p^{-\infty}}$.

Basta mostrar ahora que $K^{p^{-\infty}}$ es perfecto. Sea x algebraico sobre $K^{p^{-\infty}}$ y sea N la mínima extensión normal de K que contiene a x. Como toda extensión finita normal, N es una torre $N/D/K$ con N/D separable y D/K puramente inseparable. Por 2.5., observación 2, $D \subset K^{p^{-\infty}}$. Como x es sep/D, x es sep/$K^{p^{-\infty}}$.

Proposición 2. *Si $p = 1$, sea $E^p = E$ y, si $p > 1$, sea E^p la imagen de E con relación al automorfismo de Frobenius de Ω. Entonces, si E/K es finita, E/K es separable si, y sólo si, $E^pK = E$.*

Demostración. Por 2.5, como E/E_s es p.i., existe una potencia de p, p^k tal que $E^{p^k} \subset E_s$. Entonces, $E^pK = E$ implica (por inducción) $E^{p^k}K = E$, o sea $E = E_s$. Por otro lado, si $E^pK \neq E$ existe $x \in E$ tal que $x \notin E^pK$, lo que implica que E/E^pK es inseparable y, por lo tanto, E/K es inseparable.

Corolario. *Si E/K es una extensión algebraica separable* (no necesariamente finita) *y si $x_1, \ldots, x_n$ son* l.i./K, *entonces $x_1^p, \ldots, x_n^p$ también son* l.i./K.

Demostración. Agregando ciertos elementos $x_{n+1}, \ldots, x_m$ obtenemos una base de $F = K(x_1, \ldots, x_n)$. Entonces $KF^p = K\sum_{i=1}^{n} K^p x_i^p = \sum_{i=1}^{n} Kx_i^p = F$. Se deduce que $x_1^p, \ldots, x_m^p$ es una base de F.

Proposición 3. *Criterio de Mac Lane*

Sea E/K una extensión algebraica y Ω una clausura algebraica de E.

A. *Si E/K es separable, E y $K^{p^{-\infty}}$ son* L. D./K.

B. *Si E y $K^{p^{-1}}$ son* L. D./K, *entonces E/K es separable.*

Nótese que si E y $K^{p^{-\infty}}$ son L. D./K, entonces E y $E^{p^{-1}}$ también lo son.

Demostración. Sean $x_1, \ldots, x_n$ l.i./K en E. Si fueran l.d./$K^{p^{-\infty}}$, lo serían sobre $K^{p^{-k}}$ para algún k, y $x_i^{p^k}$ serían l.d./K, en contradicción con el corolario de la proposición 2.

Esto prueba A. Para probar B sean: $x \in E$, $F = K(x)$, $x_1, \ldots, x_n$ una K-base de F. Si E y $K^{p^{-1}}$ son L. D./K, entonces $x_1^p, \ldots, x_n^p$ son también l.i./K, pues si fuera $\sum_i a_i x_i^p = 0$ se deduciría la relación $\sum_i a_i^{p^{-1}} x_i = 0$ que implica $a_i = 0$ para todo i. Deducimos que los x_i^p forman una K-base de F y, por lo tanto, $KF^p = F$. Como x era arbitrario, esto prueba que todos los elementos de E son separables sobre K.

El criterio de Mac Lane proporciona una vía para generalizar la definición de separabilidad a extensiones cualesquiera:

Definición 1

A. *Una extensión E/K es separable cuando E y $K^{p^{-\infty}}$ son* L. D./K.

B. $x \in E$ *es separable sobre* K *cuando* $K(x)/K$ *es separable.*

Con esta definición se tiene, por ejemplo, que toda extensión trascendente pura es separable.

Definición 2. *Sea* E/K *una extensión con grado de trascendencia finito. Se dice que una base de trascendencia,* B, *de* E/K *es una base de trascendencia separante cuando* $E/K(B)$ *es algebraica y separable.*

Por ejemplo, si X es una letra, X es una base de trascendencia separante de $K(X)/K$. En general existen ciertas bases de trascendencia, como X^p (si $p > 1$) que no son bases de trascendencia separantes.

Proposición 4. *Toda extensión separable finitamente generada posee una base de trascendencia separante* (existen contraejemplos de esta afirmación si la extensión no es finitamente generada).

Demostración. Se puede suponer que $p > 1$. Sea $E = K(x_1, \ldots, x_n)$ una extensión separable y demostremos que existe un subconjunto $\{x_{i_1}, \ldots, x_{i_r}\}$ que es una base de trascendencia separante. Se puede razonar por inducción en n pues la proposición es obvia si $n = 0$. Sea $P \in K[X_1, \ldots, X_n]$ un polinomio no nulo de grado mínimo del ideal de las relaciones algebraicas de las x_i. Sean M_j los monomios de P: $P = \sum_j a_j M_j$. Se afirma que existe un M_j y una X_i tales que X_i tiene un exponente que no es múltiplo de p en M_j. En efecto, si no fuera así, existiría, para cada j, un monomio N_j tal que $M_j = N_j^p$, y los elementos $N_j(x_1, \ldots, x_n)$ serían $1.d./K^{p^{-1}}$. Por el criterio de Mac Lane, serían entonces $1.d./K$ y tendríamos una relación no trivial de la forma $\sum_j b_j N_j(x_1, \ldots, x_n) = 0$. Entonces $\sum_j b_j N_j$ sería un polinomio de grado menor que P que también estaría en el ideal de las relaciones algebraicas de los x_i.

Sea entonces X_i una letra que, en algún monomio de P, no tiene exponente múltiplo de p. El polinomio $P(x_1, \ldots, x_{i-1}, X_i, x_{i+1}, \ldots, x_n) \in K(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)[X_i]$ es irreducible (si fuera factorizable o nulo también se contradiría la definición de P) y separable. Esto prueba que x_i es separable sobre $E_i = K(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Por la hipótesis de inducción, existen $x_{i_1}, \ldots, x_{i_r}$ entre $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ que forman una base de trascendencia separante de E_i/K. Entonces $x_{i_1}, \ldots, x_{i_r}$ también son una base de trascendencia separante de E/K.

Si $E = K(x_1, \ldots, x_n)$ es una extensión trascendente pura de K (con grado de trascendencia finito) y si F es una subextensión de E, ¿será también F/K una extensión trascendente pura? Esta cuestión es todavía un problema abierto. Una respuesta muy parcial, en sentido afirmativo, se da en el teorema siguiente.

Proposición 6. *Teorema de Lüroth*

Sea $E = K(x)$ *una extensión trascendente pura de grado 1. Entonces todo cuerpo intermedio* F *es también una extensión trascendente pura de* K (de grado 1).

Demostración. Comencemos introduciendo la noción auxiliar de *altura* de un elemento y de $K(x)$. Como $K(x) \cong K(X)$, y es de la forma $f(x)/g(x)$, donde $f, g \in K[X]$ son polinomios relativamente primos. El número $n = \text{máx}(\text{gr}(f), \text{gr}(g))$ se llama altura de y.

Consideremos el polinomio $f(X) - Yg(X) \in K[X, Y]$. Pensándolo como polinomio en Y con coeficientes en $K[X]$, vemos que es irreducible y primitivo, por lo tanto, un elemento primo de $K[X, Y]$. Considerándolo como polinomio en X con coeficientes en $K[Y]$ es un elemento primo de $K[Y][X]$, y, por consiguiente, irreducible sobre $K(Y)$. Esto significa que $f(X) - yg(X)$ es irreducible sobre $K(y)$. Se ha demostrado:

$$f(X) - yg(X) = \text{Irr}(x/K(y))$$

$$\text{altura de } y = (K(x) : K(y))$$

Sea ahora F un cuerpo intermedio y elíjase y como un elemento de F de altura mínima. Vamos a demostrar que $F = K(y)$.

Consideremos el polinomio $P(X, Y) = f(X)g(Y) - f(Y)g(X)$. Tenemos que $P(X, x)/g(x) = \text{Irr}(x/K(y))$, de modo que $\text{Irr}(x/F)$ divide a $P(X, x)/g(x)$. Este polinomio $\text{Irr}(x/F)$ es de la forma:

$$\text{Irr}(x/F) = X^n + y_1X^{n-1} + \ldots + y_n =$$

$$= X^n + \frac{f_1(x)}{g_1(x)}X^{n-1} + \ldots + \frac{f_n(x)}{g_n(x)} = \frac{P'(X, x)}{g'(x)}$$

donde las fracciones $f_i(x)/g_i(x)$ son las expresiones mínimas de los $y_i \in F$. Por la elección de y, altura de $y_i = \text{máx}(\text{gr}(f_i), \text{gr}(g_i) \geq$ altura de $y = \text{máx}(\text{gr}(f), \text{gr}(g))$. P', como polinomio de $K[x][X]$, es primitivo (véase I. 2, proposición 1, B) y el denominador $g'(x)$ es el mmc de los $g_i(x)$.

Observamos que el grado de $P'(X, x)$, como polinomio en x con coeficientes en $K[X]$ es mayor que o igual a la altura de y, o sea, mayor que o igual al grado de $P(X, x)$ con relación a x. Por otro lado, como $\text{Irr}(x/F)$ divide a $P(X, x)/g(x)$, se deduce que $P'(X, x) \mid P(X, x)$ y que el grado de $P'(X, x)$ con relación a x, es igual al grado de $P(X, x)$ con relación a x. Por lo tanto, $P'(X, x)$ es asociado con $P(X, x)$ como elementos de $K[X][x]$, y, siendo ambos primitivos, son iguales.

Esto termina la demostración pues:

$$(K(x) : F) = \text{grado, con relación a } X, \text{ de } P'(X, x)$$

$$= \text{grado, con relación a } X, \text{ de } P(X, x)$$

$$= \text{grado, con relación a } x, \text{ de } P(X, x)$$

$$= \text{altura de } y = (K(x) : K(y)$$

implican $F = K(y)$.

5

EJERCICIOS

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 1

Ejercicio 1. Sea A el R-álgebra de base $(e_{ij})_{i,\,j=1,\ldots,n}$ con la multiplicación definida por

$$e_{ij}e_{kl} = \delta_{jk}e_{il} \quad (\forall i, j, k, l)$$

Demostrar que A es isomorfa al álgebra de matrices de tipo $n \times n$ con coeficientes en R.

Ejercicio 2. Sea A una R-álgebra conmutativa y considérese la aplicación $P \mapsto \hat{P}$ que a cada polinomio $P \in R[X_1, \ldots, X_n]$ asocia la función polinómica $\hat{P}: (x_1, \ldots, x_n) \mapsto ev_{(x_1, \ldots, x_n)} P$ de $\underbrace{A \times A \times \ldots \times A}_{n}$ en A.

a) Muestre que $P \mapsto \hat{P}$ es un homomorfismo de R-álgebras.

b) Si A tiene un número finito de elementos, ¿es cierto o falso que $P \mapsto \hat{P}$ es un epimorfismo (o sea que toda función de n variables de A en A es polinómica)?

c) Demostrar que si $n = 1$ y R es un anillo íntegro infinito, $P \mapsto \hat{P}$ es inyectivo.

Ejercicio 3. Hallar los R-automorfismos de $R[X]$. Si K es un cuerpo, hallar los K-automorfismos de $K(X)$.

Ejercicio 4. Sea K un cuerpo, $F = K(X)$, $E = K(X^3)$. Demostrar que $Y^3 - X^3 \in E[Y]$ es irreducible.

Ejercicio 5. ¿Es $X^n + Y^n - 1$ irreducible sobre $\mathbb{C}$?

Ejercicio 6. Sean $f, g, h \in K[X, Y]$ (K un cuerpo) y sea $\mathcal{Q} \in K[X]$ tal que $f\mathcal{Q} = gh$. Demostrar que, si los coeficientes de g como elemento de $K[X][Y]$ son primos relativos, entonces $\mathcal{Q}$ divide los coeficientes de h como elemento de $K[X][Y]$.

Ejercicio 7. Demostrar que sen x (función de R en R) no es una función polinomial.

Ejercicio 8. Demostrar $\mathbf{Z}[i\sqrt{5}]$ es un anillo factorial.

Ejercicio 9. Examinar si $(2X - 1)$ es o no un ideal maximal de $\mathbf{Z}[X]$.

Ejercicio 10. Determinar cuáles de los polinomios

a) $X^3 + 1$, b) $X^3 + X + 2$, c) $X^3 + 6X^2 + 11X + 8$, d) $X^4 + 1$,

son irreducibles sobre $\mathbb{Q}$ y sobre $\mathbb{F}_3$.

Ejercicio 11. Demostrar que $K[X, Y]$ (K un cuerpo) no es un anillo principal.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 2

Ejercicio 1. a) Si $K(a, b)/K$ es una extensión finita tal que $\text{mdc}(K(a) : K), (K(b) : K)) = 1$, hallar $(K(a, b) : K)$.

b) Hallar $(\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q})$.

Ejercicio 2. Sea x un elemento algebraico sobre el cuerpo K tal que $\text{Irr}(x/K) = X^n - a$. Si m es un número natural que divide a n, mostrar que $\text{gr}(x^m/K) = \frac{n}{m}$.

Ejercicio 3. Hallar $(\mathbb{Q}(\sqrt{2 + \sqrt{2}}) : \mathbb{Q})$ y decidir si la extensión $\mathbb{Q}(\sqrt{2 + \sqrt{2}})/\mathbb{Q}$ es normal o no. Hallar $\text{Irr}(\mathbb{Q}(\sqrt{2 + \sqrt{2}}/\mathbb{Q}(\sqrt{2}))$.

Ejercicio 4. Demostrar que la extensión $\mathbb{F}_2(X, Y)/\mathbb{F}_2(X^2, Y^2)$ no posee un elemento primitivo. ¿Cuántos cuerpos hay entre $\mathbb{F}_2(X^2, Y^2)$ y $\mathbb{F}_2(X, Y)$?

Ejercicio 5. Hallar el grado de separabilidad de $\mathbb{F}_2(X, Y)$ sobre $\mathbb{F}_2(X^2, Y^2)$. ¿Qué clase de extensión es ésta?

Ejercicio 6. Hallar un elemento primitivo de $K(\sqrt{2}, \sqrt{3})/K$, para $K = \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}$.

Ejercicio 7. Decir si es verdad o no que:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}); \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} \cdot \sqrt{3});$$

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2 + 3})$$

Ejercicio 8. Hallar los posibles grupos $\text{gal}(E/K)$ donde E es el cuerpo de descomposición de un polinomio irreducible de grado 5 de $K[X]$.

Ejercicio 9. Para cada uno de los polinomios:

$$X^4 - 10X^2 + 5, \quad X^4 + X^2 - 6, \quad X^4 - 10X^2 + 4, \quad X^4 + 4X^2 + 2,$$

determinar:

a) el cuerpo de descomposición sobre K y un elemento primitivo de la extensión correspondiente para $K = \mathbb{Q}, \mathbb{F}_3, \mathbb{F}_7$ y $\mathbb{F}_{13}$;

b) el grupo de Galois de cada una de estas extensiones.

Ejercicio 10. Sea p un número primo y w una 5-raíz primitiva sobre $\mathbb{Q}$. Hallar $\text{gal}(\mathbb{Q}(\sqrt[5]{p}, w)/\mathbb{Q})$.

Ejercicio 11. Sea $K = \mathbb{F}_5(X)$ y sea E el cuerpo de descomposición sobre K de $(Y^5 - Y - X^2)(Y^2 - w) \in K[Y]$, donde w es una 4-raíz primitiva. Determinar $\mathrm{gal}(E/K)$.

Ejercicio 12. Sea F/K una extensión inseparable de dimensión $3p$ (p primo) tal que todo cuerpo intermedio es inseparable sobre K. Hallar:

a) $\chi(K)$; b) generadores de F/K; c) las posibles dimensiones de las subextensiones de F/K.

Ejercicio 13. Si $(E : K) = 147$ y $\chi(K) = 7$, hallar los posibles valores de $(E : K)_s$. Suponiendo que $E = K(a)$, donde $a^{147} \in K$, hallar $\mathrm{Aut}(E/K)$.

Ejercicio 14. Si $p_1, \ldots, p_r$ son primos distintos, hallar $\mathrm{gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})/\mathbb{Q})$.

Ejercicio 15. Demostrar que si $\mathrm{mdc}(m, n) = 1$, entonces $\mathbb{Q}(\sqrt[m]{1})$ y $\mathbb{Q}(\sqrt[n]{1})$ son L. D. /$\mathbb{Q}$.

Ejercicio 16. Dado un cuerpo $K/\mathbb{Q}$, sea E la mínima extensión normal de $\mathbb{Q}$ que contiene a K. Hallar $\mathrm{gal}(E/\mathbb{Q})$ en los casos siguientes: a) $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, b) $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$.

En los ejercicios siguientes, "construible" significa "construible con regla y compás".

Ejercicio 17. Sea $A = \{\alpha \in \mathbb{R} / \cos \alpha \text{ es construible}\}$. Demostrar que $(A, +)$ es un grupo y que $\alpha \in A$ implica $\frac{\alpha}{2} \in A$.

Ejercicio 18. Sea $E/\mathbb{Q}$ la extensión de todos los números reales construibles. Demostrar que: a) $E/\mathbb{Q}$ es infinita; b) $\mathrm{Aut}(E/\mathbb{Q}) = \{id_{\mathbb{Q}}\}$.

Ejercicio 19. Demostrar que un ángulo de n grados es construible si, y sólo si, n es divisible por 3.

Ejercicio 20. Decidir si las raíces de $X^4 + 3X^3 + 5X^2 + 3X + 1$ son construibles.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 3

Ejercicio 1. Averiguar si la ecuación $X^7 = 1$ es resoluble por radicales sobre $\mathbb{F}_2$.

Ejercicio 2. Resolver (en característica 0) las ecuaciones: a) $X^3 + 6X + 2 = 0$, b) $X^3 + 9X + 6 = 0$.

Ejercicio 3. Resolver (en característica 0) la ecuación $X^4 - X + \frac{3}{4} = 0$.

Ejercicio 4. Decidir si $X^5 - 10X + 5 = 0$ es resoluble por radicales sobre $\mathbb{Q}$.

Ejercicio 5. Resolver $X^3 + 1 = 0$ en característica 3 y en característica 5.

Ejercicio 6. Resolver $X^3 + X^2 + 1 = 0$ en característica 13.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 4

Ejercicio 1. Demostrar que $K(X)$ y $K(Y)$ son L. D. $/K$ en $K(X,Y)$, pero la subálgebra de $K(X,Y)$ generada por ellas no es un cuerpo.

Ejercicio 2. Mostrar que $\mathbb{R}/\mathbb{Q}$ tiene grado de trascendencia infinito.

Ejercicio 3. Sean $K = \mathbb{Q}(X)$ y x una raíz de $Y^2 + X^2 + 1 \in K[Y]$. Si $E = K(x)$, demostrar que:

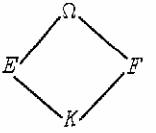
a) cada elemento de E que no está en $\mathbb{Q}$ es tras$/\mathbb{Q}$.

b) $E/\mathbb{Q}$ no es trascendente pura.

c) $E(t)/\mathbb{Q}(t)$ es trascendente pura.

Ejercicio 4. Si F/K es finitamente generada, entonces toda subextensión de F/K es también finitamente generada.

Ejercicio 5. Dada la configuración



mostrar que si E/K es trascendente pura y F/K es algebraica, entonces E y F son L. D. $/K$.

ÍNDICE DE TÉRMINOS

ÍNDICE DE SÍMBOLOS

$\{x \in A/P(x)\}$ conjunto de los elementos de A con la propiedad P.

$\{a_1, \ldots, a_n\}$ conjunto de los elementos $a_1, \ldots, a_n$.

ϕ conjunto vacío.

$|A|$ número de elementos del conjunto A.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sistema de los números naturales, enteros, racionales, reales, complejos.

Z_n anillo de los enteros módulo n.

U_n unidades del anillo Z_n.

φ_n función de Euler.

δ_{ij} delta de Kronecker.

BIBLIOGRAFÍA

(1) ALBERT, A. A. A. Fundamental Concepts of Higher Algebra. The University of Chicago Press, Chicago, Ill., 165 págs. (1956).

(2) ARTIN, E. Galois Theory, Notre Dame Mathematical Lectures No. 2, 2a. edición, Notre Dame, Ind. (1944).

(3) BOURBAKI, N. Algèbre, Hermann, París, cáps. 4 y 5, 222 págs. (1959).

(4) GENTILE, E. R. Estructuras Algebraicas II, Monografía No. 12, Serie de Matemática, OEA, Washington, D. C., 510-S-8004, 160 págs (1971).

(5) JACOBSON, N. Lectures in Abstract Algebra, Vol. III: Theory of Fields and Galois Theory, Springer-Verlag, Nueva York, N. Y., 323 págs. (1975).

(6) O'BRIEN, H. H. Estructuras Algebraicas III, Monografía No. 14, Serie de Matemática, OEA, Washington, D. C., 510-S-8268, 137 págs. (1973).

COLECCIÓN DE MONOGRAFÍAS CIENTÍFICAS

Publicadas

Serie de matemática

N° 1. La Revolución en las Matemáticas Escolares, por el Consejo Nacional de Maestros de Matemáticas de los Estados Unidos de América.
N° 2. Espacios Vectoriales y Geometría Analítica, por Luis A. Santaló.
N° 3. Estructuras Algebraicas I, por Enzo R. Gentile.
N° 4. Historia de las Ideas Modernas en la Matemática, por José Babini.
N° 5. Álgebra Lineal, por Orlando E. Villamayor.
N° 6. Álgebra Linear e Geometria Euclidiana, por Alexandre Augusto Martins Rodrigues.
N° 7. El Concepto de Número, por César A. Trejo.
N° 8. Funciones de Variable Compleja, por José I. Nieto.
N° 9. Introducción a la Topología General, por Juan Horváth.
N° 10. Funções Reais, por Djairo G. de Figueiredo.
N° 11. Probabilidad e Inferencia Estadística, por Luis A. Santaló.
N° 12. Estructuras Algebraicas II (Álgebra Lineal), por Enzo R. Gentile.
N° 13. La Revolución en las Matemáticas Escolares (Segunda Fase), por Howard F. Fehr, John Camp y Howard Kellog.
N° 14. Estructuras Algebraicas III (Grupos Finitos), por Horacio H. O'Brien.
N° 15. Introducción a la Teoría de Grafos, por Fausto A. Toranzos.
N° 16. Estructuras Algebraicas IV (Álgebra Multilineal), por Artibano Micali y Orlando E. Villamayor.
N° 17. Introdução à Análise Funcional: Espaços de Banach e Cálculo Diferencial, por Leopoldo Nachbin.
N° 18. Introducción a la Integral de Lebesgue en la Recta, por Juan Antonio Gatica.
N° 19. Introducción a los Espacios de Hilbert, por José I. Nieto.
N° 20. Elementos de Biomatemática, por Alejandro B. Engel.
N° 21. Introducción a la Computación, por Jaime Michelow.
N° 22. Estructuras Algebraicas V (Teoría de Cuerpos), por Hector A. Merklen.

Serie de física

N° 1. Concepto Moderno del Núcleo, por D. Allan Bromley.
N° 2. Panorama de la Astronomía Moderna, por Félix Cernuschi y Sayd Codina.
N° 3. La Estructura Electrónica de los Sólidos, por Leopoldo M. Falicov.
N° 4. Física de Partículas, por Igor Saavedra.
N° 5. Experimento, Razonamiento y Creación en Física, por Felix Cernuschi.
N° 6. Semiconductores, por George Bemski.
N° 7. Aceleradores de Partículas, por Fernando Alba Andrade.

N° 8. Física Cuántica, por Onofre Rojo y Harold V. McIntosh.
N° 9. La Radiación Cósmica, por Gastón R. Mejía y Carlos Aguirre.
N° 10. Astrofísica, por Carlos Jaschek y Mercedes C. de Jaschek.
N° 11. Ondas, por Oscar J. Bressan y Enrique Gaviola.
N° 12. El Láser, por Mario Garavaglia.

Serie de química

N° 1. Cinética Química Elemental, por Harold Behrens LeBas.
N° 2. Bioenergética, por Isaias Raw y Walter Colli.
N° 3. Macromoléculas, por Alejandro Paladini y Moisés Murachik.
N° 4. Mecanismo de las Reacciones Orgánicas, por Jorge A. Brieux.
N° 5. Elementos Encadenados, por Jacobo Gómez Lara.
N° 6. Enseñanza de la Química Experimental, por Francisco Giral.
N° 7. Fotoquímica de Gases, por Ralf-Dieter Penzhorn.
N° 8. Introducción a la Geoquímica, por Félix González-Bonorino.
N° 9. Resonancia Magnética Nuclear de Hidrógeno, por Pedro Joseph-Nathan.
N° 10. Cromatografía Líquida de Alta Presión, por Harold M. McNair y Benjamín Esquivel H.
N° 11. Actividad Óptica, Dispersión Rotatoria Óptica y Dicroísmo Circular en Química Orgánica, por Pierre Crabbé.
N° 12. Espectroscopia Infrarroja, por Jesús Morcillo Rubio.
N° 13. Polarografía, por Alejandro J. Arvía y Jorge A. Bolzan.
N° 14. Paramagnetismo Electrónico, por Juan A. McMillan.
N° 15. Introducción a la Estereoquímica, por Juan A. Garbarino.
N° 16. Cromatografía en Papel y en Capa Delgada, por Xorge A. Domínguez.
N° 17. Introducción a la Espectrometría de Masa de Sustancias Orgánicas, por Otto R. Gottlieb y Raimundo Braz Filho.
N° 18. Cinética Química, por Rodolfo V. Caneda.
N° 19. Fuerzas Intermoleculares, por Mateo Díaz Peña.

Serie de biología

N° 1. La Genética y la Revolución en las Ciencias Biológicas, por José Luis Reissig.
N° 2. Bases Ecológicas de la Explotación Agropecuaria en la América Latina, por Guillermo Mann F.
N° 3. La Taxonomía y la Revolución en las Ciencias Biológicas, por Elías R. de la Sota.
N° 4. Principios Básicos para la Enseñanza de la Biología, por Oswaldo Frota-Pessoa.
N° 5. A Vida da Célula, por Renato Basile.
N° 6. Microorganismos, por J. M. Gutiérrez-Vázquez.
N° 7. Principios Generales de Microbiología, por Norberto J. Palleroni.
N° 8. Los Virus, por Enriqueta Pizarro-Suárez y Gamba.
N° 9. Introducción a la Ecología del Bentos Marino, por Manuel Vegas Vélez.

N° 10. Biosíntesis de Proteínas y el Código Genético, por Jorge E. Allende.
N° 11. Fundamentos de Inmunología e Inmunoquímica, por Félix Córdoba Alva y Sergio Estrada-Parra.
N° 12. Bacteriófagos, por Romilio Espejo T.
N° 13. Biogeografía de América Latina, por Angel L. Cabrera y Abraham Willink.
N° 14. Relación Huésped-Parásito. Mecanismo de Patogenicidad de los Microorganismos, por Manuel Rodríguez Leiva.
N° 15. Genética de Poblaciones Humanas, por Francisco Rothhammer.
N° 16. Introducción a la Ecofisiología Vegetal, por Ernesto Medina.
N° 17. Aspectos de Biología Celular y la Transformación Maligna, por Manuel Rieber.
N° 18. Transporte a Través de la Membrana Celular, por P. J. Garrahan y A. F. Rega.
N° 19. Duplicación Cromosómica y Heterocromatina a Nivel Molecular y Citológico, por Nestor O. Bianchi.
N° 20. Citogenética Básica y Biología de los Cromosomas, por F. A. Sáez y Horacio Cardoso.
N° 21. Ecología de Poblaciones Animales, por Jorge E. Rabinovich.

En preparación

Serie de matemática

Estructuras Algebraicas VI (Estructuras de Álgebras), por Artibano Micali.
Estructuras Algebraicas VII (Formas Cuadráticas), por Mario Piscoya H.

Serie de física

Oceanografía Física, por Luis E. Herrera.
Teoría de Fluidos en Equilibrio, por Antonio E. Rodríguez y Roberto E. Caligaris.
Aplicação da Teoria de Grupos na Espectroscopia Raman e do Infra-Vermelho, por Jorge Humberto Nicola y Anildo Bristoti.
Teoría Estadística de la Materia, por Antonio E. Rodríguez y Roberto E. Caligaris.
Geofísica, por Alvaro F. Espinosa.
Introducción a la Espectroscopia Atómica, por Mario Garavaglia y Athos Giacchetti.
Reacciones Nucleares, por Oscar Sala y Francisco B. Coutinho.
Superconductividad, por Miguel Kiwi.
Cristalografía, por Jaime Rodríguez-Lara.
Efecto Mössbauer, por Jacques A. Danon.
Magnetismo, por Horacio A. Farach.

Serie de química

Cromatografía de Gases, por Harold M. McNair.
Síntesis Orgánica, por Eduardo Sánchez.

Catálisis Homogénea, por Eduardo Humeres A.
Catálisis Heterogénea, por Sergio Droguett.
Introducción a la Electroquímica, por Dionisio Posadas.
Corrosión, por José Rodolfo Galvele.
Fisicoquímica de Interfases, por Javier Garfias Ayala.
Química de Suelos, por Elemer u. Bornemisza.
Introducción a la Metalurgia Física, por Joaquín Hernández Marín.
Físico-Química de Superficies, por Tibor Rabockai.

Serie de biología

Etología: El Estudio del Comportamiento Animal, por Raúl Vaz-Ferreira.
Citogenética Ultraestructural y la Biología Molecular de los Cromosomas, por R. Wettstein y Roberto Sotelo.
Análisis de Sistemas en Ecología, por Gilberto C. Gallopín.
Principios Básicos de la Contracción Muscular, por Carlos Caputo.
Germinación, por Luiz Gouvêa Laboriau.
Clastogénesis y Contaminación Ambiental, por Fernando Noel Dulout.

Nota: Las personas interesadas en adquirir estas obras deben dirigirse a la Unidad de Ventas y Promoción, Organización de los Estados Americanos, Washington, D. C., 20006 o a las Oficinas de la Secretaría General de la OEA en el país respectivo.