Teoria de Galois

José Luis Tábara

jltabara@gmail.com

Índice

1. Primeros ejemplos

En estas notas todos los anillos son conmutativos y tienen unidad. Emplearemos en general la letra A para denotar un anillo. Mediante $A[x]$ (con corchetes) denotamos el anillo de polinomios con coeficientes en A. Si $a \in A$, mediante (a) denotamos el ideal principal generado por el elemento a.

Definición 1.1 *Un* cuerpo *es un anillo donde todo elemento no nulo es invertible.*

Sea k un cuerpo. El conjunto $k^* = k - \{0\}$ es un grupo (abeliano) respecto a la multiplicación. Además, todo cuerpo es en particular un anillo íntegro: si $ab = 0$, donde a es no nulo, multiplicando dicha expresión por a^{-1} obtenemos que $b = 0$ y no existen divisores de cero.

Ejemplos.

- Los conjuntos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con las operaciones habituales son cuerpos.
- El subconjunto de $\mathbb{C}$

  $$\mathbb{Q}(i) = \{a + bi \text{ con } a, b \in \mathbb{Q}\}$$

  es un cuerpo con las operaciones habituales.
- También es un cuerpo el subconjunto de $\mathbb{R}$

  $$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \text{ con } a, b \in \mathbb{Q}\}$$

- Sea p un número primo. Veamos que el anillo $\mathbb{F}_p = \mathbb{Z}/(p)$ es un cuerpo. Sea $\pi(a)$ un elemento no nulo. Entonces a no es múltiplo de p y como p es primo, el máximo común divisor de p y a es 1. Por el lema de Bezout, se puede encontrar una expresión del tipo

  $$mp + na = 1$$

donde m y n son enteros. Tomando clases de equivalencia módulo p

$$\pi(n)\pi(a) = \pi(1) = 1$$

y todo elemento no nulo es invertible.

- Todo anillo íntegro y finito es un cuerpo. Sea $a \in A$ no nulo. La aplicación

$$\begin{array}{rccc} \varphi: & A & \longrightarrow & A \\ & b & \longrightarrow & ab \end{array}$$

es inyectiva puesto que A es íntegro. Como el conjunto es finito, también es epiyectiva. Existe un elemento tal que $\varphi(b) = 1$. Esto equivale a encontrar el inverso de a.

- $\mathbb{Z}$ no es un cuerpo pues existen elementos que no son invertibles. Sin embargo existen cuerpos (por ejemplo $\mathbb{Q}$) que contienen a $\mathbb{Z}$.

- Sea n un número compuesto y $n = n_1 n_2$ una descomposición no trivial. Tomando clases de equivalencia módulo n

$$\pi(n_1)\pi(n_2) = \pi(n) = 0$$

El anillo $\mathbb{Z}/(n)$ tiene divisores de cero y no puede ser un cuerpo. Además no existe ningún cuerpo que contenga al anillo $\mathbb{Z}/(n)$.

Observación. 1 *Existe una generalización de uno de los ejemplos anteriores, aunque su demostración no es tan elemental. El teorema de Wedderbun afirma que todo anillo finito e íntegro es necesariamente conmutativo. Todo cuerpo no conmutativo es necesariamente infinito.*

2. Ideales y morfismos

Proposición 2.1 *Un anillo A es un cuerpo si y solo si sus únicos ideales son el cero y el total.*

Demostración. $\Rightarrow$) Sea A un cuerpo e I un ideal no nulo. Si $a \in I$ es no nulo, entonces $a^{-1}a = 1 \in I$ y el ideal es el total.

$\Leftarrow$) Supongamos que A posee solamente ideales triviales. Si $a \in A$ es no nulo, el ideal principal (a) es el total. Existe un elemento $b \in A$ tal que $ab = 1$ y todo elemento no nulo es invertible. $\square$

Corolario 2.2 *Un anillo cociente A/I es un cuerpo si y solo si I es un ideal maximal.*

Demostración. Gracias al morfismo de paso al cociente, los ideales de A/I se identifican con los ideales de A que contienen a I.

$\Rightarrow$) Si I es maximal, solamente existen dos ideales que lo contienen. Entonces el cociente tiene dos ideales y es un cuerpo.

$\Leftarrow$) Si A/I es un cuerpo, solamente posee dos ideales. Existen dos ideales que contienen a I, que son necesariamente el mismo y el total. El ideal es maximal. $\square$

Ejemplos.

- En $\mathbb{Z}$ los ideales maximales son de la forma (p) donde p es un primo no nulo. Esto nos da otra demostración de que $\mathbb{F}_p$ es un cuerpo.
- El polinomio x^2+1 es irreducible sobre el cuerpo $\mathbb{Q}$ y el ideal que genera es maximal. El anillo cociente $\mathbb{Q}[x]/(x^2+1)$ es un cuerpo.
- En general, si sobre un cuerpo k existen polinomios irreducibles de grado mayor que 1, se pueden construir nuevos cuerpos haciendo cocientes del anillo de polinomios.

Definición 2.1 *Un* morfismo de cuerpos *es una aplicación $\varphi : k \to k'$ que verifica:*

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1) = 1$

Un morfismo de cuerpos es simplemente un morfismo de anillos con unidad. Debido a la propiedad $\varphi(1) = 1$, un morfismo de cuerpos nunca es nulo. El núcleo es un ideal que no puede ser el total. Como un cuerpo tiene solamente dos ideales obtenemos la

Proposición 2.3 *Todo morfismo de cuerpos es inyectivo.*

Si $\varphi : k \to k'$ es morfismo y es biunívoco, entonces la aplicación inversa es también morfismo. Los morfismos biyectivos se denominan isomorfismos. Los isomorfismos de k en si mismo son los automorfismos. Dado un cuerpo k, el conjunto de sus automorfismos se designa por $\mathrm{Aut}(k)$ y es un grupo respecto a la composición. Si k y k' son cuerpos isomorfos, los grupos $\mathrm{Aut}(k)$ y $\mathrm{Aut}(k')$ son isomorfos.

Ejemplos.

- La conjugación $x \to \overline{x}$ es un automorfismo de $\mathbb{C}$.
- La inyección canónica de $\mathbb{Q}$ en $\mathbb{R}$ y la de éste en $\mathbb{C}$.
- Supongamos que existe un morfismo φ de $\mathbb{F}_p$ en k. Necesariamente se cumple

  $$\varphi(n) = \varphi(1+\overset{n)}{\cdots}+1) = \varphi(1)+\overset{n)}{\cdots}+\varphi(1) = 1+\overset{n)}{\cdots}+1$$

  Como mucho, existe un morfismo de $\mathbb{F}_p$ en k. En particular, el grupo $\mathrm{Aut}(\mathbb{F}_p)$ es trivial.
- Supongamos dado un morfismo φ de $\mathbb{Q}$ en k. Este morfismo está totalmente determinado puesto que

  $$\varphi(n) = 1+\overset{n)}{\cdots}+1 = n \cdot 1$$

  y si $q = m/n$, tenemos que $\varphi(q) = \varphi(n)\varphi(m)^{-1}$. El grupo $\mathrm{Aut}(\mathbb{Q})$ es trivial.

- Sea φ el único morfismo de anillos de $\mathbb{Q}[x]$ en $\mathbb{C}$ que sobre $\mathbb{Q}$ es la identidad y que cumple $\varphi(x) = i$. Debido a la propiedad $i^2 = -1$, la imagen del morfismo es precisamente $\mathbb{Q}(i)$. El polinomio $x^2 + 1$ pertenece al núcleo y es el generador de dicho ideal. El teorema de factorización canónica nos dice que existe un isomorfismo entre los cuerpos $\mathbb{Q}[x]/(x^2 + 1)$ y $\mathbb{Q}(i)$. El mismo razonamiento demuestra que $\mathbb{R}[x]/(x^2 + 1)$ es isomorfo a $\mathbb{C}$.

Consideremos un cuerpo k. Existe un único morfismo de $\mathbb{Z}$ en k que denominaremos característica y lo denotaremos por ch. Este morfismo viene definido por la condición $ch(n) = n \cdot 1$. Como $\mathbb{Z}$ no es un cuerpo, puede ocurrir que el morfismo no sea inyectivo. La imagen de $\mathbb{Z}$ por ch es un anillo íntegro y el núcleo de ch debe ser un ideal primo, que puede ser el ideal nulo o bien el generado por un número primo positivo.

Definición 2.2 *Un cuerpo k tiene* característica cero *si* $\mathrm{Ker}(ch) = 0$. *Tiene* característica p *si* $\mathrm{Ker}(ch) = (p)$.

Existe otra definición de característica que no hace intervenir al morfismo ch. La demostración de la equivalencia de ambas definiciones es inmediata.

Proposición 2.4 *El menor entero n que cumple $n \cdot 1 = 0$ es la característica de k. Si necesariamente dicha ecuación implica que $n = 0$, entonces k tiene característica nula.*

Si la característica es nula, podemos considerar que $\mathbb{Z}$ está contenido en el cuerpo k. Si el cuerpo tiene característica p, via el morfismo ch, se puede considerar a $\mathbb{F}_p$ como un subconjunto de k.

Ejemplos.

- Los cuerpos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen característica nula.
- El cuerpo $\mathbb{F}_p$ tiene característica p.
- Sea f un polinomio irreducible sobre $\mathbb{Q}$. El cuerpo $\mathbb{Q}[x]/(f)$ tiene característica nula. En general si un cuerpo k tiene característica p, todo cuerpo de la forma $k[x]/I$ sigue teniendo característica p.

- Sean k y K dos cuerpos tales que $k \subset K$. El morfismo $ch : \mathbb{Z} \to K$ tiene su imagen enteramente contenida en el cuerpo k y de este modo la características de k y de K coinciden.

- En todo anillo conmutativo es válido el binomio de Newton

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

  Si la característica del anillo es p y elevamos a p un binomio, todos los factores, salvo el primero y el último son nulos (los coeficientes intermedios son múltiplos de p). Esto prueba que si k tiene característica p la aplicación

$$\begin{array}{rccc} \phi: & k & \to & k \\ & a & \to & a^p \end{array}$$

  es un morfismo de cuerpos, llamado morfismo de Fröbenius. Este morfismo no es necesariamente epiyectivo.

3. Generación de anillos y cuerpos

Hemos visto que muchos anillos y cuerpos con los que hemos tratado se pueden considerar incluidos en otros anillos o cuerpos.

Definición 3.1 *Sea A un anillo. Un subconjunto $B \subset A$ es un* subanillo *si con las operaciones inducidas es un anillo. Un subconjunto $k \subset A$ es un* subcuerpo *si con las operaciones inducidas es un cuerpo.*

Ejemplos.

- $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ de $\mathbb{R}$ y de $\mathbb{C}$.

- $\mathbb{Q}$ es un subcuerpo de $\mathbb{R}$ y éste es un subcuerpo de $\mathbb{C}$.

- k es un subcuerpo del anillo $k[x]$. También es subcuerpo de $k[x]/(f)$.

- $\mathbb{Q}(i)$ es un subcuerpo de $\mathbb{C}$.

- $\mathbb{Q}(\sqrt{2})$ es un subcuerpo de $\mathbb{R}$ y por lo tanto de $\mathbb{C}$.

Proposición 3.1 *La intersección de subanillos es subanillo y la intersección de subcuerpos es subcuerpo.*

Demostración. Sea A una anillo y B_i una colección de subanillos. Veamos que la intersección $\bigcap B_i$ es también subanillo. Como $1 \in B_i$ para todo i, necesariamente $1 \in \bigcap B_i$. Sean a y b dos elementos de $\bigcap B_i$. Entonces a y b pertenecen a todo subanillo B_i. De esta forma $a+b$ y ab pertenecen a todos los B_i y también a la intersección. Si todos los B_i son cuerpos, dado $a \in \bigcap B_i$ no nulo, el mismo razonamiento prueba que $a^{-1} \in \bigcap B_i$ y es un subcuerpo. □

Gracias a esta proposición podemos hablar del subanillo o del subcuerpo generado por un subconjunto.

Definición 3.2 *Sea $S \subset A$ un subconjunto. La intersección de todos los subanillos que contienen a S se denota $[S]$ (con corchetes). Dicho anillo se dice que está* generado *por S.*

La intersección es no vacía pues existe al menos un subanillo (el propio A) que contiene a S. De todos los subanillos que contienen a S, precisamente $[S]$ es el menor de ellos: si $S \subset B$ y B es subanillo, entonces $[S] \subset B$.

Observación. 2 *El subanillo $[S]$ no determina al subconjunto S. Puede ocurrir que $S \neq S'$ y sin embargo $[S] = [S']$.*

Ejemplos.

- Sea $A = \mathbb{R}$ y $S = \{1\}$. El subanillo generado por S es precisamente $\mathbb{Z}$.
- Sea $A = \mathbb{C}$ y $S = \{1, i\}$. Si un subanillo contiene a S, necesariamente contiene a todo elemento de la forma $a + bi$ con $a, b \in \mathbb{Z}$. Pero este conjunto es ya de por si un anillo. Tenemos que $[1, i] = \mathbb{Z}(i)$, el anillo de los enteros de Gauss. Si $S = \{1, 1+i\}$ el subanillo que genera también es el de los enteros de Gauss.

- Sea $A = k[x]$. El subanillo generado por $S = k \cup \{x\}$ es todo el anillo de polinomios.

Para la construcción del subanillo generado por un subconjunto nos hemos asegurado de que al menos existe un subanillo que contiene a S. En general no podremos afirmar que existe un subcuerpo que contiene a S. Por ello solamente consideramos subcuerpos de un cuerpo y no de un anillo.

Definición 3.3 *Dado un cuerpo k y un subconjunto $S \subset k$, denotamos por (S) (con paréntesis) a la intersección de todos los subcuerpos que contienen a S.*

De nuevo (S) es el mínimo cuerpo que contiene a S. Además tenemos que $[S] \subset (S)$ pues todo cuerpo es en particular un anillo.

Observación. 3 *La notación empleada para designar el subcuerpo generado puede confundirse con la utilizada para denotar el ideal principal generado por un elemento. El contexto aclarará los posibles conflictos.*

Dado un cuerpo k la intersección de todos los subcuerpos de k necesariamente contienen al 1. El subcuerpo generado por el 1 se denomina subcuerpo primo de k. La característica del subcuerpo primo coincide con la característica del cuerpo k. Un cuerpo se denomina primo si coincide con su subcuerpo primo.

Proposición 3.2 *Los cuerpos primos son $\mathbb{F}_p$ y $\mathbb{Q}$.*

Demostración. Sea k un cuerpo primo. Dicho cuerpo debe contener a todos los múltiplos del 1. Si el cuerpo tiene característica p entonces dicho cuerpo coincide con $\mathbb{F}_p$. Si tiene característica nula, entonces el cuerpo contiene un subanillo isomorfo a $\mathbb{Z}$. Pero por ser cuerpo debe contener a todas las fracciones formadas con elementos de $\mathbb{Z}$. Entonces k contiene un cuerpo isomorfo a $\mathbb{Q}$ y por ser primo coincide con él. □

Corolario 3.3 *Si k tiene característica p su subcuerpo primo es $\mathbb{F}_p$. Si tiene característica nula su subcuerpo primo es $\mathbb{Q}$.*

Corolario 3.4 *Salvo isomorfismos solo existe un cuerpo con p elementos.*

Observación. 4 *También es cierto que existe un único cuerpo con p^n elementos (que se denota $\mathbb{F}_{p^n}$), pero la demostración de este hecho no es tan elemental. La veremos a lo largo de estas notas.*

4. Cuerpos de fracciones

Todo subanillo contenido en un cuerpo es un anillo íntegro. Veremos que todo anillo íntegro se puede considerar como subanillo de un cuerpo. Esta construcción también aclarará la relación entre $[S]$ y (S) en los casos que nos interesan.

Sea A un anillo íntegro y denotamos por A^* al conjunto $A - \{0\}$. En el producto cartesiano $A \times A^*$ introducimos la relación de equivalencia

$$(a, b) \sim (a', b') \text{ si } ab' = a'b$$

La clase de equivalencia del elemento (a, b) se denotará con la fracción a/b. Con esta notación, más sugestiva, tenemos

$$\frac{a}{b} \sim \frac{a'}{b'} \text{ si y solo si } ab' = a'b$$

En el espacio cociente introducimos las operaciones

$$\begin{aligned} \frac{a}{b} + \frac{a'}{b'} &= \frac{ab' + a'b}{bb'} \\ \frac{a}{b} \cdot \frac{a'}{b'} &= \frac{aa'}{bb'} \end{aligned}$$

Dichas definiciones son independientes de los representantes que tomemos de cada clase y dotan al conjunto cociente de estructura de anillo. El elemento neutro para la suma es $0/b$ y el elemento neutro para el producto $1/1$. Si una fracción a/b es no nula, es debido a que el numerador es no nulo. En este caso la fracción b/a es la inversa y el anillo en cuestión es un cuerpo. Este cuerpo que acabamos de construir lo denotaremos $\mathrm{Fr}(A)$.

Definición 4.1 $\mathrm{Fr}(A)$ *es el* cuerpo de fracciones *del anillo* A.

A cada elemento $a \in A$ le podemos hacer corresponder la fracción $a/1$. Esto nos da un morfismo de A en su cuerpo de fracciones que es inyectivo. Todo anillo íntegro se puede considerar un subanillo de su cuerpo de fracciones.

Observación. 5 *En el caso del anillo* $k[x]$*, es costumbre denotar a su cuerpo de fracciones mediante* $k(x)$ *(con paréntesis). Sus elementos se llaman* fracciones racionales.

El siguiente resultado se conoce como la propiedad universal del anillo de fracciones.

Proposición 4.1 *Sea* A *un anillo íntegro,* k *un cuerpo y* $\varphi : A \to k$ *un morfismo inyectivo. Existe un único morfismo de cuerpos*

$$\overline{\varphi} : \mathrm{Fr}(A) \longrightarrow k$$

que sobre A *coincide con* φ*.*

Demostración. Si $\overline{\varphi}$ es morfismo de cuerpos debe cumplir

$$\overline{\varphi}(b^{-1}) = (\overline{\varphi}(b))^{-1}$$

Como φ es inyectivo, $\varphi(b)$ es un elemento invertible del anillo si b es no nulo. Todo elemento del anillo de fracciones se puede expresar como una fracción a/b. Necesariamente se debe cumplir

$$\overline{\varphi}(a/b) = \overline{\varphi}(ab^{-1}) = \overline{\varphi}(a)\overline{\varphi}(b)^{-1} = \varphi(a)\varphi(b)^{-1}$$

y el morfismo es único.

Para demostrar la existencia del morfismo utilizamos como definición el resultado que acabamos de ver. Fácilmente se observa que la definición de $\overline{\varphi}$ no depende de la fracción tomada y que esta aplicación es un morfismo de cuerpos que sobre A coincide con φ. $\square$

Si el morfismo no es inyectivo entonces no podemos asegurar que $\varphi(b)$ es invertible y la definición de $\overline{\varphi}$ no tiene sentido para aquellas fracciones cuyo denominador tenga una imagen no invertible.

Corolario 4.2 *Un anillo es íntegro si y solo si es un subanillo de un cuerpo.*

Dado un cuerpo, cualquier subanillo $[S]$ es también íntegro. El cuerpo de fracciones de $[S]$ es el mínimo cuerpo que contiene a S y coincide con nuestra definición de (S).

Corolario 4.3 *Si k es un cuerpo, el cuerpo de fracciones de $[S]$ es (S).*

Ejemplos.

- El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$. Todo cuerpo que contenga a $\mathbb{Z}$ debe contener también a $\mathbb{Q}$ como subcuerpo. Los cuerpos de característica cero tienen un subcuerpo isomorfo a $\mathbb{Q}$.
- Dado el anillo de los enteros de Gauss, $\mathbb{Z}(i)$, su cuerpo de fracciones es $\mathbb{Q}(i)$.
- Si A es un cuerpo, su cuerpo de fracciones es (isomorfo a) A.
- Si un cuerpo k contiene a un subanillo A, entonces contiene al cuerpo de fracciones de A. En este sentido, el cuerpo de fracciones es el "mínimo" cuerpo que contiene al anillo A.

5. k-álgebras

Aunque estamos principalmente interesados en el estudio de los cuerpos, muchas veces tendremos que utilizar conceptos y resultados de la teoría de anillos. Es por esto que se estudia el concepto de k-álgebra y no simplemente el de extensión.

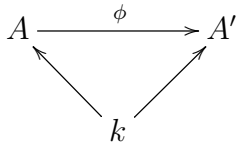
Definición 5.1 *Una k-*álgebra *es un anillo A y un morfismo de anillos $i : k \to A$. Si cambiamos el anillo A o el morfismo i obtenemos otra estructura de k-álgebra.*

En general, el morfismo se sobreentiende y una k-álgebra se denota simplemente por $k \to A$. Si tenemos un morfismo $i : k \to A$, entonces es inyectivo y la imagen $i(k)$ es canónicamente isomorfa a k. Por ello muchas veces se llama k-álgebra a un anillo que contiene como subanillo al cuerpo k. Nosotros cometeremos habitualmente este abuso de notación. Los elementos de la imagen de k se denominan constantes y son elementos invertibles del anillo. Los ideales de A no pueden contener constantes.

Definición 5.2 *Una* extensión *del cuerpo k es un k-álgebra $k \to K$ tal que K tiene estructura de cuerpo.*

Con el abuso de notación comentado, una extensión consta de dos cuerpos: el cuerpo "mayor" K, llamado muchas veces extensión, y un subconjunto k que tiene estructura de subcuerpo, que a veces llamaremos cuerpo base.

Definición 5.3 *Dadas dos k-álgebras $k \to A$ y $k \to A'$, un* morfismo de k-álgebras *(también llamado k-*morfismo*) es un morfismo de anillos $\phi : A \to A'$ que hace conmutativo el diagrama*



Si cometemos el abuso de notación de suponer que k está incluido en el anillo, un morfismo de k-álgebras no es más que un morfismo de anillos que sobre k es la identidad.

Si la aplicación es biyectiva, la aplicación inversa es también morfismo de álgebras. Podemos hablar de álgebras isomorfas.

Corolario 5.1 *Un k-morfismo entre dos extensiones es siempre inyectivo.*

Es claro que si el dominio del morfismo no es una extensión, puede ocurrir que el morfismo no sea inyectivo.

Ejemplos.

- La inyección natural $\mathbb{R} \to \mathbb{C}$ es una extensión. Normalmente relajamos la notación y decimos que $\mathbb{C}$ es una extensión de $\mathbb{R}$. Del mismo modo $\mathbb{R}$ es una extensión de $\mathbb{Q}$. El cuerpo $\mathbb{Q}(i)$ es una extensión de $\mathbb{Q}$.

- Todo cuerpo es una extensión de su subcuerpo primo. En general todo cuerpo K es una extensión de cualquier subcuerpo k que esté contenido en K.

- El anillo de polinomios $k[x]$ es una k-álgebra. El cuerpo k se identifica con los polinomios de grado cero. El general, cualquier anillo de polinomios, en un número finito o infinito de variables, es una k-álgebra.

- Sea I un ideal de $k[x]$. Como I no contiene a las constantes, podemos considerar que k está contenido en $k[x]/I$ vía la proyección canónica, que restingida a k es inyectiva. Si el ideal I es maximal, entonces es una extensión.

- Sean A_1y A_2 dos k-álgebras. Definimos el morfismo

$$\begin{array}{rccc} \varphi: & k & \longrightarrow & A_1 \times A_2 \\ & \lambda & \longrightarrow & (\lambda, \lambda) \end{array}$$

  Este morfismo dota al producto de anillos de una estructura de k-álgebra. Muchas veces este álgebra se denota $A_1 \oplus A_2$ y se llama suma directa de las álgebras.

- La identidad $\mathrm{Id} : k(x) \to k(x)$ proporciona una extensión evidente del cuerpo de fracciones racionales. Llamemos $\varphi : k(x) \to k(x)$ al único morfismo de cuerpos (propiedad universal del anillo de fracciones) que verifica $\varphi(x) = x^2$. Esta es otra extensión, no tan evidente, de $k(x)$. Es por razones como esta por lo que muchas veces se insiste en el morfismo y no se considera una extensión como una simple inclusión de cuerpos.

- Sea $i : \mathbb{Q}(\sqrt{2}) \to \mathbb{R}$ la inclusión canónica. Sea $j : \mathbb{Q}(\sqrt{2}) \to \mathbb{R}$ el morfismo $j(a + b\sqrt{2}) = a - b\sqrt{2}$. Ambas son extensiones y sin embargo no son isomorfas (pruébese que no existe ningún isomorfismo de cuerpos de $\mathbb{R}$ que haga conmutativo el diagrama).

Definición 5.4 *Dada una k-álgebra A, llamamos* subálgebra *a todo anillo $B \subset A$ que contenga a las constantes. Si ambos anillos son cuerpos se denomina* subextensión.

Como toda subálgebra contiene a las constantes, el morfismo $k \to A$ da origen a un morfismo $k \to B$ y toda subálgebra adquiere de modo natural una estructura de k-álgebra. Es fácil observar que la intersección de una colección de subálgebras es de nuevo una subálgebra. La subálgebra generada por un subconjunto $S \subset A$ es la intersección de todas las subálgebras que contienen a S. La denotaremos por $k[S]$ (con corchetes). La subálgebra $k[S]$ es un anillo que contiene por una parte al cuerpo k y por otra al conjunto S. Además cualquier anillo que contenga a esos dos conjuntos debe contener a $k[S]$.

Proposición 5.2 *La subálgebra $k[S]$ coincide con el anillo generado por el conjunto $k \cup S$.*

En el caso de que S sea un conjunto finito, $S = \{a_1, \ldots, a_n\}$, se suele emplear la notación $k[a_1, \ldots, a_n]$. En esta notación, el orden dado a los elementos carece de importancia.

Definición 5.5 *Un álgebra A es de* generación finita *si existe un conjunto finito $\{a_1, \ldots, a_n\}$ tal que $A = k[a_1, \ldots, a_n]$.*

Proposición 5.3 *Dados dos elementos a_1, a_2 del álgebra A se tiene que*

$$k[a_1][a_2] = k[a_1, a_2] = k[a_2][a_1]$$

Demostración. En los tres casos el conjunto es igual al anillo generado por el subconjunto $k \cup \{a_1\} \cup \{a_2\}$. □

Corolario 5.4 *En general se cumple*

$$k[S_1][S_2] = k[S_1 \cup S_2] = k[S_2][S_1]$$

siendo S_1 y S_2 subconjuntos arbitrarios.

Observación. 6 *Puede ocurrir que $k[S_1] = k[S_2]$ siendo $S_1 \neq S_2$. Distintos conjuntos generadores pueden dar lugar al mismo álgebra.*

Sea A una k-álgebra. Dado un conjunto finito $\{a_1, \ldots, a_n\}$ de elementos de A, existe un único morfismo de k-álgebras

$$\phi : k[x_1, \ldots, x_n] \to A$$

que verifica $\phi(x_i) = a_i$ (propiedad universal del anillo de polinomios). La imagen de este morfismo es una subálgebra que contiene a los elementos a_i. Pero por otra parte, cualquier subálgebra que contenga a dichos elementos debe contener a la imagen de ϕ. En definitiva, la imagen de ϕ coincide con la subálgebra $k[a_1, \ldots, a_n]$. El mismo razonamiento, aunque con una notación un poco más complicada, es válido para conjuntos infinitos.

Corolario 5.5 *Toda álgebra A es isomorfa a un cociente de un anillo de polinomios.*

Demostración. Tomamos un subconjunto S tal que $k[S] = A$. El morfismo ϕ inducido es epiyectivo y el teorema de factorización canónica nos da un isomorfismo deseado. Si el álgebra es de generación finita podemos tomar un anillo con un número finito de variables. □

Ejemplos.

- Entendamos $\mathbb{C}$ como un álgebra sobre $\mathbb{R}$. En este caso el conjunto $\{i\}$ genera todo el cuerpo $\mathbb{C}$. En fórmulas tenemos $\mathbb{R}[i] = \mathbb{C}$.
- Consideremos a $\mathbb{C}$ como una $\mathbb{Q}$-álgebra. El álgebra $\mathbb{Q}[i]$ coincide con el cuerpo $\mathbb{Q}(i)$.
- Sea $A = k[x]$. Este álgebra es de generación finita puesto que basta tomar $S = \{x\}$. Como vemos la notación que hemos adoptado para la subálgebra generada se adapta a nuestra notación del anillo de polinomios.

- Cualquier álgebra de generación finita sobre $\mathbb{Q}$ es un cociente de un anillo de polinomios en un número finito de variables, que es siempre un conjunto numerable. Entonces $\mathbb{R}$ no puede ser de generación finita sobre $\mathbb{Q}$.

- Consideremos a $\mathbb{R}$ como un $\mathbb{Q}$-álgebra. La subálgebra generada por los elementos $\sqrt{2}$ y $\sqrt{3}$ debe contener a todos los elementos de la forma

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

  Pero este conjunto de elementos es ya una subálgebra y debe coincidir con $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. El lector puede demostrar que además de ser subálgebra es subextensión, encontrando el inverso de cada elemento no nulo o aplicar la el resultado 7.3 que probaremos próximamente.

- Sea $\varphi : A_1 \to A_2$ un morfismo epiyectivo. Si A_1 es de generación finita, entonces A_2 también. Basta tomar como generadores de A_2 las imagenes por φ de los generadores de A_1.

Si tenemos una extensión $k \to K$ y $S \subset K$ entonces el anillo de fracciones de $k[S]$ es un subcuerpo que contiene a S. Es la mínima extensión que contiene a S. Denotamos por $k(S)$ al anillo de fracciones de $k[S]$. El cuerpo $k(S)$ también se puede definir como la intersección de todos los cuerpos que contienen al conjunto $k \cup S$, pues todos estos cuerpos tienen estructura de k-álgebra por contener a k.

Definición 5.6 *Una extensión $k \to K$ es de* generación finita *(como cuerpo) si existe un conjunto finito $\{a_1, \ldots, a_n\}$ tal que $K = k(a_1, \ldots, a_n)$.*

Cuando hablamos de generación finita podemos referirnos al anillo generado o al cuerpo generado. Debemos tener cuidado y conocer a que tipo de generación finita nos referimos. En general ello quedará claro por el contexto. Además, en casi todos los casos de interés, resulta que $k[a_1, \ldots, a_n]$ es ya un cuerpo y coincide con $k(a_1, \cdots, a_n)$. Nuevamente el orden dado a los

elementos es irrelevante y se cumplen las igualdades

$$k(a_1)(a_2) = k(a_1, a_2) = k(a_2)(a_1)$$

y su generalización a subconjuntos.

Definición 5.7 *Si la extensión puede ser generada por un solo elemento, se denomina* extensión simple*. Cualquier elemento que genere dicha extensión, se llama* elemento primitivo *de la extensión.*

En general, cualquier extensión simple puede tener varios elementos primitivos. A veces las extensiones simples aparecen camufladas como extensiones de generación finita del tipo $K = k(\alpha_1, \ldots, \alpha_n)$, puesto que no es sencillo encontrar un elemento β que cumpla $K = k(\beta)$. Por ejemplo, comprobemos que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es simple. Llamemos $\alpha = \sqrt{2} + \sqrt{3}$. Un sencillo cálculo demuestra que $\alpha^3 - 9\alpha = 2\sqrt{2}$. Dividiendo entre dos, comprobamos que $\sqrt{2} \in \mathbb{Q}(\alpha)$ y lo mismo con el otro elemento. La extensión dada coincide con $\mathbb{Q}(\alpha)$, que es simple.

Aparte de este ejemplo, tenemos el teorema del elemento primitivo que afirma, bajo condiciones muy generales, que toda extensión finita (ver la definición 7.1) es simple.

Definición 5.8 *Sea $k \to K$ una extensión y $L_1 \subset K$ y $L_2 \subset K$ dos subextensiones. La mínima extensión que contiene a $L_1 \cup L_2$ se denomina* compuesto *de L_1 y L_2 y se denota L_1L_2.*

Con nuestra antigua notación, el compuesto de dos subextensiones se denotaría $k(L_1 \cup L_2)$. En la nueva notación está claro que el orden no influye en la construcción

$$L_1L_2 = L_2L_1$$

Observación. 7 *Sea $k \to K$ una extensión. Sea S el conjunto de todas las subextensiones de K. En este conjunto existe una relación de orden dada por la inclusión conjuntista. El supremo de dos elementos L_1 y L_2 es justamente el compuesto L_1L_2. El ínfimo es la intersección conjuntista.*

6. El grupo de Galois

La teoría de Galois estudia la relación entre las extensiones de un cuerpo y ciertos grupos asociados. Estos grupos están formados por k-morfismos

Definición 6.1 *Dada una extensión $k \to K$, el conjunto de los k-isomorfismos se llama* grupo de Galois *de la extensión. Lo denotaremos* $\mathrm{Gal}(K : k)$*, aunque esta notación no es totalmente estandard.*

Este grupo es de modo natural un subgrupo de $\mathrm{Aut}(K)$, pero la estructura de estos dos grupos puede diferir enormemente.

Ejemplos.

- Dada la extensión $\mathbb{R} \to \mathbb{C}$ todo morfismo de cuerpos $\varphi : \mathbb{C} \to \mathbb{C}$ debe cumplir $\varphi(i)^2 = -1$. Necesariamente $\varphi(i) = \pm i$. Si además es $\mathbb{R}$-morfismo se verifica $\varphi(a + bi) = a + b\varphi(i)$. En un caso tenemos la identidad y en otro la conjugación compleja. El grupo $\mathrm{Gal}(\mathbb{C} : \mathbb{R})$ tiene dos elementos y es isomorfo a $\mathbb{Z}_2$.

- Sea d un número complejo que no tenga raíz racional. La extensión $\mathbb{Q} \to \mathbb{Q}(\sqrt{d})$ tiene un grupo de Galois de orden 2.

- Si dos extensiones son isomorfas sus grupos de Galois también lo son. El recíproco no es cierto: $\mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ y $\mathbb{Q} \to \mathbb{Q}(\sqrt{3})$, tienen ambas grupo de Galois $\mathbb{Z}_2$, y sin embargo no son isomorfas.

- Sea K un cuerpo de característica nula. Todo automorfismo de K debe ser la identidad sobre el subcuerpo $\mathbb{Q}$. De este modo

$$\mathrm{Gal}(K : \mathbb{Q}) = \mathrm{Aut}(K)$$

  En general, dado un cuerpo K, denotemos por k_p su subcuerpo primo. Tenemos la igualdad

$$\mathrm{Gal}(K : k_p) = \mathrm{Aut}(K)$$

- Sea $k \to k(x)$. Existen k-morfismos φ que verifican $\varphi(x) = x^n$. Estos morfismos no son epiyectivos y no pertenecen al grupo de Galois.

- Consideremos la extensión $\mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2})$, que es un subcuerpo de $\mathbb{R}$. Un morfismo queda totalmente conocido si sabemos como actua sobre un conjunto generador. En nuestro caso el único generador es $\alpha = \sqrt[3]{2}$. Como $\varphi(\alpha)^3 = 2$, necesariamente $\varphi(\alpha)$ es una raíz cúbica de 2. Como las otras raices de 2 son complejas $\varphi(\alpha) = \alpha$ y el morfismo es la identidad.

- Analicemos en detalle como se calcula el grupo de Galois de la extensión $\mathbb{Q} \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Recordemos que los elementos del cuerpo se escriben de modo único en la forma

  $$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

  Sea φ un automorfismo. Como tal debe ser una aplicación $\mathbb{Q}$-lineal. Si llamamos $\alpha = \sqrt{2}$, se tiene que $\varphi(\alpha)^2 = 2$. Necesariamente $\varphi(\alpha)$ es una de las raices de 2, y se cumple $\varphi(\sqrt{2}) = \pm\sqrt{2}$. El mismo razonamiento es válido para el otro generador. Por lo tanto solamente pueden existir, como mucho, cuatro automorfismos distintos. En este caso los cuatro existen. El grupo de Galois tiene orden cuatro y es isomorfo (esto requiere un ligero cálculo) a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proposición 6.1 $\mathrm{Gal}(\mathbb{R} : \mathbb{Q}) = \{Id\}$.

Demostración. Todo elemento del grupo debe ser la identidad sobre $\mathbb{Q}$. Además un elemento φ de este grupo debe conservar el orden de $\mathbb{R}$.

$$\text{Si } r \geq s \text{ entonces } r - s = a^2$$

Aplicando el morfismo φ

$$\varphi(r) - \varphi(s) = \varphi(a)^2 \geq 0$$

La densidad de $\mathbb{Q}$ en $\mathbb{R}$ permite concluir (si existe $r \in \mathbb{R}$ tal que $\varphi(r) \neq r$ basta tomar un racional entre ambos para obtener una contradicción). $\square$

A partir de ahora emplearemos una notación que puede inducir a error. Por ello siempre denotaremos con la letra H a los subgrupos del grupo de Galois y con la letra L a las subextensiones. En la literatura la notación de estos conceptos no es estandard.

Proposición 6.2 *Dado un subgrupo $H \subset \mathrm{Gal}(K:k)$ el conjunto*

$$H' = \{a \in K \text{ tales que } \varphi(a) = a \text{ para todo } \varphi \in H\}$$

es una subextensión de K.

Demostración. De modo inmediato se comprueba que H' es un cuerpo. Además si $a \in k$ entonces $\varphi(a) = a$ para todo elemento de $\mathrm{Gal}(K:k)$ y en particular para todo elemento $\varphi \in H$. Tenemos que $k \subset H'$ y naturalmente $H' \subset K$. □

Definición 6.2 *La subextensión H' se llama* cuerpo fijo *de H.*

Proposición 6.3 *Sea $k \to K$ una extensión y L una subextensión. Entonces* $\mathrm{Gal}(K:L)$ *es un subgrupo de* $\mathrm{Gal}(K:k)$*. Denotaremos dicho subgrupo por L'.*

Demostración. Recordemos que con este cambio de notación tenemos

$$L' = \{\varphi \in \mathrm{Gal}(K:k) \text{ tales que } \varphi(x) = x \text{ para todo } x \in L\}$$

Si un morfismo deja estables todos los elementos de L, también deja estables todos los elementos de k. □

La siguiente proposición es prácticamente una tautología.

Proposición 6.4 *Sea $k \to K$ una extensión. Con la notación convenida se cumple:*

- $K' = \{\mathrm{Id}\}$ *y* $k' = \mathrm{Gal}(K:k)$.
- *Si $L_1 \subset L_2$ entonces $L_1' \subset L_2'$.*

- $\{\mathrm{Id}\}' = K$.
- *Si* $H_1 \subset H_2$ *entonces* $H_1' \supset H_2'$.

Observación. 8 *Esta proposición presenta una aparente falta de simetría y es "lógico" esperar que se cumpla también* $\mathrm{Gal}(K : k)' = k$. *Sin embargo esta propiedad es falsa. Por ejemplo, el grupo* $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ *solamente tiene un elemento y su cuerpo invariante asociado es* $\mathbb{Q}(\sqrt[3]{2})$ *y no* $\mathbb{Q}$.

La siguiente proposición no es tan inmediata, pero su demostración es también muy sencilla. Simplemente debemos tener claras las definiciones que hemos introducido.

Proposición 6.5 *Con las notaciones anteriores* $H \subset H''$ *y* $L \subset L''$.

La situación ideal se produce cuando en la anterior proposición en vez de la inclusión tuviesemos una igualdad. Pero ya hemos visto que esto no es siempre cierto. Posteriormente veremos que las llamadas extensiones de Galois verifican la igualdad para todo subgrupo y toda extensión.

Definición 6.3 *Un subgrupo* H *o una subextensión* L *es* cerrada *si* $H = H''$ *o* $L = L''$ *respectivamente.*

7. Álgebra Lineal

En toda k-álgebra A existe una estructura natural de espacio vectorial sobre k. Denotemos por $i : k \to A$ el morfismo que da la estructura de k-álgebra. Definimos el siguiente producto escalar

$$\begin{array}{ccc} k \times A & \longrightarrow & A \\ (\lambda, a) & \longrightarrow & i(\lambda) \cdot a \end{array}$$

Si $\lambda \in k$ y $a \in A$ el producto escalar λa es la multiplicación en el anillo de los elementos $i(\lambda)$ y a. Si k es un subanillo de A y el morfismo es la inyección canónica, la multiplicación escalar es simplemente la multiplicación del anillo. Las propiedades de la multiplicación por escalares derivan de las propiedades del anillo y del hecho de que i es morfismo.

Definición 7.1 *Una k-álgebra A es de* dimensión finita *si lo es como espacio vectorial sobre k. Su dimensión se denota $[A : k]$ y se llama* grado *de A sobre k.*

Es costumbre simplificar la notación y llamar álgebras finitas a las álgebras de dimensión finita.

Observación. 9 *Estamos cometiendo el abuso de notación de sobreentender el morfismo. Por ejemplo, en la extensión* $\mathrm{Id} : k(x) \to k(x)$ *el grado $[k(x) : k(x)]$ es uno. Pero si consideramos la extensión $\varphi : k(x) \to k(x)$ que cumple $\varphi(x) = x^2$, tenemos que el grado $[k(x) : k(x)]$ es dos. Si alguna vez pueden producirse este tipo de ambigüedades lo indicaremos explícitamente.*

Corolario 7.1 *Toda subálgebra y todo cociente de un álgebra de dimensión finita tienen dimensión finita. Si dos álgebras A_1 y A_2 son de dimensión finita entonces $[A_1 \oplus A_2 : k] = [A_1 : k] + [A_2 : k]$.*

Si un álgebra es de dimensión finita, también es de generación finita como álgebra puesto que cualquier base actua como un conjunto generador (como k-álgebra). El recíproco sin embargo no es cierto: $k[x]$ es de generación finita, pero no de dimensión finita.

Proposición 7.2 *Todo cuerpo finito de característica p tiene p^n elementos.*

Demostración. Si un cuerpo k tiene característica p, contiene al cuerpo $\mathbb{F}_p$. Entonces k es un espacio vectorial de dimensión finita sobre $\mathbb{F}_p$ y tiene p^n elementos, donde n es el grado de la extensión. □

Proposición 7.3 *Sea A una k-álgebra finita e íntegra. Entonces A es un cuerpo.*

Demostración. Sea $a \in A$ no nulo. Consideramos la aplicación lineal

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & A \\ & b & \longrightarrow & ab \end{array}$$

Como A es íntegra dicha aplicación es inyectiva y por estar en dimensión finita es epiyectiva y el elemento es invertible. $\square$

El anillo de polinomios es un álgebra íntegra que no es un cuerpo. La condición de finitud es imprescindible para la validez de la proposición.

Corolario 7.4 *Sea $S \subset K$. Si $k[S]$ es un álgebra de dimensión finita entonces $k[S] = k(S)$.*

Corolario 7.5 *Sea A un álgebra de dimensión finita. Todo ideal primo no nulo de A es maximal.*

Demostración. Sea I un ideal primo. El álgebra A/I es íntegra y de dimensión finita. Como A/I es un cuerpo, el ideal I es maximal. $\square$

Si tenemos una k-álgebra A de dimensión finita, tiene al menos un ideal maximal $\mathfrak{m}$. El cociente $A/\mathfrak{m}$ es un cuerpo (llamado muchas veces cuerpo residual) que contiene a k y por lo tanto es una extensión finita.

Proposición 7.6 *Sea A un álgebra de dimensión finita. El número de ideales maximales de A es menor o igual que su dimensión.*

Demostración. Sea $\mathfrak{m}_1, \ldots, \mathfrak{m}_j$ ideales maximales de A. Por el teorema de los restos chinos se tiene un isomorfismo

$$A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_j) = A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_j$$

El lado izquierdo de la fórmula tiene dimensión menor o igual que la dimensión de A. Cada uno de los sumandos de la derecha tiene al menos dimensión 1. Necesariamente $j \leq \dim(A)$. $\square$

Recordemos de Teoría de Anillos que un anillo es reducido si no contiene elementos nilpotentes. Además, el conjunto de todos los elementos nilpotentes (el radical del anillo) coincide con la intersección de todos los ideales primos. En el caso de las álgebras de dimensión finita, la intersección de sus ideales maximales es el radical del anillo.

Proposición 7.7 *Sea A un álgebra de dimensión finita y sin radical. Entonces A es isomorfa a una suma directa de extensiones finitas.*

Demostración. Sean $\mathfrak{m}_1, \ldots, \mathfrak{m}_j$ el conjunto de ideales maximales de A. Como el álgebra no tiene radical, la intersección de los ideales es 0. Aplicando el teorema de los restos chinos

$$A = A/(0) = A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_j) = A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_j$$

obteniendose el resultado. □

Todos estos resultados abstractos toman forma en los siguientes

Ejemplos.

- Sea $A = k[x]/(f)$, siendo f un polinomio irreducible. Entonces A es una extensión. La extensión es trivial si y solo f es de primer grado.

- Sea $f = g_1 \ldots g_j$ la descomposición en factores irreducibles de un polinomio. Supongamos que ningún factor tiene multiplicidad. Por el teorema de los restos chinos

  $$A/(f) = A/(g_1) \oplus \cdots \oplus A/(g_j)$$

  Ahora el álgebra $A/(f)$ es una suma directa de extensiones, y por lo tanto carece de radical. Si todas las extensiones son triviales, el polinomio descompone en factores lineales y tiene todas sus raices en el cuerpo k. En general, el número de extensiones triviales que aparecen en su descomposición es igual al número de raices que posee el polinomio en el cuerpo.

- Sea $f = g^n$, siendo g irreducible. Entonces el álgebra $A/(f)$ tiene elementos nilpotentes (la clase de g es uno de ellos). Sin embargo el estudio de las raices del polinomio f es equivalente al estudio de las raices de g, que si da lugar a un álgebra reducida.

- Finalmente, sea $f = g_1^{n_1} \dots g_j^{n_j}$ la descomposición en factores. El álgebra $A/(f)$ es reducida si y solo si $n_i = 1$ para todo i. Para el estudio de las raices f podemos considerar el polinomio $g = g_1 \dots g_j$.

En muchas ocasiones en vez de tratar con una sola extensión, debemos tratar con varias extensiones relacionadas entre si mediante la inclusión. Llamamos torre de cuerpos a la cadena $k \to K_1 \to K_2$. Es una notación abreviada para hablar de tres extensiones, que son $k \to K_1$, $k \to K_2$ y $K_1 \to K_2$.

Proposición 7.8 *Sea $k \to K_1 \to K_2$ una torre de cuerpos. La extensión $k \to K_2$ es finita si y solo si $k \to K_1$ y $K_1 \to K_2$ son finitas y en este caso se cumple*

$$[K_2 : k] = [K_2 : K_1][K_1 : k]$$

Demostración. Sea $n = [K_2 : K_1]$ y $m = [K_1 : k]$. De álgebra lineal sabemos que $K_2 \sim {K_1}^n$ y $K_1 \sim k^m$. Sustituyendo $K_2 \sim (k^m)^n \sim k^{mn}$. $\square$

La fórmula anterior es también válida aún en el caso de que alguno de los grados sea infinito.

Observación. 10 *Sea $\{x_i\}$ una base de K_2 como K_1-espacio vectorial y sea $\{y_j\}$ una base de K_1 como k-espacio. Entonces los productos $x_i y_j$ forman una base de la extensión $k \to K_2$.*

Ejemplos.

- El cuerpo $\mathbb{C}$ tiene grado 2 sobre $\mathbb{R}$. Una base es $\{1, i\}$.
- Todo espacio vectorial de dimensión finita sobre $\mathbb{Q}$ es numerable. Entonces $\mathbb{R}$ y $\mathbb{C}$ son extensiones de $\mathbb{Q}$ de grado infinito.
- Denotemos por $k(x)$ al cuerpo de fracciones racionales. Es una extensión de grado infinito, puesto que los polinomios son un subespacio de dimensión infinita. Sin embargo, recordemos que si es finitamente generada como cuerpo pues el conjunto $\{x\}$ genera dicho cuerpo.

- Sea f un polinomio de grado n. Entonces $k[x]/(f)$ es un álgebra de grado n. Veámoslo. Todo polinomio de grado mayor que n es equivalente a un polinomio de grado menor que n. Si g es un polinomio de grado mayor que n, aplicando la división euclídea $g = cf + r$ y los polinomios g y r son equivalentes. Sin embargo dos polinomios de grado menor que n nunca pueden ser equivalentes. Las imágenes de $1, x, \cdots, x^{n-1}$ forman una base.

- $[K : k] = 1$ si y solo si k y K son isomorfos. Si consideramos que k está contenido en la extensión se tiene la igualdad en vez del isomorfismo.

- Sea $k \to K$ una extensión de grado primo. Entonces no puede existir ninguna torre $k \to L \to K$ salvo si $L = K$ ó $L = k$.

- Sea $k \to K$ una extensión. Todo k-automorfismo $\varphi : K \to K$ es una aplicación k-lineal y tenemos que $\mathrm{Gal}(K : k) \subset \mathrm{Gl}(K)$. Podemos utilizar la maquinaria del álgebra lineal para estudiar los grupos de Galois. En particular dos extensiones isomorfas tienen el mismo grado. Sin embargo el recíproco no es cierto: $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$ son ambas extensiones de $\mathbb{Q}$ de grado 2 y sin embargo no son isomorfas (un cuerpo posee raices cuadradas de 2 y el otro no).

- Sea $k \to K$ una extensión finita. Todo k-morfismo $\varphi : K \to K$ es inyectivo y por estar en dimensión finita es epiyectvo.

8. Tipos de extensiones

En esta sección empezaremos a estudiar la estrecha relación existente entre el estudio de las raices de los polinomios sobre un cuerpo k y la estructura de las extensiones de dicho cuerpo.

Sea $k \to K$ una extensión. Dado un elemento $\alpha \in K$, se induce un morfismo de álgebras $\varphi_\alpha : k[x] \to K$. Dicho morfismo es el único que cumple la condición $\varphi_\alpha(x) = \alpha$. Recordemos que la imagen de dicho morfismo coincide con $k[\alpha]$, que es el álgebra generada por el elemento α.

Definición 8.1 *Dada una extensión $k \to K$, un elemento $\alpha \in K$ es* transcendente *(sobre k) si el morfismo φ_α es inyectivo. Si el morfismo no es inyectivo decimos que α es un elemento* algebraico *(sobre k).*

En general decimos que $\alpha \in K$ es algebraico o transcendente sobre k, sobreentendiendo el morfismo que define la extensión.

Si φ_α es inyectivo, el álgebra $k[\alpha]$ es isomorfa al anillo de polinomios. En este caso la extensión $k(\alpha)$ es isomorfa al cuerpo de fracciones racionales $k(x)$. Como vemos este resultado es independiente del elemento transcendente que tomemos. En este sentido todos los elementos transcendentes son equivalentes.

Proposición 8.1 *Todas las extensiones simples transcendentes de k son isomorfas a $k(x)$.*

Si α es algebraico, el núcleo de φ_α es un ideal primo del anillo de polinomios, puesto que la imagen del morfismo es íntegra. Como en $k[x]$ todos los ideales son principales, dicho ideal está generado por un polinomio, que debido a la primalidad del ideal, es irreducible. Tomaremos siempre como generador el único polinomio que tiene como coeficiente de mayor grado la unidad. Denotaremos dicho polinomio por m_α.

Definición 8.2 *El polinomio m_α es el* polinomio mínimo *de α.*

El polinomio m_α pertenece al anillo $k[x]$, pero gracias al morfismo $k \to K$ también se puede considerar como un polinomio de $K[x]$. En este sentido, tenemos que α es una raíz del polinomio m_α y además no existe ningún polinomio en k de grado menor que tenga a α como raíz. Como m_α anula al elemento α, también se suele llamar polinomio anulador de α al polinomio mínimo. Recíprocamente, si existe un polinomio f con valores en k que tiene al elemento α como raíz, el elemento es algebraico y su polinomio mínimo es un divisor de f.

Proposición 8.2 *El polinomio mínimo de α es el único polinomio irreducible y mónico que tiene como raíz al elemento dado.*

Normalmente y para no recargar la notación supondremos que $k \subset K$ lo que implica que $k[x] \subset K[x]$.

Ejemplos.

- Sea $k \subset K$ una extensión. Todo elemento $\alpha \in k$ es algebraico sobre k y su polinomio mínimo es $x - \alpha$. Un elemento α tiene un polinomio mínimo de primer grado si y solo si α está en el cuerpo base.

- El número i es algebraico sobre $\mathbb{R}$ y su polinomio mínimo es $x^2 + 1$. Este elemento también es algebraico sobre $\mathbb{Q}$.

- $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$ y su polinomio mínimo es $x^2 - 2$.

- La raíz n-ésima de la unidad, $\xi_n = e^{\frac{2\pi i}{n}}$, es algebraica. Un polinomio que tiene como raíz a ξ_n es $x^n - 1$. Sin embargo este no es polinomio mínimo por ser reducible

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

- Los números e y π son transcendentes sobre $\mathbb{Q}$. La demostración de estos resultados (debida a Hermite y Lindemann a finales del siglo 19) no es elemental, pero la admitiremos.

- Consideremos la extensión $k \to k(x)$. El elemento x es transcendente sobre k. Si x es anulado por algún polinomio, dicho polinomio debe ser igual a cero y el morfismo es inyectivo.

- Si tenemos una torre de cuerpos $k \to L \to K$, dado un elemento $\alpha \in L$ podemos considerar dos polinomios mínimos, uno que pertenece a $k[x]$ y otro que pertenece a $L[x]$. Los denotaremos por $m_{\alpha,k}$ y por $m_{\alpha,L}$. Entonces el polinomio mínimo sobre L divide al polinomio mínimo sobre k. El polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es $x^2 - 2$ y sin embargo sobre $\mathbb{R}$ es $x - \sqrt{2}$.

En general, dado un elemento $\alpha \in K$, salvo en los casos sencillos, no es fácil encontrar el polinomio mínimo, o al menos un polinomio que anule a α. Ilustraremos como se puede conseguir en casos ligeramente más complicados.

Ejemplos.

- Sea $\alpha = \sqrt{2} + \sqrt{3}$. Dejamos una raiz "sola" en un miembro y elevamos al cuadrado

$$(\alpha - \sqrt{2})^2 = (\sqrt{3})^2$$

  De esta forma "eliminamos" una raiz. Repitiendo el argumento y pasando todo a un miembro deducimos que α satisface la ecuación polinómica

$$\alpha^4 - 10\alpha^2 + 1 = 0$$

  Algún factor de este polinomio (o él mismo si es irreducible), es el polinomio mínimo de α.

- Sea K una extensión de dimensión finita. Dado $\alpha \in K$ consideramos el endomorfismo

$$\begin{array}{rccc} h_\alpha : & K & \to & K \\ & a & \to & \alpha a \end{array}$$

  El polinomio característico de este endormorfismo, que se calcula desarrollando un determinante, tiene a α como raiz. Una ligera reflexión nos dice que el polinomio mínimo de este endomorfismo (que es un factor del polinomio característico), también anula a α. Es más, este polinomio mínimo (el del endomorfismo) coincide con el polinomio mínimo del elemento α. Así ambas notaciones no dan lugar a confusión.

Tomemos un elemento α algebraico. El teorema de factorización canónica nos da un isomorfismo de anillos $\varphi_\alpha : k[x]/(m_\alpha) \to k[\alpha]$. Como el primero es un cuerpo, necesariamente el segundo también es un cuerpo. Otra manera de ver que $k[\alpha]$ es un cuerpo es tener en cuenta que es un álgebra íntegra de dimensión finita.

Si α es un elemento algebraico, se tiene un isomorfismo entre los cuerpos $k[x]/(m_\alpha)$ y $k(\alpha)$. La extensión $k \to k(\alpha)$ es finita si y solo si el elemento α es algebraico sobre k. Resumiendo, se tiene la

Proposición 8.3 *Dada una extensión $k \to K$ son equivalentes:*

1) El elemento α es algebraico sobre k.

2) El grado $[k(\alpha) : k]$ es finito.

3) El morfimo $\varphi_\alpha : k[x] \to K$ no es inyectivo.

4) Se tiene la igualdad $k[\alpha] = k(\alpha)$.

Si se cumple alguna de la hipótesis de la proposición anterior, el grado del polinomio mínimo de α y el grado de la extensión $k \to k(\alpha)$ coinciden.

Definición 8.3 *Llamamos* grado *del elemento α al grado de su polinomio mínimo.*

Corolario 8.4 *Todo polinomio irreducible es el polinomio mínimo de algún elemento.*

Demostración. Dado un polinomio irreducible f, tenemos la extensión $k \to k[x]/(f)$. Si $\alpha = \pi(x)$, el polinomio mínimo de α es f. □

Corolario 8.5 *Toda extensión finita y simple es isomorfa a $k[x]/(f)$.*

El siguiente resultado será muy importante en el estudio de los campos de descomposición, que es tema del capítulo siguiente.

Corolario 8.6 *Sea $k \to K$ una extensión, α y β dos elementos algebraicos con el mismo polinomio mínimo. Existe un k-isomorfismo $\varphi : k(\alpha) \to k(\beta)$ que verifica $\varphi(\alpha) = \beta$. El recíproco también es cierto.*

Demostración. $\Rightarrow$) Si f es el polinomio mínimo de ambos elementos, entonces ambos cuerpos son isomorfos con $k[x]/(f)$. Un isomorfismo cumple $\phi(x) = \alpha$ y el otro cumple $\phi'(x) = \beta$. Tomamos $\varphi = \phi' \cdot \phi^{-1}$.

$\Leftarrow$) Sea φ el isomorfismo que transforma α en β y

$$m_\alpha = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

el polinomio mínimo. Si aplicamos φ a la ecuación

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

tenemos que m_α también anula a β. Por ser irreducible $m_\alpha = m_\beta$. $\square$

Definición 8.4 *Sea $k \to K$ una extensión. Dos elementos α y β de K son* conjugados *si tienen el mismo polinomio anulador.*

La relación de conjugación es de equivalencia. Si el grado del polinomio m_α es n, el polinomio puede tener como mucho n raices. El número de elementos de la clase de α nunca puede superar al grado de α.

Ya hemos visto que si α y β son conjugados entonces $k(\alpha)$ y $k(\beta)$ son extensiones isomorfas entre sí, y además isomorfas con $k[x]/(f)$. Si tenemos otra extensión $k \to K'$ y α' es solución del polinomio m_α, tenemos que también son isomorfas las extensiones $k(\alpha)$ y $k(\alpha')$.

Proposición 8.7 *Dado un polinomio irreducible f la subextensiones generadas por una cualquiera de sus raices son isomorfas entre sí.*

De este modo la subextensión generada por una raíz de f es única, aunque siempre entendiendo que esta unicidad es salvo isomorfismos. Por ello es muy habitual hablar de la extensión $k \to k(\alpha)$ siendo α la raiz de un polinomio irreducible f, sin necesidad de suponer la existencia de una extensión K que contenga a α.

Ejemplos.

- Dada la extensión $\mathbb{R} \to \mathbb{C}$, los números i y $-i$ son conjugados puesto que su polinomio anulador es $x^2 + 1$. En general $a + bi$ y $a - bi$ son conjugados y el lenguaje que empleamos se adapta al usual.

- Sea $k \subset K$ y $\varphi : K \to K$ un automorfismo que sobre k es la identidad. Si α tiene como polinomio mínimo f, entonces también es el polinomio mínimo de $\varphi(\alpha)$. Las distintas raices de un polinomio irreducible están relacionadas por automorfismos. Esta idea, expresada de momento de modo vago, es fundamental en la Teoría de Galois.

9. Extensiones algebraicas

Definición 9.1 *Una extensión $k \to K$ es* algebraica *si todo elemento de K es algebraico sobre k. En caso contrario la extensión se llama* transcendente.

Proposición 9.1 *Toda extensión finita es algebraica.*

Demostración. Daremos dos demostraciones de este resultado.

El morfismo φ_α no puede ser inyectivo pues su dominio es un espacio vectorial de dimensión infinita y la imagen es de dimensión finita.

Sea n el grado de la extensión. Dado $\alpha \in K$, el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ no pueden ser linealmente independiente. Existen constantes que verifican la ecuación

$$c_0 1 + c_1\alpha + c_2\alpha^2 + \ldots, c_n\alpha^n = 0$$

y existe un polinomio que anula a α, que es entonces algebraico. □

El inverso de esta proposición es falso. Veremos posteriormente que existen extensiones algebraicas que no son de grado finito.

Corolario 9.2 *Si en k existen polinomios irreducibles de grado mayor que uno, entonces k tiene extensiones algebraicas.*

Demostración. Si f es irreducible de grado n, entonces $k[x]/(f)$ es una extensión de grado n y es algebraica. □

Si todos los polinomios irreducibles de k son de grado 1, el polinomio mínimo de cualquier elemento algebraico es de la forma $x - \alpha$ con $\alpha \in k$ y todos los elementos algebraicos son a la vez elementos de k. Esto nos dice que solo existen extensiones algebraicas del tipo $k \to k$. Todas las extensiones algebraicas de k son isomorfas a k.

Proposición 9.3 *Una extensión es finita si y solo si es algebraica y de generación finita.*

Demostración. Claramente si la extensión tiene grado finito es de generación finita y ya hemos visto que es algebraica.

Supongamos que $K = k(\alpha_1, \ldots, \alpha_n)$. Consideremos la siguiente torre de campos

$$k \to k(\alpha_1) \to k(\alpha_1, \alpha_2) \to \cdots \to k(\alpha_1, \ldots, \alpha_n) = K$$

Como α_i es algebraico sobre k, también es algebraico sobre $k(\alpha_1, \ldots, \alpha_{i-1})$ y cada uno de los eslabones es una extensión de grado finito. La proposición 7.8 permite concluir que $k \to K$ es finita

Proposición 9.4 *Si $\alpha, \beta \in K$ son algebraicos sobre k, su suma, su producto, sus inversos y sus opuestos son también algebraicos.*

Demostración. Si α y β son algebraicos, la extensión $k \to k(\alpha, \beta)$ es finita y todos los elementos de $k(\alpha, \beta)$ son algebraicos. En particular $\alpha + \beta$, $\alpha\beta$, $-\alpha$ y α^{-1} son elementos de dicha extensión. □

Corolario 9.5 *Toda subextensión generada por un subconjunto, posiblemente infinito, de elementos algebraicos, es algebraica.*

Demostración. Sea $k \to K$ la extensión y S un conjunto de elementos algebraicos sobre k, de tal modo que $k(S) = K$. Los elementos de $k(S)$ se forman con un número finito de operaciones y un número finito de elementos de S. Dado $\beta \in k(S)$, existen elementos $\alpha_1, \ldots, \alpha_n$ tales que $\beta \in k(\alpha_1, \ldots, \alpha_n)$. Como este último cuerpo es de grado finito, todos sus elementos son algebraicos y en particular β es algebraico. □

En realidad no es dificil observar que $k(S) = k[S]$ y los elementos de este último álgebra son polinomios en los elementos de S.

Los elementos algebraicos son estables por suma, producto y toma de inversos. Es natural ver que tienen estructura de cuerpo.

Corolario 9.6 *Sea $k \to K$ una extensión totalmente arbitraria. Los elementos de K algebraicos sobre k forman una extensión algebraica de k.*

Demostración. Denotamos por Al_K dicho conjunto, que viene definido como

$$\mathrm{Al}_K = \{\alpha \in K \text{ tales que } \alpha \text{ es algebraico sobre } k\}$$

La estructura de cuerpo deriva de la proposición anterior y por definición todos los elementos del cuerpo Al_K son algebraicos. □

Definición 9.2 *El cuerpo* Al_K *se llama* cierre algebraico *de* k *en* K.

Una extensión $k \to K$ es algebraica si su cierre algebraico coincide con K. El cierre algebraico es siempre una extensión algebraica.

Ejemplos.

- La extensión $\mathbb{R} \to \mathbb{C}$ es algebraica y el cierre algebraico de $\mathbb{R}$ en $\mathbb{C}$ coincide con $\mathbb{C}$.
- Sea $k \to K$ una extensión arbitraria. Cualquier cuerpo $L \subset K$ que sea algebraico sobre k está contenido en Al_K. Podemos pensar que el cierre algebraico de k en K es la "mayor" de las extensiones algebraicas contenidas en K.
- La extensión $\mathbb{Q} \to \mathbb{C}$ no es algebraica, pues existen elementos transcendentes. El cierre algebraico de $\mathbb{Q}$ en $\mathbb{C}$ lo denotamos por $\overline{\mathbb{Q}}$. Veamos que dicha extensión no es finita. Por el criterio de irreducibilidad de Eisentein, los polinomios del tipo $x^n - 2$ son todos irreducibles sobre $\mathbb{Q}$. Si α es un elemento de $\mathbb{C}$ que cumple $\alpha^n - 2 = 0$ entonces es algebraico. El subcuerpo $\mathbb{Q}(\alpha) \subset \overline{\mathbb{Q}}$ tiene dimensión n y la extensión $\mathbb{Q} \to \overline{\mathbb{Q}}$ no puede ser finita.

Corolario 9.7 *Sea* $k \to K$ *una extensión algebraica. Cualquier subálgebra* A *de* K *es un cuerpo.*

Demostración. Sea $\alpha \in A$. El algebra que genera $k[\alpha]$ está contenida en A. Pero como α es algebraico, tenemos que $k[\alpha] = k(\alpha)$. De esta forma $k(\alpha) \subset A$ es un cuerpo y elemento α^{-1} pertenece a $k(\alpha)$ y por ende a A. □

Proposición 9.8 *Sea* $k \to K_1 \to K_2$ *una torre de cuerpos de tal manera que* $k \to K_1$ *y* $K_1 \to K_2$ *son algebraicas. Entonces* $k \to K_2$ *es algebraica.*

Demostración. Sea $\alpha \in K_2$. Como α es algebraico sobre K_1, existe un polinomio en K_1 que anula al elemento α. Denotemos dicho polinomio por $c_0 + c_1 x + \cdots + c_n x^n$. Naturalmente α es algebraico sobre el subcuerpo $k(c_0, \ldots, c_n)$ pues existe un polinomio (el que hemos escrito) con coeficientes en dicho cuerpo que anula a α. Los elementos c_i pertenecen a K_1 por lo tanto son algebraicos sobre k. Consideremos la torre de cuerpos

$$k \to k(c_0, \ldots, c_n) \to k(c_0, \ldots, c_n, \alpha) = k(c_0, \ldots, c_n)(\alpha)$$

Los eslabones son finitos y la extensión $k \to k(c_0, \ldots, c_n, \alpha)$ es finita. En particular el elemento α es algebraico sobre k. $\square$

Esta última propiedad se llama transitividad de la propiedad de ser algebraica.

10. Cuerpos algebraicamente cerrados

Es conocido que una de las mayores ventajas del cuerpo $\mathbb{C}$ sobre el cuerpo $\mathbb{R}$ es que todo polinomio sobre $\mathbb{C}$ tiene al menos una raíz, cosa que no ocurre en los reales. Generalicemos este concepto a cuerpos arbitrarios.

Definición 10.1 *Un cuerpo k es* algebraicamente cerrado *si todo polinomio no constante en k tiene una raíz.*

Si todo polinomio tiene una raíz, resulta que todo polinomio de grado n tiene exactamente n raices, alguna de las cuales puede estar repetida. Los únicos polinomios irreducibles sobre un cuerpo algebraicamente cerrado son los de grado uno. Pero entonces el cuerpo no puede tener extensiones algebraicas.

Proposición 10.1 *Dado un cuerpo k son equivalentes:*

1) El cuerpo es algebraicamente cerrado.

2) Todo polinomio de grado mayor que uno en k tiene una raíz.

3) Todo polinomio tiene en k tantas raices como su grado.

4) Los polinomios irreducibles son de grado uno.

5) Si $k \to K$ es una extensión algebraica, entonces K es isomorfo a k.

Dado un cuerpo k nos preguntamos por la existencia de una extensión K algebraicamente cerrada. Veremos que siempre existen extensiones de este tipo. Sin embargo dichas extensiones no tienen necesidad de ser isomorfas. Sin embargo, si consideramos extensiones algebraicas tenemos la existencia y la unicidad.

Definición 10.2 *Dado un cuerpo k, llamamos* cierre algebraico *de k a toda extensión K que cumpla las condiciones:*

- *K es algebraicamente cerrado.*
- *La extensión $k \to K$ es algebraica.*

El cierre algebraico de un cuerpo algebraicamente cerrado es él mismo. La extensión $\mathbb{R} \to \mathbb{C}$ proporciona un cierre algebraico de $\mathbb{R}$. Construyamos ahora un cierre algebraico de los racionales.

Proposición 10.2 *Sea $k \to K$ una extensión, de tal modo que K es algebraicamente cerrado. Entonces Al_K es un cierre algebraico de k.*

Demostración. Sea f un polinomio con coeficientes en Al_K. Sea α una raíz del polinomio en el cuerpo K. El cuerpo $\mathrm{Al}_K(\alpha)$ es una extensión algebraica de Al_K y por la transitividad de la condición de algebraico, también es algebraica sobre k. El elemento α es algebraico sobre k y pertenece a Al_K. Todo polinomio de Al_K tiene una raíz en el cuerpo y es algebraicamente cerrado. Naturalmente también es una extensión algebraica. □

Corolario 10.3 *El cuerpo $\overline{\mathbb{Q}}$ es un cierre algebraico de $\mathbb{Q}$.*

Vemos que para construir un cierre algebraico basta encontrar una extensión algebraicamente cerrada. Si la extensión no es algebraica, consideramos el cierre algebraico y el nuevo cuerpo cumple los dos requisitos exigidos.

La idea que vamos a seguir para construir un cuerpo algebraicamente cerrado que contenga a k es la siguiente. Es relativamente sencillo, utilizando el lema de Zorn, construir un cuerpo k_1 que contenga a k y a todas las raices de los polinomios de $k[x]$. Sin embargo este nuevo cuerpo puede tener polinomios irreducibles de grado mayor que uno. Por el mismo procedimiento podemos construir un cuerpo k_2 que contenga todas las soluciones de los polinomios de k_1. Veremos que el conjunto (llamemos $k_0 = k$)

$$K = \bigcup_{n=0}^{\infty} k_n$$

puede ser dotado de una estrucura de cuerpo y que es un cierre algebraico del cuerpo base k (y también de todos los cuerpos intermedios que nos han ido apareciendo).

Lema 10.4 (Artin) *Sea S una colección, posiblemente infinita, de polinomios con coeficientes en k. Existe una extensión K que contiene, al menos, una raiz de cada polinomio de S.*

Demostración. Para cada $f \in S$ construyamos una variable x_f. Ahora consideramos el anillo de polinomios $A = k[x_f]$ con $f \in S$, que tiene tantas indeterminadas como elementos tiene S. Recordemos que cualquier elemento de dicho anillo es una combinación finita de monomios en las variables dadas.

Sea $I \subset A$ el ideal generado por los elementos $f(x_f)$ con $f \in S$. En el anillo cociente A/I se cumple de modo trivial que $f(x_f) = 0$, luego todo polinomio de S tiene una solución. Sin embargo se presentan dos posibles problemas:

1. El anillo A/I puede ser trivial y entonces no puede contener a k.

2. El anillo A/I puede no ser un cuerpo.

Para solucionar el primer problema basta ver que I no coincide con A. Si ocurriese esto, una combinación finita de elementos de I sería igual a la unidad

$$1 = a_1 f_1 + \cdots + a_n f_n \text{ con } f_i \in I$$

Si esta relación es cierta en un anillo de polinomios sobre k, debe seguir siendo cierta sobre un anillo de polinomios sobre L, siendo $k \subset L$. Por el teorema de Kronecker podemos encontrar L de tal forma que contenga a todas las raices de $f_1, \ldots, f_n$. Pero entonces la relación anterior no es posible que se de en dicho cuerpo, y por tanto no puede darse tampoco en k.

En general I no es un ideal maximal, pero siempre podemos tomar un ideal maximal $\mathfrak{m}$ que contenga a I. El anillo $K = A/\mathfrak{m}$ es ya un cuerpo. Dicho cuerpo contiene de modo natural a k. Además todo polinomio de S tiene en K al menos una raiz. Hemos solucionado ambos problemas. □

Teorema 10.5 *Todo cuerpo tiene un cierre algebraico.*

Demostración. Sea $S = k[x]$. Denotemos por k_1 al cuerpo obtenido aplicando el lema de Artin. En k_1 todo polinomio de $k[x]$ tiene una raiz. Llamemos ahora $S = k_1[x]$ y aplicamos el lema de Artin, obteniendo un cuerpo, que denominamos k_2 y procedemos del mismo modo para todo natural. Obtenemos una colección de cuerpos k_i, cada uno encajado en el siguiente. Llamemos K a la unión de todos esos cuerpos. Para definir las operaciones en K, por ejemplo $\alpha + \beta$ tenemos en cuenta que tanto α como β deben pertenecer a algún k_i. La operación en K es la misma que en k_i. Evidentemente esto es independiente del i tomado, siempre y cuando contenga a los dos elementos. Es claro que con estas operaciones K es un cuerpo, que es una extensión de k. Solo falta ver que es algebraicamente cerrado.

Tomemos un polinomio $f \in K[x]$. Como tiene un número finito de coeficientes, podemos suponer que dicho polinomio tiene todos sus coeficientes en un cierto k_i. Pero entonces dicho polinomio tiene una solución en k_{i+1} y por lo tanto tiene una solución en K. □

Observación. 11 *Aunque existen otras demostraciones de la existencia de cierres algebraicos, en todas ellas, en algún momento, se tiene que apelar al Lema de Zorn o cualquiera de sus formas equivalentes.*

11. Cuerpo de descomposición

Consideremos el cuerpo $\mathbb{Q}$ de los racionales y el polinomio $x^2 + 1$. Si intentamos hallar las raices de este polinomio dentro del cuerpo $\mathbb{Q}$, observamos que carece de ellas. Si ahora consideramos el mismo polinomio pero sobre el cuerpo $\mathbb{C}$ (entendido como extensión de $\mathbb{Q}$) este polinomio si que posee dos raices, que son i y $-i$. El cuerpo $\mathbb{C}$ soluciona todos los problemas de todos los polinomios. Pero para este caso particular no es necesario considerar todos los números complejos. Existe un cuerpo intermedio entre $\mathbb{Q}$ y $\mathbb{C}$ donde el polinomio ya tiene todas las raices. Ese cuerpo no es otro que $\mathbb{Q}(i)$. Además, este cuerpo es "mínimo" en el siguiente sentido: toda extensión $\mathbb{Q} \to K \subset \mathbb{C}$ donde el polinomio tenga sus raices debe cumplir que $\mathbb{Q}(i) \subset K$. Pretendemos generalizar este tipo de resultados a cualquier cuerpo y a cualquier polinomio.

Sea f un polinomio sobre un cuerpo k. Decimos que un elemento $\alpha \in k$ es una raíz del polinomio si $f(\alpha) = 0$. El número de raices de un polinomio nunca supera al grado del polinomio. Si aplicamos la división euclídea obtenemos

$$f = c(x - \alpha) + r$$

donde el resto es una constante. Sustituyendo α en dicha expresión, necesariamente $r = 0$ y concluimos que α es raíz de f si y solo si el polinomio es divisible por $(x - \alpha)$.

Proposición 11.1 *Un polinomio f sobre un cuerpo k descompone como producto de factores lineales si y solo si todas sus raices pertenecen a k.*

Si f descompone en factores lineales tenemos una expresión del tipo

$$f = a(x - \alpha_1) \cdots (x - \alpha_n)$$

donde α_i son las raices (que son únicas) y su número, contando multiplicidades, coincide con el grado del polinomio.

Observación. 12 *Las raices de f y de af son las mismas. Para simplificar la notación a veces supondremos que el polinomio es unitario y que todos sus factores irreducibles son también unitarios. Cuando digamos que un polinomio factoriza o descompone, supondremos que lo hace en factores lineales.*

En el caso de que el polinomio no tenga todas las raices en el cuerpo, cuando descomponemos el polinomio como producto de irreducibles, debe existir algún componente que tenga grado mayor que 1. Nos concentramos ahora en los polinomios irreducibles que no sean lineales.

Sea f un polinomio irreducible sobre k que no tenga ninguna raíz en el cuerpo. Si K es una extensión donde el polinomio tiene una raíz α, hemos visto que necesariamente $k(\alpha)$ es isomorfo con $k[x]/(f)$. Si K' es otra extensión y β es una raíz en K' del mismo polinomio, existe un isomorfismo de álgebras $\varphi : k(\alpha) \to k(\beta)$ que cumple $\varphi(\alpha) = \beta$. Esto prueba la unicidad, salvo isomorfismos, de las extensiones generadas por raices de f. La existencia de dichas extensiones se prueba en la

Proposición 11.2 *Sea f un polinomio irreducible sobre un cuerpo k. Existe una extensión finita $k \to K$ donde el polinomio tiene una raíz.*

Demostración. Como f es irreducible, el ideal que genera es maximal. Denotamos por K al anillo cociente $k[x]/(f)$. Sabemos que la proyección canónica induce una extensión $\pi : k \to K$. Si denotamos por α a la imagen por π del elemento x se obtiene

$$f(\alpha) = f(\pi(x)) = \pi(f(x)) = 0$$

pues el polinomio f pertenece al núcleo de la proyección. La extensión es finita y su grado coincide con el grado del polinomio. □

Pasamos ahora al caso general de los polinomios no necesariamente irreducibles.

Corolario 11.3 (Teorema de Kronecker) *Sea f un polinomio arbitrario sobre un cuerpo k. Existe una extensión finita donde f tiene una raíz.*

Demostración. Sea n al grado del polinomio. Expresamos f como producto de polinomios irreducibles. Cada uno de los factores irreducibles tiene siempre grado menor o igual que n. Si el polinomio tiene algún factor lineal, ya tiene una raíz. Si carece de factores lineales tomamos el primer factor irreducible de su descomposición. La proposición anterior muestra que existe una extensión de grado menor o igual a n donde el factor tiene una raíz. De este modo el polinomio f tiene también una raíz. □

Si somos capaces de hallar una raíz de un polinomio, repitiendo el argumento se pueden hallar todas las raices.

Corolario 11.4 (Kronecker) *Dado un polinomio, existe una extensión finita donde el polinomio descompone.*

Demostración. Sea f el polinomio de grado n. Somos capaces de encontrar una raíz α del polinomio en una extensión $k \to K_1$ del cuerpo. En el cuerpo K_1 se cumple

$$f = (x - \alpha) f_1$$

Ahora podemos encontrar una extensión de K_1 (y por tanto de k) donde f_1 tenga una raíz e inductivamente concluimos. Aplicando la ley de la torre de cuerpos, la extensión es finita. Además su grado es siempre menor o igual que $n!$. □

Corolario 11.5 (Kronecker) *Dado un conjunto finito de polinomios, existe una extensión finita donde el polinomio descompone.*

Demostración. Basta considerar el polinomio producto. □

Ahora que ya sabemos que para todo polinomio existe al menos una extensión donde tiene todas sus raices, pretendemos encontrar el cuerpo "más pequeño" donde esto ocurra.

Definición 11.1 *Sea f un polinomio sobre un cuerpo k. Llamamos* cuerpo de descomposición *de f a toda extensión $k \to K$ que verifique:*

- *El polinomio f descompone en K.*
- *El polinomio f no descompone en ningún subcuerpo $L \subset K$.*

La existencia de cuerpos de descomposición queda garantizada por la

Proposición 11.6 *Todo polinomio tiene un cuerpo de descomposión.*

Demostración. Utilizando los resultados anteriores, podemos encontrar una extensión K donde el polinomio tiene todas sus raices. Denotemos por $\alpha_1, \ldots, \alpha_n$ las raices del polinomio, alguna de las cuales puede estar repetida. El cuerpo $k(\alpha_1, \ldots, \alpha_n)$ es un cuerpo de descomposión del polinomio, puesto que claramente contiene a todas las raices. Además ningún subcuerpo puede contener a todas las raices pues si esto ocurriera las raices de f en K no serían únicas. □

Si K es un cuerpo de descomposición y $\alpha_1, \ldots, \alpha_n$ son las raices del polinomio en K, necesariamente se cumple

$$K = k(\alpha_1, \ldots, \alpha_n)$$

Por ello se suele decir que un cuerpo de descomposición de f es el generado por sus raices. Como las raices de polinomios son de manera evidente elementos algebraicos se cumple también

$$K = k[\alpha_1, \ldots, \alpha_n]$$

Ejemplos.

- Sea x^2+1 un polimomio sobre $\mathbb{Q}$. Un cuerpo de descomposición es $\mathbb{Q}(i)$.
- Sea $ax^2 + bx + c$ un polinomio racional. El cuerpo $\mathbb{Q}(\sqrt{b^2 - 4ac})$ es un cuerpo de descomposción. Si da la casualidad de que $\sqrt{b^2 - 4ac}$ es un número racional, entonces el cuerpo de descomposición es simplemente $\mathbb{Q}$.

- Dos polinomios distintos pueden tener el mismo cuerpo de descomposición. Como ejemplo valen los polinomios $x^2 + 5$ y $x^2 + 5x + 5$. En ambos casos el cuerpo $\mathbb{Q}(\sqrt{5})$ es un cuerpo de descomposición.

- Veamos el cuerpo de descomposición de $x^4 - 2$ sobre $\mathbb{Q}$. Las soluciones complejas de este polinomio son las raices cuartas de 2:

$$\alpha_1 = \sqrt[4]{2} \quad \alpha_2 = (\sqrt[4]{2})i \quad \alpha_3 = -\sqrt[4]{2} \quad \alpha_4 = -(\sqrt[4]{2})i$$

  El cuerpo de descomposición es $\mathbb{Q}(\sqrt[4]{2}, i)$. Si construimos la torre

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

  el primer eslabón tiene dimensión 4 y el segundo 2 puesto que i no está contenido en $\mathbb{Q}(\sqrt[4]{2})$ y tiene como polinomio mínimo $x^2 + 1$. Como conclusión $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$.

- El conjunto de soluciones del polinomio entero $x^n - 1 \in \mathbb{Q}[x]$ son las raices n-ésimas de la unidad. En el plano complejo forman los vértices de un polígono regular de n lados. El conjunto de raices n-ésimas es un grupo cíclico y cualquier generador de dicho grupo se llama raíz primitiva de la unidad. Sea ξ_n una raíz primitiva, entonces todas las demás raices n-ésimas se obtienen como potencias de ella y pertenecen a $\mathbb{Q}(\xi)$, que es un cuerpo de descomposición del polinomio $x^n - 1$. Los cuerpos que se obtienen añadiendo una raíz primitiva de la unidad se llama cuerpos ciclótomicos.

Observación. 13 *El enfoque que hemos adoptado para presentar los cuerpos de descomposición de un polinomio es totalmente constructivo. Otros autores adoptan un enfoque distinto, que tiene sus ventajas. Dado un polinomio $f \in k[x]$, tiene todas sus soluciones $\alpha_1, \ldots, \alpha_n$ en la clausura algebraica K. El cuerpo de descomposición es entonces $k(\alpha_1, \ldots, \alpha_n)$. La existencia (y unicidad) del cuerpo de descomposición es entonces trivial. No es difícil, en este enfoque, definir el cuerpo de descomposición de una familia infinita de polinomios.*

12. Unicidad del cuerpo de descomposición

Una vez vista la existencia del cuerpo de descomposición sería deseable poder demostrar que, en esencia, los cuerpos de descomposición son únicos. La unicidad se obtiene salvo isomorfismo y son precisamente esos isomorfismos los que interesan en la teoría de Galois.

La ideal de la demostración es sencilla. Supongamos que K y K' son dos cuerpos de descomposición de un polinomio. Entonces $K = k(\alpha_1, \ldots, \alpha_n)$ y $K' = k(\beta_1, \ldots, \beta_n)$ donde las letras griegas designan las correspondientes raices. Tomamos un factor f_1 irreducible del polinomio. Renombrando si es necesario las letras, se puede suponer que α_1 y β_1 son raices de dicho factor irreducible. Como f_1 es irreducible, las extensiones $k(\alpha_1)$ y $k(\beta_1)$ son isomorfas. Inductivamente se puede concluir. Para realizar la demostración con todo lujo de detalles damos antes unos preliminares.

Sea $\tau : K \to L$ un morfismo de cuerpos. A cada polinomio

$$f = a_n x^n + \cdots + a_1 x + a_0 \in K[X]$$

le podemos asociar el polinomio

$$\tau_*(f) = \tau(a_n)x^n + \cdots + \tau(a_1)x + \tau(a_0) \in L[X]$$

Tenemos definido de este modo un morfismo de anillos de $K[x]$ en $L[x]$ que es inyectivo. Si τ es un isomorfismo, también lo es τ_* (a partir de ahora denotaremos por también po r τ al morfismo entre los anillos de polinomios).

Dadas dos extensiones $k \to K$ y $k \to L$ y un automorfismo $\tau : k \to k$, decimos que un morfismo de cuerpos $\varphi : K \to L$ es una extensión de τ si $\varphi(a) = \tau(a)$ para toda constante $a \in k$. Si consideramos que k está contenido en K y en L, entonces la aplicación φ al restringirla a k coincide con τ. El caso más típico es considerar que τ es la identidad y entonces no hemos hecho más que volver a definir el concepto de morfismo de álgebras.

El concepto de extensión de un isomorfismo se expresa en diagramas

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & L \\ \uparrow & & \uparrow \\ k & \xrightarrow{\tau} & k \end{array}$$

Proposición 12.1 *Dado un polinomio f irreducible sobre k, sea $\tau : k \to k$ un automorfismo. Sea K una extensión donde f tenga una raíz α y sea L una extensión donde $\tau(f)$ tenga una raíz β. Existe un isomorfismo $\varphi : k(\alpha) \to k(\beta)$ que extiende a τ y que verifica $\varphi(\alpha) = \beta$*

Demostración. El isomorfismo τ produce un isomorfismo $\tau : k[x] \to k[x]$, de tal modo que los polinomios irreducibles están relacionados por dicho isomorfismo.

Este isomorfismo hace conmutativo el diagrama

$$\begin{array}{ccc} k[x] & \xrightarrow{\tau} & k[x] \\ \uparrow & & \uparrow \\ k & \xrightarrow{\tau} & k \end{array}$$

Pasando al cociente se tiene un isomorfismo

$$\begin{array}{ccc} k[x]/(f) & \xrightarrow{\varphi} & k[x]/(\tau(f)) \\ \uparrow & & \uparrow \\ k & \xrightarrow{\tau} & k \end{array}$$

Teniendo en cuenta que $k[x]/(f) \sim k(\alpha)$ y que $k[x]/\tau_* f \sim k(\beta)$ se concluye la existencia del isomorfismo. Debido a la construcción realizada se tiene que $\varphi(\alpha) = \beta$ y además extiende a τ. $\square$

Proposición 12.2 *Dos campos de descomposición de un polinomio son k-isomorfos.*

Demostración. Sea $K = k(\alpha_1, \ldots, \alpha_n)$ y $L = k(\beta_1, \ldots, \beta_n)$. Renombrando

las raices si es necesario hemos visto que existe un isomorfismo

$$\tau_1 : k(\alpha_1) \to k(\beta_1)$$

que prolonga a la identidad. Del mismo modo existe un isomorfismo

$$\tau_2 : k(\alpha_1, \alpha_2) \to k(\beta_1, \beta_2)$$

que prolonga a τ_1 y por lo tanto prolonga a la identidad. Repitiendo el proceso n veces se obtiene el isomorfismo φ buscado. Además, si observamos dicha construcción veremos que el isomorfismo verifica $\varphi(\alpha_i) = \beta_i$. $\square$

Corolario 12.3 *Dado $f \in k[x]$, sea Σ un cuerpo de descomposición. Si L es otro cuerpo sobre el que f descompone, existe un morfismo de $\varphi : \Sigma \to L$.*

Demostración. Sean $\alpha_1, \ldots, \alpha_n$ las raices de f en L. El cuerpo generado por dichas raices es isomorfo a Σ, lo que permite crear el morfismo. $\square$

13. Cuerpos finitos

Como aplicación de este teorema de unicidad veremos la estructura de los cuerpos finitos. Necesitamos un pequeño resultado, que probaremos posteriormente (ver **??**), que nos asegura que el polinomio $x^n - x$ carece de raices múltiples.

Sea K un cuerpo finito. Hemos visto que el cardinal de K es p^n donde p es la característica de K. El conjunto $K^* = K - \{0\}$ es un grupo, respecto a la multiplicación, que posee $p^n - 1$ elementos. El teorema de Lagrange sobre grupos finitos implica que cualquier elemento del grupo elevado a su orden es la unidad. Tenemos entonces que todo elemento a de K^* verifica

$$a^{p^n-1} = 1 \Leftrightarrow a^{p^n-1} - 1 = 0$$

Todos los elementos de K^* son raices del polinomio $x^{p^n-1} - 1$. Si añadimos la raíz cero, resulta que todos los elementos de K, incluido el cero, son raices

del polinomio $x^{p^n} - x$. El cuerpo K es entonces el cuerpo de descomposición de un polinomio (sobre el cuerpo primo) y es único salvo isomorfismo.

De modo recíproco, si queremos construir un campo con p^n elementos consideramos el polinomio $x^{p^n} - x$ sobre el cuerpo $\mathbb{F}_p$ y hallamos su cuerpo de descomposición Σ. Dentro de Σ consideramos el conjunto C formado por las raices del polinomio. Pero es fácil ver, utilizando el morfismo de Fröbenius, que el conjunto C es ya un cuerpo y por lo tanto debe coincidir con Σ. Este cuerpo tiene tanto elementos como raices tiene el polinomio, esto es p^n.

Definición 13.1 *Para cada p y cada entero n existe un único cuerpo con p^n elementos. Denotamos dicho cuerpo por $\mathbb{F}_{p^n}$ (o también $\mathrm{GF}(p^n)$).*

Observación. 14 *El polinomio $x^n - x$ sobre $\mathbf{F}_p$ tiene como cuerpo de descomposición $\mathbf{F}_{p^n}$. Sin embargo existen otros polinomios que también tienen el mismo cuerpo de descomposición.*

Además de esto, el grupo multiplicativo del cuerpo es siempre un grupo ciclíco. Para probarlo debemos recordar algunas nociones de la teoría de grupos.

Sea G un grupo finito y g un elemento. Denotemos por (g) al subgrupo generado por dicho elemento. Llamamos orden de un elemento g al cardinal del grupo que genera. Por lo tanto g elevado a su orden es el elemento neutro. Ningún numero natural menor posee dicha propiedad. Llamamos exponente del grupo G al mínimo común múltiplo de los órdenes de sus elementos. Cualquier elemento del grupo elevado al exponente del grupo es necesariamente la unidad y este número es el menor de los que presentan dicha propiedad. En general, dado un grupo arbitrario, no es necesario que exista un elemento cuyo orden coincida con el exponente del grupo. Sin embargo si es cierto en los grupos abelianos.

Proposición 13.1 *Si G es abeliano, existe un elemento cuyo orden coincide con el exponente del grupo.*

Demostración. Sea $p_1^{a_1} \dots p_n^{a_n}$ la descomposición en factores del exponente del grupo. Como el exponente se obtiene a través del mínimo común múltiplo, deben existir elementos g_i cuyo orden sea múltiplo de $p_i^{a_i}$. Tomando

potencias de estos elementos, podemos encontrar elementos h_i cuyo orden sea exactamente $p_1^{a_i}$. El elemento $h_1 \dots h_n$ verifica el enunciado. $\square$

Corolario 13.2 *Si G es abeliano y su exponente coincide con su cardinal, entonces el grupo es cíclico.*

Corolario 13.3 *Si k es un cuerpo finito, k^* es un grupo cíclico.*

Demostración. Si k tiene q elementos, los elementos no nulos son raices del polinomio $x^{q-1} - 1$. Aunque algunos elementos pueden ser raices de un polinomio $x^h - 1$ de grado menor, no todos pueden cumplirlo, pues dicho polinomio tendría mas raices que su grado. Necesariamente hay un elemento de grado $q - 1$ y el subrupo que genera debe coincidir con k^*. $\square$

Como los subgrupos de los grupos cíclicos son también cíclicos obtenemos

Corolario 13.4 *Si k es finito, cualquier subgrupo de k^* es cíclico.*

El siguiente resultado es el teorema del elemento primitivo, pero válido únicamente para cuerpos finitos.

Corolario 13.5 *Toda extensión $k \to K$ donde K es finito es simple.*

Demostración. Sea θ un generador del grupo K^*. Es claro que $k(\theta)$ debe coincidir con K. $\square$

Por completitud, enunciaremos otras propiedades, que son corolarios evidentes de la teoría de Galois que analizaremos en próximos capítulos.

- Todo automorfismo del cuerpo $\mathbf{F}_{p^n}$ es una potencia del morfismo de Fröbenius.
- Los subcuerpos de $\mathbf{F}_{p^n}$ son de la forma $\mathbf{F}_{p^r}$, donde r divide a n.

14. Extensiones normales

Definición 14.1 *Una extensión $k \to K$ es* normal *si todo polinomio irreducible $f \in k[x]$ que tiene una raíz en K, descompone en factores lineales en K.*

Si la extensión es normal, todo polinomio irreducible sobre k que tenga una raíz, necesariamente tiene todas sus raices en K, alguna de las cuales puede estar repetida. Los polinomios de k que tienen raices en K son precisamente los polinomios mínimos de los elementos de K. Por ello el siguiente corolario se toma muchas veces como definición de extensión normal.

Corolario 14.1 *La extensión $k \to K$ es normal si todo polinomio mínimo m_α, con $\alpha \in K$, descompone en factores lineales en K.*

Ejemplos.

- La extensión $\mathbb{R} \to \mathbb{C}$ es normal, pues todo polinomio, irreducible o no, descompone en $\mathbb{C}$. Este razonamiento sirve para cualquier extensión $k \to K$, donde K sea algebraicamente cerrado.
- La extensión $\mathbb{Q} \to \mathbb{R}$ no es normal. El polinomio $x^3 - 2$ es irreducible sobre $\mathbb{Q}$ y tiene una raíz real, que denotamos por $\sqrt[3]{2}$. Sin embargo el polinomio no descompone en factores lineales en $\mathbb{R}$ por tener dos raices complejas conjugadas.
- Sea α la raíz cúbica real de 2. Por el mismo motivo que antes la extensión $\mathbb{Q} \to \mathbb{Q}(\alpha)$ no es normal.

Proposición 14.2 *Toda extensión finita y normal es un cuerpo de descomposición.*

Demostración. Sea $k \to K$ la extensión. Como es finita podemos encontrar elementos algebraicos $\alpha_1, \ldots, \alpha_n$ tales que $K = k(\alpha_1, \ldots, \alpha_n)$.

Denotamos por m_{α_i} a los polinomios mínimos de los generadores y por f al producto de todos ellos

$$f = m_{\alpha_1} \cdots m_{\alpha_n}$$

Por definición, α_i es raíz de m_{α_i} y como la extensión es normal, el polinomio m_{α_i} descompone en factores lineales en K. De esta forma, f también descompone en factores lineales en K. Como K está generado por raices de f, es el cuerpo de descomposición de f. $\square$

El resultado que acabamos de demostrar es ciertamente sencillo. Su recíproco también es cierto aunque tiene alguna complicación más.

Proposición 14.3 *Todo cuerpo de descomposición es una extensión finita y normal.*

Demostración. Sabemos que todo cuerpo de descomposición es de grado finito y además ese grado está acotado por $n!$, siendo n el grado del polinomio.

Supongamos que $k \to K$ es un cuerpo de descomposición de un cierto polinomio f. Tomamos un polinomio g sobre k que sea irreducible. Para demostrar este resultado consideramos un cuerpo auxiliar, que será el cuerpo de descomposición de fg. Lo denotaremos por L. Si $\theta_1, \ldots, \theta_s$ son las raices del polinomio g, veremos que todas las extensiones $K \to K(\theta_i)$ tienen el mismo grado. Si el polinomio g tiene una raíz en K, por ejemplo θ_1, se tiene que $[K(\theta_i) : K] = 1$ y todas las raices pertenecen a K.

Denotemos por θ_1 y θ_2 dos raices arbitrarias del polinomio g en el cuerpo L. Con ayuda de estas raices construimos las torres

$$k \to k(\theta_i) \to K(\theta_i) \to L$$

Además tenemos de modo evidente la torre

$$k \to K \to K(\theta_i)$$

Tenemos dos formas distintas de llegar desde el cuerpo k al $K(\theta_i)$. Aplicando la propiedad de la torre de cuerpos

$$[K(\theta_i) : k(\theta_i)][k(\theta_i) : k] = [K(\theta_i) : k] = [K(\theta_i) : K][K : k]$$

Ahora debemos tener en cuenta dos observaciones:

- Las extensiones $k \to k(\theta_1)$ y $k \to k(\theta_2)$ son isomorfas, por obtenerse de k añadiendo una raíz de un polinomio irreducible.
- La extensión $k(\theta_1) \to K(\theta_1)$ es un cuerpo de descomposición del polinomio f. Lo mismo con la otra extensión. Como los cuerpos base son isomorfos y el polinomio g es el mismo en ambas, necesariamente son isomorfas y tienen el mismo grado.

De estos razonamientos se desprende fácilmente que $[K(\theta_i) : K]$ es independiente de la raíz considerada. □

Como conclusión tenemos que las ampliaciones normales y finitas son simplemente los cuerpos de descomposición. Supondremos de ahora en adelante que cuando hablemos de extensión normal, también será finita.

Observación. 15 *Utilizando la clausura algebraica hemos definido el cuerpo de descomposición de un colección infinita de polinomios. En este caso, toda extensión normal, sea o no de dimensión finita, es el cuerpo de descomposición de un conjunto de polinomios.*

Utilizando que una extensión normal no es más que un cuerpo de descomposición, podemos dar nuevas versiones de algunos resultados ya conocidos.

Corolario 14.4 *Sea $k \to K$ una extensión normal y L un cuerpo intermedio. Entonces $L \to K$ es normal.*

Demostración. Si $f \in k[x]$ tiene como cuerpo de descomposición K, entonces el mismo polinomio, pero con coeficientes en L, también tiene como cuerpo de descomposición K. □

Corolario 14.5 *Sea $k \to K$ una extensión normal. Sea L un cuerpo intermedio y $\tau : L \to L$ un automorfismo. Existe un automorfismo $\varphi : K \to K$ que prolonga a τ.*

Demostración. Hemos visto que $L \to K$ es normal y es un cuerpo de descomposición. Cualquier automorfismo de L se prolonga a un automorfismo del campo de descomposición. □

Corolario 14.6 *Sea $k \to K$ normal y α_1 y α_2 dos raices de un polinomio irreducible sobre k. Entonces existe un morfismo φ que cumple $\varphi(\alpha_1) = \alpha_2$.*

Demostración. Tenemos que $k(\alpha_1)$ y $k(\alpha_2)$ son isomorfismos. Como K es normal, el isomorfismo se puede prolongar. □

15. Separabilidad

Dos polinomios f y g son primos entre sí, cuando su máximo común divisor sea 1. Si los polinomios pertenecen a un cuerpo k es de esperar que esos polinomios puedan dejar de ser primos en alguna extensión K, debido a que en dicha extensión "hay más polinomios" y alguno de los nuevos polinomios podría dividir a ambos. Sin embargo esta ideal es falsa. Si son primos sobre un cuerpo k, lo son sobre cualquier extensión, pues el máximo común divisor se calcula por el algoritmo de Euclides, que utiliza solamente polinomios de k. En particular, si dos polinomios son primos, no tienen ninguna raíz común. Recíprocamente, si tienen una raíz común α, entonces $(x-\alpha)$ divide a ambos polinomios y no pueden ser primos. Pero además, por la discusión anterior, no pueden tener raices comunes en ninguna extensión.

Si α es una raíz de f, la multiplicidad de la raíz es el único entero m que cumple que $(x-\alpha)^m$ divide a f y $(x-\alpha)^{m+1}$ no divide a f. Si $m = 1$ la raíz se llama simple, y si m es mayor que 1 se dice que es una raíz múltiple.

Definición 15.1 *Un polinomio irreducible se dice que es* separable *si no tiene raices múltiples en su cuerpo de descomposición.*

Si tiene raices múltiples en alguna extensión, debe tener raices múltiples en su cuerpo de descomposición. De este modo sus raices son todas distintas, independientemente de la extensión.

Para comprobar que un polinomio irreducible es separable, lo más cómodo es utilizar el concepto de derivada.

Definición 15.2 *Dado el polinomio* $f = a_n x^n + \cdots + a_1 + a_0$, *llamamos derivada de* f *y denotamos* Df *al polinomio*

$$Df = na_n x^{n-1} + (n-1)a_{n-a}x^{n-2} + \cdots + a_1$$

Las propiedades de la derivada de polinomios sobre cualquier cuerpo son similares las propiedades conocidas del Análisis y se deducen inmediatamente a partir de la definición. Enumeremos las que nos interesan.

- $D(f+g) = Df + Dg$.
- $D(fg) = (Df)g + f(Dg)$
- $D(\lambda f) = \lambda Df$ siendo λ un escalar.
- $D(f^n) = nD(f)^{n-1}$

La diferencia principal con el Análisis estriba en que $D(f)$ puede ser nula sin ser f un polinomio constante. Esto solo puede ocurrir si la característica es positiva

Proposición 15.1 *Sea* k *un cuerpo de característica* p. *Un polinomio* f *tiene derivada nula si y solo si todos sus monomios tienen como grado un múltiplo de* p.

Demostración. Sea ax^{pn} un monomio cuyo grado es un múltiplo de p.

$$D(ax^{pn}) = (pn)ax^{pn-1} = 0ax^{pn-1} = 0$$

Si queremos que $D(f) = 0$, debe ocurrir lo mismo para cada monomio de los que consta f

$$D(x^n) = nx^{n-1} = 0 \Leftrightarrow p \text{ divide a } n$$

y f es un polinomio cuyos monomios tiene siempre como grado un múltiplo de p. $\square$

Proposición 15.2 *Un polinomio $f \in k[x]$ tiene raices múltiples (en su cuerpo de descomposición) si solo si f y Df no son primos.*

Demostración. Trabajaremos en en el cuerpo de descomposición del polinomio $f \cdot Df$ donde tanto f como su derivada descomponen en factores lineales.

$\Rightarrow$) Sea α una raíz múltiple de f. Podemos escribir f como

$$f = (x-\alpha)^m g(x)$$

Derivando

$$Df = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m Dg$$

y α es también raíz de la derivada. Como tienen una raíz común f y Df no pueden ser primos.

$\Leftarrow$) Si f y Df no son primos tienen algún factor común. Ese factor común debe descomponer en factores lineales en el cuerpo de descomposición en el que estamos trabajando. Por lo tanto f y Df tienen una raíz común. Sea α una raíz común de f y Df. Entonces

$$\begin{aligned} f &= (x-\alpha)g(x) \\ Df &= (x-\alpha)h(x) \end{aligned}$$

Derivando

$$Df = g(x) + (x-\alpha)Dg$$

Tomando valores para $x = \alpha$ obtenemos que

$$D(f(\alpha) = g(\alpha)$$

y $g(x)$ tiene también como raíz α. Resulta que $g(x) = (x-\alpha)g_1(x)$

$$f = (x-\alpha)(x-\alpha)g_1$$

y α es raíz múltiple. $\square$

Hemos utilizado un cuerpo de descomposición para probar la proposición. Pero para comprobar que un polinomio tiene raices múltiples no es necesario ninguna extensión. Simplemente hallamos su derivada y el máximo común divisor, que son operaciones que se realizan sin utilizar cuerpos de descomposición.

Corolario 15.3 *Si la derivada de un polinomio irreducible no es nula, el polinomio es separable.*

Demostración. Si f es irreducible de grado n, su derivada es siempre de grado menor. Necesariamente son primos y f no posee raices múltiples. □

Corolario 15.4 *Si la característica es nula todo polinomio irreducible es separable.*

El caso de los polinomios que no son irreducibles se estudia en base a los irreducibles.

Definición 15.3 *Un polinomio, no necesariamente irreducible, es* separable *si sus factores son polinomios separables.*

Por lo tanto, los polinomios separables que no sean irreducibles, si pueden poseer raices múltiples.

Definición 15.4 *Una extensión $k \to K$ es separable si el polinomio mínimo de todo elemento de K es separable.*

Proposición 15.5 *Sea $k \to K$ una extensión separable. Si L es un cuerpo intermedio, entonces $k \to L$ y $L \to K$ son separables.*

Demostración. La extensión $k \to L$ es separable de modo evidente. Si m_α es un polinomio separable para $\alpha \in K$, necesariamente ocurre lo mismo para los elementos de L.

Dado $\alpha \in K$, el polinomio mínimo sobre L de α es siempre un divisor del polinomio mínimo de α sobre k. Si este último no tiene ninguna raíz múltiple, ningún divisor suyo puede tener raices múltiples. □

16. Polinomios irreducibles sobre $\mathbb{Q}$

Pretendemos dar condiciones necesarias para demostrar que un polinomio es irreducible sobre $\mathbb{Q}$. El lema de Gauss nos permitirá estudiar únicamente el caso de los polinomios con coeficientes en el anillo $\mathbb{Z}$, que es más sencillo.

Proposición 16.1 *Sea $a_n x^n + \cdots + a_1 x + a_0$ un polinomio con coeficientes enteros. Si α/β es una fracción irreducible que es raíz de este polinomio necesariamente α divide al término independiente a_0 y β divide al término de mayor grado a_n.*

Demostración.

Como α/β es raíz del polinomio se cumple la ecuación

$$a_n \frac{\alpha^n}{\beta^n} + a_{n-1} \frac{\alpha^{n-1}}{\beta^{n-1}} \cdots + a_1 \frac{\alpha}{\beta} + a_0 = 0$$

Para quitar denominadores multiplicamos dicha expresión por β^n

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} \beta + \cdots + a_1 \alpha \beta^{n-1} + a_0 \beta^n = 0$$

Sacando factor común α de todos los términos, salvo el último

$$\alpha(\text{número entero}) = -a_0 \beta^n$$

y α divide al producto $a_0 \beta^n$. Como α es primo con β, necesariamente α divide a a_0. Sacando factor común β se obtiene el otro resultado. $\square$

En el caso de que el polinomio sea mónico, el denominador tiene que dividir a la unidad. Las raices son números enteros y necesariamente son divisores del término independiente. Aplicando la conocida regla de Ruffini podemos hallar las raices enteras (y por lo tanto racionales) del polinomio.

Corolario 16.2 *Si un polinomio unitario con coeficientes enteros de grado 2 ó 3, no tiene raices enteras entonces es irreducible.*

Demostración.

Si el polinomio no es irreducible debe descomponer en producto de dos factores, de los cuales uno necesariamente es de primer grado. Un factor de primer grado equivale a una raíz que por la proposición anterior debe ser un número entero. □

Ejemplos.

- El polinomio $x^2 - 2$ no tiene raices racionales y es irreducible.
- Las únicas raices enteras de $x^3 - 2$ pueden ser $+2, -2, +1, -1$ y un rápido cálculo prueba que ninguna es solución. El polinomio es irreducible.
- A partir del grado cuatro, este razonamiento falla. Por ejemplo

$$x^4 + 4x^2 + 4 = (x^2 + 2)(x^2 + 2)$$

es claramente reducible y no posee raices racionales.

Definición 16.1 *Un polinomio con coeficientes enteros es* primitivo *si el máximo común divisor de sus coeficientes es* 1.

Equivalentemente, un polinomio con coeficientes enteros es primitivo si ningún primo p divide a todos los coeficientes.

Si tenemos un polinomio con coeficientes racionales, podemos multiplicarlo por un múltiplo común de todos los denominadores eliminando de este modo los denominadores. De esta forma un cierto múltiplo es un polinomio con coeficientes enteros. A cualquier polinomio con coeficientes enteros le podemos realizar la siguiente operación: calculamos el máximo común divisor de los coeficientes y sacando dicho número factor común obtenemos un polinomio primitivo multiplicado por cierta constante.

Proposición 16.3 *Dado un polinomio $q(x)$ con coeficientes racionales existe un único polinomio primitivo $q_*(x)$ que verifica*

$$q(x) = \frac{a}{b}\, q_*(x)$$

donde la fracción es irreducible.

Lema 16.4 (Gauss) *El producto de dos polinomios primitivos es primitivo.*

Demostración.

Sean $q(x)$ y $r(x)$ los dos polinomios. Escribamos explícitamente todos los polinomios con los que vamos a tratar.

$$\begin{aligned} q(x) &= a_n x^n + \cdots + a_1 x + a_0 \\ r(x) &= b_m x^m + \cdots + b_1 x + b_0 \\ q(x)r(x) &= c_{n+m} x^{n+m} + \cdots + c_1 x + c_0 \end{aligned}$$

Dado un número primo p, no todos los coeficientes de $q(x)$ son divisibles por p. Sea j el grado del menor coeficiente que no es divisible entre p. De este modo elementos $a_0, a_1, \ldots, a_{j-1}$ son divisibles entre p. Análogamente sea k el grado que cumple lo mismo en el otro polinomio.

Concentremonos en el grado $j+k$ del producto y expresemos dicho coeficiente

$$\begin{aligned} c_{j+k} = (a_0 b_{j+k} + a_1 b_{j+k-1} + \cdots + a_{j-1} b_{k+1}) + a_j b_k + \\ (a_{j+1} b_{k-1} + a_{j+2} b_{k-2} \cdots + a_{j+k} b_0) \end{aligned}$$

Todos los sumandos del primer paréntesis llevan un factor a_i divisible entre p. Por lo tanto el primer paréntesis es divisible entre p. Análogamente todos los sumandos del segundo paréntesis tienen un elemento de la forma b_i que es divisible entre p. Como ni a_j ni b_k son divisibles entre p, el coeficiente c_{j+k} no es divisible entre p. No existe ningún primo que divida a todos los coeficientes del producto, que es entonces primitivo. □

Proposición 16.5 *Un polinomio con coeficientes enteros es irreducible sobre $\mathbb{Q}$ si y solo si es irreducible sobre $\mathbb{Z}$.*

Demostración.

Sea f un polinomio con coeficientes enteros que no pueda expresarse como producto de dos polinomios enteros de grado estrictamente menor.

Supongamos que si se puede descomponer en producto de factores racionales

$$f = gh \text{ con } g, h \in \mathbb{Q}[x]$$

Sabemos que cada polinomio con coeficientes racionales se puede escribir como un múltiplo de un polinomio primitivo. Sea

$$\begin{aligned} g &= \frac{\alpha_1}{\beta_1}\, g_* \\ h &= \frac{\alpha_2}{\beta_2}\, h_* \end{aligned}$$

Uniendo todo obtenemos

$$f = \frac{\alpha_1\alpha_2}{\beta_1\beta_2}\, g_*h_* = \frac{\alpha}{\beta}\, g_*h_*$$

donde hemos simplificado la fracción convirtiendola en irreducible.

El término de la izquierda es un polinomio con coeficientes enteros. Como β no divide a α, para que el miembro de la derecha tenga también coeficientes enteros, debe dividir a todos los coeficientes del polinomio $g_*(x)h_*(x)$. Como el producto es un polinomio primitivo, necesariamente $\beta = 1$ y se obtiene la factorización

$$f = (\alpha g_*h_*$$

que está formada por dos polinomios de coeficientes enteros. Esto implica una contradicción con nuestra hipótesis. □

Ya tenemos los útiles necesarios para enunciar el criterio de irreducibilidad de Eisentein.

Proposición 16.6 *Sea $f = a_nx^n + \cdots + a_1x + a_0$ un polinomio con coeficientes enteros. Supongamos que existe un número primo p que verifica:*

- *p no divide al término de orden máximo a_n*
- *p divide a todos los demás coeficientes: $a_{n-1}, \ldots, a_1, a_0$.*

- *p^2 no divide al término independiente a_0.*

Entonces el polinomio es irreducible sobre los racionales.

Demostración.

Gracias a la proposición anterior podemos suponer que la factorización se realiza con polinomios enteros. Sea $f = gh$ donde

$$\begin{aligned} g(x) &= b_r x^r + \cdots + b_1 x + b_0 \\ h(x) &= c_s x^s + \cdots + c_1 x + c_0 \end{aligned}$$

Tenemos que $a_0 = b_0 c_0$. Como p^2 no divide a a_0, p solo divide a uno de los dos factores del producto. Supongamos que divide a b_0. Ahora $a_1 = b_0 c_1 + b_1 c_0$. De aquí se deduce que p divide a b_1 e inductivamente se demuestra que divide al término de mayor grado b_r de $g(x)$. Pero entonces el término de mayor grado del producto (que es $b_r c_s$) es divisible por p. Contradicción. □

Ejemplos.

- $x^n - 2$ es irreducible aplicando el criterio de Eisentein con $p = 2$.
- En general $x^n - p$ es irreducible si p es un número primo.

Observación.

Prácticamente todos los resultados y demostraciones se pueden realizar en un anillo que sea un dominio de factorización única. En este caso el papel de $\mathbb{Z}$ lo juega el anillo A y el papel de $\mathbb{Q}$ el cuerpo de fracciones del anillo íntegro.

Sean $k \to K$ y $k \to L$ dos extensiones de un mismo cuerpo. El conjunto de morfismos de álgebra (k-morfismos) de K en L lo denotaremos por $\mathrm{Mor}(K, L)$. En algunos casos este conjunto admite una interpretación sencilla. Uno de los casos más interesantes se da cuando K es una extensión simple. Estudiamos el caso transcendente y el algebraico por separado.

Proposición 16.7 *Sea $k(\alpha)$ una extensión simple transcendente de k. Dado un morfismo $\varphi : k(\alpha) \to L$ el elemento $\varphi(\alpha)$ es transcendente. Reciprocamente, si $\beta \in L$ es transcendente, existe un morfismo $\varphi : k(\alpha) \to L$ que verifica $\varphi(\alpha) = \beta$.*