Apunte Cuerpos y Algebras

Alicia Labra

2019

Índice

1. Introducción

Este curso necesita del curso previo *Grupos y Anillos*. En particular, todo resultado y notación de este curso se asume como conocido. El curso *Cuerpos y Álgebras* es un curso más avanzado sobre estos dos objetos. Los conocimientos son más profundos pues es un curso terminal de álgebra. Estos apuntes se han hecho con la colaboración de los Profesores Antonio Behn, Alicia Labra, Giancarlos Lucchini y por Claudio Bravo, alumno de doctorado en Ciencias mención Matemáticas, de nuestro Programa de Doctorado.

Objetivos Generales:

1. Conocer más profundamente propiedades de cuerpos, diferentes tipos de extensiones de cuerpos, solubilidad por radicales.
2. Tener una buena base sobre el estudio de algunos tipos de álgebras, álgebras tensorial simétrica y exterior.

Objetivos Específicos:

1. Conocer y aplicar propiedades de extensiones finitas y algebraicas.
2. Conocer teorema de extensión de homomorfismos y la unicidad de la clausura algebraica.
3. Comprender las extensiones separables e inseparables, los cuerpos perfectos.
4. Conocer y saber la relación entre extensiones normales, cuerpo de descomposición de un polinomio.
5. Conocer y trabajar con extensiones Galoisianas. Teorema de Galois.
6. Comprender y trabajar las extensiones de Kummer y Artin-Scheider
7. Conocer las extensiones ciclotómicas y la solubilidad por radicales.

8. Conocer algunos ejemplos de álgebras como son: álgebras de funciones y álgebra de matrices.

9. Comprender el producto tensorial de álgebras y la extensión del cuerpo de escalares. Conocer las álgebras tensorial, simétrica y exterior.

10. Optativo: Conocer y comprender álgebras simples y semisimples. Teorema de Wedderburn.

2. Cuerpos

2.1. Parte Básica

Sea R anillo conmutativo con unidad 1_R.

Definición 2.1. *Para cada $n \in \mathbb{Z}$ definamos*

$$n \cdot 1_R = \begin{cases} \underbrace{1_R + 1_R + \ldots + 1_R}_{n \text{ veces}} & n \in \mathbb{N} \\ 0 & n = 0 \\ \underbrace{(-1_R) + (-1_R) + \ldots + (-1_R)}_{(-n) \text{ veces}} & (-n) \in \mathbb{N} \end{cases}$$

De inmediato, se tiene $\forall n, m \in \mathbb{Z}$.

1. $(n+m) \cdot 1_R = n \cdot 1_R + m \cdot 1_R$.

2. $(nm) \cdot 1_R = (n \cdot 1_R)(m \cdot 1_R)$.

Definición 2.2. *Se define la característica de R, como el menor entero positivo n tal que $n \cdot 1_R = 0$. Si no existe tal entero n diremos que el anillo R tiene característica 0.*

Ejemplo 2.1. *$\mathbb{Z}/n\mathbb{Z}$ tiene característica n.*

Notación: *$car(R)$.*

Por las propiedades 1. y 2. enteriores se tiene de inmediato que

Observación 2.1. *$\phi : \mathbb{Z} \longrightarrow R$ tal que $\phi(n) = n \cdot 1_R$, es homomorfismo de anillos.*

Lema 2.1. *Sea R anillo conmutativo con 1_R y de característica n, entonces R contiene un subanillo isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Si R tiene característica 0, entonces R contiene un subanillo isomorfo a $\mathbb{Z}$.*

Demostración. Consideremos $\phi : \mathbb{Z} \longrightarrow R$ tal que $\phi(n) = n \cdot 1_R$, homomorfismo de anillos ya definido. Observamos que $Ker(\phi) = \{n \in \mathbb{Z} | n \cdot 1_R = 0\}$ es un ideal de $\mathbb{Z}$. Como $\mathbb{Z}$ es Dominio de Ideales Principales se concluye que $Ker(\phi) = \langle t \rangle = t\mathbb{Z}$ con t positivo y el menor entero tal que $t \cdot 1_R = 0$.

Si $\text{car}(R) = n$, entonces $Ker(\phi) = n\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z} \simeq \phi(\mathbb{Z})$ que es un subanillo de R.

Si $\text{car}(R) = 0$, entonces $m \cdot 1_R \neq 0 \; \forall \; m \in \mathbb{Z}$ Luego $Ker(\phi) = \{0\}, \phi$ inyectiva y $\mathbb{Z} \simeq \phi(\mathbb{Z})$ que es un subanillo de R. □

Definición 2.3. *Un cuerpo es un anillo conmutativo F con uno 1_F en el que todo elemento no nulo tiene inverso multiplicativo.*

Ejemplo 2.2. $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, *con p primo.*

Notación: En lo que sigue usaremos la notación $1_F = 1$.

Veamos ahora un criterio para saber si estamos en presencia de un subcuerpo:

Proposición 2.1. *Sea L un subconjunto de un cuerpo F con al menos dos elementos, entonces L es subcuerpo de F si y sólo si*

1. $\forall \, x, y \in L$, $x - y \in L$;
2. $\forall \, x, y \in L \setminus \{0\}$, $xy^{-1} \in L$.

Demostración. Es claro de la definición de subcuerpo que se cumplen 1. y 2. .La primera propiedad nos dice que L es un subgrupo aditivo de F. La segunda propiedad aplicada a $y = x$ nos dice que $1 \in L$ (nótese que existen elementos en $L \setminus \{0\}$ ya que L posee al menos dos elementos). La misma propiedad aplicada a $x = 1$ nos dice entonces que para todo $y \in L$, y^{-1} también pertenece a L. Finalmente, la misma propiedad con y^{-1} nos dice que L

es cerrado por multiplicación, por lo que se trata de un subanillo unitario (y conmutativo) donde todo elemento es invertible. Es decir, L es un subcuerpo. El sentido inverso de la proposición es obvio de la definición de subcuerpo. □

Ejemplo 2.3. *Otro ejemplo de cuerpo es $F(x)$, el cuerpo de fracciones del anillo de polinomios $F[x]$ para F otro cuerpo. En este caso, F es un subcuerpo de $F(x)$.*

Teorema 2.1. *Sea F un cuerpo. Entonces* $\text{car}(F) = 0$ *o* $\text{car}(F) = p$ *con p un número primo. Además, si* $\text{car}(F) = 0$ *(resp.* $\text{car}(F) = p$*), entonces F contiene un subcuerpo isomorfo a $\mathbb{Q}$ (resp. $\mathbb{F}_p$).*

Para demostrar este teorema, recordemos un resultado importante del curso de Grupos y Anillos:

Teorema 2.2. *Sea R un dominio de integridad. Entonces todo cuerpo que contiene a R contiene a su cuerpo de fracciones $Q(R)$.*

Demostración del Teorema 2.1. Consideremos el homomorfismo $\phi : \mathbb{Z} \to F : 1_{\mathbb{Z}} \mapsto 1_F$ que define la característica de F. Por Lema 2.1 tenemos

Si $\text{car}(F) = n$, entonces $Ker(\phi) = n\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z} \simeq \phi(\mathbb{Z})$ que es un subanillo de F.

Probaremos que n es un número primo. Supongamos que no es así. Digamos $n = ab$ con $1 < a, b < n$. Entonces

$$0 = n \cdot 1 = (a \cdot b) \cdot 1 = a(b \cdot 1) = (a \cdot 1)(b \cdot 1),$$

pero como F es cuerpo $a \cdot 1 = 0 \ \vee \ b \cdot 1 = 0$ lo cual contradice la elección de n. Concluimos entonces que n es primo y $\mathbb{Z}/n\mathbb{Z}$ es un cuerpo. Luego $\phi(\mathbb{Z})$ que es un subcuerpo de F y $\phi(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$ con p primo.

Si $\text{car}(F) = 0$, entonces $Ker(\phi) = \{0\}$, ϕ inyectiva y $\mathbb{Z} \simeq \phi(\mathbb{Z})$ que es un subanillo de F. Sea $S = \phi(\mathbb{Z})$. Como $S \subseteq F$ y F cuerpo, entonces S no tiene divisores de cero. Por Teorema 2.2 se tiene que $Q(S) \subseteq F$. Como $\mathbb{Z} \simeq S$ entonces $\mathbb{Q} \simeq Q(S)$. □

Observación 2.2. *Si K es un cuerpo de característica $p > 0$, entonces para todo $\alpha \in K$ tenemos que $p\alpha = 0$. En efecto:*

$$p\alpha = p(\alpha \cdot 1) = p(1 \cdot \alpha) = (p \cdot 1)\alpha = 0 \cdot \alpha = 0.$$

Definición 2.4. *El subcuerpo de F del Teorema 2.1 se llama* subcuerpo primo *de F. Lo denotamos P.*

Observación 2.3. *Sea P es el subcuerpo primo de F. Si* $\text{car}(F) = 0$*, entonces $P \simeq \mathbb{Q}$. Si* $\text{car}(F) = p$*, entonces $P \simeq \mathbb{F}_p$.*

Ya vimos la noción de subcuerpo. Siguiendo la similitud con grupos, anillos y módulos, deberíamos estudiar ahora los homomorfismos de cuerpos y los cocientes de cuerpos. Sin embargo, estas dos nociones se portan de una forma bien peculiar en el caso de los cuerpos. Es más, basta con recordar un poco la teoría de anillos para darse cuenta que no podemos obtener un cuerpo al cocientar por un subcuerpo, por lo que no vale la pena buscar una noción de cociente en este marco. Los homomorfismos sí tienen un sentido sin embargo:

Definición 2.5. *Un* homomorfismo *de cuerpos K, L es un homomorfismo de anillos que respeta la unidad, es decir, un homomorfismo de anillos $\varphi : K \to L$ tal que $\varphi(1_K) = 1_L$.*

Observación 2.4. $\varphi(0_F) = 0_{F'} \quad y \quad \varphi(1_F) = 1_{F'}$.

Lema 2.2. *Si $\varphi : F \longrightarrow F'$ es homomorfismo de cuerpos, entonces φ es inyectivo.*

Demostración. Basta notar que $Ker(\varphi)$ es un ideal de F que es cuerpo. Luego, los únicos ideales son los triviales F y $\{0\}$. Si $Ker(\varphi) = F$, entonces $\varphi = 0$ lo cual es imposible pues todo homomorfismo de cuerpos lleva 1_F en $1'_F$. Por lo tanto, $Ker(\varphi) = \{0\}$ y φ es inyectivo. □

Si no podemos fabricar cocientes y tan solo podemos comparar cuerpos metiendo unos dentro de otros con homomorfismos, veamos si dado un cuerpo podemos construir otros más grandes que lo contengan. El siguiente teorema va en esta dirección.

Teorema 2.3 (Teorema de Kronecker)**.** *Sea F cuerpo y sea Q un polinomio no constante en $F[x]$. Entonces existe un cuerpo K que contiene un subcuerpo isomorfo a F, en el cual Q tiene una raíz.*

Demostración. Consideremos $K = F[x]/\langle P\rangle$ con P factor irreducible de Q. Como $F[x]$ es un D. I. P entonces $\langle P\rangle$ es maximal y K es cuerpo. Consideremos el epimorfismo canónico $\pi : F[x] \longrightarrow F[x]/\langle P\rangle$ tal que

$$\pi(h(x)) = h(x) + \langle P\rangle$$
$$(\pi(x) = x + \langle P\rangle)$$

Sea $\varphi = \pi\mid_F : F \longrightarrow F[x]/\langle P\rangle$, es decir, $\varphi(1) = 1 + \langle P\rangle$. Por Lema 2.2, φ es inyectivo, luego $F \simeq \varphi(F) = Im(F) \subseteq K$ y $\varphi(F)$ es subcuerpo de K. Falta ver que existe $\alpha \in K$ tal que $P(\alpha) = 0$. Tomemos $\alpha = x + \langle P\rangle$. Entonces $P(\alpha) = P(x) + \langle P\rangle = \langle P\rangle = 0_K$. Finalmente $\alpha \in K$ es raíz de Q pues P es factor de Q. □

Observación 2.5. *Sea P polinomio irreducible en $\mathbb{Q}[x]$ de grado n. Entonces $K = F[x]/\langle P\rangle = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle P\rangle \mid a_i \in F\}$. En efecto sea $H(x) + \langle P\rangle \in K$. Por algoritmo de división en $F[x]$, hay únicos $Q, R \in F[x]$ tales que*

$H(x) = \underbrace{Q(x)P(x)}_{\in\langle P\rangle} + R(x)$, $R = 0 \vee gr(R) < gr(P) = n$.

Se tiene que $gr(R) \leq n-1$, y por lo tanto $R(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ y $H(x) + \langle P\rangle = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + \langle P\rangle$.

Notación. *A partir de ahora, veremos muchos casos de anillos de polinomios cocientados por ideales maximales (generados por polinomios irreducibles). Para evitar una notación desagradable del estilo $\pi(x) = x + \langle P\rangle$, preferiremos a menudo una notación simplificada como $\pi(x) = \bar{x}$, dejando el ideal por el que estamos cocientando subentendido.*

Observación 2.6. *Usando la notación anterior tenemos que $b_0 + b_1x + b_2x^2 + b_{n-1}x^{n-1} + \langle P\rangle = b_0 + (b_1x + \langle P\rangle) + (b_2x^2 + \langle P\rangle) + (b_{n-1}x^{n-1} + \langle P\rangle) = b_0 + b_1(x + \langle P\rangle) + b_2(x^2 + \langle P\rangle) + b_{n-1}(x^{n-1} + \langle P\rangle) = b_0 + b_1(x + \langle P\rangle) + b_2(x + \langle P\rangle)^2 + b_{n-1}(x + \langle P\rangle)^{n-1} = b_0 + b_1\bar{x} + b_2\bar{x}^2 + b_{n-1}\bar{x}^{n-1}$.*

Ejemplo 2.4. *Consideremos el cuerpo $\mathbb{Q}$ y el polinomio irreducible x^3-2 (use por ejemplo el critero de Eisenstein). Obtenemos entonces el cuerpo $L=\mathbb{Q}[x]/\langle x^3-2\rangle$, en el cual todo elemento se escribe de la forma $a+b\bar{x}+c\bar{x}^2$ con $a,b,c\in\mathbb{Q}$. De nuevo, la suma es coordenada a coordenada y la multiplicación se calcula multiplicando los polinomios en $\bar{x}$ y reemplazando toda aparición de $\bar{x}^n$ con $n\geq 3$ por $2\bar{x}^{n-3}$. Así, obtenemos*

$$(a+b\bar{x}+c\bar{x}^2)(d+e\bar{x}+f\bar{x}^2)=(ad+2bf+2ce)+(ae+bd+2cf)\bar{x}+(af+be+cd)\bar{x}^2.$$

En el curso de Grupos y Anillos se vió que el anillo de polinomios $K[x]$ puede ser visto como un K-módulo de forma natural. Como K es un cuerpo, esta estructura es de hecho una estructura de espacio vectorial. Lo mismo ocurre de hecho para todo cociente de $K[x]$ por un ideal maximal y por ende los cuerpos que hemos fabricado con el teorema anterior resultan tener un base bien explícita.

Teorema 2.4. *Sea $P\in F[x]$, polinomio irreducible de grado n sobre F. Sea $K=F[x]/\langle P\rangle$ y sea $\theta=x+\langle P\rangle=\bar{x}$ raíz de P en K. Entonces, los elementos $1,\theta,\theta^2,\ldots,\theta^{n-1}$ forman una base de K como espacio vectorial sobre F. En particular,*

$$K=\{a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}\,|\,a_i\in F\ \forall i\}.$$

Veamos algunos ejercicios antes de demostrarlo.

Ejemplo 2.5. *Sea $F=\mathbb{Q}$, P polinomio irreducible en $\mathbb{Q}[x]$, donde $P(x)=x^3-2$. Sea $\theta=\bar{x}$ una raíz de P. Encuentre $(1+\theta+\theta^2)^{-1}$.*

Solución: Por el Teorema 2.4 tenemos que $K=\mathbb{Q}[x]/\langle P\rangle=\{a_0+a_1\theta+a_2\theta^2/a_i\in\mathbb{Q}\}$, pues $gr(x^3-2)=3$ y $\theta^3=2$.

Sea $(1+\theta+\theta^2)^{-1}=a+b\theta+c\theta^2$ con $a,b,c\in\mathbb{Q}$ por determinar.

Sabemos que

$(1+\theta+\theta^2)^{-1}\cdot(1+\theta+\theta^2)=1=1+0\theta+0\theta^2$, luego

$(a+b\theta+c\theta^2)\ (1+\theta+\theta^2)=1$

$a+a\theta+a\theta^2+b\theta+b\theta^2+b\theta^3+c\theta^2+c\theta^2+c\theta^3+b\theta^4=1$, luego

$a + a\theta + a\theta^2 + b\theta^2 + 2b + c\theta^2 + 2c + 2c\theta = 1$

Como $\{1, \theta, \theta^2\}$ es linealmente independiente (por Teorema 2.4)

$$\left.\begin{array}{rcl} a + 2b + 2c & = & 1 \\ a + b + 2c & = & 0 \\ a + b + c & = & 0 \end{array}\right\} \Longrightarrow c = 0.$$

Se sigue que,

$$\left.\begin{array}{rcl} a + 2b & = & 1 \\ a + b & = & 0 \end{array}\right\} \Longrightarrow \begin{array}{rcl} b & = & 1 \\ a & = & -1 \end{array}$$

Por lo tanto, $(1 + \theta + \theta^2)^{-1} = -1 + \theta$.

Veamos la demostración del Teorema 2.4.

Demostración. i) Por Observación 2.5 el conjunto del enunciado es conjunto generador de K.

ii) Veamos si $\{1_k, \theta, \ldots, \theta^{n-1}\}$ es linealmente independiente sobre F. Supongamos que es linealmente dependiente sobre F. Entonces, existen $b_0, \ldots, b_{n-1} \in F$ no todos nulos tales que $b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1} = 0_K = \langle P \rangle$. Reescribiendo queda

$b_0 + b_1\bar{x} \ldots + b_{n-1}\bar{x}^{n-1} = 0 + \langle P \rangle$, luego $b_0 + b_1x + \ldots + b_{n-1}x^{n-1} + \langle P \rangle = \langle P \rangle$, y se sigue que $b_0 + b_1x + \ldots + b_{n-1}x^{n-1} \in \langle P \rangle$. Concluimos que $b_0 + b_1x + \ldots + b_{n-1}x^{n-1} = QP$ con Q polinomio en $F[x]$. Como $gr(P)) = n$ tenemos una contradicción y se tiene que $\{1_K, \theta, \ldots, \theta^{n-1}\}$ es linealmente independiente sobre F y entonces $\{1_K, \theta, \ldots, \theta^{n-1}\}$ es base de K sobre F. Por lo tanto, $dim_F(K) = n$.

□

2.2. Extensiones de cuerpos

Ya vimos que la única comparación interesante que podemos hacer entre cuerpos es inyectando unos dentro de otros. Es por esto que la nomenclatura clásica de subcuerpo es reemplazada en este marco por una nueva definición.

Definición 2.6. *Sea L un cuerpo y K un subcuerpo de L. Decimos entonces que L es una extensión de K y anotamos L/K (léase "L sobre K"), o $K \subset L$, o a veces también*

$$\begin{array}{c} L \\ | \\ K. \end{array}$$

Observación 2.7. *Ojo, la notación que acabamos de definir no debe ser confundida con un cociente ya que, como ya vimos, no existen cocientes interesantes de cuerpos. El símbolo "/" seguirá denotando sin embargo un cociente cuando tratemos con anillos de polinomios y sus cuerpos cocientes.*

La gran mayoría de las extensiones que estudiaremos son como la que construimos en la sección precedente. Como vimos, éstas correspondían a un espacio vectorial sobre el subcuerpo. Esto es un hecho general para las extensiones de cuerpo: en efecto, dada una extensión L/K, L es claramente un K-módulo bajo la acción de suma y multiplicación evidentes, lo que hace de L un K-espacio vectorial.

Definición 2.7. *Sea K un cuerpo y L una extensión de K. Definimos el* grado *de la extensión L/K, anotado $[L : K]$, como la dimensión sobre K de L, es decir como $\dim_K(L)$. Si $[L : K]$ es finito, decimos que la extensión es finita, de lo contrario decimos que es infinita.*

Observación 2.8. *Cada cuerpo puede considerarse como espacio vectorial sobre su cuerpo primo.*

El hecho que el grado sea definido como una dimensión de espacios vectoriales hace que éste goce de ciertas propiedades interesantes, como la siguiente:

Teorema 2.5. *Sean $M/L/K$ extensiones de cuerpos. Entonces M/K es finita si y solo si M/L y L/K lo son. Y en ese caso tenemos*

$$[M : K] = [M : L][L : K].$$

Demostración. Si M/K es finita, entonces L es un sub-K-espacio vectorial de M y es por ende de dimensión finita. Además, una K-base de M es claramente un conjunto generador de M como L-espacio vectorial, por lo que M/L también es finita.

Supongamos ahora que M/L y L/K son finitas de grados respectivos $[M : L] = m$ y $[L : K] = n$. Sean $\{\alpha_1, \ldots, \alpha_m\}$ y $\{\beta_1, \ldots, \beta_n\}$ respectivamente una L-base de M y una K-base de L. Demostraremos que el conjunto

$$\{\alpha_i\beta_j \mid 1 \leq i \leq m,\, 1 \leq j \leq n\},$$

es una K-base de M.

Consideremos entonces un elemento arbitrario $x \in M$. Como los α_i forman una L-base, existen *únicos* $a_1, \ldots, a_m \in L$ tales que $x = \sum_{i=1}^{m} a_i\alpha_i$. Ahora, para cada $a_i \in L$, existen *únicos* $b_{i,j} \in K$ tales que $a_i = \sum_{j=1}^{n} b_{i,j}\beta_j$ ya que los β_j son una K-base de L. Tenemos entonces que

$$x = \sum_{i=1}^{m} a_i\alpha_i = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{i,j}\beta_j\alpha_i = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{i,j}(\alpha_i\beta_j),$$

donde los $b_{i,j} \in K$ son únicos. Esto prueba que los $\alpha_i\beta_j$ forman una K-base de M. □

Si uno de los lados de la igualdad del teorema anterior es infinito, el otro también lo es. Más aún tenemos

i) Si $[M : L]$ es infinita, entonces existen infinitos elementos de M que son linealmente independientes sobre L, . Luego existen infinitos elementos de M que son linealmente independientes sobre K. Por lo tanto, $[M : K]$ es infinito.

ii) Si $[L : K]$ es infinito. Entonces, existe base $\{\delta_i\}$ infinita de L sobre K. Por lo tanto, no puede haber base finita de M sobre K.

iii) Si $[M : K]$ es infinito, entonces $[M : L]$ o $[L : K]$ es infinito, pues de lo contrario $[M : K]$ seria finita.

Recordemos ahora la noción de "anillo generado por un conjunto" en el marco de cuerpos.

Definición 2.8. *Sea K un cuerpo, L/K una extensión y $\alpha_1, \ldots, \alpha_n \in L$. Definimos el* subcuerpo generado por $\alpha_1, \ldots, \alpha_n$ *como el menor subcuerpo de L que contiene a K y a $\alpha_1, \ldots, \alpha_n$. Denotamos este cuerpo por $K(\alpha_1, \ldots, \alpha_n)$.*

Si L/K es una extensión tal que $L = K(\alpha)$ para algún $\alpha \in L$, decimos entonces que L/K es una extensión simple *de K. En este caso, llamamos a α un* elemento primitivo.

Ejemplo 2.6. *Sea K un cuerpo y sea P un polinomio irreducible. Entonces el cuerpo $L = K[x]/\langle P\rangle$ del Teorema 2.3 es generado por $\alpha = \bar{x}$. En efecto, todo cuerpo que contiene a α y a K debe contener a $\alpha^2, \ldots, \alpha^{n-1}$ y por ende a las combinaciones K-lineales de éstos elementos, las cuales generan ya todo el cuerpo L.*

Este fenómeno es más general de lo que parece. Con el siguiente teorema demostraremos en efecto que la construcción del Teorema 2.3 aparece dentro de extensiones abstractas de la forma más natural.

Teorema 2.6. *Sea K un cuerpo, L/K una extensión y $P \in K[x]$ un polinomio irreducible. Supongamos que existe $\alpha \in L$ tal que $P(\alpha) = 0$. Entonces*

$$K(\alpha) \simeq K[x]/\langle P\rangle.$$

Observación 2.9. *Este Teorema nos dice de hecho que* todo *cuerpo que contiene una raíz de P posee un subcuerpo isomorfo al construido en el Teorema 2.3 y que éste último es por ende el cuerpo más pequeño que posee una tal raíz, salvo isomorfismo.*

Demostración del Teorema 2.6. Consideremos el homomorfismo de anillos

$$\varphi : K[x] \to K(\alpha) \subset L,$$
$$Q \mapsto Q(\alpha).$$

Verificar que se trata de un homomorfismo de anillos es un simple ejercicio. Ahora, por definición de α, vemos que $P \in \ker(\varphi)$, por lo que $\langle P\rangle \subset \ker(\varphi)$. Pero el ideal $\langle P\rangle$ es maximal ya que P es irreducible. Esto nos dice que o bien $\ker(\varphi) = K[x]$ o $\ker(\varphi) = \langle P\rangle$. La primera opción no es posible sin embargo ya que la restricción de φ a K corresponde claramente a la identidad y no al homomorfismo nulo. Tenemos pues que $\ker(\varphi) = \langle P\rangle$ y por ende

$$K[x]/\langle P\rangle = K[x]/\ker(\varphi) \simeq \mathrm{im}(\varphi) = K(\alpha),$$

lo que prueba el teorema. Para ver la última igualdad, basta con notar que $\text{im}(\varphi)$ contiene a K y contiene a $\alpha = \varphi(x)$, por lo que contiene a $K(\alpha)$ por definición de éste. □

Ejemplo 2.7. *Sea* $F = \mathbb{Q}(\sqrt[n]{2})$ *el menor subcuerpo de* $\mathbb{R}$ *que contiene a* $\mathbb{Q}$ *y* $\sqrt[n]{2}$*. Demuestre que* $F = \{a_0 + a_1\sqrt[n]{2} + \cdots + a_{n-1}\sqrt[n]{2^{n-1}} : a_i \in \mathbb{Q}\}$*. Determine* $[F : \mathbb{Q}] = dim_{\mathbb{Q}}F$*.*

Solución: Sea $X = \{a_0 + a_1\sqrt[n]{2} + \cdots + a_{n-1}\sqrt[n]{2^{n-1}} : a_i \in \mathbb{Q}\}$. Como $\sqrt[n]{2} \in L$, es facil demostra que $X \subset L$. Luego, para demostrar que $L = X$, basta demostra que X es un cuerpo. Esto ya que, como $\sqrt[n]{2} \in X$ y $\mathbb{Q} \subset X$ se tiene que $X \supset L$. En lo que sigue demostraremos que X es un cuerpo. Sea $\phi : \mathbb{Q}[x] \to X$ el homomorfismo de anillos definido por $\phi(x) = \sqrt[n]{2}$. Claramente ϕ es sobreyectivo y $P(x) = x^2 - 2 \in \ker(\phi)$. Note que por criterio de Einsentein, se tiene que P es irreducible. Dado que $\mathbb{Q}[x]$ es un DIP, podemos suponer que $\ker(\phi) = \langle S\rangle$. Entonces $P(x) = S(x)T(x)$, para cierto $T \in \mathbb{Q}[x]$. Como P es irreducible, tenemos que $T \in \mathbb{Q}$ y en particular $\langle P\rangle = \ker(\phi)$. Concluimos que $X \cong \mathbb{Q}[x]/\langle P\rangle$ es un cuerpo. Para calcular $[F : \mathbb{Q}]$ note que $\{1, \sqrt[n]{2}, \cdots, \sqrt[n]{2^{n-1}}\}$ es una base de X como $\mathbb{Q}$ espacio vectorial. Esto pues claramente genera el espacio y sus elementos son linealmente independientes, debido a que si no, existiría un polinomio de grado menor que P que se anula en $\sqrt[n]{2}$, lo que contradice el hecho de que $\ker(\phi) = \langle P\rangle$. Se sigue que $[F : \mathbb{Q}] = \dim_{\mathbb{Q}}F = n$.

Ejercicio 2.1. *Sea* $F = \mathbb{Q}$*,* P *polinomio en* $\mathbb{Q}[x]$*, donde* $P(x) = 3x^2 + 5x + 10$*. Pruebe que* P *es irreducible en* $\mathbb{Q}[x]$ *y si* θ *es una raíz de* P*. Encuentre* $(1 - \theta)^2 + (7 + \theta)^{-1}$*.*

Del Teorema 2.6 deducimos inmediatamente el siguiente corolario.

Corolario 2.1. *Sea* K *un cuerpo,* L/K *una extensión y* $P \in K[x]$ *un polinomio irreducible* de grado n*. Supongamos que existe* $\alpha \in L$ *tal que* $P(\alpha) = 0$*. Entonces*

$$K(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\} \subset L.$$

Veamos ahora la transitividad de estas definiciones.

Lema 2.3. *Sea* L/K *una extensión de cuerpos y sean* $\alpha, \beta \in L$*. Entonces* $K(\alpha, \beta) = K(\alpha)(\beta)$*.*

Demostración. Por definición, $K(\alpha)(\beta)$ es el menor subcuerpo que contiene a $K(\alpha)$ y a β. Por lo tanto, $K(\alpha)(\beta)$ contiene a K, a α y a β, por lo que $K(\alpha,\beta) \subset K(\alpha)(\beta)$ ya que $K(\alpha,\beta)$ es el menor cuerpo que contiene a K, a α y a β.

Por otro lado, $K(\alpha,\beta)$ contiene por definición a K y a α, por lo que $K(\alpha) \subset K(\alpha,\beta)$. Como además contiene a β, vemos que $K(\alpha)(\beta) \subset K(\alpha,\beta)$, lo que concluye la demostración. □

Observación 2.10. *Sea $K(\alpha) \cong K[x]/\langle P\rangle$, una extensión simple, donde $\langle P\rangle$ es un polinomio irreducible. Entonces $\{s(x) \in K[x] : s(\alpha) = 0\} = \langle P\rangle$.*

Ejemplo 2.8. *Sea $L = \mathbb{F}_5(\sqrt{2})$ el menor cuerpo que contiene a $\mathbb{F}_5$ y una raíz de $2 \in \mathbb{F}_5$.*

i) Muestre que L es una extensión cuadrática de $\mathbb{F}_5$.

ii) Pruebe que x^2+2 se descompone en $L[x]$.

Solución i) Sabemos que $L \simeq \mathbb{F}_5[x]/(p(x))$, para cierto polinomio irreducible $p(x) \in \mathbb{F}_2[x]$ tal que $p(\sqrt{2}) = 0$. Por definición, x^2-2 se anula en $\sqrt{2}$. Por lo tanto, si demostramos que x^2-2 es irreducible en $\mathbb{F}_5[x]$, tenemos que $[L : \mathbb{F}_5] = \deg(x^2-2) = 2$. Observe que $\mathbb{F}_5^2 = \{0, 1, -1\}$. Por lo tanto x^2-2 no tiene raíces en $\mathbb{F}_5$. Esto implica que x^2-2 es irreducible sobre $\mathbb{F}_5[x]$.

ii) Note que $(2\sqrt{2})^2 = 8 = -2$ en L. Por lo tanto $x^2+2 = (x-2\sqrt{2})(x+2\sqrt{2})$ en $L[x]$.

Ejemplo 2.9. *Sea $w = e^{\frac{2\pi i}{3}}$ raíz cúbica de la unidad y considere el cuerpo $L = \mathbb{Q}(\sqrt[3]{2}, w)$.*

i). Pruebe que $[L : \mathbb{Q}] = 6$.

ii). Muestre que $\sqrt[3]{2} \notin L$, para todo $L = \mathbb{Q}(\theta_1, \cdots, \theta_n)$, donde $\theta_i^2 \in \mathbb{Q}$.

Solución: i). Sabemos que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3-2) = 3$. Por la multiplicatividad del grado, para probar lo pedido, basta demostrar que $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$. En efecto, sabemos que $Q(x) = x^2+x+1$ es un polinomio que se anula en w. Por otro lado, sabemos que $L \cong \mathbb{Q}(\sqrt[3]{2})[x]/\langle P\rangle$, donde P es un polinomio irreducible. La observación anterior implica que P divide a x^2+x+1. Por lo tanto $[L : \mathbb{Q}(\sqrt[3]{2})] \leq 2$. Si $[L : \mathbb{Q}(\sqrt[3]{2})] = 1$, entonces el

cuerpo $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ conincide con L, el cual contiene el elemento no real, a saber $w \in L$. Esto implica que $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$ y se concluye lo pedido.

ii). Definimos $L_i = \mathbb{Q}(\theta_1, \cdots, \theta_i)$, para $i \in \{1, \cdots n\}$. Note que $L_{i+1} = L_i(\theta_{i+1})$, donde $\theta_{i+1}^2 \in L_i$. Por lo tanto $[L_{i+1} : L_i] \in \{1, 2\}$. Esto implica que $[L : \mathbb{Q}] = 2^t$, para cierto $t \leq n$. Luego, si $\sqrt[3]{2} \in L$, se tiene que $\mathbb{Q}(\sqrt[3]{2}) \subset L$, por lo que 3 divide a 2^t. Esto nos lleva a una contradicción.

El siguiente corolario se demuestra fácilmente por inducción.

Corolario 2.2. *Sea L/K una extensión de cuerpos y sean $\alpha_1, \ldots, \alpha_n \in L$. Entonces*

$$K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1)(\alpha_2) \ldots (\alpha_n)$$

.

Definición 2.9. *Una extensión L/K es* finitamente generada *si existen elementos $\alpha_1, \ldots, \alpha_n \in L$ tales que $L = K(\alpha_1, \ldots, \alpha_n)$.*

Terminemos esta sección mostrando que todas estas construcciones son invariantes si cambiamos los cuerpos por cuerpos isomorfos. Notemos entonces que, dado un homomorfismo (forzosamente inyectivo) de cuerpos $\varphi : K \to L$, tenemos un homomorfismo natural de anillos (también inyectivo)

$$\begin{aligned} &\psi : K[x] \to L[x], \\ &\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \varphi(a_i) x^i. \end{aligned}$$

Es fácil ver además que ψ es un isomorfismo si φ lo es. Un tal isomorfismo envía claramente polinomios irreducibles a polinomios irreducibles.

Proposición 2.2. *Sea $\varphi : K \to L$ un isomorfismo de cuerpos. Sea α una raíz del polinomio irreducible $P \in K[x]$ en alguna extensión de K. Sea Q la imagen de P en $L[x]$ y sea β una raíz de Q en alguna extensión de L. Entonces existe un isomorfismo de cuerpos $\sigma : K(\alpha) \to L(\beta)$ tal que $\sigma|_K = \varphi$, es decir, σ extiende φ.*

Demostración. Consideremos el isomorfismo $\psi : K[x] \to L[x]$ de más arriba que envía P a Q y notemos que $\psi|_K = \varphi$. Si lo componemos con la proyección canónica $\pi : L[x] \to L[x]/\langle Q\rangle$ y luego con el isomorfismo $\theta : L[x]/\langle Q\rangle \to L(\beta)$, obtenemos un homomorfismo de anillos epiyectivo

$$\theta \circ \pi \circ \psi : K[x] \to L(\beta),$$

ya que los tres homomorfismos son epiyectivos. Ahora, como ψ y θ son isomorfismos y $\ker(\pi) = \langle Q\rangle$, tenemos que

$$\begin{aligned}
\ker(\theta \circ \pi \circ \psi) &= (\theta \circ \pi \circ \psi)^{-1}(0) \\
&= \psi^{-1}(\pi^{-1}(\psi^{-1}(0))) \\
&= \psi^{-1}(\pi^{-1}(\ker(\psi))) \\
&= \psi^{-1}(\pi^{-1}(0)) \\
&= \psi^{-1}(\ker(\pi)) \\
&= \psi^{-1}(\langle Q\rangle) \\
&= \langle P\rangle.
\end{aligned}$$

Además, como $\pi|_L = \mathrm{id}_L$ y $\theta|_L = \mathrm{id}_L$, vemos que $(\theta \circ \pi \circ \psi)|_K = \varphi$. Por el teorema de isomorfismo deducimos entonces que $\theta \circ \pi \circ \psi$ induce un isomorfismo $\xi : K[x]/\langle P\rangle \to L(\beta)$ cuya restricción a $K \subset K[x]/\langle P\rangle$ es φ. Componiendo con el isomorfismo $K(\alpha) \simeq K[x]/\langle P\rangle$, cuya restricción a K es claramente la identidad, tenemos el isomorfismo deseado. □

2.3. Extensiones Algebraicas

La extensión de cuerpos $\mathbb{C}/\mathbb{Q}$ nos ofrece dos tipos de elementos del cuerpo $\mathbb{C}$ que no están en $\mathbb{Q}$. Aquellos que se pueden obtener como raíz de un polinomio con coeficientes en $\mathbb{Q}$, como i ó $\sqrt{2}$, llamados números *algebraicos*; y aquellos que no pueden ser obtenidos de esta manera, como π o e, llamados números *trascendentes*. La noción de extensión algebraica generaliza este ejemplo particular.

Definición 2.10. *Sea L/K una extensión de cuerpos. Un elemento $\alpha \in L$ se dice* algebraico sobre K *si α es raíz de un polinomio no nulo $P \in K[x]$. Un elemento que no es algebraico sobre K se dice* trascendente *sobre K.*

Observación 2.11. *La demostración de que un número es trascendente no es fácil. Por ejemplo Hermite en 1873 dió la primera demostración de la trascendencia de e. Para π, esto fue demostrado por primera vez por Lambert en 1766. Véase el libro* Proofs from The Book *de Aigner y Ziegler para una linda demostración de estas (y más) trascendencias.*

Observación 2.12. *Todo elemento $\alpha \in K$ es algebraico sobre K ya que es raíz del polinomio $P(x) = x - \alpha$. En particular, π y e son algebraicos sobre $\mathbb{R}$.*
También vemos fácilmente que si $\alpha \in L$ es algebraico sobre K, entonces α es algebraico sobre cualquier cuerpo intermedio $K \subset M \subset L$.

Ejemplo 2.10. *El elemento $\alpha = \sqrt{2}$ es algebraico sobre $\mathbb{Q}$, ya que es raíz del polinomio $P(x) = x^2 - 2$. También el elemento $\alpha = \sqrt{3} + \sqrt{5}$. En efecto, α es raíz del polinomio*

$$\begin{aligned} P(x) &= (x + \sqrt{3} + \sqrt{5})(x + \sqrt{3} - \sqrt{5})(x - \sqrt{3} + \sqrt{5})(x - \sqrt{3} - \sqrt{5}) \\ &= ((x + \sqrt{3})^2 - \sqrt{5}^2)((x - \sqrt{3})^2 - \sqrt{5}^2) \\ &= (x^2 + 3 + 2x\sqrt{3} - 5)(x^2 + 3 - 2x\sqrt{3} - 5) \\ &= (x^2 - 2 + 2x\sqrt{3})(x^2 - 2 - 2x\sqrt{3}) \\ &= (x^2 - 2)^2 - (2x\sqrt{3})^2 \\ &= x^4 - 4x^2 + 4 - 12x^2 \\ &= x^4 - 16x^2 + 4 \in \mathbb{Q}[x]. \end{aligned}$$

A priori, dado un elemento $\alpha \in L$ algebraico sobre $K \subset L$, pueden haber muchos polinomios $P \in K[x]$ para los cuales α es raíz. Basta de hecho con tomar uno de ellos y considerar todos sus múltiplos en el anillo $K[x]$. Ahora, existe uno que es más importante que todos los otros.

Proposición 2.3. *Sea L/K una extensión de cuerpos y sea $\alpha \in L$ un elemento algebraico sobre K. Entonces existe un* único *polinomio mónico irreducible $m_{\alpha,K} \in K[x]$ tal que α es*

raíz de $m_{\alpha,K}$. Además, $m_{\alpha,K}$ es el polinomio mónico de menor grado en $K[x]$ del cual α es una raíz y todo otro tal polinomio es un múltiplo de éste.

Demostración. Consideremos el homomorfismo de evaluación $\varphi : K[x] \to L$ definido por $\varphi(p) = p(\alpha)$. Como $K[x]$ es un DIP, el núcleo de φ está generado por un polinomio $m_{\alpha,K}$ que podemos suponer mónico. Como $K[x]/(m_{\alpha,K}) \cong \varphi(K[x]) \subseteq L$ y L es un cuerpo, sabemos que $m_{\alpha,K}$ es irreducible. Si $p(x) \in K[x]$ es tal que $p(\alpha) = 0$, entonces $p \in \ker(\varphi)$ por lo que $p(x)$ es divisible por $m_{\alpha,K}$. Esto demuestra además la minimalidad del grado de $m_{\alpha,K}$ y su unicidad. □

Definición 2.11. *Sea L/K una extensión de cuerpos y sea $\alpha \in L$ un elemento algebraico sobre K. El polinomio $m_{\alpha,K}$ de la última proposición se llama el* polinomio minimal de α. *Definimos el* grado de α *como el grado de su polinomio minimal.*

De la segunda afirmación de la Proposición 2.3 deducimos inmediatamente el siguiente corolario.

Corolario 2.3. *Sean $K \subset L \subset M$ extensiones de cuerpos y sea $\alpha \in M$ un elemento algebraico sobre K. Entonces α es algebraico sobre L y $m_{\alpha,L}$ divide a $m_{\alpha,K}$ en $L[x]$.*

Demostración. La primera afirmación fue observada un poco más arriba. La segunda es una consecuencia directa de la segunda parte de la Proposición 2.3. □

Otro corolario interesante para encontrar polinomios minimales es el siguiente:

Corolario 2.4. *Sea L/K una extensión de cuerpos, sea $\alpha \in L$ un elemento algebraico sobre K y sea $P \in K[x]$ tal que $P(\alpha) = 0$. Entonces $P = m_{\alpha,K}$ si y solo si P es mónico e irreducible en $K[x]$.*

Ejemplo 2.11. *$\sqrt{2}$ es algebraico de grado 2 sobre $\mathbb{Q}$ ya que $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$ y éste polinomio es irreducible en $\mathbb{Q}[x]$. Sin embargo, $\sqrt{2}$ es de grado 1 sobre $\mathbb{R}$ ya que $m_{\sqrt{2},\mathbb{R}} = x - \sqrt{2}$.*

Ejercicio 2.2. *Pruebe que $\alpha = \sqrt{3} + \sqrt{5}$ es algebraico sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt{5})$ de grados respectivos 4, 2 y 2.*

Recordemos ahora el Teorema 2.6 y su Corolario 2.1. A la luz de estas nuevas definiciones y resultados, obtenemos inmediatemante lo siguiente:

Teorema 2.7. *Sea L/K una extensión de cuerpos. Sea $\alpha \in L$ un elemento algebraico sobre K. Entonces*

$$K[x]/\langle m_{\alpha,K} \rangle \cong K(\alpha) \subset L,$$

y por lo tanto

$$[K(\alpha) : K] = \deg(m_{\alpha,K}).$$

Demostración. Ejercicio ☺ □

Visto este teorema, deducimos inmediatamente que toda extensión generada por un elemento algebraico α es finita ya que su dimensión es igual al grado del polinomio minimal de α. Esto admita un resultado recíproco.

Proposición 2.4. *Sea L/K una extensión de cuerpos y sea $\alpha \in L$. Entonces α es algebraico sobre K si y solo si $K(\alpha)$ es una extensión finita de K.*

Demostración. Como ya vimos, si α es algebraico, entonces $[K(\alpha) : K] = \deg(m_{\alpha,K}) < \infty$. Veamos entonces el caso opuesto. Sea $\alpha \in L$ y supongamos que $[K(\alpha) : K] = n < \infty$. Entonces la familia de $n+1$ elementos $1, \alpha, \alpha^2, \ldots, \alpha^n \in K(\alpha)$ es K-linealmente dependiente y por ende existe una combinación K-lineal no trivial de estos elementos que es nula. Es decir, existen $a_0, a_1, \ldots, a_n \in K$, no todos nulos, tales que

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Esto nos dice que el polinomio no nulo $P(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ es tal que $P(\alpha) = 0$, lo que prueba que α es algebraico. □

Ejemplo 2.12. *Retomemos algunas extensiones ya vistas:*

1. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$,

2. $[\mathbb{R}(\pi) : \mathbb{R}] = 1$ *(en general,* $[L : K] = 1 \Leftrightarrow L = K$*)*

3. $[\mathbb{C} : \mathbb{R}] = 2$, *ya que* $\mathbb{C} = \mathbb{R}(i)$ *y* $m_{i,\mathbb{R}}(x) = x^2 + 1$.

Ejercicio 2.3. *Pruebe que* $\sqrt{15} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$ *y que* $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{15})] = 2$.

Todos estos ejemplos son casos de extensiones algebraicas.

Definición 2.12. *Decimos que* L *es una* extensión algebraica *de* K *si todo elemento de* L *es algebraico sobre* K.

Observación 2.13. *Atención. Esta noción es más general que las extensiones del tipo* $K(\alpha_1, \ldots, \alpha_n)/K$. *En efecto, todas éstas son de dimensión finita (véase un poco más abajo), mientras que existen extensiones algebraicas de dimensión infinita, como veremos más adelante.*

Contentémonos por ahora con demostrar la afirmación contrapuesta, que es un fácil corolario de la Proposición 2.4.

Proposición 2.5. *Toda extensión finita* L/K *es algebraica.*

Demostración. Debemos demostrar que todo elemento $\alpha \in L$ es algebraico sobre K. Ahora, como $\alpha \in L$ y $K \subset L$, tenemos que $K(\alpha) \subset L$. El Teorema 2.5 nos dice entonces que $K(\alpha)/K$ es finita y por ende α es algebraico sobre K por la Proposición 2.4. □

Demostremos ahora lo que mencionábamos en la última observación.

Proposición 2.6. *Sea* L/K *una extensión de cuerpos y sean* $\alpha, \beta \in L$ *elementos algebraicos sobre* K. *Entonces* $K(\alpha, \beta)$ *es finita y por ende algebraica sobre* K.

Demostración. Tenemos la torre de cuerpos

$$\begin{array}{c} K(\alpha, \beta) \\ | \\ K(\alpha) \\ | \\ K. \end{array}$$

Ahora, como α es algebraico, la extensión $K(\alpha)/K$ es de dimensión finita. Por otra parte, como β es algebraico sobre K, también lo es sobre $K(\alpha)$. Recordando entonces que $K(\alpha,\beta) = K(\alpha)(\beta)$, vemos que la extensión $K(\alpha,\beta)/K(\alpha)$ es finita por el mismo argumento. El Teorema 2.5 nos dice entonces que $K(\alpha,\beta)/K$ es finita de dimensión igual a $[K(\alpha,\beta) : K(\alpha)][K(\alpha) : K]$. □

Tenemos los siguientes corolarios inocentes de esta última proposición.

Corolario 2.5. *Sea L/K una extensión de cuerpos y sean $\alpha_1, \ldots, \alpha_n \in L$ elementos algebraicos sobre K. Entonces $K(\alpha_1, \ldots, \alpha_n)$ es finita y por ende algebraica sobre K.*

Demostración. Esto se demuestra por inducción sobre n a partir de la proposición. □

Corolario 2.6. *Sea L/K una extensión de cuerpos y sean $\alpha, \beta \in L$ elementos no nulos algebraicos sobre K. Entonces $\alpha \pm \beta$, $\alpha\beta$ y α/β son algebraicos sobre K.*

Demostración. En efecto, $K(\alpha,\beta)$ contiene a $\alpha \pm \beta$, $\alpha\beta$ y α/β y ya probamos que $K(\alpha,\beta)/K$ es algebraica. □

Ejercicio 2.4. *Pruebe que $[\mathbb{Q}(\sqrt{3})(\sqrt{5}) : \mathbb{Q}] = 4$ y encuentre una base de $\mathbb{Q}(\sqrt{3})(\sqrt{5})$ sobre $\mathbb{Q}$.*

Un corolario harto menos inocente es el siguiente.

Corolario 2.7. *Sea L/K una extensión de cuerpos. Entonces el subconjunto*

$$A := \{\alpha \in L \mid \alpha \text{ algebraico sobre } K\},$$

es un subcuerpo de L. □

En otras palabras, si α es la raíz de un polinomio en $K[x]$ y β es la raíz de otro polinomio en $K[x]$, entonces su suma, producto y cociente también son raíces de *algún* polinomio en $K[x]$. Esto no es nada de evidente *a priori*. De hecho, encontrar estos polinomios puede ser muy difícil en general.

Ejercicio 2.5. *Sean $K = \mathbb{Q}$, $\alpha = \sqrt{2}$ y $\beta = \sqrt{3} + 1$. Encuentre $m_{\alpha+\beta,\mathbb{Q}}$, $m_{\alpha-\beta,\mathbb{Q}}$, $m_{\alpha\beta,\mathbb{Q}}$ y $m_{\alpha/\beta,\mathbb{Q}}$. Hint: Mire cómo encontramos el polinomio minimal en los ejemplos más arriba.*

Ahora ya podemos caracterizar las extensiones finitas:

Teorema 2.8. *Una extensión L/K es finita si y solo si $L = K(\alpha_1, \ldots, \alpha_m)$ con $\alpha_1, \ldots, \alpha_m \in L$ elementos algebraicos sobre K. Es decir, una extensión L/K es finita si y solo si es algebraica y finitamente generada.*

Demostración. Acabamos de ver que $K(\alpha_1, \ldots, \alpha_m)$ es finita si cada uno de los α_i es algebraico sobre K.

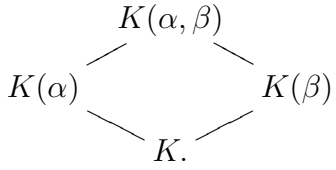
Por otra parte, si L/K es finita, entonces es finitamente generada (por los elementos de una base como K-espacio vectorial) y es algebraica.

Para el otro, ya vimos que toda extensión finita es algebraica, por lo que bastará con demostrar que es finitamente generada. Demostraremos esto por inducción sobre $n = [L : K]$. Si $n = 1$, entonces $L = K$ y la afirmación es por ende evidente. Si $n > 1$, nuestra hipótesis de inducción es que el teorema es válido para toda extensión de grado menor que n. Ahora, sea $\alpha_1 \in L \setminus K$. Entonces $K \subsetneq K(\alpha_1) \subset L$, por lo que $n = [L : K(\alpha_1)][K(\alpha_1) : K]$ y $[K(\alpha_1) : K] > 1$. Esto nos dice que $[L : K(\alpha_1)] < n$ y por ende, por hipótesis de inducción, existen $\alpha_2, \ldots, \alpha_m \in L$ algebraicos sobre $K(\alpha_1)$ tales que $L = K(\alpha_1)(\alpha_2, \ldots, \alpha_m) = K(\alpha_1, \ldots, \alpha_m)$, lo que concluye la demostración. □

Estudiemos ahora un caso particular de extensión generada por dos elementos.

Lema 2.4. *Sea L/K una extensión y sean $\alpha, \beta \in L$ elementos algebraicos sobre K. Sean $m = [K(\alpha) : F]$ y $n = [K(\beta) : F]$ y supongamos que $(m, n) = 1$. Entonces $[K(\alpha, \beta) : K(\alpha)] = n$, $[K(\alpha, \beta) : K(\beta)] = m$ y $[K(\alpha, \beta) : K] = mn$.*

Demostración. Consideremos la torre de cuerpos



Sea $t = [K(\alpha, \beta) : K(\alpha)] = \deg(m_{\beta,K(\alpha)})$. Tenemos entonces que

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : F] = tm.$$

Bastará entonces con probar que $t = n$. El caso de $[K(\alpha, \beta) : K(\beta)] = m$ se demuestra de la misma manera intercambiando α y β.

Como $K \subset K(\beta) \subset K(\alpha, \beta)$, tenemos que $n|mt$. Pero $(m, n) = 1$, por lo que $n|t$. Ahora, $n = [K(\beta) : K]$ es también el grado de $m_{\beta,K}$ y, por el Corolario 2.3, tenemos que $m_{\beta,K(\alpha)}$ divide a $m_{\beta,K}$. Esto nos dice que

$$t = [K(\alpha, \beta) : K(\alpha)] = \deg(m_{\beta,K(\alpha)}) \leq \deg(m_{\beta,K}) = n,$$

por lo que obtenemos que $n = t$, lo que concluye la demostración. □

Observación 2.14. *De la demostración deducimos también lo siguiente: Sea L/K una extensión y sean $\alpha, \beta \in L$ elementos algebraicos sobre K. Sean $m = [K(\alpha) : K]$ y $n = [K(\beta) : K]$. Si $(m, n) \neq 1$, todavía podemos deducir que $t \leq n$ y por ende $[K(\alpha, \beta) : K] = mt \leq mn$.*

Esto es un caso particular del composito *de dos extensiones de cuerpos (aquí, $K(\alpha)/K$ y $K(\beta)/K$). En general, dada una extensión L/K y dos subextensiones M/K y N/K, se define el composito $MN \subset L$ de M y N como el subcuerpo más pequeño de L que contiene a M y a N.*

Ejercicio 2.6. *Pruebe que, en particular, los elementos $\alpha^i \beta^j$ con $0 \leq i \leq m-1$ y $0 \leq j \leq n-1$ forman un conjunto generador del K-espacio vectorial $K(\alpha, \beta)$, que es una base si $(m, n) = 1$. (Esto también se puede generalizar para exhibir un conjunto generador de un composito MN/K como K-espacio vectorial).*

Analicemos ahora el caso particular de las extensiones cuadráticas (i.e. de grado 2). Para un cuerpo K, notemos $(K^*)^2$ el conjunto de los cuadrados no nulos en K.

Ejemplo 2.13. *Sea K un cuerpo de característica distinta de 2. Entonces una extensión L/K es de grado 2 si y solo si $L = K(\sqrt{D})$ para algún $D \in K^* \setminus (K^*)^2$.*

En efecto, el Teorema 2.7 nos dice que $[K(\sqrt{D}) : K] = 2$ *ya que el polinomio* $m_{\sqrt{D},K}$ *es claramente* $x^2 - D$ *si* D *no es un cuadrado en* K*. Por otra parte, sea* L/K *una extensión de grado 2 y sea* $\alpha \in L \setminus K$*. Como* $[L : K] = 2$*, los elementos* $1, \alpha, \alpha^2$ *son* K*-linealmente dependientes, lo que nos dice que existen* $a, b, c \in K$ *no todos nulos tales que* $a\alpha^2 + b\alpha + c = 0$*. Ahora, si* $a = 0$*, entonces* $\alpha = -\frac{c}{b} \in K$*, lo que contradice nuestra hipótesis sobre* α*. Por ende,* $a \neq 0$ *y entonces el polinomio* $ax^2 + bx + c$ *es de grado 2 y tiene a* α *como raíz. Esto nos dice que*

$$\alpha = \frac{-b \pm \sqrt{D}}{2a}, \quad \text{donde } D = b^2 - 4ac \in K^* \setminus (K^*)^2.$$

En efecto, si D *fuese un cuadrado, entonces* $\alpha \in K$*, lo que es nuevamente una contradicción. Como ya vimos, esto nos dice que* $[K(\sqrt{D}) : K] = 2$*. Pero*

$$2 = [L : K] = [L : K(\sqrt{D})][K(\sqrt{D}) : K] = 2[L : K(\sqrt{D})],$$

y por ende $[L : K(\sqrt{D})] = 1$*, lo que nos dice que* $L = K(\sqrt{D})$*.*

Concluyamos esta sección sobre las extensiones algebraicas demostrando la transitividad de éstas.

Teorema 2.9. *Sean* L/K *y* M/L *extensiones algebraicas de cuerpos. Entonces* M/K *también es algebraica.*

Observación 2.15. *Nótese que en el caso particular de las extensiones finitas (que son todas algebraicas) esto ya fue demostrado en el Teorema 2.5.*

Demostración. Debemos mostrar que todo elemento $\alpha \in M$ es algebraico sobre K. Ahora, sabemos por hipótesis que α es algebraico sobre L, lo que nos dice que existe un polinomio $P \in L[x]$ tal que $P(\alpha) = 0$. Escribamos $P(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in L$ para $0 \leq i \leq n$ y consideremos el cuerpo $N := K(a_0, \ldots, a_n) \subset L$. El Teorema 2.8 nos dice entonces que N/K es una extensión finita. Además, vemos que $P \in N[x]$ y, como $P(\alpha) = 0$, vemos que α es algebraico sobre N. Esto nos dice que la extensión $N(\alpha)/N$ es una extensión finita y por ende la extensión $N(\alpha)/K$ también es finita. Vemos entonces que α pertenece a una

extensión finita (por ende algebraica) de K y por lo tanto se trata de un elemento algebraico sobre K. □

Observación 2.16. *Evidentemente tenemos la afirmación recíproca: si L/K y M/L son extensiones y M/K es algebraica, entonces L/K y M/L también lo son.*

2.4. Cuerpo de descomposición de un polinomio

La construcción dada en el Teorema 2.3 nos asegura que, dado un cuerpo K y un polinomio irreducible $P \in K[x]$, podemos encontrar una extensión L/K, definida por $L = K[x]/\langle P\rangle$ tal que P tiene una raíz α en L. Esto significa que, cuando miramos el polinomio P como un elemento de $L[x]$, éste es divisible por el polinomio $x-\alpha$. Una pregunta natural que uno puede hacerse entonces es ¿qué podemos decir del polinomio $Q \in L[x]$ tal que $P = (x-\alpha)Q$? Veamos algunos ejemplos sencillos:

Ejemplo 2.14.

K	P	L	α	Q *factorizado en* $L[x]$
$\mathbb{R}$	x^2+1	$\mathbb{C}$	$i=\sqrt{-1}$	$x+i$
$\mathbb{Q}$	x^2-2	$\mathbb{Q}(\sqrt{2})$	$\sqrt{2}$	$x+\sqrt{2}$
$\mathbb{Q}$	$x^4+x^3+x^2+x+1$	$\mathbb{Q}(\zeta_5)$	$\zeta_5 = e^{\frac{2\pi i}{5}}$	$(x-\zeta_5^2)(x-\zeta_5^3)(x-\zeta_5^4)$
$\mathbb{Q}$	x^4-16x^2+4	$\mathbb{Q}(\sqrt{3},\sqrt{5})$	$\sqrt{3}+\sqrt{5}$	$(x-\sqrt{3}+\sqrt{5})(x+\sqrt{3}-\sqrt{5})(x+\sqrt{3}+\sqrt{5})$
$\mathbb{F}_2$	x^3+x+1	$\mathbb{F}_8$	α	$(x+\alpha^2)(x+\alpha^2+\alpha)$

A la vista de estos ejemplos, uno podría pensar que el polinomio Q siempre se factoriza en pedazos de grado 1. En otras palabras, la extensión $L = K[x]/\langle P\rangle$ contendría todas las raíces del polinomio P. Sin embargo, esto se debe solo a que hemos tomado ejemplos muy pequeños. La realidad es en verdad otra:

Ejemplo 2.15. *Consideremos la extensión $\mathbb{R}/\mathbb{Q}$ y sea $P \in \mathbb{Q}[x]$ dado por $P(x) = x^3-2$. Entonces $\mathbb{Q}[x]/\langle P\rangle \simeq Q(\sqrt[3]{2}) \subset \mathbb{R}$. Sin embargo*

$$x^3-2 = (x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4}) \in \mathbb{Q}(\sqrt[3]{2})[x],$$

y el polinomio $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ *es irreducible en* $\mathbb{Q}(\sqrt[3]{2})$*! Para probar esto basta con ver que su discriminante es* $\Delta = \sqrt[3]{2}^2 - 4\sqrt[3]{4} = -3\sqrt[3]{4} < 0$*. Esto nos dice que las raíces de este polinomio son complejas y por lo tanto no pertenecen a* $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$*.*

Esto justifica la definición a continuación.

Definición 2.13. *Sea* L/K *una extensión de cuerpos y sea* $F \in K[x]$ *un polinomio de grado* ≥ 1*. Decimos que* L *es un* cuerpo de descomposición *de* F *si:*

1. *al ver* F *como un elemento de* $L[x]$*, éste se factoriza en un producto de factores lineales, es decir,*

$$F(x) = a(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n) \in L[x], \quad a \in L, \quad a \neq 0.$$

2. L *es el menor subcuerpo donde* F *se descompone totalmente en factores lineales.*

Observación 2.17. *El cuerpo de descomposición es el cuerpo más pequeño en el que* P *se descompone en un producto de factores lineales, lo que justifica su nombre. Siguiendo esa línea, si* P *es irreducible, el cuerpo* $K[x]/\langle P\rangle$ *es el cuerpo más pequeño tal que* P *se rompe en al menos dos factores, de los cuales uno es lineal. Por esto se le suele llamar* cuerpo de ruptura*. Nótese sin embargo que la noción de cuerpo de ruptura tiene sentido solo para polinomios irreducibles, mientras que el cuerpo de descomposición tiene sentido para todo polinomio* P *de grado* ≥ 1*.*

Ejemplo 2.16. *Demuestre que el cuerpo de descomposición de* $P(x) = x^6 - 3$ *sobre* $\mathbb{F}_5$ *tiene grado dos. Sug. Recuerde que* $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$*.*

Solución: Observe que $3 = 2^3$ en $\mathbb{F}_5$, por ende $x^6 - 3 = (x^2 - 2)(x^4 + 2x^2 + 4)$. Escribiendo $x^4 + 2x^2 + 4 = (x^2 + ax + b)(x^2 + cx + d)$ se obtiene que $a = -c = 2$ y $b = d = -2$. Por lo tanto $x^6 - 3 = (x^2 - 2)(x^2 + 2x - 2)(x^2 - 2x - 2)$. Sea θ una raíz de $x^2 - 2$ en un cuerpo que es extensión de $\mathbb{F}_5$, luego $\theta^2 = 2$. Escribimos $z = a\theta + b$. Luego si $z^2 \pm 2z - 2 = 0$, se tiene que $z = 2\theta \mp 1$ o $z = -2\theta \mp 1$. Esto implica que el cuerpo de descomposión de P es $L = \mathbb{F}_5(\theta)$, el cual sabemos tiene grado 2 sobre $\mathbb{F}_5$.

No es claro a priori que el cuerpo de descomposición de de un polinomio exista. Es por ello que demostraremos ahora su existencia.

Teorema 2.10. *Sea K un cuerpo y sea $F \in K[x]$ un polinomio de grado n. Entonces existe un cuerpo de descomposición L de F.*

Demostración. La demostración de la existencia de una extensión de K que cumple 1., será por inducción sobre $n = \deg(F)$. Supongamos primero que $n = 1$. Entonces claramente F ya es lineal en $K[x]$ y por ende $L = K$ es un cuerpo de descomposición de L (la segunda propiedad es obvia en este caso).

Sea $n > 1$ y supongamos que para todo polinomio en $K[x]$ de grado $< n$, hay extensión de K que cumple 1.

Sea $F \in K(x)$, de grado n. Si F se descompone en sólo factores de grado 1, no hay nada que demostrar.

Supongamos que hay un factor P irreducible en $K(x), gr(P) \geq 2$. Por Teorema 2.3, hay extensión K_1 de K donde P tiene una raíz α_1.(K_1 es el cuerpo de ruptura de P.) Es decir, $P(x) = (x - \alpha_1)Q_1(x)$ donde $Q_1 \in K_1[x]$. Por lo tanto,

$$F(x) = (x - \alpha_1)Q_2(x), \quad gr(Q_2) = n - 1$$

descomposición en $K_1[x]$.

Por hipótesis de inducción, hay extensión de E de K_1 donde Q_2 y por lo tanto, F se descompone totalmente en factores lineales. Luego, E contiene todas las raíces de F. Por principio de inducción completa, para cualquier polinomio de grado $n \geq 1$, hay extensión E de K que cumple 1.

Consideremos la extensión E de K construída antes. Sea ahora $L = \cap T$ donde $K \subseteq T, T$ subcuerpo de E que contiene todas las raíces de F.

Entonces L es el cuerpo de descomposición de F sobre K. □

Ejemplo 2.17. *El cuerpo de descomposición $K/\mathbb{Q}$ de $P \in \mathbb{Q}[x]$ definido por $P(x) = x^4 - 2$ es $\mathbb{Q}(\sqrt[4]{2}, i)$. En efecto, en este cuerpo tenemos que $i^a\sqrt[4]{2}$ es una raíz de P para $a = 0, 1, 2, 3$,*

por lo que

$$P(x) = x^4 - 2 = (x - \sqrt[4]{2})(x - i\sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2}) \in K[x].$$

Para probar que se trata del cuerpo más pequeño que factoriza a P de esta manera, basta con notar que tanto $\sqrt[4]{2}$ como $i\sqrt[4]{2}$ tienen que estar en K ya que ambos son raíces de P. Esto implica que $i\sqrt[4]{2}/\sqrt[4]{2} = i$ también debe estar en K. Es decir, $\mathbb{Q}(\sqrt[4]{2}, i) \subset K$.

Ejemplo 2.18. *El cuerpo de descomposición $K/\mathbb{Q}$ de $P \in \mathbb{Q}[x]$ definido por $P(x) = (x^2 - 5)(x^2 - 7)$ es $\mathbb{Q}(\sqrt{5}, \sqrt{7})$. En efecto, en este cuerpo tenemos que $\pm\sqrt{5}$ y $\pm\sqrt{7}$ son raíces de P, por lo que*

$$P(x) = x^4 - 2 = (x - \sqrt{5})(x + \sqrt{5})(x - \sqrt{7})(x + \sqrt{7}) \in K[x].$$

Para probar que se trata del cuerpo más pequeño que factoriza a P de esta manera, basta con notar que tanto $\sqrt{5}$ como $\sqrt{7}$ tienen que estar en K ya que ambos son raíces de P. Esto implica que $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \subset K$.

Ejercicio 2.7. *Determine el grado $[K : \mathbb{Q}]$ en los últimos dos ejemplos. ¿Son iguales a los grados de los cuerpos de ruptura respectivos?*

Ejemplo 2.19 (Cuerpos ciclotómicos)**.** *Un* cuerpo ciclotómico *es el cuerpo de descomposición del polinomio $x^n - 1 \in \mathbb{Q}[x]$ para algún $n \in \mathbb{N}$. Sabemos que las raíces n-ésimas de 1 en $\mathbb{C}$ son de la forma:*

$$e^{\frac{2\pi i k}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right), \qquad k = 0, \ldots, n-1.$$

Nótese que estas raíces forman un grupo cíclico para la multiplicación. En particular, si $K/\mathbb{Q}$ es un cuerpo que contiene a $e^{\frac{2\pi i}{n}}$, entonces K contiene a todas las raíces de $x^n - 1$ y por ende al cuerpo de descomposición correspondiente. Esto nos dice que un cuerpo ciclotómico es siempre de la forma $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ para algún n.

Definición 2.14. *Una* raíz primitiva *n-ésima de la unidad, es un generador del grupo cíclico de las raíces n-ésimas de 1. La denotamos por ζ_n.*

Como ya vimos, $e^{\frac{2\pi i}{n}}$ es una raíz primitiva n-ésima de la unidad, lo que nos dice que un cuerpo ciclotómico es siempre de la forma $\mathbb{Q}(\zeta_n)$ para algún n. Pero claramente no es la única. Recordando lo que sabemos de grupos cíclicos, vemos que si ζ_n es una raíz primitiva, entonces todas las otras raíces primitivas son de la forma ζ_n^a con $(a, n) = 1$.

Más adelante veremos que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, donde φ es la función de Euler, la cual cuenta los enteros a entre 0 y n que son coprimos a n. Veamos por ahora el caso particular del polinomio $x^p - 1$ con p primo. En este caso, tenemos que

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

Por lo tanto, como ζ_p es una raíz de $x^p - 1$ y $\zeta_p \neq 1$ (ya que 1 no genera el grupo), tenemos que ζ_p es una raíz de

$$\Phi_p(x) = \frac{x^{p-1}}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Q}[x].$$

Ahora, este polinomio es irreducible sobre $\mathbb{Q}$. En efecto, consideremos el polinomio

$$Q(x) := \Phi_p(x + 1) = \frac{(x + 1)^p - 1}{x + 1 - 1} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}.$$

Como p divide a $\binom{p}{i}$ para todo $1 \leq i < p$ pero $\binom{p}{p} = 1$ y $\binom{p}{1} = p$, vemos que Q verifica el criterio de Eisenstein y es por ende irreducible. Entonces Φ_p también lo es, ya que toda factorización de Φ_p induce claramente una factorización de Q. Todo esto nos prueba que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Ejercicio 2.8. *Pruebe que el cuerpo de descomposición $K/\mathbb{Q}$ de $P \in \mathbb{Q}[x]$ definido por $P(x) = x^p - 7$ es $\mathbb{Q}(\sqrt[p]{7}, \zeta_p)$ para p un número primo. Determine $[K : \mathbb{Q}]$. Hint: use el método de los ejemplos precedentes.*

Concluyamos esta sección mostrando que, al igual que los cuerpos de ruptura, los cuerpos de descomposición son invariantes si cambiamos los cuerpos de base por cuerpos isomorfos.

Observación 2.18. *Vimos en el previo a la Proposición 2.2 que todo $\varphi : K \to L$ isomorfismo de cuerpos se extiende a un isomorfismo de anillos $\psi : K[x] \to L[x]$, que lleva un polinomio $F \in K[x]$, en un polinomio $G \in L[x]$ obtenido de F al aplicar φ a los coeficientes.*

Teorema 2.11. *Sean $\varphi : K \to L$ isomorfismo de cuerpos y F, G los polinomio de la observación anterior. Sea E cuerpo de descomposición de F sobre K y M cuerpo de descomposición de G sobre L. Entonces existe $\sigma : E \longrightarrow M$ isomorfismo que extiende φ, es decir, $\sigma \mid_K = \varphi$.*

Demostración. 2.2 Como vimos antes φ se extiende a un isomorfismo de $K[x]$ en $L[x]$ y los irreducibles en $K[x]$ se van a irreducibles en $L[x]$.

Usaremos inducción sobre $n = gr(F)$.

$$\begin{aligned} n = 1 \qquad F(x) &= ax + b;\ a \neq 0,\ F(x) \in K[x] \\ G(x) &= \varphi(a)x + \varphi(b);\ \ \varphi(a) \neq 0,\ G(x) \in L[x] \end{aligned}$$

Tomando $E = K,\ M = L$ y $\sigma = \varphi$ se tiene que el Teorema vale para $n = 1$.

Supongamos que el teorema ha sido probado para cualquier cuerpo K, isomorfismo φ y polinomio en $K[x]$ de grado $< n$.

Sea $F \in K[x],\ gr(F) = n$. Si F se descompone completamente en $K[x]$, entonces G se descompone completamente en $L[x]$. Se toma $E = K,\ M = L$ y $\sigma = \varphi$.

Sea ahora F de grado n y sea P factor irreducible de F en $K[x]$ de grado ≥ 2 y sea P' el correspondiente factor irreducible de G en $L[x]$.

Sea $\alpha \in E$ raíz de P y $\beta \in M$ raíz de P', entonces $\varphi : K \longrightarrow L$ se extiende por Proposición 2.2 a $g : K(\alpha) \longrightarrow L(\beta)$ isomorfismo de cuerpos. Tenemos que

$$F(x) = (x - \alpha)F_1(x) \in K(\alpha)[x] \text{ y } G(x) = (x - \beta)G_1(x) \in L(\beta)[x]$$

Tenemos que E es el cuerpo de descomposición de F sobre K.Afirmamos que E es cuerpo de descomposición de F_1 sobre $K(\alpha)$. Supongamos que no, o sea hay $L_1 \subset E$ tal que es cuerpo de descomposición de F_1 sobre $K(\alpha)$. Como $\alpha \in K(\alpha)$ entonces L_1 contendría todas las raíces de L. Lo que es una contradicción pues E es el cuerpo de descomposición de F. Similarmente, M es el cuerpo de descomposición de $F_1(x)$ sobre $L(\beta)$.

Como $gr(F_1) = n - 1$, por hipótesis de inducción hay $\sigma : E \longrightarrow M$ isomorfismo que extiende $g : K(\alpha) \longrightarrow L(\beta)$ que a su vez extiende a $\varphi : K \longrightarrow L$ Por lo tanto, $\sigma : E \longrightarrow M$ es un isomorfismo que extiende $\varphi : K \longrightarrow L$.

Por Principio de inducción completa el Teorema vale para cualquier polinomio F de grado $n \in \mathbb{N}$.

□

Corolario 2.8. *El cuerpo de descomposición de un polinomio F sobre K es único, salvo isomorfismo.*

Demostración. En el teorema anterior tomemos $\varphi = id_K$ y $G = F$. □

2.5. Cuerpos Algebraicamente Cerrados y Clausura Algebraica de un cuerpo

El teorema fundamental del álgebra nos asegura que todo polinomio $P \in \mathbb{C}[x]$ no constante posee raíces en $\mathbb{C}$. Es más, nos dice que $\mathbb{C}$ es el cuerpo de descomposición de P. Visto lo que hemos aprendido, $\mathbb{C}$ es entonces un cuerpo que no posee extensiones algebraicas no triviales. Pero no es el único tal cuerpo.

Definición 2.15. *Un cuerpo K se dice* algebraicamente cerrado *si todo $P \in K[x]$ no constante tiene una raíz en K.*

Observación 2.19. *En un cuerpo algebraicamente cerrado K, todo polinomio $P \in K[x]$ no constante tiene* todas *sus raíces en K. En efecto, si P admite una raíz $\alpha \in K$, entonces $P = (x-\alpha)Q$ con $Q \in K[x]$. Pero entonces Q tiene una raíz no trivial. Iterando este proceso, llegamos a una factorización de P en $K[x]$ en factores lineales y por ende todas sus raíces están en K.*

Definición 2.16. *Sea K un cuerpo. Una* clausura algebraica *de K es una extensión $\bar{K}$ que es algebraica sobre K y tal que todo polinomio $P \in K[x]$ no constante se factoriza totalmente en $\bar{K}[x]$, es decir*

$$P = a(x - \alpha_1) \cdots (x - \alpha_t), \quad 0 \neq a \in K, \alpha_i \in \bar{K}.$$

Una clausura algebraica $\bar{K}$ de K es entonces una extensión que descompone todo polinomio no constante en $K[x]$ en factores lineales. El nombre "clausura algebraica" sugiere sin embargo que $\bar{K}$ es algebraicamente cerrado. Esto no es evidente a priori, ya que hay más polinomios en $\bar{K}[x]$ que en $K[x]$. De esto se trata el siguiente resultado.

Proposición 2.7. *Sea $\bar{K}$ una clausura algebraica de un cuerpo K. Entonces $\bar{K}$ es algebraicamente cerrado.*

Demostración. Sea $P \in \bar{K}[x]$ un polinomio y sea α una raíz de P en alguna extensión $L/\bar{K}$. Entonces $\bar{K}(\alpha)/\bar{K}$ y $\bar{K}/K$ son extensiones algebraicas. Esto nos dice que $\bar{K}(\alpha)/K$ es una extensión algebraica también, por lo que existe un polinomio $Q \in K[x]$ tal que α es raíz de Q. Ahora, como $Q \in K[x]$, tenemos que

$$Q = a(x - \alpha_1) \cdots (x - \alpha_t), \quad 0 \neq a \in K, \alpha_i \in \bar{K},$$

por lo que alguno de los $\alpha_i \in \bar{K}$ debe ser nuestro α inicial. Esto prueba que $\alpha \in \bar{K}$ y por ende P tiene al menos una raíz en $\bar{K}$, lo que nos dice que $\bar{K}$ es algebraicamente cerrado. □

Queremos probar ahora que todo cuerpo K posee una clausura algebraica. Intuitivamente, uno querría "juntar" todos los cuerpos de dscomposición para los infinitos polinomios en $K[x]$, pero la unión solo tiene sentido si vemos estos cuerpos inmersos en un cuerpo más grande para empezar. Existe una forma de hacer esto sin invocar un cuerpo más grande que contenga a todos los cuerpos de descomposición, pero esto implica el uso del lema de Zorn y de la noción de "límite inductivo". Para evitar este problema, haremos la demostración en dos pasos.

Proposición 2.8. *Sea K un cuerpo y sea L/K un cuerpo algebraicamente cerrado. Entonces*

$$M = \{\alpha \in L \mid \alpha \text{ es algebraico sobre } K\},$$

es una clausura algebraica de K.

Demostración. El Corolario 2.7 nos dice que un tal conjunto es un subcuerpo de L, el cual es claramente algebraico por definición. Bastará con probar entonces que todo polinomio no constante en $K[x]$ se descompone en factores lineales en $M[x]$.

Sea $P \in K[x]$ un polinomio no constante. Como L es algebraicamente cerrado, tenemos que

$$P = a(x - \alpha_1) \cdots (x - \alpha_t), \quad 0 \neq a \in K, \alpha_i \in L.$$

Esto nos dice que cada uno de los $\alpha_i \in L$ es algebraico sobre K, por lo que $\alpha_i \in M$. Por lo tanto, tenemos la misma descomposición en $M[x]$, lo que implica que M es una clausura algebraica de K. □

Ya sabemos entonces como construir la clausura algebraica si somos capaces de encontrar un cuerpo suficientemente grando como para contener a K y ser algebraicamente cerrado. Esto se puede hacer con harto menos esfuerzo que el argumento que sugeríamos precedentemente, siguiendo una idea de Artin (que de todas formas utiliza Zorn).

Proposición 2.9. *Para todo cuerpo K existe un cuerpo algebraicamente cerrado L que lo contiene.*

Demostración. Para cada polinomio $P \in K[x]$ mónico y no constante, consideremos una variable x_P y definamos el anillo de polinomios en *infinitas* variables $R = K[\ldots, x_P, \ldots]$.

Dentro de este anillo, definimos el ideal

$$I := \langle P(x_P) \mid P \in K[x] \rangle,$$

esto es, evaluar el polinomio P (que tiene una sola variable) en la variable x_P, lo que nos da un polinomio de una variable en R, luego tomar el ideal generado por éstos, es decir

$$I := \{Q_1 P_1(x_{P_1}) + \cdots Q_n P_n(x_{P_n}) \mid Q_i \in R,\ P_i \in K[x],\ n \in \mathbb{N}\}.$$

Probemos por contradicción que $I \neq R$, lo que equivale a probar que $1 \notin I$. De lo contrario, tendríamos

$$Q_1 P_1(x_{P_1}) + \cdots + Q_n P_n(x_{P_n}) = 1,$$

para ciertos $Q_i \in R$, $P_i \in K[x]$, $n \in \mathbb{N}$. Denotemos x_{P_i} simplemente por x_i y denotemos $x_{n+1}, \ldots, x_m$ las otras eventuales variables que podrían aparecer en los polinomios $Q_i \in R$ (nótese que cada uno tiene una cantidad *finita* de variables; es el anillo R que tiene

infinitas variables). Entonces podemos ver cada uno de los polinomios Q_i como elementos de $K[x_1, \ldots, x_m]$, con lo que obtenemos la igualdad

$$Q_1(x_1, \ldots, x_m)P_1(x_1) + \cdots Q_n(x_1, \ldots, x_m)P_n(x_n) = 1.$$

Sea ahora K'/K una extensión finita que contiene una raíz α_i de $P_i \in K[x]$ para cada $1 \leq i \leq n$. Entonces al evaluar esta igualdad en $x_i = \alpha_i$ para $1 \leq i \leq n$ y en $x_i = 0$ para $n+1 \leq i \leq m$, como $P_i(\alpha_i) = 0$, obtenemos la contradicción $1 = 0$ en K'. Esto prueba que $I \neq R$

Sabiendo que $I \neq R$, tenemos que existe un ideal maximal $M \subset R$ que contiene a I (es aquí donde usamos el Lema de Zorn, véase el curso de Grupos y Anillos). El cociente $L_1 = R/M$ corresponde entonces a un cuerpo que contiene a K de forma natural, pero no es necesariamente algebraicamente cerrado. Ahora, por construcción, todo polinomio $P \in K[x]$ tiene como raíz en $L_1 = R/M$ a la imagen de x_P, ya que $P(x_P) \in I \subset M$ y por ende $P(\bar{x}_P) = \overline{P(x_P)} = 0 \in L$.

Pero esto no basta, ya que debemos construir un cuerpo L tal que todo polinomio en $L[x]$ tiene una raíz en L. Construyamos entonces, siguiendo *el mismo procedimiento*, un cuerpo L_2 que contiene a L_1 y tal que todo polinomio $P \in L_1[x]$ tiene una raíz en L_2, también un cuerpo L_3 que contiene a L_2 y tal que todo polinomio $P \in L_2[x]$ tiene una raíz en L_3, y así sucesivamente, de forma que tendremos una cadena de cuerpos

$$K \subset L_1 \subset L_2 \subset \cdots \subset L_k \subset \cdots,$$

en la cual todo polinomio $P \in L_k[x]$ tiene una raíz en L_{k+1} para todo $k \in \mathbb{N}$. Definamos finalmente entonces

$$L := \bigcup_{k \in \mathbb{N}} L_k,$$

y demostremos que es el cuerpo que buscamos (ejercicio: demuestre que es un cuerpo!). Como L es la reunión de los L_k, dado un polinomio $P \in L[x]$, cada uno de sus coeficientes está en algún L_k y por ende están todos contenidos en el más grande de ellos, digamos L_{k_0}. Por ende existe una raíz de P en $L_{k_0+1} \subset L$ y esto prueba que L es algebraicamente cerrado. $\square$

Teorema 2.12. *Sea $\varphi : K \to K'$ un isomorfismo de cuerpos, sea $\bar{K}/K$ una clausura algebraica de K y sea $\bar{K}'/K'$ una clausura algebraica de K'. Entonces existe un isomorfismo de cuerpos $\bar{\varphi} : \bar{K} \to \bar{K}'$ que extiende φ, es decir $\bar{\varphi}|_K = \varphi$.*

Observación 2.20. *Este teorema nos permite hablar de LA clausura algebraica de un cuerpo en lugar de UNA clausura algebraica, ya que dos clausuras distintas son isomorfas. Si bien haremos el abuso de lenguaje al hablar de "LA" clausura algebraica, es importante saber que el isomorfismo entre dos clausuras no es único en general, lo que introduce una ambigüedad en la forma en la que identificamos dos clausuras algebraicas y por ende siembra la duda con respecto a su "unicidad". Lo mismo ocurre con "EL" cuerpo de descomposición de un polinomio y es precisamente la* Teoría de Galois *la que mide en cierta manera esta ambigüedad en ambos casos.*

Demostración. Esto es una consecuencia de la unicidad del cuerpo de descomposición, es decir, del Teorema 2.11 y del Lema de Zorn. En efecto, consideremos el siguiente conjunto

$$E = \{\psi : L \to \bar{K}' \mid K \subset L \subset \bar{K},\ \psi|_K = \varphi\},$$

y ordenémoslo de la siguiente manera: decimos que $(\psi_1, L_1) \geq (\psi_2, L_2)$ si $L_1 \supset L_2$ y $\psi_1|_{L_2} = \psi_2$. Queremos aplicar el Lema de Zorn a este conjunto ordenado.

Notemos ante todo que $E \neq \emptyset$, ya que φ nos da una inclusión de K en $\bar{K}'$. Sea entonces $\mathcal{C} \subset \mathcal{E}$ una cadena, es decir, un subconjunto de E totalmente ordenado. Consideremos el subconjunto de $\bar{K}$ definido por

$$L_{\mathcal{C}} := \bigcup_{(\psi, L) \in \mathcal{C}} L.$$

Es fácil ver entonces, gracias a la Proposición 2.1, que se trata de un subcuerpo de $\bar{K}$ que contiene a K. Definamos un homomorfismo $\psi_{\mathcal{C}} : L_{\mathcal{C}} \to \bar{K}'$ de la siguiente manera: para $x \in L_{\mathcal{C}}$, sea $(\psi, L) \in \mathcal{C}$ tal que $x \in L$ y definamos $\psi_{\mathcal{C}}(x) := \psi(x) \in \bar{K}'$. La definición de $(\psi_1, L_1) \geq (\psi_2, L_2)$ nos asegura que esta definición no depende de la elección de $(\psi, L) \in \mathcal{C}$ y por ende $\psi_{\mathcal{C}}$ está bien definida. Es un fácil ejercicio el ver que $\psi_{\mathcal{C}}$ es un homomorfismo de cuerpos tal que $\psi_{\mathcal{C}}|_K = \varphi$, por lo que $(\psi_{\mathcal{C}}, L_{\mathcal{C}})$ es un elemento de E y una cota superior de $\mathcal{C}$. Podemos entonces aplicar el Lema de Zorn a E.

El Lema de Zorn nos asegura que existe un elemento maximal en E, es decir, un subcuerpo $L_0 \subset \bar{K}$ y un homomorfismo $\psi_0 : L_0 \to \bar{K}'$ tal que $\psi_0|_K = \varphi$ que no admite elementos más grandes en E. Sea L_0' la imagen de ψ_0 en $\bar{K}'$ y sea $\alpha \in \bar{K}$. Como $\bar{K}$ es una clausura algebraica de K, tenemos que α es algebraico sobre K y por ende algebraico sobre L_0. Podemos entonces considerar el cuerpo de descomposición $L_0 \subset M_0 \subset \bar{K}$ del polinomio minimal m_{α,L_0} y su imagen vía ψ_0, la cual corresponde a un polinomio irreducible en $L_0'[x]$ y nos permite definir el cuerpo de descomposición $L_0' \subset M_0' \subset \bar{K}'$. El Teorema 2.11 nos asegura entonces que existe un homomorfismo $\tilde{\psi}_0 : M_0 \to M_0'$ cuya restricción a L_0 es ψ_0, es decir $(\tilde{\psi}_0, M_0) \geq (\psi_0, L_0)$. La maximalidad de (ψ_0, L_0) nos dice entonces que $M_0 = L_0$ y por ende la extensión es de grado 1, lo que nos dice que $\deg(P) = 1$ y por ende $\alpha \in L_0$. Esto prueba que $\bar{K} = L_0$ y por ende, definiendo $\bar{\varphi} := \psi_0$, tenemos el homomorfismo buscado.

Falta mostrar que $\bar{\varphi}$ es un isomorfismo. Sea $\alpha' \in \bar{K}'$ y sea $P' \in K'[x]$ su polinomio minimal. Entonces existe $P \in K[x]$ cuya imagen es P'. Ahora, sabemos que

$$P = (x - \alpha_1) \cdots (x - \alpha_n) \in \bar{K}[x],$$

por lo que

$$P' = (x - \bar{\varphi}(\alpha_1)) \cdots (x - \bar{\varphi}(\alpha_n)) \in \bar{K}'[x].$$

Esto nos dice que α' es uno de los $\bar{\varphi}(\alpha_i)$ y por ende está contenido en la imagen de $\bar{\varphi}$. Esto prueba que $\bar{\varphi}(\bar{K}) = \bar{K}'$ y por ende $\bar{\varphi}$ es un isomorfismo. □

Ejemplo 2.20. *Sea L una extensión finita de K. Pruebe que L es el cuerpo de descomposición de un polinomio en $K[x]$ si y solamente si todo polinomio irreducible en $K[x]$ que tiene una raíz en L se factoriza completamente en $L[x]$.*

Demostración: Supongamos que todo polinomio irreducible que tiene una raíz en L se factoriza completamente. Escribimos $L = K(\theta_1, \cdots, \theta_r)$ y sea $P_i = m_{\theta_i,K}$. Note que P_i es irreducible y tienen una raíz en L. Por lo tanto P_i se descompone completamente en L. Esto implica que L es el cuerpo de descomposición de $P(x) = \prod_{i=1}^{r} P_i(x)$. Supongamos ahora que L es el cuerpo de descomposición de un polinomio $Q \in L[x]$ y sea $\overline{K}$ una clausura

algebraica de K que contiene a L. Para concluir lo pedido basta probar que si $\alpha, \beta \in \overline{K}$ son raíces de un polinomio irreducible $P(x) \in K[x]$ y $\alpha \in L$, entonces $\beta \in L$. Por la Proposición 2.2, se tiene que existe un isomorfismo $i : K(\alpha) \to K(\beta)$ tal que $i|_K = \text{id}$. Note que L es un cuerpo de descomposición de $Q \in K(\alpha)[x]$. Por el mismo argumento $L(\beta)$ es un cuerpo de descomposición de $Q \in K(\beta)[x]$. Luego, por el Teorema 2.11 existe un isomorfismo $\psi : L(\alpha) \to L(\beta)$ tal que $\psi|_{K(\alpha)} = \text{id}$. Por lo tanto, si $\alpha \in L$, tenemos que $1 = [L(\alpha) : L] = \frac{[L(\alpha):K(\alpha)][K(\alpha):K]}{[L:K]} = \frac{[L(\beta):K(\beta)][K(\beta):K]}{[L:K]} = [L(\beta) : L]$. Concluimos que $\beta \in L$.

Definición 2.17. *Sea $P \in K[x]$ un polinomio dado por $P = \sum_{i=0}^{n} a_i x^i$. Definimos el* polinomio derivado *de P como el polinomio $P' \in K[x]$ dado por $P'(x) := \sum_{i=1}^{n} i a_i x^{i-1}$.*

Observación 2.21. *La derivación $P \mapsto P'$ respeta la suma, es decir $(P+Q)' = P'+Q'$ para todo $P, Q \in K[x]$. La multiplicación no es respetada, pero tenemos que $(PQ)' = PQ' + P'Q$ para todo $P, Q \in K[x]$.*

La noción de polinomio derivado permite detectar si hay raíces repetidas en un polinomio y calcular su multiplicidad, esto es, la cantidad de veces que aparecen. Definamos pues este concepto y demostremos esta afirmación.

Definición 2.18. *Sea $P \in K[x]$ y sea α una raíz de P en K. Decimos que α es una raíz de* multiplicidad *m si $P = (x - \alpha)^m Q$ con $Q \in K[x]$ y $Q(\alpha) \neq 0$. Si $m = 1$, decimos que α es una raíz* simple*.*

Teorema 2.13. *Sea K un cuerpo y sea $\bar{K}$ la clausura algebraica. Sea $P \in K[x]$ un polinomio no constante y sea $\alpha \in \bar{K}$ una raíz de P. Entonces la multiplicidad de α es mayor a 1 si y solo si $P'(\alpha) = 0$ (i.e. si α es raíz de P').*

Demostración. Escribamos $P = (x - \alpha)^m Q$ con $Q(\alpha) \neq 0$. Entonces

$P' = m(x - \alpha)^{m-1} Q + (x - \alpha)^m Q' = (x - \alpha)^{m-1}(mQ + (x - \alpha)Q')$.

Vemos entonces que, si $m > 1$, $P'(\alpha) = 0$. Y si $m = 1$, $P' = Q + (x - \alpha)Q'$ y por ende

$P'(\alpha) = Q(\alpha) + (\alpha - \alpha)Q'(\alpha) = Q(\alpha) \neq 0$. □

Teorema 2.14. *Para todo primo p, y todo $n \in \mathbb{N}$, existe un único, salvo isomorfismo, cuerpo finito con p^n elementos, que denotaremos $\mathbb{F}_{p^n}$.*

Demostración. Consideremos el cuerpo $\mathbb{F}_p$ y el polinomio $F(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

Tomemos

$L = \{\alpha \in \bar{\mathbb{F}}_p \mid \alpha \text{ es raíz de } x^{p^n} - x\} = \{\alpha \in \bar{\mathbb{F}}_p \mid \alpha^{p^n} - \alpha = 0\}$

Probaremos que L es un cuerpo con p^n elementos y es un cuerpo de descomposición del polinomio $x^{p^n} - x$. En efecto, L es subcuerpo de $\bar{\mathbb{F}}_p$ pues sean $\alpha, \beta \in L$. Probemos que $\alpha\beta, \alpha^{-1} \in L$.

Tenemos que $(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0$. De donde $\alpha\beta \in L$.

Sea ahora $\alpha \neq 0$. Luego $(\alpha^{-1})^{p^n} - \alpha^{-1} = (\alpha^{p^n})^{-1} = \alpha^{-1} - \alpha^{-1} = 0$, es decir, $\alpha^{-1} \in L$.

Falta ver que $(\alpha - \beta) \in L$. Usando el Binomio de Newton tenemos

$$\begin{aligned}(\alpha-\beta)^{p^n} &= \alpha^{p^n} + (-1)^1\tbinom{p^n}{1}\,\alpha^{p^n-1}\beta + (-1)^2\tbinom{p^n}{2}\alpha^{p^n-2}\beta^2\ldots \\ \ldots &+ (-1)^{p^n-1}\tbinom{p^n}{p^n-1}\alpha\beta^{p^n-1} + \beta^{p^n}(-1)^{p^n}\end{aligned}$$

$$p \mid \binom{p^n}{1};\ p \mid \binom{p^n}{2}, \ldots, p \mid \binom{p^n}{p^n-1}$$

$$\text{luego} \quad (\alpha-\beta)^{p^n} = \alpha^{p^n} + (-1)^{p^n}\beta^{p^n} = \alpha + (-1)^{p^n}\beta$$

1. Si $p = 2$, se tiene que $-1 \equiv 1 (mod\, 2)$ entonces $(\alpha - \beta)^{p^n} = \alpha - \beta$. Por lo tanto, $\alpha - \beta \in L$ y L es subcuerpo de $\bar{\mathbb{F}}_p$

2. Si $p > 2$, p es impar, $(-1)^{p^n} = -1$ y se tiene

$$(\alpha - \beta)^{p^n} = \alpha - \beta \Longrightarrow \alpha - \beta \in L$$

Probemos ahora que L tiene p^n elementos.

Sea $F(x) = x^{p^n} - x$, luego $F'(x) = p^n\, x^{p^n-1} - 1 = -1$.

Así, α raíz de $F(x) \Longleftrightarrow F'(\alpha) = 1 \neq 0$. Luego por Teorema 2.13, la multiplicidad de α es 1 y todas las reíces son simples y $gr(x^{p^n} - x) = p^n$. Por lo tanto, $x^{p^n} - x$ tiene p^n raíces.

Finalmente, como L es de característica p, $\mathbb{F}_p \subseteq L$ y $L =$ cuerpo de descomposición de $x^{p^n} - x$ sobre $\mathbb{F}_p$ y es único salvo isomorfismo $\square$

2.6. Extensiones Separables e Inseparables

Cuando definimos la noción de cuerpo de descomposición L/K de un polinomio $P \in K[x]$, dijimos que éste debía escribirse como un producto

$$P(x) = a(x - \alpha_1) \cdots (x - \alpha_t), \quad 0 \neq a \in K, \alpha_i \in L.$$

Es natural el querer ver a los elementos $\alpha_1, \ldots, \alpha_t$ como elementos distintos en L. Sin embargo, esto no tiene por qué ser cierto en general, incluso si P es irreducible. La presencia de repeticiones en las raíces de un polinomio irreducible es un fenómeno particular que da origen a las nociónes de extensión *separable* e *inseparable*.

Definición 2.19. *Sea $P \in K[x]$ un polinomio no constante. Decimos que P es* separable *si todas sus raíces en su cuerpo de descomposición son simples. En caso contrario, decimos que P es* inseparable.

Ejemplo 2.21. *Todo polinomio de grado 1 en $K[x]$ es separable.*

Ejemplo 2.22. *El polinomio $P \in \mathbb{Q}[x]$ dado por $P(x) = (x^2 - 3)(x^2 - 5)$ es separable ya que, en $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$,*

$$P(x) = (x - \sqrt{3})(x + \sqrt{3})(x - \sqrt{5})(x + \sqrt{5}).$$

Por otra parte, el polinomio $Q \in \mathbb{Q}[x]$ dado por $Q(x) = (x - 2)^3(x^2 + 1)$ no es separable ya que 2 no es una raíz simple.

Ejemplo 2.23. *El polinomio $P \in \mathbb{F}_p[x]$ dado por $P(x) = x^p - 1$ es inseparable, ya que*

$$P(x) = x^p - 1 = x^p - 1^p = (x - 1)^p,$$

y por ende 1 no es una raíz simple.

Ejemplo 2.24. *El polinomio $P \in \mathbb{F}_p[x]$ dado por $P(x) = x^{p^n} - x$ es separable, ya que*

$$P'(x) = p^n x^{p^n - 1} - 1 = -1,$$

y por ende todas las raíces son simples.

A pesar de que la definición de (in)separabilidad depende del cuerpo de descomposición, se puede averiguar si un polinomio es separable o inseparable sin necesidad de fabricar la extensión correspondiente. Todo pasa por el siguiente resultado.

Lema 2.5. *Si dos polinomios $P, Q \in K[x]$ tienen un factor común no trivial en alguna extensión $L[x]$ (por ejemplo, en el cuerpo de descomposición de uno de ellos), entonces tienen un factor común no trivial en $K[x]$.*

Demostración. Un factor común de los polinomios, divide al máximo común divisor de estos en $L[x]$. Pero el máximo común divisor de P y Q está en $K[x]$ por lo que es un factor común no trivial de éstos en $K[x]$. □

Lema 2.6. *Sean $P, Q \in K[x]$ polinomios. Entonces PQ es separable si y solo si P y Q son separables y $(P, Q) = 1$.*

Demostración. Si $(P, Q) = R \neq 1$, entonces toda raíz de R aparece dos veces en el producto PQ, por lo que PQ es inseparable. Y si alguno de los dos es inseparable, es evidente que PQ también lo es.

Por otro lado, si $(P, Q) = 1$ y ambos polinomios son separables, entonces todas las raíces de P son distintas y lo mismo ocurre con las de Q. Además, como $(P, Q) = 1$, estos polinomios no pueden compartir raíces dada la observación de más arriba. Por lo tanto, PQ es separable. □

Proposición 2.10. *Sea $P \in K[x]$ un polinomio no constante y sea P' su polinomio derivado. Entonces P es separable si y solo si $(P, P') = 1$.*

Demostración. Por definición, P es separable si y solo si toda raíz α de P es de multiplicidad 1. El Teorema 2.13 nos dice que esto ocurre si y solo si, para toda raíz α de P, tenemos que $P'(\alpha) \neq 0$. Esto es equivalente a decir que P y P' no tienen raíces en común. Finalmente, el Lema 2.5 nos dice entonces que esto es equivalente a $(P, P') = 1$. □

Lema 2.7. *Sea $P \in K[x]$ polinomio irreducible en $K[x]$. Si P tiene una raíz múltiple entonces $P' = 0$.*

Demostración. Si $P \in K[x]$, es irreducible en $K[x]$ entonces los únicos factores son P y las constantes no nulas. Si P tiene una raíz múltiple en L cuerpo de descomposición de P entonces P y p tienen un factor no trivial en $L[x]$ y por Lema 2.5, tienen un factor no trivial en $K[x]$. Luego $(P, P') = H,\ gr(H) \geq 1$. Por lo tanto, $H \mid P \ \wedge \ H \mid P'$ Pero los únicos factores de P son las constantes no nulas y P. Como $gr(H) \geq 1, H = P$ y $P \mid P'$. Como $gr(P') < gr(P)$, se tiene que $P' = 0$. □

Con el criterio de seoarabilidad a la mano, podemos concentrarnos en los polinomios irreducibles para probar el siguiente resultado:

Proposición 2.11. *Sea K un cuerpo de característica 0. Entonces todo polinomio irreducible $P \in K[x]$ es separable. En particular, todo polinomio es producto de polinomios separables.*

Demostración. Sea $P \in K[x]$ un polinomio irreducible. Escribamos $P(x) = \sum_{i=0}^{n} a_i x^i$ con $n \geq 1$ (P es irreducible y por ende no invertible y no nulo). Entonces su derivado se escribe $P'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. Ahora, como $na_n \neq 0 \in K$, vemos que P' es un polinomio de grado $n-1$, en particular no nulo. Y como los únicos divisores de P son sí mismo o 1 (salvo constantes), vemos entonces que $(P, P') = 1$ y por lo tanto P es separable gracias a la Proposición 2.10. □

Ejercicio 2.9. *¿Qué falla en esta demostración si K es de característica $p \neq 0$?*

Veamos ahora qué podemos decir del caso de característica positiva.

Para estos cuerpos K tenemos el **monomorfismo de Frobenius**.

Sea $\varphi : K \longrightarrow K, \quad a \longrightarrow a^p$ es homomorfismo de cuerpos pues:

$$\varphi(a+b) = (a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \ldots + pab^{p-1} + b^p = a^p + b^p \qquad \forall\ a, b \in K.$$

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b) \qquad \forall\ a, b \in K.$$

Por lo tanto, φ es inyectiva, por Lema 2.2.

Proposición 2.12. *Sea K cuerpo de de característica p.*

1. *Sea* $K^p := \{a^p \mid a \in K\}$ *entonces* K^p *es subcuerpo de* K.

2. *Si* K *es finito y de característica* p *entonces* $K = K^p$, *es decir,* $\forall\, x \in K,\ x = y^p$ *con* $y \in K$.

Demostración. 1. Sean $x, y \in K^p$ probaremos que $x - y \in K^p \ \wedge\ xy^{-1} \in K,\ y \neq 0$.

$$x = a^p \wedge y = b^p, \Longrightarrow \quad x - y = a^p - b^p = (a-b)^p \in K^p,\ car(K) = P$$

$$xy^{-1} = a^p (b^p)^{-1} = (ab^{-1})^p \in K^p$$

2. En efecto, el homomorfismo de Frobenius es inyectivo y como K es finito es biyectivo. De donde $Im\,(\varphi) = K^p$ luego, $K^p = K$. □

Esta propiedad de los cuerpos finitos es interesante y exige por ende una definición.

Definición 2.20. *Decimos que un cuerpo* K *es* perfecto *si* $\mathrm{car}(K) = 0$ *o bien* $\mathrm{car}(K) = p$ *y* $K^p = K$.

Ejemplo 2.25. *Dada la definición y la proposición anterior, vemos que todo cuerpo finito es perfecto.*

El siguiente lema nos ayudará a entender qué es lo que ocurre en este caso con los polinomios irreducibles.

Lema 2.8. *Sea* K *cuerpo de de característica* $p > 0$ *y sea* $P \in K[x]$ *un polinomio no constante. Entonces* $P' = 0$ *si y solo si* $P \in K[x^p]$, *es decir,* $P(x) = \sum_{i=0}^{n} a_i (x^p)^i$ *con* $a_i \in K$.

Demostración. Escribamos $P(x) = \sum_{j=0}^{m} b_j x^j$ con $b_j \in K$. Entonces $P'(x) = \sum_{j=1}^{n} j b_j x^{j-1}$. Vemos entonces que $P' = 0$ si y solo si $jb_j = 0$ para todo $1 \leq j \leq m$. Ahora, como $p = 0$ y $j \neq 0$ para todo j primo a p, tenemos que $P' = 0$ si y solo si $b_j = 0$ para todo j primo a p. En otras palabras, $b_j \neq 0$ solo si $j = ip$ para algún $i \in \mathbb{N}$, por lo que podemos escribir

$$P(x) = \sum_{i=0}^{n} b_{ip} x^{ip} = \sum_{i=0}^{n} a_i (x^p)^i,$$

donde $a_i := b_{ip} \in K$. □

Y la consecuencia no se hace esperar.

Proposición 2.13. *Sea K cuerpo de de característica $p > 0$ y sea $P \in K[x]$ un polinomio irreducible. Entonces P es inseparable si y solo si $P' = 0$, es decir, si y solo si $P \in K[x^p]$.*

Demostración. Supongamos que $P' = 0$. Entonces $(P, P') = P \neq 1$, por lo que P es inseparable gracias a la Proposición 2.10. Por otra parte, si P es inseparable, la Proposición 2.10 nos dice entonces que $(P, P') \neq 1$, por lo que existe un polinomio no constante $Q \in K[x]$ tal que $Q|P$ y $Q|P'$. Ahora, como P es irreducible, esto implica que $Q = P$ salvo una constante, por lo que $P|Q$ y por ende $P|P'$. Pero como $\deg(P') < \deg(P)$, la única posibilidad es que $P' = 0$. La última afirmación viene del lema anterior. □

Ejemplo 2.26. *Un ejemplo de polinomio irreducible e inseparable es el siguiente: consideremos el cuerpo $K = \mathbb{F}_p(t)$ de funciones racionales sobre el cuerpo $\mathbb{F}_p$. Entonces el polinomio $P \in K[x]$ dado por $P(x) = x^p - t$ es irreducible e inseparable ya que $P' = 0$. Para probar que es irreducible, notamos que t es un elemento primo en el anillo $\mathbb{F}_p[t]$ y usamos Criterio de Einsentein pues $K = \mathbb{F}_p(t)$ es el cuerpo de cocientes de $\mathbb{F}_p[t]$.*

Ejercicio 2.10. *Sea $K = \mathbb{F}_p(t)$. Calcule el grado $[K : K^p]$.*

Ejemplo 2.27. *Vemos también que $\mathbb{F}_p(t)$ no es perfecto gracias al ejercicio anterior.*

Recordemos ahora un resultado importante del curso Grupos y Anillos:

Lema 2.9 (Lema de Gauss)**.** *Sea R un dominio de factorización única, sea $F = Q(R)$ y sea $P \in R[x]$. Si P es reducible en $F[x]$, entonces P es reducible en $R[x]$. Más precisamente, si $P = AB$ con $A, B \in F[x]$ polinomios* no constantes*, entonces existe $r \in F$ tal que $rA(x), r^{-1}B(x) \in R[x]$, de forma que $(rA)(r^{-1}B)$ es una factorización de P en $R[x]$.*

Ejemplo 2.28. *Sea $\mathbb{F}_p$ el cuerpo finito de p elementos. Sea $L = \mathbb{F}_p(u, v)$ el cuerpo de cocientes del anillo de polinomios $\mathbb{F}_p[u, v]$ y sea $K = \mathbb{F}_p(u^p, v^p)$ el cuerpo de cocientes del anillo de polinomios $\mathbb{F}_p[u^p, v^p]$. Demuestre que L/K es una extensión de grado p^2, en donde todo elemento de L es inseparable sobre K o bien pertenece a K.*

Solución: Considere $F = \mathbb{F}_p(u, v^p) = \text{Quot}(\mathbb{F}_p[u, v^p])$. Note que $F = K(u)$ y que $L = F(v)$. El elemento $u \in F$ se anula en el polinomio $P(x) = x^p - u^p \in K[x]$, donde u^p es un elemento primo en el anillo $\mathbb{F}_p(v^p)[u^p]$. Por criterio de Einsenstein tenemos que P es irreducible en $\mathbb{F}_p(v^p)[u^p]$. Luego, por lema de Gauss, tenemos que P es irreducible en $K[x]$. Esto implica que $[F : K] = p$. Por otro lado $v \in L$ se anula en el polinomio $Q(x) = x^p - v^p \in F[x]$, donde v^p es un elemento primo en el anillo $\mathbb{F}_p(u)[v^p]$. Por criterio de Einsenstein tenemos que Q es irreducible en $\mathbb{F}_p(u)[v^p]$. Luego, por lema de Gauss, tenemos que Q es irreducible en $F[x]$. Esto nos lleva a que $[L : F] = p$. Concluimos que $[L : K] = p^2$. Considere ahora un elemento $y \in L$ cualquiera. Por definición de cuerpo de cocientes $y = \frac{r(u,v)}{s(u,v)}$, donde $s(u, v) \neq 0$. Note que todo polinomio $r(u, v) = p_0(u) + p_1(u)v + \cdots + p_n(u)v^n \in \mathbb{F}_p[u, v]$ satisface que $r(u, v)^p = p_0(u)^p + p_1(u)^p v^p + \cdots + p_n(u)^p v^{np}$. Ahora bien, todo polinomio $q(u) = a_0 + a_1 u + \cdots + a_n u^n \in \mathbb{F}_p[u]$ cumple con $q(u)^p = a_0 + a_1 u^p + \cdots + a_n u^{np}$, puesto que $a_i^p = a_i$, para todo $a_i \in \mathbb{F}_p$. De esto se sigue que $r(u, v)^p = r(u^p, v^p)$. Por lo tanto $y^p = \frac{r(u^p,v^p)}{s(u^p,v^p)} \in K$. Esto implica que el elemento $y \in L$ satisface el polinomio $p(x) = x^p - \alpha$, con $\alpha \in K$. Por lo tanto $m_{y,K}(x)$ divide a $x^p - \alpha$. Note que $p(x) = (x - y)^p$ en F. Por ende $m_{y,K}(x)$ es inseparable o bien tiene grado 1. Esto nos permite concluir que $y \in L$ es inseparable sobre K o bien $y \in K$.

Definición 2.21. *Una extensión algebraica E/K se dice* puramente inseparable *si los únicos elementos separables son los elementos de K.*

Ejercicio 2.11. *Sea K cuerpo de de característica $p > 0$ y sea $\bar{K}$ su clausura algebraica. Considere el subconjunto*

$$K^{p^{-\infty}} := \{x \in \bar{K} \mid \exists\, n \in \mathbb{N},\, x^{p^n} \in K\} \subset \bar{K}.$$

Pruebe que L es un subcuerpo de $\bar{K}$, que $K^{p^{-\infty}}/K$ es puramente inseparable y que $K^{p^{-\infty}}$ es perfecto.

Como vimos, lo que falla en la demostración de la Proposición 2.11 para cuerpos de característica positiva es que el polinomio derivado de un polinomio irreducible puede ser

nulo, lo que no ocurre en característica 0. La separabilidad de los polinomios irreducibles no está entonces asegurada en un cuerpo de característica $p > 0$. Sin embargo, esta situación se arregla en el caso de los cuerpos perfectos.

Proposición 2.14. *Sea K un cuerpo perfecto. Entonces todo polinomio irreducible $P \in K[x]$ es separable. En particular, todo polinomio es producto de polinomios separables.*

Demostración. El caso de característica 0 corresponde a la Proposición 2.11, por lo que podemos suponer que $\text{car}(K) = p > 0$. Sea $P \in K[x]$ un polinomio irreducible y supongamos que es inseparable. La Proposición 2.13 nos dice entonces que $P \in K[x^p]$, es decir que podemos escribir $P(x) = \sum_{i=0}^{n} a_i x^{ip}$ con $a_i \in K$. Ahora, como K es perfecto, sabemos que $K = K^p$ y por ende, para todo $0 \leq i \leq n$ existe $b_i \in K$ tal que $a_i = b_i^p$. Tenemos entonces que

$$P(x) = \sum_{i=0}^{n} a_i x^{ip} = \sum_{i=0}^{n} b_i^p (x^i)^p = \sum_{i=0}^{n} (b_i x^i)^p = \left(\sum_{i=0}^{n} b_i x^i \right)^p .$$

Esto nos dice que $P = Q^p$ con $Q(x) = \sum_{i=0}^{n} b_i x^i$, lo que contradice el hecho que P es irreducible. Por lo tanto P es separable. □

Definición 2.22. *Decimos que una extensión algebraica de cuerpos L/K es* separable *si todo elemento de L es raíz de un polinomio separable sobre K. Una extensión algebraica que no es separable se dice* inseparable.

Ejercicio 2.12. *Pruebe que toda extensión finita de $\mathbb{Q}$ es separable.*

Recordemos que todo elemento algebraico $\alpha \in L$ en una extensión L/K es raíz de un polinomio irreducible $m_{\alpha,K} \in K[x]$. Dada la Proposición 2.14 y la última definición, tenemos entonces que *toda extensión de un cuerpo perfecto es separable*. Esto justifica de hecho la nomenclatura de los cuerpos perfectos, ya que las extensiones separables son aquéllas con las que uno quiere trabajar. Una de las razones es el corolario al siguiente teorema, muy importante en teoría de cuerpos.

Teorema 2.15. *Sea L/K una extensión separable y sean $\alpha, \beta \in L$ elementos algebraicos sobre K. Entonces $K(\alpha, \beta)/K$ es simple, es decir, existe un elemento $\gamma \in K(\alpha, \beta) \subset L$ tal que $K(\alpha, \beta) = K(\gamma)$.*

Corolario 2.9 (Teorema del elemento primitivo)**.** *Toda extensión L/K finita y separable es simple.*

Demostración. Asumiendo el teorema, vemos inmediatamente por inducción que el resultado es cierto para todo subcuerpo $K(\alpha_1, \ldots, \alpha_n) \subset L$ con $\alpha_i \in L$ algebraico sobre K. Ahora, como L/K es finita, el Teorema 2.8 nos dice que es algebraica y finitamente generada, es decir $L = K(\alpha_1, \ldots, \alpha_n)$ para ciertos $\alpha_i \in L$, lo que prueba el resultado. □

Demostración del Teorema 2.15. La demostración es distinta dependiendo de si K es finito o infinito. Supongamos primero que K es finito de cardinal q. Como $K(\alpha, \beta)$ es una extensión algebraica y finitamente generada, se trata de una extensión finita de K por el Teorema 2.8 y por ende de un K-espacio vectorial de dimensión finita. Vemos entonces que el cardinal de $K(\alpha, \beta)$ es q^m para algún $m \in \mathbb{N}$. Recordemos ahora un resultado del curso de Grupos y Anillos:

Lema 2.10. *Sea K un cuerpo finito. Entonces K^* es un grupo cíclico.*

Usando este lema, vemos que $K(\alpha, \beta)^*$ es un grupo cíclico de órden $q^m - 1$. Sea $\gamma \in K(\alpha, \beta)$ un generador de $K(\alpha, \beta)^*$ como grupo. Entonces existen $m_1, m_2 \in \mathbb{N}$ tales que $\gamma^{m_1} = \alpha$ y $\gamma^{m_2} = \beta$. Esto prueba que $\alpha, \beta \in K(\gamma)$ y por ende $K(\alpha, \beta) \subset K(\gamma)$. Pero como $\gamma \in K(\alpha, \beta)$, tenemos que $K(\alpha, \beta) = K(\gamma)$, lo que concluye la demostración en este caso.

Supongamos ahora que K es infinito. Sean $P = m_{\alpha,K}$ y $Q = m_{\beta,K}$ los polinomios minimales de α y β en $K[x]$. Como L/K es separable, sabemos que α es raíz de un polinomio separable $P_1 \in K[x]$, pero como P es el polinomio minimal de α, vemos que $P | P_1$ y por ende P es separable también. El mismo argumento con β nos dice que Q es separable y por ende las raíces de estos dos polinomios son todas distintas entre sí.

Sean $\alpha_2, \ldots, \alpha_m$ las otras raíces de P y sean $\beta_2, \ldots, \beta_n$ las otras raíces de Q en algún cuerpo de descomposición. Consideremos los elementos

$$\frac{\alpha_i - \alpha}{\beta - \beta_j}, \quad 2 \leq i \leq m,\ 2 \leq j \leq n.$$

Como K es infinito, existe un elemento $\gamma_0 \in K$ que es distinto a todos estos elementos. Sea $\gamma = \alpha + \gamma_0\beta$. Tenemos entonces que $K(\gamma) \subset K(\alpha, \beta)$ de forma obvia, ya que $\gamma_0 \in K$. Para concluir, debemos probar ahora que $K(\alpha, \beta) \subset K(\gamma)$. Y para esto bastará con probar que $\alpha, \beta \in K(\gamma)$.

Comencemos con β. Notemos que por definición tenemos que $\gamma - \gamma_0\beta = \alpha$, pero

$$\gamma - \gamma_0\beta_j = \alpha + \gamma_0(\beta - \beta_j) \neq \alpha_i, \quad 2 \leq i \leq m,\ 2 \leq j \leq n,$$

y claramente $\gamma - \gamma_0\beta_j \neq \alpha$ ya que $\beta \neq \beta_j$. En otras palabras, la única forma de obtener una raíz de P con la expresión $\gamma - \gamma_0 x$ para $x \in \{\beta, \beta_2, \ldots \beta_n\}$ es la primera igualdad. Consideremos entonces el polinomio $R \in K(\gamma)[x]$ dado por $R(x) = P(\gamma - \gamma_0 x)$. Entonces β es una raíz de R ya que

$$R(\beta) = P(\gamma - \gamma_0\beta) = P(\alpha) = 0.$$

Por otra parte, para todo $2 \leq j \leq n$, tenemos que β_j no es raíz de R. En efecto,

$$R(\beta_j) = P(\gamma - \gamma_0\beta_j) \neq 0,$$

ya que de lo contrario $\alpha + \gamma_0(\beta - \beta_j)$ sería igual a alguno de los α_i, lo cual descartamos al construir γ_0.

Tenemos entonces que β es *la única* raíz común de $Q \in K[x] \subset K(\gamma)[x]$ y $R \in K(\gamma)[x]$, lo que nos dice que $(x - \beta)$ divide a Q en $K(\gamma)[x]$ y por ende $\beta \in K(\gamma)$. Es fácil ver entonces que $\alpha = \gamma - \gamma_0\beta \in K(\gamma)$, lo que concluye la demostración. □

2.7. Cuerpos y polinomios ciclotómicos

En la sección 2.4 estudiamos un poco los cuerpos ciclotómicos y probamos que el polinomio ciclotómico Φ_p es irreducible. Ahora los estudiaremos en más detalle, así como la extensión de $\mathbb{Q}$ que éstos generan como cuerpo de descomposición. Recordemos entonces:

Definición 2.23. *El* n-ésimo cuerpo ciclotómico *es el cuerpo de descomposición del polinomio* $x^n - 1 \in \mathbb{Q}[x]$.

El n-ésimo polinomio ciclotómico Φ_n *es el polinomio cuyas raíces son las raíces* n*-ésimas* primitivas *de* 1*, es decir*

$$\Phi_n(x) := \prod_{\substack{1\leq a\leq n\\(a,n)=1}} (x-\zeta_n^a).$$

En particular, $gr(\Phi_n)=\varphi(n)$*, donde* φ *es la función de Euler, donde para cada* $n\in\mathbb{N}, \varphi(n)$ *es el número de enteros positivos* $a, 1\leq a\leq n, (a,n)=1$.

Denotemos por μ_n el grupo de las raíces n-ésimas de la unidad y recordemos que las raíces primitivas corresponden a los generadores de este grupo cíclico. Recordemos también que en μ_n se encuentran todas las raíces d-ésimas de la unidad para todo divisor $d|n$ (i.e. $\mu_d\subset\mu_n$). Además, el orden del elemento ζ_n^a es igual a $\frac{n}{(a,n)}$, lo que nos dice que ζ_n^a, aparte de ser una raíz n-ésima, es una raíz *primitiva* d-ésima de la unidad con $d=\frac{n}{(a,n)}$ (es decir, un generador de μ_d). Vemos por lo tanto que en el producto

$$x^n-1=\prod_{\zeta\in\mu_n}(x-\zeta),$$

se encuentran todas las raíces primitivas d-ésimas de la unidad para cada divisor $d|n$. Por otra parte, toda raíz n-ésima de la unidad tiene que ser una raíz primitiva para algún $d|n$, a saber, para d igual a su orden. En otras palabras, acabamos de demostrar lo siguiente.

Proposición 2.15. *Tenemos la igualdad polinomial*

$$x^n-1=\prod_{d|n}\Phi_d(x).$$

Pero esta igualdad, ¿dónde tiene lugar? Para ello debemos estudiar los coeficientes de Φ_n. Recordemos que si p es primo ya sabemos que

$$\Phi_p(x)=x^{p-1}+\cdots+x+1.$$

Por otra parte, claramente $\Phi_1(x)=x-1$. Dada la Proposición 2.15, para averiguar Φ_4 tenemos entonces que dividir x^4-1 por $\Phi_1\Phi_2$, es decir

$$\Phi_4=\frac{x^4-1}{(x-1)(x+1)}=\frac{x^4-1}{x^2-1}=x^2+1.$$

De la misma manera, podemos obtener Φ_6 dividiendo $x^6 - 1$ por $\Phi_1\Phi_2\Phi_3$, lo que nos da $\Phi_6(x) = x^2 - x + 1$.

Con esto ya podemos empezar a conjeturar que los coeficientes de Φ_n son tan solo 0, 1 y -1. Y de hecho esto es así hasta $n = 104$, pero lamentablemente

$$\begin{aligned}\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \mathbf{2}x^{41} - x^{40} - x^{39} + x^{36} + x^{35} \\ + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} \\ + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - \mathbf{2}x^7 - x^6 - x^5 + x^2 + x + 1.\end{aligned}$$

Pero al menos podemos demostrar que:

Proposición 2.16. *Para todo $n \in \mathbb{N}$, Φ_n es un polinomio mónico en $\mathbb{Z}[x]$.*

Demostración. La demostración sigue la idea que veníamos usando, a saber, inducción sobre n. Ya tenemos el resultado para $n = 1$ (y de hecho hasta $n = 7$ por lo menos).

Supongamos pues que $\Phi_m \in \mathbb{Z}[x]$ y que es mónico para todo $m < n$ y probemos lo mismo para Φ_n. Gracias a la Proposición 2.15, ya sabemos que

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \prod_{d|n, d<n} \Phi_d(x)\Phi_n(x),$$

lo que nos dice inmediatamente que Φ_n es mónico ya que todos los otros polinomios en la igualdad lo son. Además, obtenemos que $x^n - 1 = P\Phi_n$ con $P \in \mathbb{Z}[x]$, ya que P corresponde al producto de los Φ_d con $d|n$ y $d < n$, los cuales están todos en $\mathbb{Z}[x]$.

Usando lema de Gauss, vemos que existe $r \in \mathbb{Q}$ tal que $x^n - 1 = (rP)(r^{-1}\Phi_n)$ y $rP, r^{-1}\Phi_n \in \mathbb{Z}[x]$. Ahora, sabiendo que P y Φ_n son mónicos, vemos que $rP, r^{-1}\Phi_n \in \mathbb{Z}[x]$ solo si $r = 1$, por lo que $\Phi_n \in \mathbb{Z}[x]$, lo que concluye la demostración. □

Gracias a este resultado, vemos que la factorización dada por la Proposición 2.15 ocurre en $\mathbb{Z}[x]$. Cabe preguntarse ahora si esta factorización puede ser reducida a factores más pequeños o si cada Φ_n es irreducible en $\mathbb{Z}[x]$ (o $\mathbb{Q}[x]$, dado el Lema de Gauss).

Proposición 2.17. *Para todo $n \in \mathbb{N}$, el polinomio Φ_n es irreducible en $\mathbb{Q}[x]$.*

Demostración. Como decíamos, bastará con demostrar que Φ_n es irreducible en $\mathbb{Z}[x]$ gracias al Lema de Gauss. Supongamos entonces por contradicción que $\Phi_n = PQ$ con $P, Q \in \mathbb{Z}[x]$, P irreducible y Q no constante, ambos mónicos.

Sea ζ una raíz de P. Como se trata de una raíz de Φ_n, sabemos que ζ es una raíz primitiva n-ésima de la unidad. Sea ahora p un primo que no divide a n. Entonces $(p, n) = 1$ y por lo tanto ζ^p es también una raíz primitiva n-ésima de la unidad y por ende raíz de Φ_n.

Supongamos por un instante que ζ^p es raíz de Q. Entonces ζ es raíz del polinomio $R \in \mathbb{Z}[x]$ dado por $R(x) = Q(x^p)$. Pero como P es irreducible y mónico y $P(\zeta) = 0$, sabemos que $P = m_{\zeta,\mathbb{Q}}$, lo que nos dice que $P|R$ por la Proposición 2.3 ya que $R(\zeta) = 0$. Sea $S \in \mathbb{Z}[x]$ tal que $R = PS$ y consideremos la reducción módulo p de esta igualdad, es decir $\bar{R} = \bar{P}\bar{S} \in \mathbb{F}_p[x]$. Ahora, notemos que, en $\mathbb{F}_p[x]$,

$$\bar{P}(x)\bar{S}(x) = \bar{R}(x) = \bar{Q}(x^p) = \bar{Q}(x)^p,$$

ya que $a^p = a$ para todo coeficiente $a \in \mathbb{F}_p$. Como $\mathbb{F}_p[x]$ es un DFU, vemos que $\bar{P}$ y $\bar{Q}$ tienen al menos un factor en común en $\mathbb{F}_p[x]$, lo que nos dice que el polinomio $\bar{\Phi}_n = \bar{P}\bar{Q} \in \mathbb{F}_p[x]$ tiene al menos una raíz múltiple en $\mathbb{F}_p$ y por ende el polinomio $x^n - 1$ tiene al menos una raíz múltiple en $\mathbb{F}_p$. Pero este polinomio es separable en $\mathbb{F}_p[x]$ ya que su derivado es nx^{n-1}, el cual es claramente coprimo a $x^n - 1$. Esto es una contradicción que nos asegura que ζ^p no es una raíz de Q.

Sabemos entonces que, para toda raíz ζ de P y para todo primo p que no divide a n, ζ^p es una raíz de P. Sea ahora ζ una raíz de P y $a \in \mathbb{N}$ un entero tal que $(a, n) = 1$. Entonces $a = p_1 \cdots p_k$ con $(p_i, n) = 1$, por lo que ζ^{p_1} es una raíz de P, por lo que $(\zeta^{p_1})^{p_2}$ es una raíz de P, y así sucesivamente hasta ver que $\zeta^a = \zeta^{p_1 \cdots p_n}$ es una raíz de P *para todo entero a primo a* n. Esto nos dice que P tiene al menos $\varphi(n)$ raíces y por ende su grado es al menos $\varphi(n)$. Pero $gr(P) \leq gr(\Phi_n) = \varphi(n)$. Esto prueba que Q es constante, contradiciendo nuestra hipótesis inicial sobre la reducibilidad de Φ_n, lo que prueba que es irreducible. □

Corolario 2.10. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Demostración. En efecto, dada la Proposición anterior, vemos gracias a Proposición 2.3 que $\Phi_n = m_{\zeta_n,\mathbb{Q}}$. El Teorema 2.7 nos dice entonces que $[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ es igual a $gr(\Phi_n) = \varphi(n)$. □

3. Teoría de Galois

Cuando tomamos un cuerpo de descomposición de un polinomio $P \in K[x]$, en cierto modo, agregamos a K todas las raíces de P. Sin embargo, también en un cierto modo, todas estas raíces son el mismo objeto ya que tienen la misma definición, a saber, son "el" objeto tal que $P(\alpha) = 0$. ¿Por qué la existencia de una raíz implica casi inmediatamente la existencia de otras distintas? ¿De dónde viene esta diferencia? La Teoría de Galois, cuyo nombre original era "Teoría de la ambiguedad", estudia estas diferencias y similitudes entre los diversos elementos algebraicos que uno agrega a un cuerpo al descomponer un polinomio.

La teorá de Galois es un puente entre el álgebra clásica, el estudio de ecuaciones polinomiales, y el álgebra moderna que enfatiza aspectos mas estructurales como cuerpos, anillos, grupos etc.

3.1. El grupo de automorfismos de un cuerpo

El objeto crucial que consideraremos es el siguiente:

Definición 3.1. *Sea K un cuerpo. Denotamos por* $\mathrm{Aut}(K)$ *el grupo de automorfismos de cuerpo de K, es decir:*

$$\mathrm{Aut}(K) = \{\sigma : K \to K \mid \sigma \text{ isomorfismo de cuerpos}\}.$$

Recordemos que se trata de un grupo con respecto a la composición de funciones.

Sea $\sigma \in \mathrm{Aut}(K)$. Diremos que σ fija a un elemento $\alpha \in K$ *si $\sigma(\alpha) = \alpha$. Diremos que σ* fija a un subcuerpo $K_0 \subset K$ *si $\sigma|_{K_0} = \mathrm{id}|_{K_0}$, es decir, si σ fija a α para todo $\alpha \in K_0$.*

Sea L/K una extensión. Entonces el subgrupo de los automorfismos que fijan K es denotado por

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}|_K\}.$$

Ejercicio 3.1. *Pruebe que* $\mathrm{Aut}(L/K)$ *es efectivamente un subgrupo de* $\mathrm{Aut}(L)$.

Al no mover al cuerpo K, el grupo $\mathrm{Aut}(L/K)$ deja invariante al anillo $K[x]$ y por ende a todos sus polinomios. Sin embargo, el grupo sí mueve a los elementos de L, muchos de los cuales están definidos por polinomios en $K[x]$. En otras palabras, la acción de $\mathrm{Aut}(L/K)$ respeta las "descripciones" de los elementos de L que son algebraicos sobre K. Más precisamente:

Proposición 3.1. *Sea L/K una extensión y $\alpha \in L$ un elemento algebraico sobre K. Entonces, para todo $\sigma \in \mathrm{Aut}(L/K)$, $\sigma(\alpha)$ es una raíz del polinomio $m_{\alpha,K} \in K[x]$. En particular, α y $\sigma(\alpha)$ tienen el mismo polinomio minimal o irreducible. En otras palabras, σ permuta las raíces de los polinomios irreducibles.*

Demostración. Sea $P = m_{\alpha,K}$ dado por $P(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in K$. Entonces $P(\alpha) = 0$ por definición. Ahora, como σ fija a K, tenemos que $\sigma(a_i) = a_i$ para todo i. Y como σ es un homomorfismo, obtenemos:

$$P(\sigma(\alpha)) = \sum_{i=0}^{n} a_i \sigma(\alpha)^i = \sum_{i=0}^{n} \sigma(a_i)\sigma(\alpha^i) = \sigma\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sigma(P(\alpha)) = \sigma(0) = 0,$$

lo que prueba que $\sigma(\alpha)$ es una raíz de P. □

Ejemplo 3.1. *Determinemos el grupo* $\mathrm{Aut}(L/\mathbb{Q})$ *para* $L = \mathbb{Q}(\sqrt{5})$, $L = \mathbb{Q}(\sqrt[3]{5})$ *y* $L = \mathbb{Q}(\zeta_5)$.

En el primer caso, sabemos que una $\mathbb{Q}$-base de L es $\{1, \sqrt{5}\}$, por lo que todo elemento se escribe de la forma $a + b\sqrt{5}$ con $a, b \in \mathbb{Q}$. Sea $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$. Como σ es la identidad sobre $\mathbb{Q}$ y un homorfismo sobre L, vemos que $\sigma(a + b\sqrt{5}) = a + b\sigma(\sqrt{5})$, por lo que basta con fijar la imagen de $\sqrt{5}$. Ahora, dada la Proposición 3.1, sabemos que $\sigma(\sqrt{5})$ es una raíz de $x^2 - 5$, osea, igual a $\pm\sqrt{5}$. Si $\sigma(\sqrt{5}) = \sqrt{5}$, entonces $\sigma = \mathrm{id}_L$. De lo contrario tenemos que $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$. Esta fórmula nos da un homomorfismo de cuerpos ya que claramente es $\mathbb{Q}$-lineal (en particular, respeta la suma) y biyectiva, y en lo que concierne a la multiplicación, tenemos:

$$\begin{aligned}\sigma((a + b\sqrt{5})(c + d\sqrt{5})) &= \sigma(ac + 5bd + (ad + bc)\sqrt{5}) \\ &= ac + 5bd - (ad + bc)\sqrt{5} = (a - b\sqrt{5})(c - d\sqrt{5}) = \sigma(a + b\sqrt{5})\sigma(c + d\sqrt{5}).\end{aligned}$$

Si llamamos entonces σ_0 a este automorfismo particular, tenemos que $\mathrm{Aut}(L/\mathbb{Q}) = \{\mathrm{id}_L, \sigma_0\} \simeq \mathbb{Z}/2\mathbb{Z}$.

En el segundo caso, sabemos que una $\mathbb{Q}$-base de L es $\{1, \sqrt[3]{5}, \sqrt[3]{5}^2\}$, por lo que todo elemento se escribe de la forma $a + b\sqrt[3]{5} + c\sqrt[3]{5}^2$ con $a, b, c \in \mathbb{Q}$. Sea $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$. Como σ es la identidad sobre $\mathbb{Q}$ y un homorfismo sobre L, vemos que $\sigma(a + b\sqrt[3]{5} + c\sqrt[3]{5}^2) = a + b\sigma(\sqrt[3]{5}) + c\sigma(\sqrt[3]{5})^2$, por lo que basta con fijar la imagen de $\sqrt[3]{5}$. Ahora, dada la Proposición 3.1, sabemos que $\sigma(\sqrt[3]{5})$ es una raíz de $x^3 - 5$. Pero sabemos bien que las otras raíces de este polinomio son complejas y que $\mathbb{Q}(\sqrt[3]{5})$ está contenido en los reales. Por lo tanto, la única raíz de $x^3 - 5$ que está disponible en L es la misma $\sqrt[3]{5}$, por lo que $\sigma = \mathrm{id}_L$. Tenemos entonces que $\mathrm{Aut}(L/\mathbb{Q}) = \{\mathrm{id}_L\}$ *es el grupo trivial.*

En el tercer caso, sabemos que una $\mathbb{Q}$-base de L es $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$. Una vez más vemos entonces que $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$ está completamente *determinada por la imagen de ζ_5. La Proposición 3.1 nos dice entonces que $\sigma(\sqrt{5})$ es una raíz quinta primitiva de la unidad, es decir, $\sigma(\zeta_5) = \zeta_5^{a_\sigma}$ con $a_\sigma \in \{1, 2, 3, 4\}$. Al igual que en el primer caso, podemos verificar a la mano que cada uno de estos casos define un homomorfismo de cuerpos, pero es más fácil usar la Proposición 2.2 para notar que tal isomorfismo existe y es único. Si denotamos por σ_i el automorfismo tal que $a_\sigma = i$, entonces* $\mathrm{Aut}(L/\mathbb{Q}) = \{\sigma_1 = \mathrm{id}_L, \sigma_2, \sigma_3, \sigma_4\}$, *grupo isomorfo a $(\mathbb{Z}/5\mathbb{Z})^*$ vía el homomorfismo de grupos $\sigma_i \mapsto i \mod 5$.*

Ejercicio 3.2. *Determine el grupo* $\mathrm{Aut}(L/\mathbb{Q})$ *para* $L = \mathbb{Q}(\sqrt{3}, i)$

Ejercicio 3.3. *Demuestre que, para todo cuerpo K de característica 0,* $\mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{Q})$. *¿Cuál es la proposición análoga en característica positiva?*

Ejercicio 3.4. *Determine el grupo* $\mathrm{Aut}(\mathbb{Q}(i)(\sqrt[4]{3})/\mathbb{Q}(i))$.

El principio de concentrarse en los generadores de una extensión para calcular automorfismos como hicimos en estos ejemplos, nos permite demostrar el siguiente corolario de la Proposición 3.1, el cual nos será útil más adelante.

Lema 3.1. *Sea L/K una extensión finita. Entonces el grupo $G = \mathrm{Aut}(L/K)$ es finito.*

Demostración. En efecto, sabemos entonces que $L = K(\alpha_1, \ldots, \alpha_n)$ para ciertos elementos algebraicos $\alpha_i \in L$ para los cuales definimos $m_i = \deg(m_{\alpha_i,K})$. La Proposición 3.1 nos dice que, para todo $\sigma \in G$ y para todo $1 \leq i \leq n$, σ induce una permutación $\tau_{\sigma,i} \in S_{m_i}$ de las m_i raíces de $m_{\alpha_i,K}$. Vemos fácilmente que esto define homomorfismos $G \to S_{m_i}$ y, tomando el producto de ellos, obtenemos un homomorfismo de grupos

$$\begin{aligned} \varphi : G &\to \prod_{i=1}^{n} S_{m_i} \\ \sigma &\mapsto (\tau_{\sigma,1}, \ldots, \tau_{\sigma,n}). \end{aligned}$$

Ahora, si $\tau_{\sigma,i} = \mathrm{id}$ para todo $1 \leq i \leq n$, entonces σ fija a todos los α_i y por ende fija a todo $L = K(\alpha_1, \ldots, \alpha_n)$ ya que fija también a K por definición. Esto prueba que $\sigma = \mathrm{id}$ y por ende el homomorfismo φ es inyectivo. Por lo tanto, G es un subgrupo del grupo finito $\prod_{i=1}^{n} S_{m_i}$. □

El caso de un cuerpo de descomposición

La diferencia entre el segundo de los tres ejemplos acá arriba y los otros dos radica en que el segundo es el único que no es un cuerpo de descomposición. Cuando lidiamos con un cuerpo de descomposición, sabemos que todas las raíces del polinomio están presentes y por ende tenemos más posibilidades para permutarlas, lo que lleva a la existencia de automorfismos en $\mathrm{Aut}(L/K)$. Cuando el cuerpo es solo de ruptura, la existencia de otras raíces no está asegurada, lo que se vio claramente en el segundo caso. Estudiemos pues más en detalle el caso de los cuerpos de descomposición.

Recordemos ante todo que el Teorema 2.11 nos dice que, dado un isomorfismo $\varphi : K \to K'$, un polinomio $P \in K[x]$ y su imagen P' en $K'[x]$, y los cuerpos de descomposición respectivos L y L', existe un homomorfismo $\psi : L \to L'$ que extiende φ. Lo que nunca hicimos en ese entonces, es preguntarnos *cuantos* homomorfismos ψ pueden existir, y esto es crucial para el estudio de $\mathrm{Aut}(L/K)$.

Proposición 3.2. *Sean $K, K', \varphi, P, P', L, L'$ como acá arriba. Entonces el número de isomorfismos $\psi : L \to L'$ que extienden φ es menor o igual a $[L : K]$ y la igualdad se obtiene si y solo si L/K es separable.*

Demostración. Demostraremos el resultado por inducción sobre $n = [L : K]$. El caso $n = 1$ es evidente, ya que entonces $L = K$ y $L' = K'$, por lo que ψ está forzado a ser φ y es por ende único (y nótese que L/K es obviamente separable).

Supongamos ahora que el resultado es válido para todo cuerpo de descomposición de grado menor que n sobre otro cuerpo. Escribamos $P = QR$ con $Q, R \in K[x]$ y Q irreducible y tomemos una raíz α de Q. Si denotamos por Q' y R' las imágenes respectivas de Q y R en $K'[x]$ vía φ, tenemos que $P' = Q'R'$. Entonces, para todo $\psi : L \to L'$ que extiende φ, tenemos que $Q'(\psi(\alpha)) = \psi(Q(\alpha)) = \psi(0) = 0$, por lo que la imagen de α tiene que ser una raíz de Q'. Vemos entonces que toda extensión ψ de φ genera un homomorfismo de cuerpos $\sigma : K(\alpha) \to L'$ dado por la elección de una raíz β del polinomio Q'. Ahora, no hay más que $\deg(Q') = \deg(Q) = [K(\alpha) : K]$ homomorfismos $\sigma : K(\alpha) \to L'$ que extienden $\varphi : K \to K'$ ya que no hay más que $\deg(Q')$ raíces β. Además, la Proposición 2.2 nos asegura que existe un tal homomorfismo para cada raíz β de Q', por lo que hay *exactamente* $[K(\alpha) : K]$ extensiones si y solo si Q' es separable, lo que ocurre si y solo si Q es separable.

Sabiendo que $[L : K] = [L : K(\alpha)][K(\alpha) : K]$, vemos que solo nos falta contar las extensiones de un $\sigma : K(\alpha) \to L'$ dado a isomorfismos $\psi : L \to L'$. Fijemos entonces un tal σ, definamos $\beta = \sigma(\alpha)$ de forma que $\sigma(K(\alpha)) = K'(\beta)$ y notemos que $[K(\alpha) : K] > 1$, por lo que $[L : K(\alpha)] < n$. Está claro que L y L' son los cuerpos de descomposición respectivos de $P \in K(\alpha)[x]$ y $P' \in K'(\beta)$. Podemos entonces usar la hipótesis de inducción con respecto a $K(\alpha), K'(\beta), \sigma, P, P', L, L'$, lo que nos dice que no hay más que $[L : K(\alpha)]$ extensiones $\psi : L \to L'$ de $\sigma : K(\alpha) \to K'(\beta)$, con igualdad si y solo si P es separable.

En conclusión, para cada una de las (a lo más) $[K(\alpha) : K]$ extensiones σ de φ, hay (a lo más) $[L : K(\alpha)]$ extensiones ψ de σ, por lo que hay (a lo más) $[L : K]$ extensiones ψ de φ, con igualdad si y solo si P es separable. □

Aplicando esta proposición al isomorfismo id : $K \to K$ y a $L' = L$, podemos estudiar

$\mathrm{Aut}(L/K)$.

Corolario 3.1. *Sea L el cuerpo de descomposición de un polinomio $P \in K[x]$. Entonces $|\mathrm{Aut}(L/K)| \leq [L:K]$ y se tiene la igualdad si y solo si P es separable.*

3.2. El grupo de Galois, subgrupos y subcuerpos

El tipo de extensiones del último corolario es precisamente el que nos interesa en Teoría de Galois, por lo que les daremos un nombre preciso.

Definición 3.2. *Una extensión finita L/K se dice* de Galois *o* galoisiana *si $|\mathrm{Aut}(L/K)| = [L:K]$. Si L/K es galoisiana, entonces denotamos el grupo $\mathrm{Aut}(L/K)$ por $\mathrm{Gal}(L/K)$ y lo llamamos el* grupo de Galois *de la extensión.*

Observación 3.1. *Esta definición no permite una generalización directa para extensiones infinitas. Resulta además que el resto de la teoría de Galois requiere algunas modificaciones para obtener resultados esperados como la correspondencia entre subextensiones y subgrupos. En estos apuntes solo consideraremos extensiones algebraicas finitas.*

Ejemplo 3.2. *Si L es el cuerpo de descomposición de un polinomio separable $P \in K[x]$, entonces L/K es galoisiana. En ese caso, decimos que $\mathrm{Gal}(L/K)$ es* el grupo de Galois del polinomio *P.*

Ejemplo 3.3 (Cuerpos ciclotómicos)**.** *Sabemos por definición que $\mathbb{Q}(\zeta_n)$ es el cuerpo de descomposición del polinomio $x^n - 1 \in \mathbb{Q}[x]$, polinomio separable ya que corresponde al producto de los polinomios irreducibles (y distintos entre sí) Φ_d para $d|n$, los cuales son todos irreducibles (y por ende separables ya que estamos en característica 0). El Corolario 3.1 nos dice entonces que $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es una extensión galoisiana y que su grupo de Galois es de orden $\varphi(n)$.*

En este caso podemos ir un poco más lejos y afirmar que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. En efecto, como vimos en el caso de $n = 5$ más arriba, basta con definir un isomorfismo

$$(\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \ : \ [a \mod n] \mapsto [\sigma_a : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n) : \zeta_n \mapsto \zeta_n^a].$$

El hecho de que σ_a es un isomorfismo viene de la Proposición 2.2, ya que ζ_n^a es una raíz primitiva de la unidad al igual que ζ_n (i.e. una raíz del polinomio irreducible $\Phi_n = m_{\zeta_n,\mathbb{Q}}$) cuando $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Es un ejercicio fácil entonces el ver que $\sigma_a \circ \sigma_b = \sigma_{ab}$.

Ejemplo 3.4. *Sea $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Entonces la extensión $K/\mathbb{Q}$ es galoisiana y su grupo de Galois es isomorfo al grupo dihedral de orden 8, es decir, al grupo.*

$$D_8 = \langle r, s \mid r^4 = s^2 = 1,\ sr = r^3 s \rangle$$

En efecto, K es el cuerpo de descomposición del polinomio $x^4 - 2$, cuyas raíces son $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $i^2\sqrt[4]{2}$ e $i^3\sqrt[4]{2}$. Siendo todas distintas, vemos que el polinomio es separable y por ende el orden de $\mathrm{Gal}(K/\mathbb{Q})$ es igual a $[K : \mathbb{Q}] = 8$. Ahora, un automorfismo $\varphi : K \to K$ debe cumplir $\varphi(\sqrt[4]{2}) = i^a\sqrt[4]{2}$ con $a \in \{0, 1, 2, 3\}$ y también $\varphi(i) = (-1)^b i$ con $b \in \{0, 1\}$, ya que éstas son las dos raíces de $x^2 + 1 = m_{i,\mathbb{Q}}(x)$. Definamos entonces una aplicación

$$f : \mathrm{Gal}(K/\mathbb{Q}) \to D_8 : \varphi \mapsto r^a s^b,$$

donde a y b son los enteros dados acá arriba. Sabiendo que $|\mathrm{Gal}(K/\mathbb{Q})| = |D_8| = 8$, bastará con demostrar que se trata de un homomorfismo de grupos inyectivo para probar que son isomorfos.

Consideremos entonces dos automorfismos $\varphi, \psi \in \mathrm{Gal}(K/\mathbb{Q})$ y sean $f(\varphi) = r^a s^b$ y $f(\psi) = r^c s^d$ sus respectivas imágenes en D_8. Esto nos dice que

$$\varphi(\sqrt[4]{2}) = i^a(\sqrt[4]{2}), \quad \varphi(i) = (-1)^b i, \quad \psi(\sqrt[4]{2}) = i^c(\sqrt[4]{2}), \quad \psi(i) = (-1)^d i.$$

Vemos entonces que

$$(\varphi \circ \psi)(\sqrt[4]{2}) = \varphi(\psi(\sqrt[4]{2})) = \varphi(i^c\sqrt[4]{2}) = \varphi(i)^c\varphi(\sqrt[4]{2}) = (-1)^{bc} i^c i^a \sqrt[4]{2} = i^{a+c+2bc}\sqrt[4]{2}.$$

y

$$(\varphi \circ \psi)(i) = \varphi(\psi(i)) = \varphi((-1)^d i) = (-1)^d\varphi(i) = (-1)^d(-1)^b i = (-1)^{b+d} i.$$

Por lo tanto, $f(\varphi \circ \psi) = r^{a+c+2bc}s^{b+d} \in D_8$. Por otra parte, un cálculo directo nos dice que $s^b r^c = r^{c+2bc}s^b$, por lo que

$$f(\varphi)f(\psi) = r^a s^b r^c s^d = r^a r^{c+2bc} s^b s^d = r^{a+c+2bc} s^{b+d} = f(\varphi \circ \psi),$$

lo que confirma que tenemos un homomorfismo de grupos.

La inyectividad es evidente, ya que la imagen de φ es trivial si y solo si $\varphi(\sqrt[4]{2}) = \sqrt[4]{2}$ y $\varphi(i) = i$, lo que implica que φ fija a todas las raíces de $x^4 - 2$. Pero K es el cuerpo generado por estas raíces, por lo que φ fija a K y corresponde por ende a la identidad sobre K.

Ejercicio 3.5. *¿Es $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ una extensión galoisiana de $\mathbb{Q}$? Si lo es, calcule su grupo de Galois y diga a qué grupo es isomorfo.*

Ejercicio 3.6. *Encuentre el cuerpo de descomposición y el grupo de Galois del polinomio $P \in \mathbb{Q}[x]$ dado por $P(x) = x^3 - 3x + 1$. ¿A qué grupo es isomorfo? Hint: Verifique que el discriminante del polinomio es un cuadrado en $\mathbb{Q}$ y use la fórmula para las soluciones de una ecuación cúbica.*

Dejando de lado los ejemplos, volvamos a la Teoría de Galois. Asociando un grupo $G = \mathrm{Gal}(L/K)$ a toda extensión galoisiana L/K, la teoría de Galois nos permite mirar y comparar subobjetos en dos contextos distintos: subgrupos $H < G$ y subcuerpos $K \subset M \subset L$. La siguiente proposición nos permite comenzar estas comparaciones.

Proposición 3.3. *Sea L un cuerpo, sea $G = \mathrm{Aut}(L)$ y sea H un subgrupo de G. Entonces el subconjunto $\mathrm{Fix}(H) \subset L$ dado por*

$$\mathrm{Fix}(H) := \{a \in L \mid \sigma(a) = a, \forall\, \sigma \in H\},$$

es un subcuerpo de L.

Definición 3.3. *El subcuerpo dado por la proposición anterior se llama el* cuerpo de los invariantes *o* cuerpo fijo *de H y se denota por L^H.*

Demostración. Siguiendo la Proposición 2.1, todo lo que tenemos que demostrar es que:

- $\forall\, x, y \in \mathrm{Fix}(H)$, $x - y \in \mathrm{Fix}(H)$;
- $\forall\, x, y \in \mathrm{Fix}(H) \setminus \{0\}$, $xy^{-1} \in \mathrm{Fix}(H)$.

Ahora, vemos claramente que, dados $x, y \in \mathrm{Fix}(H)$, para todo $\sigma \in H \subset \mathrm{Aut}(L)$ tenemos que

- $\sigma(x-y) = \sigma(x) - \sigma(y) = x - y$, por lo que $x - y \in \mathrm{Fix}(H)$;
- $\sigma(xy^{-1}) = \sigma(x)\sigma(y)^{-1} = xy^{-1}$ si $y \neq 0$, por lo que $xy^{-1} \in \mathrm{Fix}(H)$.

□

Ejercicio 3.7. *Sea K un cuerpo, $G = \mathrm{Aut}(K)$ y sean $H_1 \leq H_2 \leq G$ subgrupos de G. Pruebe que $\mathrm{Fix}(H_2)$ es un subcuerpo de $\mathrm{Fix}(H_1)$.*

Tenemos entonces una manera de asociar subcuerpos a los subgrupos de un grupo de Galois. Cabe preguntarse si tenemos algo parecido en el sentido inverso. El siguiente lema va en esta dirección.

Lema 3.2. *Sean $K \subset L \subset M$ cuerpos. Entonces $\mathrm{Aut}(M/L)$ es un subgrupo de $\mathrm{Aut}(M/K)$.*

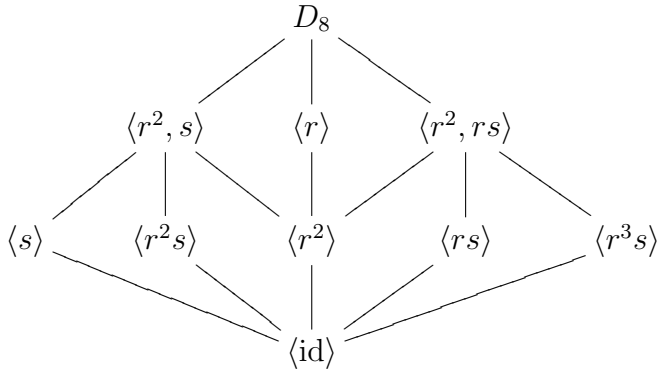
Demostración. Ya vimos a modo de ejercicio que ambos grupos son subgrupos de $\mathrm{Aut}(M)$, por lo que bastará con notar que $\mathrm{Aut}(M/L) \subset \mathrm{Aut}(M/K)$. Ahora, esto es evidente ya que un automorfismo que fija a L forzosamente fija a $K \subset L$. □

El corolario evidente es que, dada una extensión galoisiana L/K de grupo de Galois G, un subcuerpo $K \subset M \subset L$ define un subgrupo de $G = \mathrm{Aut}(L/K)$ sencillamente como $\mathrm{Aut}(L/M)$.

Ejercicio 3.8. *Sea K un cuerpo, $G = \mathrm{Aut}(K)$ y sean $H_1 \leq H_2 \leq G$ subgrupos de G. Pruebe que $\mathrm{Fix}(H_2)$ es un subcuerpo de $\mathrm{Fix}(H_1)$.*

Vemos entonces que, por una parte, a cada subcuerpo de una extensión galoisiana L/K podemos asociarle un subgrupo del grupo de Galois $G = \mathrm{Gal}(L/K)$. Por otra parte, a cada subgrupo del grupo de Galois podemos asociarle un subcuerpo de la extensión. Además, esta ida y vuelta entre cuerpos y grupos invierte las inclusiones gracias a los lemas y ejercicios precedentes. El teorema fundamental de la Teoría de Galois es que esta ida y vuelta es además una biyección, lo cual no tiene nada de evidente. Veamos un ejemplo.

Ejemplo 3.5. *Volvamos al ejemplo de la extensión $K/\mathbb{Q}$ con $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Sea G su grupo de Galois, el cual es isomorfo a D_8 como ya vimos. Intentemos ahora encontrar todos sus subgrupos y de obtener los cuerpos fijos respectivos. Un diagrama de los subgrupos de D_8 es el siguiente:*



Usando el isomorfismo entre G y D_8 que definimos más arriba, podemos interpretar r y s como automorfismos en $\mathrm{Aut}(K/\mathbb{Q})$:

$$r(\sqrt[4]{2}) = i\sqrt[4]{2}, \quad r(i) = i, \quad y \quad s(\sqrt[4]{2}) = \sqrt[4]{2}, \quad s(i) = -i.$$

Así, vemos por ejemplo que el subcuerpo correspondiente al subgrupo $\langle r\rangle$ corresponde al subcuerpo de los elementos fijos por r, por lo que $\sqrt[4]{2} \notin \mathrm{Fix}(\langle r\rangle)$, pero $i \in \mathrm{Fix}(\langle r\rangle)$. Esto nos hace pensar que $\mathrm{Fix}(\langle r\rangle) = \mathbb{Q}(i)$, pero debemos demostrar que no hay más que esto. Notemos entonces que una $\mathbb{Q}$-base del cuerpo K es

$$\{1, i, \sqrt[4]{2}, i\sqrt[4]{2}, \sqrt[4]{2}^2, i\sqrt[4]{2}^2, \sqrt[4]{2}^3, i\sqrt[4]{2}^3\},$$

(para convencerse de esto, basta con notar que los 4 reales son una $\mathbb{Q}(i)$-base de K) y que r

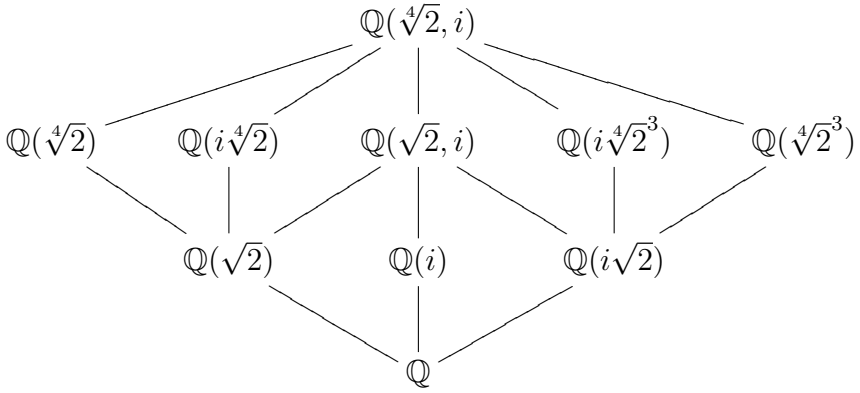
y s corresponden en esta base respectivamente a las matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \quad y \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Un poco de álgebra lineal nos dice entonces que $\mathrm{Fix}(\langle r\rangle)$ *es efectivamente el subespacio de los* $a+bi$ *con* $a,b\in\mathbb{Q}$*, es decir,* $\mathrm{Fix}(\langle r\rangle)=\mathbb{Q}(i)$*. De la misma manera vemos por ejemplo que* $\mathrm{Fix}(\langle s\rangle)$ *es* $\mathbb{Q}(\sqrt[4]{2})$*. Y calculando las matrices correspondientes a los otros elementos de* D_8 *(lo cual es fácil dada la simplicidad de las de* r *y* s*), obtenemos fácilmente la lista siguiente:*

- $\mathrm{Fix}(D_8)=\mathbb{Q}$*;*
- $\mathrm{Fix}(\langle r^2,s\rangle)=\mathbb{Q}(\sqrt{2})$*;*
- $\mathrm{Fix}(\langle r\rangle)=\mathbb{Q}(i)$*;*
- $\mathrm{Fix}(\langle r^2,rs\rangle)=\mathbb{Q}(i\sqrt{2})$*;*
- $\mathrm{Fix}(\langle s\rangle)=\mathbb{Q}(\sqrt[4]{2})$*;*
- $\mathrm{Fix}(\langle r^2s\rangle)=\mathbb{Q}(i\sqrt[4]{2})$*;*
- $\mathrm{Fix}(\langle r^2\rangle)=\mathbb{Q}(\sqrt{2},i)$*;*
- $\mathrm{Fix}(\langle rs\rangle)=\mathbb{Q}(i\sqrt[4]{2}^3)$*;*
- $\mathrm{Fix}(\langle r^3s\rangle)=\mathbb{Q}(\sqrt[4]{2}^3)$*;*
- $\mathrm{Fix}(\langle \mathrm{id}\rangle)=K=\mathbb{Q}(\sqrt[4]{2},i)$*;*

Poniéndolo en forma de diagrama, obtenemos ¡el inverso del diagrama anterior!



Ejercicio 3.9. *Encuentre los subgrupos de* $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ *y los respectivos cuerpos fijos. Haga lo mismo con* $\mathrm{Aut}(\mathbb{Q}(\sqrt{3}, \sqrt{7})/\mathbb{Q})$ *y con* $\mathrm{Aut}(\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q})$*. En los tres casos, dibuje los diagramas respectivos.*

Ejercicio 3.10. *En cada uno de las 3 extensiones* $K/\mathbb{Q}$ *anteriores (ejemplo + ejercicio), considere dos subgrupos* $1 \leq H_1 \leq H_2 \leq G$ *y compare* $[H_2 : H_1]$ *con* $[K^{H_1} : K^{H_2}]$*. ¿Qué puede concluir?*

3.3. El Teorema Fundamental de la Teoría de Galois

Vistos estos ejemplos, uno podría preguntarse si existen otros subcuerpos aparte de los que acabamos de dibujar. Es a esto que responde el siguiente teorema:

Teorema 3.1 (Teorema Fundamental de la Teoría de Galois)**.** *Sea* L/K *una extensión galoisiana de grupo de Galois* G*. Entonces existe una correspondencia biyectiva entre los subcuerpos* $K \subset M \subset L$ *y los subgrupos* $H \leq G$ *dada por*

$$\begin{array}{ccc} \mathcal{C} = \{\mathcal{M} \text{ cuerpo } \mid \mathcal{K} \subset \mathcal{M} \subset \mathcal{L}\} & \longleftrightarrow & \mathcal{G} = \{\mathcal{H} \text{ grupo } \mid \mathcal{H} \leq \mathcal{G}\} \\ M & \mapsto & \mathrm{Aut}(L/M) \\ L^H & \hookleftarrow & H \end{array}$$

Esta correspondencia invierte las inclusiones, es decir, si $M, M' \in \mathcal{C}$ *corresponden respectivamente a* $H, H' \in \mathcal{G}$*, entonces* $M \subset M' \Leftrightarrow H' \leq H$*. Además, en este caso, tenemos que* $[M' : M] = [H : H']$*.*

Para demostrar este resultado, necesitaremos previamente la noción de caracteres de un grupo.

Definición 3.4. *Sea G un grupo y K un cuerpo. Un* carácter *de G con valores en K es un homomorfismo de grupos $\chi : G \to K^*$.*

Esta noción corresponde a la de carácter lineal en el contexto más general de teoría de representaciones.

Dado un grupo G de orden n (puede ser infinito), consideraremos el conjunto de las funciones $\{G \to K\}$ como un K-espacio vectorial de dimensión n, el cual denotaremos por $V_G \simeq K^n$. Un carácter χ puede ser visto entonces como un elemento particular de V_G.

Proposición 3.4. *Sean $\chi_1, \ldots, \chi_n$ caracteres distintos de un grupo G con valores en un cuerpo K. Entonces el conjunto de vectores $\{\chi_1, \ldots, \chi_n\} \subset V_G$ es K-linealmente independiente.*

Demostración. Supongamos por contradicción que el conjunto es linealmente dependiente. Entonces existen elementos $a_1, \ldots, a_n \in K$, no todos nulos, tales que $\sum_{i=1}^n a_i\chi_i = 0 \in V_G$. Como existe al menos una combinación lineal no nula, podemos considerar una de ellas con un número minimal m de a_i no nulos. Salvo reordenamiento de los χ_i, podemos asumir entonces que existen $a_1, \ldots, a_m \in K^*$ tales que $\sum_{i=1}^m a_i\chi_i = 0$ y que no existe una combinación lineal nula con menos sumandos (excepto la trivial).

Ahora, como se trata de funciones, la última igualdad es equivalente a $\sum_{i=1}^m a_i\chi_i(g) = 0$ para todo $g \in G$. Sea ahora $g_0 \in G$ tal que $\chi_1(g_0) \neq \chi_m(g_0)$. Un tal elemento existe ya que $\chi_1 \neq \chi_m$. Entonces podemos escribir $\sum_{i=1}^m a_i\chi_i(gg_0) = 0$ ya que $gg_0 \in G$. Esto nos dice que

$$\sum_{i=1}^m a_i\chi_i(gg_0) = \sum_{i=1}^m a_i\chi_i(g)\chi_i(g_0) = \sum_{i=1}^m \chi_i(g_0)a_i\chi_i(g) = 0 \quad \forall\, g \in G,$$

y por otra parte, multiplicando derechamente la suma original por $\chi_m(g_0)$:

$$\sum_{i=1}^m \chi_m(g_0)a_i\chi_i(g) = 0 \quad \forall\, g \in G.$$

Restando ambas igualdades, tenemos entonces que

$$\sum_{i=1}^{m}(\chi_i(g_0) - \chi_m(g_0))a_i\chi_i(g) = 0 \quad \forall\, g \in G,$$

es decir, $\sum_{i=1}^{m}(\chi_i(g_0) - \chi_m(g_0))a_i\chi_i = 0$, y esta combinación lineal es no trivial ya que $\chi_m(g_0) - \chi_1(g_0) \neq 0$, pero tiene un elemento menos que nuestra combinación original ya que el último término desaparece. Esto contradice la minimalidad de m. □

Notación. *Ya sabemos que todo homomorfismo de cuerpos $\sigma : K \to L$ es inyectivo, lo que nos permitió siempre ver K como un subcuerpo de L. A partir de ahora, estaremos considerando varios homomorfismos $\sigma_i : K \to L$ a la vez, por lo que será importante tener en cuenta el homomorfismo y no solo su imagen como subcuerpo de L. Es por esto que introduciremos la noción de* incrustación*, que no es más que un homomorfismo de cuerpos (forzosamente inyectivo) $\sigma : K \to L$.*

Observación 3.2. *Toda incrustación $\sigma : K \to L$ induce un homomorfismo de grupos multiplicativos $K^* \to L^*$, por lo que a toda incrustación le podemos asociar un carácter χ_σ de K^* con valores en L.*

Corolario 3.2. *Sean $\sigma_1, \ldots, \sigma_n$ incrustaciones distintas de un cuerpo K en un cuerpo L. Entonces el conjunto de los caracteres $\{\chi_{\sigma_i}\}$ es linealmente independiente en V_{K^*}. En particular, si $L = K$, tenemos que distintos automorfismos de un cuerpo K inducen caracteres linealmente independientes.*

Con esto ya podemos demostrar el resultado que nos dará la última línea del Teorema 3.1.

Teorema 3.2. *Sea L un cuerpo, G un subgrupo finito de* $\mathrm{Aut}(L)$ *y sea $K = L^G$. Entonces $[L : K] = |G|$, es decir, $[L : L^G] = |G|$.*

Demostración. Recordemos que los elementos de G pueden ser vistos como incrustaciones $\sigma : L \longrightarrow L$, por lo que los denotaremos por $\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Supongamos que $n > [L : K]$

y lleguemos a una contradicción. Sea $m = [L : K]$. Luego hay una base $w_1, \ldots, w_m$ de L sobre K. Formemos un sistema de ecuaciones que tiene n incógnitas y m ecuaciones

$$\begin{array}{rcl} \sigma_1(w_1)x_1 + & \ldots & +\sigma_n(w_1)x_n = 0 \\ \sigma_1(w_2)x_1 + & \ldots & +\sigma_n(w_2)x_n = 0 \\ \vdots & & \vdots \\ \sigma_1(w_m)x_1 + & \ldots & +\sigma_n(w_m)x_n = 0 \end{array} \qquad (*)$$

Como $n > m$, hay solución no trivial $\beta_1, \ldots, \beta_n \in K$.

Queremos probar que $\forall\, \alpha \in K,\ \sigma_1(\alpha)\beta_1 + \ldots + \sigma_n(\alpha)\beta_n = 0$ con β_i no todos nulos. Por lo tanto, $\sigma_1, \ldots, \sigma_n$ son linealmente dependientes sobre K. Contradicción.

Sean $a_1, \ldots, a_m$ elementos arbitrarios de L, luego $\sigma_j(a_j) = a_j\, \forall\, j$, pues $K = Fix(G) = L^G$.

En el sistema (*) multipliquemos la primera ecuación por a_1, la segunda ecuación por $a_2, \ldots,$ la n-ésima ecuación por a_m y queda:

$$\begin{array}{rcl} \sigma_1(a_1w_1)x_1 + & \ldots & +\sigma_n(a_1w_1)x_n = 0 \\ \sigma_1(a_2w_2)x_1 + & \ldots & +\sigma_n(a_2w_2)x_n = 0 \\ \vdots & & \vdots \\ \sigma_1(a_mw_m)x_1 + & \ldots & +\sigma_n(a_mw_m)x_n = 0 \end{array}$$

Como $\beta_1, \ldots, \beta_n$ es solución no trivial, tenemos

$$\begin{array}{rcl} \sigma_1(a_1w_1)\beta_1 + & \ldots & +\sigma_n(a_1w_1)\beta_n = 0 \\ \vdots & & \vdots \\ \sigma_1(a_mw_m)\beta_1 + & \ldots & +\sigma_n(a_mw_m)\beta_n = 0 \end{array}$$

Sumando, queda:

$$\begin{array}{rcl} \sigma_1(a_1w_1 + a_2w_2 + & \ldots & +a_mw_m)\beta_1 \\ +\sigma_2(a_1w_1 + a_2w_2 + & \ldots & +a_mw_m)\beta_2 \\ \vdots & & \vdots \\ +\sigma_n(a_1w_1 + a_2w_2 + & \ldots & +a_mw_m)\beta_n = 0 \end{array}$$

Como $a_1, \ldots, a_n$ son arbitrarios y $w_1, \ldots, w_n$ es base de L sobre K, se tiene que para cada $\alpha \in L\ \sigma_1(\alpha)\beta_1 + \ldots + \sigma_n(\alpha)\beta_n = 0$, con β_i no todos nulos y así $\{\sigma_1 \ldots \sigma_n\}$ linealmente dependiente sobre K. Contradicción. Por lo tanto, $n \leq [L : K] = m$.

Nos falta eliminar el caso $n < [L : K]$ Probaremos que también en este caso hay contradicción. Como $n < [L : K]$ entonces el número de elementos de L que son linealmente independientes sobre K es mayor que n. Supongamos que $\alpha_1, \ldots, \alpha_{n+1} \in L$ son linealmente independientes sobre K, y consideremos el sistema de ecuaciones:

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \quad \ldots \quad + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \qquad\qquad \vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \quad \ldots \quad + \sigma_n(\alpha_{n+1})x_{n+1} = 0 \end{aligned}$$

de n ecuaciones y $n+1$ incógnitas, luego, hay solución no trivial $\beta_1, \ldots, \beta_{n+1}$ no todos nulos.

$$\sigma_i(\alpha_1)\beta_1 + \sigma_i(\alpha_2)\beta_2 + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0 \quad (M)$$

Además se tiene que al menos uno de los $\beta_i \notin K$. Pues si $\beta_i \in K \, \forall \, i$ entonces $\sigma_1(\alpha_1)\beta_1 + \ldots + \sigma_1(\alpha_{n+1})\beta_{n+1} = 0$ con β_i no todos nulos, $\beta_i \in K$. Contradicción pues $\{\alpha_1, \ldots, \alpha_{n+1}\}$, es linealmente independiente sobre K, y σ_1 automorfismo, luego $\{\sigma_1(\alpha_1), \ldots, \sigma_{n+1}(\alpha_{n+1}\}$ linealmente independiente sobre K.

Entre todas las soluciones $\beta_1, \ldots, \beta_{n+1}$, tomemos un número minimal r con $\beta_i \neq 0$. Reordenando si es necesario quedan $(\beta_1, \ldots, \beta_r)$, con $\beta_i \neq 0 \, \forall \, i = 1, \cdots, r$ mínimo.

Si dividimos por β_r, tenemos $(\beta'_1, \beta'_2, \ldots, \beta'_{r-1}, 1)$ donde $\beta'_i = \frac{\beta_i}{\beta_r}$ y tenemos una expresión.

$$\sigma_i(\alpha_1)\beta'_1 + \ldots + \sigma_i(\alpha_{r-1})\beta'_{r-1} + \sigma_i(\alpha_r) = 0, \beta'_i \neq 0. \, \forall \, i = 1, \ldots, r-1 \quad (M')$$

Supongamos que $\beta_1 \notin K$. Luego, $\beta'_1 \notin K$ cuerpo fijo por G, es decir, $\exists k_0$ tal que $\sigma_{k_0}(\beta'_1) \neq \beta'_1$. Por lo tanto,

$\forall \, j = 1, \ldots, r-1, \; \sigma_{k_0}(\sigma_j(\alpha_1)\beta'_1) + \ldots + \sigma_{k_0}(\sigma_j(\alpha_{r-1})\beta'_{r-1}) + \sigma_{k_0}(\sigma_j(\alpha_r)) = 0$

y

$(\sigma_{k_0} \circ \sigma_j)(\alpha_1)\sigma_{k_0}(\beta'_1) + \ldots + (\sigma_{k_0} \circ \sigma_j)(\alpha_{r-1})\sigma_{k_0}(\beta'_{r-1}) + \sigma_{k_0} \circ \sigma_j(\alpha_r) = 0$

Como G es grupo $\sigma_{k_0} \circ \sigma_1, \ldots, \sigma_{k_0} \circ \sigma_n$ son los σ_i en algún orden. Sea $\sigma_{k_0} \circ \sigma_j = \sigma_i, \; i, j \in \{1, \ldots, n\}$. Tenemos así

$$\sigma_i(\alpha_1)\sigma_{k_0}(\beta'_1) + \ldots + \sigma_i(\alpha_{r-1})\sigma_{k_0}(\beta'_{r-1}) + \sigma_i(\alpha_r) = 0, \; \forall \; i = 1, \ldots, r-1 \quad (N)$$

(M') - (N) :

$$\sigma_i(\alpha_1)[\beta'_1 - \sigma_{k_0}(\beta'_1)] + \ldots + \sigma_i(\alpha_{r-1})[\beta'_{r-1} - \sigma_{k_0}(\beta'_{r-1})] = 0$$

Como $\beta_1' - \sigma_{k_0}(\beta_1') \neq 0$, hay contradicción con la elección de r. Por lo tanto, el caso $n < [L:K]$ lleva a contradicción y finalmente se tiene entonces que $n = [L:K]$ y $|G| = [L:K]$. □

Observación 3.3. *En el teorema anterior tomando* $G = \mathrm{Aut}(L)$ *y* $K = L^G$ *se tiene* $[L:K] = |\mathrm{Aut}(L)|$.

El primer corolario que podemos deducir de este resultado es una generalización del Corolario 3.1.

Corolario 3.3. *Sea* L/K *una extensión finita. Entonces* $|\mathrm{Aut}(L/K)| \leq [L:K]$ *y se tiene la igualdad si y solo si* $K = \mathrm{Fix}(\mathrm{Aut}(L/K))$.

Demostración. Sea $G = \mathrm{Aut}(L/K)$ y sea $K_1 = L^G$. Entonces $K \subset K_1 \subset L$ ya que por definición los elementos de K son fijados por G. Como L/K es finita, el Lema 3.1 nos dice que $\mathrm{Aut}(L/K)$ es un subgrupo finito de $\mathrm{Aut}(L)$. Podemos entonces aplicar el Teorema 3.2, el cual nos dice que $|\mathrm{Aut}(L/K)| = [L:K_1] \leq [L:K]$. Además, como $[L:K] = [L:K_1][K_1:K]$, tenemos igualdad si y solo si $[K_1:K] = 1$, es decir, si y solo si $K = K_1 = L^G = \mathrm{Fix}(\mathrm{Aut}(L/K))$. □

Un segundo corolario inmediato es el siguiente enunciado, el cual nos acerca a la biyección enunciada en el Teorema Fundamental:

Corolario 3.4. *Sea* L *un cuerpo,* G *un subgrupo finito de* $\mathrm{Aut}(L)$ *y* $K = L^G$. *Entonces* $G = \mathrm{Aut}(L/K)$.

Demostración. Está claro que los elementos de G son automorfismos de L que fijan K, por lo que G es un subgrupo de $\mathrm{Aut}(L/K)$. Ahora, el Teorema 3.2 nos dice que $[L:K] = |G|$, mientras que el Corolario 3.3 nos dice que $|\mathrm{Aut}(L/K)| = [L:K]$, por lo que ambos grupos son iguales. □

En particular, con esto ya podemos demostrar un enunciado de "inyectividad".

Corolario 3.5. *Sea L un cuerpo y sean G_1, G_2 subgrupos finitos de* $\mathrm{Aut}(L)$. *Si $L^{G_1} = L^{G_2}$, entonces $G_1 = G_2$.*

Demostración. Supongamos que $L^{G_1} = L^{G_2}$. El Corolario 3.4 nos dice entonces que

$$G_2 = \mathrm{Aut}(L/L^{G_2}) = \mathrm{Aut}(L/L^{G_1}) = G_1,$$

. □

Ya vimos desde el comienzo que el cuerpo de descomposición de un polinomio separable es un ejemplo de extensión galoisiana. Veremos ahora que este ejemplo es en realidad una caracterización de estas extensiones, junto con la noción de extensión *normal*

Teorema 3.3 (Propiedades de una extensión de Galois)**.** *Sea L/K una extensión de cuerpos.*

1. *Si L/K es galoisiana, entonces todo polinomio irreducible en $K[x]$ que tiene una raíz en L tiene todas las raíces en L.*

2. *L/K es galoisiana si y solo si L es el cuerpo de descomposición de un polinomio separable sobre K.*

Demostración. Para demostrar la primera afirmación, notemos ante todo que L/K es una extensión finita. Sea entonces G el grupo finito $\mathrm{Gal}(L/K)$ (cf. el Lema 3.1) y notemos que $K = L^G$ por el Corolario 3.4. Consideremos entonces un polinomio irreducible $P \in K[x]$ y $\alpha \in L$ una raíz de P. Debemos demostrar que toda otra raíz de P está en L.

Escribamos $G = \{\sigma_1, \ldots, \sigma_n\}$ y consideremos los elementos $\sigma_i(\alpha) \in L$ para $1 \leq i \leq n$. Eliminando las posibles repeticiones, esto nos da elementos distintos $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_t \in L$ con $t \leq n$. Como $G = \mathrm{Aut}(L/K)$, la Proposición 3.1 nos dice entonces que estos α_i son todos raíces distintas de P, por lo que el polinomio $Q \in L[x]$ definido por $Q(x) := \prod_{i=1}^{t}(x - \alpha_i)$ divide a P en $L[x]$. Consideremos ahora la acción de G sobre $L[x]$ vía la acción en cada coeficiente. Tenemos que para cada $\tau \in G$,

$$\tau(Q(x)) = \tau\left(\prod_{i=1}^{t}(x - \alpha_i)\right) = \prod_{i=1}^{t}(x - \tau(\alpha_i)).$$

Pero el conjunto de los $\tau(\alpha_i)$ es exactamente el conjunto de los α_i ya que τ no hace más que permutar las raíces de P (y si dos raíces son distintas, entonces sus imágenes por τ lo son también ya que τ es un automorfismo). Tenemos entonces que $\tau(Q) = Q$, por lo que sus coeficientes están en $L^G = K$. En otras palabras, $Q \in K[x]$. Pero sabemos que Q divide a P y este último es irreducible y mónico, por lo que $Q = P$. Vemos entonces que las raíces de P son precisamente los α_i, los cuales están en L. Además, P es separable ya que los α_i son todos distintos.

Para demostrar la segunda afirmación, notemos que el Corolario 3.1 nos indica que el cuerpo de descomposición de un polinomio separable es de Galois, por lo que basta con demostrar la afirmación recíproca. Sea entonces L/K una extensión galoisiana (y por ende finita y separable). Por el Corolario del elemento primitivo, existe $\alpha \in L$ tal que $L = K(\alpha)$ y L es el cuerpo de descomposición del polinomio minimal de α.

□

Observación 3.4. *Una extensión L/K es* normal *si verifica el enunciado número 1 del Teorema 3.3.*

Tenemos entonces varias caracterizaciones de una extensión galoisiana:

- *extensión normal y separable;*
- *cuerpo de descomposición de un polinomio separable;*
- *extensión L/K tal que $K = \mathrm{Fix}(\mathrm{Aut}(L/K))$;*
- *extensión L/K tal que $|\mathrm{Aut}(L/K)| = [L : K]$.*

Ya tenemos entonces todo lo necesario para demostrar el Teorema 3.1, cuyo enunciado reescribimos aquí:

Teorema (Teorema Fundamental de la Teoría de Galois)**.** *Sea L/K una extensión galoisiana con grupo de Galois G. Entonces existe una correspondencia biyectiva entre los subcuerpos*

$K \subset M \subset L$ y los subgrupos $H \leq G$ dada por

$$\begin{array}{ccc} \mathcal{C} = \{\mathcal{M} \text{ cuerpo } \mid \mathcal{K} \subset \mathcal{M} \subset \mathcal{L}\} & \longleftrightarrow & \mathcal{G} = \{\mathcal{H} \text{ grupo } \mid \mathcal{H} \leq \mathcal{G}\} \\ M & \mapsto & \mathrm{Aut}(L/M) \\ L^H & \hookleftarrow & H \end{array}$$

Esta correspondencia invierte las inclusiones, es decir, si $M, M' \in \mathcal{C}$ corresponden respectivamente a $H, H' \in \mathcal{G}$, entonces $M \subseteq M' \Leftrightarrow H' \subseteq H$. Además, en este caso, tenemos que $[M' : M] = [H : H']$.

Demostración. Denotemos por φ_1 (resp. φ_2) las aplicaciones $\mathcal{C} \to \mathcal{G}$ (resp. $\mathcal{G} \to \mathcal{C}$) del enunciado.

Del Corolario 3.4 tenemos que si $H \subseteq G$, entonces $\mathrm{Aut}(L/L^H) = H$, de manera que $\varphi_1 \circ \varphi_2 = \mathrm{id}_{\mathcal{G}}$. Por otra parte, si M es un subcuerpo de L que contiene a K, entonces L/M es una extensión de Galois y por lo tanto $M = L^{\mathrm{Aut}(L/M)}$, de manera que $\varphi_2 \circ \varphi_1 = \mathrm{id}_{\mathcal{C}}$.

Esto prueba en particular que φ_1 y φ_2 son biyecciones. La afirmación sobre la inversión de las inclusiones se deduce inmediatamente del Lema 3.2 y del ejercicio que se encuentra justo después.

Finalmente, si $M \subseteq M' \in \mathcal{C}$ corresponden respectivamente a $H \subseteq H' \in \mathcal{G}$, la igualdad $[M' : M] = [H : H']$ se obtiene a partir de la definición de extensión galoisiana de la siguiente manera:

$$[M' : M] = \frac{[L : M]}{[L : M']} = \frac{|\mathrm{Aut}(L/M)|}{|\mathrm{Aut}(L/M')|} = \frac{|H|}{|H'|} = [H : H'],$$

ya que tanto L/M como L/M' son extensiones galoisianas según lo que demostramos más arriba. □

Recopilemos ahora algunas consecuencias inmediatas de este teorema y de su demostración.

Proposición 3.5. *Sea L/K una extensión de Galois y sea $K \subset M \subset L$ una subextensión, entonces L/M es de Galois y además*

$$[L : M] = |\mathrm{Gal}(L/M)| \qquad y \qquad [M : K] = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|}.$$

□

Proposición 3.6. *Sean $K \subset M \subset L$ cuerpos y supongamos que L/K es de Galois. Entonces M/K es de Galois si y solo si $\mathrm{Gal}(L/M)$ es un subgrupo normal de $\mathrm{Gal}(L/K)$. Además, en ese caso tenemos que $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.*

Demostración. Sean $G = \mathrm{Gal}(L/K)$ y $H = \mathrm{Gal}(L/M) \leq G$. Supongamos que $H \lhd G$ y demostremos que M/K es galoisiana. Sean $g \in G$, $h \in H$ y $x \in M = L^H$. Entonces

$$h(g(x)) = (hg)(x) = (gg^{-1}hg)(x) = g((g^{-1}hg)(x)).$$

Pero $g^{-1}hg \in H$ ya que $H \lhd G$, por lo que $(g^{-1}hg)(x) = x$ ya que $x \in M = L^H$. Vemos entonces que $h(g(x)) = g(x)$ para todo $h \in H$, lo que nos dice que $g(x) \in M = L^H$. En otras palabras, vemos que $g(M) = M$ para todo $g \in G$.

Esto define entonces un homomorfismo de grupos $G \to \mathrm{Aut}(M/K) : g \mapsto g|_M$ cuyo núcleo es H. En efecto, está claro que todo elemento de H actúa trivialmente sobre M, mientras que el Teorema Fundamental nos dice que los elementos de G que actúan trivialmente (i.e. se restringen a la identidad) sobre M son precisamente los elementos de $\mathrm{Aut}(L/M) = H$. Tenemos entonces una inyección $G/H \hookrightarrow \mathrm{Aut}(M/K)$, lo que nos dice que

$$|\mathrm{Aut}(M/K)| \geq |G/H| = \frac{|G|}{|H|} = \frac{[L : K]}{[L : M]} = [M : K].$$

Pero el Corolario 3.3 nos dice que tenemos la desigualdad opuesta, por lo que $|\mathrm{Aut}(M/K)| = [M : K]$ y por ende M/K es galoisiana. Nótese que en particular esto nos da el isomorfismo del enunciado.

Supongamos ahora que M/K es galoisiana y probemos que $H \lhd G$. Como M/K es galoisiana, se trata del cuerpo de descomposición de un cierto polinomio separable $P \in K[x]$.

Sean entonces $g \in G$, $h \in H$ y α un raíz de P. Entonces $g(\alpha)$ es otra raíz de P por la Proposición 3.1. En particular, $g(\alpha) \in M = L^H$, lo que nos dice que

$$(g^{-1}hg)(\alpha) = g^{-1}(h(g(\alpha))) = g^{-1}(g(\alpha)) = (g^{-1}g)(\alpha) = \alpha.$$

Como esto es cierto para toda raíz de P y éstas generan la extensión M/K, vemos que $(ghg^{-1})|_M = \mathrm{id}_M$. Esto implica que $g^{-1}hg \in H$ por el Teorema Fundamental. Siendo esto cierto para todo $g \in G$ y $h \in H$, tenemos que $H \lhd G$. □

Ejercicio 3.11. *Sea $K = \mathbb{Q}(\sqrt[8]{2}, i)$. Pruebe que $K/\mathbb{Q}$ es galoisiana y calcule el grupo* $\mathrm{Gal}(K/\mathbb{Q})$. *Clasifique los subcuerpos de K en un diagrama.*

Ejercicio 3.12. *Sea $L = \mathbb{Q}(\zeta_n)$ el n-ésimo cuerpo ciclotómico y sea $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.*

1. *Pruebe que $[L : K] = 2$ y $[K : \mathbb{Q}] = \frac{\varphi(n)}{2}$.*
2. *Pruebe que L/K y $K/\mathbb{Q}$ son galoisianas.*
3. *Describa* $\mathrm{Gal}(L/K)$ *y* $\mathrm{Gal}(K/\mathbb{Q})$.

Proposición 3.7. *Sea L/K una extensión de Galois y sean M, M' subcuerpos de L que contienen a K. Sean H, H' los subgrupos respectivos de $G = \mathrm{Gal}(L/K)$ según el Teorema Fundamental. Entonces $M \cap M'$ y MM' son subcuerpos de L de grupos correspondientes $\langle H, H' \rangle$ y $H \cap H'$ respectivamente.*

Recordemos que la notación MM' se refiere al composito de M y M', es decir, el subcuerpo más pequeño de L que contiene tanto a M como a M' y que $\langle H, H' \rangle$ es menor subgrupo de G que contiene a H y H'.

Demostración. Notemos que por la propiedad de revertir inclusiones de la correspondencia de Galois, tenemos

$$M \cap M' \subseteq M \Rightarrow \mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/M \cap M')$$

y

$$H \subseteq \langle H, H' \rangle \Rightarrow L^{\langle H, H' \rangle} \subseteq L^H$$

Ordenemos la información que tenemos:

$$\begin{aligned} H = \mathrm{Gal}(L/M) &\subseteq \mathrm{Gal}(L/M \cap M') \\ H' = \mathrm{Gal}(L/M') &\subseteq \mathrm{Gal}(L/M \cap M') \\ \therefore \langle H, H' \rangle &\subseteq \mathrm{Gal}(L/M \cap M') \\ L^{\langle H,H' \rangle} &\subseteq L^H = M \\ L^{\langle H,H' \rangle} &\subseteq L^{H'} = M' \\ \therefore L^{\langle H,H' \rangle} &\subseteq M \cap M' \\ \therefore \mathrm{Gal}(L/M \cap M') &\subseteq \langle H, H' \rangle \end{aligned}$$

Concluimos que $\mathrm{Gal}(L/M \cap M') = \langle H, H' \rangle$ y $L^{\langle H,H' \rangle} = M \cap M'$.

La demostración de que $\mathrm{Gal}(L/MM') = H \cap H'$ y $L^{H \cap H'} = MM'$ es similar y se la dejamos al lector. □

Ejercicio 3.13. *Sea* $K = \mathbb{Q}(\sqrt[8]{2}, i)$. *Pruebe que* $K/\mathbb{Q}$ *es galoisiana y calcule el grupo* $\mathrm{Gal}(K/\mathbb{Q})$. *Clasifique los subcuerpos de* K *en un diagrama.*

Ejemplo 3.6. *Sea* $K = \mathbb{Q}(\xi_n)$ *cuerpo de descomposición de* $f(x) = x^n - 1 \in \mathbb{Q}[x]$, *entonces* $E = \mathbb{Q}(\xi_n + \frac{1}{\xi_n})$ *es cuerpo intermedio entre* K *y* $\mathbb{Q}$

i) Pruebe que $\xi_n + \frac{1}{\xi_n} = 2cos(\frac{2\pi}{n})$.

ii) Encuentre $Gal(K/E)$

iii) Pruebe que $[\mathbb{Q}(\xi_n + \frac{1}{\xi_n}) : \mathbb{Q}] = \frac{\varphi(n)}{2}$.

Solución:

$$\begin{array}{lll} K = & \mathbb{Q}(\xi_n) & K = \mathbb{Q}(\xi_n) \\ & | \text{ de grado } \varphi(n) & | \\ & \mathbb{Q} & E = \mathbb{Q}(\xi_n + \frac{1}{\xi_n}) \\ & & | \\ & & \mathbb{Q} \end{array}$$

Tenemos que $\xi_n = cos(\frac{2\pi}{n}) + i\, sin(\frac{2\pi}{n})$

$$\frac{1}{\xi_n} = \xi_n^{-1} = cos(\frac{2\pi}{n}) - i\, sin(\frac{2\pi}{n})$$

Luego,

$$\xi_n + \frac{1}{\xi_n} = 2cos(\frac{2\pi}{n}).$$

Luego tenemos i).

ii) Sea $E = \mathbb{Q}(\xi_n + \frac{1}{\xi_n})$. Queremos $\sigma : K \longrightarrow K$ automorfismo que deja dijo E. Sabemos que $K/\mathbb{Q}$ es de Galois. Luego, por consecuencia Teoría Fundamental de Galois.

K/E es de Galois y así $[K : E] = |Gal\,(K/E)|$

$$\begin{aligned} \sigma(\xi_n) &= \xi_n^a, \;\; 1 \leq a < n \;\; (n,a) = 1 \\ \sigma(q) &= q, \; \sigma(\xi_n + \tfrac{1}{\xi_n}) = \xi_n + \tfrac{1}{\xi_n} \\ \xi_n^a &= cos(\tfrac{2\pi}{n}a) + i\, sin(\tfrac{2\pi}{n}a) \\ \xi_n^a + \tfrac{1}{\xi_n^a} &= 2cos(\tfrac{2\pi}{n}a) \end{aligned}$$

Para que σ fije E, las únicas posibilidades para a son 1 y $n-1$.

Luego hay 2 automorfismos $\sigma_1 = id_K$, $\sigma_2(\xi_n) = \xi_n^{n-1} = \frac{1}{\xi_n}$, pues $\xi_n^n = 1 = \xi_n \cdot \xi_n^{n-1} = 1$. Luego, $Gal(K/E) \simeq C_2$ grupo cíclico de orden 2.

iii) Tenemos que $\varphi_n = [K : \mathbb{Q}] = [K : E]\,[E : \mathbb{Q}]$

Como $[K : E] = 2$ tenemos que $[E : \mathbb{Q}] = \varphi(n)/2$.

Ejercicio 3.14. *Sea $L = \mathbb{Q}(\zeta_n)$ el n-ésimo cuerpo ciclotómico y sea $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.*

1. *Pruebe que $[L : K] = 2$ y $[K : \mathbb{Q}] = \frac{\varphi(n)}{2}$.*

2. *Pruebe que L/K y $K/\mathbb{Q}$ son galoisianas.*

3. *Describa* $\mathrm{Gal}(L/K)$ *y* $\mathrm{Gal}(K/\mathbb{Q})$.

Ejercicio 3.15. *Sea K un cuerpo finito y sea L/K una extensión finita. Pruebe que L/K es galoisiana y describa* $\mathrm{Gal}(L/K)$ *en función de los cardinales de K y L.*

3.4. Extensiones por Radicales

La noción de *solubilidad por radicales* y la pregunta sobre su existencia son muy antiguas. Ésta se basa en los siguientes hechos: La ecuación cuadrática

$$ax^2 + bx + c = 0,$$

tiene por solución los elementos

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \qquad \text{y} \qquad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

en la cual intervienen raíces cuadradas. Esto ya era conocido por los mesopotámicos a comienzos de la historia. También está el hecho de que las ecuaciones cúbicas admiten fórmulas similares, que usan raíces cúbicas, descubiertas por los matemáticos italianos Niccolò Fontana (más conocido como Tartaglia por su tartamudeo) y Scipione del Ferro, las cuales fueron finalmente publicadas por Girolamo Cardano en su *Ars Magna*. En esta obra encontramos también fórmulas para la ecuación cuártica, las cuales fueron desarrolladas por el alumno de Cardano, Ludovico Ferrari.

Demos pues una definición formal de esta noción de "fórmulas con raíces".

Definición 3.5. *Sea K un cuerpo y $P \in K[x]$ un polinomio. Decimos que P es* soluble por radicales*, si las raíces de P se pueden obtener en términos de los coeficientes de P vía las cinco operaciones algebraicas básicas: suma, resta, multiplicación, división y extracción de raíces (cuadradas, cúbicas, etc.)*

Si bien el Teorema Fundamental del Álgebra garantiza la existencia de las raíces de un polinomio con coeficientes complejos, su demostración no entrega un método para el cálculo de dichas raíces. La solubilidad por radicales es una manera formal de preguntar si existe un tal método y las fórmulas de las que hablábamos más arriba responden a esta pregunta afirmativamente para polonomios de grado ≤ 4, es decir, todo polinomio de grado menor o igual a 4 es soluble por radicales. Es natural el preguntarse entonces si tales fórmulas pueden existir para polinomios de grado arbitario.

Sin embargo, en 1824, el jóven matemático noruego Niels Henrik Abel (quien murió a los 26 años de tuberculosis) dio la primera demostración aceptada de la no solubilidad de la quíntica.

Teorema 3.4 (Teorema de Abel)**.** *Si $P \in K[x]$ es un polinomio* genérico *de grado mayor o igual a 5, entonces P no es soluble por radicales.*

No entraremos en detalles sobre la noción de "polinomio genérico", pero entendamos por esto que si los coeficientes de P son vistos como variables independientes, entonces no existe una fórmula que dependa de estas variables y que nos de las raíces de P usando solo las 5 operaciones básicas.

Todo esto es una consecuencia de un resultado mucho más general, desarrollado por Galois en una de sus memorias.

Teorema 3.5 (Teorema de Galois)**.** *Un polinomio $P \in K[x]$ es soluble por radicales si y solo si su grupo de Galois asociado es soluble.*

Dicho sea de paso que la definición de un grupo soluble viene precisamente de este teorema. Son aquellos grupos que permiten *resolver* las ecuaciones polinomiales a las cuales están asociados.

Empezaremos con extensiones por radicales simples, que son extensiones de un cuerpo F que se obtienen agregando a F una raíz n-ésima de un elemento $a \in F$. Se anotan $F(\sqrt[n]{a})$ y se las llama *extensiones de Kummer.* Para cuerpos de característica p con p primo, se considera extensiones de la forma $F(\rho^{-1}(a))$, se llaman *extensiones de Artin-Schreier,* donde $\rho(x) = x^p - x$ y $\rho^{-1}(a) = x$ sí y sólo sí $\rho(x) = a$ sí y sólo sí $x^p - x = a$.

Definición 3.6. *Una extensión K de F se dice cíclica si es de Galois y $Gal(K/F)$ es un grupo cíclico.*

Proposición 3.8. *Sea F cuerpo que contiene todas las raíces n-ésimas de la unidad y $car(F)$ no divide a n. Entonces $F(\sqrt[n]{a})$ con $a \in F$ es cíclica de grado un divisor de n.*

Demostración. Como F contiene todas las raíces n-ésimas de la unidad se tiene que $K = F(\sqrt[n]{a})$ es el cuerpo de descomposición del polinomio $x^n - a$. Luego K es Galois sobre F.

Se tiene que $\forall\ \sigma \in Gal(K/F)$, $\sigma(\sqrt[n]{a})$ es otra raíz de $x^n - a$, luego $\sigma(\sqrt[n]{a}) = \xi_\sigma(\sqrt[n]{a})$, donde $\xi_\sigma \in G_n$ el grupo de todas las raíces n-ésimas de la unidad. Como F contiene todas las raíces n-ésimas de la unidad, $F \supseteq G_n$.

Definimos $\varphi : Gal(K/F) \longrightarrow G_n, \quad \sigma \longrightarrow \xi_\sigma$. Como $(\sigma \circ \tau)(\sqrt[n]{a}) = \sigma(\tau(\sqrt[n]{a})) = \sigma(\xi_\tau(\sqrt[n]{a})) = \xi_\tau\sigma(\sqrt[n]{a}) = \xi_\tau\xi_\sigma(\sqrt[n]{a}) = \xi_\sigma\xi_\tau\sqrt[n]{a}$. Luego la aplicación anterior es homorfismo de grupos y $Ker(\varphi) = \{id_{Gal(K/F)}\}$, luego φ es inyectiva y $Gal(K/F) \simeq \varphi(Gal(K/F))$ que es subgrupo de G_n. Luego $Gal(K/F)$ es un grupo cíclico y $|Gal(K/F)| = [K : F]$ divide a $n = |G_n|$. □

Proposición 3.9. *Cualquier extensión cíclica de n sobre F cuerpo que contiene todas las raíces n-ésimas de la unidad y $car(F)$ no divide a n es de la forma $F(\sqrt[n]{a})$ para algún $a \in F$*

Demostración. Sabemos que $F \supseteq G_n$. Sea $\sigma \in G = Gal(K/F)$. Para $\alpha \in K, \xi \in G_n$ definamos el resolvente de Lagrange como

$$(\alpha, \xi) = \alpha + \xi\sigma(\alpha) + \xi^2\sigma^2(\alpha) + \cdots + \xi^{n-1}\sigma^{n-1}(\alpha) \ \in K \ \ (*)$$

Al aplicar σ a (α, ξ) queda

$\sigma(\alpha, \xi) = \sigma(\alpha) + \xi\sigma^2(\alpha) + \xi^2\sigma^2(\alpha) + \cdots + \xi^{n-1}\sigma^n(\alpha)$

Pero $\xi^{n-1} = \xi^{-1}$ y $\sigma^n = 1$. Luego reordenado los términos, la expresión anterior queda

$$\sigma(\alpha, \xi) = \xi^{-1}(\alpha, \xi), \ \ \forall\ \alpha \in K, \ \ \forall\ \xi \in G_n \ \ (**)$$

De lo anterior sigue que, $\sigma(\alpha, \xi)^n = (\xi^{-1})^n(\alpha, \xi)^n = (\alpha, \xi)^n$, luego $(\alpha, \xi)^n \in Fix(G) = F$ para cualquier $\alpha \in K$ y cualquier $\xi \in G_n$.

Tomemos ahora ξ_n una raíz n-ésima de la unidad, como $id, \sigma, \cdots, \sigma^{n-1}$ son linealmente independientes, de (*) sigue que hay $\alpha \in K$ tal que $(\alpha, \xi_n) \neq 0$.

Iterando (**) tenemos que

$$\sigma^i(\alpha, \xi_n) = \xi_n^{-i}(\alpha, \xi), \ \ i = 0, 1 \cdots$$

Por lo tanto σ^i no fija (α, ξ_n) para $i < n$. Por lo cual (α, ξ_n) no puede estar en ningún subcuerpo propio de K, luego $K = F((\alpha, \xi_n))$. Como ya vimos que $(\alpha, \xi)^n \in Fix(G) = F$ para cualquier $\alpha \in K$ y cualquier $\xi \in G_n$, se tiene que $(\alpha, \xi_n)^n = a \in F$ y tenemos que $F(\sqrt[n]{a}) = F((\alpha, \xi_n)) = K$. □

En lo que sigue trataremos con cuerpos F de característica 0, luego toda extensión finita de F es separable.

Definición 3.7. *Una extensión K de un cuerpo F se dice que es una extensión radical o por radicales de F, si existe una cadena de subcuerpos*

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = K$$

tal que $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $a_i \in K_i$, $\forall\ i = 0, 1 \cdots, s-1$, o bien $K_{i+1} = K_i(\alpha_i)$, $\alpha_i^{n_i} \in K_i$, $\forall\ i = 0, 1 \cdots, s-1$,

Observación 3.5. *Una extensión por radicales K de F se escribe*

$$K = F(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \cdots, \sqrt[n_{s-1}]{a_{s-1}}),$$

donde $a_1 \in F$, $a_j \in F(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \cdots, \sqrt[n_{j-1}]{a_{j-1}})$, $j = 2, \cdots, s$,
o bien de la forma

$$K = F(b_1, b_2, \cdots, b_{s-1}),$$

donde $b_1 \in F$, $b_j^{n_j} \in F(b_1, b_2, \cdots, b_{j-1})$, $j = 2, \cdots, s$.

Definición 3.8. *Un polinomio $f(x) \in F[x]$ es soluble por radicales sobre F si hay extensión por radical L de F tal que $F \subseteq K \subseteq L$ donde K es el cuerpo de descomposición de $f(x)$ sobre F, es decir, si todas sus raíces están en una extensión por radicales de F.*

Las demostraciones de las dos proposiciones siguientes no sigue lo hecho en el Dummit, si no que es una adaptación de lo hecho por Luis Arenas en sus apuntes.

Ejercicio 3.16. *Sea G grupo finito. Pruebe que son equivalentes:*

i) G es soluble.

ii) G posee una cadena finita de subgrupos $\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_s = G$ tal que para cada i, $H_i \trianglelefteq H_{i+1}$ y los cuocientes H_{i+1}/H_i son cíclicos de orden primo.

iii) G posee una cadena finita de subgrupos $\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_t = G$ tal que para cada i, $N_i \trianglelefteq G$ y los cuocientes N_{i+1}/N_i son abelianos.

Proposición 3.10. *Sea $f(x) \in F[x]$ un polinomio con raíces distintas y K su cuerpo de descomposición de $f(x)$ sobre F. Entonces si $Gal(K/F)$ es un grupo soluble entonces $f(x)$ es soluble por radicales.*

Demostración. Sea $G = Gal(K/F$ un grupo soluble. Sea $n = [K : F]$ y sea ξ_n una raíz primitiva n-ésima de la unidad. Consideremos $F(\xi_n)$ y $K(\xi_n)$. Notemos que $K = F(a_1, \cdots, a_n)$ donde $a_1, \cdots, a_n$ son las raíces distintas de $f(x) = 0$. Además por corolario al teorema 2.15, existe c tal que $K = F(c)$. Entonces $E = K(\xi_n) = F(\xi_n, c)$ y E es Galoisiana sobre F. Además hay homorfismo

$$\phi : Gal(E/F(\xi_n)) \longrightarrow Gal(K/F)$$

donde $\phi(\sigma)$ es la restricción de σ a K. Entonces ϕ es inyectiva y por lo tanto $G = Gal(E/F(\xi_n))$ es soluble.

Luego G posee una cadena finita de subgrupos $\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_s = G$ tal que para cada i, $H_i \trianglelefteq H_{i+1}$ y los cuocientes H_{i+1}/H_i son cíclicos de orden primo, por Ejercicio 3.16. Sean $E_i = Fix(H_i)$ cada i y se tiene por Teorema de Galois que

$$E_0 \supseteq E_1 \supseteq \cdots \supseteq E_s$$

donde E_{i+1} es extensión cíclica de E_i. Como $E_s = Fix(G) = Fix(Gal(E/F(\xi_n))) = F(\xi_n)$, y $E_0 = Fix(H_0) = E$ se tiene que

$$F(\xi_n) \subseteq E_{s-1} \subseteq \cdots \subseteq E_0 = E$$

luego $f(x) = 0$ es soluble por radicales sobre $F(\xi_n)$. Como $F(\xi_n)$ se obtiene de F agregando una raíz de 1 se tiene que $f(x) = 0$ es soluble por radicales sobre F. □

Corolario 3.6. *Sea $f(x) \in F[x]$ de grado ≤ 4, entonces $f(x)$ es soluble por radicales.*

En efecto sabemos que $Gal(K/F)$ donde K es el cuerpo de descomposición de $f(x)$ sobre F, permuta las raíces de $f(x)$.

Luego $Gal(K/F) \simeq S_m \subseteq S_4$, donde $m =$ número de raíces distintas de $f(x)$ y S_4 es un grupo soluble.

Veamos ahora el recíproco de la Proposición anterior.

Proposición 3.11. *Sea $f(x) \in F[x]$ es soluble por radicales y si K es el cuerpo de descomposición de $f(x)$ sobre F entonces $Gal(K/F)$ es un grupo soluble.*

Demostración. Sea $[K : F] = n$ y sea ξ_n una raíz primitiva n-ésima de la unidad. Entonces $F(\xi_n)$ es extensión de Galois de F y $Gal(F(\xi_n)/F)$ es un grupo abeliano por ejercicio 1 de la guía 6. Además como K es extensión Galoisiana finita de F, $K = F(a_1, \cdots, a_t)$. Además por corolario al teorema 2.15, existe c tal que $K = F(c)$. entonces $K(\xi_n) = F(\xi_n, c)$ es también Galoisiana sobre F.

Se concluye que para toda extensión Galoisiana K de F, el grupo $Gal(K(\xi_n)/F(\xi_n))$ es normal en $Gal(K(\xi_n)/F)$ y su cuociente es abeliano, luego soluble, de donde $Gal(K(\xi_n)/F)$ es soluble sí y sólo sí $Gal(K(\xi_n)/F(\xi_n))$ es soluble.

Por otro lado, si ϕ es la restricción de $K(\xi_n)$ a K, se tiene

$$Gal(K/F) \simeq \phi[Gal(K(\xi_n)/F)],$$

es decir, si $Gal(K(\xi_n)/F)$ es soluble también lo es $Gal(K/F)$. En particular podemos suponer entonces que F contiene las raíces n-ésimas de la unidad.

Si K es el cuerpo de descomposición de $f(x)$ sobre F y $f(x)$ es soluble por radicales entonces existe cadena de subcuerpos de L, extensión por radicales de F y $K \subseteq L$.

$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = L, \ K \subseteq L$$

tal que $L_{i+1} = L_i(\sqrt[n_i]{a_i}), \quad a_i \in L_i, \quad \forall\ i = 0, 1 \cdots, s-1$, o sea para cada i, L_{i+1} es una extensión cíclica de L_i. Luego $Gal(L_{i+1}/L_i)$ es cíclico, luego abeliano. Sea $E_i = L_i \cap K$, $i =$

$1, \cdots, s$. Entonces $Gal(E_{i+1}/E_i) = \phi_i[Gal(L_{i+1}/L_i)]$, donde ϕ_i es la restricción de L_{i+1} a E_{i+1}. Sea $G_i = Gal(K/E_i)$. Entonces G_{i+1} es normal en G_i para cada i y por ejercicio **??** $G_i/G_{i+1} \simeq Gal(E_{i+1}/E_i)$ es abeliano.

Tenemos así una cadena de subgrupos

$$G_0 \supseteq G_1 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \supseteq \cdots \supseteq G_s$$

con G_i/G_{i+1} abelianos cada i, $G_0 = Gal(K/E_0) = Gal(K/L_0 \cap K) = Gal(K/F)$ y $G_s = \{id\}$, de donde $Gal(K/F)$ es un grupo soluble. □

Proposición 3.12. *Sea $f(x) \in \mathbb{Q}[x]$ irreducible de grado primo p. Si $f(x)$ tiene exactamente dos raíces no reales en el cuerpo $\mathbb{C}$ entonces $Gal(K/\mathbb{Q})$ es isomorfo a S_p, donde K es cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$.*

Demostración. $[K : \mathbb{Q}] = p$. Luego $f(x)$ tiene dos raíces complejas que son conjugadas y $p - 1$ raíces reales. Sea K el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$, entonces K es galoisiana sobre $\mathbb{Q}$ y sea $G = Gal(K/\mathbb{Q})$. Se tiene que $\sigma : K \longrightarrow K$, definida por $\sigma(\alpha) = \overline{\alpha}$, el conjugado de α es un automorfismo que fija los reales. Luego hay una transposición en G.

Sea u una raíz de $f(x)$, luego $[\mathbb{Q}(u) : \mathbb{Q}] = gr(f(x)) = p$. Se tiene $\mathbb{Q} \subseteq \mathbb{Q}(u) \subseteq K$, y $[K : \mathbb{Q}] = [K : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}]$. Luego, $p \mid [K : \mathbb{Q}]]$ y por lo tanto $p \mid |G|$.

Luego G contiene un ciclo de longitud p y como habíamos visto contiene una transposición luego $G \simeq S_p$. □

Ejercicio 3.17. *Sea $f(x) = x^5 + 2x^3 + 8x^2 - 2$ polinomio irreducible sobre $\mathbb{Q}[x]$ por criterio de Einsenstein para el primo $p = 2$. Averigue si es soluble por radicales.*

Ejemplo 3.7. *(ver Libro de A. Labra y A. Suazo) Demostraremos que el polinomio $f(x) = x^6 + bx^3 + c \in \mathbb{Q}$ es soluble por radicales sobre $\mathbb{Q}$.*

Utilizando la fórmula que permite encontrar las raíces de un polinomio de grado 2, obtenemos que $x^3 = \frac{1}{2}(-b + \gamma)$ o $x^3 = \frac{1}{2}(-b - \gamma)$ donde $\gamma \in \mathbb{C}$ es una raíz cuadrada de $b^2 - 4c$.

Sean α, β en $\mathbb{C}$ raíces de los polinomios $x^3 - \frac{1}{2}(-b+\gamma)$ y $x^3 - \frac{1}{2}(-b-\gamma)$ respectivamente y ω una raíz cúbica primitiva de la unidad. Entonces α, $\alpha\omega$, $\alpha\omega^2$ son raíces de $x^3 - \frac{1}{2}(-b+\gamma)$ y β, $\beta\omega$, $\beta\omega^2$ son raíces de $x^3 - \frac{1}{2}(-b-\gamma)$. Por lo tanto, el cuerpo de descomposición de $f(x)$ es $\mathbb{Q}(\alpha, \beta, \alpha\omega, \alpha\omega^2, \beta\omega, \beta\omega^2) = \mathbb{Q}(\omega, \alpha, \beta)$. Dado que $\alpha^3 = \frac{1}{2}(-b+\gamma) \in \mathbb{Q}(\omega, \alpha, \beta)$, entonces $\gamma \in \mathbb{Q}(\omega, \alpha, \beta)$ y luego $\mathbb{Q}(\omega, \alpha, \beta) = \mathbb{Q}(\gamma, \omega, \alpha, \beta)$. Como, $\gamma^2 \in \mathbb{Q}$, $\omega^3 = 1 \in \mathbb{Q}(\gamma)$, $\alpha^3 \in \mathbb{Q}(\gamma, \omega)$ y $\beta^3 \in \mathbb{Q}(\gamma, \omega, \alpha)$, entonces $f(x) = x^6 + bx^3 + c \in \mathbb{Q}[x]$ es soluble por radicales sobre $\mathbb{Q}$,

Ejercicio 3.18. *a) Considere el polinomio $g(x) = x^3 + px + q \in \mathbb{Q}[x]$, con $pq \neq 0$. Considere la ecuación cuadrática $x^2 + qx - \frac{1}{27}p^3 = 0 \quad (*)$. Vea que las soluciones de (*) son $x_1 = -\frac{1}{2}q + \delta$, $x_2 = -\frac{1}{2}q - \delta \in \mathbb{C}$ y $\delta^2 = \frac{1}{4}q^2 + \frac{1}{27}p^3$. Sea $u \in \mathbb{C}$ tal que $u^3 = x_1$. Si $v = -\frac{p}{3u}p^3$, entonces $v^3 = x_2$. Pruebe que las raíces de $g(x)$ son $u + v, u\xi_3 + v\xi_3^2, u\xi_3^2 + v\xi_3$, donde ξ_3 es una raíz primitiva cúbica de la unidad.*

b) Usando el método del problema anterior encuentre todas las raíces complejas de $g(x) = x^3 + 3ix - 1 - i$.

Ejemplo 3.8. *Todo polinomio $P \in K[x]$ de la forma $P(x) = x^6 + ax^3 + b$ es soluble por radicales. En efecto, una raíz de este polinomio verifica*

$$x^3 = \frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

por lo que, si denotamos $D = a^2 - 4b$, $\alpha = \frac{1}{2}(-a + \sqrt{D})$ y $\beta = \frac{1}{2}(-a - \sqrt{D})$, entonces

$$K \subset K(\sqrt{D}) \subset K(\sqrt[3]{\alpha}, \sqrt{D}) \subset K(\sqrt[3]{\alpha}, \sqrt[3]{\beta}, \sqrt{D}) \subset K(\sqrt[3]{\alpha}, \sqrt[3]{\beta}, \zeta_3, \sqrt{D}),$$

es una cadena de extensiones radicales puras y tal que el último eslabón contiene a las 6 raíces de P.

Ejercicio 3.19. *Sea $P \in \mathbb{Q}[x]$ el polinomio dado por $P(x) = x^5 + 2x^3 + 8x^2 - 2$. Demuestre que P es irreducible y averigue si es soluble por radicales.*

Ejercicio 3.20. *Pruebe que $x^5 - 3$ es soluble por radicales.*

Ejercicio 3.21. *Pruebe que $x^5 - 6x + 3$ no es soluble por radicales.*

4. Algebras

4.1. Generalidades

Sea R un anillo conmutativo con unidad.

Definición 4.1. *Una R-álgebra o un álgebra sobre R es un R-módulo A unitario, sobre el cual se define una aplicación R-bilineal*

$$\begin{aligned} m : A \times A &\to A \qquad \textit{llamada multiplicación en } A \\ (x, y) &\to x \cdot y \end{aligned}$$

es decir,

$$\forall x_1, x_2, y \in A, \qquad m(x_1 + x_2, y) = m(x_1, y) + m(x_2, y),$$

$$\forall x, y_1, y_2 \in A, \qquad m(x, y_1 + y_2) = m(x, y_1) + m(x, y_2),$$

$$\forall x, y \in A, \forall r \in R, \qquad rm(x, y) = m(rx, y) = m(x, ry).$$

A es asociativa sí y sólo sí

$$\forall x, y, z \in A \qquad m(m(x, y), z) = m(x, m(y, z)).$$

A es conmutativa sí y sólo sí

$$\forall x, y \in A \qquad m(x, y) = m(y, x).$$

A tiene elemento uno (o unidad) denotado por 1_A si y sólo si existe $1_A \in A$ tal que

$$\forall x \in A, \qquad m(x, 1_A) = m(1_A, x) = x.$$

Observación: Si A posee elemento uno, éste es único.

Ejemplo 4.1. *Todo cuerpo conmutativo F tiene estructura natural de F-álgebra, asociativa, conmutativa con elemento uno.*

Ejemplo 4.2. *Sea M un R-módulo entonces $A = \pounds_R(M) = \{ f : M \to M \ / \ f \ R\text{-lineal} \}$ es una R-álgebra al definir $f \cdot g = f \circ g \ \ \forall f, g \in A$; y en este caso A es asociativa, con elemento uno y en general no conmutativa.*

Ejemplo 4.3. *(Algebra de funciones). Sea R anillo conmutativo con unidad, y X conjunto no vacio, entonces $R^X = \{f : X \to R \ / \ f \text{ función}\}$ es una R-álgebra bajo la suma y producto de funciones y producto por escalar y en este caso es asociativa, con elemento uno y conmutativa.*

Ejemplo 4.4. *Sea R anillo conmutativo con unidad, entonces R es una $\mathbb{Z}$-álgebra.*

Ejemplo 4.5. *(Algebra de polinomios). Sea R anillo conmutativo con unidad, entonces $R[x]$ es una R-álgebra.*

Ejemplo 4.6. *(Algebra de matrices). Sean A una R-álgebra, $n \geq 1$ entonces*

$$M_n(A) = \{(x_{ij})_{1\leq i\leq n, 1\leq j\leq n} | x_{ij} \in A\}$$

provisto de la suma, de la multiplicación por escalar y el producto usual de matrices es un álgebra sobre R, llamada el álgebra de matrices de $n \times n$ sobre R.

Sea A un álgebra sobre R, con unidad $1_A \neq 0$. Denotemos por $\varepsilon_{ij} = (x_{ij})_{1\leq i\leq n, 1\leq j\leq n}$ la matriz tal que

$$\begin{cases} x_{rs} = 1 & si \ \ r = i \ y \ s = j \\ x_{rs} = 0 & en \ todo \ otro \ caso \end{cases}$$

entonces se tienen las siguientes propiedades:

1. $\varepsilon_{ij}\varepsilon_{kr} = 0 \quad \forall j \neq k$
2. $\varepsilon_{ij}\varepsilon_{jr} = \varepsilon_{ir} \quad \forall i, j, r \in \{1, \ldots, n\}$
3. $\{\varepsilon_{ij}\}_{i,j\in\{1,\ldots,n\}}$ *es una base del A-módulo libre $M_n(A)$ y*

$$(x_{ij})_{i,j} = \sum_{i,j} \varepsilon_{ij} x_{ij} = \sum_{i,j} x_{ij}\varepsilon_{ij} \ \ \forall (x_{ij})_{i,j} \in M_n(A)$$

Ejemplo 4.7. *(Algebra de dimensión finita sobre un cuerpo.) Sean F un cuerpo, A un espacio vectorial de dimensión finita sobre F y $\{e_1, \ldots, e_n\}$ una base de A sobre F, entonces existen escalares $\gamma_{ijk} \in F$ tales que*

$$e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k \qquad \forall i, j \in \{1, \ldots, n\}$$

Estos productos definen sobre A una estructura de álgebra sobre F. Los n^3 escalares γ_{ijk} se llaman las constantes de estructura del álgebra A.

Recíprocamente, dada una familia $\{\gamma_{ijk}\}_{k=1}^{n}$ con i, j fijos, existe una única estructura de álgebra sobre A tal que la tabla de multiplicación es

$$e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k \qquad \forall i, j \in \{1, 2, \ldots, n\}$$

Ejemplo 4.8. *(Algebra de cuaterniones). Sean F cuerpo, car $(F) \neq 2$, $a, b \in F - \{0\}$, A un espacio vectorial sobre F de base $\{1, i, j, k\}$. Definamos*

(*) $\qquad i^2 = a, \quad j^2 = b, \quad ij = -ji = k$

Si usamos asociatividad, se tienen las relaciones siguientes

(**) $\qquad k^2 = -ab; \quad ik = -ki = aj; \quad jk = -kj = -bi.$

Recíprocamente las relaciones (*); (**), $1 \cdot i = i \cdot 1 = i$, $1 \cdot j = j \cdot 1 = j$ y $1 \cdot k = k \cdot 1 = k$ definen sobre A una estructura de F-álgebra asociativa; con unidad $1_A = 1$, no conmutativa. Se llama álgebra de cuaterniones sobre F y se denota por $A = \left(\frac{a,b}{F}\right)$.

En el caso $F = \mathbb{R}$, $a = b = -1$, se tienen los cuaterniones reales descubiertos por Hamilton en 1843 y $\left(\frac{-1,-1}{\mathbb{R}}\right)$ se denota por $\mathbb{H}$.

Definición 4.2. *Sean A una R-álgebra y B un submódulo de A. Se dice que B es una subálgebra de A sí y sólo sí $x \cdot y \in B \ \ \forall x, y \in B$*

Ejemplo 4.9. *Sea A una R-álgebra asociativa, con unidad entonces el conjunto $Z(A) = \{x \in A / x \cdot a = a \cdot x \ \ \forall a \in A\}$ es una subálgebra de A, llamada el centro de A.*

Ejemplo 4.10. *Sea $\{B_i\}_{i \in I}$ una familia no vacía de subálgebras de A, entonces $\cap_{i \in I} B_i$ es una subálgebra de A.*

Ejemplo 4.11. *Sean A una R-álgebra, S un subconjunto de A, $\{B_i\}_{i \in I}$ familia de de subálgebras de A que contienen a S, entonces $\cap_{i \in I} B_i$ es una subálgebra de A que contiene S y es la más pequeña subálgebra de A que contiene S. Se dice que $\cap_{i \in I} B_i$ es la subálgebra de A generada por S y que S es un sistema de generadores para ésta subálgebra.*

Observación 4.1. *Sea A una R-álgebra asociativa con unidad $1_A \neq 0$ entonces $\varphi : R \to Z(A), \quad \alpha \to \alpha \cdot 1_A$ es un homomorfismo de anillos. Recíprocamente sea A un anillo con unidad, entonces cualquier homomorfismo de anillos de R en $Z(A)$ provee a A de una estructura de R-módulo y por lo tanto A es una R-álgebra. Además, si $\varphi : R \to Z(A)$ es inyectivo entonces $R \simeq \varphi(R)$, que es un subanillo de $Z(A)$.*

Ejemplo 4.12. *Sean F cuerpo y A una F-álgebra asociativa con unidad $1_A \neq 0$ entonces $\varphi : F \to Z(A)$ es inyectiva y F puede identificarse con un subanillo del centro de A.*

Definición 4.3. *Un álgebra de división D es una R-álgebra $D \neq \{0\}$ con unidad en la que todo elemento no nulo es invertible.*

Ejemplo 4.13. $\mathbb{H}$ *es un álgebra de división. En efecto, sea $x = a_0 + a_1 i + a_2 j + a_3 k$, entonces su conjugado es $\bar{x} = a_0 - a_1 i - a_2 j - a_3 k$. Se tiene*

$$x\bar{x} = a_0^2 + a_1^2 + a_2^2 + a_3^2 = N(x).$$

$$x \neq 0 \quad \Rightarrow \quad x^{-1} = \frac{\bar{x}}{N(x)} \in H$$

Definición 4.4. *Sean A una R-álgebra, I un submódulo de A. Se dice que:*

1. *I es un ideal izquierdo de A sí y sólo sí $a \cdot y \in I \ \forall a \in A \ \forall y \in I$.*
2. *I es un ideal derecho de A sí y sólo sí $y \cdot a \in I; a \cdot y \in I \wedge y \cdot a \in I \ \forall a \in A \ \forall y \in I$,*
3. *I es un ideal bilátero de A sí y sólo sí I es un ideal por la izquierda y por la derecha de A.*

Definición 4.5. *Un álgebra A es simple sí y sólo sí $A \neq \{0\}$ y no tiene ideales propios.*

Lema 4.1. *Sean D un álgebra de división, $n \geq 1$ entonces $M_n(D)$ es simple.*

Demostración. Sean I ideal de $M_n(D)$, $I \neq \{0\}$ y $X = (x_{ij})_{i,j} \in M_n(D)$

$$I \neq \{0\} \Rightarrow \exists Y = (y_{ij})_{i,j} \in M_n(D), \ Y \in I - \{0\}$$

Supongamos que $y_{rs} \neq 0$, luego y_{rs} es invertible en D y

$$X = (x_{ij})_{i,j} = \sum_{i,j} \varepsilon_{ij} x_{ij} = \sum_{i,j} \varepsilon_{ir} Y \varepsilon_{sj} y_{rs}^{-1} x_{ij}$$

Como $Y \in I$ e I es ideal de $M_n(D)$ se tiene que $X \in I$ y $M_n(D) \subset I$.

Por lo tanto, $M_n(D)$ es simple. □

4.2. Homorfismos de álgebras

Definición 4.6. *Sean A, A' dos R-álgebras. Se dice que una función $f : A \to A'$ es un homomorfismo de álgebras sí y sólo sí f es un homomorfismo de módulos y $f(a \cdot b) = f(a)f(b)$ $\forall\, a, b \in A$, es decir,*

i) $f(a+b) = f(a) + f(b)$ $\forall\, a, b \in A$,

ii) $f(ra) = rf(a)$ $\forall\, r \in R$, $\forall\, a \in A$,

iii) $f(a \cdot b) = f(a)f(b)$ $\forall a, b \in A$.

Observación 4.2. *En el caso en que A y A' tengan elemento uno se pide que $f(1_A) = 1_{A'}$. Esto se consigue, por ejemplo, cuando f es epiyectiva.*

En forma natural se definen los conceptos de isomorfismo, y automorfismo de álgebras.

Observación 4.3. *$\phi : A \longrightarrow A'$ homomorfismo de álgebras, entonces, $Ker(\phi)$ es un ideal de A.*

Observación 4.4. *A simple y $\phi : A \longrightarrow A'$ homomorfismo de álgebras, $\phi \neq 0$, entonces, ϕ es inyectiva.*

En efecto sea $\phi \neq 0$, luego $Ker(\phi) \neq A$ y como $Ker(\phi)$ es ideal de A y A simple se tiene que $Ker(\phi) = \{0\}$.

Sea I ideal de una R-álgebra A. Para cada $x, y \in A$, definimos la relación $x \equiv y \ (mod\ I) \iff x - y \in I$. Entonces $\equiv$ es de equivalencia y sus clases de equivalencia se anotan $x + I$ con $x \in A$. Entonces el conjunto cuociente $A/I = \{x + I / x \in A\}$ es un R-álgebra con:

i) $(x+I)+(y+I)=(x+y)+I \quad \forall x,y \in A.$

ii) $\alpha(x+I)=\alpha x+I \ \forall \alpha \in R, \ \forall x \in A.$

iii) $(x+I)+(y+I)=xy+I \quad \forall x,y \in A.$

A/I se llama el álgebra cuociente de A por I.

Teorema 4.1. *Sea I ideal de A, entonces: $\pi : A \longrightarrow A/I$, $x \longrightarrow x+I$ es un epimorfismo de núcleo I. Claramente, es un epimorfismo y*

$$\begin{aligned} Ker(\pi) &= \{x \in A \ / \ \pi(x)=0_{A/I}\} \\ &= \{x \in A \ / \ x+I=I\} \\ &= \{x \in A \ / \ x \in I\}=I \end{aligned}$$

Teorema 4.2. *Sea $\phi : A \longrightarrow A'$ homomorfismo de R-álgebras, entonces, $A/Ker(\phi) \cong \phi(A)$. En efecto*

$$\begin{aligned} \psi : A/Ker(\phi) &\longrightarrow \phi(A) \\ a+Ker(\phi) &\longrightarrow \phi(a) \end{aligned}$$

es el homomorfismo pedido.

Teorema 4.3. *Sean I, J ideales de algún álgebra A sobre R, entonces:*

$$I+J/J \cong I/I \cap J$$

Demostración. Debemos definir un epimorfismo $\varphi : I+J \longrightarrow I/I \cap J$ de álgebras de núcleo J. Si definimos $\varphi(i+j)=i+I \cap J$ se cumple lo pedido. Lo único que debemos ver que φ está bien definida. Sean $i+j=i_1+j_1$. Luego $i-i_1=j_1-j \in J$, pero $i-i_1 \in I$. Luego $i-i_1 \in I \cap J$ y tenemos $i+I \cap J=j+I \cap J$. □

Proposición 4.1. Existencia de homomorfismo de álgebras

Sean A, B, C tres R-álgebras. Sean $\phi : A \to B$, $\pi : A \to C$ homomorfismos de R-álgebras y π epiyectivo. Entonces existe un único homomorfismo de álgebras $f : C \to B$ tal

que $f \circ \pi = \phi$, *es decir, el siguiente diagrama conmuta*

$$\begin{array}{ccc} A & \overset{\phi\, homo}{\longrightarrow} & B \\ \pi\ epi \downarrow & \nearrow & \exists! f\ homo \\ C & & \end{array}$$

$\Leftrightarrow ker(\pi) \subseteq ker(\phi)$,

Demostración. Supongamos que hay homomorfismo de álgebras $f : C \to B$ tal que $f \circ \pi = \phi$. Sea $x \in Ker(\pi)$, luego $\pi(x) = 0$, y $\phi(x) = (f \circ \pi)(x) = f(\pi(x)) = f(0) = 0$. Por lo tanto $\phi(x) = 0$ y $x \in Ker(\phi)$.

Supongamos ahora que $Ker(\pi) \subseteq Ker(\phi)$. Definamos $f : C \longrightarrow B$ por $f(p) = \phi(x)$, donde $p = \pi(x)$, pues π es epiyectiva. Veamos que f está bien definida. Sea $p_1 = p_2$. Como π es epiyectiva, hay $x_1, x_2 \in A$ tal que $p_1 = \pi(x_1) \wedge p_2 = \pi(x_2)$. Ya que $p_1 = p_2$ se tiene que $\pi(x_1) = \pi(x_2)$ y $\pi(x_1 - x_2) = 0$. Por lo tanto, $x_1 - x_2 \in Ker(\pi) \subseteq Ker(\phi)$ y $\phi(x_1 - x_2) = 0$, de donde $\phi(x_1) = \phi(x_2)$. Por lo tanto $f(p_1) = f(p_2)$. Por la misma definición de f se tiene que $f \circ \pi = \phi$.

La unicidad de f tal que $f \circ \pi = \phi$ se obtiene del hecho de que π es epiyectiva, o sea, $\pi(A) = C$.

Falta sólo probar que $f : C \to B$ es homomorfismo de álgebras.

Sean $p_1, p_2 \in C$ y $r \in R$. Por ser π es epiyectiva hay $x_1, x_2 \in A$ tal que $p_1 = \pi(x_1) \wedge p_2 = \pi(x_2)$. Entonces

$f(p_1+p_2) = g(\pi(x_1)+\pi(x_2)) = g(\pi(x_1+x_2)) = \phi(x_1+x_2) = \phi(x_1)+\phi(x_2) = f(p_1)+f(p_2)$.

En forma similar se prueba que para todo $r \in R$, y para todo $p_1 \in C$, se tiene $g(rp_1) = rg(p_1)$. Luego f es homomorfismod e R-módulos.

Finalmente, sean $p_1, p_2 \in C$. Por ser π es epiyectiva hay $x_1, x_2 \in A$ tal que $p_1 = \pi(x_1) \wedge p_2 = \pi(x_2)$. Entonces

$f(p_1p_2) = g(\pi(x_1)\pi(x_2)) = g(\pi(x_1x_2)) = \phi(x_1x_2) = \phi(x_1)\phi(x_2) = f(p_1)f(p_2)$.

Luego f es homomorfismo de R-álgebras.

□

4.3. Producto Tensorial de Álgebras.

Previamente, necesitamos definir aplicaciones bilineales y el producto tensorial de dos R-módulos M y N.

Definición 4.7. *Sean M N, y T tres R-módulos. Una aplicación $\varphi : M \times N \longrightarrow T$ se dice bilineal sí y sólo sí satisface:*

1. $\varphi(x + rx', y) = \varphi(x, y) + r\varphi(x', y) \ \ \forall\, x, x' \in M, y \in N, r \in R,$
2. $\varphi(x, y + ry') = \varphi(x, y) + r\varphi(x, y') \ \ \forall\, x \in M, y, y' \in N, r \in R,$

Observación 4.5. *Dada una aplicación $\varphi : M \times N \longrightarrow T$, para cada $a \in M, b \in N$ se definen las aplicaciones $\varphi_a : N \longrightarrow T$ por $\varphi_a(n) = \varphi(a, n)\ \forall\ n \in N$ y $\varphi_b : M \longrightarrow T$ por $\varphi_b(m) = \varphi(m, b)\ \forall\ m \in M$. Se tiene que φ bilineal sí y sólo sí φ_a y φ_b lineales cada $a \in M, b \in N$.*

Observación 4.6. *Si $\varphi : M \times N \longrightarrow T$ es una aplicación bilineal, entonces $\varphi(x, 0) = 0,\ \forall\, x \in M,$ y $\varphi(0, y) = 0,\ \forall\, y \in N$.*

Definición 4.8. *Se llama imagen de la aplicación bilineal $\varphi : M \times N \longrightarrow T$ al submódulo de T generado por el conjunto $\varphi(M \times N) = [\varphi(M \times N)]$*

$$= \{ \sum_{finita} \alpha_i \varphi(m_i, n_i) / \alpha_i \in R,\ m_i \in M,\ n_i \in N\}$$

$$= \{ \sum_{finita} \varphi(m_i', n_i) / m_i' \in M,\ n_i \in N\}$$

Ejercicio 4.1. *Sean R-módulos M, N y T tres R-módulos. Pruebe que*

1. *$Bil(M \times N; T) = \{\varphi : M \times N \longrightarrow T \mid \varphi$ bilineal $\}$ es un R-módulo.*
2. *Si $\varphi : M \times N \longrightarrow T$ es bilineal y $g : T \longrightarrow L$ es lineal con L un R-módulo entonces $g \circ \varphi : M \times N \longrightarrow L$ es bilineal.*

Ejemplo 4.14. *Sean T un $\mathbb{Z}$-módulo, $m, n \in \mathbb{N}$ tales que $(m, n) = 1$ y $\varphi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow T$ aplicación bilineal. Pruebe que $\varphi = 0$.*

Definición 4.9. *Un producto tensorial de dos R-módulos M y N es un par (T, φ) donde T es un R-módulo y $\varphi : M \times N \longrightarrow T$ es una aplicación bilineal tal que cumple la siguiente propiedad universal: $\forall$ P, R-módulo y $\forall \psi : M \times N \longrightarrow P$ bilineal $\exists! f : T \longrightarrow P$ función R-lineal tal que $f \circ \varphi = \psi$, es decir, el diagrama siguiente conmuta.*

$$\begin{array}{ccc} M \times N & \overset{\forall\, \psi\, bil}{\longrightarrow} & P \\ bil\, \varphi \downarrow & \nearrow & \exists! f\, lineal \\ T & & \end{array}$$

Proposición 4.2. *Si (T, φ) es un producto tensorial para M y N, entonces $T = [\varphi(M \times N)] =$ submódulo generado por $\varphi(M \times N)$*

Demostración. Como (T, φ) es un producto tensorial para M se tiene y N, se tiene:

$$\begin{array}{ccc} M \times N & \overset{\forall\, \psi\, bil}{\longrightarrow} & [\varphi(M \times N)] \\ bil\, \varphi \downarrow & \nearrow & \exists! f\, lineal \\ T & & \end{array}$$

$\exists! f$ tal que $f \circ \varphi = \psi$ que conmuta el diagrama.

Sea

$$\begin{array}{rcl} \psi : M \times N & \longrightarrow & [\varphi(M \times N)] \\ (m, n) & \longrightarrow & \varphi(m, n) \end{array}$$

ψ es bilineal, pues φ lo es.

Luego, por propiedad Universal del Producto tensorial

$$\exists! f : T \longrightarrow [\varphi(M \times N)]$$

R-lineal, tal que $f \circ \varphi = \psi$

Sabemos que $[\varphi(M \times N)] \subseteq T$, nos falta probar que $T \subseteq [\varphi(M \times N)]$.

Tenemos

$$\begin{array}{ccc} M \times N & \stackrel{\varphi}{\longrightarrow} & T \\ bil\,\varphi \downarrow & \nearrow & \exists! id_T \ lineal \\ T & & \end{array}$$

Luego existe única $id_T : T \longrightarrow T$ lineal tal que $id_T \circ \varphi = \varphi$.

Sea $g : T \longrightarrow T$ definida por $g(t) = f(t) \in [\varphi(M \times N)] \subseteq T$. Entonces g es lineal y $\forall\ (x, y) \in M \times N,\ (g \circ \varphi)(x, y) = g(\varphi(x, y)) = f(\varphi(x, y)) = \psi(x, y) = \varphi(x, y)$ por definición de la función ψ. Por lo tanto, $g \circ \varphi = \varphi$ de donde $g = id_T$.

Luego,

$$T = id_T(T) = g(T) = f(T) \subseteq [\varphi(M \times N)].$$

□

Proposición 4.3. *i) Sean (T, φ) y (T', φ') dos productos tensoriales para M y N. Entonces $\exists! f : T \longrightarrow T'$ isomorfismo de módulos tal que $f \circ \varphi = \varphi'$.*

ii) Si (T, φ) es producto tensorial de M y N y $f : T \longrightarrow T'$ es isomorfismo, entonces $(T', f \circ \varphi)$ es producto tensorial para M y N.

Demostración. i) (T, φ) producto tensorial para M y N

$$\begin{array}{ccc} M \times N & \stackrel{\forall\, \psi\ bil}{\longrightarrow} & T' \\ \varphi \downarrow & \nearrow & \exists! f \\ T & & \end{array}$$

Definamos $\psi(m, n) = \varphi'(m, n)$, entonces ψ es bilineal pues φ' lo es.

Luego, $\exists! f : T \longrightarrow T'$ lineal tal que $f \circ \varphi = \psi$

$$\text{luego } (f \circ \varphi)(m, n) = \psi(m, n) = \varphi'(m, n),\ \forall\, (m, n) \in M \times N.$$

y $f \circ \varphi = \varphi'$.

Como (T', φ') producto tensorial de M y N se tiene

$$\begin{array}{ccc} M \times N & \stackrel{\psi_1\ bil}{\longrightarrow} & T \\ \varphi'\ bil \downarrow & \nearrow & \exists! g \ lineal \\ T' & & \end{array}$$

Definamos $\psi_1(m,n) = \varphi(m,n) \ \forall \ (m,n) \in M \times N$. Entonces ψ_1 es bilineal.

Luego por propiedad del producto tensorial $\exists! g : T' \longrightarrow T$ lineal, tal que $g \circ \varphi' = \psi_1$.

Probemos que $g = f^{-1}$

$$\begin{aligned}(g \circ f) \circ \varphi(m,n) &= g \circ (f \circ \varphi)(m,n) \\ &= g \circ \varphi'(m,n) \\ &= \psi_1(m,n) = \varphi(m,n), \forall (m,n) \in M \times N.\end{aligned}$$

Luego $(g \circ f) \circ \varphi = \varphi$ pero $T = [\varphi(M \times N)]$ de donde $g \circ f = id_T$

Nos falta probar que $f \circ g = id_{T'}$. Recordemos que $T' = [\varphi'(M \times N)]$

$$\begin{aligned}(f \circ g) \circ \varphi'(m,n) &= f \circ (g \circ \varphi'(m,n)) = f \circ \psi_1(m,n) \\ &= f \circ \varphi(m,n) = \varphi'(m,n)\end{aligned}$$

Luego, $f \circ g \circ \varphi' = \varphi'$, pero $T' = [\varphi'(m,n)]$ de donde $f \circ g = id_{T'}$. Por lo tanto $f^{-1} = g$ y f es un isomorfismo.

ii) Sea (T, φ) es producto tensorial para M y N y $f : T \longrightarrow T'$ isomorfismo de R-módulo. Probemos que $(T', f \circ \varphi)$ es producto tensorial para M y N.

Sea P un R-módulo y $\psi : M \times N \longrightarrow P$ bilineal. Por encontrar única $g : T' \longrightarrow P$ lineal tal que $g \circ (f \circ \varphi) = \psi$.

Tenemos el diagrama

$$\begin{array}{ccc} M \times N & \xrightarrow{\forall \psi} & P \\ \varphi \downarrow & & \\ T & & \\ f \downarrow & & \\ T' & & \end{array}$$

Como (T, φ) es producto tensorial para M, N, $\exists! h : T \longrightarrow P$ lineal tal que $h \circ \varphi = \psi$. (*)

$$\begin{array}{ccc} M \times N & \xrightarrow{\forall \psi} & P \\ \varphi \ bil \downarrow & \nearrow & \exists! h \ lineal \\ T & & \\ f \downarrow & & \\ T' & & \end{array}$$

f es isomorfismo luego $\exists f^{-1}$ lineal $f^{-1}: T' \longrightarrow T$.

Sea $g = h \circ f^{-1}: T' \longrightarrow P$ entonces g es lineal y

$$\begin{aligned} g \circ (f \circ \varphi) &= (h \circ f^{-1}) \circ (f \circ \varphi) = h \circ (f^{-1} \circ f) \circ \varphi \\ &= h \circ id_t \circ \varphi = h \circ \varphi = \psi \text{ por } (*) \end{aligned}$$

Veamos unicidad de g tal que $g \circ (f \circ \varphi) = \psi$ $(**)$

Como $g = h \circ f^{-1}$, si hay g' que cumple $(**)$ entonces habría dos h que cumplen $h \circ \varphi = \psi$ $(*)$. Contradicción.

□

Vimos que dados M y N R-módulos si existe un producto tensorial (T, φ) para M y N éste, es único (salvo isomorfismo) por proposición 4.3 parte i) y se anota:

$$T = M \otimes_R N$$

$$\begin{aligned} \varphi: M \times N &\longrightarrow M \otimes N \qquad \text{es bilineal} \\ (x, y) &\longrightarrow \varphi(x, y) = x \otimes y \end{aligned}$$

$$(x + x') \otimes y = x \otimes y + x' \otimes y \quad \forall\ x, x' \in M,\ \forall y \in N.$$

$$x \otimes (y + y') = x \otimes y + x \otimes y \quad \forall\ x \in M,\ \forall y, y' \in N.$$

$$\alpha x \otimes y = (\alpha x) \otimes y,\ \alpha x \otimes y = x \otimes \alpha y\ \forall\ x \in M,\ y \in N,\ \alpha \in R.$$

Además $M \otimes_R N = [\varphi(M \otimes N)]$, por lo tanto,

$$\forall\, z \in M \otimes_R N, z = \sum_{i=1}^{k} \varphi(m_i, n_i) = \sum_{i=1}^{k} m_i \otimes n_i$$

y la Propiedad Universal queda

$$\forall\ P,\ \forall\ \psi: M \times N \longrightarrow P \text{ bilineal}, \exists! f: M \otimes_R N \longrightarrow P \text{ lineal tal que } f \circ \varphi = \psi.$$

$$\begin{array}{ccc} M \times N & \xrightarrow{\forall \psi} & P \\ \varphi \downarrow & \nearrow & \exists! f \\ M \otimes_R N & & \end{array}$$

Nota: Dados M y N dos R-módulos, $T = M \otimes_R N$, $\varphi : M \otimes_R N \ \ (x, y) \longrightarrow x \otimes y$. Entonces Bil $(M \times N, P) \simeq Hom_R(M \otimes_R N, P) \quad \forall\, P,\ R$-módulo.

Antes de probar la existencia del producto tensorial de dos R-módulos M y N veamos algunos ejercicios.

Ejercicio 4.2. $R \otimes_R M \simeq M$.

$$\begin{array}{ccc} R \times M & \overset{\forall\, \psi\ bil}{\longrightarrow} & M \\ \varphi\ bil \downarrow & \nearrow & \exists! f\ lineal \\ R \otimes_R M & & \end{array}$$

Sea $\psi : R \times M \longrightarrow M,\ \psi(\alpha, m) = \alpha m$. ψ es bilineal. Luego $\exists! f : R \otimes_R M \longrightarrow M$ lineal, tal que $f \circ \varphi = \psi$. Así, $\forall\, \alpha \in R,\ \forall\, y \in M$,

$$\begin{aligned} (f \circ \varphi)(\alpha, y) &= \psi(\alpha, y) \\ f(\alpha \otimes y) &= \alpha y \end{aligned}$$

Definamos: $g : M \longrightarrow R \otimes_R M,\ \ m \longrightarrow 1 \otimes m$. Entonces g es lineal y $(g \circ f)(\alpha \otimes y) = g(\alpha y) = 1 \otimes \alpha y = \alpha \otimes y$. Luego, $(g \circ f)(z) = z\ \ \forall\ z \in R \otimes_R M$. De donde, $g \circ f = id_{R \otimes_R M}$.

Ejercicio 4.3. $M \otimes_R N \simeq N \otimes_R M$.

Ejemplo 4.15. *Sea F cuerpo, entonces* $F[x] \otimes_F F[y] \simeq F[x, y]$

Tenemos que

$$F[x, y] = \left\{ \sum_{ij} a_{ij} x^i y^j \mid a_{ij} \in F \right\}$$

y el diagrama siguiente

$$\begin{array}{ccc} F[x] \times F[y] & \overset{\forall\, \psi\ bil}{\longrightarrow} & F[x, y] \\ \varphi\ bil \downarrow & & \exists! f\ lineal \\ F[x] \otimes_F F[y] & & \end{array}$$

donde $\varphi(p(x), q(x)) = p(x) \otimes q(x)$, es bilineal.

Definamos $\psi(\sum_{i=0}^{n} a_i x^i,\ \sum_{j=0}^{t} b_j y^j) = \sum_i \sum_j a_i b_j x^i y^j$. Entonces ψ es bilineal.

Luego $\exists! f : F[x] \otimes_F F[y] \longrightarrow F[x,y]$ lineal, tal que $f \circ \varphi = \psi$. Por lo tanto,

$$f\Big(\sum_{i=0}^{n} a_i x^i \otimes \sum_{j=0}^{t} b_j y^j\Big) = \sum_i \sum_j a_i b_j x^i y^j$$

Encontremos $f^{-1} = g$

Sea $g : F[x,y] \longrightarrow F[x] \otimes_F F[y]$, definida por:

$$g\Big(\sum_{i,j} a_{ij} x^i y^j\Big) = \sum_{i,j} a_{ij} x^i \otimes y^j$$

Entonces g es lineal y

$$\begin{aligned}(g \circ f) \quad & (\textstyle\sum_i a_i x^i \otimes \sum_j b_j y^j) \\ = \quad & g(f(\textstyle\sum_i a_i x^i \otimes \sum_j b_j y^j)) \\ = \quad & g(\textstyle\sum_{i,j} a_i b_j x^i y^j) \\ = \quad & \textstyle\sum_{i,j} a_i b_j x^i \otimes y^j \\ = \quad & \textstyle\sum_i a_i x^i \otimes \sum_j b_j y^j\end{aligned}$$

pues $\otimes$ es bilineal, luego $g \circ f = id_{F[x] \otimes_F F[x]}$. Por otro lado,

$$\begin{aligned}(f \circ g) \quad & (\textstyle\sum_{i,j} a_{ij} x^i y^j) \\ = \quad & f(\textstyle\sum_{i,j} a_{ij} x^i \otimes y^j) \\ = \quad & \textstyle\sum_{i,j} a_{ij} x^i y^j\end{aligned}$$

Por lo tanto $f \circ g = id_{F[x,y]}$ y f es invertible, y f es isomorfismo.

Existencia del Producto Tensorial.

Consideremos el R-módulo libre

$$R^{(M \times N)} = \left\{ \sum_{(x,y) \in M \times N} \alpha_{(x,y)}(x,y) \;\middle|\; \alpha_{(x,y)} \in R,\ (\alpha_{(x,y)})_{(x,y) \in M \times N} \text{ de soporte finito} \right\}$$

de base $M \times N$.

Sea S es el submódulo de $R^{(M\times N)}$ generado por elementos del tipo

$$(x + x', y) - (x, y) - (x', y)$$

$$(x, y + y') - (x, y) - (x, y')$$

$$\alpha(x, y) - (\alpha x, y)$$

$$\alpha(x, y) - (x, \alpha y)$$

$$\forall \quad x, x' \in M, \;\; y, y' \in N, \;\; \alpha \in R$$

Definamos

$$M \otimes_R N = R^{(M\times N)} \,/\, S$$

y consideremos las aplicaciones

$i : M \times N \to R^{(M\times N)}$, $(x, y) \to (x, y)$ y $\pi : R^{(M\times N)} \to R^{(M\times N)} \,/\, S$ epimorfismo canónico

Probaremos que $(R^{(M\times N)} \,/\, S, \;\; \pi \circ i)$ es un producto tensorial para M y N.

Tenemos el diagrama

$$\begin{array}{rcl} M \times N & \overset{\forall\, \psi \; bil}{\longrightarrow} & P \\ i \downarrow & & \\ R^{(M\times N)} & & \\ \pi \downarrow & & \\ R^{(M\times N)}/S & & \end{array}$$

Definamos

$$\varphi : M \times N \to M \otimes_R N, \;\; \text{tal que} \;\; \varphi = \pi \circ i,$$

Luego,

$$\varphi : M \times N \to M \otimes_R N, \;\; (x, y) \to (x, y) + S$$

Probemos que

$$\varphi : M \times N \to M \otimes_R N, \;\; (x, y) \to (x, y) + S$$

es bilineal. Sean $x, x' \in M, y \in N, \alpha \in R$. Entonces $(x+x', y) - (x, y) - (x', y) \in S \iff (x+x', y) + S = (x, y) + (x', y) + S \iff (x+x', y) + S = (x, y) + S + (x', y) + S \iff \varphi(x + x', y) = \varphi(x, y) + \varphi(x', y)$. Además $\alpha(x, y) - (\alpha x, y) \in S \iff \alpha(x, y) + S = (\alpha x, y) + S \iff \alpha((x, y) + S) = (\alpha x, y) + S \iff \alpha\varphi(x, y) = \varphi(\alpha x, y)$. Por lo tanto, φ es lineal en la primera variable. En forma similar se ve que φ es lineal en la segunda variable. Luego φ es bilineal.

Denotemos para cada $x \in M$, y cada $\in N$, $(x, y) + S = x \otimes y$ y se tiene que $M \otimes_R N$ está generado como R- módulo por $\{(x, y) + S = x \otimes y \mid x \in M, y \in N\}$.

Veamos que se cumple la Propiedad Universal. Sean P un R- módulo, $\psi : M \times N \to P$ una aplicación bilineal. Por ser $R^{(M\times N)}$ un módulo libre existe $h : R^{(M\times N)} \to P$ lineal tal que $h \circ i = \psi$, es decir, para cada $x \in M, y \in N$, $h \circ i(x, y) = \psi(x, y)$ o bien para cada $x \in M, y \in N, h(x, y) = \psi(x, y)$.

$$\begin{array}{rcl} M \times N & \xrightarrow{\psi} & P \\ i\downarrow & \nearrow & h \\ R^{(M\times N)} & & \\ \pi\downarrow & & \\ R^{(M\times N)}/S & & \end{array}$$

Para demostrar que existe $f : R^{(M\times N)} \,/\, S \to P$, lineal tal que $f \circ \pi = h$ se necesita probar que $Ker(\pi) \subseteq Ker(h)$, es decir, que $S \subseteq Ker(h)$ y aplicar proposición 4.1 que también es válida para módulos y aplicaciones lineales. Basta trabajar con los generadores de S. Tomemos por ejemplo $(x, y+y') - (x, y) - (x, y')$. Entonces como h es lineal, $h((x, y+y') - (x, y) - (x, y')) = h(x, y+y') - h(x, y) - h(x, y') = (h\circ i)(x, y+y') - (h\circ i)(x, y) - (h\circ i)(x, y') = \psi(x, y+y') - \psi(x, y) - \psi(x, y') = 0$, pues ψ es bilineal. Similarmente se procede con los otros generadores.

Finalmente veamos que $f \circ \varphi = \psi$. Para ello usaremos que $f \circ \pi = h$ y que $h \circ i = \psi$. En efecto, $f \circ \varphi = f \circ (\pi \circ i) = (f \circ \pi) \circ i = h \circ i = \psi$.

Producto Tensorial de Álgebras.

Proposición 4.4. *Sean A, B dos R- álgebras, $A \otimes_R B$ el producto tensorial de los R-módulos A y B entonces existe una única aplicación bilineal $\phi : A \otimes_R B \times A \otimes_R B \to A \otimes_R B$ definida por $\phi(x \otimes y, m \otimes n) = xm \otimes yn$; $\forall\ x, m \in A,\ \forall\ y, n \in B$. En particular se tiene que*

$$(x \otimes y)(m \otimes n) = xm \otimes yn,\ \forall\ x, m \in A,\ \forall\ y, n \in B.$$

Demostración. Para cada $m \in A,\ n \in B$ se define:

$$\psi_{m,n} : A \times B \to A \otimes_R B \text{ por } \psi_{m,n}(x, y) = xm \otimes yn\ \forall\ x \in A,\ \forall\ y \in B.$$

Entonces $\psi_{m,n}$ es bilineal. Luego existe un única aplicación lineal

$$f_{m,n} : A \otimes_R B \to A \otimes_R B \text{ tal que } f_{m,n}(x \otimes y) = \psi_{m,n}(x, y) = xm \otimes yn\ \forall\ (x, y) \in A \times B.$$

Es decir el diagrama siguiente conmuta

$$\begin{array}{rcl} A \times B & \stackrel{\psi_{m,n}}{\longrightarrow} & A \otimes_R B \\ \varphi \downarrow & \nearrow & \exists! f_{m,n} \\ A \otimes_R B & & \end{array}$$

Además se tiene:

$$f_{m+m',n} = f_{m,n} + f_{m',n}\ \forall\ m, m' \in A,\ \forall\ n \in B$$

$$f_{m,n+n'} = f_{m,n} + f_{m,n'}\ \forall\ m \in A,\ \forall\ n, n' \in B$$

$$f_{\alpha m,n} = \alpha f_{m,n} = f_{m,\alpha n}\ \forall\ m \in A,\ \forall\ n \in B,\ \forall\ \alpha \in R$$

Definamos ahora

$$\phi : A \times B \to Hom_R(A \otimes_R B, A \otimes_R B),\ \text{ por } \phi(m, n) = f_{m,n}\ \forall\ m \in A,\ \forall\ n \in B.$$

Entonces ϕ es bilineal y tenemos el diagrama

$$\begin{array}{rcl} A \times B & \stackrel{\phi}{\longrightarrow} & Hom_R(A \otimes_R B, A \otimes_R B) \\ \varphi \downarrow & \nearrow g & \\ A \otimes_R B & & \end{array}$$

Luego existe una única función lineal

$g : A \otimes_R B \to Hom_R(A \otimes_R B, A \otimes_R B)$ tal que $g(m,n) = \phi(m,n) \ \forall \ m \in A, \ \forall \ n, n' \in B$

Por lo tanto,

$$g(m \otimes n)(x \otimes y) = f_{m,n}(x \otimes y) = xm \otimes yn.$$

La aplicación

$\phi : A \otimes_R B \times A \otimes_R B \to A \otimes_R B$, definida por $\phi(z, z') = zz' = g(z')(z) \ \forall \ z, z' \in A \otimes_R B$

es bilinear y satisface

$$\phi(x \otimes y, m \otimes n) = g(m \otimes n)(x \otimes y) = f_{m,n}(x \otimes y) = xm \otimes yn.$$

Finalmente, ϕ es la única aplicación lineal que satisface la condición pedida.

□

Observación 4.7. *$A \otimes_R B$ provisto de $(x \otimes y)(m \otimes n) = xm \otimes yn \ \forall \ x, m \in A, \ y, n \in B$ es un álgebra. Además se tiene: (i) A y B asociativas $\Longrightarrow$ $A \otimes_R B$ asociativa, (ii) A y B conmutativas $\Longrightarrow$ $A \otimes_R B$ conmutativa, (iii) $1_{A \otimes_R B} = 1_A \otimes 1_B$.*

Ejercicio 4.4. *Sean F cuerpo, A una F-álgebra, con unidad. Pruebe que*

$M_n(F) \otimes_F A \simeq M_n(A)$ (isomorfismo de álgebras).

Proposición 4.5. *Sean F cuerpo, A y B F-álgebras, con unidad. $\{b_i\}_{i \in I}$ elementos de B linealmente independientes sobre F. Pruebe que*

$$\sum_{j \in J} a_j \otimes b_j = 0 \Rightarrow a_j = 0 \quad \forall \ j \in J.$$

Demostración. Supongamos que $a_t \neq 0$, para algún t. Sea $g : A \to F$ lineal tal que $g(a_t) \neq 0$, por ejemplo, tomar $g = a_t'$. Sea $f : B \to F$, lineal tal que $f(b_t) \neq 0$, y $f(b_i) = 0$, para todo $i \neq t$ por ejemplo, $f = b_t'$. Sea $\psi : A \times B \to F$, definida por $\psi(a, b) = g(a)f(b), \ \forall \ a \in A, b \in B$. Entonces ψ es bilineal. Por propiedad de producto tensorial existe una única $h : A \otimes_F B \to F$, lineal tal que $h(a \otimes b) = g(a)f(b), \ \forall \ a \in A, b \in B$.

Por lo tanto, $0 = h(0) = h(\sum_{j \in J} a_j \otimes b_j) = h(a_1 \otimes b_1) + \cdots + h(a_t \otimes b_t) + \cdots = g(a_1)f(b_1) + \cdots + g(a_t)f(b_t) + \cdots = g(a_t)f(b_t) \neq 0$. Contradicción. Luego, $a_j = 0 \quad \forall \ j \in J$. □

Así como formamos $M \otimes_R N$, podemos formar $M_1 \otimes_R M_2 \otimes_R \ldots \otimes_R M_n$, un producto tensorial de n, R-módulos.

Recordemos que $\psi : M_1 \times M_2 \times \ldots \times M_n \longrightarrow P$ con P un R-módulo cualquiera, es multilineal o n-lineal si

$$\begin{aligned}&\forall\ m_i, m_i' \in M_i,\ \ \forall\ \alpha \in R,\ \ \psi(m_1, \ldots, m_{i-1}, \alpha m_i + m_i', \ldots, m_n)\\ &= \alpha\psi(m_1, \ldots, m_i, \ldots, m_n) + \psi(m_1, \ldots, m_i', \ldots, m_n)\end{aligned}$$

Así $\psi : M_1 \times M_2 \times M_3 \longrightarrow P$ es trilineal

$$\begin{aligned}\iff \psi(\alpha m_1 + m_1', m_2, m_3) &= \alpha\psi(m_1, m_2, m_3) + \psi(m_1', m_2, m_3),\\ \psi(m_1, \alpha m_2 + m_2', m_3) &= \alpha\psi(m_1, m_2, m_3) + \psi(m_1, m_2', m_3),\\ \psi(m_1, m_2, \alpha m_3, m_3') &= \alpha\psi(m_1, m_2, m_3) + \psi(m_1, m_2, m_3').\end{aligned}$$

Observación 4.8. *Propiedad Universal. Para todo P, R-módulo, $\forall\,\psi$ multilineal, $\exists! f$ R-lineal tal que $f \circ \varphi = \psi$. Es decir,*

$$f(m_1 \otimes m_2 \otimes \ldots \otimes m_n) = \psi(m_1, \ldots, m_n)$$

y tenemos el diagrama

$$\begin{array}{ccc} M_1 \times \ldots \times M_n & \overset{\forall\,\psi}{\longrightarrow} & P \\ \varphi\downarrow & \nearrow & \exists! f \\ M_1 \otimes_R M_2 \otimes_R \ldots \otimes_R M_n & & \end{array}$$

4.4. Álgebra Tensorial $T(M)$ de un R-módulo M.

Para cada k, definamos: $T^k(M) = M \otimes_R M \otimes_R \ldots \otimes_R M$ k factores *con* $k \geq 1$ y pongamos $T^0(M) = R$. Los elementos de $T^k(M)$ se llaman k-tensores.

Definamos

$$T(M) = \oplus_{k=0}^{\infty} T^k(M) = R \oplus M \oplus (M \otimes_R M) \oplus \ldots$$

es una suma directa de R-módulos. Cada elemento de $T(M)$ es una combinación lineal de k-tensores para diferentes $k \geq 0$. Además M se identifica con $T^1(M)$ luego M es un R-submódulo de $T(M)$.

Nota:

1. $z \in T^k(M) \Longrightarrow z = \sum_{\text{finita}} m_{1i} \otimes \ldots \otimes m_{ki}$

2. Sea $R\{x_i \mid i \in \mathbb{N}\}$ polinomios no conmutativos en las variables $x_1, x_2, x_3, \ldots$ entonces

$$T(M) \simeq \ R\{x_i \mid i \in \mathbb{N}\}, \ \text{via} \ m_{1i} \otimes m_{2i} \otimes \ldots \otimes m_{ki} \longrightarrow x_{1i}x_{2i}\ldots x_{ki}.$$

Ejemplo concreto: Sea M libre de base $\{e_1, e_2\}$ (M tiene rango 2). Base de $T(M)$: $1, e_1, e_2, e_1 \otimes e_2, e_2 \otimes e_1, e_1 \otimes e_1, e_2 \otimes e_2, e_1 \otimes e_1 \otimes e_1, e_1 \otimes e_2 \otimes e_1, e_2 \otimes e_1 \otimes e_1, e_1 \otimes e_1 \otimes e_2, e_2 \otimes e_2 \otimes e_1, e_2 \otimes e_1 \otimes e_2, e_1 \otimes e_2 \otimes e_2, e_2 \otimes e_2 \otimes e_2, \ldots$

La base de $R\{x_i \mid i \in \mathbb{N}\}$ está formada por monomios:

$1, x_1, x_2, x_1x_2, x_2x_1, x_1^2, x_2^2, x_1^3, x_1x_2x_1, x_2x_1^2, x_1^2x_2, x_2^2x_1, x_2x_1x_2, x_1x_2^2, x_2^3, \ldots$

Teorema 4.4. *Sea M un R-módulo entonces*

1. *$T(M)$ es una R-álgebra, que contiene a M con la multiplicación definida por:*

$$\begin{array}{ccccc} (m_1 \otimes \ldots \otimes m_i) & (m'_1 \otimes \ldots \otimes m'_j) & = m_1 \otimes \ldots \otimes m_i \otimes m'_1 \otimes \ldots \otimes m'_j \\ \downarrow & \downarrow & \downarrow \\ \textit{i-factores} & \textit{j-factores} & \textit{i+j-factores} \end{array}$$

   Que se extiende a una suma, usando distributividad. Se tiene que $T^i(M)T^j(M) \subseteq T^{i+j}(M)$.

2. *Propiedad Universal de $T(M)$. Sea A una R-álgebra y $h : M \longrightarrow A$ un homomorfismo de R-módulos. Entonces $\exists! \phi : T(M) \longrightarrow A$ homomorfismo de álgebras, tal que $\phi|_M = h$.*

Demostración. 1. Definamos

$$\xi : \underbrace{M \times \ldots \times M}_{\text{i}-factores} \times \underbrace{M \times \ldots \times M}_{\text{j}-factores} \longrightarrow T^{i+j}(M)$$

por

$$\xi((m_1, \ldots, m_i), (m'_1, \ldots, m'_j)) = m_1 \otimes \ldots \otimes m_i \otimes m'_1 \otimes \ldots \otimes m'_j$$

Como ξ multilineal, $\exists! g$ lineal tal que $g \circ \varphi = \xi$. Es decir, el siguiente diagrama conmuta.

$$\begin{array}{rcl} M \times M \times \ldots \times M \times M \times M \times \ldots \times M & \overset{\xi \text{ multi}}{\longrightarrow} & T^{i+j} \\ \varphi \downarrow & \nearrow & \exists! g \\ (M \otimes_R \ldots \otimes_R M) \otimes_R (M \otimes_R \ldots \otimes_R M) & & \\ = T^i(M) \otimes_R T^j(M) & & \end{array}$$

De aquí se define el producto en $T^i(M)T^j(M)$ como

$$= (m_1 \otimes \ldots \otimes m_i)(m'_1 \otimes \ldots \otimes m'_j) = m_1 \otimes m_2 \otimes \ldots \otimes m_i \otimes m'_1 \otimes \ldots \otimes m'_j$$

2. Consideremos $h : M \longrightarrow A$ un homomorfismo de R-módulos. Entonces para cada j,

$$\psi_j : M \times M \times M \times \ldots \times M(j \text{ veces }) \longrightarrow A$$

definido por $(m_1, m_2 \cdots, m_j) \longrightarrow h(m_1)h(m_2)\cdots h(m_j)$ es una aplicación R-multilineal de $M \times M \times M \times \ldots \times M(j$ veces) en A. Este induce para cada j, un homomorfismo g_j de R-módulos de $T^j(M)$ en A que lleva $m_1 \otimes \cdots \otimes m_j$ en $h(m_1)h(m_2)\cdots h(m_j)$ por observación 4.8.

$$\begin{array}{rcl} M \times \ldots \times & \overset{\forall \psi_j}{\longrightarrow} & A \\ \downarrow & \nearrow & \exists! g_j \\ T^j(M) & & \end{array}$$

Por la definición del producto en la parte 1. de este teorema se tiene que $\phi : T(M) \longrightarrow A$, $\phi_{T^j} = g_j$ es un homorfismo de álgebras.

□

Observación 4.9. *Sea V un espacio vectorial de dimensión finita sobre un cuerpo F con base $B = \{v_1, \cdots, v_n\}$. Entonces los k-tensores $v_{i1} \otimes v_{i2} \otimes \cdots \otimes v_{ik}$ con $v_{ij} \in B$ son base de $T^k(V)$ como espacio vectorial sobre F. En particular, $dim_F(T^k(V)) = n^k$.*

Definición 4.10. *Un anillo S es un anillo graduado si es suma directa de subgrupos aditivos, $S = S_0 \oplus S_1 \oplus \cdots$ tal que $S_i S_j \subseteq S_{i+j}$. Los elementos de S_k se dicen homogéneos de grado k y S_k se llama la componente homogénea de S de grado k.*

Un ideal I de un anillo graduado S se dice ideal graduado si $I = \oplus_{k\geq 0}(I \cap S_k)$.
Un homomorfismo de anillos $\varphi : S \longrightarrow T$ de anillos graduados se dice homomorfismo de anillos graduados si respeta las graduaciones de S y de T, es decir, $\varphi(S_k) \subseteq T_k$, $\forall\ k \geq 0$,

Observación 4.10. *Note que $S_0S_0 \subseteq S_0$, luego S_0 es un subanillo del anillo graduado S y S es un S_0-módulo. Además si S_0 está en el centro de S y contiene a 1_S entonces S es una S_0-álgebra. Notemos también que el ideal I es graduado si cualquier suma $i_{k_1} + \cdots + i_{k_n}$ de elementos homogéneos de distintos grados $k_1, \cdots, k_n$ está en I entonces cada sumando individual $i_{k_1}, \cdots, i_{k_n}$ está el mismo en I.*

Ejemplo 4.16. *El álgebra tensorial $T(M)$ de un R-módulo M es un anillo graduado.*

Proposición 4.6. *Sea S anillo graduado, sea I ideal graduado de S y sea $I_k = I \cap S_k$, $\forall\ k \geq 0$. Entonces S/I es un anillo graduado cuya componente de grado k es isomorfa a S_k/I_k.*

Demostración. Consideremos la aplicación $g : S = \oplus_{k\geq 0}S_k \longrightarrow \oplus_{k\geq 0}(S_k/I_k)$, definida por $(s_0, \cdots, s_k, \cdots) \longrightarrow (s_0 + I_0, \cdots, s_k + I_k, \cdots)$ la cual es epiyectiva y su núcleo es $I = \oplus_{k\geq 0}I_k$ y es un homorfismo de anillos graduados. □

4.5. Álgebra Simétrica $S(M)$ de un R-módulo M .

Será un cuociente del álgebra tensorial $T(M)$. Sea $C(M)$ el ideal de $T(M)$ generado por todos los elementos de la forma $m_1 \otimes m_2 - m_2 \otimes m_1$, $m_1, m_2 \in M$. El álgebra cuociente $S(M) = T(M)/C(M)$ se llama álgebra simétrica del módulo M.

Observación 4.11. *Algunas propiedades del álgebra $S(M)$:*

a) $S(M)$ es conmutativa.

b) $C(M)$ está generado por tensores homogéneos de grado 2 y es un ideal graduado.

Por proposición 4.6 el álgebra simétrica es un anillo graduado cuya componente homogénea de grado k es $S^k(M) = T^k(M)/C^k(M)$, donde $C^k(M) = C(M) \cap T^k(M)$, luego los elementos de $C^k(M)$ son sumas finitas de elementos de la forma

$m_1 \otimes \cdots m_{i-1} \otimes (m_i \otimes m_{i+1} - m_{i+1} \otimes m_i) \otimes m_{i+2} \otimes \cdots \otimes m_k$ con $m_i \in M$, $k \geq 2$, $1 \leq i < k$.

Además $S^1(M) = M, S^0(M) = R$ y $C(M) \cap M = \{0\},\ S(M) = R \oplus M \oplus S^2(M) \oplus \cdots$

Definición 4.11. *Sean M y N dos R-módulos. Una función multilineal $\varphi : M \times \cdots \times M$ (k factores) $\longrightarrow N$ se dice simétrica si $\varphi(m_1, \cdots, m_k) = \varphi(m_{\sigma(1)}, \cdots, m_{\sigma(k)})$ para todas las permutaciones σ de $1, \cdots, k$.*

Teorema 4.5. *Sea M un R-módulo entonces*

1. *La k-ésima potencia simétrica de M, $S^k(M)$ es igual a $m_1 \otimes \cdots \otimes m_k$ (k factores) módulo el submódulo generado por todos los elementos de la forma $(m_1 \otimes \cdots \otimes m_k) - (m_{\sigma(1)}, \cdots, m_{\sigma(k)})$ para toda las permutaciones σ del grupo simétrico S_k.*

2. *Propiedad Universal para funciones multilineales simétricas.*

   Para cada k, si $\psi_k : M \times \cdots \times M$ (k factores) $\longrightarrow N$ es k multilineal simétrica, entonces existe un único homomorfismo de R-módulos $\phi_k : S^k(M) \longrightarrow N$ tal que $\psi_k = \phi_k \circ i_k$, donde $i_k : M \times \cdots \times M$ (k factores) $\longrightarrow S^k(M)$ es la aplicación definida por $i_k(m_1, \cdots, m_k) = m_1 \otimes \cdots m_k + C^k(M)$.

3. *Propiedad Universal para funciones hacia álgebras conmutativas.*

   Sea A una R-álgebra conmutativa y $h : M \longrightarrow A$ un homomorfismo de R-módulos. Entonces $\exists! \phi : S(M) \longrightarrow A$ homomorfismo de álgebras, tal que $\phi|_M = h$.

Demostración. Tenemos que los elementos de $C^k(M)$ en el ideal $C(M)$ son sumas finitas de elementos de la forma $m_1 \otimes \cdots m_{i-1} \otimes (m_i \otimes m_{i+1} - m_{i+1} \otimes m_i) m_{i+2} \otimes \cdots \otimes m_k$ con $m_i \in M,\ k \geq 2,\ 1 \leq i < k$. Estos elementos corresponden a los mencionados en 1. para la transposición $(ii+1)$ en el grupo simétrico S_k. Como cada σ es producto de transposiciones se puede ver que cada elemento en 1. puede escribirse como suma de elementos de la forma anterior.

2.- Para cada k, sea $\psi_k : M \times \cdots \times M$ (k factores) $\longrightarrow N$ k multilineal simétrica. Como

$(T^k(M), \varphi_k)$ es producto tensorial $\exists! f_k : T^k(M) \longrightarrow N$ lineal tal que $f_k \circ \varphi_k = \psi_k$. (*)

$$\begin{array}{rcl} M \times \cdots \times M (k \text{ factores }) & \overset{\psi_k mul\ sim}{\longrightarrow} & N \\ \varphi_k \downarrow & \nearrow & \exists! f_k \ lineal \\ T^k(M) & & \\ \pi_k \downarrow & & \\ S^k(M) = T^k(M)/C^k(M) & & \end{array}$$

Por Proposición 4.1, existe única $\phi_k : S^k(M) \longrightarrow N$ tal que $\phi_k \circ \pi_k = f_k \iff C^k(M) = Ker(\pi_k) \subseteq Ker(f_k)$.

Basta tomar generadores de $C^k(M)$, es decir, elementos de la forma $x = m_1 \otimes \cdots m_{i-1} \otimes (m_i \otimes m_{i+1} - m_{i+1} \otimes m_i) m_{i+2} \otimes \cdots \otimes m_k$.

Como ψ_k es multilineal simétrica por (*) se tiene que $f_k(x) = 0$. Finalmente si $i_k = \pi_k \circ \varphi_k$ entonces $\phi_k \circ i_k = \phi_k \circ (\pi_k \circ \varphi_k) = (\phi_k \circ \pi_k) \circ \varphi_k = f_k \circ \varphi_k = \psi_k$ por (*), es decir $\psi_k = \phi_k \circ i_k$.

La demostración de 3. es muy similar a la parte 2. del teorema del álgebra $T(M)$. □

4.6. Álgebra Exterior $\Lambda(M)$ de un R-módulo M .

Queremos definir un producto $\wedge$ con las propiedades multilineales de $\otimes$ y $m_1 \wedge \ldots \wedge m_k$ sea cero si $m_i = m_j$ algún $i, j, i \neq j$. Será definida como un cuociente del álgebra tensorial $T(M)$.

Sea $A(M)$ el ideal de $T(M)$ generado por todos los elementos de la forma $m \otimes m$, $m \in M$. El álgebra cuociente $\Lambda M = T(M)/A(M)$ se llama álgebra exterior del módulo M. Como en el caso del álgebra simétrica, el ideal $A(M)$ es generado por elementos homogéneos luego es ideal graduado.

$$\pi : T(M) \longrightarrow \Lambda(M)$$

$$\begin{aligned} \pi(m_1 \otimes \ldots \otimes m_k) &= m_1 \wedge m_2 \wedge \ldots \wedge m_k = \overline{m_1 \otimes \ldots \otimes m_k} \\ &= m_1 \otimes \ldots \otimes m_k + A(M) \end{aligned}$$

Por proposición 4.6 el álgebra exterior es graduada, con la k-ésima componente $\Lambda^k(M) = T^k(M)/A^k(M)$. $\Lambda^k(M)$ se llama la k potencia exterior de M. Se identifica R con $\Lambda^0(M)$

y M con $\Lambda^1(M)$ y se considera M como R-submódulo de $\Lambda(M)$. Se tiene que $\Lambda(M) = R \oplus M \oplus \Lambda^2(M) \oplus \cdots$

Los elementos de $A^k(M)$ son sumas finitas de elementos de la forma:

$$m_1 \otimes \ldots \otimes m_{i-1} \otimes m \otimes m \otimes m_{i+2} \otimes \ldots \otimes m_k$$

donde $k \geq 2$, $1 \leq i < k$. Son k-tensores con igual componente i-ésima y (i+1)-ésima.

Definición 4.12. *Sean M y N dos R-módulos. Una función multilineal $\varphi : M \times \cdots \times M$ (k factores) $\longrightarrow N$ se dice alternada si $\varphi(m_1, \cdots, m_k) = 0$ cuando $m_i = m_{i+1}$ para algún i.*

La multiplicación

$$(m_1 \wedge m_2 \wedge \ldots \wedge m_i)(m'_1 \wedge m_2 \wedge \ldots \wedge m'_j) = m_1 \wedge m_2 \wedge \ldots \wedge m_i \wedge m'_1 \wedge m_2 \wedge \ldots \wedge m'_j$$

en el algebra exterior se llama producto cuña o exterior. Por definición de cuociente, esta multiplicación es alternada, pues

$$m_1 \wedge m_2 \wedge \ldots \wedge m_{i-1} \wedge m \wedge m \wedge m_{i+2} \wedge \ldots \wedge m_k = 0$$

Teorema 4.6. *a) La k-ésima potencia exterior de M, $\Lambda^k(M)$ es igual a $T^k(M)$ módulo, el submódulo generado por elementos de la forma $m_1 \otimes m_2 \otimes \ldots \otimes m_k$, con $m_i = m_j$ algún $i \neq j$.*

En particular, $m_1 \wedge \ldots \wedge m_k = 0$, si $m_i = m_j$, algún $i \neq j$.

b) Propiedad Universal para funciones multilineales alternadas.

Para cada k si $\psi_k : M \times \ldots \times M$ (k factores) $\longrightarrow N$ es multilineal alternada, entonces $\exists! \phi_k : \Lambda^k(M) \longrightarrow N$ homomorfismo de R-módulos tal que $\phi_k \circ i_k = \psi_k$ con $i : M \times \ldots \times M \longrightarrow \Lambda^k(M)$, definida por:

$$i_k(m_1, \ldots, m_k) = m_1 \wedge \ldots \wedge m_k$$

Demostración. Sabemos que los elementos de $A^k(M)$ son de la forma

$$m_1 \otimes \ldots \otimes m_{i-1} \otimes m \otimes m \otimes m_{i+2} \otimes \ldots \otimes m_k \qquad (*)$$

Luego tienen también la forma $m_1 \otimes \ldots \otimes m_k$ con $m_i = m_j \ i \neq j$, lo cual es inmediato con $j = i + 1$.

Recíprocamente, dado:

$$m_1 \otimes \ldots \otimes m_i \otimes \ldots \otimes m_i \otimes \ldots \otimes m_k \in A^k(M)$$

Queremos ver que posible llevar el m_i del lugar j al lugar $i + 1$

$$A^k(M) \subseteq A(M)$$

$$(m + m') \otimes (m' + m) = m \otimes m' + m \otimes m + m' \otimes m' + m' \otimes m$$

$$m' \otimes m = -m \otimes m' + [\underbrace{(m + m') \otimes (m' + m) - m \otimes m - m' \otimes m'}_{\in A(M)}]$$

$$m' \otimes m \equiv -m \otimes m' \ (mod\, A(M)) \in A(M)$$

Por lo tanto,

$$m_1 \otimes \ldots \otimes m_i \otimes \ldots \otimes m_i \otimes \ldots \otimes m_k \equiv \pm m_1 \otimes \ldots \otimes m_i \otimes \ldots \otimes m_k \ \ mod\,(A(M))$$

b) Muy similar a la demostraciones del teorema 4.4 y la observación 4.8, observando que $A^k(M)$ está contenido en el núcleo de cualquier función alternada de $T^k(M)$ a N, para usar la proposición 4.1. □

Ejemplo 4.17. *Sea V espacio vectorial sobre F, $V = \langle v \rangle$, $dim_F(V) = 1$ ¿Qué es ΛV?*

Solución: Se tiene que

$$\Lambda V = F \oplus V \oplus \Lambda^2 V \oplus \Lambda^3 V \oplus \ldots$$

Sea $x \in \Lambda^2(V)$ Luego $x = \alpha v \wedge v = 0$. Por lo tanto, $\Lambda^k(V) = 0 \ \forall\, k \geq 2$ y $\Lambda V = F \oplus V$

Ejemplo 4.18. *Sea $V = \langle v, v' \rangle \, dim_F(V) = 2$. ¿Qué es ΛV?*

Solución: Se tiene que

$$\Lambda V = F \oplus V \oplus \Lambda^2(V) \oplus \Lambda^3(V) \oplus \dots$$

Sea $z \in \Lambda^2(V)$. Sean $\alpha_1, \alpha_2, \beta_1, \beta_2 \in F$.

$$\begin{aligned} z &= (\alpha_1 v + \alpha v') \wedge (\beta_1 v + \beta_2 v') \\ &= \alpha_1\beta_1 v \wedge v + \alpha_1\beta_2 v \wedge v' + \alpha_2\beta_1 v' \wedge v + \alpha_2\beta_2 v' \wedge v' \\ &= \alpha_1\beta_2 v \wedge v' + \alpha_2\beta_1 v' \wedge v \\ &= \alpha_1\beta_2 v \wedge v' - \alpha_2\beta_1 v \wedge v' \\ &= (\alpha_1\beta_2 - \alpha_2\beta_1) v \wedge v' \end{aligned}$$

Por lo tanto, $\Lambda^2(V) = F\, v \wedge v'$. Si $A = \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix}$ Entonces $\alpha_1\beta_2 - \alpha_2\beta_1 = det(A)$ y $z = det(A) v \wedge v'$

$\Lambda^3(V) = 0 = \Lambda^k(V)\ \forall\, k \geq 3$, pues hay 2 vectores v y $v' \neq s$; en $\Lambda^3 V$ siempre van a existir 2 vectores iguales en $v_1 \wedge v_2 \wedge v_3$ con $v_i = v$ o $v_i = v'$.

Por lo tanto, $\Lambda V = F \oplus V \oplus F\ v \wedge v'$.

Observación 4.12. *Se puede generalizar a*

$$dim V = n \ \wedge\ z = det(A) v_1\ y\ \dots \wedge v_n$$

donde $\{v_1, \dots, v_n\}$ *es base de* V, $z \in \Lambda^n(V)$.

Referencias

[1] Abuabuad, C. Módulos, Apuntes Departamento de Matemáticas, Facultad de Ciencias, 1980.

[2] Arenas, L. Anillos y cuerpos, Apuntes Departamento de Matemáticas, Facultad de Ciencias, 2011.

[3] Behn, A. Apuntes de Cuerpos y Algebras, 2018.

[4] Dummit, D. S., Foote, R. M. Abstract Algebra, John Wiley and Sons, Inc. Third Ed. 2004.

[5] Hernstein, I. N. Topics in Algebra, Blaidell Publishing Company, 1964.

[6] Labra, A., Suazo, A., Elementos de la Teoría de Cuerpos, Comunicaciones Noreste Ltda. J. C. Saéz Editor. Primera Edición Febrero 2012. ISBN 978-956-306-069-0

5. Guías

Guía 1, Cuerpos y álgebras

1. Pruebe que $\mathbb{Q}[i] = \{a + bi \ / \ a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{C}$ llamado cuerpo de cuocientes de los enteros de Gauss, con las operaciones:

   $(a + bi) + (c + di) = (a + c) + (b + d)i$ y

   $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

2. Pruebe que todo dominio de integridad (anillo conmutativo en el cual $ab = 0 \Rightarrow a = 0 \vee b = 0$) finito es un cuerpo.

3. Sean F_1, F_2 subcuerpos de un cuerpo F. Se llama Composito de F_1 y F_2 y se anota F_1F_2 al menor subcuerpo de F que contiene a F_1 y F_2. Pruebe que el composito de $\mathbb{Q}(\sqrt{2})$ y de $\mathbb{Q}(\sqrt[3]{2})$ es el cuerpo $\mathbb{Q}(\sqrt[6]{2})$.

4. Sea F subcuerpo de un cuerpo K y sea $Y \subseteq K$ entonces el subanillo de K generado por F e Y es la intersección de todos los subanillos de K que contienen a F y a Y. Se representa por $F[Y]$ y sus elementos son sumas finitas de elementos de la forma $f_{i_1 i_2 \cdots i_r} y_{i_1} \cdots y_{i_r}$, con $f_{i_1 i_2 \cdots i_r} \in F$ y $y_{i_1}, \cdots, y_{i_r} \in Y$. El subcuerpo generado por F e Y es el cuerpo de fracciones de $F[Y]$ y se anota por $F(Y)$. Si $Y = \{u_1, \cdots, u_r\}$ entonces $F[Y]$ se escribe $F[u_1, \cdots, u_r]$ y $F(Y)$ se escribe $F(u_1, \cdots, u_r)$. Sea $Y, Z \subseteq K$. Pruebe que

   i) $F[Y \cup Z] = F[Y][Z] = F[Z][Y]$.

   ii) $F(Y \cup Z) = F(Y)(Z) = F(Z)(Y)$.

5. Muestre que el polinomio P es irreducible en $\mathbb{F}_7[x]$, donde $P(x) = x^3 + x^2 + x + 2$. Pruebe que el cuerpo $K = \mathbb{F}_7[x]/ < P >$ tiene 7^3 elementos y encuentre el inverso multiplicativo del elemento $2 + 3x + 5x^2 + < P > \in K$.

6. Considere el cuerpo $\mathbb{F}_2$ y el polinomio $P \in \mathbb{F}_2[x]$ dado por $P(x) = x^2 + x + 1$. Pruebe que P es irreducible y encuentre la fórmula de la multiplicación en $K = \mathbb{F}_2[x]/\langle P \rangle$. Encuentre en particular el inverso multiplicativo de $\bar{x} \in K$.

7. Muestre que el polinomio P es irreducible en $\mathbb{Q}[x]$, donde $P(x) = x^3 + 9x + 6$. Sea θ una raíz de P. Encuentre el inverso de $1 + \theta$ en $\mathbb{Q}(\theta)$.

8. Muestre que el polinomio P es irreducible en $\mathbb{Q}[x]$ donde $P(x) = x^3 - 2x - 2$. Sea θ una raíz de P. Calcule $(1 + \theta)(1 + \theta + \theta^2)$ y $\frac{1+\theta}{1+\theta+\theta^2}$ elementos de $\mathbb{Q}(\theta)$.

9. Muestre que el polinomio P es irreducible en $\mathbb{F}_2[x]$, donde $P(x) = x^3 + x + 1$. Sea θ una raíz de $p(x)$. Calcule las potencias de θ en $\mathbb{F}_2(\theta)$.

10. Pruebe que $\mathbb{Q}(2^{\frac{1}{3}}) = \{a + b2^{\frac{1}{3}} + c4^{\frac{1}{3}} \ / \ a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$ y que $[\mathbb{Q}(2^{\frac{1}{3}}) : \mathbb{Q}] = 3$.

11. Pruebe directamente que la aplicación $a + b\sqrt{2} \to a - b\sqrt{2}$ es un isomorfismo de $\mathbb{Q}(\sqrt{2})$ en sí mismo.

12. Sea $\varphi : F \to F'$ isomorfismo de cuerpos. Entonces φ un isomorfismo natural de $F[x]$ en $F'[x]$. Sea P polinomio irreducible en $F[x]$ y sea $P' \in F'[x]$ el polinomio obtenido de P al aplicar el homomorfismo φ a los coeficientes de P. Pruebe que P' es irreducible en $F'[x]$.

Guía 2, Cuerpos y álgebras

1. Sea $F = \mathbb{F}_2$ cuerpo finito de dos elementos. Sea $P(x) = x^2 + x + 1 \in F[x]$. Pruebe que P es irreducible en $\mathbb{F}_2[x]$. Sea θ una raíz de P. Luego $[\mathbb{F}_2(\theta) : \mathbb{F}_2] = 2$. Encuentre la tabla de multiplicación de $\mathbb{F}_2(\theta)$

2. Sea K una extensión de un cuerpo F, $\alpha \in K$ y $b \in F$.

   a) Demostrar que $F(b + \alpha) = F(\alpha)$.

   b) Si $b \in F$ es no nulo, demostrar que $F(b\alpha) = F(\alpha)$.

3. Demostrar que $[\mathbb{Q}(\sqrt{2},\sqrt{6}):\mathbb{Q}]=4$.

4. Sean K_1, K_2 subcuerpos de un cuerpo K. Considere el Composito K_1K_2 de K_1 y K_2. Sean K_1, K_2 extensiones finitas de un cuerpo F. Pruebe que $[K_1K_2:F]\leq [K_1:F]\,[K_2:F]$

5. Sea $a=\sqrt{2}+\sqrt{3}$ y sean $L=\mathbb{Q}(a)$ y $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

   i) Pruebe que $\sqrt{6}\in L$ y $[K:\mathbb{Q}]=4$.

   ii) Demuestre que $L\neq\mathbb{Q}(\sqrt{6})$ y concluir que $L=K$.

   iii) Encontrar un polinomio irreducible sobre $\mathbb{Q}[x]$ que se anule en a.

6. Considere el siguiente diagrama de cuerpos

$$\begin{array}{c}(\mathbb{Q}(\sqrt{2}))(\sqrt[3]{5})\\ |\\ \mathbb{Q}(\sqrt{2})\\ |\\ \mathbb{Q}\end{array}$$

   a) Demostrar que $\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$ es una extensión finita de $\mathbb{Q}$ de grado 6.

   b) Demostrar que: $\mathbb{Q}(\sqrt{2}+\sqrt[3]{5})=\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$ y pruebe que $\sqrt{2}+\sqrt[3]{5}$ es algebraico sobre $\mathbb{Q}$.

Guía 3, Cuerpos y álgebras

1. Sean $p_1,\cdots,p_n$ primos distintos entre sí. Pruebe que

$$[\mathbb{Q}(\sqrt{p_1},\cdots,\sqrt{p_n}):\mathbb{Q}]=2^n\ \ \forall\, n\in\mathbb{N}.$$

2. Sean $p_1,\cdots,p_n$ primos distintos entre sí y $F=\mathbb{Q}(\sqrt{p_1},\cdots,\sqrt{p_n})$. Sean $q_1,\cdots,q_r$ primos distintos entre sí y distintos de los p_i.

   Pruebe que $\sqrt{q_1\cdots q_r}$ no pertenece a F.

3. Pruebe que si $[K(a) : K]$ es impar entonces $K(a) = K(a^2)$.

4. Sea $L = K(\alpha) \simeq K[x]/\langle P\rangle$ una extensión de grado n de K y $\sigma : L \to L$ un automorfismo tal que $\sigma|_K = \mathrm{id}$.

   i). Pruebe que $\sigma(\alpha)$ es una raíz de P. Concluya que, si P tiene todas sus raíces distintas, entonces:

   $$\mathrm{Aut}(L/K) = \{\sigma : L \to L \text{ automorfismo } : \sigma|_K = \mathrm{id}\},$$

   cumple con $|\mathrm{Aut}(L/K)| \leq n$.

   ii). Sea $L = \mathbb{Q}(\sqrt{d})$, con $d \in \mathbb{Z}$ libre de cuadrados.

   Pruebe $|\mathrm{Aut}(L/\mathbb{Q})| = 2$.

5. Sea K una extensión de F y $\alpha \in K$ un elemento transcendente sobre F. Demuestre que existe un isomorfismo de cuerpos entre $Q(F[x])$ (el cuerpo de cocientes de $F[x]$) y $F(\alpha)$, que es la identidad sobre F.

6. Sea E extensión algebraica de F. Dos elementos α y $\beta \in E$ se dicen conjugados si $m_{\alpha,F} = m_{\beta,F}$. Por ejemplo, en $E = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$, ξ_3 y ξ_3^2 son conjugados, donde ξ_3 es raíz primitiva cúbica de la unidad. Sean α, β algebraicos sobre F con α de grado n.

   Considere la función $\varphi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ definida por $\varphi_{\alpha,\beta}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1} \ \forall \ c_i \in F$. Pruebe que $\varphi_{\alpha,\beta}$ es un isomorfismo sí y sólo sí α y β son conjugados.

7. Encuentre el cuerpo de descomposición de los siguientes polinomios:

   i) $f(x) = x^4 - 3$ sobre $\mathbb{Q}$ ii) $f(x) = x^4 - 6x^2 - 2$ sobre $\mathbb{Q}$.

8. Considere el cuerpo de descomposición $E = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ del polinomio $f(x) = (x^2 - 2)(x^2 - 3)$ sobre $\mathbb{Q}$.

   Pruebe que $\varphi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2} \ \forall \ a, b \in \mathbb{Q}(\sqrt{3})$ es un automorfismo de E tal que $\varphi(x) = x$ para todo x en $\mathbb{Q}(\sqrt{3})$.

9. Determine el cuerpo de descomposición L de $p(x) = x^4 - 2 - i$ sobre $\mathbb{Q}(i)$. Luego calcule $[L : \mathbb{Q}]$.

10. Determine el cuerpo de descomposición de $p(x) = x^4 - 6x^2 + 2$ sobre $\mathbb{Q}$.

11. Sea $n \in \mathbb{N}$ y $\mathbb{F}_p$ el cuerpo de p elementos. Sea L el cuerpo de descomposicón del polinomio $G(x) = x^{p^n} - x$ sobre $\mathbb{F}_p[x]$. Muestre que G no tiene raíces repetidas y que G es reducible sobre $\mathbb{F}_p[x]$. Pruebe que L es el conjunto de raíces de G. Concluya que $[L : \mathbb{F}_p] = n$.

Guía 4, Cuerpos y álgebras

1. Sea $K \subset L \subset \overline{K}$, donde L/K es una extensión finita. Pruebe que L es el cuerpo de descomposición de un polinomio en $K[x]$ si y solamente si para todo homomorfismo $\phi : L \to \overline{K}$ tal que $\phi|_K = \text{id}$ se cumple que $\phi(L) = L$.

2. Sea α algebraico sobre K. Pruebe que cada monomorfismo φ de $K(\alpha)$ en $\overline{K}$ tal que $\varphi(a) = a \ \ \forall\, a \in K$ lleva α en un conjugado β de α sobre K. Recíprocamente, por cada conjugado β de α sobre K, hay sólo un monomorfismo $\varphi_{\alpha,\beta}$ de $K(\alpha)$ en $\overline{K}$ que lleva α en β y cada a en K en sí mismo.

3. Sea $\overline{\mathbb{Q}_\mathbb{C}} = \{\alpha \in \mathbb{C} \ / \ \alpha \text{ es algebraico sobre } \mathbb{Q}\}$.

   i) Pruebe que $\overline{\mathbb{Q}_\mathbb{C}}$ es algebraicamente cerrado.

   ii) Pruebe que $[\overline{\mathbb{Q}_\mathbb{C}} : \mathbb{Q}]$ es infinita.

   iii) Pruebe que el conjunto formado por todos los elementos algebraicos sobre $\mathbb{R}$ es numerable.

   iv) Pruebe que $\overline{\mathbb{Q}_\mathbb{C}} \cap \mathbb{R}$ es subcuerpo propio de $\mathbb{R}$, luego $\overline{\mathbb{Q}_\mathbb{C}}$ es subcuerpo propio de $\mathbb{C}$.

4. Sea F cuerpo finito con q elementos y sea K una extensión finita de F de grado n. Pruebe que K tiene q^n elementos. Usando este ejercicio, construya un cuerpo con 3^2 elementos.

5. Sea K un cuerpo finito. Pruebe que K tiene p^n elementos, donde $p = \text{car}(K)$ y n es algún natural.

6. Sea K cuerpo con p^n elementos. Pruebe que $a^{p^n} = a$ para todo elemento a en K.

7. Sea $K = \{a_1, \cdots, a_{p^n}\}$. Pruebe que el polinomio $f(x) = x^{p^n} - x$ se factoriza en $K[x]$ como $f(x) = (x - a_1) \cdots (x - a_{p^n})$.

Guía 5, Cuerpos y álgebras

1. Pruebe que

$$x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^{\times}} (x - \alpha)$$

Concluya que $\prod_{\alpha \in \mathbb{F}_{p^n}^{\times}} \alpha = (-1)^{p^n}$, luego el producto de elementos distintos de cero de un cuerpo finito es 1 si $p = 2$ y -1 si p es impar. Si p es impar y $n = 1$, obtenga el teorema de Wilson: $(p-1)! \equiv -1(mod p)$.

2. Considere el polinomio $P(x) \in \mathbb{F}_p[x]$ dado por $P(x) = x^p - x + a$ con $a \in \mathbb{F}_p^*$. Sea $\alpha \in \bar{\mathbb{F}}_p$ una raíz de $P(x)$.

i). Pruebe que $\alpha + b$ es una raíz de $P(x)$ para todo $b \in \mathbb{F}_p$. Concluya que $P(x)$ es separable.

ii). Sea $F \subset F(\alpha) \subset \overline{F}$, donde $\alpha \in \overline{F}$ es un elemento algebraico y sea $X = \left\{\phi : F(\alpha) \to \overline{F} : \phi|_F = \text{id}\right\}$. Demuestre que $|X| \leq n$ y que $|X| = n$ si y solamente si $m_{\alpha,F}(x)$ es separable.

iii). Concluya que $P(x)$ es irreducible.

3. Pruebe que si $P(x) = x^p - x - q$ es irreducible sobre $\mathbb{F}_p$ entonces es P es separable.

4. Estudie la separabilidad de $H(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ sobre $\mathbb{F}_2[x]$. Note que $H(x) = Q(x)T(x)$, donde $Q(x) = x^3 + x + 1$ y $T(x) = x^3 + x^2 + 1$.

5. Pruebe que todo divisor Q en $K[x]$ de un polinomio separable P es separable.

6. Pruebe que si un polinomio P en $K[x]$ es separable, también lo es sobre cualquier extensión L de K.

7. Pruebe que cada extensión finita de un cuerpo finito es separable.

8. Sean $K \subseteq L \subseteq E$ cuerpos tal que E/K separable. Pruebe que E/L y L/K son separables.

Guía 6, Cuerpos y álgebras

1. Pruebe que d divide a n si y solo si $x^d - 1$ divide a $x^n - 1$. Sugerencia: Si $n = qd + r$ entonces $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$.

2. Sea $a > 1$ entero. Pruebe que para cada par n, d de enteros positivos se tiene que d divide a n si y solo si $a^d - 1$ divide a $a^n - 1$. Concluya que: d divide a n si y solo si $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$.

3. Pruebe que cada extensión finita de un cuerpo finito es separable.

4. Encuentre el polinomio ciclotómico para $n = 6, 8, 9, 10$ y 12.

5. Pruebe que si $n = p^k m$, donde p es primo y m es relativamente primo con p entonces hay exactamente m raíces distintas $n-$ ésimas de la unidad sobre un cuerpo de característica p.

6. Pruebe que si n es impar $n > 1$, entonces $\Phi_{2n}(x) = \Phi_n(x)$.

7. Sea l primo y sea $\Phi_l(x) = x^{l-1} + \cdots + x + 1 \in \mathbb{Z}[x]$ el $l-$ésimo polinomio ciclotómico, que es irreducible sobre $\mathbb{Z}$. Sea p un número primo y ζ una raíz primitiva $l-$ ésima de la unidad.

   a) Pruebe que si $p = l$, entonces $\Phi_l(x) = (x-1)^{l-1} \in \mathbb{F}_l[x]$.

   b) Sea $p \neq l$ y sea f la menor potencia de p tal que $p^f \equiv 1 \bmod l$. Use el hecho de que $\mathbb{F}_{p^n}^{\times}$ es un grupo cíclico para mostrar que $n = f$ es la menor potencia p^n de p tal que $\zeta \in \mathbb{F}_{p^n}$. Concluya que el polinomio minimal de ζ sobre $\mathbb{F}_p$ tiene grado f.

c) Muestre que $\mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$ para cualquier a no divisible por p. Una inclusión es inmediata, para la otra, note que $\zeta = (\zeta^a)^b$ donde b es el inverso multiplicativo de a mod l. Concluya usando b) que, en $\mathbb{F}_p[x], \Phi_l(x)$ es el producto de $\frac{l-1}{f}$ polinomios irreducibles distintos de grado f.

d) En particular pruebe que en $\mathbb{F}_p, \Phi_7$ es $(x-1)^6$ para $p = 7$, un producto de factores lineales distintos para $p \equiv 1 \bmod 7$, un producto de dos polinomios cúbicos irreducibles para $p \equiv 2, 4 \bmod 7$ y es irreducible para $p \equiv 3, 5 \bmod 7$.

Guía 7, Cuerpos y álgebras

1. Es claro que $id : \mathbb{C} \longrightarrow \mathbb{C},\ a + bi \to a + bi$ y $\sigma : \mathbb{C} \to \mathbb{C},\ a + bi \longrightarrow a - bi$ son automorfismos de $\mathbb{C}$. Pruebe que son los únicos automorfismos de $\mathbb{C}$ que dejan fijo $\mathbb{R}$.

2. Determine el grupo $\mathrm{Aut}(L/\mathbb{Q})$ para $L = \mathbb{Q}(\sqrt{5}, \sqrt{7})$ y para $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ el cuerpo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$.

3. Sea F subcuerpo de $\mathbb{C}$ entonces los polinomios $P(x) = x^3 + ax^2 + bx + c \in F[x]$ y $Q(y) = y^3 + (b - \frac{1}{3}a^2)y + c - \frac{1}{3}ab + \frac{2}{27}a^3 \in F[x]$ tienen el mismo cuerpo de descomposición. Sug. tomar $y = x + \frac{1}{3}a$.

4. Sean F subcuerpo de $\mathbb{C}, P(x) = x^3 + bx + c$ polinomio irreducible en $F[x]$. Sean α, β, γ raíces de P en $\mathbb{C}$. Pruebe que $K = F(\delta_0, \alpha)$ es el cuerpo de descomposición de P donde $\delta_0 = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \in \mathbb{C}$ es una raíz de $Q(x) = x^2 + 4b^3 + 27c^2$ y $\alpha \in \mathbb{C}$ es una raíz de P.

5. Pruebe que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es una extensión de Galois sobre $\mathbb{Q}$ y que el grupo $G = Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ es isomorfo al grupo de Klein.

6. Sea $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ el cuerpo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$. Pruebe que $Gal(E/\mathbb{Q})$ es isomorfo a S_3 grupo simétrico de 3 letras.

7. Sean F subcuerpo de $\mathbb{C}, P(x) = x^3 + bx + c \in F[x]$ polinomio irreducible en $F[x]$ y E cuerpo de descomposición de P. Pruebe que

a) Si $-4b^3 - 27c^2$ es un cuadrado en F, entonces $\text{Gal}(E/F)$ es un grupo de orden 3, isomorfo a C_3, grupo cíclico de orden 3.

b) Si $-4b^3 - 27c^2$ no es un cuadrado en F, entonces $\text{Gal}(E/F)$ es un grupo de orden 6, isomorfo a S_3, grupo simétrico de 3 letras.

8. Encuentre el grupo de Galois de P sobre $\mathbb{Q}$, donde a) $P(x) = x^3 + 5 \in \mathbb{Q}[x]$, $P(x) = x^3 - 5x - 1 \in \mathbb{Q}[x]$.

Guía 8, Cuerpos y álgebras

1. Considere el cuerpo de funciones racionales $E = K(t), K$ cuerpo. Pruebe que los automorfismos de E que dejan fijo K son las funciones racionales $t \longrightarrow \frac{at+b}{ct+d}$, con $a, b, c, d \in K, ad - bc \neq 0$.

2. Sea K cuerpo cuya característica es relativamente prima con n. Sea ξ_n una raíz primitiva n-ésima de la unidad. Pruebe que $Gal(K(\xi_n)/K)$ es abeliano.

3. A continuación se presentarán 3 afirmaciones, en cada una de ellas usted deberá decidir si la afirmación es verdadera o falsa, justificando su elección con una demostración o un contraejemplo.

   i) Existe alguna extensión finita $K/\mathbb{Q}$, que contenga infinitos cuerpos intermedios. Es decir, existen infinitos cuerpos F tal que $\mathbb{Q} \subseteq F \subseteq K$.

   ii) Sea K/F una extensión Galoisiana con grupo de Galois G y $a \in K$, entonces $K = F(a)$ si y solo si $\forall\, \sigma, \tau \in G,\ \sigma(a) = \tau(a) \rightarrow \sigma = \tau$.

   iii) $\text{Gal}(K/\mathbb{Q}) \simeq S_3$, donde K es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $x^3 + x - 1$.

4. Sean K_1, K_2 dos extensiones de Galois sobre F. Pruebe que

   a) La intersección $K_1 \cap K_2$ es Galois sobre F.

b) El Composito K_1K_2 es Galois sobre F. Su grupo de Galois es isomorfo al subgrupo H de $Gal(K_1/F) \times Gal(K_2/F)$ formado por los elementos cuyas restricciones a la intersección $K_1 \cap K_2$ sean iguales.

5. K_1, K_2 dos extensiones de Galois sobre F tales que $K_1 \cap K_2 = F$. Entonces $Gal(K_1K_2/F) = Gal(K_1/F) \times Gal(K_2/F)$. Recíprocamente, si K es Galois sobre F y $G = Gal(K/F) = G_1 \times G_2$, con G_1, G_2 subgrupos de G,entonces K es el Composito de dos extensiones de Galois K_1 y K_2 de F tales que $K_1 \cap K_2 = F$.

Guía 9. Cuerpos y álgebras

1. Sea p primo. Pruebe que $\mathbb{F}_{p^n}$ es extensión de Galois sobre $\mathbb{F}_p$ con grupo de Galois cíclico de orden n generado por el automorfismo de Frobenius.

2. Sea K extensión de Galois sobre F y sea F' una extensión cualquiera de F. i) Pruebe que KF' es extensión de Galois sobre F' con grupo de Galois isomorfo a un subgrupo de $Gal(K/F)$. Más precisamente, $Gal(KF'/F') \simeq Gal(K/K \cap F'$

   ii) $[KF' : F] = \frac{[K:F][F':F]}{[K \cap F':F]}$

3. Sean K_1, K_2 dos extensiones de Galois sobre F. Entonces a) La intersección $K_1 \cap K_2$ es Galois sobre F.

   b) El Composito K_1K_2 es Galois sobre F. Su grupo de Galois es isomorfo al subgrupo H de $Gal(K_1/F) \times Gal(K_2/F)$ formado por los elementos cuyas restricciones a la intersección $K_1 \cap K_2$ sean iguales.

4. Sea E extensión finita y separable de F. Entonces E está contenida en una extensión K que es Galois sobre F y minimal en el sentido que en $\overline{K}$, cualquier otra extensión de Galois de F que contiene a E contiene a K. Esta extensión K de F se llama la clausura de Galois de E sobre F.

5. Sea G grupo finito. Pruebe que son equivalentes: i) G es soluble.

ii) G posee una cadena finita de subgrupos $\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_s = G$ tal que para cada $i,\ H_i \trianglelefteq H_{i+1}$ y los cuocientes H_{i+1}/H_i son cíclicos de orden primo.

iii) G posee una cadena finita de subgrupos $\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_t = G$ tal que para cada $i,\ N_i \trianglelefteq G$ y los cuocientes N_{i+1}/N_i son abelianos.

6. Considere el polinomio $g(x) = x^3 + px + q \in \mathbb{Q}[x]$, con $pq \neq 0$. Considere la ecuación cuadrática $x^2 + qx - \frac{1}{27}p^3 = 0 \ \ (*)$. Vea que las soluciones de (*) son $x_1 = -\frac{1}{2}q + \delta,\ x_2 = -\frac{1}{2}q - \delta \in \mathbb{C}$ y $\delta^2 = \frac{1}{4}q^2 + \frac{1}{27}p^3$. Sea $u \in \mathbb{C}$ tal que $u^3 = x_1$. Si $v = -\frac{p}{3u}p^3$, entonces $v^3 = x_2$. Pruebe que las raíces de $g(x)$ son $u + v, u\xi_3 + v\xi_3^2, u\xi_3^2 + v\xi_3$, donde ξ_3 es una raíz primitiva cúbica de la unidad.

7. Usando el método del problema anterior encuentre todas las raíces complejas de $g(x) = x^3 + 3ix - 1 - i$.

8. a) Pruebe que $f(x) = x^5 - 3$ es soluble por radicales.

   b) Pruebe que $f(x) = x^5 - 6x + 3$ no es soluble por radicales.

Guía 10. Cuerpos y álgebras

1. Sea G grupo y sea R anillo conmutativo con unidad. Denote

$$RG = \{f \in R^G \mid f(x) = 0 \ \text{ para casi todo } \ x \in G\}.$$

   Defina suma y producto por escalar de los elementos de RG usuales y defina una multiplicación en RG por convolución

$$(fg)(x) = \sum_{\text{finita } (y,z)\ x=yz} f(y)g(z),\ f(y)g(z) \neq 0$$

   Entonces RG es una R- álgebra, llamada álgebra de grupo de G sobre R.

2. Sea $A,\ R$-álgebra con unidad e I ideal de A. Pruebe:

   (a) Si $1 \in I$ entonces $I = A$.

   (b) Si A es de división y u invertible, $u \in I$ entonces $I = A$.

3. Pruebe que $\mathbb{H}$ es álgebra simple. Use el corchete de Lie $[x, y] = xy - yx$.

4. Sea A un álgebra sobre F, de dimensión finita. Averigue que relaciones deben satisfacer las constantes de estructura para que el álgebra sea asociativa.

5. $A = \left(\frac{a,b}{F}\right) = F \oplus F_i \oplus F_j \oplus F_k$; el F- espacio vectorial $F_i \oplus F_j \oplus F_k$ se denota por A_+ y se llama cuaterniones puros.

   Sea $x \in \left(\frac{a,b}{F}\right) - \{0\}$, $x = c + z$ con $c \in F$ y $z \in A_+$. Pruebe que $x \in A_+ \Leftrightarrow x \notin Z(A) \wedge x^2 \in Z(A)$.

6. Sea $A = \left(\frac{a,b}{F}\right)$ álgebra de cuaterniones sobre F, car $(F) \neq 2$ y sea $x = c + z \in A = F \oplus A_+$. Se definen $\bar{x} = c - z$ y $N(x) = x\bar{x}$ y se llaman el conjugado y la norma del cuaternión x. Se tienen las siguientes propiedades:

   (a) $\forall x \in A,\ \ N(x) \in F,\ \ x\bar{x} = \bar{x}x,\ \ \bar{\bar{x}} = x.$

   (b) $\forall x \in F,\ \ \bar{x} = x.$

   (c) $\forall x, y \in A,\ \ \overline{x + y} = \bar{x} + \bar{y},\ \ \overline{xy} = \bar{y}\bar{x}.$

   (d) $\forall x, y \in A,\ \ N(x) = N(\bar{x}),\ N(xy) = N(x)N(y).$

   (e) $\forall k \in F,\ \forall x \in A\ \ N(k) = k^2,\ N(kx) = k^2 N(x).$

7. Sea $A = \left(\frac{a,b}{F}\right)$ álgebra de cuaterniones sobre F, car $(F) \neq 2$. Entonces son equivalentes:

   (i) A es un álgebra de división.

   (ii) $x \in A, x \neq 0 \Rightarrow N(x) \neq 0$.

   (iii) Si c_0, c_1, c_2 satisfacen la ecuación $x_0^2 = ax_1^2 + bx_2^2$ entonces $c_0 = c_1 = c_2 = 0$.

8. Sea A un espacio vectorial sobre F, de dimensión finita. Pruebe que dos sistemas de constantes de estructura α_{ijk} y β_{ijk} definen sobre A estructuras de álgebras isomorfas, no necesariamente asociativas si y sólo si existe $\varphi : A \to A$ lineal biyectiva tal que

$$\varphi(e_i \star e_j) = \varphi(e_i) \circ \varphi(e_j)\ \ \forall i, j \in \{1, \ldots, n\}$$

donde

$$e_i \star e_j = \sum_{k=1}^{n} \alpha_{ijk} e_k; \quad e_i \circ e_j = \sum_{k=1}^{n} \beta_{ijk} e_k$$

si y sólo si

$$\sum_{k=1}^{n} \alpha_{ijk} x_{rk} = \sum_{s,t=1}^{n} \beta_{ijk} x_{si} x_{tj}, \ 1 \leq i, j, r \leq n,$$

donde $(x_{ij}) \in M_n(F)$ es la matriz invertible asociada a φ con respecto a la base $\{e_1, \ldots, e_n\}$ de A.

Guía 11. Cuerpos y álgebras

1. Considere el álgebra de funciones $A = \mathbb{R}^{\mathbb{R}}$. Encuentre subálgebras de A, ideales derechos e izquierdos de A. ¿ Existen ideales biláteros de A?

2. Sea A una R-álgebra con uno, $f : A \longrightarrow A$ homomorfismo tal que $f(1) = 1$ y $\delta : A \longrightarrow A$ una f-derivación, es decir, $\forall \ a, b \in A, \ \delta(ab) = \delta(a)b + f(a)\delta(b)$. En $A[x]$ definamos un nuevo producto

$$x^i x^j = x^{i+j}, \quad xa = ax = f(a)x + \delta(a) \ \forall \ a \in A$$

Denotemos por $A[x, f, \delta]$ esta nueva estructura. Pruebe que $A[x, f, \delta]$ es una R-álgebra usando S la subálgebra de $\mathrm{End}_R(A[x])$ generada por los endomorfismos $\lambda_a, \ a \in A$ y φ donde

$$\lambda_a(\sum a_i x^i) = \sum a a_i x^i, \quad \varphi(\sum a_i x^i) = \sum f(a_i)\delta(a_i) x^i$$

Defina $\sigma : A[x, f, \delta] \longrightarrow S$ por $\sigma(\sum a_i x^i) = \sum \lambda_{a_i} \circ \varphi^i$ y pruebe que σ es un homorfismo de R-módulos y que la multiplicación en $A[x, f, \delta]$ se corresponde por σ con la multiplicación en S.

3. Considerar la $\mathbb{R}$-álgebra $A = \mathbb{C}[x, f, 0]$ donde f es la conjugación en $\mathbb{C}$. Pruebe que

   a) $Z(A) = \mathbb{R}[x^2]$,

   b) $A/ < x^2 + 1 > \simeq \mathbb{H}$,

c) $A/ < x^4 + 1 > \simeq M_2(\mathbb{C})$.

Para (c) usar el homomorfismo inducido por $\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & f(a) \end{pmatrix}$ y $\varphi(x) = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$

4. Sean M, N, T R-módulos. Pruebe que

$$Bil(M \times N; T) \simeq Hom_R(M, Hom_R(N, T)).$$

5. Sean S subanillo de R, y $N \simeq R^n$, pruebe que $S \otimes_R N \simeq S^n$

6. Sea G grupo abeliano finito de orden n. Pruebe que el $\mathbb{Q}$-módulo $\mathbb{Q} \otimes_{\mathbb{Z}} G$ es cero.

7. Pruebe que $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$, $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$. Más en general, pruebe que $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$. Donde d es el máximo comn divisor de m y n.

8. Sean I, J ideales de R, entonces $R/I, R/J$ son $R-$ módulos. Pruebe que

$$R/I \otimes_R R/J \simeq R/(I + J)$$

9. En el anillo $R = \mathbb{Z}[x]$, sea $I = (2, x)$ el ideal generado por 2 y por x. Entonces el anillo $\mathbb{Z}/2\mathbb{Z} = R/I$ es un $R-$ módulo aniquilado por x y por 2. a) Pruebe que $\varphi : I \times I \to \mathbb{Z}/2\mathbb{Z}$, definida por $\varphi(a_0 + \cdots + a_n x^n, b_0 + \cdots + b_m x^m) = \frac{a_0}{2} b_1 \mod 2$ es R-bilineal.

   b) Pruebe que hay un homomorfismo de $R-$ módulos de $I \otimes_R I \to \mathbb{Z}/2\mathbb{Z}$, que lleva $p(x) \otimes q(x)$ en $\frac{p(0)}{2} q'(0)$, donde $q'(x)$ es el polinomio derivado de $q(x)$.

   c) Pruebe que $2 \otimes x \neq x \otimes 2$.

10. Sea M, N, T tres R-módulos. Pruebe que: $(M \otimes_R N) \otimes_R T \simeq M \otimes_R (N \otimes_R T$.

Guía 12. Cuerpos y álgebras

1. Sea V espacio vectorial sobre $\mathbb{R}$ de base $\{e_1, e_2\}$. Pruebe que $e_1 \otimes e_2 - e_2 \otimes e_1 \neq a \otimes b$, con $a, b \in V$.

2. Sean M, M', N, N' R-módulos. Pruebe que:

   a) $(M \oplus M') \otimes_R N \simeq (M \otimes_R N) \oplus (M' \otimes_R N)$.

   b) $M \otimes_R (N \oplus N') \simeq (M \otimes_R N) \oplus (M \otimes_R N')$.

3. Sean M, M', N, N' R-módulos, $f : M \to M',\ g : N \to N'$ aplicaciones lineales. Pruebe que

   i) hay única aplicación lineal $h : M \otimes_R N \to M' \otimes_R N'$ tal que $h(m \otimes n) = f(m) \otimes g(n)\ \ \forall\, m \in M, n \in N$. h se anota $f \otimes g$.

   ii) $id_M \otimes id_N = id_{M \otimes_R N}$.

   iii) f y g epiyectivas $\Rightarrow f \otimes g$ epiyectiva

4. Sean I ideal de R, entonces R/I es un $R-$ módulo. Sea M un R-módulo. Pruebe que $R/I \otimes_R M \simeq M/IM$

5. Sean G, G' grupos. Pruebe que

$$R(G \times G') \simeq R[G] \otimes_R R[G'] \ \text{ (isomorfismo de álgebras)}$$

6. Sean F cuerpo, A, B F-álgebras asociativas, con unidad. Pruebe que

$$Z(A \otimes_F B) = Z(A) \otimes_F Z(B)$$

7. Sean F cuerpo, A una F-álgebra, K una extensión de F. Entonces $A_K = K \otimes_F A$ es un álgebra que se llama la extensión escalar de A. Si A es de dimensión finita y $\{a_1, a_2, \cdots, a_n\}$ es una base de A entonces $z \in A_K,\ z = \sum_{i=1}^{n} \alpha_i \otimes a_i$.

8. $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{C}$ (isomorfismo de anillos)

Guía 13. Cuerpos y álgebras

1. Pruebe que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = \{0\}$.

2. El producto tensorial $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ es libre de rango 4 como módulo sobre $\mathbb{R}$, de base $\{e_1 = 1 \otimes 1,\ \ e_2 = 1 \otimes i,\ \ e_3 = i \otimes 1,\ \ e_4 = i \otimes i\}$. i) Escriba la mutiplicación de dos elementos cualesquiera en el álgebra $A = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

   ii) Sea $\varepsilon_1 = \frac{1}{2}(e_1 + e_4),\ \varepsilon_2 = \frac{1}{2}(e_1 - e_4)$. Pruebe que $\varepsilon_1\varepsilon_2 = 0,\ \ \varepsilon_1 + \varepsilon_2 = 1,\ \ \varepsilon_j^2 = \ \ \varepsilon_j$ para $j = 1, 2$. (ε_1 y ε_2 se llaman elementos idempotentes ortogonales). Deduzca que A es isomorfa como anillo al producto directo de dos ideales principales: $A \simeq A\varepsilon_1 \times A\varepsilon_2$.

   iii) Pruebe que la aplicación $\varphi : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ definida por $\varphi(z_1, z_2) = (z_1 z_2, z_1\overline{z_2})$ es un aplicación $\mathbb{R}-$ bilineal.

   iv) Sea $\phi : A \to \mathbb{C} \times \mathbb{C}$ el homomorfismo de $\mathbb{R}-$ módulos obtenido de φ de la parte iii). Pruebe que $\phi(\varepsilon_1) = (0, 1)$ y $\phi(\varepsilon_2) = (1, 0)$. Pruebe que ϕ es isomorfismo de $\mathbb{C}$ álgebras, es decir $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$

3. Pruebe que en $\mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2$ se tiene que $(1, 1) \otimes (1, 4) + (1, -2) \otimes (-1, 2) = 6(1, 0) \otimes (0, 1) + 3(1, 0) \otimes (0, 1)$.

4. Sea V un $\mathbb{R}$ espacio vectorial de base $\{e_1, e_2\}$. Pruebe que el elemento $e_1 \otimes e_2 - e_2 \otimes e_1 \in V \otimes_{\mathbb{R}} V$ no puede escribirse como un tensor simple $a \otimes b$ para cualquier $a, b \in V$.

5. Pruebe que si M es un R-módulo cíclico entonces $T(M) = S(M)$.

6. Sea V un F espacio vectorial de dimensión n. Pruebe que $S(V)$ es isomorfa a la F-álgebra graduada de anillos de polinomios en n variables.

7. Sea $x \in \Lambda^k(M), y \in \Lambda^t(M)$. Pruebe que $x \wedge y = (-1)^{kt} y \wedge x$.

8. Sea V espacio vectorial de dimensión finita sobre un cuerpo F con base $B = \{v_1, \cdots, v_n\}$ entonces los vectores

$$v_{i1} \wedge v_{i2} \wedge \cdots \wedge v_{ik} \text{ para } 1 \leq i_1 < i_2 \cdots < i_k \leq n$$

   son una base de $\Lambda^k(V)$, y $\Lambda^k(V) = \{0\}$ si $k > n$. Cunado $k = 0$, el vector base es el elemento 1 de F.

9. Sea $R = \mathbb{Z}[x, y]$ e $I =< x, y >$.

   a) Pruebe que si $ax + by = a'x + b'y$ en R entonces $a' = a + yf$ y $b' = b - xf$ para algún polinomio $f(x, y) \in R$.

   b) Pruebe que la función $\varphi : I \times I \longrightarrow \mathbb{Z} = R/I$ definida por $\varphi(ax + by, cx + dy) = (ad - bc) + I$ es bilineal alternada.

10. Sea $R = \mathbb{Z}[x, y]$.

    a) Si $M = R$, entonces $\Lambda^2(M) = \{0\}$.

    b) Si $M = I =< x, y >$, entonces $\Lambda^2(I) \neq \{0\}$. Use la función φ construída en el ejercicio anterior.

11. Sea R un dominio de integridad y sea F su cuerpo de cuocientes.

    a) Considerando F como un R-módulo, pruebe que $\Lambda^2(F) = \{0\}$.

    b) Sea I cuaquier R-submódulo de F, por ejemplo, cualquier ideal de R. Pruebe que $\Lambda^i(I)$ es un módulo de torsión cada $i \geq 2$, es decir, para cada $x \in \Lambda^i(I)$ hay un elemento no nulo r en R tal que $rx = 0$.

    c) De un ejemplo de un dominio de integridad R, un R-módulo I en F con $\Lambda^i(I) \neq \{0\}$ para $i \geq 0$.