Apunte Cuerpos y Algebras

Giancarlo Lucchini

2017

Índice

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 están basados en los apuntes del curso dictado por Alicia Labra el 2016.

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 el teorema de extensión de homomorfismos y la unicidad de la clausura algebraica.
3. Comprender las extensiones separables e inseparables, los cuerpos perfectos.
4. Conocer la relación entre extensiones normales y el 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-Schreier.
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.

1. Cuerpos

1.1. Parte Básica

Comencemos por la noción de *característica* de un anillo (la cual es interesante solo en teoría de cuerpos). Sea R un anillo conmutativo y unitario. Podemos entonces considerar el homomorfismo de anillos $\varphi : \mathbb{Z} \to R$ que envía $1_{\mathbb{Z}}$ a 1_R (y por ende envía n a la suma de n veces 1_R).

Notación. Para cada $n \in \mathbb{Z}$ escribimos $n \cdot 1$, o sencillamente n, la imágen $\varphi(n)$ de n en R.

Definición 1.1.1. Definimos la *característica* $\mathrm{car}(R)$ de R, como el único entero no negativo $n \in \mathbb{Z}$ tal que $\ker(\varphi) = n\mathbb{Z}$. En particular, n es el menor entero no negativo tal que $n \cdot 1 = 0$ en R.

Ejemplo 1.1.2. El anillo $\mathbb{Z}/n\mathbb{Z}$ tiene característica n.

Ejemplo 1.1.3. Un anillo de polinomios $R[x]$ posee la misma característica que el anillo R ya que $1_{R[x]} \in R$.

En general, todo anillo conmutativo y unitario contiene un subanillo isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/n\mathbb{Z}$ para algún $n \in \mathbb{N}$ y es éste el que define su característica. En efecto, se trata de la imagen de $\varphi : \mathbb{Z} \to R$ la cual, como sabemos, es isomorfa a $\mathbb{Z}/\ker(\varphi)$. En particular, un anillo es de característica 0 si y solo si éste posee un subanillo isomorfo a $\mathbb{Z}$.

Recordemos ahora rápidamente la definición de un cuerpo.

Definición 1.1.4. Un *cuerpo* es un anillo conmutativo unitario K en el que todo elemento no nulo es invertible, es decir, $K^* = K \setminus \{0\}$. Un *subcuerpo* $L \subset K$ es un subanillo que además es un cuerpo.

Por convención, decimos que el anillo trivial $\{0\}$ NO es un cuerpo. Es decir que, al considerar un anillo unitario, asumimos que $1 \neq 0$.

Ejemplo 1.1.5. Ejemplos de cuerpos son $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ con p primo. $\mathbb{Q}$ es un subcuerpo de $\mathbb{R}$ y éste es un subcuerpo de $\mathbb{C}$. 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 $F(x)$.

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

Proposición 1.1.6. *Sea L un subconjunto de un cuerpo K con al menos dos elementos, entonces L es subcuerpo de K si y solo si*

1. $\forall\, x, y \in L,\ x - y \in L$;

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

Demostración. La primera propiedad nos dice que L es un subgrupo aditivo de K. 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. □

La característica de un cuerpo, a diferencia de la característica de un anillo arbitrario, no puede ser cualquier entero $n \in \mathbb{N}$.

Teorema 1.1.7. *Sea K un cuerpo. Entonces* $\mathrm{car}(K) = 0$ *o* $\mathrm{car}(K) = p$ *con p un número primo. Además, si* $\mathrm{car}(K) = 0$ *(resp.* $\mathrm{car}(K) = p$*), entonces K 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 1.1.8. *Sea R un dominio de integridad. Entonces todo cuerpo que contiene a R contiene a su cuerpo de fracciones $Q(R)$.*

Demostración del Teorema 1.1.7. Consideremos el homomorfismo $\varphi : \mathbb{Z} \to K : 1_{\mathbb{Z}} \mapsto 1_K$ que define la característica de K. El núcleo de este homomorfismo es $n\mathbb{Z}$ con $n = \mathrm{car}(K)$, por lo que debemos demostrar que $n = 0$ o bien $n = p$ con p primo.

Supongamos que $n \neq 0$ y que no es un número primo. Entonces podemos escribir $n = ab$ con $1 < a, b < n$, lo que nos dice que $\varphi(a) \neq 0$ y $\varphi(b) \neq 0$. Pero $\varphi(a)\varphi(b) = \varphi(ab) = 0$ y por ende $\varphi(a) = 0$ o $\varphi(b) = 0$ ya que K es un cuerpo. Como $a, b < n$, esto contradice la definición de n. Tenemos entonces que $n = 0$ o $n = p$ con p primo.

Ahora, si $n \neq 0$, entonces $n = p$, por lo que $\varphi(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ es un subcuerpo de K. De lo contrario, tenemos que $\varphi(\mathbb{Z}) \simeq \mathbb{Z}$ y entonces $\mathbb{Z}$ es un subanillo de K. El Teorema 1.1.8 nos dice entonces que K posee un subcuerpo isomorfo a $\mathbb{Q} = Q(\mathbb{Z})$. □

Observación.
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 1.1.9. El subcuerpo de K del Teorema 1.1.7 se llama *subcuerpo primo* de K. Lo denotamos P.

Observación.
P es el subcuerpo más pequeño de K y corresponde a la intersección de todos los subcuerpos de K. Si $\text{car}(K) = 0$, entonces $P \simeq \mathbb{Q}$. Si $\text{car}(K) = p$, 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 1.1.10. Un *homomorfismo* de cuerpos es un homomorfismo de anillos que respeta la unidad, es decir, un homomorfismo de anillos $\varphi : K \to L$ tal que $\varphi(1_K) = 1_L$.

Pero como dijimos, éstos se comportan de una forma peculiar.

Lema 1.1.11. *Sea $\varphi : K \to L$ un homomorfismo de cuerpos. Entonces φ es inyectivo.*

Demostración. Basta con recordar que $\ker(\varphi)$ es un *ideal* de K y que K es un cuerpo. Luego, sus únicos ideales son los triviales: K y $\{0\}$. El primero corresponde al homomorfismo trivial de anillos $\varphi = 0$, el cual no respeta la unidad y por ende no es un homomorfismo de cuerpos. El segundo nos dice precisamente que φ es inyectivo. □

Observación.
Es precisamente esta observación sobre los ideales de un cuerpo la que nos dice que no existe una buena noción de cociente (recuerde que los cocientes de anillos se definen con ideales).

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 1.1.12 (Teorema de Kronecker)**.** *Sea K un cuerpo y sea $Q \in K[x]$ un polinomio. Entonces existe un cuerpo L que contiene un subcuerpo isomorfo a K en el cual Q tiene una raíz.*

Demostración. Consideremos el anillo $K[x]$ y el ideal $\langle P\rangle$ con P un factor irreducible de Q. Como P es irreducible y $K[x]$ es un DIP, sabemos que se trata de un ideal maximal. Definamos entonces L como el cociente $K[x]/\langle P\rangle$, que es cuerpo por maximalidad de $\langle P\rangle$. Tenemos entonces la proyección canónica $\pi : K[x] \to L$, mientras que por otra parte tenemos la inyección $\iota : K \to K[x]$ que a $a \in K$ le asocia el polinomio constante (i.e. de grado 0) $a \in K[x]$. Entonces podemos considerar el homomorfismo compuesto $\pi \circ \iota : K \to L$. Como π y ι son homomorfismos de anillos que respetan la unidad, la compuesta también lo hace. Por lo tanto, $\iota \circ \pi$ es un homomorfismo de cuerpos y, por el Lema 1.1.11, se trata de una inyección. Esto prueba que L contiene una copia de K.

Para ver que existe $\alpha \in L$ tal que $P(\alpha) = 0$, consideremos el polinomio $x \in K[x]$ y sea $\alpha = \pi(x)$. Entonces $P(\alpha) = P(\pi(x)) = \pi(P(x)) = \pi(P) = 0$, lo que concluye la demostración. (Nótese que podemos dar vuelta P y π ya que π es un homomorfismo y por ende respeta las sumas y multiplicaciones que aparecen en P). □

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.

En el curso de Grupos y Anillos vimos 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 corre 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 1.1.13. *Sea $P \in K[x]$ un polinomio irreducible de grado n. Sea $L = K[x]/\langle P\rangle$ y sea $\alpha = \bar{x} \in L$. Entonces los elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ forman una base de L como K-espacio vectorial y, en particular,*

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

Demostración. Demostremos primero que el conjunto del enunciado es un conjunto generador de L como K-espacio vectorial. Para ello, consideremos un elemento non nulo $\beta \in L^*$ y escribamos $\beta = \bar{Q}$ con $Q \in K[x]$. Como $K[x]$ es un dominio euclideano, sabemos que existen $R, S \in K[x]$ tales que $Q = PS + R$ con $\deg(R) < n$ ($R \neq 0$ ya que de lo contrario $\beta = \bar{Q} = 0$). Vemos entonces que $\beta = \bar{Q} = \bar{R} \in L$ y, como $\deg(R) < n$, sabemos que $R = \sum_{i=0}^{n-1} a_i x^i$ con $a_i \in K$. Esto nos dice que

$$\bar{R} = \sum_{i=0}^{n-1} a_i \bar{x}^i = \sum_{i=0}^{n-1} a_i \alpha^i \quad \text{con } a_i \in K,$$

lo que prueba que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ genera a L como K-espacio vectorial.

Demostremos ahora que se trata de una base, es decir, que los elementos en $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ son K-linealmente independientes. Supongamos entonces que

$$\sum_{i=0}^{n-1} a_i \alpha^i = 0 \in L \quad \text{con } a_i \in K.$$

Si definimos entonces $Q = \sum_{i=0}^{n-1} a_i x^i \in K[x]$, vemos que $\bar{Q} = \sum_{i=0}^{n-1} a_i \bar{x}^i = 0 \in L$ y por ende $Q \in \langle P \rangle$, es decir $Q = PR$ con $R \in K[x]$. Ahora, todo múltiplo no nulo de P tiene un grado que divide a $\deg(P) = n$, pero $\deg(Q) \leq n-1$ (no hay necesariamente igualdad ya que no hemos dicho que $a_{n-1} \neq 0$), por lo que $Q = 0$ y por ende $a_i = 0$ para todo i. Esto prueba que los elementos en $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ son K-linealmente independientes. □

Ejemplo 1.1.14. Consideremos el cuerpo $\mathbb{R}$ y el polinomio irreducible x^2+1. Con la construcción de más arriba obtenemos pues el cuerpo $K = \mathbb{R}[x]/\langle x^2+1 \rangle$, en el cual todo elemento se escribe de la forma $a + b\bar{x}$ con $a, b \in \mathbb{R}$. La suma en este cuerpo es la suma coordenada a coordenada, como en todo espacio vectorial. La multiplicación, por su parte, viene dada por

$$(a + b\bar{x})(c + d\bar{x}) = ac + ad\bar{x} + bc\bar{x} + bd\bar{x}^2 = (ac - bd) + (ad + bc)\bar{x},$$

donde podemos ver que $\bar{x}^2$ fue reemplazado por -1, lo que tiene sentido ya que $\bar{x}^2 + 1 = 0$ en este cuerpo. Evidentemente, como estas fórmulas de suma y multiplicación corresponden a las de los números complejos, tenemos entonces un isomorfismo de cuerpos

$$\begin{aligned} \varphi : K &\to \mathbb{C}, \\ a + b\bar{x} &\mapsto a + bi. \end{aligned}$$

Ejemplo 1.1.15. 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

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

Ejercicio. 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 $\bar{x} \in K$.

1.2. 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 1.2.1. 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.
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 un cociente sin embargo 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 1.2.2. 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.
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 1.2.3. *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. □

Observación.
Si asumimos que "$\infty \cdot n = \infty$" para todo $n \in \mathbb{N} \cup \{\infty\}$, entonces la igualdad del enunciado sigue estando correcta para extensiones infinitas.

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

Definición 1.2.4. Sea K un cuerpo, L/K una extensión y $\alpha_1, \ldots, \alpha_n \in L$. Definimos el *subcuerpo generado por* $\alpha_1, \ldots, \alpha_n$ $K(\alpha_1, \ldots, \alpha_n)$ 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 1.2.5. Sea K un cuerpo y sea P un polinomio irreducible. Entonces el cuerpo $L = K[x]/\langle P\rangle$ del Teorema 1.1.12 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 1.1.12 aparece dentro de extensiones abstractas de la forma más natural.

Teorema 1.2.6. *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.
Este Teorema nos dice de hecho que *todo* cuerpo que contiene una raíz de P posee un subcuerpo isomorfo al construido en el Teorema 1.1.12 y que éste último es por ende el cuerpo más pequeño que posee una tal raíz, salvo isomorfismo.

Demostración del Teorema 1.2.6. Consideremos el homomorfismo de anillos

$$\begin{aligned} \varphi : K[x] &\to K(\alpha) \subset L, \\ Q &\mapsto Q(\alpha). \end{aligned}$$

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 $\mathrm{Im}(\varphi)$ contiene a K y contiene a $\alpha = \varphi(x)$, por lo que contiene a $K(\alpha)$ por definición de éste. □

Del Teorema 1.1.13 deducimos inmediatamente el siguiente corolario.

Corolario 1.2.7. *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 1.2.8. *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. □

El siguiente corolario se demuestra fácilmente por inducción.

Corolario 1.2.9. *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 1.2.10. 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 1.2.11. *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. □

1.3. 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 1.3.1. 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.
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.
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 1.3.2. 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 1.3.3. *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 $K[x]/(m_{\alpha,K}) \cong \varphi(K[x]) \subseteq L$ es un dominio, 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. □

raíz, podemos considerar uno de éstos con grado minimal, el cual denotamos por $P \in K[x]$. Podemos suponer además que P es mónico, ya que basta con dividirlo por su propio coeficiente dominante y esto no afecta sus raíces. Afirmamos que $m_{\alpha,K} = P$ y que éste es único. $P = QR$ con $Q, R \in K[x]$ polinomios de grado mayor o igual a 1 y por ende $\deg(Q), \deg(R) < \deg(P)$. Entonces Esto contradice la minimalidad del grado de P, por lo que esta situación es imposible y P es irreducible. múltiplo de P. Por división euclideana tenemos que $Q = PS + R$ con $S, R \in K[x]$ y $R = 0$ o $\deg(R) < \deg(P)$. Vemos entonces que, como $P(\alpha) = Q(\alpha) = 0$, otra vez la minimalidad del grado de P. polinomio $Q \in K[x]$ del mismo grado y tal que $Q(\alpha) = 0$ es un múltiplo de éste por lo que acabamos de ver. Entonces $P = QR$ con $\deg(R) = \deg(P) - \deg(Q) = 0$, por lo que R es constante y entonces Q es mónico si y solo si $R = 1$.

Definición 1.3.4. 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 es llamado el *polinomio minimal de α*. Definimos el *grado de α* como el grado de su polinomio minimal.

De la segunda afirmación de la Proposición 1.3.3 deducimos inmediatamente el siguiente corolario.

Corolario 1.3.5. *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 1.3.3. □

Otro corolario interesante para encontrar polinomios minimales es el siguiente:

Corolario 1.3.6. *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 1.3.7. $\sqrt{2}$ 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. 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 1.2.6 y su Corolario 1.2.7. A la luz de estas nuevas definiciones y resultados, obtenemos inmediatemante lo siguiente:

Teorema 1.3.8. *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 1.3.9. *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 1.3.10. 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. $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$,

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

Ejercicio. 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 1.3.11. Decimos que L es una *extensión algebraica* de K si todo elemento de L es algebraico sobre K.

Observación.
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 1.3.9.

Proposición 1.3.12. *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 1.2.3 nos dice entonces que $K(\alpha)/K$ es finita y por ende α es algebraico sobre K por la Proposición 1.3.9. □

Demostremos ahora lo que mencionábamos en la última observación.

Proposición 1.3.13. *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 1.2.3 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 1.3.14. *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 1.3.15. *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. □

Un corolario harto menos inocente es el siguiente.

Corolario 1.3.16. *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. 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 1.3.17. *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.

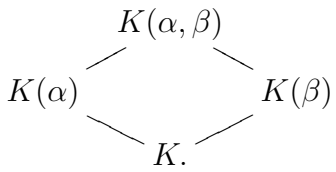
bastará con demostrar que es finitamente generada. Demostraremos esto por inducción sobre $n = [L : K]$. Si $n = 1$, entonces $L = K$ y la afirmación es por ende evidente. Si $n > 1$, nuestra hipótesis de inducción es que el teorema es válido para toda extensión de grado menor que n. Ahora, sea $\alpha_1 \in L \setminus K$. 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 1.3.18. *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 1.3.5, 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.
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. 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 1.3.19. 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 1.3.8 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 $L = K(\sqrt{D})$.

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

Teorema 1.3.20. *Sean L/K y M/L extensiones algebraicas de cuerpos. Entonces M/K también es algebraica.*

Observación.
Nótese que en el caso particular de las extensiones finitas (que son todas algebraicas) esto ya fue demostrado en el Teorema 1.2.3.

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 1.3.17 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.
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.

1.4. Cuerpo de descomposición de un polinomio

La construcción dada en el Teorema 1.1.12 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 1.4.1.

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	$\mathbb{Q}(\sqrt{2})$	$\sqrt{2}$	$x+\sqrt{2}$
$\mathbb{Q}$	$x^4+x^3+x^2+x+1$	$\mathbb{Q}(\zeta_5)$	$\zeta_3 = e^{\frac{2\pi i}{3}}$	$(x-\zeta_5^2)(x-\zeta_5^3)(x-\zeta_5^4)$
$\mathbb{Q}$	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 1.4.2. 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 1.4.3. Sea L/K una extensión de cuerpos y sea $P \in K[x]$ un polinomio de grado ≥ 1. Decimos que L es un *cuerpo de descomposición* de P si:

1. al ver P como un elemento de $L[x]$, éste se factoriza en un producto de factores lineales (i.e. de grado 1);

2. L es el cuerpo más pequeño con esta propiedad, es decir, para todo otro cuerpo M con la propiedad 1, existe un homomorfismo de cuerpos (forzosamente inyectivo) $L \to M$ que extiende la inclusión $K \to M$.

Observación.
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.

No es claro a priori que un tal cuerpo exista. Es por ello que demostraremos ahora su existencia.

Teorema 1.4.4. *Sea K un cuerpo y sea $P \in K[x]$ un polinomio de grado n. Entonces existe un cuerpo de descomposición L de P. Además, L es una extensión finita (y por lo tanto algebraica) de K y $[L : K] \leq n!$.*

Observación.
Dada la segunda propiedad de un cuerpo de descomposición, está claro que si tenemos dos cuerpos de descomposición L_1, L_2 de P, entonces $L_1 \simeq L_2$. En efecto, esta propiedad nos da inyecciones $L_1 \to L_2$ y $L_2 \to L_1$ de K-espacios vectoriales de dimensión finita, lo que basta para probar que estas inyecciones son isomorfismos.

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

Supongamos ahora que $n > 1$ y que el resultado es cierto para todo polinomio P tal que $\deg(P) < n$. Sea R un factor irreducible de P y consideremos el cuerpo de ruptura $K' = K[x]/\langle R\rangle$. Entonces $P = (x - \alpha)Q$ para algún $\alpha \in K'$ y algún $Q \in K'[x]$ con $\deg(Q) = n - 1$. La hipótesis de inducción nos dice que existe un cuerpo de descomposición L/K' de $Q \in K'[x]$. Demostremos que la extensión L/K es entonces un cuerpo de descomposición de $P \in K[x]$.

Es evidente que si Q es un producto de factores lineales en $L[x]$, entonces $P = (x - \alpha)Q$ también lo es, lo que prueba la primera propiedad de un cuerpo de descomposición. Por otra parte, si M/K es otra extensión tal que P se descompone de esta manera en $M[x]$, tomemos un elemento $\beta \in M$ tal que $R(\beta) = 0$. Entonces $K' = K[x]/\langle R\rangle \simeq K(\beta) \subset M$ por la Proposición 1.2.11 y por lo tanto podemos ver K' como un subcuerpo de M y esta inclusión extiende la inclusión de K en M. Usando la hipótesis de inducción nuevamente sobre el cuerpo de descomposición L de Q, vemos entonces que existe un homomorfismo inyectivo $L \to M$ que extiende la inclusión de K' en M, por ende también la de K. Esto prueba que L es un cuerpo de descomposición de P.

Finalmente, notemos que por hipótesis de inducción $[L : K'] \leq (n-1)!$, mientras que claramente $[K' : K] = \deg(P) = n$, por lo que $[L : K] \leq n!$.

□

Ejemplo 1.4.5. 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 1.4.6. 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. Determine el grado $[K : \mathbb{Q}]$ en los últimos dos ejemplos. ¿Son iguales a los grados de los cuerpos de ruptura respectivos?

Ejemplo 1.4.7 (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:

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

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 1.4.8. 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. 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.

Teorema 1.4.9. *Sea $\varphi : K \to K'$ un isomorfismo de cuerpos, sea $P \in K[x]$ un polinomio de grado ≥ 1 y sea $P' \in K'[x]$ el polinomio obtenido al aplicar φ a los coeficientes de P. Sea L un cuerpo de descomposición de P sobre K y sea L' un cuerpo de descomposición de P' sobre K'. Entonces existe un isomorfismo de cuerpos $\sigma : L \to L'$ que extiende φ, es decir $\sigma|_K = \varphi$.*

Demostración. Esto es una sencilla consecuencia de la segunda propiedad de un cuerpo de descomposición. En efecto, el homomorfismo $\varphi : K \to K'$ nos permite

ver K como un subcuerpo de L'. Esto induce un homomorfismo (inyectivo) $\sigma : L \to L'$ que extiende la inclusión de K en L' (la cual no es nada más que φ). De la misma manera, usando el isomorfismo inverso $\varphi^{-1} : K' \to K$, obtenemos un homomorfismo (inyectivo) $L' \to L$. Como ambos son K-espacios vectoriales de dimensión finita por el Teorema 1.4.4, esto prueba que σ es un isomorfismo. □

1.5. 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 1.5.1. Un cuerpo K se dice *algebraicamente cerrado* si todo $P \in K[x]$ no constante tiene una raíz en K.

Observación.
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 1.5.2. 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 1.5.3. *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 1.5.4. *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 1.3.16 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 ya 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 1.5.5. *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. □

Teorema 1.5.6. *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.
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 1.4.9 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 $\mathcal{C} \subset E$ 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 1.1.6, 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 1.4.9 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. □

Para otra demostración de la existencia de la clausura algebraica, supondremos que el lector tiene conocimientos básicos sobre cardinalidad. Necesitaremos el siguiente lema:

Lema 1.5.7. *Si E/K es una extensión algebraica de cuerpos, entonces el cardinal de E no puede exceder al cardinal de $K[x]$. En el caso de que K sea un cuerpo infinito, esto quiere decir que $|E| = |K|$.*

Demostración. Sea S el conjunto de los pares (f, α), con $f \in K[x]$ un polinomio no nulo y $\alpha \in E$ tal que $f(\alpha) = 0$. Como para cada polinomio f, el número de α tales que $(f, \alpha) \in S$ es finito, tenemos que $|S| \leq \aleph_0 |K[x]| = |K[x]|$. Por otra parte E se inyecta en S enviando $\alpha \mapsto (m_{\alpha,K}, \alpha)$ de manera que $|E| \leq |S|$. □

Demostración alternativa de la existencia de $\overline{K}$. Fijemos un conjunto S de cardinalidad mayor a la de $K[x]$ (podría ser el conjunto potencia de $K[x]$) y elijamos cualquier función inyectiva de K en S de manera de indetificar a K con su imagen dentro de S. De esta manera podemos suponer que $K \subseteq S$.

Muchos de los subconjuntos de S pueden convertirse en cuerpos definiendo las operaciones necesarias en ellos. Denotaremos un cuerpo construido de esta forma por un par $(E, \mathcal{E})$ donde $E \subset S$ es el conjunto subyacente al cuerpo y $\mathcal{E}$ denota

la estructura que convierte a E en un cuerpo. (En otras palabras, $\mathcal{E}$ es un par de funciones $E \times E \to E$ que definen la suma y el producto en E.) En particular nuestro cuerpo original es el par $(K, \mathcal{K})$ para cierta estructura fija $\mathcal{K}$.

Definimos una relación de orden $(E_1, \mathcal{E}_1) \leq (E_2, \mathcal{E}_2)$ si $E_1 \subseteq E_2$ como subconjuntos de S y la restricción de la estructura $\mathcal{E}_2$ a E_1 es exactamente la estructura $\mathcal{E}_1$. En otras palabras, $(E_1, \mathcal{E}_1) \leq (E_2, \mathcal{E}_2)$ quiere decir que $(E_2, \mathcal{E}_2)$ es una extensión de cuerpos de $\leq (E_1, \mathcal{E}_1)$.

Ahora sea $\mathcal{P}$ el conjunto de todos los cuerpos $(E, \mathcal{E})$ con $E \subseteq S$ tales que $(K, \mathcal{K}) \leq (E, \mathcal{E})$ y esta extensión es algebraica. Notemos que $\mathcal{P}$ no es vacío pues $(K, \mathcal{K}) \in \mathcal{P}$.

Como pretendemos aplicar el lema de Zorn al conjunto parcialmente ordenado $\mathcal{P}$, debemos verificar que si $\mathcal{L}$ es un subconjunto totalmente ordenado de $\mathcal{P}$, entonces tiene una cota superior en $\mathcal{P}$. Para construir una cota superior $(B\mathcal{B})$, ponemos $B = \bigcup E$ donde $(E, \mathcal{E})$ recorre $\mathcal{L}$ y definimos $\mathcal{B}$ como sigue: si $x, y \in B$, entonces, dado que $\mathcal{L}$ es totalmente ordenado, podemos encontrar $(E, \mathcal{E}) \in \mathcal{L}$ tal que $x, y \in E$. Definimos xy y $x + y$ de la misma forma como están definidos en $(E, \mathcal{E})$. Faltaría verificar que esto está bien definido y que realmente hace que $(B\mathcal{B})$ sea una extensión algebraica de $(K, \mathcal{K})$. Esos detalles se los dejaremos al lector.

Ahora sea $(M, \mathcal{M})$ un elemento maximal de $\mathcal{P}$. Para demostrar que este cuerpo es una clausura algebraica de $(K, \mathcal{K})$, mostraremos que no existe una extensión algebraica no trivial del cuerpo $(M, \mathcal{M})$. Supongamos que L fuera una tal extensión. Por el lema 1.5.7, $|L| < |S|$ y por lo tanto $|L \setminus M| < |S \setminus M|$ y existe una inyección de $L \setminus M$ en $S \setminus M$. Identificando $L \setminus M$ con su imagen en $S \setminus M$, tenemos $L \subseteq S$ y podemos transportar la estructura de cuerpo de L por medio de esta identificación. Lo que resulta es un elemento de $\mathcal{P}$ estrictamente mayor que $(M, \mathcal{M})$, contradiciendo su maximalidad. □

1.6. 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 1.6.1. 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.
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 1.6.2. 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 1.6.3. *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

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

□

Definición 1.6.4. 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 1.6.5. Todo polinomio de grado 1 en $K[x]$ es separable.

Ejemplo 1.6.6. 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 1.6.7. 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.

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 1.6.8. *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 1.6.9. *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 1.6.10. *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 1.6.3 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 1.6.8 nos dice entonces que esto es equivalente a $(P, P') = 1$. □

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

Proposición 1.6.11. *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 1.6.10. □

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

Veamos ahora qué podemos decir del caso de característica positiva. El siguiente lema nos ayudará a entender qué es lo que ocurre en este caso con los polinomios irreducibles.

Lema 1.6.12. *Sea K cuerpo de de característica $p > 0$ y sea $P \in K[x]$ un polinomio. 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 1.6.13. *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 1.6.10. Por otra parte, si P es inseparable, la Proposición 1.6.10 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 1.6.14. 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, basta con tomar una raíz α de P en alguna clausura algebraica de K y ver que

$$(x - \alpha)^p = x^p - \alpha^p = x^p - t = P(x),$$

lo que prueba que P tiene una única raíz con multiplicidad p. Esto prueba en particular que $\mathbb{F}_p(t)$ no es perfecto.

Vemos entonces que el fenómeno que debemos estudiar en característica positiva, es cuándo un polinomio irreducible $P \in K[x]$ proviene de $K[x^p]$. La siguiente definición va en este sentido.

Definición 1.6.15. Sea K un cuerpo de característica $p > 0$. Llamamos *homomorfismo de Frobenius* al homomorfismo de cuerpos

$$\begin{aligned} F : K &\to K, \\ x &\mapsto x^p. \end{aligned}$$

Nótese que se trata realmente de un homomorfismo de cuerpos (inyectivo, dado el Lema 1.1.11), ya que, como todo alumno de enseñanza media adoraría, en un cuerpo de característica p tenemos que

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

En efecto, como $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ y los divisores de $i!$ y $(p-i)!$ no pueden incluir a p a menos que $i = 0, p$, vemos que $p | \binom{p}{i}$ si $i \neq 0, p$. Por otra parte, es evidente ver que $(xy)^p = x^p y^p$ y que $1^p = 1$, lo que prueba que φ es un homomorfismo de cuerpos.

De esta definición podemos sacar lo siguiente.

Proposición 1.6.16. *Sea K un cuerpo de característica $p > 0$. Entonces el conjunto*

$$K^p := \{x^p \mid x \in K\},$$

es un subcuerpo de K.

Si K es además finito, entonces $K^p = K$, es decir, todo elemento de K puede ser escrito como una potencia p-ésima.

Demostración. El conjunto K^p no es nada menos que la imagen $F(K)$ del homomorfismo de Frobenius, por lo que es un subcuerpo.

En el caso en que K es finito, tenemos que K^p es un subcuerpo de K con el mismo cardinal que K (recuerde que F es inyectivo), por lo que $K^p = K$. □

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

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

Definición 1.6.17. Decimos que un cuerpo K es *perfecto* si $\text{car}(K) = 0$ o bien $\text{car}(K) = p$ y $K^p = K$.

Ejemplo 1.6.18. Dada la definición y la proposición anterior, vemos que todo cuerpo finito es perfecto. Vemos también que $\mathbb{F}_p(t)$ no es perfecto gracias al ejercicio anterior.

Definición 1.6.19. Una extensin algebraica E/K se dice *puramente inseparable* si los nicos elementos separables son los elementos de K.

Ejercicio. 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 1.6.11 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 1.6.20. *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 1.6.11, 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 1.6.13 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. $\square$

Definición 1.6.21. 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. 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 1.6.20 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 1.6.22. *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 1.6.23 (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 1.3.17 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 1.6.22. 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 1.3.17 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 1.6.24. *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. □

Definición 1.6.25. Supongamos que E/K es una extensión algebraica y $\overline{K}$ es la clausura algebraica de K. El *grado de separabilidad* de la extensión se define como el número de K-homomorfismos de E en $\overline{K}$ y se denota por $[E : K]_s$.

Proposición 1.6.26. *Sea $K[\alpha]/K$ una extensión algebraica simple. Entonces*

1. *car$(K) = 0 \Rightarrow [K[\alpha] : K] = [K[\alpha] : K]_s$*
2. *car$(K) = p > 0 \Rightarrow [K[\alpha] : K] = p^m[K[\alpha] : K]_s$ para algún entero $m \geq 0$.*

Demostración. Sea $f \in K[x]$ el polinomio minimal de α y supongamos que su grado es n. Si $\varphi K[\alpha] \to \overline{K}$, entonces $f(\varphi(\alpha)) = 0$ y el valor de $\varphi(\alpha)$ determina completamente el homomorfismo φ.

Si $\text{car}(K) = 0$, entonces f tiene n raíces diferentes en $\overline{K}$ y, por el teorema 1.2.11, para cada β tal que $f(\beta) = 0$, existe un K-homomorfismo $\varphi : K[\alpha] \to \overline{K}$ tal que $\varphi(\alpha) = \beta$. Concluimos que $[K[\alpha] : K] = [K[\alpha] : K]_s$ en este caso.

Si $\text{car}(K) = p > 0$, entonces $f = g(x^{p^m})$ para algún entero $m \geq 0$ y algún polinomio g irreducible y separable. El grado de g es $r = \frac{n}{p^m}$ y si sus raíces son $\beta_1, \ldots \beta_r$, entonces

$$f(x) = (x^{p^m} - \beta_1) \ldots (x^{p^m} - \beta_r).$$

Como cada factor $(x^{p^m} - \beta_i)$ tiene una única raíz en $\overline{K}$, f tiene exactamente r raíces diferentes. Por el mismo argumento anterior, concluimos que $[K[\alpha] : K]_s = r$ y $[K[\alpha] : K] = p^m[K[\alpha] : K]_s$. □

Proposición 1.6.27. *Si $F/E/K$ son extensiones algebraicas sucesivas, entonces $[F : K]_s = [F : E]_s[E : K]_s$.*

Demostración. Podemos suponer que $E \subseteq \overline{K}$. Un K-homomorfismo $\varphi : E \to \overline{K}$ se puede extender a $\sigma : \overline{K} \to \overline{K}$. Si $\psi : F \to \overline{K}$ es un E-homomorfismo, entonces $\sigma \circ \psi$ es un K-homomorfismo que extiende φ. Recíprocamente, si ξ es un K-homomorfismo que extiende φ, entonces $\sigma^{-1} \circ \xi$ es un E-homomorfismo. Por lo tanto existen $[F : E]_s$ homomorfismos de F en $\overline{K}$ que extienden φ.

Podemos ahora agrupar los K-homomorfismos $F \to \overline{K}$ en $[E : K]_s$ clases según su restricción a E. Como cada clase contiene $[F : E]_s$ homomorfismos, concluimos que existen $[F : E]_s[E : K]_s$ K-homomorfismos. □

1.7. Interludio 1: Cuerpos finitos

Ya sabemos que para todo primo p existe un cuerpo finito $\mathbb{F}_p$ dado por $\mathbb{Z}/p\mathbb{Z}$. Cabe preguntarse si existen otros cuerpos finitos aparte de éstos. Una primera idea sería el considerar las extensiones finitas de $\mathbb{F}_p$, las cuales son finitas ya que se trata de $\mathbb{F}_p$-espacios vectoriales de dimensión finita. ¿Cuáles son los cardinales de estas extensiones? ¿Habrán otros ejemplos?

Para responder a la segunda pregunta, basta con recordar que todo cuerpo de característica p posee a $\mathbb{F}_p$ como subcuerpo. Ahora, dado un cuerpo finito, es evidente que no puede contener a $\mathbb{Z}$ y por ende su característica tiene que ser un primo p dado y por ende tiene que contener a $\mathbb{F}_p$, por lo que se trata de un $\mathbb{F}_p$-espacio vectorial de dimensión finita y finalmente de una extensión finita de $\mathbb{F}_p$. No hay pues otros cuerpos finitos además de las extensiones finitas de $\mathbb{F}_p$ para cada p. Veamos cuales son sus cardinales y su clasificación.

Como se trata de $\mathbb{F}_p$-espacios vectoriales de dimensión finita, tenemos que el cardinal de estos cuerpos debe ser de la forma p^n con $n \in \mathbb{N}$. El siguiente teorema nos da entonces una respuesta completa a nuestras preguntas.

Teorema 1.7.1. *Para todo primo p y todo entero $n \in \mathbb{N}$, existe un único cuerpo finito (salvo isomorfismo) con p^n elementos, denotado $\mathbb{F}_{p^n}$, el cual corresponde al cuerpo de descomposición del polinomio $P \in \mathbb{F}_p[x]$ dado por $P(x) = x^{p^n} - x$.*

Demostración. Consideremos el cuerpo $\mathbb{F}_p$ y su clausura algebraica $\bar{\mathbb{F}}_p$. Sea $P \in \mathbb{F}_p[x]$ el polinomio dado por $P(x) = x^{p^n} - x$. Podemos entonces considerar el cuerpo de descomposición $K/\mathbb{F}_p$ de P en $\bar{F}_p$. Esto nos dice que

$$P(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{p^n}) \in K[x],$$

y las raíces α_i son todas distintas entre sí. En efecto, tenemos que

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

por lo que $P'(\alpha_i) \neq 0$ para todo $1 \leq i \leq p^n$ y por ende toda raíz es de multiplicidad 1. Esto nos dice que K contiene ya p^n elementos al menos. Debemos probar pues que no contiene ningún otro.

Como K es un cuerpo de descomposición, sabemos que es el cuerpo más pequeño que contiene a los α_i. Bastará con probar entonces que el conjunto de los α_i, es decir, el conjunto $L = \{x \in \bar{F}_p \mid P(x) = 0\}$ es ya un subcuerpo de $\bar{F}_p$. Ahora, la Proposición 1.1.6 nos dice que este conjunto es un subcuerpo si y solo si

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

Sean entonces $x, y \in L$, es decir, $P(x) = P(y) = 0$. Tenemos que

$$(x - y)^{p^n} = \sum_{k=0}^{p^n} \binom{p^n}{k} x^k (-y)^{p^n - k},$$

pero claramente $p \mid \binom{p^n}{k}$ si $1 \leq k \leq p^n - 1$, por lo que

$$(x - y)^{p^n} = x^{p^n} + (-y)^{p^n} = x^{p^n} - y^{p^n},$$

ya que si $(-1)^{p^n} = -1$ si p es impar y si $p = 2$ entonces $1 = -1 \in L$. Vemos entonces finalmente que

$$P(x - y) = (x - y)^{p^n} - (x - y) = x^{p^n} - x - (y^{p^n} - y) = P(x) - P(y) = 0,$$

por lo que $x - y \in L$. Por otra parte, si $x, y \neq 0$, tenemos que

$$(xy^{-1})^{p^n} = x^{p^n}(y^{p^n})^{-1} = xy^{-1},$$

ya que $x^{p^n} = x$ e $y^{p^n} = y$. Entonces claramente $P(xy^{-1}) = (xy^{-1})^{p^n} - xy^{-1} = 0$, lo que prueba que $xy^{-1} \in L$.

Probemos finalmente la unicidad. Sea M un cuerpo de cardinal p^n. Como todo cuerpo es un espacio vectorial sobre su cuerpo primo, vemos que el cuerpo primo de M tiene que ser $\mathbb{F}_p$ y por ende M contiene a $\mathbb{F}_p$. Ahora, el grupo M^* tiene orden $p^n - 1$ y por ende $x^{p^n-1} = 1$ para todo $x \in M^*$. Multiplicando por x tenemos que $x^{p^n} = x$ para todo $x \in M^*$. Y como claramente esto también es cierto para $0 \in M$, vemos que para todo elemento de M, $P(x) = 0$ y por ende M contiene al cuerpo de descomposición de P, que es del mismo cardinal. La unicidad del cuerpo de descomposición (Teorema 1.4.9) concluye la demostración. □

Observación.
Si $q = p^n$, entonces el cuerpo de descomposición de $P(x) = x^{q^r} - x \in \mathbb{F}_q[x]$ es $\mathbb{F}_{q^r}$.

Teorema 1.7.2 (Conteo de polinomios irreducibles)**.** *El número $M(n, q)$ de polinomios mónicos irreducibles de grado n en $\mathbb{F}_q[x]$ está dado por la siguiente fórmula descubierta por Gauß:*

$$M(n, q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

donde μ es la función de Möbius definida por

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n \text{ es producto de } k \text{ primos distintos} \\ 0 & \text{si } n \text{ es divisible por el cuadrado de algún primo} \end{cases}$$

Demostración. Recordemos que $x^{q^n} - x$ es el producto de todos los polinomios mónicos irreducibles cuyo grado divide a n de manera que

$$q^n = \sum_{d|n} dM(n, q)$$

Usando la fórmula de inversión de Möbius con $f(n) = M(n, q)$ y $g(n) = nq^n$, llegamos al resultado propuesto. □

En clase esbozamos una demostración diferente, sin usar la fórmula de inversión de Möbius y le invitamos a escribirla en detalle.

Lema 1.7.3 (Fórmula de inversión de Möbius)**.** *Si f y g son funciones definidas en todos los números naturales que satisfacen la relación*

$$f(n) = \sum_{d|n} g(d)$$

entonces también se cumple

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

Demostración. Demostremos primero que

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

Si $n = 1$ no hay más que demostrar. Si $n = p^k m$, con $k > 0$ y m relativamente primo con p, entonces podemos agrupar los divisores de n según la potencia de p que los divida.

$$\sum_{d|n} \mu(d) = \sum_{j=0}^{k} \sum_{d'|m} \mu(p^j d') = \sum_{d'|m} \mu(d') - \sum_{d'|m} \mu(d') = 0$$

Para la fórmula que sigue usaremos que $c \mid \frac{n}{d} \Leftrightarrow d \mid \frac{n}{c}$

$$\begin{aligned} \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) g(c) \\ &= \sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d) g(c) \\ &= g(n) \end{aligned}$$

□

1.8. Interludio 2: Construcciones con regla y compás y números constructibles

La teoría de cuerpos tiene como aplicación inesperada la solución (negativa) a tres clásicos problemas de la matemática griega clśica:

1. *El problema de Delfos: la duplicación del cubo:* Construir, con la ayuda de una regla y un compás, un cubo cuyo volumen sea exactamente el doble del de un cubo dado.

2. *La trisección del ángulo:* Construir, con la ayuda de una regla y un compás, un ángulo equivalente al tercio de un ángulo dado.

3. *La cuadratura del círculo:* Construir, con la ayuda de una regla y un compás, un cuadrado con la misma área que la de un círculo dado.

Recordemos que por "regla", se entiende un objeto que nos permite trazar una recta tan larga como sea posible que pasa por dos puntos dados. Pero un tal objeto no tiene graduación alguna, por lo que no se puede usar para "medir" distancias. Para esto se usa el compás, que nos permite copiar distancias de un lado a otro, así como construir círculos cuyo radio corresponde a la distancia entre dos puntos dados.

Para atacar tales problemas, necesitamos pues al menos dos puntos en el plano, los cuales asimilaremos a los puntos $P_0 := (0,0)$ y $P_1 := (1,0)$ del plano cartesiano $\mathbb{R}^2$. A partir de éstos, veremos cuales son los puntos del plano que podemos construir, lo que nos lleva a al siguiente definición:

Definición 1.8.1. Sea $\mathcal{C}$ un conjunto de puntos en el plano. Decimos que una recta es *constructible a partir de* $\mathcal{C}$ si ésta pasa por al menos dos puntos de $\mathcal{C}$. Decimos que un círculo es *constructible a partir de* $\mathcal{C}$ si su centro corresponde a un punto de $\mathcal{C}$ y su radio corresponde a la distancia entre dos puntos de $\mathcal{C}$.

Decimos que un punto P del plano es *constructible* si existe una sucesión de puntos $P_2, P_3, \ldots, P_n = P$ tal que, si llamamos $\mathcal{C}_m$ el conjunto $\{P_0, P_1, \ldots, P_m\}$ para todo $1 \leq m < n$, el punto P_{m+1} corresponde a una de las siguientes opciones:

- la intersección de dos rectas constructibles a partir de $\mathcal{C}_m$;
- la intersección de una recta y un círculo constructibles a partir de $\mathcal{C}_m$;
- la intersección de dos círculos constructibles a partir de $\mathcal{C}_m$.

Decimos que un número real es *constructible* si éste corresponde a una de las coordenadas (x, y) de un punto constructible.

Ejercicio. Pruebe que $P = (0,1)$ es constructible.

Ejercicio. Pruebe que, dados tres puntos P, Q, R, la recta paralela y la recta perpendicular a $\overline{PQ}$ que pasan por R son constructibles a partir de $\{P, Q, R\}$.

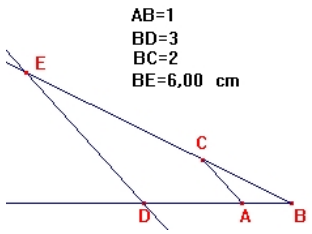
Pruebe que el punto medio del segmento $\overline{PQ}$ y la simetral del mismo son constructibles.

Dada esta definición, recordemos como la geometría puede ser puesta en relación con las operaciones aritméticas clásicas que encontramos en teoría de cuerpos. He aquí las primeras frases del célebre texto *La Geometría* de René Descartes:

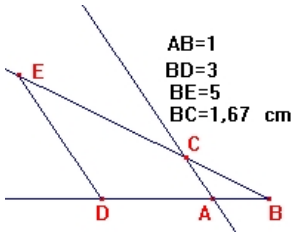
Todos los problemas de Geometría pueden reducirse fácilmente a tales términos, que no es necesario conocer de antemano más que la longitud de algunas líneas rectas para construirlos.

Y así como la aritmética no comprende más que cuatro o cinco operaciones, que son la adición, la sustracción, la multiplicación, la división y la extracción de raíces, que pueden tomarse como una especie de división, así también no hay otra cosa que hacer en geometría, respecto a las líneas que se buscan, para prepararlas a ser conocidas, que agregarles o quitarles otras, o bien, teniendo una, que llamaré la unidad para relacionarla lo más posible con los números, y que ordinariamente puede ser tomada a discreción, y teniendo luego otras dos, encontrar una cuarta que sea a una de esas dos, como la otra es a la unidad, que es lo mismo que la multiplicación; o bien encontrar una cuarta que sea a una de esas dos como la unidad es a la otra, lo que es lo mismo que la división; o, en fin, encontrar una, dos, o varias medias proporcionales entre la unidad y alguna otra línea, lo que es lo mismo que extraer la raíz cuadrada, o cúbica, etc. Y yo no temeré introducir estos términos de aritmética en la geometría, a fin de hacerme más inteligible.

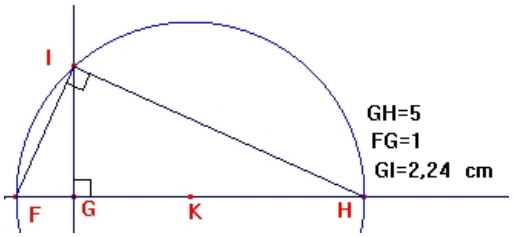
En términos mas inteligibles, Descartes nos dice que en geometría tenemos construcciones equivalentes a la suma y resta (esto es fácil de ver), pero también a la multiplicación y la división, ¡e incluso la extracción de raíces cuadradas! Basta con fijar un largo que equivaldría al número 1, el cual Descartes llama "unidad". He aquí algunos ejemplos:



Multiplicación de 2 por 3



División de 5 por 3



Extracción de la raíz cuadrada de 5

Ejercicio. Explique por qué estas figuras representan realmente la multiplicación, división y la extracción de raíces cuadradas y porqué son constructibles.

Esto nos demuestra inmediatamente lo siguiente:

Proposición 1.8.2. *El conjunto C de los números constructibles es un subcuerpo de $\mathbb{R}$ cerrado por raíces cuadradas. Es decir, para todo $x \in C$ tal que $\sqrt{x} \in \mathbb{R}$, tenemos que $\sqrt{x} \in C$.*

Demostración. En efecto, las operaciones de Descartes nos dicen inmediatamente que podemos sumar, restar, multiplicar y dividir distancias entre puntos constructibles. Ahora, como podemos copiar toda tal distancia al eje de las abscisas gracias al compás, podemos ver que toda tal distancia define un número constructible x vía el punto $(x, 0)$. El subconjunto $C \subset \mathbb{R}$ es entonces un subcuerpo de $\mathbb{R}$.

Para probar que C es además cerrado por raíces cuadradas, basta con ver que la última construcción de acá arriba nos permite construir un segmento de largo $\sqrt{x}$ a partir de un segmento de largo $x \geq 0$, por lo que $x \in C \Rightarrow \sqrt{x} \in C$ si $x \geq 0$, lo que equivale a $\sqrt{x} \in \mathbb{R}$. □

Vista esta proposición, todo lo que tenemos que hacer para resolver los problemas griegos es averiguar lo siguiente:

1. *La duplicación del cubo:* El número $\sqrt[3]{2}$ es constructible?
2. *La trisección del ángulo:* El número $\cos(\frac{\theta}{3})$ es constructible si $\cos(\theta)$ lo es?
3. *La cuadratura del círculo:* El número π es constructible?

En efecto:

1. Para duplicar el volumen de un cubo, basta con multiplicar su lado por $\sqrt[3]{2}$, por lo que este número sería constructible de poderse resolver el problema (y el problema claramente se resuelve si este número es constructible).
2. Todo ángulo que aparece en una construcción geométrica puede ser llevado al eje de las abscisas en $\mathbb{R}^2$ e intersectado con el círculo unitario, dando lugar al punto $(\cos(\theta), \sin(\theta))$. La trisección del ángulo equivale pues a obtener el punto correspondiente al ángulo $\frac{\theta}{3}$.
3. El área de un círculo dado es πr^2, donde r es su radio. Un cuadrado de la misma área tiene entonces un lado igual a $\sqrt{\pi} r$, por lo que debemos construir el número $\sqrt{\pi}$, o bien π, ya que sacar raíces cuadradas es siempre posible en C.

Sin embargo, la Proposición 1.8.2 y las construcciones geométricas de Descartes nos indican que el cuerpo C no es un cuerpo cualquiera y por ende no necesariamente contiene a éstos números. El teorema clave que resuelve todas estas preguntas fue enunciado por Wantzel en 1837 y es el siguiente:

Teorema 1.8.3 (Wantzel)**.** *Sea $t \in \mathbb{R}$. Entonces t es un número constructible si y solo si existe un entero $n \geq 1$ y una sucesión $K_1, K_2, \ldots, K_n$ de subcuerpos de $\mathbb{R}$ tal que:*

- $K_1 = \mathbb{Q}$*;*
- *para todo $1 \leq m < n$, $K_m \subset K_{m+1}$ y $[K_{m+1} : K_m] = 2$;*
- $t \in K_n$*.*

En particular, el cuerpo $C \subset \mathbb{R}$ de los números constructibles corresponde al cuerpo más pequeño de característica 0 cerrado por raíces cuadradas de números positivos.

El corolario que nos será útil para demostrar que los problemas griegos no tienen solución es el siguiente:

Corolario 1.8.4. *Sea $t \in \mathbb{R}$ un número constructible. Entonces $[\mathbb{Q}(t) : \mathbb{Q}] = 2^m$ para algún $m \in \mathbb{N}$.*

Demostración. En efecto, el teorema nos dice que $t \in K_n$ y

$$[K_n : Q] = \prod_{i=1}^{n-1} [K_{i+1} : K_i] = \prod_{i=1}^{n-1} 2 = 2^{n-1}.$$

Ahora, $[\mathbb{Q}(t) : \mathbb{Q}]$ divide a $[K_n : \mathbb{Q}] = 2^{n-1}$ y por ende $[\mathbb{Q}(t) : \mathbb{Q}] = 2^m$ para algún $m \in \mathbb{N}$. □

Ante todo, he aquí un lema geométrico-algebraico que nos ayudará a demostrar el teorema.

Lema 1.8.5. *Sea D una recta $\mathbb{R}^2$ que pasa por los puntos $A = (a_1, a_2)$ y $B = (b_1, b_2)$. Entonces D está dada por una ecuación de la forma $\alpha x + \beta y + \gamma = 0$ con $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2)$.*

De la misma manera, sea C un círculo de $\mathbb{R}^2$ de centro $A = (a_1, a_2)$ et radio igual a la distancia entre los puntos $B = (b_1, b_2)$ y $C = (c_1, c_2)$. Entonces C está dado por una ecuación de la forma $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$ con $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

Demostración. Ejercicio ◡̈ □

Demostración del Teorema de Wantzel. Como t es constructible, sabemos que el punto $P = (t, 0)$ es constructible. Por definición, esto significa que existe una sucesión $P_2, P_3, \ldots . P_n = P$ de puntos de $\mathbb{R}^2$ constructibles cada uno a partir de los precedentes.

Definamos entonces $K_1 = \mathbb{Q}$ y definamos inductivamente el cuerpo K_m para $m \geq 2$ como el cuerpo $K_{m-1}(x_m, y_m)$, donde x_m e y_m son las coordenadas de P_m.

Ahora, el punto P_m corresponde a la intersección de rectas y/o círculos definidos con los puntos P_i con $i < m$. El Lema 1.8.5 nos dice entonces que las ecuaciones que definen estas rectas y/o círculos tienen coeficientes en K_{m-1} ya que $x_i, y_i \in K_{m-1}$ para todo $i < m$. En particular, las coordenadas x_m, y_m del punto P_m verifican uno de los siguientes sistemas de ecuaciones:

$$\begin{aligned} \alpha_1 x_m + \beta_1 y_m + \gamma_1 &= 0, \\ \alpha_2 x_m + \beta_2 y_m + \gamma_2 &= 0, \end{aligned}$$

o bien

$$\begin{aligned} \alpha_1 x_m + \beta_1 y_m + \gamma_1 &= 0, \\ x_m^2 + y_m^2 - 2\alpha_2 x_m - 2\beta_2 y_m + \gamma_2 &= 0, \end{aligned}$$

o bien

$$\begin{aligned} x_m^2 + y_m^2 - 2\alpha_1 x_m - 2\beta_1 y_m + \gamma_1 &= 0, \\ x_m^2 + y_m^2 - 2\alpha_2 x_m - 2\beta_2 y_m + \gamma_2 &= 0, \end{aligned}$$

con $\alpha_i, \beta_i, \gamma_i \in K_{m-1}$. Luego de unos pocos cálculos, vemos que x_m e y_m pertenecen a una misma extensión trivial o cuadrática de K_{m-1}, es decir, $[K_m : K_{m-1}] \in \{1, 2\}$. Salvo eliminar las repeticiones, la sucesión de cuerpos $K_1, K_2, \ldots, K_n$ es entonces la pedida en el enunciado del teorema.

Para demostrar la última afirmación del teorema, sea C' el cuerpo más pequeño de característica 0 cerrado por raíces cuadradas de números positivos. Como $C \supset \mathbb{Q}$ y, según la Proposición 1.8.2, C es cerrado por raíces cuadradas, vemos que $C \supset C'$. Por otra parte, todo elemento $t \in C$ es obtenido a partir de $\mathbb{Q}$ tomando raíces cuadradas gracias a lo que acabamos de demostrar (véase el estudio de las extensiones cuadráticas al final de la sección 1.3). Esto prueba que $C \subset C'$. □

Resolvamos entonces los problemas griegos uno por uno. Comencemos por el problema de Delos.

Proposición 1.8.6. *La duplicación del cubo con regla y compás es imposible.*

Demostración. Visto todo lo que hemos hecho, basta con probar que $\sqrt[3]{2}$ no es un número constructible. Ahora, está claro que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, por lo que el Corolario 1.8.4 nos dice que $\sqrt[3]{2}$ no es constructible. □

Proposición 1.8.7. *La trisección del ángulo con regla y compás es imposible.*

Demostración. Basta con demostrar la imposibilidad para un ángulo constructible dado. Consideremos el ángulo $\theta = 60°$, el cual es claramente constructible. La igualdad trigonométrica clásica

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta),$$

nos dice que $\cos(20°)$ es una raíz de la ecuación

$$4x^3 - 3x - \frac{1}{2} = 0,$$

la cual no tiene raíces en $\mathbb{Q}$, por lo que $[\mathbb{Q}(\cos(20°)) : \mathbb{Q}] = 3$ y por lo tanto $\cos(20°)$ no es constructible. Esto implica que la trisección de $60°$ con regla y compás es imposible. □

Proposición 1.8.8. *La cuadratura del círculo con regla y compás es imposible.*

Demostración. Visto todo lo que hemos hecho, basta con probar que π no es un número constructible. Ahora, el Teorema de Wantzel nos dice en particular que todo número constructible es algebraico sobre $\mathbb{Q}$. Pero π es trascendente sobre $\mathbb{Q}$ (lo cual no demostraremos aquí), por lo que no puede ser constructible. □

Observación.
El teorema de Wantzel sirve también para atacar otro problema geométrico clásico: la construcción con regla y compás de un n-ágono regular para $n \in \mathbb{N}$. Esta aplicación necesita sin embargo un poco de teoría de Galois en cuerpos ciclotómicos, por lo que la dejaremos para más adelante.

1.9. Interludio 3: Cuerpos y polinomios ciclotómicos

En la sección 1.4 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 1.9.1. 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

$$\Phi_n(x) := \prod_{\substack{0 \le a \le n-1 \\ (a,n)=1}} (x - \zeta_n^a).$$

En particular, $\deg(\Phi_n) = \varphi(n)$, donde φ es la función de Euler.

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 1.9.2. *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 1.9.2, 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 1.9.3. *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 1.9.2, ya sabemos que

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

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 $\mathbb{Z}[x]$. Recordemos ahora un resultado importante del curso Grupos y Anillos:

Lema 1.9.4 (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 $R[x]$.*

Usando este lema, 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 1.9.2 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 1.9.5. *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 1.3.3 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 $\deg(P) \leq \deg(\Phi_n) = \varphi(n)$. Esto prueba que $\bar{Q}$ es constante, contradiciendo nuestra hipótesis inicial sobre la reducibilidad de Φ_n, lo que prueba que es irreducible. □

Corolario 1.9.6. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Demostración. En efecto, dada la Proposición anterior, vemos gracias a Proposición 1.3.3 que $\Phi_n = m_{\zeta_n, \mathbb{Q}}$. El Teorema 1.3.8 nos dice entonces que $[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ es igual a $\deg(\Phi_n) = \varphi(n)$. □

2. 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.

2.1. El grupo de automorfismos de un cuerpo

El objeto crucial que consideraremos es el siguiente:

Definición 2.1.1. 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. 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 2.1.2. *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 2.1.3. 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 2.1.2, 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 2.1.2, 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 2.1.2 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 1.2.11 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. 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. 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 2.1.2, el cual nos será útil más adelante.

Lema 2.1.4. *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 2.1.2 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 1.4.9 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 2.1.5. *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 1.2.11 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 2.1.6. *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.*

2.2. 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 2.2.1. 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.

Ejemplo 2.2.2. 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 2.2.3 (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 2.1.6 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 1.2.11, 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 2.2.4. 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. ¿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. Encuentre el cuerpo de descomposición y el grupo de Galois del polinomio $P \in \mathbb{Q}(i)[x]$ dado por $P(x) = x^3 - 2x + 1$. ¿A qué grupo es isomorfo? *Hint: Verifique que el discriminante del polinomio es un cuadrado en* $\mathbb{Q}(i)$ *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 2.2.5. *Sea K un cuerpo, sea $G = \mathrm{Aut}(K)$ y sea H un subgrupo de G. Entonces el subconjunto $\mathrm{Fix}(H) \subset K$ dado por*

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

es un subcuerpo de K.

Definición 2.2.6. El subcuerpo dado por la proposición anterior se llama el *cuerpo de los invariantes* o *cuerpo fijo* de H y se denota por K^H.

Demostración. Siguiendo la Proposición 1.1.6, 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 $\sigma \in H \subset \mathrm{Aut}(K)$ 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 $xy^{-1} \in \mathrm{Fix}(H)$.

□

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

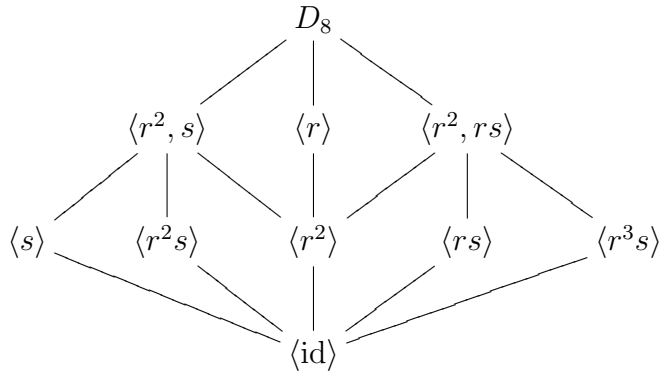
Demostración. Ya vimos a modo de ejercicio que ambos grupos son subgrupos de $\mathrm{Aut}(M)$, por lo que bastará con notar que $\mathrm{Aut}(M/L) \subset \mathrm{Aut}(M/K)$. Ahora, esto es evidente ya que un automorfismo que fija a L forzosamente fija a $K \subset L$. □

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. 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 2.2.8. 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 $\mathrm{Aut}(K/\mathbb{Q})$:

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

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

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

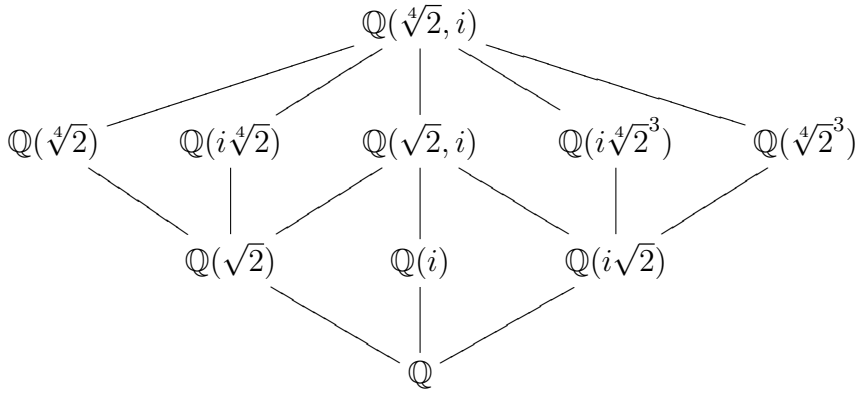
(para convencerse de esto, basta con notar que los 4 reales son una $\mathbb{Q}(i)$-base de K) y que r y s corresponden en esta base respectivamente a las matrices

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

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:

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

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



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

Ejercicio. 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?

2.3. 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 2.3.1 (Teorema Fundamental de la Teoría de Galois)**.** *Sea L/K una extensión galosiana 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*

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

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

Si G es un grupo de orden n (n pudiendo ser infinito), entonces podemos ver 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 ξ puede ser visto entonces como un elemento particular de V_G.

Proposición 2.3.3. *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.
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 2.3.4. *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 2.3.1.

Teorema 2.3.5. *Sea L un cuerpo, G un subgrupo finito de $\mathrm{Aut}(L)$ y sea $K = L^G$. Entonces $[L : K] = |G|$.*

Demostración. Sea $m = [L : K]$ y supongamos por el contrario que $n \neq m$. Demostraremos que esto nos lleva a una contradicción. Recordemos que los elementos de G pueden ser vistos como incrustaciones $\sigma : L \to L$, por lo que los denotaremos $\{\sigma_1, \ldots, \sigma_n\}$.

Supongamos entonces primero que $n > m$. Sabemos entonces que existe una K-base $\{v_1, \ldots, v_m\} \in L$. Podemos formar entonces un sistema de m ecuaciones con n incógnitas:

$$\begin{aligned}
\sigma_1(v_1)x_1 + \sigma_2(v_1)x_2 + \cdots + \sigma_n(v_1)x_n &= 0;\\
\sigma_1(v_2)x_1 + \sigma_2(v_2)x_2 + \cdots + \sigma_n(v_2)x_n &= 0;\\
&\vdots\\
\sigma_1(v_m)x_1 + \sigma_2(v_m)x_2 + \cdots + \sigma_n(v_m)x_n &= 0.
\end{aligned}$$

Como hay más incógnitas que ecuaciones, sabemos que existe al menos una solución no trivial $\{\beta_1, \ldots, \beta_n\} \in L^n$ a este sistema. Ahora, recordemos que los elementos de G fijan K, es decir $\sigma_i(a) = a$ para todo $a \in K$ y todo $1 \leq i \leq n$. Entonces, si $a_j \in K$ para $1 \leq j \leq m$, podemos multiplicar la primera ecuación por a_1, la segunda por a_2 y así sucesivamente, luego evaluar en los β_i para obtener las igualdades:

$$a_j(\sigma_1(v_j)\beta_1 + \sigma_2(v_j)\beta_2 + \cdots + \sigma_n(v_j)\beta_n) = 0, \quad 1 \leq j \leq m,$$

o bien, como $a_j \in K$,

$$\sigma_1(a_j v_j)\beta_1 + \sigma_2(a_j v_j)\beta_2 + \cdots + \sigma_n(a_j v_j)\beta_n = 0, \quad 1 \leq j \leq m.$$

Sumando estas m igualdades y aplicando la linearidad de los σ_i, obtenemos la igualdad

$$\sigma_1\left(\sum_{j=1}^{m} a_j v_j\right)\beta_1 + \sigma_2\left(\sum_{j=1}^{m} a_j v_j\right)\beta_2 + \cdots + \sigma_n\left(\sum_{j=1}^{m} a_j v_j\right)\beta_n = 0.$$

Ahora, esta igualdad es cierta sin importar los valores que tomen los diversos a_j. Es decir, esta igualdad es cierta *para todo* elemento de la forma $\sum_{j=1}^{m} a_j v_j$. Pero los v_j forman una K-base de L, por lo que tenemos la igualdad

$$\sigma_1(\alpha)\beta_1 + \sigma_2(\alpha)\beta_2 + \cdots + \sigma_n(\alpha)\beta_n = 0,$$

para todo $\alpha \in L$. Esto nos dice que la combinación lineal

$$\beta_1\sigma_1 + \beta_2\sigma_2 + \cdots + \beta_n\sigma_n$$

es trivial en V_{L^*}. El Corolario 2.3.4 nos dice entonces que los β_i son todos nulos, lo que es una contradicción ya que se trata de una solución no trivial del sistema. Esto prueba que $n \leq [L : K]$.

Supongamos ahora que $n < [L : K]$. Esto nos dice que la dimensión de L como K-espacio vectorial es mayor que n, por lo que existen elementos $\alpha_1, \ldots, \alpha_{n+1} \in L$ que son K-linealmente independientes. Consideremos entonces un nuevo sistema de n ecuaciones con $n + 1$ incógnitas:

$$\begin{aligned}
\sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0;\\
\sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \cdots + \sigma_2(\alpha_{n+1})x_{n+1} &= 0;\\
&\vdots\\
\sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0.
\end{aligned}$$

Nuevamente, como hay más incógnitas que ecuaciones, sabemos que existe al menos una solución no trivial $\{\gamma_1, \ldots, \gamma_{n+1}\} \in L^{n+1}$ a este sistema. Notemos además que, para toda tal solución, al menos uno de los γ_i no está en K ya que, de lo contrario, éstos podrían entrar en los σ_j por K-linearidad, de forma de obtener las ecuaciones

$$\sigma_j\left(\sum_{i=1}^{n+1} \gamma_i\alpha_i\right) = 0,$$

lo que implica que $\sum_{i=1}^{n+1} \gamma_i\alpha_i = 0$ y esto contradice la K-independencia lineal de los α_i.

De todas las posibles soluciones $\{\gamma_1, \ldots, \gamma_{n+1}\} \in L^{n+1}$ a este sistema, consideremos una con la mayor cantidad de ceros. Reordenando las incógnitas de ser

necesario, podemos suponer entonces que $\gamma_i \neq 0$ para todo $1 \leq i \leq r$ y $\gamma_i = 0$ para todo $i > r$ con r minimal. Como el sistema es lineal, podemos dividir esta solución por γ_r, de forma de obtener una nueva solución $\{\gamma_1', \ldots, \gamma_{r-1}', 1, 0, \ldots, 0\} \in L^{n+1}$ con $\gamma_i' \neq 0$ para $1 \leq i \leq r-1$. Obtenemos entonces las igualdades

$$\sigma_j(\alpha_1)\gamma_1' + \cdots + \sigma_j(\alpha_{r-1})\gamma_{r-1}' + \sigma_j(\alpha_r) = 0, \quad 1 \leq j \leq n. \tag{1}$$

Y como ya notamos antes, podemos suponer (salvo un nuevo reordenamiento) que $\gamma_1' \notin K$. Esto implica que existe un cierto k para el cual $\sigma_k(\gamma_1') \neq \gamma_1'$. Apliquemos este automorfismo a cada una de las igualdades para obtener

$$\sigma_k\sigma_j(\alpha_1)\sigma_k(\gamma_1') + \cdots + \sigma_k\sigma_j(\alpha_{r-1})\sigma_k(\gamma_{r-1}') + \sigma_k\sigma_j(\alpha_r) = 0, \quad 1 \leq j \leq n.$$

Pero como G es un grupo, sabemos que el conjunto $\{\sigma_k\sigma_j \mid 1 \leq j \leq n\}$ es simplemente el conjunto G nuevamente, por lo que estas n ecuaciones corresponden salvo reordenamiento al conjunto de ecuaciones

$$\sigma_j(\alpha_1)\sigma_k(\gamma_1') + \cdots + \sigma_j(\alpha_{r-1})\sigma_k(\gamma_{r-1}') + \sigma_j(\alpha_r) = 0, \quad 1 \leq j \leq n. \tag{2}$$

Restando las igualdades en (1) y aquéllas en (2), obtenemos finalmente las igualdades

$$\sigma_j(\alpha_1)[\sigma_k(\gamma_1') - \gamma_1'] + \cdots + \sigma_j(\alpha_{r-1})[\sigma_k(\gamma_{r-1}') - \gamma_{r-1'}] = 0, \quad 1 \leq j \leq n,$$

lo que corresponde a una nueva solución $\{\sigma_k(\gamma_1') - \gamma_1', \ldots, \sigma_k(\gamma_{r-1}') - \gamma_{r-1'}, 0, 0, \ldots, 0\} \in L^{n+1}$ del sistema inicial. Se trata de una solución no trivial ya que $\sigma_k(\gamma_1') - \gamma_1' \neq 0$ y sin embargo es una solución con más ceros que la anterior, lo que contradice la minimalidad de r. Esto nos permite concluir que $n = m = [L : K]$ □

El primer corolario que podemos deducir de este resultado es una generalización del Corolario 2.1.6.

Corolario 2.3.6. *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 2.1.4 nos dice que $\mathrm{Aut}(L/K)$ es un subgrupo finito de $\mathrm{Aut}(L)$. Podemos entonces aplicar el Teorema 2.3.5, 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 2.3.7. *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 2.3.5 nos dice que $[L : K] = |G|$, mientras que el Corolario 2.3.6 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 2.3.8. *Sea L un cuerpo y sean $G_1 \neq G_2$ subgrupos finitos de* $\mathrm{Aut}(L)$. *Entonces* $L^{G_1} \neq L^{G_2}$.

Demostración. Supongamos por contradicción que $L^{G_1} = L^{G_2}$. El Corolario 2.3.7 nos dice entonces que

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

lo que contradice nuestra hipótesis. □

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* (de la cual no hemos hablado, pero con la cual hemos jugado en ayudantía).

Teorema 2.3.9 (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.*

Observación.
Una extensión L/K es *normal* si verifica el enunciado número 1. Ya probamos en ayudantía que una tal extensión corresponde al cuerpo de descomposición de algún polinomio $P \in K[x]$.

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 $|\mathrm{Aut}(L/K)| = [L : K]$.

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 2.1.4) y notemos que $K = L^G$ por el Corolario 2.3.7. 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 2.1.2 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

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

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 2.1.6 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). Sea $\alpha_1, \ldots, \alpha_n$ una K-base de L y sea $P_i := m_{\alpha_i,K} \in K[x]$ el polinomio minimal respectivo para $1 \leq i \leq n$. Notemos entonces que, por lo que acabamos de demostrar, los polinomios P_i son separables y todas sus raíces están en L.

Definamos pues $P \in K[x]$ como el producto de los P_i *sin repeticiones*, es decir, si dos P_i son iguales, solo consideramos una copia de éste. Entonces todas las raíces de P son distintas, ya que se trata de un producto de polinomios separables, irreducibles, mónicos y distintos entre sí. Además, todas ellas están en L y por ende L es el cuerpo de descomposición del polinomio separable P, ya que se encuentra generado por sus raíces. □

Ya tenemos entonces todo lo necesario para demostrar el Teorema 2.3.1, cuyo enunciado reescribimos aquí:

Teorema (Teorema Fundamental de la Teoría de Galois)**.** *Sea L/K una extensión galosiana 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*

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

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 $[M' : M] = [H : H']$.

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

Demostremos que la aplicación φ_2 es biyectiva: La inyectividad corresponde precisamente al Corolario 2.3.8. Para verificar la epiyectividad, consideremos un subcuerpo $K \subset M \subset L$. Como L/K es de Galois, sabemos que se trata del cuerpo de descomposición de un polinomio separable $P \in K[x]$. Ahora, podemos mirar este polinomio como un elemento de $M[x]$, en cuyo caso L/M es claramente el cuerpo de descomposición de $P \in M[x]$. Esto nos dice que L/M es galoisiana y por ende $M = \mathrm{Fix}(\mathrm{Aut}(L/M))$ dadas las caracterizaciones obtenidas más arriba. Ahora, claramente $H = \mathrm{Aut}(L/M)$ es un subgrupo de $G = \mathrm{Aut}(L/K)$, por lo que $M = \varphi_2(H)$, lo que prueba la epiyectividad.

Notemos ahora que el argumento anterior nos prueba además que $\varphi_2 \circ \varphi_1 = \mathrm{id}_{\mathcal{C}}$ ya que es justamente $H = \mathrm{Aut}(L/M) = \varphi_1(M)$ el subgrupo que usamos. Por otra parte, el Corolario 2.3.7 prueba precisamente que $\varphi_1 \circ \varphi_2 = \mathrm{id}_{\mathcal{G}}$.

Esto prueba que φ_1 y φ_2 son funciones inversas una de la otra. La afirmación sobre la inversión de las inclusiones se deduce inmediatamente del Lema 2.2.7 y del ejercicio que se encuentra justo después.

Finalmente, si $M \subset M' \in \mathcal{C}$ corresponden respectivamente a $H \geq H' \in \mathcal{G}$, 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 2.3.10. *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 2.3.11. *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 2.3.6 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 2.1.2. 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 $(ghg^{-1})|_M = \mathrm{id}_M$ (nótese que $(g^{-1hg})|_K = \mathrm{id}_K$ ya que $g^{-1}hg \in G = \mathrm{Aut}(L/K)$). 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 $H \lhd G$. □

Proposición 2.3.12. *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'.

Demostración. Está claro que $M \cap M' = L^H \cap L^{H'}$ corresponde a los elementos que son simultáneamente fijados por H y H', es decir, $M \cap M' = L^{H \cup H'}$. Probemos entonces que $L^{H \cup H'} = L^{\langle H, H' \rangle}$, en cuyo caso el Teorema Fundamental nos dice que se trata en particular de un subcuerpo de L ya que $\langle H, H' \rangle$ es un subgrupo de G. Como $H \cup H' \subset \langle H, H' \rangle$, vemos inmediatamente que $L^{H \cup H'} \supset L^{\langle H, H' \rangle}$. Ahora, sea $x \in L^{H \cup H'}$ y $g \in \langle H, H' \rangle$. Entonces existen $h_1, \dots h_n \in H$ y $h'_1, \dots, h'_n \in H'$ tales que $g = h_1 h'_1 \cdots h_n h'_n$. Vemos entonces que:

$$\begin{aligned} g(x) = (h_1 h'_1 \cdots h_n h'_n)(x) = (h_1 h'_1 \cdots h'_{n-1} h_n)(h'_n(x)) = (h_1 h'_1 \cdots h'_{n-1} h_n)(x) \\ = (h_1 h'_1 \cdots h_{n-1} h'_{n-1})(h_n(x)) = (h_1 h'_1 \cdots h_{n-1} h'_{n-1})(x), \end{aligned}$$

y así sucesivamente hasta ver que $g(x) = x$, lo que prueba que $x \in L^{\langle H, H' \rangle}$ y por ende $L^{H \cup H'} \subset L^{\langle H, H' \rangle}$, lo que concluye la demostración en este caso.

Veamos ahora el composito $MM' \subset L$. Notemos que $H \cap H'$ es un subgrupo de G y por ende le corresponde un subcuerpo $K \subset M_0 \subset L$ el cual contiene a M y M' por el Teorema Fundamental ya que $H \cap H'$ es un subgrupo de H y de H'. Entonces $MM' \subset M_0$ por definición del composito. Sea ahora H_0 el subgrupo de G que corresponde a MM'. Entonces los elementos de H_0 fijan a MM' y por ende fijan en particular a M y a M'. El Teorema Fundamental nos dice entonces que los elementos de H_0 están contenidos en H y en H', es decir, $H_0 \subset H \cap H'$. Una última aplicación del Teorema Fundamental nos dice entonces que $MM' \supset M_0$, lo que prueba la igualdad de estos dos cuerpos y por ende $H \cap H'$ es el grupo que corresponde a MM'. □

Para una respuesta completa del siguiente ejercicio (que haremos juntos en clases), véase las páginas 577–581 del Dummit-Foote.

Ejercicio. 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. 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. 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.

2.4. 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 2.4.1. 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 2.4.2 (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 2.4.3 (Teorema de Galois)**.** *Un polinomio $P \in K[x]$ es soluble por radicales si y solo si su grupo de Galois asociado es soluble.*

Sea dicho de paso, 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.

2.4.1. Extensiones de Kummer y Artin-Schreier

Empezaremos nuestro estudio de las ecuaciones solubles por radicales con el ejemplo más básico: las extensiones por radicales simples. Se trata de las extensiones L/K obtenidas agregando a K una raíz n-ésima de un elemento $a \in K$, es decir, $L = \sqrt[n]{a}$. Tales extensiones son llamadas *extensiones de Kummer*. Para cuerpos de característica p, las extensiones de Kummer presuponen que n es primo a p. Aquéllas de la forma $L = K(\sqrt[p]{a})$ son, como ya lo hemos visto, extensiones inseparables, por lo que escapan a la Teoría de Galois y no nos interesan pues en este marco (sobre todo porque no hay ambigüedad alguna en este caso).

Un ejemplo análogo en característica p a las extensiones de Kummer de grado p, pero que sí es separable, son las llamadas *extensiones de Artin-Schreier*. Se trata de extensiones de la forma $L = K(\alpha)$, donde α es una raíz del polinomio $x^p - x - a$ con $a \in K$.

Comencemos pues con una definición

Definición 2.4.4. Una extensión L/K se dice *abeliana* (resp. *cíclica*) si es galoisiana y $\mathrm{Gal}(L/K)$ es un grupo abeliano (resp. cíclico).

Proposición 2.4.5. *Sea K un cuerpo que contiene todas las raíces n-ésimas de la unidad y tal que* $\mathrm{car}(K)$ *no divide a n. Sea $a \in K$ y $L = K(\sqrt[n]{a})$. Entonces L/K es una extensión cíclica de grado un divisor de n.*

Demostración. Sea $\alpha = \sqrt[n]{a}$. Como K contiene todas las raíces n-ésimas de la unidad, tenemos que L es el cuerpo de descomposición del polinomio $x^n - a \in K[x]$. En efecto, las raíces de este polinomio son $\zeta\alpha$ con $\zeta \in \mu_n$, las cuales se encuentran

claramente en L ya que $\mu_n \subset K \subset L$ y $\alpha \in L$. Nótese además que todas estas raíces son distintas entre sí ya que $\zeta_n \neq 1$ dada la hipótesis sobre $\mathrm{car}(K)$. Esto nos dice que L/K es galoisiana.

Sea ahora $\sigma \in G = \mathrm{Gal}(L/K)$. Entonces $\sigma(\alpha)$ es otra raíz de $x^n - a$, por lo que $\sigma(\alpha) = \zeta_\sigma \alpha$, donde $\zeta_\sigma \in \mu_n$. Como α genera la extensión L/K, sabemos que dos elementos $\sigma, \tau \in G$ tales que $\zeta_\sigma = \zeta_\tau$ son iguales. Tenemos entonces una inyección:

$$\begin{aligned} \varphi : G &\hookrightarrow \mu_n, \\ \sigma &\mapsto \zeta_\sigma, \end{aligned}$$

la cual es además un homomorfismo de grupos. En efecto, para $\sigma, \tau \in G$ tenemos que, como $\zeta_\tau \in \mu_n \subset K$,

$$\zeta_{\sigma\tau}\alpha = (\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\zeta_\tau \alpha) = \zeta_\tau \sigma(\alpha) = \zeta_\tau \zeta_\sigma \alpha,$$

lo que prueba que $\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau$ (recuerde que la multiplicación en L es conmutativa). Esto prueba que G es isomorfo a un subgrupo de $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$, por lo que se trata de un grupo cíclico de orden un divisor de n. En particular, el grado de L/K es igual al orden de G y por ende un divisor de n. □

Si llamamos *extensiones de Kummer* a estas extensiones cíclicas, es porque fue él quien las estudió y demostró en particular el resultado siguiente, el cual corresponde a la recíproca de la proposición anterior.

Proposición 2.4.6. *Sea K un cuerpo que contiene todas las raíces n-ésimas de la unidad y tal que* $\mathrm{car}(K)$ *no divide a n. Sea L/K una extensión cíclica de grado un divisor de n. Entonces L/K es una extensión de Kummer, es decir, $L = K(\sqrt[n]{a})$ con $a \in K$.*

Demostración. Sea $\sigma \in G = \mathrm{Gal}(L/K)$ un generador de G. Sabemos entonces en particular que $\sigma^n = \mathrm{id}_L$. Para $\alpha \in L$ y $\zeta \in \mu_n$, definamos el *resolvente de Lagrange* como

$$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha) \in L.$$

Al aplicar σ al elemento (α, ζ) queda

$$\begin{aligned} \sigma(\alpha, \zeta) &= \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-2}\sigma^{n-1}(\alpha) + \zeta^{n-1}\sigma^n(\alpha) \\ &= \zeta^{n-1}\alpha + \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-2}\sigma^{n-1}(\alpha) \\ &= \zeta^{-1}(\alpha, \zeta). \end{aligned}$$

De esto deducimos rápidamente iterando que $\sigma^i(\alpha, \zeta) = \zeta^{-i}(\alpha, \zeta)$. En particular, vemos también que

$$\sigma((\alpha, \zeta)^n) = \sigma(\alpha, \zeta)^n = \zeta^{-n}(\alpha, \zeta)^n = (\alpha, \zeta)^n,$$

por lo que $(\alpha,\zeta)^n \in L^{\langle\sigma\rangle} = L^G = K$.

Sea ahora ζ_n una raíz primitiva n-ésima de la unidad. Como $\mathrm{id}, \sigma, \ldots, \sigma^{n-1} \in G$ son L-linealmente independientes como caracteres en V_{L^*}, la mera definición del resolvente de Lagrange nos dice que existe un $\alpha \in L$ tal que $(\alpha,\zeta_n) \neq 0$. Y dado que $\sigma^i(\alpha,\zeta_n) = \zeta_n^{-i}(\alpha,\zeta_n)$, vemos que σ^i no fija (α,ζ_n) para $i < n$. Esto nos dice que el subgrupo de G correspondiente a $K((\alpha,\zeta_n))/K$ por el Teorema Fundamental es el grupo trivial, por lo que $L = K((\alpha,\zeta_n))$. Pero como ya vimos que $(\alpha,\zeta_n)^n \in K$, tenemos que $L = K(\sqrt[n]{a})$ con $a = (\alpha,\zeta_n)^n \in K$. □

Veamos ahora el caso de las extensiones cíclicas de grado p en cuerpos de característica p.

Proposición 2.4.7 (Extensiones de Artin-Schreier)**.** *Sea K un cuerpo de característica p y sea L/K una extensión cíclica de grado p. Entonces $L = K(\alpha)$, donde α es una raíz de del polinomio $x^p - x - a$ para algún $a \in K$. Además, toda extensión no trivial de este tipo es cíclica de grado p.*

Demostración. Comencemos por la última afirmación. Sea $a \in K$ y sea $P \in K[x]$ el polinomio dado por $P(x) = x^p - x - a$. Supongamos que P no tiene raíces en K y notemos que, si α es una raíz de P, entonces $\alpha + \ell$ es también una raíz de P para $\ell \in \mathbb{F}_p$ (recuerde que todo cuerpo de característica p contiene a $\mathbb{F}_p$). Vemos entonces que L es el cuerpo de descomposición del polinomio separable P (su derivada es 1) y por ende L/K es galoisiana.

Sea ahora $\sigma \in G = \mathrm{Gal}(L/K)$. Entonces $\sigma(\alpha)$ es otra raíz de P, por lo que $\sigma(\alpha) = \alpha + \ell_\sigma$ con $\ell_\sigma \in \mathbb{F}_p$. Como α genera la extensión L/K, sabemos que dos elementos $\sigma, \tau \in G$ tales que $\ell_\sigma = \ell_\tau$ son iguales. Tenemos entonces una inyección:

$$\begin{aligned} \varphi : G &\hookrightarrow \mathbb{F}_p, \\ \sigma &\mapsto \ell_\sigma, \end{aligned}$$

la cual es además un homomorfismo de grupos (donde $\mathbb{F}_p$ es un grupo aditivo). En efecto, para $\sigma, \tau \in G$ tenemos que, como $\ell_\tau \in \mathbb{F}_p \subset K$,

$$\alpha + \ell_{\sigma\tau} = (\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha + \ell_\tau) = \sigma(\alpha) + \ell_\tau = \alpha + \ell_\sigma + \ell_\tau,$$

lo que prueba que $\ell_{\sigma\tau} = \ell_\sigma + \ell_\tau$. Esto prueba que G es isomorfo a un subgrupo de $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$, por lo que se trata de un grupo cíclico de orden un divisor de p. Y como asumimos que la extensión era no trivial, tenemos que se trata de una extensión cíclica de grado p.

Sea ahora L/K una extensión cíclica de grado p y sea σ un generador de $\mathrm{Gal}(L/K)$. Entonces los elementos $1, \sigma, \ldots, \sigma^{p-1} \in \mathrm{Gal}(L/K)$ son todos distintos entre sí e inducen caracteres distintos entre sí. Y como los caracteres son L-linealmente independientes en V_{L^*}, existe un elemento $\theta \in L$ tal que $\theta + \sigma(\theta) +$

$\cdots + \sigma^{p-1}(\theta) \neq 0$. Nótese que este elemento es claramente fijo por σ. Consideremos entonces el elemento

$$\alpha := -\frac{\sigma(\theta) + 2\sigma^2(\theta) + \cdots + (p-1)\sigma^{p-1}(\theta)}{\theta + \sigma(\theta) + \cdots + \sigma^{p-1}(\theta)} \in L.$$

Vemos entonces que

$$\sigma(\alpha) = -\frac{(p-1)\theta + \sigma^2(\theta) + 2\sigma^3(\theta) + \cdots + (p-2)\sigma^{p-1}(\theta)}{\theta + \sigma(\theta) + \cdots + \sigma^{p-1}(\theta)},$$

y por lo tanto, recordando que $p - 1 = -1$ ya que estamos en característica p,

$$\alpha - \sigma(\alpha) = -\frac{\theta + \sigma(\theta) + \cdots + \sigma^{p-1}(\theta)}{\theta + \sigma(\theta) + \cdots + \sigma^{p-1}(\theta)} = -1,$$

o en otras palabras, $\sigma(\alpha) = \alpha + 1$. Esto prueba que $\alpha \notin K$ y por ende $L = K(\alpha)$ ya que el grado $[L : K(\alpha)]$ divide a p y no es igual a 1. Por inducción, obtenemos también inmediatamente que $\sigma^i(\alpha) = \alpha + i$. Definamos $a \in K$ como el producto $a := \prod_{i=0}^{p-1} \sigma^i(\alpha)$. Nótese que realmente está en K ya que es fijo por σ (y por ende por todo $\mathrm{Gal}(L/K)$). Vemos entonces que

$$a = \prod_{i=0}^{p-1} \sigma^i(\alpha) = \prod_{i=0}^{p-1} (\alpha + i) = \alpha^p - \alpha,$$

lo que prueba que α es raíz del polinomio $x^p - x - a \in K[x]$. □

Ejercicio. Confirme este último cálculo en un cuerpo L de característica p:

$$\prod_{i=0}^{p-1} (\alpha + i) = \alpha^p - \alpha.$$

2.4.2. Solubilidad por radicales

Convención: En lo que sigue, supondremos por simplicidad que los cuerpos con los que trabajamos son todos de característica 0. Históricamente el problema de la solubilidad por radicales iba dirigido a estos cuerpos (y más precisamente a subcuerpos de $\mathbb{C}$). Y si bien la mayor parte de los argumentos se generalizan a característica positiva, esto podría alargar inútilmente los enunciados y demostraciones. En particular, de ahora en adelante, todo polinomio irreducible $P \in K[x]$ es separable.

Comencemos entonces nuestro análisis sobre la solubilidad por radicales de las ecuaciones polinomiales con una nueva definición que explicita aún más esta noción.

Definición 2.4.8. Una extensión L/K es llamada una *extensión radical o por radicales* si existe una cadena de subcuerpos

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = L,$$

tal que $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ con $a_i \in K_i$ para todo $0 \leq i \leq r-1$. O bien, de forma equivalente, $K_{i+1} = K_i(\alpha_i)$ con $\alpha_i^{n_i} \in K_i$ para todo $0 \leq i \leq r-1$.

Observación.
Una extensión por radicales L/K se escribe $L = K(\alpha_1, \ldots, \alpha_r)$, donde $\alpha_1^{n_1} \in K$ y $\alpha_j^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1})$ para $j \geq 2$.

Así, nuestra definición original de un polinomio soluble por radicales puede ser reemplazada por la siguiente definición:

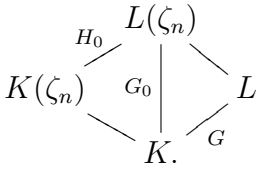
Definición 2.4.9. Un polinomio $P \in K[x]$ es *soluble por radicales* si su cuerpo de descomposición está contenido en una extensión por radicales.

En efecto, las cuatro primeras operaciones básicas están disponibles sobre todo cuerpo, en particular sobre el cuerpo K que contiene a todos los coeficientes de P, y la extracción de raíces corresponde precisamente a una extensión radical simple. El iterar este proceso corresponde a considerar extensiones radicales en toda generalidad.

Recordemos ahora el Teorema 2.4.3, el cual nos da la relación entre la noción de *grupo soluble* y *polinomio soluble por radicales*, demostrada por Galois.

Teorema 2.4.10 (Teorema de Galois)**.** *Un polinomio $P \in K[x]$ es soluble por radicales si y solo si su grupo de Galois asociado es soluble.*

Demostración. Sea L el cuerpo de descomposición del polinomio $P \in K[x]$, sea $G = \mathrm{Gal}(L/K)$ y $n = [L : K]$. Consideremos la extensión $L(\zeta_n)/K$. Se trata del cuerpo de descomposición del polinomio $P \cdot (x^n - 1)$. Si algún factor de P divide a $x^n - 1$, entonces podemos elminarlo y $L(\zeta_n)$ es aún el cuerpo de descomposición del polinomio restante. Como este polinomio es separable, tenemos entonces que $L(\zeta_n)/K$ es una extensión galoisiana cuyo grupo denotamos por G_0. Como $K(\zeta_n)/K$ y L/K son subextensiones galoisianas de $L(\zeta_n)/K$, sabemos que les corresponden subgrupos normales de G_0. Así, tenemos el siguiente diagrama de grupos y cuerpos:



Supongamos primero que G es un grupo soluble. La proyección $\pi : G_0 \to G$ induce por restricción un homomorfismo $H_0 = \mathrm{Gal}(L(\zeta_n)/K(\zeta_n)) \to G$, el cual resulta ser inyectivo. En efecto, la imagen de $\sigma \in H_0 \subset G_0$ no es más que la restricción $\sigma|_L$ (como L/K es de Galois, $\sigma(L) = L$, por lo que tiene sentido esta definición). Y un $\sigma \in H_0$ en el núcleo de este homomorfismo fija tanto a L como a ζ_n (porque $\sigma \in H_0$ fija a $K(\zeta_n)$), por lo que se trata de la identidad. Esto nos dice que H_0 es isomorfo a un subgrupo de G y por ende H_0 es soluble también.

Como H_0 es soluble, existe una cadena de subgrupos $H_i \leq H_0$ para $0 \leq i \leq m$ tales que: $H_m = \{e\}$, $H_i \lhd H_{i-1}$ para todo $1 \leq i \leq m$ y H_{i-1}/H_i es cíclico para todo $1 \leq i \leq m$. Sea K_i el subcuerpo de $L(\zeta_n)$ correspondiente a cada H_i. Entonces K_i/K_{i-1} es una extensión cíclica para cada $1 \leq i \leq m$ y por lo tanto de Kummer por la Proposición 2.4.6. Esto nos dice que $L(\zeta_n)/K(\zeta_n)$ es una extensión radical. Pero como $K(\zeta_n)/K$ también es una extensión radical, vemos que $L(\zeta_n)/K$ es una extensión radical que contiene a L, lo que prueba que P es soluble por radicales.

Supongamos ahora que P es soluble por radicales y demostremos que G es un grupo soluble. Para esto, basta con demostrar que G_0 es soluble, ya que G es un cociente de G_0. Ahora, sabemos que $\mathrm{Gal}(K(\zeta_n)/K) \simeq G_0/H_0$ es abeliano (Ejemplo 2.2.3), por lo que basta con demostrar que el subgrupo H_0 es soluble. Ahora, si $P \in K[x]$ es soluble por radicales, entonces $P \in K(\zeta_n)[x]$ claramente también lo es. Y como $L(\zeta_n)$ es el cuerpo de descomposición en ese caso, vemos que podemos reemplazar L/K por $L(\zeta_n)/K(\zeta_n)$ y G por H_0 para concluir la demostración. Es decir, podemos suponer que $\zeta_n \in K$.

Bajo esta suposición, sea

$$K = K_0 \subset K_1 \subset \cdots \subset K_r,$$

la cadena de subcuerpos tales que $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ con $a_i \in K_i$ para todo $0 \leq i \leq r-1$ y tal que $L \subset K_r$. Como $\zeta_n \in K$, la proposición 2.4.5 nos dice entonces que K_i/K_{i-1} es cíclica para todo $1 \leq i \leq r$. Sea ahora $L_i := K_i \cap L$. Entonces la extensión L_i/L_{i-1} sigue siendo cíclica para todo $1 \leq i \leq r$ (ejercicio). El Teorema Fundamental nos dice entonces que estas extensiones corresponden a subgrupos

$$\{e\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

tales que G_{i-1}/G_i es cíclico, lo que prueba que G es soluble. □

Ejercicio. Demuestre lo pedido al final de la demostración. Más precisamente, demuestre lo siguiente:

Sean L/K una extensión galoisiana, $K \subset M_0 \subset M_1$ extensiones tales que M_1/M_0 es galoisiana y sean $L_i = M_i \cap L$ para $i = 0, 1$. Entonces L_1/L_0 es galoisiana y $\mathrm{Gal}(L_1/L_0)$ es isomorfo a un cociente de $\mathrm{Gal}(M_1/M_0)$.

Un corolario de este gran teorema explica por qué existen fórmulas para los polinomios de grado ≤ 4.

Corolario 2.4.11. *Sea $P \in K[x]$ un polinomio de grado ≤ 4. Entonces P es soluble por radicales.*

Demostración. Sea L el cuerpo de descomposición de P. Sabemos entonces que $\mathrm{Gal}(L/K)$ permuta las raíces de P, por lo que se trata de un subgrupo de S_4 ya que no hay más que 4 raíces a lo más para permutar. Ahora, S_4 es un grupo soluble, como lo demuestra la cadena

$$\{\mathrm{id}\} \lhd K \lhd A_4 \lhd S_4,$$

donde K es el grupo de Klein generado por las dobles transposiciones. Por lo tanto, G es soluble. □

Este corolario claramente no se puede generalizar ya que, a partir de $n = 5$, el grupo S_n no es soluble porque A_n es simple. Sin embargo, esto no siginifica que la solubilidad por radicales sea imposible para polinomios de grado ≥ 5, ya que no sabemos a priori si el grupo de Galois de un polinomio arbitrario es igual a S_n o a A_n. Para esto, necesitamos trabajar un poco más.

Observación.
Al tomar un polinomio "genérico" como

$$P(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + f \in \mathbb{Q}(a, b, c, d, e, f)[x],$$

el grupo de Galois será realmente S_5. Esto es porque la palabra "genérico" quiere decir que no existe ninguna relación algebraica entre los coeficientes a, b, c, d, e, f, o más precisamente que no existe un polinomio de 6 variables con coeficientes en $\mathbb{Q}$ que anule a estos elementos. La consecuencia es que las raíces del polinomio P no están sujetas tampoco a una tal relación y por ende cada una "vive en una extensión algebraica distinta", lo que fuerza al grupo de Galois a ser tan grande como le es posible.

Pero todo esto es muy abstracto, así que bajemos al mundo de los polinomios con coeficientes racionales y demostremos lo siguiente.

Proposición 2.4.12. *Sea $P \in \mathbb{Q}[x]$ un polinomio irreducible de grado p primo y sea K su cuerpo de descomposición. Supongamos que P tiene exactamente dos raíces no reales en $\mathbb{C}$. Entonces $G = \mathrm{Gal}(K/\mathbb{Q})$ es isomorfo a S_p.*

Esta proposición nos dice que existen (¡infinitos!) polinomios irreducibles en $\mathbb{Q}[x]$ cuyo grupo de Galois es S_p, probando la imposibilidad de encontrar una solución por radicales y corroborando así el Teorema de Abel (Teorema 2.4.2).

Demostración. Por hipótesis, P tiene dos raíces complejas y $p-2$ raíces reales. Estas dos raíces complejas deben ser conjugadas ya que el producto y la suma de todas las raíces de P están en $\mathbb{Q}$ (de hecho, corresponden respectivamente a los coeficientes a_0 y a_{p-1} de $P(x) = \sum_{i=0}^{p} a_i x^i$). Entonces el automorfismo $\sigma \in \mathrm{Aut}(\mathbb{C})$ que corresponde a la conjugación compleja permuta las raíces de P (fija las reales e intercambia las complejas) y es por ende un automorfismo de K, es decir, $\sigma \in \mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{Q})$. Esto prueba que, visto como un subgrupo de S_p, G posee una transposición.

Por otra parte, sea α una raíz cualquiera de P. Entonces $\mathbb{Q}(\alpha) \subset K$ y claramente $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, por lo que $p|[K : \mathbb{Q}]$ y entonces p divide al orden de G ya que $K/\mathbb{Q}$ es galoisiana. El teorema de Cauchy nos dice entonces que existe un elemento de orden p en $G \subset S_p$, es decir, un p-ciclo.

Tenemos entonces que G es un subgrupo de S_p que posee una transposición y un p-ciclo. Un resultado clásico de teoría de grupos nos dice entonces que G es todo S_p. □

Ejemplo 2.4.13. 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. 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. Pruebe que $x^5 - 3$ es soluble por radicales.

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

2.5. Interludio 4: Construcción de polígonos regulares con regla y compás

La construcción de un polígono regular con regla y compás es un problema que podemos tratar con las mismas técnicas que nos ayudaron a resolver los tres problemas imposibles de los antiguos griegos. La razón por la que dejamos este estudio hasta ahora es que este nuevo problema necesita además de la estructura galoisiana de ciertas extensiones.

Observación.
Notemos antes de empezar que ya teníamos suficientes herramientas para afirmar que la construcción en toda generalidad es imposible. En efecto, la construcción de un octadecágono regular (esto es, un polígono regular de 18 lados) implica la posibilidad de construir un ángulo de $\frac{\pi}{9}$, es decir trisectar el ángulo de $\frac{\pi}{3} = 60°$, lo cual ya descartamos anteriormente.

Para lidiar con este problema, será más práctico el ver el plano $\mathbb{R}^2$ sobre el cual estamos trabajando como el plano complejo, lo que nos obliga a redefinir los números constructibles.

Definición 2.5.1. Decimos que $z \in \mathbb{C}$ es un número constructible si $z = a + bi$ con $a, b \in \mathbb{R}$ constructibles.

Notemos inmediatamente que esto no trae nada nuevo a la teoría (aparte del hecho que ahora podemos multiplicar y dividir en $\mathbb{R}^2$). Es decir, un punto $(a, b) \in \mathbb{R}^2$ es constructible con regla y compás si y solo si el complejo correspondiente $z = a + bi$ es constructible. Veamos lo que ocurre con el teorema de Wantzel (Teorema 1.8.3) en este contexto.

Proposición 2.5.2. *Sea $z \in \mathbb{C}$. Entonces z es un número constructible si y solo si existe un entero $n \geq 1$ y una sucesión $K_0, K_1, \ldots, K_n$ de subcuerpos de $\mathbb{C}$ tal que:*

- $K_0 = \mathbb{Q}$;
- *para todo $0 \leq m < n$, $K_m \subset K_{m+1}$ y $[K_{m+1} : K_m] = 2$;*
- $z \in K_n$.

En particular, el cuerpo $C \subset \mathbb{C}$ de los números constructibles corresponde al cuerpo más pequeño de característica 0 cerrado por raíces cuadradas.

Demostración. Supongamos que existe una cadena de cuerpos como en el enunciado con $z \in K_n$. Demostremos por inducción que, para todo m, todo número en K_m (y en particular, z) es constructible. Para $m = 0$ esto es evidente ya que $K_0 = \mathbb{Q}$ y ya sabemos que los números racionales son constructibles. Supongamos entonces que todo número en K_m es constructible y probemos que también es el caso para K_{m+1}. Como $[K_{m+1} : K_m] = 2$, sabemos que existe $x \in K_m$ tal que $K_{m+1} = K_m(\sqrt{x})$. Ahora, sabemos que $|\sqrt{x}| = \sqrt{|x|}$ y $\arg(\sqrt{x}) = \arg(x)/2$. Y como sabemos bien, a todo largo se le puede construir su raíz y todo ángulo puede ser dividido en dos con regla y compás. Por lo tanto el punto $(a, b) \in \mathbb{R}^2$ correspondiente a $\sqrt{x} = a + bi$ se construye fácilmente con regla y compás a partir del punto correspondiente a x, lo que prueba que $\sqrt{x}$ es constructible. Y como también la suma y multiplicación de constructibles son constructibles (recuerde que

en la multiplicación de dos complejos solo intervienen multiplicaciones de reales y cambios de signo), vemos que todo elemento de $K_{m+1} = K_m(x)$ es constructible.

Nótese de paso que esto prueba que C es el cuerpo más pequeño de característica 0 cerrado por raíces cuadradas ya que todo elemento $z \in C$ es obtenido a partir de $\mathbb{Q}$ tomando raíces cuadradas y $\mathbb{Q}$ es el cuerpo más pequeño de característica 0.

En el sentido opuesto, sea $z \in \mathbb{C}$ un número constructible, es decir $z = a + bi$ con $a, b \in \mathbb{R}$ constructibles. Esto implica que existen cadenas $\mathbb{Q} = K_0 \subset \ldots \subset K_s$ y $\mathbb{Q} = L_0 \subset \ldots \subset L_t$ de extensiones cuadráticas con $a \in K_s$ y $b \in L_t$. Escribamos $L_{i+i} = L_i(\sqrt{D_i})$ con $D_i \in L_i$ y definamos K_{s+i+1} como $K_{s+i}(\sqrt{D_i})$. Esto nos da una cadena $\mathbb{Q} = K_0 \subset \ldots \subset K_{n+m}$ de extensiones cuadráticas o triviales. Eliminando las extensiones triviales, obtenemos una cadena $K_0 \subset \ldots \subset K_r$ de extensiones cuadráticas con $a, b \in K_r$ (de hecho, K_r es el composito $K_s L_t$). Vemos entonces que $z \in K_{r+1} = K_r(i)$. □

Vemos entonces que nuestro problema de construir un n-ágono regular se traduce de la siguiente manera:

Corolario 2.5.3. *El n-ágono regular se puede construir con regla y compás si y solo si $\zeta_n \in \mathbb{C}$ es constructible.*

Demostración. En efecto, si el n-ágono regular es constructible, podemos construir otro con su centro en $0 \in \mathbb{C}$ y con un vértice en $1 \in \mathbb{C}$. Los otros vértices caen entonces exactamente en $\mu_n = \{\zeta_n^a \mid 0 \leq a \leq n-1\}$. Este conjunto pertenece a $C \subset \mathbb{C}$ si y solo si $\zeta_n \in C$. □

La pregunta que nos estamos haciendo entonces es la siguiente: ¿Es ζ_n constructible? Es decir: ¿Está $\zeta_n \in C$? O más preciso aún: ¿Está $\mathbb{Q}(\zeta_n)$ contenido en C? Un primer criterio que podemos usar es el siguiente:

Proposición 2.5.4. *Sea $K/\mathbb{Q}$ una extensión finita tal que $K \subset C$. Entonces $[K : \mathbb{Q}] = 2^r$ para algún $r \in \mathbb{N}$.*

Demostración. Como $\mathbb{Q}$ es de característica 0, tenemos que $K/\mathbb{Q}$ es separable y por ende $K = \mathbb{Q}(\alpha)$ con $\alpha \in C$. La definición de C nos dice entonces que $K = K_r$ para una torre de extensiones cuadráticas $\mathbb{Q} = K_0 \subset \ldots \subset K_r$, lo que prueba que $[K : \mathbb{Q}] = 2^r$. □

Ahora, ya sabemos bastante bien que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, por lo que cabe preguntarse cuando tenemos $\varphi(n) = 2^r$. Recordemos que, por el Teorema chino de los restos, si $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ con los p_i primos distintos, entonces

$$\varphi(n) = \prod_{i=1}^{s} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1).$$

Si queremos que este producto sea igual a 2^r, vemos entonces que $\alpha_i = 1$ para todo primo impar y además $p_i - 1 = 2^{r_i}$ para todo $1 \leq i \leq s$. Es decir, acabamos de demostrar lo siguiente:

Proposición 2.5.5. *Si ζ_n es constructible, entonces $n = 2^r p_1 p_2 \cdots p_s$, donde los p_i son primos distintos de la forma $2^{r_i} + 1$ para todo $1 \leq i \leq s$.* □

Como vemos, consideraciones básicas sobre el teorema de Wantzel nos dicen que la lista de posibles n se reduce bastante. Por otra parte, a comienzos del siglo XIX (es decir, antes de que este teorema fuera demostrado) Gauss ya había encontrado un método para construir un n-ágono regular con $n = 17 = 2^4+1$, el cual generalizó a números primos de la forma $2^r + 1$. Agreguemos a eso el siguiente lema:

Lema 2.5.6. *Sean $m, n \in \mathbb{N}$ coprimos. Supongamos que el n-ágono y el m-ágono regular son constructibles con regla y compás. Entonces el mn-ágono regular también lo es.*

Demostración. Si $(m, n) = 1$, entonces existen $a, b \in \mathbb{Z}$ tales que $am + bn = 1$, por lo que

$$\zeta_{mn} = \zeta_{mn}^{am+bn} = \zeta_{mn}^{am}\zeta_{mn}^{bn} = (\zeta_{mn}^{m})^a(\zeta_{mn}^{n})^b = \zeta_n^a\zeta_m^b,$$

por lo que ζ_{mn} es constructible si ζ_m y ζ_n lo son. □

Y entonces el resultado de Gauss más nuestras deducciones a partir del teorema de Wantzel nos dicen que:

Teorema 2.5.7. *El n-ágono regular es constructible con regla y compás si y solo si $n = 2^r p_1 p_2 \cdots p_s$ donde los p_i son primos distintos de la forma $2^{r_i} + 1$ para todo $1 \leq i \leq s$.* □

Demostración. Ya demostramos uno de los sentidos de este enunciado gracias a Wantzel, por lo que solo no queda demostrar el resultado de Gauss. Esto sin embargo, lo haremos de manera moderna usando la Teoría de Galois.

Supongamos entonces que n es como en el enunciado, sea $K = \mathbb{Q}(\zeta_n)$ y consideremos la extensión $K/\mathbb{Q}$. Debemos demostrar que $K \subset C$. Para esto, basta con recordar que el grupo de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$ es de orden $\varphi(n) = 2^t$ para algún $t \in \mathbb{N}$ y se trata por ende de un 2-grupo. Ahora, sabemos que todo 2-grupo tiene un subgrupo H de índice 2 (resultado del curso Grupos y Anillos), lo que nos define una subextensión $\mathbb{Q} \subset L \subset K$ tal que $[L : \mathbb{Q}] = 2$. El orden de H es entonces 2^{t-1}, por lo que se trata también de un subgrupo y posee entonces un subgrupo de índice 2. Iterando este procedimiento obtenemos una cadena de subgrupos

$$G = H_0 > H_1 > H_2 > \cdots > H_t = \{\mathrm{id}\},$$

tal que $[H_i : H_{i+1}] = 2$ para todo $0 \leq i \leq t-1$. Por el Teorema Fundamental, esta cadena induce una cadena de subcuerpos

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = K,$$

tal que $[L_{i+1} : L_i]$ para todo $0 \leq i \leq t-1$. Como $\zeta_n \in K = L_t$, tenemos que ζ_n es constructible. □

Observación.
Nótese que, si bien demostramos que el n-ágono regular es constructible, es otra historia el encontrar un proceso *geométrico* que permita su construcción. Para esto, deberíamos encontrar elementos explícitos $\alpha_i \in L_i$ para cada i tales que $L_{i+1} = L_i(\sqrt{\alpha_i})$ y luego expresar ζ_n en función de α_n. Esto es, en el fondo, de lo que trata el método de Gauss.

3. Algebras

Ahora dejaremos de lado la Teoría de Galois y las extensiones de cuerpos para estudiar anillos más generales que uno puede construir a partir de un cuerpo o de otros anillos conmutativos. Éstas son las *álgebras*.

3.1. Generalidades

Comencemos de forma bien general volviendo al marco de anillos.

Definición 3.1.1. Sea R un anillo conmutativo unitario. Un *álgebra sobre* R o *R-álgebra* es un R-módulo unitario A, equipado con una aplicación R-bilineal

$$\begin{aligned} m : A \times A &\to A \\ (x, y) &\mapsto xy \end{aligned}$$

llamada *multiplicación* en A. Recuerde que R-bilineal significa que, para todo $x, x', y, y' \in A$ y para todo $r \in R$,

- $(x + rx')y = x + r(x'y)$;
- $x(y + ry') = xy + r(xy')$.

Decimos además que:

- A es *asociativa* si $(xy)z = x(yz)$ para todo $x, y, z \in A$;
- A es *conmutativa* si $xy = yx$ para todo $x, y, \in A$;

- A es *unitaria* si existe un elemento $1_A \in A$ tal que $1_A x = x 1_A = x$ para todo $x \in A$.

Observación.
Toda R-álgebra asociativa es un anillo con la suma de R-módulo y su propia multiplicación. Si además A es unitaria, entonces obtenemos naturalmente un homomorfismo de anillos $\varphi : R \to A$ vía $\varphi(r) := r1_A$.

Ejercicio. Sean A, R dos anillos unitarios con R conmutativo y sea $\varphi : R \to A$ un homomorfismo de anillos que envía 1_R a 1_A. Demuestre que A posee una estructura natural de R-álgebra asociativa y unitaria.

Ejemplo 3.1.2. Sea R un anillo conmutativo unitario. Entonces R es una $\mathbb{Z}$-álgebra. En efecto, el homomorfismo natural $\varphi : \mathbb{Z} \to R$ con el que definimos la característica de un anillo (¡al comienzo de estos apuntes!) y el ejercicio anterior nos aseguran que R es un $\mathbb{Z}$-módulo con una multiplicación $\mathbb{Z}$-bilineal.

Ejemplo 3.1.3 (Álgebra de polinomios)**.** Sea R un anillo conmutativo unitario. Entonces $R[x]$ es una R-álgebra asociativa, conmutativa y unitaria.

Ejemplo 3.1.4 (Algebra de funciones)**.** Sea R un anillo conmutativo unitario y X un conjunto no vacio. Entonces $R^X = \{f : X \to R\}$ es una R-álgebra bajo la suma y producto clásicos de funciones y su estructura de R-módulo viene dada sencillamente por la multiplicación por escalar. Esta álgebra es asociativa, conmutativa y unitaria.

Ejemplo 3.1.5. Sea R un anillo conmutativo unitario y sea M un R-módulo. Entonces $A = \mathcal{L}_R(M) := \{f : M \to M \mid f \, R\text{-lineal}\}$ es una R-álgebra bajo la suma clásica y la composición de funciones. Se trata de un álgebra asociativa y unitaria, pero en general no conmutativa.

Notación. Como se ve en este último ejemplo, usaremos en esta parte del curso la noción de "función R-lineal" como sinónimo de "homomorfismo de R-módulos", ya que es precisamente esto lo que siginifica en el marco clásico de espacios vectoriales en álgebra lineal.

Ejemplo 3.1.6 (Álgebra de matrices)**.** Sea A una R-álgebra y sea $n \geq 1$. Entonces

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

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* $n \times n$ sobre A.

Supongamos además que A es asociativa y unitaria y denotemos por $\varepsilon_{ij} = (x_{ij})$ la matriz tal que $x_{rs} = 1$ si $(r, s) = (i, j)$ y $x_{rs} = 0$ en caso contrario. Estos elementos de $M_n(A)$ se comportan de la siguiente manera:

1. si $j \neq k$, entonces $\varepsilon_{ij}\varepsilon_{kr} = 0$;

2. $\varepsilon_{ij}\varepsilon_{jr} = \varepsilon_{ir}$ para todo $1 \leq i, j, r \leq n$.

3. $\{\varepsilon_{ij}\}_{1\leq i,j\leq n}$ es una base del A-módulo libre $M_n(A)$.

Ejemplo 3.1.7 (Algebra de dimensión finita sobre un cuerpo)**.** Sean K un cuerpo, A un K-espacio vectorial de dimensión finita sobre y $\{e_1, \ldots, e_n\}$ una K-base de A. Para $1 \leq i, j, k \leq n$, fijemos $\gamma_{ijk} \in K$ y definamos, para $1 \leq i, j \leq n$,

$$e_i e_j := \sum_{k=1}^{n} \gamma_{ijk} e_k.$$

Extendiendo estos productos a todo A por K-linealidad, obtenemos una estructura de K-álgebra sobre A. Los n^3 escalares γ_{ijk} se llaman las constantes de estructura del álgebra A (asociadas a la base de los e_i).

Recíprocamente, dada un álgebra A de dimension finita sobre K, basta fijar una K-base $\{e_1, \ldots, e_n\}$ y notar que los productos $e_i e_j$ se pueden escribir entonces como combinación lineal de los e_k para obtener escalares γ_{ijk} tales que A es la K-álgebra que corresponde a estas constantes de estructura.

Ejemplo 3.1.8 (Álgebra de cuaterniones)**.** Sean K un cuerpo de caracaterística distinta de 2 y sean $a, b \in K^*$. Consideremos el K-espacio vectorial A de base $\{1, i, j, k\}$ y definamos

$$i^2 = a, \quad j^2 = b, \quad k^2 = ab, \quad ij = -ji = k, \quad jk = -kj = -bi, \quad ki = -ik = -aj.$$

Esto define sobre A una estructura de K-álgebra asociativa, unitaria y no conmutativa llamada el *álgebra de cuaterniones* sobre K asociada al par (a, b) y denotada $A = (\frac{a,b}{K})$.

Nótese que, asumiendo la asociatividad, las dos primeras igualdades junto con la cuarta implican las otras tres. Además, en el caso de $K = \mathbb{R}$ y $a = b = -1$, obtenemos los clásicos cuaterniones de Hamilton $\mathbb{H}$.

Vistos estos ejemplos, pasemos a otras definiciones básicas. Recordando que una R-álgebra (asociativa) no es más que un anillo con estructura de R-módulo (o un R-módulo con estructura de anillo), no debe ser difícil el imaginar las nociones de subálgebra y de homomorfismo de álgebras. En efecto:

Definición 3.1.9. Sea A una R-álgebra. Una *R-subálgebra* B de A es un R-submódulo cerrado por multiplicación (i.e. que a la vez es un subanillo si A es asociativa).

Veamos algunas proposiciones (a demostrar como ejercicio) a modo de ejemplo:

Ejemplo 3.1.10. Sea A una R-álgebra asociativa y unitaria. Entonces el conjunto

$$Z(A) := \{x \in A \mid xa = ax, \, \forall a \in A\},$$

es una subálgebra de A llamada el *centro* de A.

Observación.
El homomorfismo natural $\varphi : R \to A$ definido anteriormente para toda R-álgebra asociativa y unitaria A tiene siempre su imagen contenida en $Z(A)$ ya que R es conmutativo. En particular, si K es un cuerpo y A una K-álgebra asociativa unitaria, entonces K puede identificarse con un subanillo del centro de A.

Ejemplo 3.1.11. Sea $\{B_i\}_{i \in I}$ una familia no vacía de subálgebras de A. Entonces $\bigcap_{i \in I} B_i$ es una subálgebra de A.

Ejemplo 3.1.12. Sean A una R-álgebra y $S \subset A$ un subconjunto de A. Sea I_S el conjunto de las subálgebras B de A que contienen a S. Entonces $\bigcap_{B \in I_S} B$ es la menor subálgebra de A que contiene S. Se dice que $\bigcap_{B \in I_S} B$ es *la subálgebra de A generada por S* y que S es un *sistema de generadores* para ésta subálgebra.

Pasemos ahora a la noción de homomorfismo. Como decíamos, esto es en el fondo una fusión entre homomorfismos de módulos y homomorfismos de anillos. En efecto:

Definición 3.1.13. Sean A, A' dos R-álgebras. Un *homomorfismo de R-álgebras* entre A y A' es un homomorfismo de R-módulos $f : A \to A'$ que respeta la multiplicación en ambas álgebras. En otras palabras:

- para todo $a, b \in A$ y para todo $r \in R$, $f(a + rb) = f(a) + rf(b)$;
- para todo $a, b \in A$, $f(ab) = f(a)f(b)$.

Si además ambas álgebras son unitarias, pedimos que un homomorfismo $f : A \to A'$ envíe 1_A a $1_{A'}$.

De la misma manera definimos los conceptos de isomorfismo, epimorfismo, monomorfismo, endomorfismo y automorfismo de álgebras. También definimos el *núcleo* $\ker(f)$ de f como la preimagen del elemento $0 \in A'$.

Recordemos ahora que el núcleo es el objeto perfecto para definir los objetos cocientes. En efecto, en el marco de grupos todo núcleo era un subgrupo normal y viceversa, mientras que en el marco de anillos todo núcleo era un ideal y viceversa. Definamos el objeto correspondiente en este caso.

Definición 3.1.14. Sean A una R-álgebra e I un R-submódulo de A. Decimos que I es *ideal izquierdo* de A si $ay \in I$ para todo $a \in A$ e $y \in I$. Las nociones de *ideal derecho* e *ideal bilateral* (o sencillamente "ideal") se definen de forma análoga.

Vemos entonces claramente que, para todo homomorfismo de R-álgebras $f : A \to A'$, el núcleo $\ker(f)$ es un ideal de A. Por otra parte, dado un ideal I de una R-álgebra A, podemos considerar el R-módulo cociente A/I y equiparlo con la multiplicación dada por $(a+I)(b+I) := ab+I$. Como $aI, Ib \subset I$, vemos que esta multiplicación está bien definida, lo que nos provee la noción de *álgebra cociente*, también denotada por A/I. Tenemos en particular el siguiente resultado (cuya demostración es un simple ejercicio).

Proposición 3.1.15. *Sea I un ideal de A. Entonces la función $\pi : A \to A/I : x \mapsto x + I$ es un epimorfismo de núcleo I.*

Tenemos también los ya clásicos teoremas de isomorfismo (también demostrables como ejercicio).

Teorema 3.1.16. *Sea $f : A \to A'$ un homomorfismo de R-álgebras. Entonces $f(A)$ es una R-subálgebra de A' y $A/\ker(f)$ es isomorfa a $f(A)$.*

Teorema 3.1.17. *Sean I, J ideales de alguna R-álgebra A. Entonces $(I+J)/J \simeq I/(I \cap J)$.*

Teorema 3.1.18. *Sean $I \subset J$ ideales de alguna R-álgebra A. Entonces $A/J \simeq (A/I)/(J/I)$.*

Teorema 3.1.19 (Propiedad universal del cociente)**.** *Sean A, B, C tres R-álgebras. Sean $f : A \to B$ y $\pi : A \to C$ homomorfismos de R-álgebras con π epiyectivo. Entonces las dos propiedades siguientes son equivalentes:*

- *existe un único homomorfismo de álgebras $\varphi : C \to B$ tal que $\varphi \circ \pi = f$, es decir, el siguiente diagrama conmuta*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\,\varphi} & \\ C & & \end{array},$$

- $\ker(\pi) \subset \ker(f)$.

Demostración. Supongamos la primera propiedad. Entonces, para $a \in \ker(\pi)$, tenemos que

$$f(a) = \varphi \circ \pi(a) = \varphi(\pi(a)) = \varphi(0) = 0,$$

por lo que $a \in \ker(f)$, lo que prueba la segunda propiedad.

Supongamos ahora que $\ker(\pi) \subset \ker(f)$ y definamos $\varphi : C \to B$ con la fórmula $\varphi(c) := f(a)$, donde $c = \pi(a)$. Nótese que un tal a siempre existe ya que π es epiyectivo. Por otra parte, si a' es otro elemento tal que $\pi(a') = c$, entonces $\pi(a -$

$a') = c - c = 0$ y por ende $a - a' \in \ker(\pi) \subset \ker(f)$. Esto implica que $f(a') = f(a' + (a - a')) = f(a)$ y por ende $\varphi(c)$ no depende de la elección de la preimagen a. Además, si $a, a' \in A$ son preimágenes respectivas de $c, c' \in C$ por π, entonces $a + ra'$ y aa' son respectivamente preimágenes de $c + rc'$ y cc' ya que π es un homomorfismo de R-álgebras. Como f también es un homomorfismo, obtenemos que

$$\varphi(c + rc') = f(a + ra') = f(a) + rf(a') = \varphi(c) + r\varphi(c'),$$
$$\varphi(cc') = f(aa') = f(a)f(a') = \varphi(c)\varphi(c'),$$

lo que prueba que φ es un homomorfismo de R-álgebras. Finalmente, la definición misma asegura que $\varphi \circ \pi = f$ y esto asegura su unicidad, ya que entonces $\varphi(\pi(a)) = f(a)$ para todo $a \in A$ y por ende $\varphi(c) = f(a)$ si $c = \pi(a)$ (y siempre existe un tal a por epiyectividad de π). □

Estudiemos ahora un instante un caso particular de álgebras que son aquellas que ya no tienen cocientes interesantes porque no tiene ideales interesantes:

Definición 3.1.20. Una R-álgebra A es *simple* si $A \neq \{0\}$ y no tiene ideales propios no nulos.

Observación.
Si A es un álgebra simple y $f : A \to A'$ es un homomorfismo de álgebras no nulo, entonces ϕ es inyectiva. En efecto, $\ker(f)$ es un ideal de A y éste no puede ser todo A ya que f es no nulo, por lo que $\ker(f) = \{0\}$.

Un ejemplo particular de álgebras simples son las álgebras de división.

Definición 3.1.21. Una *R-álgebra de división* es una R-álgebra $D \neq \{0\}$ asociativa y unitaria en la que todo elemento no nulo es invertible.

La simplicidad de estas álgebras es evidente ya que todo ideal no nulo debe contener a 1_A y por ende a todo A.

Ejemplo 3.1.22. Los cuaterniones de Hamilton $\mathbb{H}$ forman un álgebra de división. En efecto, si $x = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$, entonces su *conjugado* está definido como $\bar{x} = a_0 - a_1 i - a_2 j - a_3 k$ y para estos elementos tenemos que

$$x\bar{x} = a_0^2 + a_1^2 + a_2^2 + a_3^2 = N(x) \in \mathbb{R},$$

por lo que $x(\frac{1}{N(x)}\bar{x}) = 1 \in \mathbb{H}$.

La simplicidad de las álgebras de división va de hecho un poco más lejos.

Lema 3.1.23. *Sea D un álgebra de división y sea $n \geq 1$. Entonces $M_n(D)$ es simple.*

Demostración. Sea I un ideal no nulo de $M_n(D)$, sea $Y = (y_{ij}) \in I$ un elemento arbitrario no nulo y sea y_{rs} una coordenada no nula de Y. Notemos que, por un cálculo directo,

$$\varepsilon_{ir} Y \varepsilon_{sj} = y_{rs} \varepsilon_{ij}.$$

Por lo tanto, para todo $X = (x_{ij}) \in M_n(D)$ tenemos que

$$X = (x_{ij}) = \sum_{i,j} x_{ij} \varepsilon_{ij} = \sum_{i,j} x_{ij} y_{rs}^{-1} \varepsilon_{ir} Y \varepsilon_{sj},$$

lo que nos dice que $X \in I$ y por ende $I = M_n(D)$. Esto prueba que $M_n(D)$ es simple. □

3.2. Producto Tensorial

El producto tensorial es una herramienta de la teoría de módulos. Sin embargo, con ella se pueden construir álgebras a partir de un módulo dado y eso la convierte en un objeto de estudio que nos interesa particularmente en esta parte del curso que trata de álgebras.

3.2.1. Producto tensorial de módulos

Definamos pues para comenzar la noción del producto tensorial de dos R-módulos. Esto nos lleva primero a la noción de aplicaciones bilineales, las cuales definimos a continuación.

Definición 3.2.1. Sean M, N y T tres R-módulos. Una aplicación $\varphi : M \times N \to T$ se dice *R-bilineal* si, para todo $x, x' \in M$, $y, y' \in N$ y $r \in R$, tenemos que:

- $\varphi(x + rx', y) = \varphi(x, y) + r\varphi(x', y)$;
- $\varphi(x, y + ry') = \varphi(x, y) + r\varphi(x, y')$.

Llamamos *imagen de* φ y denotamos $\mathrm{Im}(\varphi)$ al submódulo de T generado por el conjunto $\varphi(M \times N)$, es decir:

$$\begin{aligned} \mathrm{Im}(\varphi) &= \left\{ \sum_{i=1}^{s} \alpha_i \varphi(m_i, n_i) \mid \alpha_i \in R,\, m_i \in M,\, n_i \in N,\, s \in \mathbb{N} \right\} \\ &= \left\{ \sum_{i=1}^{s} \varphi(m_i', n_i) \mid m_i' \in M,\, n_i \in N,\, s \in \mathbb{N} \right\} \end{aligned}$$

Observación.
Dada una aplicación $\varphi : M \times N \to T$, para cada $a \in M$ y para cada $b \in N$ se pueden definir las aplicaciones

$$\varphi_a : N \to T : n \mapsto \varphi(a, n), \varphi_b : M \to T \qquad\qquad m \mapsto \varphi(m, b).$$

Vemos entonces que φ es R-bilineal si y solo si φ_a y φ_b son R-lineales *para todo* $a \in M$ y $b \in N$. (Recuerde que una aplicación es R-lineal si se trata de un homomorfismo de R-módulos.)

En particular, si φ es R-bilineal, entonces $\varphi(a, 0) = \varphi(0, b) = 0$ para todo $a \in M$ y $b \in N$.

Ejercicio. Sean M, N y T tres R-módulos. Pruebe que $\mathrm{Bil}_R(M, N; T) = \{\varphi : M \times N \to T \mid \varphi\, R\text{-bilineal}\}$ es un R-módulo isomorfo a $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, T))$ y a $\mathrm{Hom}_R(N, \mathrm{Hom}_R(M, T))$.

Sea L un cuarto R-módulo. Prueba que si $\varphi : M \times N \to T$ es R-bilineal y $g : T \to L$ es R-lineal entonces $g \circ \varphi : M \times N \to L$ es R-bilineal.

Ejercicio. Sea T un $\mathbb{Z}$-módulo y sean $m, n \in \mathbb{N}$ tales que $(m, n) = 1$. Sea $\varphi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to T$ una aplicación $\mathbb{Z}$-bilineal. Pruebe que $\varphi = 0$.

Las definiciones, observaciones y ejercicios que preceden nos incitan a pensar que hay una relación estrecha entre bilinealidad y linealidad. Ahora, es para ésta última que poseemos herramientas poderosísimas como son todos los resultados del álgebra lineal (al menos cuando R es un cuerpo). Quisiéramos entonces poder ver las aplicaciones bilineales $M \times N \to T$ como aplicaciones lineales de alguna manera, eventualmente cambiando los objetos M, N y T por otros objetos que le estén relacionados. El pasar de $\mathrm{Bil}_R(M, N; T)$ a $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, T))$ es una idea interesante, pero tiene la desventaja de ser poco simétrica ya que nos fuerza a conservar M y a cambiar N y T por $\mathrm{Hom}_R N, T$. El producto tensorial $M \otimes N$ de M y N es un objeto que responde a esta interrogativa y cuya definición depende de una propiedad universal, como la que estudiamos hace un rato para los cocientes.

Definición 3.2.2. Sean M, N dos R-módulos. Un producto tensorial de M y N es un par (T, φ) donde T es un R-módulo y $\varphi : M \times N \to T$ es una aplicación R-bilineal que cumple la siguiente propiedad universal:

Para todo R-módulo P y para toda aplicación R-bilineal $\psi : M \times N \to P$, existe *una única* función R-lineal $f : T \to P$ tal que $f \circ \varphi = \psi$, es decir, el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} M \times N & \xrightarrow{\psi} & P\,. \\ {\scriptstyle\varphi}\big\downarrow & \nearrow_{\exists!\, f} & \\ T & & \end{array}$$

Una definición como ésta (a saber, una que usa una propiedad universal), asegura que el producto tensorial, *si existe alguno*, es *único* salvo *único* homomorfismo, lo que nos permite definirlo bien de una vez por todas como EL producto tensorial (esto es precisamente lo que NO ocurría con las clausuras algebraicas). Luego hemos de concentrarnos en demostrar su existencia, ya que de lo contrario estamos construyendo castillos en el aire. Para acercarnos al objetivo de probar la unicidad, la siguiente proposición nos será útil.

Proposición 3.2.3. *Sea (T, φ) un producto tensorial de M y N. Entonces $T = \mathrm{Im}(\varphi)$.*

Demostración. En efecto, sea $P = \mathrm{Im}(\varphi) \subset T$ el submódulo de T correspondiente a la imágen de φ. Entonces claramente la aplicación R-bilineal $\varphi : M \times N \to T$ induce una aplicación R-bilineal $\psi : M \times N \to P$ simplemente definida por $\psi(a, b) := \varphi(a, b)$. Ahora, la propiedad universal del producto tensorial nos dice que tenemos un diagrama conmutativo

$$\begin{array}{ccc} M \times N & \xrightarrow{\psi} & P\,, \\ {\scriptstyle\varphi}\big\downarrow & \nearrow_{\exists!\, f} & \\ T & & \end{array}$$

por lo que $\psi = f \circ \varphi$. Consideremos entonces la función R-lineal $g : T \to T$ definida por $g(t) := f(t) \in P \subset T$. Como $\varphi(a, b) \in P \subset T$, vemos que

$$\varphi(a, b) = \psi(a, b) = f(\varphi(a, b)) = g(\varphi(a, b)),$$

para todo $a \in M$ y $b \in N$. En otras palabras, tenemos que $\varphi = g \circ \varphi$. Ahora, si aplicamos la propiedad universal a la mismísima $\varphi : M \times N \to T$, vemos que existe *una única* función R-lineal g tal que $\varphi = g \circ \varphi$. Sin embargo, sabemos bien que la identidad id_T posee esta propiedad también. La unicidad implica entonces que $g = \mathrm{id}_T$, por lo que, para todo $t \in T$, tenemos que $t = g(t) = f(t) \in P$, lo que prueba que $P \supset T$ y por ende $P = T$. □

Probemos pues la unicidad del producto tensorial a partir de su propiedad universal.

Proposición 3.2.4. *Sean M, N dos R-módulos. Sean (T, φ) y (T', φ') dos productos tensoriales de M y N. Entonces existe un* único *isomorfismo de R-módulos $f : T \to T'$ tal que $f \circ \varphi = \varphi'$.*

Además, si (T, φ) es un producto tensorial de M y N y $f : T \to T'$ es un isomorfismo, entonces $(T', f \circ \varphi)$ es un producto tensorial para M y N.

Demostración. Como (T, φ) es un producto tensorial de M y N y $\varphi' : M \times N \to T'$ es bilineal, la propiedad universal nos dice que existe un único homomorfismo de R-módulos $f : T \to T'$ tal que $f \circ \varphi = \varphi'$. Bastará con demostrar entonces que se trata de un isomorfismo. Ahora, (T', φ') es también un producto tensorial de M y N y $\varphi : M \times N \to T$ es bilineal, por lo que la propiedad universal nos dice también que existe un único homomorfismo de R-módulos $g : T' \to T$ tal que $g \circ \varphi' = \varphi$. Tenemos entonces que

$$(g \circ f) \circ \varphi = g \circ (f \circ \varphi) = g \circ \varphi' = \varphi,$$

y también

$$(f \circ g) \circ \varphi' = f \circ (g \circ \varphi') = f \circ \varphi = \varphi'.$$

Sea ahora $t \in T$. La Proposición 3.2.3 nos dice que $\mathrm{Im}(\varphi) = T$, por lo que existen elementos $m_1, \ldots, m_\ell \in M$ y $n_1 \ldots, n_\ell \in N$ tales que $t = \sum_{i=1}^{\ell} \varphi(m_i, n_i)$. Recordando que $g \circ f$ es R-lineal si f y g lo son, tenemos entonces que

$$(g \circ f)(t) = (g \circ f)\left(\sum_{i=1}^{\ell} \varphi(m_i, n_i)\right) = \sum_{i=1}^{\ell} (g \circ f)(\varphi(m_i, n_i)) = \sum_{i=1}^{\ell} \varphi(m_i, n_i) = t,$$

lo que prueba que $(g \circ f) = \mathrm{id}_T$ y por ende f es inyectiva. De la misma manera, para $t' \in T'$, la Proposición 3.2.3 nos dice que existen elementos $m'_1, \ldots, m'_{\ell'} \in M$ y $n'_1 \ldots, n'_{\ell'} \in N$ tales que $t' = \sum_{i=1}^{\ell'} \varphi'(m'_i, n'_i)$. Vemos entonces que

$$(f \circ g)(t') = (f \circ g)\left(\sum_{i=1}^{\ell'} \varphi'(m'_i, n'_i)\right) = \sum_{i=1}^{\ell'} (f \circ g)(\varphi'(m'_i, n'_i)) = \sum_{i=1}^{\ell'} \varphi'(m'_i, n'_i) = t',$$

lo que prueba que $(f \circ g) = \mathrm{id}_{T'}$ y por ende f es epiyectiva. Esto prueba que f es un isomorfismo.

Para la segunda afirmación, está claro que $\varphi' := f \circ \varphi : M \times N \to T'$ es R-bilineal, por lo que debemos probar que cumple la propiedad universal. Consideremos entonces un R-módulo P y una aplicación R-bilineal $\psi : M \times N \to P$. La propiedad universal aplicada a (T, φ) nos dice que existe *una única* función R-lineal $g : T \to P$ tal que $g \circ \varphi = \psi$. Componiendo con $f^{-1} : T' \to T$, que es una función R-lineal ya que f lo es, obtenemos una función R-lineal $g' = g \circ f^{-1} : T' \to P$ tal que

$$g' \circ \varphi' = (g \circ f^{-1}) \circ (f \circ \varphi) = g \circ f^{-1} \circ f \circ \varphi = g \circ \varphi = \psi.$$

Esto prueba la parte existencial de la propiedad universal.

Sea ahora $g'' : T' \to P$ otra función tal que $g'' \circ \varphi' = \psi$. Nótese que, como $f^{-1} \circ f = \mathrm{id}_T$, entonces $f^{-1} \circ \varphi' = f^{-1} \circ f \circ \varphi = \varphi$. Entonces $g''' = g'' \circ f : T \to P$ es una función R-lineal tal que $g'' = g''' \circ f^{-1}$ y

$$g''' \circ \varphi = (g'' \circ f) \circ (f^{-1} \circ \varphi') = g'' \circ f \circ f^{-1} \circ \varphi' = g'' \circ \varphi' = \psi.$$

Por lo tanto, por la unicidad de la propiedad universal aplicada a (T, φ), tenemos que $g''' = g$, lo que prueba que $g'' = g''' \circ f^{-1} = g \circ f^{-1} = g'$ y por ende g' es única. □

Ahora que sabemos que, de existir un producto tensorial (y así es en toda generalidad, véase el Teorema 3.2.8) éste es único salvo único isomorfismo, podemos hablar de EL producto tensorial y definir la siguiente notación:

Notación. El producto tensorial de M y N es denotado por $M \otimes_R N$ (y a veces $M \otimes N$ si el anillo R está implícito) y la aplicación $\varphi : M \times N \to M \otimes_R N$ envía el par (m, n) al objeto $m \otimes n \in M \otimes_R N$.

La bilinealidad de φ queda entonces expresada por las siguientes propiedades:

- $(m + m') \otimes n = m \otimes n + m' \otimes n$ para todo $m, m' \in M$, $n \in N$;
- $m \otimes (n + n') = m \otimes n + m \otimes n'$ para todo $m \in M$, $n, n' \in N$;
- $r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$ para todo $r \in R$, $m \in M$, $n \in N$.

Además, dada la Proposición 3.2.3, vemos que todo elemento $t \in M \otimes_R N$ se escribe de la forma $t = \sum_{i=1}^{\ell} m_i \otimes n_i$.

La relación entre bilinealidad y linealidad queda reflejada entonces en la siguiente proposición.

Proposición 3.2.5. *Sean M, N dos R-módulos. Entonces existe un isomorfismo de R-módulos entre* $\mathrm{Bil}(M, N; P)$ *y* $\mathrm{Hom}_R(M \otimes_R N, P)$ *para todo R-módulo P.*

Demostración. Sean $B = \mathrm{Bil}(M, N; P)$ y $H = \mathrm{Hom}_R(M \otimes_R N, P)$. Recordemos que la estructura de R-módulo sobre B y H está dada por la suma de funciones y por $(r\varphi)(m, n) = r(\varphi(m, n))$ para todo $r \in R$ y $\varphi \in B$ y $(rf)(t) = r(f(t))$ para todo $f \in H$. Notemos ahora que la propiedad universal de $M \otimes_R N$ nos da precisamente una aplicación $\Theta : B \to H$ ya que a toda aplicación bilineal $\varphi \in B$ le asocia una función lineal $\Theta(\varphi) \in H$. Explícitamente, Θ está definida de la siguiente manera: para $\varphi \in B$, y $t = \sum_{i=1}^{\ell} m_i \otimes n_i \in M \otimes_R N$ tenemos que:

$$(\Theta(\varphi))(t) := \sum_{i=1}^{\ell} \varphi(m_i, n_i).$$

En efecto, la propiedad universal nos dice que $(\Theta(\varphi))(m \otimes n) = \varphi(m, n)$ para todo par $(m, n) \in M \times N$ y lo único que hicimos fue extender por R-linealidad de $\Theta(\varphi)$.

Notemos ahora que, para todo $r \in R$ y $\varphi, \varphi' \in B$, tenemos que

$$\begin{aligned}(\Theta(\varphi + r\varphi'))(t) = \sum_{i=1}^{\ell} (\varphi + r\varphi')(m_i, n_i) &= \sum_{i=1}^{\ell} \varphi(m_i, n_i) + r \sum_{i=1}^{\ell} \varphi'(m_i, n_i) \\ &= \Theta(\varphi)(t) + r(\Theta(\varphi'))(t) = (\Theta(\varphi) + r\Theta(\varphi'))(t),\end{aligned}$$

para todo $t \in M \otimes_R N$, lo que prueba que Θ es un homomorfismo de R-módulos.

Finalmente, debemos demostrar que se trata de un isomorfismo. Supongamos entonces que $\Theta(\varphi) = 0$ para algún $\varphi \in B$. Esto nos dice que, para todo $t \in M \otimes_R N$, $(\Theta(\varphi))(t) = 0$. En particular, si $t = m \otimes n$, vemos que $\varphi(m, n) = 0$. Como esto es cierto para todo $m \in M$ y $n \in N$, obtenemos que $\varphi = 0$, lo que prueba la inyectividad de Θ.

Ahora, para probar la epiyectividad, sea $f : M \otimes_R N \to P$ un elemento de H, es decir, una función R-lineal. Definamos entonces una función bilineal $\varphi : M \times N \to P$ como $\varphi(m, n) := f(m \otimes n)$. La bilinealidad de φ viene de la linealidad de f y de las propiedades de $m \otimes n$, por lo que $\varphi \in B$. Vemos entonces por definición y por linealidad de f que $\Theta(\varphi) = f$, lo que prueba la epiyectividad de Θ. □

Veamos ahora algunas propiedades del producto tensorial antes de probar su existencia.

Proposición 3.2.6. *Sean M, N, P tres R-módulos. Entonces existen isomorfismos canónicos*

- $R \otimes_R M \simeq M$;
- $M \otimes_R N \simeq N \otimes_R M$;
- $(M \otimes_R N) \otimes_R P \simeq M \otimes_R (N \otimes_R P)$;
- $(M \oplus N) \otimes_R P \simeq (M \otimes_R P) \oplus (N \otimes_R P)$.

Demostración. El primer isomorfismo viene dado por

$$\begin{aligned} f : R \otimes_R M &\to M \\ r \otimes m &\mapsto rm. \end{aligned}$$

Este homomorfismo está bien definido ya que corresponde a la función R-bilineal $\varphi : R \times M \to M$ que envía (r, m) a rm. Para probar que es un isomorfismo, basta con considerar el homomorfismo

$$\begin{aligned} g : M &\to R \otimes_R M \\ m &\mapsto 1 \otimes m. \end{aligned}$$

Vemos entonces que $(f \circ g)(m) = m$ y $(g \circ f)(r \otimes m) = 1 \otimes (rm) = r \otimes m$, por lo que f y g son la inversa una de la otra, lo que prueba que son isomorfismos.

El segundo isomorfismo viene dado por

$$\begin{aligned} f : M \otimes_R N &\to N \otimes_R M \\ m \otimes n &\mapsto n \otimes m. \end{aligned}$$

Este homomorfismo está bien definido ya que corresponde a la función bilineal $\varphi : M \times N \to N \times M$ que envía (m, n) a $n \otimes m$. Como su inversa es absolutamente evidente, está claro que se trata de un isomorfismo.

El tercer isomorfismo viene dado por

$$\begin{aligned} f : (M \otimes_R N) \otimes_R P &\to M \otimes_R (N \otimes_R P) \\ (m \otimes n) \otimes p &\mapsto m \otimes (n \otimes p). \end{aligned}$$

Este homomorfismo está bien definido ya que corresponde a la función bilineal $\varphi : (M \otimes_R N) \times P \to M \otimes_R (N \otimes_R P)$ que envía $(\sum_{i=1}^n m_i \otimes n_i, p)$ a $\sum_{i=1}^n m_i \otimes (n_i \otimes p)$. Y esta también está bien definida ya que, para todo $p \in P$ tenemos que la función $\psi_p : M \times N \to M \otimes_R (N \otimes_R P)$ que envía (m, n) a $m \otimes (n \otimes p)$ es R-bilineal, lo que asegura que la función $\varphi_p : M \otimes_R N \to M \otimes_R (N \otimes_R P)$ dada por $t \mapsto \varphi(t, p)$ está bien definida. Como la inversa de f es absolutamente evidente, está claro que se trata de un isomorfismo.

El cuarto isomorfismo viene dado por

$$\begin{aligned} f : (M \oplus N) \otimes_R P &\to (M \otimes_R P) \oplus (N \otimes_R P) \\ (m + n) \otimes p &\mapsto m \otimes p + n \otimes p. \end{aligned}$$

Este homomorfismo está bien definido ya que corresponde a la función bilineal $\varphi : (M \oplus N) \times P \to (M \otimes_R P) \oplus N \otimes_R P$ que envía $(m + n, p)$ a $m \otimes p + n \otimes p$. Para probar que es un isomorfismo, basta con considerar los homomorfismos

$$\begin{aligned} g_1 : M \otimes_R P &\to (M \oplus N) \otimes_R P \\ m \otimes p &\mapsto (m + 0) \otimes p, \\ g_2 : N \otimes_R P &\to (M \oplus N) \otimes_R P \\ n \otimes p &\mapsto (0 + n) \otimes p. \end{aligned}$$

Estos dos homomorfismos definen un homomorfismo

$$\begin{aligned} g : (M \otimes_R P) \oplus (N \otimes_R P) &\to (M \oplus N) \otimes_R P \\ m \otimes p + n \otimes p' &\mapsto g_1(m \otimes p) + g_2(n \otimes p'), \end{aligned}$$

que es claramente el inverso de f, lo que prueba que esta última es un isomorfismo. □

Ejercicio. Verifique la bilinealidad de las funciones φ de la demostración.

Ejemplo 3.2.7. Sea K un cuerpo. Entonces $K[x] \otimes_K K[y]$ es isomorfo a $K[x, y]$. En efecto, consideremos la función $\varphi : K[x] \times K[y] \to K[x, y]$ dada por la multiplicación

de polinomios. Esta función es claramente K-bilineal, por lo que le corresponde una función K-lineal

$$\begin{aligned} f : K[x] \otimes_K K[y] &\to K[x,y] \\ P(x) \otimes Q(y) &\to P(x)Q(y) \end{aligned}$$

Bastará entonces con encontrar una inversa de esta función. Como todo polinomio en $K[x,y]$ se escribe de la forma $\sum_{0\leq i,j\leq n} a_{ij}x^iy^j$, podemos considerar la función

$$\begin{aligned} g : K[x,y] &\to K[x] \otimes_K K[y] \\ \sum_{0\leq i,j\leq n} a_{ij}x^iy^j &\sum_{0\leq i,j\leq n} a_{ij}x^i \otimes y^j. \end{aligned}$$

Está claro entonces que $f\circ g = \mathrm{id}_{K[x,y]}$, mientras que, si escribimos $P(x) = \sum_{i=0}^n b_i x^i$ y $Q(y) = \sum_{j=0}^n c_j y^j$, tenemos entonces por K-bilinealidad que

$$P(x) \otimes Q(y) = \left(\sum_{i=0}^n b_i x^i\right) \otimes \left(\sum_{j=0}^n c_j y^j\right) = \sum_{1\leq i,j\leq n} b_i c_j (x^i \otimes y^j),$$

lo que nos permite comprobar fácilmente que $g \circ f = \mathrm{id}_{K[x]\otimes_K K[y]}$.

Pasemos entonces finalmente a la existencia del producto tensorial.

Teorema 3.2.8. *Sean M, N dos R-módulos. Entonces existe un (único) producto tensorial $(M \otimes_R N, \varphi)$ de M y N.*

Demostración. Consideremos el R-módulo libre de base $M \times N$, es decir:

$$R^{(M\times N)} = \left\{ \sum_{(x,y)\in M\times N} r_{(x,y)}(x,y) \mid r_{(x,y)} \in R, \text{ suma finita} \right\}$$

Consideremos ahora el subconjunto S de $R^{(M\times N)}$ de *todos* elementos de la forma

- $(x+x',y) - (x,y) - (x',y)$ con $x, x' \in M$ e $y \in N$, o bien
- $(x,y+y') - (x,y) - (x,y')$ con $x \in M$ e $y, y' \in N$, o bien
- $r(x,y) - (rx,y)$ con $r \in R$, $x \in M$ e $y \in N$, o bien
- $r(x,y) - (x,ry)$ con $r \in R$, $x \in M$ e $y \in N$.

Sea T el submódulo de $R^{(M\times N)}$ generado por S, definamos

$$M \otimes_R N := R^{(M\times N)}/T,$$

y denotemos por $\pi : R^{(M\times N)} \to M \otimes_R N$ la proyección canónica. Consideremos finalmente la aplicación $\iota : M \times N \to R^{(M\times N)}$ que al par (x, y) le asocia el elemento $(x, y) \in R^{(M\times N)}$ (es decir, $r_{(x,y)} = 1$ y $r_{(x',y')} = 0$ para $(x', y') \neq (x, y)$) y definamos $\varphi := \pi \circ \iota$.

Debemos probar que $(M \otimes_R N, \varphi)$, tal y como lo hemos definido, es un producto tensorial de M y N.

Comencemos pues con la bilinealidad de $\varphi : M \times N \to M \otimes_R N$. Sean $x, x' \in M$, $y, y' \in N$ y $r \in R$. Entonces

$$\varphi(x + rx', y) = \pi(\iota(x + rx', y)) = \pi((x + rx', y)),$$

pero como $(x+x', y)-(x, y)-(x', y) \in S \subset P$, tenemos que $\pi((x+rx', y)-(x, y)-(rx', y)) = 0$, por lo que, por R-linealidad de π,

$$\pi((x + rx', y)) = \pi((x, y)) + \pi(rx', y).$$

De la misma manera, como $r(x', y) - (rx', y) \in S \subset P$, tenemos que

$$r\pi((x', y)) = \pi((rx', y)),$$

y por lo tanto

$$\varphi(x + rx', y) = \pi((x + rx', y)) = \pi((x, y)) + r\pi(x', y).$$

La linealidad por la derecha se prueba exactamente de la misma manera, usando los dos generadores de T que no hemos usado aún.

Veamos ahora la propiedad universal. Para todo elemento $(x, y) \in R^{(M\times N)}$, denotemos por $x \otimes y$ el elemento $\pi((x, y)) \in M \otimes_R N$. Está claro entonces que el R-módulo $M \otimes_R N$ está generado por el conjunto $\{x \otimes y \mid x \in M,\ y \in N\}$.

Sea P un R-módulo y $\psi : M \times N \to P$ una aplicación R-bilineal. Intentemos primero definir una función R-lineal $h : R^{(M\times N)} \to P$ a partir de ψ. Para esto, basta con definir la imágen de la base y extender por R-linealidad ya que se trata de un módulo libre. Definamos entonces h de forma que $h((x, y)) := \psi(x, y)$. Nótese que tenemos en particular $h \circ \iota = \psi$.

Consideremos ahora un elemento de la forma $\alpha_1 = (x+x', y)-(x, y)-(x', y) \in S \subset T = \ker(\pi)$. Vemos entonces que, por la R-bilinealidad de ψ,

$$h(\alpha_1) = h((x+x', y))-h((x, y))-h((x', y)) = \psi(x+x', y)-\psi(x, y)-\psi(x', y) = 0.$$

De la misma manera, para $\alpha_2, \alpha_3, \alpha_4 \in T$ respectivamente de las 3 formas restantes en S, tenemos que

$$h(\alpha_2) = h((x, y+y')) - h((x,y)) - h((x,y')) = \psi(x, y+y') - \psi(x,y) - \psi(x,y') = 0,$$
$$h(\alpha_3) = rh((x,y)) - h((rx,y)) = r\psi(x,y) - \psi(rx,y) = 0,$$
$$h(\alpha_4) = rh((x,y)) - h((x,ry)) = r\psi(x,y) - \psi(x,ry) = 0.$$

Como S genera a T como R-módulo, vemos entonces que $T = \ker(\pi) \subset \ker(h)$. La propiedad universal del cociente (Proposición 3.1.19, en su versión para módulos) nos dice entonces que existe una única función R-lineal $f : M \otimes_R N \to P$ tal que $h = f \circ \pi$. Tenemos entonces que

$$\psi = h \circ \iota = f \circ \pi \circ \iota = f \circ \varphi,$$

lo que prueba la parte existencial de la propiedad universal.

Para probar la unicidad, si suponemos que $f' : M \otimes_R N \to P$ es otra función R-lineal que cumple $\psi = f' \circ \varphi$, entonces $f' \circ \pi \circ \iota = f' \circ \pi \circ \iota$, lo que implica que $f' \circ \pi$ y $f \circ \pi$ coinciden en la imagen de ι. Pero la imagen de ι son los generadores de $R^{(M \times N)}$, por lo que $f' \circ \pi = f \circ \pi$. La unicidad de la propiedad universal del cociente nos dice entonces que $f' = f$. □

Nótese que en el caso en que el anillo R es un cuerpo K, el producto tensorial es una herramienta que construye un K-espacio vectorial $V \otimes_K W$ a partir de dos K-espacios vectoriales V y W. Cabe preguntarse qué podemos decir de las dimensiones de éste nuevo espacio y si podemos encontrar una K-base de éste a partir de K-bases de V y W. Concluyamos pues esta subsección con resultados en esta dirección.

Proposición 3.2.9. *Sea K un cuerpo y sean V, W dos K-módulos. Sea I un conjunto finito y sean $\{v_i\}_{i \in I}$ elementos de V y $\{w_i\}_{i \in I}$ elementos de W. Supongamos que los elementos $\{w_i\}_{i \in I}$ son K-linealmente independientes. Entonces*

$$\sum_{i \in I} v_i \otimes w_i = 0 \in V \otimes_K W \;\Rightarrow\; v_i = 0 \quad \forall\, i \in I.$$

Demostración. Supongamos que $v_t \neq 0$ para algún $t \in I$. Sea $f : V \to K$ una función K-lineal tal que $f(v_t) \neq 0$. Sea $g : W \to K$ una aplicación K-lineal tal que $g(w_t) \neq 0$ y $g(w_i) = 0$ para todo $i \neq t$. Consideremos entonces la aplicación K-bilineal $\psi : V \times W \to K$ definida por $\psi(v,w) := f(v)g(w)$ para $v \in V$ y $w \in W$. La propiedad universal del producto tensorial nos dice entonces que existe una única aplicación K-lineal $h : V \otimes_K W \to K$ tal que $h(v \otimes w) = f(v)g(w)$ para $v \in V$ y $w \in W$. Por lo tanto, como $g(w_i) = 0$ para todo $i \neq t$,

$$0 = h(0) = h\left(\sum_{i \in I} v_i \otimes w_i\right) = \sum_{i \in I} h(v_i \otimes w_i) = \sum_{i \in I} f(v_i)g(w_i) = f(v_t)g(w_t) \neq 0,$$

ya que $f(v_t) \neq 0$ y $g(w_t) \neq 0$. Esto es una contradicción, por lo que $a_i = 0$ para todo $i \in I$. □

Corolario 3.2.10. *Sea K un cuerpo y sean V, W dos K-módulos. Sean $\{v_i\}_{i\in I}$ una K-base de V y $\{w_j\}_{j\in J}$ una K-base de W. Entonces una K-base de $V \otimes_K W$ está dada por los $\{v_i \otimes w_j\}_{i\in I,\, j\in J}$.*

Demostración. De la construcción de $V \otimes_K W$, sabemos que los $\{v_i \otimes w_j\}_{i\in I,\, j\in J}$ son un conjunto generador, por lo que bastará con probar que son K-linealmente independientes. Consideremos entonces una combinación lineal nula

$$\sum_{i\in I,\, j\in J} \lambda_{i,j} v_i \otimes w_j = 0,$$

y notemos que

$$\sum_{i\in I,\, j\in J} \lambda_{i,j} v_i \otimes w_j = \sum_{j\in J} \sum_{i\in I} \lambda_{i,j} v_i \otimes w_j = \sum_{j\in J} \left(\sum_{i\in I} \lambda_{i,j} v_i \right) \otimes w_j,$$

por lo que la Proposición anterior nos dice que $\sum_{i\in I} \lambda_{i,j} v_i = 0$ para todo $j \in J$. Como los v_i son K-linealmente independientes, esto implica que $\lambda_{i,j} = 0$ para todo $i \in I$ y $j \in J$, lo que prueba que los $\{v_i \otimes w_j\}_{i\in I,\, j\in J}$ son K-linealmente independientes. □

3.2.2. Producto tensorial de álgebras

Dado que toda R-álgebra es un R-módulo, podemos imaginar fácilmente lo que debe ser un producto tensorial de álgebras como R-módulo. La pregunta es si este nuevo módulo cuenta con una multiplicación natural deducible a partir de las multiplicaciones de las dos álgebras involucradas. De esto trata la siguiente proposición.

Proposición 3.2.11. *Sean A, B dos R-álgebras y sea $A \otimes_R B$ el producto tensorial de los R-módulos A y B. Entonces existe una única aplicación R-bilineal*

$$m : (A \otimes_R B) \times (A \otimes_R B) \to (A \otimes_R B)$$

tal que

$$m(a \otimes b, a' \otimes b') = aa' \otimes bb' \quad \forall, a, a' \in A,\, b, b' \in B.$$

Demostración. Sean $a' \in A$ y $b' \in B$ y definamos la función R-bilineal

$$\begin{aligned} \psi_{a',b'} : A \times B &\to A \otimes_R B, \\ (a, b) &\mapsto aa' \otimes bb'. \end{aligned}$$

La R-bilinealidad se deduce inmediatamente de las propiedades de los elementos de $A \otimes_R B$ y de la R-bilinealidad de las multiplicaciones en A y B. La propiedad universal del producto tensorial nos dice entonces que existe una única aplicación R-lineal $f_{a',b'} : A \otimes_R B \to A \otimes_R B$ tal que, para todo $a \in A$ y $b \in B$,

$$f_{a',b'}(a \otimes b) = \psi_{a',b'}(a, b) = aa' \otimes bb'.$$

Ahora, usando nuevamente las propiedades de los elementos de $A \otimes_R B$ y la R-bilinealidad de las multiplicaciones en A y B, vemos que, para todo $a', a'' \in A$, $b', b'' \in B$ y $r \in R$,

$$\begin{aligned} f_{a'+a'',b'} &= f_{a',b'} + f_{a'',b'}, \\ f_{a',b'+b''} &= f_{a',b'} + f_{a',b''}, \\ f_{ra',b'} &= r f_{a',b'} = f_{a',rb'} \end{aligned}$$

En otras palabras, tenemos una aplicación R-bilineal dada por

$$\phi : A \times B \to \mathrm{Hom}_R(A \otimes_R B, A \otimes_R B), (a', b') \qquad \mapsto f_{a',b'}$$

Usando la propiedad universal del producto tensorial nuevamente, vemos que existe una única función R-lineal

$$g : A \otimes_R B \to \mathrm{Hom}_R(A \otimes_R B, A \otimes_R B),$$

tal que $g(a' \otimes b') = \phi(a', b') = f_{a',b'}$ para todo $a' \in A$ y $b' \in B$. Recordando que tenemos un isomorfismo natural entre

$$\mathrm{Hom}_R(A \otimes_R B, \mathrm{Hom}_R(A \otimes_R B, A \otimes_R B)) \quad \text{y} \quad \mathrm{Bil}_R(A \otimes_R B, A \otimes_R B; A \otimes_R B),$$

vemos que a g le corresponde una única función R-bilineal

$$m : (A \otimes_R B) \times (A \otimes_R B) \to (A \otimes_R B),$$

tal que, para todo $a, a' \in A$ y $b, b' \in B$,

$$m(a \otimes b, a' \otimes b') := f_{a',b'}(a \otimes b) = aa' \otimes bb'.$$

□

Así, el módulo $A \otimes_R B$ provisto de esta nueva aplicación m es un R-álgebra. Pero además tenemos que

Proposición 3.2.12. *Sean A, B dos R-álgebras.*

- *Si A y B son asociativas, entonces $A \otimes_R B$ es asociativa.*
- *Si A y B son conmutativas, entonces $A \otimes_R B$ es conmutativas.*
- *Si A y B son unitarias, entonces $A \otimes_R B$ es unitaria y $1_{A \otimes_R B} = 1_A \otimes 1_B$.*

Demostración. ¡Ejercicio! □

Ejercicio. Sea K un cuerpo y sea A una K-álgebra unitaria. Demuestre que existe un isomorfismo de K-álgebras $M_n(K) \otimes_K A \simeq M_n(A)$.

3.2.3. Aplicaciones multilineales y productos tensoriales iterados

Ya vimos en la Proposición 3.2.6 que, dados tres R-módulos M, N, P, podemos formar el triple producto tensorial $M \otimes_R N \otimes_R P$ simplemente como $(M \otimes_R N) \otimes_R P$ o bien como $M \otimes_R (N \otimes_R P)$, ya que ambos son canónicamente isomorfos. Es más, dado que $M \otimes_R N$ es canónicamente isomorfo a $N \otimes_R M$, podemos reordenar los tres módulos de cualquier manera y obtener siempre isomorfismos canónicos entre todos estos objetos. Esto apunta hacia la idea de que el objeto $M \otimes_R N \otimes_R P$ verifica una cierta propiedad universal que no depende del orden de M, N y P. Esto se generaliza a n módulos sin dificultad y el término clave es la siguiente definición.

Definición 3.2.13. Sean $M_1, \ldots, M_n, P$ R-módulos. Decimos que una aplicación

$$\psi : M_1 \times \cdots \times M_n \to P,$$

es *R-n-lineal* (o *R-multilineal* si n está subentendido) si, para todo $1 \leq i \leq n$ y para todo $m_i, m_i' \in M_i$ y $r \in R$, tenemos que

$$\begin{aligned}&\psi(m_1, \ldots, m_{i-1}, m_i + rm_i', m_{i+1}, \ldots, m_n) = \\ &\quad = \psi(m_1, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_n) + r\psi(m_1, \ldots, m_{i-1}, m_i', m_{i+1}, \ldots, m_n).\end{aligned}$$

Ejemplo 3.2.14. Sea R^n el módulo libre de rango n y consideremos sus elementos $x \in R^n$ como vectores columna. Entonces podemos ver los elementos $(x_1, \ldots, x_n) \in R^n \times \cdots \times R^n$ como matrices $A \in M_n(R)$. Entonces la aplicación determinante

$$\det : R^n \times \cdots \times R^n \to R : A \mapsto \det(A),$$

es R-n-lineal.

De la misma manera en que el producto tensorial de dos módulos factoriza las aplicaciones bilineales, tenemos entonces que el producto tensorial de n módulos factoriza las aplicaciones n-lineales vía la misma propiedad universal:

Teorema 3.2.15. *Sean $M_1, \ldots, M_n$ R-módulos, sea*

$$T = M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_n,$$

y sea $\varphi : M_1 \times \cdots M_n \to T$ la aplicación R-n-lineal obtenida por la iteración de productos tensoriales

$$M_1 \otimes_R (M_2 \otimes_R (\cdots \otimes_R (M_{n-1} \otimes_R M_n))).$$

Entonces, para todo R-módulo P y para toda aplicación R-n-lineal $\psi : M_1 \times \cdots \times M_n \to P$ existe una única *función R-lineal $f : T \to P$ tal que $f \circ \varphi = \psi$, es decir, el diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} M_1 \times \cdots \times M_n & \xrightarrow{\psi} & P\,. \\ {\scriptstyle\varphi}\big\downarrow & \nearrow_{\exists!\, f} & \\ T & & \end{array}$$

Observación.
Como los objetos que verifican una propiedad universal son siempre únicos salvo único isomorfismo, vemos que si hubiésemos escogido otra aplicación φ construida con otro orden de productos tensoriales, habríamos encontrado la misma aplicación luego de identificar los dos productos tensoriales (i.e. luego de "eliminar los paréntesis").

En particular, la multilinealidad de φ queda entonces expresada por la siguiente propiedad:

$$m_1 \otimes \cdots \otimes (m_i + r m_i') \otimes \cdots \otimes m_n = m_1 \otimes \cdots \otimes m_i \otimes \cdots \otimes m_n + r(m_1 \otimes \cdots \otimes m_i' \otimes \cdots \otimes m_n),$$

para todo $r \in R$, todo $m_j \in M_j$ con $j \neq i$, todo $m_i, m_i' \in M_i$ y todo $1 \leq i \leq n$. Además, todo elemento $t \in M_1 \otimes_R \cdots \otimes_R M_n$ se escribe de la forma

$$t = \sum_{j=1}^{\ell} m_{1j} \otimes \cdots \otimes m_{nj}.$$

Demostración. La demostración de este teorema es por inducción sobre n partiendo con $n = 2$, para el cual ya demostramos esta propiedad universal (nótese que 2-lineal es lo mismo que bilineal).

Supongamos entonces que el teorema es cierto para $n-1$ e intentemos demostrarlo para n. Tenemos que $T = M_1 \otimes_R T_0$ con

$$T_0 = M_2 \otimes_R M_3 \otimes_R \cdots \otimes_R M_n,$$

y éste módulo viene equipado con una aplicación natural $\varphi_0 : M_2 \times \cdots \times M_n \to T_0$, la cual verifica la propiedad universal para aplicaciones R-multilineales por hipótesis de inducción (los paréntesis pueden ser eliminados dada la observación anterior).

Sea entonces P un R-módulo y $\psi : M_1 \times \cdots \times M_n \to P$ una aplicación R-n-lineal. Sea $m_1 \in M_1$ y consideremos la inclusión

$$\begin{aligned} \iota_{m_1} : M_2 \times \cdots \times M_n &\to M_1 \times \cdots \times M_n \\ (m_2, \ldots, m_n) &\mapsto (m_1, m_2, \ldots, m_n). \end{aligned}$$

Vemos entonces que la composición $\psi \circ \iota_{m_1}$ es una aplicación R-$(n-1)$-lineal por la multilinealidad de ψ. La propiedad universal de (T_0, φ_0) nos dice entonces que existe una única aplicación R-lineal $f_{m_1} : T_0 \to P$ tal que $\psi_{m_1} \circ \varphi_0 = \psi \circ \iota_{m_1}$, es decir

$$\begin{aligned} f_{m_1} : T_0 = M_2 \otimes_R \cdots \otimes_R M_n &\to P \\ m_2 \otimes \cdots \otimes m_n &\mapsto \psi(m_1, m_2, \ldots, m_n). \end{aligned}$$

Con esto podemos definir una función R-bilineal de la siguiente manera:

$$\begin{aligned} \psi_0 : M_1 \times T_0 &\to P \\ (m_1, m_2 \otimes \cdots \otimes m_n) &\mapsto \psi(m_1, m_2, \ldots, m_n), \end{aligned}$$

es decir $\psi_0(m_1, t_0) = f_{m_1}(t_0)$. La R-linealidad por la izquierda viene de la R-multilinealidad de ψ y por la derecha corresponde a la R-linealidad de los f_{m_1}. La propiedad universal del producto tensorial nos dice que existe una única aplicación R-lineal $f : T = M_1 \otimes_R T_0 \to P$ tal que $f \circ \varphi_1 = \psi_0$, donde φ_1 es la aplicación canónica $M_1 \times T_0 \to M_1 \otimes_R T_0$. Notemos ahora que tenemos un diagrama conmutativo:

$$\begin{array}{ccc} M_1 \times \cdots \times M_n & \xrightarrow{\mathrm{id} \times \varphi_0} & M_1 \times T_0 \\ & {\scriptstyle \varphi} \searrow \quad \swarrow {\scriptstyle \varphi_1} & \\ & T & \end{array}$$

ya que por ambos lados un elemento $(m_1, \ldots, m_n) \in M_1 \times \cdots \times M_n$ va a parar a $m_1 \otimes \cdots \otimes m_n \in T$. Vemos entonces que

$$f \circ \varphi = f \circ \varphi_1 \circ (\mathrm{id} \times \varphi_0) = \psi_0 \circ (\mathrm{id} \times \varphi_0) = \psi,$$

lo que prueba la existencia de f. La unicidad se deduce de la unicidad de ψ_0, la cual es única ya que está definida por los f_{m_1} y éstos son únicos también para cada $m_1 \in M_1$. □

3.3. Álgebra Tensorial $T(M)$ de un R-módulo M

Si consideramos un R-módulo M, cabe preguntarse si éste admite alguna estructura multiplicativa interesante. En el marco de espacios vectoriales esto corresponde a definir una multiplicación entre vectores. Ahora, la función que a dos elementos $m, n \in M$ asocia el elemento $m \otimes n$ tiene las propiedades que uno esperaría de una tal mulitplicación. El único obstáculo es que ¡$m \otimes n$ no es un elemento de M! Esto sin embargo no debe desalentarnos, ya que basta con "agregar" $M \otimes_R M$ al módulo M para que esta multiplicación tenga sentido. Pero ahora nos falta entonces definir una mutiplicación en $M \otimes_R M$ y así...

Este problema que aparentemente se repite hasta el infinito puede ser resuelto con una suma directa (¡infinita!). Y es de esto precisamente que se trata la construcción del álgebra tensorial $T(M)$. Pero veamos antes unas definiciones de orden teórico.

Definición 3.3.1. Un anillo S es un *anillo graduado* si se le puede escribir como una suma directa de subgrupos aditivos de la siguiente manera

$$S = \bigoplus_{n=0}^{\infty} S_n,$$

de forma que $S_i S_j \subset S_{i+j}$ (donde $AB := \{ab \mid a \in A,\, b \in B\}$). Los elementos de S_n se dicen *homogéneos de grado* n y S_n se llama la *componente homogénea* de S de grado n.

Un ideal I de un anillo graduado S se dice *ideal graduado* si $I = \bigoplus_{n=0}^{\infty}(I \cap S_n)$. Un *homomorfismo de anillos graduados* es un homomorfismo de anillos $\varphi : S \longrightarrow T$ que respeta las graduaciones de S y de T, es decir, $\varphi(S_n) \subset T_n$ para todo $n \in \mathbb{N}$.

Observación.
Nótese que $S_0 S_0 \subset S_0$, por lo que S_0 es un subanillo del anillo graduado S y S es un S_0-módulo. Si además S es unitario, entonces claramente $1_S \in S_0$. Por lo tanto, si S_0 está en el centro de S, entonces S es una S_0-álgebra.

Nótese también que todo ideal graduado I de S es un subanillo graduado sencillamente definiendo I_n como $I \cap S_n$.

Ejemplo 3.3.2. Sea R un anillo. Entonces el anillo de polinomios $S = R[x]$ es un anillo graduado y S_n corresponde a los monomios de grado n.

La noción de ideal graduado permite definir cocientes graduados, como lo prueba la siguiente proposición.

Proposición 3.3.3. *Sea S un anillo graduado y sea I un ideal graduado de S. Entonces S/I es un anillo graduado cuya componente de grado n es isomorfa a S_n/I_n.*

Demostración. Nótese que cada S_n es un S_0-módulo y que cada I_n es un respectivo S_0-submódulo. Esto nos dice que, como S_0-módulos

$$S/I = \left(\bigoplus_{n=0}^{\infty} S_n\right) / \left(\bigoplus_{n=0}^{\infty} I_n\right) \simeq \bigoplus_{n=0}^{\infty} S_n/I_n.$$

Ahora, como la multiplicación de S/I está definida a partir de la multiplicación de S, vemos claramente que, si denotamos por π la proyección canónica $S \to S/I$,

$$(S_i/I_i)(S_j/I_j) = \pi(S_i)\pi(S_j) = \pi(S_i S_j) \subset \pi(S_{i+j}) = S_{i+j}/I_{i+j}.$$

□

Demostremos ahora un lema que nos será útil en las construcciones de más abajo.

Lema 3.3.4. *Sea S un anillo graduado y sea I un ideal generado por elementos homogéneos. Entonces I es un ideal graduado.*

Demostración. Debemos demostrar que $I = \bigoplus_{n=0}^{\infty} I \cap S_n$. La contención $\supset$ es evidente, por lo que bastará con demostrar la contención $\subset$. Sea entonces $a \in I$, el cual podemos escribir como $a = \sum_{i=0}^{t} a_i$ con $a_i \in S_i$ para cierto $t \in \mathbb{N}$. Debemos probar que $a_i \in I$ para cada $0 \leq i \leq \ell$.

Ahora, como $a \in I$ e I está generado por elementos homogéneos, tenemos que existen $b_j, c_j \in S$ y $r \in \mathbb{N}$ tales que $a = \sum_{j=1}^{r} b_j e_j c_j$ con e_j homogéneo. Escribamos $b_j = \sum_{k=0}^{s} b_{jk}$ y $c_j = \sum_{k=0}^{s} c_{jk}$ con $b_{jk}, c_{jk} \in S_k$, de forma que

$$a = \sum_{j=1}^{r} \sum_{k=0}^{s} \sum_{\ell=0}^{s} b_{jk} e_j c_{j\ell}.$$

Dado que $S_i S_j \subset S_{i+j}$ y los $b_{jk}, c_{j\ell}$ y e_j son homogéneos, vemos entonces que, si denotamos por $d_j \geq 0$ el grado de e_j,

$$a_i = \sum_{j=1}^{r} \sum_{k=0}^{i-d_j} b_{jk} e_j c_{j(i-d_j-k)},$$

lo que prueba que $a_i \in I$ y por ende I es un ideal graduado. □

El álgebra tensorial $T(M)$ de un R-módulo M es otro ejemplo de anillo graduado, el cual definimos a continuación.

Definición 3.3.5. Para M un R-módulo y $k \in \mathbb{N}$ un entero, definimos $T^k(M)$ como el producto tensorial iterado de k copias de M, es decir

$$T^k(M) := \underbrace{M \otimes_R M \otimes_R \cdots \otimes_R M}_{k \text{ veces}}.$$

En particular, para $k = 1$ tenemos $T^1(M) = M$ y definimos también $T^0(M) = R$. Los elementos de $T^k(M)$ se llaman *k-tensores*.

Definimos el *álgebra tensorial* $T(M)$ de M como el R-módulo

$$T(M) = \bigoplus_{k=0}^{\infty} T^k(M) = R \oplus M \oplus (M \otimes_R M) \otimes \cdots,$$

equipado con la siguiente multiplicación $T(M) \times T(M) \to T(M)$. Si $k, \ell \in \mathbb{N}$, usamos el producto tensorial $\otimes$, es decir

$$(m_1 \otimes \cdots \otimes m_k) \cdot (m'_1 \otimes \cdots \otimes m'_\ell) := m_1 \otimes \cdots \otimes m_k \otimes m'_1 \otimes \cdots \otimes m'_\ell.$$

Y si $k = 0$ ó $\ell = 0$, entonces usamos la multiplicación por escalar (recuerde que $T^0(M) = R$). Luego extendemos por linealidad para sumas finitas. Por último, identificamos a M con el submódulo $T^1(M)$ de $T(M)$.

Observación.
Sea V un espacio vectorial de dimensión n sobre un cuerpo K con base $B = \{v_1, \ldots, v_n\}$. Entonces los k-tensores $v_{i1} \otimes v_{i2} \otimes \cdots \otimes v_{ik}$ con $v_{ij} \in B$ forman una K-base de $T^k(V)$. En particular, $\dim_K(T^k(V)) = n^k$.

Teorema 3.3.6. *La multiplicación en $T(M)$ definida acá arriba está bien definida y el álgebra $T(M)$ verifica la siguiente propiedad universal:*

Sea A una R-álgebra unitaria y sea $f : M \to A$ un homomorfismo de R-módulos. Entonces existe un único homomorfismo de R-álgebras unitarias $\phi : T(M) \to A$ tal que $\phi|_M = f$.

Observación.
Como $T(M)$ está definido como una suma directa, todo elemento es una suma finita de tensores, pero éstos no tienen porqué ser del mismo largo. Por ejemplo, un elemento de $T(M)$ es $r + m_1 + m_2 \otimes m_3 \otimes m_4$.

En particular, tenemos que $1_{T(M)} = 1_R \in T^0(M) \subset T(M)$ y por ende $T(M)$ es un álgebra unitaria. También es un álgebra asociativa, como se ve claramente de la definición de su producto. Sin embargo, no tiene ninguna razón a priori para ser conmutativa (véase los ejemplos más abajo).

Demostración. Notemos que, como $T(M)$ es una suma directa, entonces

$$T(M) \times T(M) = \bigoplus_{k,\ell \in \mathbb{Z}_{\geq 0}} T^k(M) \times T^\ell(M),$$

por lo que bastará con probar que la multiplicación está bien definida y es R-bilineal sobre los sumandos $T^k(M) \times T^\ell(M)$, ya que luego la extendemos por linealidad para sumas finitas. Esto es evidente para el par $(k, \ell) = (0, 0)$ ya que se trata de la multiplicación en R. Sean entonces $k, \ell \in \mathbb{Z}_{\geq 0}$ con $\ell > 0$ y fijemos un elemento $t \in T^k(M)$. Consideremos la aplicación ℓ-lineal

$$\begin{aligned} \varphi_{t,\ell} : M^\ell &\to T^{k+\ell}(M), \\ (m_1, \ldots, m_\ell) &\mapsto t \otimes m_1 \otimes \cdots \otimes m_\ell, \end{aligned}$$

donde el primer $\otimes$ puede ser omitido si $k = 0$. La propiedad universal del producto tensorial nos dice entonces que existe una única aplicación R-lineal

$$\begin{aligned} f_{t,\ell} : T^\ell(M) &\to T^{k+\ell}(M), \\ t_1 = m_1 \otimes \cdots \otimes m_\ell &\mapsto t \otimes t_1 = t \otimes m_1 \otimes \cdots \otimes m_\ell. \end{aligned}$$

Esto prueba que la multiplicación por la derecha es R-lineal. Invirtiendo k y ℓ, el mismo argumento prueba que es R-lineal por la izquierda, por ende R-bilineal.

Probemos ahora la propiedad universal. Sea $f : M \to A$ un homomorfismo de R-módulos y sea $k \in \mathbb{Z}_{\geq 0}$. Definiremos homomorfismos de R-módulos $f_k : T^k(M) \to A$ como sigue:

Para $k = 0$, definimos $f_0 : T^0(M) \to A$ usando el homomorfismo natural $R \to A$ dado por la estructura de álgebra de A, es decir $r \mapsto r \cdot 1_A$.

Para $k = 1$, definimos $f_1 : T^1(M) \to A$ sencillamente como $f_1 = f$ ya que $T^1(M) = M$.

Para $k \geq 2$, consideramos la aplicación $\varphi_k : M^k \to A$ dada por $\varphi(m_1, \ldots, m_k) = f(m_1) \cdots f(m_n)$. Esta aplicación es claramente R-k-lineal ya que f es R-lineal y la multiplicación de A es R-bilineal (y por ende R-k-lineal si la iteramos). La propiedad universal del producto tensorial nos dice entonces que existe una única aplicación lineal $f_k : T^k(M) \to A$ tal que $f_k(m_1 \otimes \cdots \otimes m_k) = f(m_1) \cdots f(m_k)$.

Definamos entonces $\phi : T(M) \to A$ como el homomorfismo dado por los f_k con $k \geq 0$. Vemos que

$$\phi(m_1 \otimes \cdots \otimes m_k) = f_k(m_1 \otimes \cdots \otimes m_k) = f(m_1) \cdots f(m_k) = \phi(m_1) \cdots \phi(m_k),$$

por lo que ϕ es una aplicación que respeta la multiplicación y la suma. La definición de f_0 asegura también que ϕ respeta la multiplicación por escalares. Es además la igualdad de acá arriba la que asegura la unicidad de $\varphi|_{T^k(M)}$ para $k \geq 2$ ya que las f_k son las únicas que verifican esta igualdad. Para $k = 1$ es la condición $\varphi|_M = f$ que asegura la unicidad de $\varphi|_{T^1(M)}$ y para $k = 0$ tenemos que todo homomorfismo de álgebras debe enviar $1_{T(M)}$ a 1_A, lo que asegura que $\varphi|_{T^0(M)}$ es el homomorfismo natural $R \to A$ por R-linealidad. □

La observación que hicimos sobre la base de $T^k(V)$ para V un K-espacio vectorial se generalizan en realidad a todo R-módulo libre.

Ejemplo 3.3.7. Sea M un R-módulo libre de base $\{e_1, e_2\}$. Entonces $T(M)$ es un módulo libre de rango infinito y de base

$$\{1,\ e_1,\ e_2,\ e_1 \otimes e_1,\ e_1 \otimes e_2,\ e_2 \otimes e_1,\ e_2 \otimes e_2,\ e_1 \otimes e_1 \otimes e_1,\ e_1 \otimes e_1 \otimes e_2,\ e_1 \otimes e_2 \otimes e_1,$$
$$e_1 \otimes e_2 \otimes e_2,\ e_2 \otimes e_1 \otimes e_1,\ e_2 \otimes e_1 \otimes e_2,\ e_2 \otimes e_2 \otimes e_1,\ e_2 \otimes e_2 \otimes e_2,\ \text{etc.}\}$$

Ejemplo 3.3.8. Sea R un anillo conmutativo y unitario. Definimos el álgebra de polinomios no conmutativos en n variables $R\{x_1, \ldots, x_n\}$ como las sumas finitas de monomios en las variables $x_1, \ldots, x_n$, las cuales *no conmutan*, es decir, $x_i x_j \neq x_j x_i$ si $i \neq j$.

Esta álgebra es isomorfa al álgebra $T(M)$ para el módulo libre $M = R^n$. En efecto, si denotamos una base de M como $\{e_1, \ldots, e_n\}$, entonces tenemos un isomorfismo $\varphi : T(M) \to R\{x_1, \ldots, x_n\}$ definido por $\varphi(e_{i_1} \otimes \cdots \otimes e_{i_k}) \mapsto x_{i_1} \cdots x_{i_k}$. En particular, la base de $R\{x_1, x_2\}$ está formada por los monomios

$$1,\ x_1,\ x_2,\ x_1^2,\ x_1x_2,\ x_2x_1,\ x_2^2,\ x_1^3,\ x_1^2x_2,\ x_1x_2x_1,\ x_1x_2^2,\ x_2x_1^2,\ x_2x_1x_2,\ x_2^2x_1,\ x_2^3,\ \text{etc.}$$

Ejercicio. Sea R un anillo conmutativo y unitario, I un ideal de R y M el R-módulo R/I. Pruebe que $T(M)/I$ es isomorfo al álgebra de polinomios $R/I[x]$.

Ejercicio. Sea M un R-módulo. Pruebe que $T(M)$ está generada como R-álgebra por $T^1(M)$, es decir, por los $m \in M$.

3.4. Álgebra Simétrica $S(M)$ de un R-módulo M .

Ya vimos que el álgebra tensorial $T(M)$ nos permite fabricar un álgebra de polinomios no conmutativos, los cuales resultan coincidir con los polinomios habituales cuando trabajamos con una sola variable. Cabe preguntarse entonces si no tendremos alguna construcción tensorial que permita encontrar el álgebra de polinomios clásica en lugar de esta versión no conmutativa. Para esto, necesitamos "que $m \otimes n$ sea igual a $n \otimes m$" en algún sentido.

Basta entonces con recordar cómo construimos el producto tensorial cuando probamos su existencia. Tomamos el módulo generado por todos los objetos que nos interesaba tener (i.e. los $m \otimes n$) y luego cocientábamos por elementos que aseguraran las igualdades que necesitábamos (que corresponden a la biliniealidad de los tensores). Ahora, gracias a $T(M)$, tenemos elementos que parecen polinomios, pero que no conmutan. ¡Hagámoslos conmutar pues!

Definición 3.4.1. Sea M un R-módulo. Definimos el *álgebra simétrica* $S(M)$ de M como el cociente $T(M)/C(M)$, donde $C(M)$ es el ideal de $T(M)$ generado por los elementos de la forma $m \otimes n - n \otimes m$ para $m, n \in M$.

Llamamos la *k-ésima potencia simétrica* de M al submódulo $S^k(M)$ de $S(M)$ definido como la imagen de $T^k(M)$.

Notación. El producto en $S(M)$ es denotado de la forma clásica (i.e. sin símbolo alguno). En particular, la imagen de $m_1 \otimes m_2 \otimes \cdots \otimes m_n$ en $S(M)$ es denotada por $m_1 m_2 \cdots m_n$.

Recordemos que $T(M)$ es una R-álgebra asociativa, por lo que es en particular un anillo, lo que nos permite hablar sin problemas del ideal generado por un subconjunto.

Verifiquemos ahora que una tal construcción tiene las propiedades esperadas.

Proposición 3.4.2. *El álgebra simétrica $S(M)$ es conmutativa y graduada. Su componente de grado k es $S^k(M)$. Además, $S^0(M) = R$ y $S^1(M) = M$.*

Demostración. Denotemos por π la proyección canónica $T(M) \to S(M)$. Para probar que $S(M)$ es conmutativa, basta con notar que $S(M)$ es generada por los elementos de la forma $\pi(m)$ con $m \in M = T^1(M)$, ya que π es epiyectiva y los $m \in M$ generan $T(M)$ como R-álgebra. Entonces, si consideramos $m, n \in M$, vemos que

$$\pi(m)\pi(n) = \pi(m \otimes n) = \pi(m \otimes n - (m \otimes n - n \otimes m)) = \pi(n \otimes m) = \pi(n)\pi(m),$$

por lo que todo par de generadores conmutan. Esto nos dice que $S(M)$ es conmutativa.

La Proposición 3.3.3 nos dice que para probar que $S(M)$ es graduada, basta con probar que $C(M)$ es un ideal graduado. Ahora, esto es una consecuencia inmediata del Lema 3.3.4 ya que los elementos que generan $C(M)$ son todos homogéneos de grado 2.

Finalmente, notemos que $C(M)_k = C(M) \cap T^k(M) = \{0\}$ para $k = 0, 1$ ya que $C(M)$ está contenido en la imagen de la aplicación R-trilineal

$$T(M) \times T^2(M) \times T(M) \to T(M),$$

dada por la multiplicación y esta imagen está contenida en $\bigoplus_{k=2}^{\infty} T^k(M)$. Esto nos da la conclusión sobre $S^0(M)$ y $S^1(M)$. □

Si bien definimos esta álgebra basándonos en un caso particular en el cual esperamos obtener un álgebra de polinomios, sería práctico poder describirla de forma abstracta con una propiedad universal (lo cual será útil para demostrar que efectivamente se tiene un álgebra de polinomios con esta construcción). Definamos pues los objetos que corresponden a dicha propiedad universal.

Definición 3.4.3. Sean M y N dos R-módulos. Una función R-n-lineal $\varphi : M^n \to N$ se dice *simétrica* si $\varphi(m_1, \ldots, m_k) = \varphi(m_{\sigma(1)}, \ldots, m_{\sigma(k)})$ para toda permutación σ de $1, \ldots, k$.

Así, una función R-bilineal φ es simétrica si $\varphi(x, y) = \varphi(y, x)$, lo cual es bastante natural como definición. La definición que acabamos de dar generaliza esta noción obvia de aplicación simétrica.

Vemos entonces la propiedad universal del álgebra simétrica.

Teorema 3.4.4. *Sea M un R-módulo. Entonces:*

1. *El R-módulo $S^k(M)$ es isomorfo al cociente de $T^k(M)$ por el submódulo generado por los elementos de la forma $m_1 \otimes \cdots \otimes m_k - m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)}$ con $m_i \in M$ y σ una permutación.*

2. *El R-módulo $S^k(M)$ posee la siguiente propiedad universal (que lo vuelve único salvo único isomorfismo):*

   Para todo R-módulo N y toda función R-k-lineal simétrica $\psi : M^k \to N$, existe una única *función R-lineal $f : S^k(M) \to N$ tal que $f \circ \varphi = \psi$, es decir, el diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} M^k & \xrightarrow{\psi} & N\ , \\ {\scriptstyle\varphi}\downarrow & \nearrow_{\exists!\, f} & \\ S^k(M) & & \end{array}$$

   donde $\varphi : M^k \to S^k(M)$ envía $(m_1, m_2, \ldots, m_k)$ a $m_1 m_2 \cdots m_k$.

3. *La R-álgebra $S(M)$ posee la siguiente propiedad universal (que la vuelve única salvo único isomorfismo):*

   Sea A una R-álgebra conmutativa *y sea $f : M \to A$ un homomorfismo de R-módulos. Entonces existe un único homomorfismo de R-álgebras $\phi : S(M) \to A$ tal que $\phi|_M = f$.*

Demostración. Para probar el primer punto, bastará con demostrar que el submódulo descrito es precisamente $C^k(M) = C(M) \cap T^k(M)$. Como vimos en la demostración del Lema 3.3.4, los elementos de $C^k(M)$ se escriben de la forma

$$t_k = \sum_{i=1}^{r} a_i \otimes e_i \otimes b_i,$$

con $e_i = m_i \otimes n_i - n_i \otimes m_i \in T^2(M)$, $a_i \in T^j(M)$ y $b_i \in T^{k-2-j}(M)$. Vemos claramente entonces que

$$a_i \otimes e_i \otimes b_i = a_i \otimes m_i \otimes n_i \otimes b_i - a_i \otimes n_i \otimes m_i \otimes b_i,$$

es de la forma descrita en el enunciado para σ la transposición que intercambia $j+1$ y $j+2$. Como las transposiciones generan todo el grupo de permutaciones, obtenemos el resultado.

Para probar el segundo enunciado, utilicemos la propiedad universal de $T^k(M)$. Dada una función R-k-lineal simétrica $\psi : M^k \to N$, esta propiedad universal nos asegura la existencia de una única aplicación R-lineal $\phi : T^k(M) \to N$ tal que $\phi(m_1 \otimes \cdots \otimes m_k) = \psi(m_1, \ldots, m_k)$. Ahora, como ψ es simétrica, tenemos que, para todo $1 \leq j \leq k-2$, todo $a = a_1 \otimes \cdots \otimes a_j \in T^j(M)$, $b = b_1 \otimes \cdots \otimes b_{k-2-j} \in T^{k-2-j}(M)$ y todo $m, n \in M$,

$$\phi(a \otimes m \otimes n \otimes b) = \psi(a_1, \ldots, m, n, b_1, \ldots) = \psi(a_1, \ldots, n, m, b_1, \ldots) = \phi(a \otimes n \otimes m \otimes b).$$

En otras palabras,

$$\phi(a \otimes (m \otimes n - n \otimes m) \otimes b) = \phi(a \otimes m \otimes n \otimes b) - \phi(a \otimes n \otimes m \otimes b) = 0,$$

lo que prueba que ϕ se anula en $C^k(M)$. La propiedad universal del cociente nos dice entonces que existe una única aplicación lineal $f : S^k(M) \to N$ que envía $m_1 m_2 \cdots m_k$ a $\psi(m_1, \ldots, m_k)$, lo que equivale a decir que $f \circ \varphi = \psi$.

El último enunciado se demuestra utilizando la propiedad universal de $T(M)$. Dada una R-álgebra conmutativa A y un homomorfismo de R-módulos $f : M \to A$, existe un único homomorfismo de R-álgebras $\varphi : T(M) \to A$ tal que $\varphi|_M = f$. Ahora, como A es conmutativa, tenemos que, para todo $m, n \in M$

$$\varphi(m \otimes n - n \otimes m) = \varphi(m)\varphi(n) - \varphi(n)\varphi(m) = 0,$$

lo que prueba que φ se anula en $C(M)$. La propiedad universal del cociente nos dice entonces que existe un único homomorfismo de R-álgebras $\phi : S(M) \to A$ que envía $m_1 m_2 \cdots m_k$ a $\varphi(m_1, \ldots, m_k)$ y en particular $m \in M = S^1(M) = T^1(M)$ a $\varphi(m) = f(m)$, lo que equivale a decir que $\phi|_M = f$. □

Ejercicio. Sea M un R-módulo libre de rango n. Pruebe que $S(M)$ es isomorfo al álgebra de polinomios $R[x_1, \ldots, x_n]$. Deduzca una base para el álgebra simétrica de un espacio vectorial de dimensión finita.

Observación.
De la misma forma en que los espacios vectoriales pueden ser estudiados de forma abstracta sin depender de una base, las álgebras de polinomios pueden ser estudiadas de forma abstracta sin depender de su conjunto generador canónico, a saber las variables $x_1, \ldots, x_n$. En efecto, dado el resultado del último ejercicio, vemos que a cada base de un R-módulo libre M corresponde un conjunto generador de $S(M)$ como álgebra de polinomios (i.e. un conjunto de "variables"). El no fijar una base de M corresponde entonces a no fijar un conjunto de "variables" generadoras de los "polinomios" en $S(M)$

3.5. Álgebra Exterior $\Lambda(M)$ de un R-módulo M

El álgebra exterior es una noción complemetaria o "dual" a la de álgebra simétrica. Es más, sobre un cuerpo K, podemos recuperar completamente el espacio de 2-tensores $T^2(V)$ de un K-espacio vectorial V a partir de sus partes simétrica y exterior.

La idea es definir un producto $\wedge$ que se comporte como el célebre producto exterior en $\mathbb{R}^3$, es decir, que sea multilineal como $\otimes$, pero que sea nulo apenas aparezca el mismo elemento dos veces (lo que suele ser llamado "antisimetría" o "alternancia").

Definición 3.5.1. Sea M un R-módulo. Definimos el *álgebra exterior* $\Lambda(M)$ de M como el cociente $T(M)/A(M)$, donde $A(M)$ es el ideal de $T(M)$ generado por los elementos de la forma $m \otimes m$ para $m \in M$.

Llamamos la *k-ésima potencia exterior* de M al submódulo $\Lambda^k(M)$ de $\Lambda(M)$ definido como la imagen de $T^k(M)$.

Notación. El producto en $\Lambda(M)$ es denotado por el símbolo $\wedge$ (cuña, o *wedge* en inglés). En particular, la imagen de $m_1 \otimes \cdots \otimes m_n$ en $\Lambda(M)$ es denotada por $m_1 \wedge \cdots \wedge m_n$.

Proposición 3.5.2. *El álgebra exterior $\Lambda(M)$ es graduada. Su componente de grado k es $\Lambda^k(M)$. Además, $\Lambda^0(M) = R$ y $\Lambda^1(M) = M$.*

Demostración. La Proposición 3.3.3 nos dice que para probar que $\Lambda(M)$ es graduada, basta con probar que $A(M)$ es un ideal graduado. Ahora, esto es una consecuencia inmediata del Lema 3.3.4 ya que los elementos que generan $A(M)$ son todos homogéneos de grado 2.

Notemos además que $A(M)_k = A(M) \cap T^k(M) = \{0\}$ para $k = 0, 1$ ya que $A(M)$ está contenido en la imagen de la aplicación R-trilineal

$$T(M) \times T^2(M) \times T(M) \to T(M),$$

dada por la multiplicación y esta imagen está contenida en $\bigoplus_{k=2}^{\infty} T^k(M)$. Esto nos da la conclusión sobre $\Lambda^0(M)$ y $\Lambda^1(M)$. □

Al igual que con el álgebra simétrica, los factores de esta álgebra pueden ser descritos con una propiedad universal con las siguientes funciones.

Definición 3.5.3. Sean M y N dos R-módulos. Una función R-n-lineal $\varphi : M^n \to N$ se dice *alternada* si $\varphi(m_1, \cdots, m_n) = 0$ cuando $m_i = m_{i+1}$ para algún i.

Ejemplo 3.5.4. La aplicación $M^n \to \Lambda^n(M)$ obtenida por composición de la aplicación natural $M^n \to T^n(M)$ (que es R-n-lineal) con la proyección canónica $\pi_n : T^n(M) \to \Lambda^n(M)$ (que es R-lineal) es alternada. En efecto, esta composición envía $(m_1, \ldots, m_n)$ a $m_1 \wedge \cdots \wedge m_n$ y claramente esta expresión es nula si $m_i = m_{i+1}$ ya que

$$m_1 \wedge \cdots \wedge m_i \wedge m_i \wedge \cdots \wedge m_n = \pi_n(m_1 \otimes \cdots m_i \otimes m_i \otimes \cdots \otimes m_n) = \pi_n(t \otimes (m_i \otimes m_i) \otimes t'),$$

con $t, t' \in T(M)$, y $t \otimes (m_i \otimes m_i) \otimes t'$ está claramente en $A(M)$.

Teorema 3.5.5. *Sea M un R-módulo. Entonces:*

1. *El R-módulo $\Lambda^k(M)$ es isomorfo al cociente de $T^k(M)$ por el submódulo generado por los elementos de la forma $m_1 \otimes \cdots \otimes m_k$ con $m_i \in M$ y $m_i = m_j$ para algún par $i \neq j$. En particular, $m_1 \wedge \cdots \wedge m_k = 0$ si $m_i = m_j$ para algún par $i \neq j$.*

2. *El R-módulo $\Lambda^k(M)$ posee la siguiente propiedad universal (que lo vuelve único salvo único isomorfismo):*

   Para todo R-módulo N y toda función R-k-lineal alternada $\psi : M^k \to N$, existe una única *función R-lineal $f : \Lambda^k(M) \to N$ tal que $f \circ \varphi = \psi$, es decir, el diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} M^k & \xrightarrow{\psi} & N\ , \\ {\scriptstyle\varphi}\downarrow & \nearrow_{\exists!\, f} & \\ \Lambda^k(M) & & \end{array}$$

   donde $\varphi : M^k \to \Lambda^k(M)$ envía $(m_1, \ldots, m_k)$ a $m_1 \wedge \cdots \wedge m_k$.

Demostración. Para probar el primer punto, bastará con demostrar que el submódulo descrito es precisamente $A^k(M) = A(M) \cap T^k(M)$. Como vimos en la demostración del Lema 3.3.4, los elementos de $A^k(M)$ se escriben de la forma

$$t_k = \sum_{i=1}^{r} a_i \otimes e_i \otimes b_i,$$

con $e_i = m_i \otimes m_i \in T^2(M)$, $a_i \in T^j(M)$ y $b_i \in T^{k-2-j}(M)$. Vemos claramente entonces que $a_i \otimes e_i \otimes b_i$ es de la forma descrita en el enunciado, por lo que $A^k(M)$ está contenido en este submódulo. Para probar lo opuesto, notemos que para todo $m, n \in M$ tenemos que $m \wedge n = -n \wedge m$ ya que

$$m \wedge n + n \wedge m = m \wedge m + m \wedge n + n \wedge m + n \wedge n = (m+n) \wedge (m+n) = 0.$$

Por lo tanto,

$$m_1 \wedge \cdots \wedge (m_{j-1} \wedge m_j) \wedge \cdots \wedge m_k = -m_1 \wedge \cdots \wedge (m_j \wedge m_{j-1}) \wedge \cdots \wedge m_k,$$

e iterando el proceso con $m_i = m_j$,

$$m_1 \wedge \cdots \wedge m_i \wedge \cdots \wedge m_j \wedge \cdots \wedge m_k = (-1)^{j-i} m_1 \wedge \cdots \wedge m_i \wedge m_j \wedge \cdots \wedge m_k = 0,$$

lo que prueba que $m_1 \otimes \cdots \otimes m_k \in A^k(M)$ si $m_i = m_j$.

Para probar el segundo enunciado, utilicemos la propiedad universal de $T^k(M)$. Dada una función R-k-lineal alternada $\psi : M^k \to N$, esta propiedad universal nos asegura la existencia de una única aplicación R-lineal $\phi : T^k(M) \to N$ tal que $\phi(m_1 \otimes \cdots \otimes m_k) = \psi(m_1, \ldots, m_k)$. Ahora, como ψ es alternada, tenemos que, para todo $1 \leq j \leq k-2$, todo $a = a_1 \otimes \cdots \otimes a_j \in T^j(M)$, $b = b_1 \otimes \cdots \otimes b_{k-2-j} \in T^{k-2-j}(M)$ y todo $m \in M$,

$$\phi(a \otimes m \otimes m \otimes b) = \psi(a_1, \ldots, m, m, b_1, \ldots) = 0,$$

lo que prueba que ϕ se anula en $A^k(M)$. La propiedad universal del cociente nos dice entonces que existe una única aplicación lineal $f : \Lambda^k(M) \to N$ que envía $m_1 \wedge \cdots \wedge m_k$ a $\psi(m_1, \ldots, m_k)$, lo que equivale a decir que $f \circ \varphi = \psi$. □

Ejemplo 3.5.6. Sea K un cuerpo y sea V un K-espacio vectorial de dimensión 1, es decir $V = \langle v \rangle$. Entonces $\Lambda(V)$ es bastante sencilla. En efecto, como todo elemento de V se escribe αv con $\alpha \in K$, tenemos que todo elemento de $\Lambda^2(V)$ es una suma de elementos de la forma $(\alpha v) \wedge (\beta v) = \alpha\beta(v \wedge v) = 0$. Por lo tanto, $\Lambda^2(V) = 0$ y de la misma manera vemos que $\Lambda^k(V) = 0$ para todo $k \geq 2$, por lo que $\Lambda(V) = \Lambda^0(V) \oplus \Lambda^1(V) = K \oplus V$.

Ejemplo 3.5.7. Sea K un cuerpo y sea V un K-espacio vectorial de dimensión 2. Aquí $\Lambda(V)$ se complica un poco, pero vemos que $\Lambda^k(V) = 0$ para todo $k \geq 3$. Evidentemente, basta con mostrar esto para $k = 3$, donde todo elemento es una suma de elementos de la forma $v \wedge w \wedge x$. Si $w = \alpha v$ con $\alpha \in K$, entonces $v \wedge w = 0$ por lo visto anteriormente y por ende $v \wedge w \wedge x = 0$. De lo contrario, v y w son K-linealmente independientes y forman por lo tanto una K-base de V, lo que nos dice que

$$v \wedge w \wedge x = v \wedge w \wedge (\alpha v + \beta w) = \alpha(v \wedge w \wedge v) + \beta(v \wedge w \wedge w) = 0.$$

Por lo tanto, tenemos que

$$\Lambda(V) = K \oplus V \oplus \Lambda^2(V).$$

Veamos ahora la estructura de $\Lambda^2(V)$. Sea $\{v_1, v_2\}$ una base de V. Entonces una base de $T^2(V)$ es

$$\{v_1 \otimes v_1,\ v_1 \otimes v_2,\ v_2 \otimes v_1,\ v_2 \otimes v_2\}.$$

Pero sabemos que $t_1 = v_1 \otimes v_1$, $t_2 = v_2 \otimes v_2 \in A^2(V)$, al igual que

$$t_0 = (v_1 + v_2) \otimes (v_1 + v_2) = v_1 \otimes v_1 + v_1 \otimes v_2 + v_2 \otimes v_1 + v_2 \otimes v_2.$$

Ahora, todo otro elemento del núcleo $A^2(V)$ de la proyección $T^2(V) \to \Lambda^2(V)$ es una combinación lineal de elementos de la forma

$$(\alpha v_1 + \beta v_2) \otimes (\alpha v_1 + \beta v_2) = \alpha\beta t_0 + \alpha(\alpha - \beta)t_1 + \beta(\beta - \alpha)t_2.$$

Esto nos dice que $\dim_K(A^2(V)) = 3$ y por lo tanto $\Lambda^2(V)$ es de dimensión 1. Y ese es el caso ya que $v_1 \wedge v_2 \neq 0$. Por lo tanto, tenemos que

$$\Lambda(V) \simeq K \oplus V \oplus K.$$

Ejercicio. Generalice este argumento para probar que $\Lambda^k(V) = 0$ para todo $k > \dim_K(V)$.

3.6. Interludio 5: Álgebras centrales simples

El estudio de las álgebras de división de dimensión finita sobre un cuerpo son un tema clásico en álgebra abstracta. Famoso es el resultado de Frobenius que nos dice que las únicas álgebras de división asociativas de dimensión finita sobre $\mathbb{R}$ son $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$, los cuarteniones de Hamilton.

Teniendo ahora a la mano la herramienta del producto tensorial, uno podría preguntarse si éste nos permite fabricar nuevas álgebras de división a partir de las ya conocidas. Tomado literalmente, esto no funciona prácticamente nunca. Pero si cambiamos el objeto de interés por el de *álgebra central simple*, que es más general, sí podemos usar esta nueva herramienta a nustro favor.

Comencemos pues con la definición de este nuevo objeto:

Definición 3.6.1. Sea K un cuerpo y A una K-álgebra. Decimos que A es una *álgebra central simple* si A es simple, de dimensión finita sobre K y $Z(A) \simeq K$.

Ejemplo 3.6.2. Una K-álgebra de división de centro K es un álgebra central simple. En particular, $\mathbb{R}$ y $\mathbb{H}$ son $\mathbb{R}$-álgebras centrales simples (pero no $\mathbb{C}$, ya que su centro no es $\mathbb{R}$).

Ejemplo 3.6.3. El álgebra de matrices $M_n(K)$ es un álgebra central simple. De forma más general, si D es un álgebra de división de centro K, entonces $M_n(D)$ es una K-álgebra central simple.

Ejercicio. Pruebe esta última afirmación. *Hint: Pruebe usando la D-base canónica de $M_n(D)$ que una matriz central es diagonal con todas sus coordenadas iguales.*

Vemos entonces que las álgebras centrales simples mezclan de una forma interesante las álgebras de matrices con las álgebras de división, que son las que nos interesan. En lo que sigue, demostraremos que estas son todas la álgebras centrales simples (Teorema de Wedderburn) y luego buscaremos la manera de "borrar" las álgebras de matrices para poder estudiar tan solo la "parte de división" de las álgebras centrales simples.

Teorema 3.6.4 (Wedderburn)**.** *Sea R un álgebra asociativa (o anillo) unitaria simple y sea I un ideal izquierdo minimal. Entonces $D = \mathrm{End}_R(I)$ es una R-álgebra de división y existe un isomorfismo canónico $R \simeq \mathrm{End}_D(I)$.*

Demostración. El hecho de que $D = \mathrm{End}_R(I)$ sea una R-álgebra de división se deduce del hecho que I es un R-módulo simple (por minimalidad).

Notemos ahora que $D = \mathrm{End}_R(I)$ actúa sobre I de la forma natural, es decir, evaluando un endomorfismo $d \in D$ en un elemento $a \in I$. Definamos entonces una aplicación $\varphi : R \to \mathrm{End}_D(I)$ de la siguiente manera: a $r \in R$ le asociamos el

endomorfismoφ_r de multiplicación por r, es decir $a \mapsto ra$. Entonces φ_r es realmente un elemento de $\mathrm{End}_D(I)$ ya que, para todo $d \in D$ y $a, a' \in I$,

$$\varphi_r(a + da') = r(a + d(a')) = ra + r(d(a')) = ra + d(ra') = \varphi_r(a) + d(\varphi_r(a')).$$

Probemos que φ es un isomorfismo de R-álgebras. Es fácil ver que $\varphi_{r+r'} = \varphi_r + \varphi_{r'}$ y que $\varphi_{rr'} = \varphi_r \circ \varphi_{r'}$, por lo que bastará con probar que se trata de una biyección. Ahora, notemos que $\varphi_{1_R} = \mathrm{id}_I$, por lo que la imagen de φ es no nula. Como R es simple, esto implica que $\ker(\varphi) = \{0\}$ y tenemos por ende la inyectividad. Para probar la epiyectividad, bastará con probar que la imagen de φ es un ideal izquierdo de $\mathrm{End}_D(I)$, ya que acabamos de notar que $\mathrm{id}_I = 1_{\mathrm{End}_D(I)}$ está en la imagen.

Notemos ahora que, para $a \in I$, la multiplicación por la derecha $b \mapsto ba$ es un elemento d_a de $D = \mathrm{End}_R(I)$. Entonces, para todo elemento $f \in \mathrm{End}_D(I)$ y para todo $a \in I$ tenemos que $f(ba) = f(d_a(b)) = d_a(f(b)) = f(b)a$. Esto implica que

$$f(\varphi_b(a)) = f(ba) = f(b)a = \varphi_{f(b)}(a),$$

y por lo tanto $\varphi(I) \subset \varphi(R)$ es un ideal izquierdo de $\mathrm{End}_D(I)$. Pero nosotros queremos que $\varphi(R)$ sea un ideal izquierdo. Es entonces que recordamos que R es simple, lo que nos dice que $IR = R$ ya que IR es un ideal bilateral no nulo de R. Por lo tanto

$$\varphi(R) = \varphi(IR) = \varphi(I)\varphi(R),$$

lo que corresponde a un ideal izquierdo ya que $\varphi(I)$ es un ideal izquierdo. □

El corolario de este teorema en el marco de las álgebras centrales simples es el siguiente:

Corolario 3.6.5. *Sea K un cuerpo y sea A una K-álgebra central simple. Entonces $A \simeq M_n(D)$ para alguna K-álgebra de división D (a fortiori de dimensión finita y centro K).*

Demostración. Sea I un ideal izquierdo minimal. Un tal ideal existe ya que todo ideal de A es un K-espacio vectorial y por ende existe uno de dimensión minimal no nula. El teorema 3.6.4 nos dice entonces que A es isomorfa a $\mathrm{End}_D(I)$ con D la K-álgebra de división $\mathrm{End}_A(I)$. Como I es un K-módulo de dimensión finita, vemos que se trata de un D-módulo libre de rango finito (ejercicio), por lo que su anillo de endomorfismos $\mathrm{End}_D(I)$ es isomorfo al anillo $M_n(D)$. □

Vemos entonces que, si uno considera que las álgebras de matrices son "triviales", la parte interesante de un álgebra central simple es el álgebra de división que lleva dentro. Debemos asegurarnos sin embargo que un álgebra central simple no oculte dos álgebras de división distintas. Para esto es el siguiente resultado:

Teorema 3.6.6. *Sea K un cuerpo y sean D y D' dos K-álgebras de dvisión de dimensión finita. Supongamos que existe un isomorfismo entre $M_n(D)$ y $M_m(D')$ para ciertos $m, n \in \mathbb{N}$. Entonces $D \simeq D'$ y $m = n$.*

Demostración. Sea $R = M_n(D)$ y sea N un R-módulo simple. Probaremos que existe un isomorfismo (no canónico) $\mathrm{End}_R(N) \simeq D$. Esto probará que la clase de siomorfismo de D está determinada por el álgebra R y por ende que $D \simeq D'$. La igualdad $m = n$ sigue entonces por la dimensión de éstas álgebras sobre K.

Probemos entonces el isomorfismo anunciado. Consideremos el espacio $N = D^n$ de vectores columna con coeficientes en D. Entonces el álgebra $R = M_n(D)$ actúa naturalmente por la izquierda sobre N, es decir, N es un R-módulo por la izquierda que además es *simple* (ejercicio). Por otra parte, $N = D^n$ es de forma evidente un D-módulo por la derecha (la acción es coordenada a coordenada). Definamos entonces una aplicación

$$\varphi : D \to \mathrm{End}_R(N),$$

enviando $d \in D$ al endomorfismo $\varphi_d : x \mapsto xd$. Como una acción es por la izquierda y la otra por la derecha, está claro que φ_d es un R-endomorfismo de N. Además, vemos fácilmente que φ es un homomorfismo de K-álgebras. Como D es simple y $\varphi \not\equiv 0$, bastará con probar la epiyectividad de φ. Sea $\lambda \in \mathrm{End}_R(N)$ un endomorfismo cualquiera y escribamos

$$\lambda(e_1) = e_1 d_1 + \cdots + e_n d_n,$$

donde $d_i \in D$ y $\{e_1, \ldots, e_n\}$ es la base canónica de $N = D^n$. Entonces $\lambda = \varphi_{d_1}$ ya que

$$\lambda(e_j) = \lambda(\varepsilon_{j1} e_1) = \varepsilon_{j1} \lambda(e_1) = e_j d_1,$$

para todo $1 \leq j \leq n$. □

Podemos pues, a cada álgebra central simple, asociarle un álgebra de división sin ambigüedad. Veamos ahora, como anunciamos al comienzo, que si bien el producto tensorial de dos álgebras de división no tiene porqué dar un álgebra de división, el producto tensorial de dos álgebras centrales simples sí se porta como uno quisiera.

Definición 3.6.7. Sea K un cuerpo y A una K-álgebra. Definimos el *álgebra opuesta* A° de A como el álgebra dada por $A^\circ = \{a^\circ \mid a \in A\}$ con suma y multiplicación dadas por

$$(a+b)^\circ = a^\circ + b^\circ, \qquad \lambda(a^\circ) = (\lambda a)^\circ, \qquad (ab)^\circ = b^\circ a^\circ,$$

para $a, b \in A$ y $\lambda \in K$.

Observación.
Si A es un álgebra de división, entonces A° también lo es. Lo mismo va para central y simple.

Proposición 3.6.8. *Sea K un cuerpo y D una K-álgebra de división de dimensión finita. Entonces $D \otimes_K D^\circ \simeq M_n(K)$ para $n = \dim_K(D)$.*

Demostración. ¡Ejercicio! □

Esta proposición nos dice entonces que el producto de dos álgebras de división no tiene porqué ser de división, ya que las álgebras de matrices no son nunca de división. Pero no es así con las álgebras centrales simples.

Teorema 3.6.9. *Sea K un cuerpo y sean A, A' dos K-álgebras centrales simples. Entonces $A \otimes_K A'$ es una K-álgebra central simple.*

Demostración. Notemos ante todo que $A \otimes_K A'$ es de dimensión finita sobre K ya que A y A' lo son.

Probemos entonces que $A \otimes_K A'$ es central. Como A y A' son centrales, tenemos que $Z(A) = K$ y $Z(A') = K$, por lo que $Z(A) \otimes_K Z(A') = K \otimes_K K \simeq K$ es una subálgebra central de $Z(A \otimes_K A')$. Debemos demostrar que no hay más que estos elementos centrales.

Sea $a'_1, \ldots, a'_n$ una K-base de A' y $xA \otimes_K A'$. Entonces podemos escribir x de forma única como una suma

$$x = \sum_{i=1}^{n} a_i \otimes a'_i,$$

con $a_i \in A$. Supongamos ahora que $x \in Z(A \otimes_K A')$. Entonces para todo $a \otimes 1 \in A \otimes_K A'$ tenemos que $y = (a \otimes 1)x = x(a \otimes 1)$, lo que se traduce por

$$y = \sum_{i=1}^{n} (aa_i) \otimes a'_i = \sum_{i=1}^{n} (a_i a) \otimes a'_i.$$

Pero como la escritura es única para todo $y \in A \otimes A'$, obtenemos que $aa_i = a_i a$ para todo $a \in A$. Esto prueba que $a_i \in Z(A) = K$ para todo i y por lo tanto, por K-bilinealidad, $x = 1 \otimes a'$ con $a' \in A'$. Como x es central, vemos entonces inmediatamente que $a' \in Z(A') = K$ y por lo tanto $x \in Z(A) \otimes_K Z(A')$.

Probemos para terminar que $A \otimes_K A'$ es simple. Sea $I \subset A \otimes_K A'$ un ideal no nulo y supongamos primero que existe un elemento no nulo de la forma $a \otimes a'$ en I. Como A es simple y a es no nulo, existen entonces $a_i, b_i \in A$ tales que $\sum_{i=1}^{n} a_i a b_i = 1$, por lo que

$$\sum_{i=1}^{n} (a_i \otimes 1)(a \otimes a')(b_i \otimes 1) = 1 \otimes a' \in I.$$

Un argumento similar para a' nos prueba entonces que $1 = 1 \otimes 1 \in I$, por lo que $I = A \otimes_K A'$.

Veamos ahora el caso de un ideal I cualquiera (i.e. uno que no posee necesariamente un elemento como el anterior). Sea entonces $x \in I$ un elemento no nulo y supongamos que $x = \sum_{i=1}^{n} a_i \otimes a_i'$ con n minimal (y $n \geq 2$, si no ya terminamos). En particular, tenemos que los $a_i \in A$ son K-linealmente independientes y lo mismo ocurre con los $a_i' \in A$. Aplicando el argumento anterior a $a_n \in A$, vemos que podemos asumir que $a_n = 1 \in K = Z(A)$, y por lo tanto $a_{n-1} \notin K = Z(A)$.

Existe entonces un elemento $b \in A$ que no conmuta con a_{n-1}. Consideremos pues el siguiente elemento:

$$(b \otimes 1)x - x(b \otimes 1) = \sum_{i=1}^{n} (ba_i - a_i b) \otimes a_i' \in I.$$

Como $a_n = 1$, el último término de la suma es nulo. Sin embargo, el $(n-1)$-ésimo término es no nulo ya que a_{n-1} no conmuta con b. Esto nos dice que existe un elemento en I de escritura más corta que la de x, lo que contradice la minimalidad. Esto prueba que siempre existe un elemento con $n = 1$ y por lo tanto concluye la demostración. □

El corolario natural de este teorema es que, si tenemos dos álgebras (centrales) de división y las tensorizamos para obtener otra álgebra, no obtenemos un álgebra de división, pero sí un álgebra central simple, es decir un *álgebra de matrices sobre un álgebra de división*. Si olvidamos entonces la "parte matricial" de esta álgebra, tenemos una "multiplicación" en el conjunto de las álgebras centrales de división. Esta es la multiplicación del grupo de Brauer, el cual definimos a continuación y concluye este interludio por falta de tiempo.

Definición 3.6.10. Sea K un cuerpo. Decimos que dos K-álgebras centrales simples A, A' son *Brauer-equivalentes* si existen $m, n \in \mathbb{N}$ tales que $M_m(A) \simeq M_n(A')$.

En particular, $M_n(K)$ es Brauer-equivalente al álgebra trivial $A = K$ y $M_n(D)$ es equivalente a D, lo que "trivializa la parte matricial".

Ejercicio. Pruebe que la Brauer-equivalencia es una verdadera relación de equivalencia en el conjunto de las K-álgebras centrales simples.

Definición 3.6.11. Definimos el *grupo de Brauer* de K como el grupo $\mathrm{Br}(K)$ cuyos elementos son las clases de Brauer-equivalencia y cuya multiplicación es el producto tensorial. Es decir, si denotamos por $[A]$ la clase de una K-álgebra central simple A, entonces $[A] \cdot [A'] = [A \otimes_K A']$.

Ejercicio. Pruebe que la multiplicación en el grupo de Brauer está bien definida, es decir que la clase de $A \otimes_K A'$ es independiente de la elección de A dentro de $[A]$ (resp. A' dentro de $[A']$).

Pruebe además que el elemento neutro de $\mathrm{Br}(K)$ corresponde a la clase $[M_n(K)]$ y que el inverso de $[A]$ es $[A^\circ]$.

Ejemplo 3.6.12. Dado el teorema de Frobenius (no demostrado en este curso), sabemos que las únicas $\mathbb{R}$-alǵebras centrales simples son $M_n(\mathbb{R})$ y $M_n(\mathbb{H})$, por lo que $\mathrm{Br}(\mathbb{R})$ consiste en (el único) grupo con 2 elementos. En particular, vemos que la clase $[\mathbb{H}]$ es de orden 2 y por ende que $\mathbb{H} \simeq \mathbb{H}^\circ$.

Ejercicio. Sea K un cuerpo algebraicamente cerrado. Entonces $\mathrm{Br}(K) = 0$. *Hint: pruebe que la subálgebra de una K-álgebra de división D generada por un elemento $x \in D \setminus K$ es una extensión finita de K.*

La trivialidad del grupo de Brauer no está reservada tan solo a los cuerpos algebraicamente cerrados. En efecto, otro teorema de Wedderburn (que no demostraremos aquí) nos dice que:

Teorema 3.6.13 (Wedderburn)**.** *Toda álgebra de división finita es un cuerpo.*

Ejercicio. Pruebe que esto último implica que $\mathrm{Br}(\mathbb{F}) = 0$ para todo cuerpo finito $\mathbb{F}$.