Extensiones de cuerpos

Andrés Abella

13 de julio de 2020

Índice

1. Anillos y polinomios

En esta sección se introducen los conceptos necesarios para el estudio de las extensiones de cuerpos y la teoría de Galois.

1.1. Anillos

En lo que sigue veremos brevemente algunas propiedades de anillos que necesitamos para nuestra teoría.
Un *anillo* es una estructura $(A, +, \cdot, 0, 1)$ en la cual A es un conjunto, $0, 1$ son elementos de A y $+, \cdot$ son dos operaciones en A llamadas *suma* y *producto* respectivamente, que verifican las siguientes propiedades

1. $x + (y + z) = (x + y) + z, \ \forall x, y, z \in A$.
2. $x + 0 = 0 + x = x, \ \forall x \in A$.
3. $\forall x \in A$ existe $y \in A$ tal que $x + y = y + x = 0$.
4. $x + y = y + x, \ \forall x, y \in A$.
5. $x(yz) = (xy)z, \ \forall x, y, z \in A$.
6. $x1 = 1x = x, \ \forall x \in A$.
7. $x(y + z) = xy + xz$ y $(x + y)z = xz + yz, \ \forall x, y, z \in A$.

Observación 1.1. Los neutros de la suma y producto (0 y 1) son únicos. También, dado $x \in A$, el elemento y que verifica la tercera propiedad es único, se le llama el *opuesto* de x y se escribe $y = -x$.

Si el producto es conmutativo, es decir si se verifica $xy = yx$, para todo $x, y \in A$, entonces decimos que A es un anillo *conmutativo*. Por ejemplo $\mathbb{Z}$ (los enteros) es un anillo conmutativo mientras que $M_n(\mathbb{R})$ (las matrices cuadradas) con $n \geq 2$ es un anillo no conmutativo.

De ahora en adelante todos los anillos que consideraremos son <u>conmutativos</u>. También vamos a asumir siempre que vale $0 \neq 1$ (en caso contrario es $A = \{0\}$).

Sea A un anillo. De la existencia de opuestos se deduce la propiedad cancelativa de la suma: $x + y = x + z$ implica $y = z$. Luego de $0x = (0 + 0)x = 0x + 0x$ deducimos que vale $0x = 0$, para todo $x \in A$. Si $x, y \in A$ son no nulos y verifican $xy = 0$, entonces decimos que x e y son *divisores de cero*. Si A no tiene divisores de cero, entonces decimos que A es un *dominio*. La no existencia de divisores de cero equivale a la propiedad cancelativa del producto: si $xy = xz$ y $x \neq 0$, entonces $y = z$. Un ejemplo de dominio es $\mathbb{Z}$.
Un elemento $x \in A$ se dice *invertible* si existe $y \in A$ tal que $xy = yx = 1$. En ese caso el elemento y es único, se le llama el *inverso* de x y se escribe $y = x^{-1}$. En $\mathbb{Z}$ los únicos elementos invertibles son ± 1, que son inversos de sí mismos.
Si todo elemento no nulo de A es invertible, entonces decimos que A es un *cuerpo*. Ejemplos de cuerpos son los números racionales $\mathbb{Q}$, los reales $\mathbb{R}$ y los complejos $\mathbb{C}$. Notar que todo cuerpo es un dominio.

Sea A un anillo. Un *subanillo* de A es un subconjunto $B \subset A$ tal que

$$0, 1 \in B; \quad x, y \in B \ \Rightarrow \ x + y \in B \text{ y } xy \in B; \quad x \in B \ \Rightarrow \ -x \in B.$$

Por ejemplo, $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ son subanillos. Notar que si $B \subset A$ es un subanillo, entonces B es un anillo con las operaciones de A restringidas a B. Un subanillo de un dominio es un dominio. En particular todo subanillo de un cuerpo es un dominio.

Un *ideal* de A es un subconjunto $K \subset A$ tal que

$$0 \in K; \quad x, y \in K \ \Rightarrow \ x+y \in K; \quad x \in K, \ y \in A \Rightarrow \ xy \in K.$$

Si $K \subset A$ es un ideal y $1 \in K$, entonces $K = A$; lo mismo sucede si K contiene un elemento invertible. Los conjuntos $\{0\}$ y A son ideales de A, todo otro ideal se dice que es *propio*. Notar que un cuerpo no tiene ideales propios. Si $b \in A$, entonces el conjunto $\langle b \rangle := bA = \{bx : \ x \in A\}$ es un ideal llamado el *ideal principal* generado por b. En $\mathbb{Z}$ todos los ideales son principales (por la existencia de la división entera).

Si A y B son dos anillos, un *morfismo de anillos* entre A y B es una función $\varphi : A \to B$ que verifica

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(1) = 1, \quad \forall a, b \in A.$$

Si φ es morfismo, entonces $\operatorname{Ker}(\varphi) := \{a \in A : \ \varphi(a) = 0\}$ es un ideal de A y $\operatorname{Im}(\varphi)$ es un subanillo de B. Un *isomorfismo* de anillos es un morfismo de anillos que es biyectivo.

Si K es un ideal de A, entonces definimos una relación en A mediante

$$x \sim y \quad \overset{\text{def}}{\Longleftrightarrow} \quad x - y \in K \quad \Leftrightarrow \quad \exists k \in K \text{ t.q. } x = y + k.$$

Esta relación es de equivalencia. Dado $x \in A$, el conjunto $\overline{x} := \{y \in A : \ y \sim x\}$ es la *coclase* correspondiente a x. Notar $\overline{x} = x + K := \{x + k : \ k \in K\}$. Si $x \sim y$ y $x' \sim y'$, entonces existen $k, k' \in K$ tales que $x = y + k$ y $x' = y' + k'$. Luego

$$x + x' = y + y' + (k + k') \quad \text{y} \quad xx' = yy' + (xk' + y'k + kk') \quad \Rightarrow \quad x + x' \sim y + y' \quad \text{y} \quad xx' \sim yy'.$$

Est implica que podemos definir una suma y un producto en el conjunto cociente $A/K := \{\overline{x} : \ x \in A\}$ mediante $\overline{x} + \overline{y} := \overline{x+y}$ y $\overline{x}\,\overline{y} := \overline{xy}$, para todo $x, y \in A$. Es fácil de probar que A/K es un anillo con las operaciones definidas anteriormente. La *proyección canónica* es la función $\pi : A \to A/K$ definida por $\pi(x) = \overline{x}$. Notar que π es un morfismo de anillos sobreyectivo y $\operatorname{Ker}\pi = K$.

Proposición 1.2. *Si $\varphi : A \to B$ es un morfismo de anillos, entonces φ induce un morfismo inyectivo de anillos $\hat{\varphi} : A/\operatorname{Ker}\varphi \to B$ mediante $\hat{\varphi}(\overline{x}) = \varphi(x)$, para todo $x \in A$. Vale $\operatorname{Im}\hat{\varphi} = \operatorname{Im}\varphi$. Luego si φ es sobreyectivo, entonces $\hat{\varphi}$ es un isomorfismo.*

Dem. Lo único que probaremos es que $\hat{\varphi}$ está bien definida, el resto es fácil.

Si $\overline{x} = \overline{y} \quad \Rightarrow \quad \exists k \in K$ t.q. $x = y + k \quad \Rightarrow \quad \varphi(x) = \varphi(y) + \varphi(k) = \varphi(y) + 0 = \varphi(y) \quad \Rightarrow \quad \hat{\varphi}(x) = \hat{\varphi}(y)$. □

Enteros módulo n. Sea n un entero positivo y consideramos el ideal $n\mathbb{Z}$. El anillo cociente $\mathbb{Z}/n\mathbb{Z}$ es el anillo de los *enteros módulo n*. Escribiremos $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Vale $\mathbb{Z}_n = \left\{\overline{0}, \ \overline{1}, \ldots, \overline{n-1}\right\}$, luego $\mathbb{Z}_n$ es un anillo finito con n elementos. Notar que en $\mathbb{Z}_6$ vale $\overline{2} \times \overline{3} = \overline{0}$, luego $\mathbb{Z}_6$ no es un dominio.

Proposición 1.3. *Dado $0 \neq n \in \mathbb{Z}^+$, las siguientes afirmaciones son equivalentes*

$$n \textit{ es primo}; \quad \mathbb{Z}_n \textit{ es un dominio;} \quad \mathbb{Z}_n \textit{ es un cuerpo.}$$

Dem. La prueba es esencialmente la misma que veremos de la proposición 1.17, así que la omitiremos. □

1.2. Polinomios.

En esta sección veremos una construcción formal del anillo de los polinomios. En lo que sigue D es un dominio y K es un cuerpo.

Al conjunto de las sucesiones $(a_n) = (a_0, a_1, \dots)$ con coeficientes en D tales que existe $m \in \mathbb{N}$ tal que $a_n = 0$, para todo $n > m$ lo escribimos $D[X]$. El conjunto $D[X]$ es un anillo con la suma y producto definidos por $(a_n) + (b_n) = (c_n)$ y $(a_n)(b_n) = (d_n)$, siendo

$$c_n = a_n + b_n, \quad d_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0, \quad \forall n \in \mathbb{N}.$$

Al conjunto $D[X]$ con estas operaciones se le llama el *anillo de polinomios* en una indeterminada, o en una variable. Sus elementos son los *polinomios* con coeficientes en D. El mapa $\varphi : D \to D[X]$ definido por $\varphi(a) = (a, 0, 0, \dots)$ es un morfismo inyectivo de anillos. Luego identificando D con $\varphi(D)$, escribimos $a = (a, 0, 0, \dots)$ y consideramos a D como subanillo de $D[X]$. Los elementos de D pensados en $D[X]$ son los *polinomios constantes*. Sea $X := (0, 1, 0, 0, \dots)$. Notar que vale

$$X = (0, 1, 0, 0, \dots), \quad X^2 = (0, 0, 1, 0, 0, \dots), \quad X^3 = (0, 0, 0, 1, 0, 0, \dots), \quad \cdots$$

Luego si $a \in D$, es

$$a = (a, 0, 0, 0, \dots), \quad aX = (0, a, 0, 0, 0, \dots), \quad aX^2 = (0, 0, a, 0, 0, 0, \dots), \quad \dots$$

Esto implica que si $(a_n) \in D[X]$ y $m \in \mathbb{N}$ es tal que $a_n = 0$ para todo $n > m$, entonces

$$(a_n) = (a_0, a_1, \dots, a_m, 0, 0, \dots) = a_0 + a_1 X + \cdots + a_m X^m.$$

Al polinomio $f = \sum_i a_i X^i \in D[X]$ lo escribiremos f o $f(X)$, según convenga. Si $f = \sum_{i=0}^n a_i X^i$ es un polinomio no nulo y $a_n \neq 0$, entonces decimos que a_n es el *coeficiente principal* de f, que n es el *grado* de f y escribimos $\operatorname{gr} f = n$. Si el coeficiente principal es 1, entonces decimos que el polinomio es *mónico*. Para el polinomio nulo no se le define el grado o se dice que su grado es $-\infty$. Notar que dados $f, g \in D[X]$, si escribimos $f = a_n X^n + \cdots + a_0$ y $g = b_m X^m + \cdots + b_0$, entonces $fg = a_n b_m X^{n+m} + \cdots + a_0 b_0$. Luego vale $\operatorname{gr}(fg) = gr f + \operatorname{gr} g$. Esto implica que $D[X]$ también es un dominio.

Función polinómica. A cada polinomio $f = \sum_i a_i X^i \in D[X]$ se le puede asociar una función $\hat{f} : D \to D$ definida por $\hat{f}(x) = \sum_i a_i x^i$, para todo $x \in D$. La correspondencia $f \mapsto \hat{f}$ es inyectiva si y solo si D es infinito. Aún así se suele escribir siempre f en vez de $\hat{f}$.

Proposición 1.4. *Si $f \in D[X]$ y $a \in D$ entonces $\exists\, g \in D[X]$ tal que $f = (X - a)g + f(a)$.*

Dem. Ejercicio (funciona la misma prueba de secundaria). □

El proceso de obtener el polinomio g anterior es lo que se conoce como la *división de f por $X - a$*.

Raíces. Decimos que $a \in D$ es *raíz* de $f \in D[X]$ si verifica $f(a) = 0$. Dividiendo f por $X - a$ obtenemos que $a \in D$ es raíz de $f \in D[X]$ si y solo si existe $g \in D[X]$ tal que $f = (X - a)g$. Notar que vale $\operatorname{gr} g = \operatorname{gr} f - 1$. El proceso anterior puede seguirse aplicando. Considerando el polinomio g, si $g(a) = 0$, entonces existe $h \in D[X]$ tal que $g = (X - a)h$. Luego $f = (X - a)^2 g$. Así seguimos hasta obtener $n > 0$ y $h \in D[X]$ tales que $f = (X - a)^n h$ y $h(a) \neq 0$. El *orden de multiplicidad* de a como raíz de f es el entero n. Si $n = 1$ entonces decimos que a es una raíz *simple*, en caso contrario decimos que es una raíz *múltiple*.

Observación 1.5. El argumento que recién aplicamos permite probar que un polinomio de grado n tiene a lo más n raíces contadas con su orden de multiplicidad. Esto implica la inyectividad de la correspondencia $f \mapsto \hat{f}$ antes mencionada.

El siguiente resultado se utiliza para encontrar las raíces racionales de los polinomios con coeficiente enteros.

Proposición 1.6. *Si $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ admite una raíz racional r/s, con r y s primos entre sí, entonces $r \mid a_0$ y $s \mid a_n$.*

Dem. Es $a_0 + a_1(r/s) + \cdots + a_n(r/s)^n = 0$. Multiplicando por s^n obtenemos

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0 \ \Rightarrow\ -\left(a_0 s^{n-1} + a_1 r s^{n-2} + \cdots + a_{n-1} r^{n-1}\right) s = a_n r^n. \quad (1)$$

Luego $s \mid a_n r^n$, y como r y s son primos entre sí, entonces $s \mid a_n$. La otra relación se obtiene despejando $a_0 s^n$ en la primer fórmula de (1). □

Observación 1.7. El *teorema fundamental del álgebra*[1] dice que todo polinomio complejo de grado positivo admite alguna raíz. Aplicando inducción en el grado, se deduce que si $f \in \mathbb{C}[X]$ es de grado positivo, entonces existen $a \in \mathbb{C}$, $u_1, \ldots, u_r \in \mathbb{C}$ distintos entre sí y $n_1, \ldots, n_r \in \mathbb{Z}^+$ tales que

$$f = a(X - u_1)^{n_1} \cdots (X - u_r)^{n_r}.$$

Notar que a es el coeficiente principal de f, $u_1, \ldots, u_r$ son sus raíces y $n_1, \ldots, n_r$ son los órdenes de multiplicidad de las raíces respectivas.

Divisibilidad. Sea D un dominio. Dados $f, g \in D[X]$, si existe $h \in D[X]$ tal que $f = gh$, entonces decimos que g *divide* a f o que f es un *múltiplo* de g, y escribimos $g \mid f$.

Cuando K es un cuerpo, dados $f, g \in K[X]$, con $g \neq 0$, si no sabemos si g divide o no a f, entonces podemos hacer la *división entera* de f entre g, que es un algoritmo que les asocia dos polinomios $q, r \in K[X]$, llamados respectivamente el *cociente* y r el *resto*, que verifican $f = gq + r$ y $r = 0$ o $r \neq 0$ y $\operatorname{gr} r < \operatorname{gr} g$. Este algoritmo es el mismo que se estudia en los cursos de secundaria, que resumimos en el siguiente resultado.

Proposición 1.8. *Sea K un cuerpo. Si $f, g \in K[X]$ y $g \neq 0$, entonces existen únicos $q, r \in K[X]$ tales que $f = gq + r$ y $r = 0$ o $r \neq 0$ y $\operatorname{gr} r < \operatorname{gr} g$.* □

Observación 1.9. La división entera también se puede hacer en $D[X]$, siendo D un dominio, pero en ese caso necesitamos que el coeficiente principal de g sea invertible (en $\mathbb{Z}$ tiene que ser ± 1).

Proposición 1.10. *Si K es un cuerpo, entonces todo ideal de $K[X]$ es principal.*

Dem. Sea I un ideal de $K[X]$. Si es $I = \{0\}$, entonces $I = \langle 0 \rangle$. En caso contrario, sea $g \in I$ tal que $\operatorname{gr} g = n$, siendo $n = \min\{\operatorname{gr} f :\ 0 \neq f \in I\}$. Si $f \in I$, dividiendo f entre g obtenemos $q, r \in K[X]$ tales que $f = gq + r$ y $r = 0$ o $r \neq 0$ y $\operatorname{gr} r < \operatorname{gr} g$. Al ser $f, g \in I$, deducimos $r \in I$, luego la minimalidad del grado de g implica que necesariamente es $r = 0$; luego $f = gq \in \langle g \rangle$. De esto se deduce $I = \langle g \rangle$. □

Observación 1.11. Si $\{0\} \neq I \subset K[X]$ es un ideal, entonces vimos que existe $f \in I$ tal que $I = \langle f \rangle$. Notar que $I = \langle f \rangle$ implica que f es de grado mínimo entre los polinomios no nulos que están en I. Si $g \in I$ es otro elemento tal que $I = \langle g \rangle$, entonces valen $f \mid g$ y $g \mid f$, luego existe $0 \neq a \in K$ tal que $f = ag$. Esto implica que si $\{0\} \neq I \subset K[X]$ es un ideal, entonces existe un único polinomio mónico $f \in I$ tal que $I = \langle f \rangle$.

Máximo común divisor. Sean $f, g \in K[X]$ no ambos nulos. El conjunto $I = \{mf + ng :\ m.n \in K[X]\}$ es un ideal de $K[X]$, luego existe un único polinomio mónico $d \in I$ tal que $I = \langle d \rangle$. El polinomio d se llama el *máximo común divisor* de f y g, y queda caracterizado por las siguientes condiciones

$$d \mid f,\ d \mid g; \qquad \text{si } h \mid f,\ h \mid g \ \Rightarrow\ h \mid d; \qquad d \text{ es mónico.}$$

Escribimos $d = \operatorname{mcd}(f, g)$. Notar $d \in I$, luego existen $h, k \in K[X]$ tales que $d = hf + kg$. Esta relación se conoce como la *identidad de Bézout*. Dos polinomios $f, g \in K[X]$ se dicen *primos entre sí*, si $\operatorname{mcd}(f, g) = 1$. Notar que f y g son primos entre sí si y solo si existen $h, k \in K[X]$ tales que $hf + kg = 1$.

[1]Este teorema se prueba en los cursos de análisis complejo. Nosotros lo asumiremos como válido.

Algoritmo de Euclides. Dados $f, g \in K[X]$ con $g \neq 0$, si $f = gq + r$ es la división entera de f entre g, entonces es fácil de probar que los divisores comunes a f y g coinciden con los divisores comunes a g y r. Esto implica $\operatorname{mcd}(f, g) = \operatorname{mcd}(g, r)$.

El *algoritmo de Euclides* es un método para hallar el máximo común divisor, que describimos a continuación. Sean $f, g \in K[X]$ con $g \neq 0$. Consideremos $f = gq_1 + r_1$ la división entera de f entre g. Si $r_1 \neq 0$, entonces dividimos g entre r_1 obteniendo $g = q_2 r_1 + r_2$. Si $r_2 \neq 0$, entonces dividimos r_1 entre r_2 obteniendo $r_1 = q_3 r_2 + r_3$. Y así seguimos en la medida que los restos obtenidos $r_1, r_2, \ldots$ sean no nulos. Por lo que observamos anteriormente, es

$$\operatorname{mcd}(f, g) = \operatorname{mcd}(g, r_1) = \operatorname{mcd}(r_1, r_2) = \operatorname{mcd}(r_2, r_3) = \cdots$$

Como los restos verifican $\operatorname{gr} g > \operatorname{gr} r_1 > \operatorname{gr} r_2 > \cdots$, entonces existe algún n tal que $r_n \neq 0$ y $r_{n+1} = 0$. En ese caso obtenemos $\operatorname{mcd}(f, g) = \operatorname{mcd}(r_n, 0)$. Luego si a es el coeficiente principal de r_n y $d = \frac{1}{a} r_n$, entonces $\operatorname{mcd}(f, g) = d$. Notar que despejando r_n en función de f y g en las ecuaciones

$$f = gq_1 + r_1, \quad g = q_2 r_1 + r_2, \quad r_1 = q_3 r_2 + r_3, \quad \cdots, \quad r_{n-2} = q_n r_{n-1} + r_n,$$

se obtienen dos polinomios $h, k \in K[X]$ que verifican $d = hf + kg$

La definición de máximo común divisor se generaliza a familias finitas de polinomios. Dados $f_1, \ldots, f_n \in K[X]$, existe un único polinomio $d = \operatorname{mcd}(f_1, \ldots, f_n) \in K[X]$ llamado el *máximo común divisor* de $f_1, \ldots, f_n$, que queda caracterizado por verificar las siguientes condiciones

$$d \mid f_i, \ \forall i; \qquad \text{si } h \mid f_i, \ \forall i \ \Rightarrow \ h \mid d; \qquad d \text{ es mónico.}$$

Como antes, si $\operatorname{mcd}(f_1, \ldots, f_n) = 1$, entonces decimos que $f_1, \ldots, f_n$ son *primos entre sí*.

Polinomios irreducibles Un polinomio $f \in K[X]$ se dice *irreducible* si no es constante y verifica que si $g, h \in K[X]$ son tales que $f = gh$, entonces g o h es constante. Esto último quiere decir que la única forma de factorizarlo es $f = a\left(a^{-1} f\right)$, con $0 \neq a \in K$.

Ejemplos 1.12.

1. En $K[X]$ todo polinomio de grado 1 es irreducible (para todo cuerpo K).
2. En $\mathbb{C}[X]$ los irreducibles son los polinomios de grado 1 (por el teorema fundamental del álgebra).
3. En $\mathbb{R}[X]$ los irreducibles son los polinomios de grado 1 o los del tipo $aX^2 + bX + c$, con $b^2 - 4ac < 0$.
4. En $\mathbb{Q}[X]$ hay más polinomios irreducibles que en $\mathbb{R}[X]$ pero no tenemos una forma simple de caracterizarlos. Por ejemplo $X^2 - 2$ es irreducible en $\mathbb{Q}[X]$, pero es reducible en $\mathbb{R}[X]$

Los dos resultados siguientes se usan para estudiar la irreducibilidad de polinomios con coeficientes en $\mathbb{Q}$.

Proposición 1.13 (Lema de Gauss)**.** *Sea $f \in \mathbb{Z}[X]$. Si existen $g, h \in \mathbb{Q}[X]$ tales que $f = gh$, entonces existe $a \in \mathbb{Q}$ no nulo tal que $g_0 = ag \in \mathbb{Z}[X]$, $h_0 = a^{-1} h \in \mathbb{Z}[X]$ y $f = g_0 h_0$.*

Luego $f \in \mathbb{Z}[X]$ no constante es irreducible en $\mathbb{Q}[X]$ si y solo si no existen dos polinomios no constantes $g, h \in \mathbb{Z}[X]$ tales que $f = gh$.

Dem. Mirar en la bibliografía. □

Ejemplo 1.14. Queremos estudiar la irreducibilidad de $f = X^4 + X + 11 \in \mathbb{Q}[X]$. Sus posibles raíces racionales son ± 11 y ninguna de esas es raíz. Luego f no se puede factorizar como producto de un polinomio de grado uno por uno de grado tres. La otra posibilidad es que se escriba como producto de dos polinomios de grado dos. Por el lema de Gauss alcanza con estudiar el caso en que estos polinomios tienen coeficientes enteros. Supongamos entonces que existen $g = aX^2 + bX + c$ y $h = \alpha X^2 + \beta X + \gamma$ en $\mathbb{Z}[X]$ tales que $f = gh$. Desarrollando el producto e igualando coeficientes obtenemos que $f = gh$ equivale a

$$a\alpha = 1, \quad a\beta + b\alpha = 0, \quad a\gamma + b\beta + c\alpha = 0, \quad b\gamma + c\beta = 1, \quad c\gamma = 11.$$

La primer ecuación implica $a = \alpha = \pm 1$. Podemos suponer $a = \alpha = 1$ (dado que $f = gh = (-g)(-h)$). Sustituyendo esos valores obtenemos

$$\beta + b = 0, \quad \gamma + b\beta + c = 0, \quad b\gamma + c\beta = 1, \quad c\gamma = 11.$$

Las soluciones de la última ecuación son $c = \pm 1$ y $\gamma = \pm 11$ o $c = \pm 11$ y $\gamma = \pm 1$. Pero es fácil de probar usando la regla de Cramer que el sistema $\beta + b = 0$ y $b\gamma + c\beta = 1$ no tiene soluciones enteras para ninguno de estos valores de c y γ. Luego no existen polinomios no constantes $g, h \in \mathbb{Z}[X]$ tales que $f = gh$. Esto termina de probar que f es irreducible en $\mathbb{Q}[X]$

Proposición 1.15 (Criterio de irreducibilidad de Eisenstein)**.** *Sea $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ con $n \geq 1$ y $a_n \neq 0$. Supongamos que existe un número primo $p \in \mathbb{N}$ tal que*

$$p \mid a_i, \ \forall\ 0 = 1, \dots, n-1; \qquad p \nmid a_n; \qquad p^2 \nmid a_0.$$

Entonces f es irreducible en $\mathbb{Q}[X]$.

Dem. Supongamos razonando por el absurdo que f es reducible en $\mathbb{Q}[X]$, entonces el lema de Gauss implica que existen $g = \sum_{i=0}^{r} b_i X^i$ y $h = \sum_{i=0}^{s} d_i X^i$ en $\mathbb{Z}[X]$ tales que $f = gh$, con $1 \leq r, s < n$. Como es $a_0 = b_0 c_0$, $p \mid a_0$ y $p^2 \nmid a_0$, entonces podemos asumir $p \mid b_0$ y $p \nmid c_0$. Si valiese $p \mid b_i$ para todo i, entonces sería $p \mid a_n$ contradiciendo nuestras hipótesis. Luego existe $1 \leq h \leq r$ tal que $p \mid b_0, \dots, b_{h-1}$ y $p \nmid b_h$. Pero en ese caso, de $p \mid a_h$ y $a_h = b_h c_0 + b_{h-1} c_1 + b_{h-2} c_2 + \cdots$, deducimos $p \mid b_h c_0$, contradiciendo que es $p \nmid c_0$ y $p \nmid b_h$. □

Proposición 1.16. *Sean $f, g \in K[X]$, con f irreducible. Si $f \nmid g$, entonces $\operatorname{mcd}(f, g) = 1$.*

Dem. Sea $d = \operatorname{mcd}(f, g)$. Como f es irreducible y $d \mid f$, entonces $d = 1$ o existe $0 \neq k \in K$ tal que $f = kd$. En el segundo caso, como es $d \mid g$, obtendríamos $f \mid g$ en contra de nuestras hipótesis. Luego $d = 1$. □

La siguiente es una propedad importante de los polinomios irreducibles.

Proposición 1.17. *Dado $0 \neq f \in K[X]$, las siguientes afirmaciones son equivalentes*

1. *El polinomio f es irreducible en $K[X]$.*
2. *El anillo cociente $K[X]/\langle f \rangle$ es un cuerpo.*
3. *El anillo cociente $K[X]/\langle f \rangle$ es un dominio.*

Dem. ($1 \Rightarrow 2$). Sea $\overline{g} \in K[X]/\langle f \rangle$. Si $\overline{g} \neq \overline{0}$, entonces f no divide a g y por la proposición anterior es $\operatorname{mcd}(f, g) = 1$. Luego existen $r, s \in K[X]$ tales que $1 = fr + gs$ y por lo tanto $\overline{g}\,\overline{s} = \overline{1}$ en $K[X]/\langle f \rangle$.
($2 \Rightarrow 3$). Esto es evidente.
($3 \Rightarrow 1$). Si f fuese constante, entonces sería $\langle f \rangle = K[X]$ y por lo tanto $K[X]/\langle f \rangle = \{0\}$ que no es un dominio; luego f no es constante. Sean $g, h \in K[X]$ tales que $f = gh$. Entonces es $\overline{g}\,\overline{h} = \overline{0}$ en $K[X]/\langle f \rangle$ que es un dominio, luego alguno de ellos es nulo. Supongamos $\overline{g} = \overline{0}$. Entonces existe $p \in K[X]$ tal que $g = fp$. Luego $f = gh = fph$ implica $ph = 1$ y por lo tanto h es una constante no nula. □

Proposición 1.18. *Sean $f, g, h \in K[X]$. Si $f \mid gh$ y $\operatorname{mcd}(f, g) = 1$, entonces $f \mid h$.*

Dem. Consideremos el anillo $A = K[X]/\langle f \rangle$. Como es $\operatorname{mcd}(f, g) = 1$, entonces existen $h, k \in K[X]$ tales que $hf + kg = 1$. Esto implica $\overline{k}\overline{g} = \overline{1}$, luego $\overline{g}$ es invertible en A. La condición $f \mid gh$ implica $\overline{g}\overline{h} = \overline{0}$, y como $\overline{g}$ es invertible, concluimos $\overline{h} = \overline{0}$ en A, lo cual equivale a $f \mid h$. □

Corolario 1.19. *Si f es irreducible y $f \mid gh$, entonces $f \mid g$ o $f \mid h$.*

Dem. Aplicar la proposición anterior junto con la proposición 1.16. □

El siguiente resultado muestra la importancia de los poliomios irreducibles. Decimos que $f, g \in K[X]$ son *asociados* si existe $0 \neq a \in K$ tal que $f(X) = ag(X)$.

Teorema 1.20. *Sea $f \in K[X]$ un polinomio no constante. Entonces vale lo siguiente.*

1. *Existen $f_1, \ldots, f_n \in K[X]$ irreducibles tales que $f = f_1 \cdots f_n$.*
2. *La descomposición anterior es única a menos de cambiar $f_1, \ldots, f_n$ por polinomios asociados.*

Dem. Existencia. Por inducción en el grado de f. Si $\operatorname{gr} f = 1$, entonces f es irreducible y ya está probado. Supongamos $\operatorname{gr} f \geq 2$ y que la tesis vale para los polinomios de grado menor que $\operatorname{gr} f$. Si f es irreducible, entonces ya está. En caso contrario es $f = gh$ con g, h polinomios no constantes de grado menor que n. La hipótesis inductiva implica que existen polinomios irreducibles $g_1, \ldots, g_r$ y $h_1, \ldots, h_s$ tales que $g = g_1 \cdots g_r$ y $h = h_1 \cdots h_s$. Luego es $f = g_1 \cdots g_r h_1 \cdots h_s$, en que todos los factores son irreducibles.

Unicidad. Supongamos que vale $f_1 \cdots f_n = k_1 \cdots k_m$, en que todos los factores son irreducibles. Entonces f_1 divide a $k_1 \cdots k_m$, luego el corolario 1.19 implica que f_1 divide a alguno de los factores. Rordenando podemos suponer que f_1 divide a k_1, y como ambos son irreducibles deducimos que existe una constante $a_1 \in K$ tal que $k_1 = af_1$; luego k_1 y f_1 son asociados. Entonces

$$f_1 \cdots f_n = k_1 \cdots k_m \quad \Rightarrow \quad f_1 f_2 \cdots f_n = a_1 f_1 k_2 \cdots k_m \quad \underset{f_1 \neq 0}{\Longrightarrow} \quad f_2 \cdots f_n = a_1 k_2 \cdots k_m.$$

Luego f_2 divide a $k_2 \cdots k_m$ y podemos seguir repitiendo el procedimiento hasta terminar con todos los f_i. Como no puede suceder que un producto de polinomios irreducibles sea igual a una constante, deducimos que es $n = m$ y que cada f_i está asociado con algún k_j. □

Observación 1.21. Si en la factorización $f = f_1 \cdots f_n$ agrupamos los polinomios asociados, obtenemos que si $f \in K[X]$ es un polinomio no constante, entonces se puede factorizar de la forma $f = g_1^{m_1} \cdots g_r^{m_r}$, en la cual $g_1, \ldots, g_r \in K[X]$ son polinomios irreducibles no asociados y $m_1, \ldots, m_r$ son enteros positivos. Además esa descomposición es única a menos de cambiar $g_1, \ldots, g_r$ por polinomios asociados. Esta factorización $f = g_1^{m_1} \cdots g_r^{m_r}$ se llama la *descomposición factorial* de f.

Cuerpo de expresiones racionales. Veremos que a $K[X]$ le podemos asociar un cuerpo $K(X)$, tal que $K[X]$ es un subanillo de $K(X)$ y los elementos de $K(X)$ son cocientes de elementos de $K[X]$ (como $\mathbb{Z} \subset \mathbb{Q}$).

Formalmente lo que hacemos es lo siguiente. En el conjunto $\{(f, g) \in K[X] \times K[X] : \; g \neq 0\}$ definimos la siguiente relación: $(f, g) \sim (f', g')$ si y solo si $fg' = f'g$. Es fácil de probar que esta relación es de equivalencia. A la clase de equivalencia de (f, g) la escribimos f/g. Luego

$$f/g = f'/g' \qquad \Leftrightarrow \qquad fg' = f'g.$$

Sea $K(X) = \{f/g : \; f, g \in K[X], \; g \neq 0\}$ el conjunto cociente. Es un ejercicio el probar que, en forma análoga a las operaciones en $\mathbb{Q}$, tiene sentido definir una suma y producto en $K(X)$ mediante

$$\frac{f}{g} + \frac{h}{k} = \frac{fk + gh}{gk}, \qquad \frac{f}{g} \times \frac{h}{k} = \frac{fh}{gk}.$$

Con esas operaciones el conjunto $K(X)$ es un cuerpo llamado el *cuerpo de expresiones racionales* con coeficientes en K. El mapa $K[X] \to K(X)$ definido por $f \mapsto f/1$ es un morfismo inyectivo de anillos; luego $K(X)$ contiene un subanillo que es una copia de $K[X]$ y podemos pensar $K[X]$ como subanillo de $K(X)$, escribiendo $f = f/1$.

Notar que tenemos $K \subset K[X] \subset K(X)$, en que K y $K(X)$ son cuerpos y $K[X]$ es un dominio.

Proposición 1.22. *Sean K y F cuerpos. Si $\varphi : K[X] \to F$ es un morfismo inyectivo de anillos, entonces φ induce un morfismo de anillos $\hat{\varphi} : K(X) \to F$ mediante $\hat{\varphi}(f/g) = \varphi(f)\varphi(g)^{-1}$, para todo $f/g \in K(X)$.*

Dem. Probaremos solo que $\hat{\varphi}$ está bien definida, dejando el resto como ejercicio. Para eso, si $f/g = h/k$, entonces $fk = gh$ y por lo tanto $\varphi(f)\varphi(k) = \varphi(g)\varphi(h)$. Como φ es inyectiva, es $\varphi(g) \neq 0$ y $\varphi(h) \neq 0$ y por lo tanto $\varphi(f)\varphi(g)^{-1} = \varphi(h)\varphi(k)^{-1}$. Luego $f/g = h/k$ implica $\varphi(f)\varphi(g)^{-1} = \varphi(h)\varphi(k)^{-1}$. □

Una forma equivalente de enunciar el resultado anterior es la siguiente.

Proposición 1.23. *Sean K y F cuerpos. Si $\varphi : K[X] \to F$ es un morfismo inyectivo de anillos, entonces existe un único morfismo de anillos $\hat{\varphi} : K(X) \to F$ tal que $\hat{\varphi}|_{K[X]} = \varphi$.* □

Con al misma prueba se demuestra el siguiente.

Proposición 1.24. *Sea F un cuerpo arbitrario. Si $\varphi : \mathbb{Z} \to F$ es un morfismo inyectivo de anillos, entonces φ induce un morfismo de anillos $\hat{\varphi} : \mathbb{Q} \to F$ mediante $\hat{\varphi}(m/n) = \varphi(m)\varphi(n)^{-1}$, para todo $m/n \in \mathbb{Q}$.* □

La construcción de los polinomios en una variable se generaliza naturalmente a varias variables, obteniéndose el *anillo de polinomios en varias variables* $K[X_1, \ldots, X_n]$, $n \geq 1$. Sus elementos son sumas finitas del tipo

$$\sum a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad a_{i_1,\ldots,i_n} \in K$$

Este anillo es un dominio y tiene asociado su *cuerpo de expresiones racionales* $K(X_1, \ldots, X_n)$, que está formado por cocientes de elementos de $K[X_1, \ldots, X_n]$.

2. Cuerpos

2.1. Definiciones básicas

Recordar que un *cuerpo* es un anillo conmutativo con unidad $K \neq \{0\}$ en el cual todo elemento no nulo es invertible. Si $u, v \in K$ y $v \neq 0$, entonces escribiremos $u/v = uv^{-1}$.

Un subconjunto F de K se dice que es un *subcuerpo* de K si verifica

$$1 \in F; \quad u - v \in F, \quad u/v \in F, \quad \forall u, v \in F, \; v \neq 0.$$

Claramente si $F \subset K$ es un subcuerpo, entonces F es un cuerpo con las operaciones de K restringidas a F.

Ejemplos 2.1. 1. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ es una cadena de subcuerpos.

2. Si p es un número primo, entonces el cociente $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ es un cuerpo.

3. Si K es un cuerpo y $f \in K[X]$ es un polinomio irreducible, entonces el cociente $K[X]/\langle f\rangle$ es un cuerpo.

4. Si K es un cuerpo, entonces tenemos las inclusiones $K \subset K[X] \subset K(X)$, siendo K un subcuerpo de $K(X)$ y $K[X]$ un subanillo de $K(X)$.

Sea F un cuerpo y $\{K_\lambda\}_{\lambda\in\Lambda}$ una familia de subcuerpos de F. Es fácil de probar que $\bigcap_{\lambda\in\Lambda} K_\lambda$ es un subcuerpo de F. Luego si $\mathcal{X}$ es la familia de todos los subcuerpos de F que contienen a $\bigcup_{\lambda\in\Lambda} K_\lambda$, entonces $\bigcap_{L\in\mathcal{X}} L$ es el menor subcuerpo de F que contiene a todos los K_λ y se llama la *composición* de la familia $\{K_\lambda\}_{\lambda\in\Lambda}$. Si $\Lambda = \{1,\dots,n\}$, entonces escribimos $K_1 \cdots K_n$ para denotar la composición de $K_1,\dots,K_n$.

Observación 2.2. Si K y L son subcuerpos de F, entonces podemos describir su composición KL de la manera siguiente. El conjunto $A = \{\sum_{i=1}^n k_i l_i : \ k_i \in K,\ l_i \in L,\ i = 1,\dots,n,\ n = 1,2,\dots\}$ es el menor subanillo de F que contiene a $K \cup L$, luego $KL = \{a/b : \ a,b \in A,\ b \neq 0\}$.

Observación 2.3. Si F es un cuerpo y $K \subset L \subset F$ son subcuerpos, decimos que L es un cuerpo *intermedio* entre K y F. Lo anterior prueba que el conjunto de cuerpos intermedios entre K y F forma un *retículo completo* respecto a la inclusión, es decir es un conjunto parcialmente ordenado en el cual todo subconjunto no vacío tiene supremo e ínfimo. En particular el supremo de $\{E, L\}$ es EL y el ínfimo es $E \cap L$.
Notar que si G es un grupo, entonces el conjunto de sus subgrupos también forma un retículo completo respecto a la inclusión.

Sea F un cuerpo y $K \subset F$ un subcuerpo.

Si $u_1,\dots,u_n \in F$, entonces definimos

$$\begin{aligned} K[u_1,\dots,u_n] &:= \{f(u_1,\dots,u_n) : \ f \in K[X_1,\dots,X_n]\}, \\ K(u_1,\dots,u_n) &:= \left\{\frac{f(u_1,\dots,u_n)}{g(u_1,\dots,u_n)} : \ f,g \in K[X_1,\dots,X_n],\ g(u_1,\dots,u_n) \neq 0\right\}. \end{aligned}$$

Notar que $K[u_1,\dots,u_n]$ es el menor subanillo de F que contiene a K y a $u_1,\dots,u_n$, y $K(u_1,\dots,u_n)$ es el menor subcuerpo de F que verifica lo mismo.

La construcción anterior puede generalizarse cambiando $\{u_1,\dots,u_n\}$ por un subconjunto arbitrario de F. Si S es un subconjunto de F, entonces se definen

$$\begin{aligned} K[S] &:= \{f(u_1,\dots,u_n) : \ f \in K[X_1,\dots,X_n],\ u_1,\dots,u_n \in S,\ n = 1,2,\dots\}, \\ K(S) &:= \{a/b : \ a,b \in K[S],\ b \neq 0\}. \end{aligned}$$

Vale $K \cup S \subset K[S] \subset K(S)$, siendo $K[S] \subset F$ un subanillo y $K(S) \subset F$ un subcuerpo.

Observación 2.4. Si K y L son subcuerpos de F, entonces $K(L) = L(K) = KL$.

A los morfismos de anillos entre cuerpos se les llama *morfismos de cuerpos*.

Observación 2.5. Sea $\varphi : K \to F$ un morfismo de cuerpos. Si $0 \neq a \in K$, entonces de $aa^{-1} = 1$ deducimos $1 = \varphi(a)\varphi\left(a^{-1}\right)$; luego $\varphi(a) \neq 0$ y $\varphi\left(a^{-1}\right) = \varphi(a)^{-1}$. Esto implica $\operatorname{Ker}(\varphi) = \{0\}$. Luego todo morfismo de cuerpos es inyectivo.

Si un morfismo de cuerpos φ es sobreyectivo, entonces es biyectivo y se dice que es un *isomorfismo*. Si existe un isomorfismo entre K y F decimos que son *isomorfos* y escribimos $K \simeq F$.

Característica. Sea K un cuerpo. El *cuerpo primo* de K es la intersección de todos los subcuerpos de K, y es el menor subcuerpo de K. Sea $a \in K$. Para $n \in \mathbb{N}$ definimos recursivamente $na \in K$ mediante

$$0a = 0, \quad (n+1)a = na + a, \ \forall n \in \mathbb{N}.$$

Esta definición se extiende a los enteros negativos mediante $(-n)a := -(na)$, para todo $n \in \mathbb{N}$. Notar que si P es el cuerpo primo de K, entonces $n1_K \in P$ para todo $n \in \mathbb{Z}$. Luego podemos definir $\varphi : \mathbb{Z} \to P$ mediante $\varphi(n) = n1_K$, para todo $n \in \mathbb{Z}$. Es un ejercicio el verificar que φ es un morfismo de anillos.

Proposición 2.6. *Si P es el cuerpo primo de K, entonces $P \simeq \mathbb{Q}$ o $P \simeq \mathbb{Z}_p$ para algún primo p.*

Dem. Consideremos el morfismo $\varphi : \mathbb{Z} \to P$ definido por $\varphi(n) = n1_K$.

Si $\varphi : \mathbb{Z} \to P$ es inyectivo, entonces (proposición 1.24) φ induce un morfismo de cuerpos de $\tilde{\varphi} : \mathbb{Q} \to P$ definido por $\tilde{\varphi}(m/n) = \varphi(m)\varphi(n)^{-1}$. Luego $\tilde{\varphi}(\mathbb{Q})$ es un subcuerpo de P y por lo tanto $P = \tilde{\varphi}(\mathbb{Q}) \simeq \mathbb{Q}$.

Si φ no es inyectivo, entonces existe $p \in \mathbb{Z}^+$ tal que $\operatorname{Ker}(\varphi) = p\mathbb{Z}$. Luego (proposición 1.2) φ induce un morfismo de anillos inyectivo $\hat{\varphi} : \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \to P$ tal que $\hat{\varphi}(\mathbb{Z}_p) = \varphi(\mathbb{Z}_p)$. Como $\hat{\varphi}(\mathbb{Z}_p)$ es un subanillo del cuerpo P, resulta que $\hat{\varphi}(\mathbb{Z}_p)$ es un dominio. Y como φ es inyectivo, deducimos que $\mathbb{Z}_p \simeq \hat{\varphi}(\mathbb{Z}_p)$ es un dominio. Luego (proposición 1.3) p es un número primo y $\mathbb{Z}_p$ es un cuerpo. Entonces $\hat{\varphi}(\mathbb{Z}_p) \simeq \mathbb{Z}_p$ es un cuerpo y por lo tanto $\hat{\varphi}(\mathbb{Z}_p) = P$. Luego $P = \hat{\varphi}(\mathbb{Z}_p) \simeq \mathbb{Z}_p$. □

Sea K un cuerpo y P el cuerpo primo de K. Si $P \simeq \mathbb{Q}$, decimos que K tiene *característica cero* y escribimos $\operatorname{car} K = 0$. Si $P \simeq \mathbb{Z}_p$, decimos que K tiene *característica positiva* p y escribimos $\operatorname{car} K = p$.

Observaciones 2.7.

1. Si $\operatorname{car} K = p > 0$, entonces $p = \min\{n \in \mathbb{Z}^+ : \ n1_K = 0\}$.
2. Si K es finito, entonces $\operatorname{car} K = p > 0$.
3. Si p es un primo, entonces $\mathbb{Z}_p(X)$ es un cuerpo infinito de característica p.

2.2. Extensiones

Comenzamos con algunas definiciones.

1. Si K y F son dos cuerpos tales que K es un subcuerpo de F, entonces escribimos F/K y decimos que F es una *extensión* de K.
2. Una extensión F/K se dice que está *generada* por $S \subset F$, si $F = K(S)$. En el caso en que S sea un conjunto finito, entonces se dice que F/K está *finitamente generada*. Luego F/K está finitamente generada si y solo si existen $u_1, \ldots, u_n \in F$ tales que $F = K(u_1, \ldots, u_n)$.
3. Una extensión F/K es *simple* si existe $u \in F$ tal que $F = K(u)$, en ese caso se dice que u es un *elemento primitivo* de la extensión.
4. Si F es una extensión de K, entonces F es un K-espacio vectorial. A la dimensión de F como K-espacio vectorial se le llama el *grado* de F/K y se escribe $[F : K] = \dim_K F$. La extensión F/K se dice *finita* si $[F : K] < \infty$, e *infinita* en caso contrario.

Proposición 2.8. *Si $F \supset E \supset K$ es una torre de extensiones, entonces F/K es finita si y solo si F/E y E/K son finitas. En caso de ser finitas, vale $[F : K] = [F : E][E : K]$.*

Dem. Si $\{e_i : \ i \in I\}$ es una base de E como K-espacio y $\{f_j : \ j \in J\}$ es una base de F como E-espacio, entonces es facil de probar que $\{e_i f_j : \ (i,j) \in I \times J\}$ es una base de F como K-espacio. □

Elementos algebraicos y trascendentes. Sea F/K una extensión y $u \in F$ fijos. Consideramos $K[u] = \{f(u) : \ f \in K[X]\}$ que es un subanillo de F. Notar que $\varepsilon_u : K[X] \to K[u]$ definido por $\varepsilon(f) = f(u)$ es un morfismo de anillos sobreyectivo.

Si $\operatorname{Ker}(\varepsilon_u) = \{0\}$, entonces decimos que u es *trascendente* sobre K. En este caso $\varepsilon_u : K[X] \to K[u]$ es un isomorfismo de anillos. Aplicando la proposición 1.22 deducimos que la composición $K[X] \xrightarrow{\varepsilon_u} K[u] \hookrightarrow K(u)$ induce un morfismo de cuerpos $\varphi : K(X) \to K(u)$ definido por $f/g \mapsto f(u)/g(u)$. Claramente φ es sobreyectivo, luego φ es un isomorfismo. En resumen, si u es trascendente, entonces $K[u] \simeq K[X]$ y $K(u) \simeq K(X)$.

Si $\operatorname{Ker}(\varepsilon_u) \neq \{0\}$, entonces decimos que u es *algebraico* sobre K. En este caso existe un único polinomio $f \in K[X]$ mónico de grado positivo tal que $\operatorname{Ker}(\varepsilon_u) = \langle f \rangle$. Notar que $K[X]/\langle f \rangle \simeq K[u]$ que es un dominio por ser un subanillo de un cuerpo, luego la proposición 1.17 implica que f es irreducible y $K[X]/\langle f \rangle$ es un cuerpo. Esto implica que $K[u] \simeq K[X]/\langle f \rangle$ es un subcuerpo de $K(u)$ y por lo tanto $K(u) = K[u] \simeq K[X]/\langle f \rangle$. El polinomio f se llama el *polinomio irreducible* de u sobre K y se escribe $f = \operatorname{Irr}_K(u)$. Observar que el polinomio irreducible de u sobre K queda determinado por ser un polinomio mónico $f \in K[X]$ que tiene raíz u y verifica cualquiera de las siguientes condiciones:

1. f es de grado mínimo entre los polinomios que se anulan en u.
2. si $g \in K[X]$ es tal que $g(u) = 0$, entonces f divide a g.
3. f es irreducible.

Ejemplos 2.9.

1. El elemento $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$. Es $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{2}\right) = X^2 - 2$ y $\mathbb{Q}\left[\sqrt{2}\right] = \mathbb{Q}\left(\sqrt{2}\right)$ es un cuerpo. Notar $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\right\}$.
2. Los elementos π y e son trascendentes sobre $\mathbb{Q}$ (ver [3]).

Notar que si K es un cuerpo y $f \in K[X]$, entonces el anillo cociente $K[X]/\langle f \rangle$ tiene estructura de K-espacio vectorial definiendo $a \cdot \overline{f(X)} = \overline{af(X)}$, para todo $a \in K$ y $f(X) \in K[X]$.

Lema 2.10. *Sea K un cuerpo y $f \in K[X]$ un polinomio de grado $n > 0$. Entonces*

$$\mathcal{B} = \left\{\overline{1}, \overline{X}, \overline{X}^2, \dots, \overline{X}^{n-1}\right\}$$

es una base de $K[X]/\langle f \rangle$ como K-espacio vectorial.

Dem. Si $g \in K[X]$, entonces dividiendo g entre f obtenemos que existen $q, r \in K[X]$ tales que $g = fq + r$ y $r = 0$ o $r \neq 0$ y $\operatorname{gr} r < n$. Luego si $r = r_0 + r_1X + \cdots + r_{n-1}X^{n-1}$, entonces $\overline{g} = \overline{r} = r_0\overline{1} + r_1\overline{X} + \cdots + r_{n-1}\overline{X}^{n-1}$. Esto prueba que $\mathcal{B}$ es un conjunto generador de $K[X]/\langle f \rangle$. Sean ahora $a_0, \dots, a_{n-1} \in K$ tales que $a_0\overline{1} + a_1\overline{X} + \cdots + a_{n-1}\overline{X}^{n-1} = \overline{0}$. Entonces f divide a $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$, pero como el grado de f es n, la única posibilidad es $a_0 = \cdots = a_{n-1} = 0$, luego $\mathcal{B}$ es linealmente independiente. $\square$

Teorema 2.11. *Sea F/K una extensión y $u \in F$. Las siguientes afirmaciones son equivalentes:*

1. *u es algebraico sobre K.*
2. *$K[u] = K(u)$.*
3. *$K(u)/K$ es finita.*

Dem. Si $u=0$ todo es obvio. Sea $u\neq 0$.
(1) $\Rightarrow$ (2). Esto ya lo vimos.
(2) $\Rightarrow$ (1). Como $K[u]$ es un cuerpo, entonces existe $g\in K[X]$ tal que $u^{-1}=g(u)$ y por lo tanto u es raíz de $Xg-1\in K[X]$.
(1) $\Rightarrow$ (3). Como u es algebraico sobre K, entonces $K(u)=K[u]\simeq K[X]/\langle \operatorname{Irr}_K(u)\rangle$, en que el isomorfismo es $f(u)\leftrightarrow \overline{f}$. Luego aplicando el lema 2.10 deducimos que si $\operatorname{gr}\operatorname{Irr}_K(u)=n$, entonces $\left\{1,u,\dots,u^{n-1}\right\}$ es una base de $K(u)$ sobre K.
(3) $\Rightarrow$ (1): Si $[K(u):K]=n$, entonces $\{1,u,\dots,u^n\}$ es linealmente dependiente sobre K, luego existen $a_0,\dots,a_n\in K$ no todos nulos tales que $a_0+a_1u+\cdots+a_nu^n=0$. $\square$

Observación 2.12. Notar que en el teorema anterior probamos que si u es algebraico sobre K y el grado de $\operatorname{Irr}_K(u)$ es n, entonces $[K(u):K]=n$ y $\left\{1,u,\dots,u^{n-1}\right\}$ es una base de $K(u)$ sobre K.

Proposición 2.13. *Sea $F\supset E\supset K$ una torre de extensiones y $u\in F$ algebraico sobre K. Entonces u es algebraico sobre E y $\operatorname{Irr}_E(u)$ divide a $\operatorname{Irr}_K(u)$ en $E[X]$.*

Dem. Sea $f=\operatorname{Irr}_K(u)\in K[X]$. Como es $K[X]\subset E[X]$, entonces $f\in E[X]$ y $f(u)=0$, luego u es algebraico sobre E y $\operatorname{Irr}_E(u)\mid f$ en $E[X]$. $\square$

Ejemplo 2.14. Consideremos la extensión $\mathbb{R}\supset\mathbb{Q}$ y $u=\sqrt{2}+\sqrt{3}$. El elemento u verifica

$$\begin{aligned} u-\sqrt{2}=\sqrt{3}\ \Rightarrow\ \left(u-\sqrt{2}\right)^2=3\ \Rightarrow\ u^2-2\sqrt{2}u+2=3\ \Rightarrow\ \left(u^2-1\right)^2=\left(2\sqrt{2}u\right)^2\\ \Rightarrow\ u^4-2u^2+1=8u^2\ \Rightarrow\ u^4-10u^2+1=0.\end{aligned}$$

Luego u es raíz de $f=X^4-10X^2+1\in\mathbb{Q}[X]$. Estudiaremos la irreducibilidad de f. Notar que por el lema de Gauss alcanza con probar que f es irreducible en $\mathbb{Z}[X]$. Si f no es irreducible, entonces es porque se puede escribir como producto de un polinomio de grado 1 por uno de grado 3 o por dos de grado 2. Si se diese el primer caso, entonces f tendría una raíz racional, pero aplicando la proposición 1.6 deducimos que eso no ocurre. La otra posibilidad es que existan $a,b,c,\alpha,\beta,\gamma\in\mathbb{Z}$ tales que

$$X^4-10X^2+1=\left(aX^2+bX+c\right)\left(\alpha X^2+\beta X+\gamma\right).$$

Luego tiene que valer

$$a\alpha=1,\quad a\beta+b\alpha=0,\quad a\gamma+b\beta+c\alpha=-10,\quad b\gamma+c\beta=0,\quad c\gamma=1.$$

Como estamos en $\mathbb{Z}$, la primer igualdad implica $a=\alpha=\pm1$. Podemos suponer $a=\alpha=1$ (si no, entonces multiplicamos ambos polinomios por -1). Luego obtenemos

$$\beta+b=0,\quad \gamma+b\beta+c=-10,\quad b\gamma+c\beta=0,\quad c\gamma=1.$$

De la última ecuación obtenemos $c=\gamma=\pm1$. Sustituyendo por esos valores en las fórmulas de arriba obtenemos dos posibilidades

$$\begin{aligned} \beta+b=0,\quad b\beta=-12,\quad b+\beta=0\quad &\Rightarrow\quad b^2=12,\\ \beta+b=0,\quad b\beta=-8,\quad -b-\beta=0\quad &\Rightarrow\quad b^2=8.\end{aligned}$$

Como ninguna de esas ecuaciones tiene solución en $\mathbb{Z}$, deducimos que $f=X^4-10X^2+1$ es irreducible en $\mathbb{Z}[X]$ y por lo tanto en $\mathbb{Q}[X]$. Luego $\operatorname{Irr}_{\mathbb{Q}}(u)=X^4-10X^2+1$. Esto implica $[\mathbb{Q}(u):\mathbb{Q}]=4$.

Notar que en este caso se pueden hallar fácilmente las raíces de f que son $\pm\sqrt{2}\pm\sqrt{3}$; luego

$$f = \left(X-\sqrt{2}-\sqrt{3}\right)\left(X-\sqrt{2}+\sqrt{3}\right)\left(X+\sqrt{2}-\sqrt{3}\right)\left(X+\sqrt{2}+\sqrt{3}\right).$$

A partir de la factorización de arriba obtenemos

$$\begin{aligned} f &= \left(X^2-2\sqrt{2}X-1\right)\left(X^2+2\sqrt{2}X-1\right) \text{ en } \mathbb{Q}\left(\sqrt{2}\right)[X],\\ f &= \left(X^2-2\sqrt{3}X+1\right)\left(X^2+2\sqrt{3}X+1\right) \text{ en } \mathbb{Q}\left(\sqrt{3}\right)[X],\\ f &= \left(X^2-5-2\sqrt{6}\right)\left(X^2-5+2\sqrt{6}\right) \text{ en } \mathbb{Q}\left(\sqrt{6}\right)[X]. \end{aligned}$$

Notar que $u^{-1}=\sqrt{3}-\sqrt{2}$, luego $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}\in\mathbb{Q}(u)$ y por lo tanto $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt{6})$ son subcuerpos de $\mathbb{Q}(u)$. Es fácil de probar que vale $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{3}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{6}\right):\mathbb{Q}\right]=2$, luego $\left[\mathbb{Q}(u):\mathbb{Q}\left(\sqrt{2}\right)\right]=\left[\mathbb{Q}(u):\mathbb{Q}\left(\sqrt{3}\right)\right]=\left[\mathbb{Q}(u):\mathbb{Q}\left(\sqrt{6}\right)\right]=2$. Esto implica $u\notin\mathbb{Q}\left(\sqrt{2}\right)$, $u\notin\mathbb{Q}\left(\sqrt{3}\right)$ y $u\notin\mathbb{Q}\left(\sqrt{6}\right)$. Por lo tanto

$$\operatorname{Irr}_{\mathbb{Q}(\sqrt{2})}(u)=X^2-2\sqrt{2}X-1,\qquad \operatorname{Irr}_{\mathbb{Q}(\sqrt{3})}(u)=X^2-2\sqrt{3}X+1,\qquad \operatorname{Irr}_{\mathbb{Q}(\sqrt{6})}(u)=X^2-5-2\sqrt{6}.$$

Corolario 2.15. *Si F/K es una extensión y $u_1,\dots,u_n\in F$ son algebraicos sobre K, entonces*

$$K(u_1,\dots,u_n)=K[u_1,\dots,u_n].$$

Dem. Como u_1 es algebraico sobre K, es $K(u_1)=K[u_1]$. Como u_2 es algebraico sobre K, entonces es algebraico sobre $K(u_1)$, luego

$$K(u_1,u_2)=\big(K(u_1)\big)(u_2)=\big(K(u_1)\big)[u_2]=\big(K[u_1]\big)[u_2]=K[u_1,u_2].$$

El resto sigue por inducción en n. □

Definición 2.16. Una extensión F/K se dice *algebraica* si todo elemento de F es algebraico sobre K, en caso contrario se dice que es *trascendente*.

Ejemplos 2.17.

1. K/K es algebraica.
2. $K(X)/K$ es trascendente y simple.
3. $\mathbb{C}/\mathbb{R}$ es finita y simple ($[\mathbb{C}:\mathbb{R}]=2$, $\mathbb{C}=\mathbb{R}(i)$).
4. $\mathbb{R}/\mathbb{Q}$ es trascendente (e y π son trascendentes sobre $\mathbb{Q}$).

Las extensiones que más nos interesan son las finitas. Los siguientes resultados describen algunas de sus propiedades.

Teorema 2.18.

1. *Toda extensión finita es algebraica.*
2. *Una extensión es finita si y solo si está finitamente generada por elementos algebraicos.*

Dem. (1). Si F/K es finita y $u\in F$, entonces la proposición 2.8 implica que $K(u)/K$ es finita y por lo tanto u es algebraico sobre K. Luego F/K es algebraica.

(2). Sea F/K finita y $\{u_1,\dots,u_n\}$ una base de F como K-espacio vectorial. Entonces $u_1,\dots,u_n$ son algebraicos sobre K por la parte (1) y $F=Ku_1+\cdots+Ku_n\subset K(u_1,\dots,u_n)\subset F$, luego $F=K(u_1,\dots,u_n)$.

Recíprocamente, supongamos que $F = K(u_1, \ldots, u_n)$, con $u_1, \ldots, u_n$ algebraicos sobre K. Consideremos la torre

$$F = K(u_1, \ldots, u_n) \supset K(u_1, \ldots, u_{n-1}) \supset \cdots \supset K(u_1, u_2) \supset K(u_1) \supset K.$$

Como u_1 es algebraico sobre K, entonces $K(u_1)/K$ es finita. Como u_2 es algebraico sobre K, entonces u_2 es algebraico sobre $K(u_1)$, luego $K(u_1, u_2)/K(u_1)$ es finita. Razonando de esta forma se prueba que $K(u_1, \ldots, u_i)/K(u_1, \ldots, u_{i-1})$ es finita para todo $i = 2, \ldots, n$. Luego aplicando reiteradamente la proposición 2.8 se deduce que F/K es finita. $\square$

Observación 2.19. La extensión $\mathbb{Q}(S)/\mathbb{Q}$ siendo $S = \left\{\sqrt{p} : \ p \text{ primo}\right\}$, es algebraica pero no es finita[2].

Proposición 2.20. *Sea F/K una extensión y consideremos $E = \{u \in F : \ u \text{ es algebraico sobre } K\}$. Entonces E es un subcuerpo de F y por lo tanto E/K es una extensión algebraica.*

Dem. Es claro que $K \subset E$. Sean $u, v \in E$, con $v \neq 0$. La extensión $K(u,v)/K$ es algebraica por el teorema anterior. Como $u - v, uv^{-1} \in K(u,v)$, entonces son algebraicos sobre K, es decir, $u - v, uv^{-1} \in E$. $\square$

Observación 2.21. El cuerpo E construido en la proposición anterior es la mayor extensión algebraica de K contenida en F.

La siguiente proposición permite construir extensiones finitas, partiendo de extensiones finitas conocidas.

Proposición 2.22. *Asumimos que todos los cuerpos son subcuerpos de algún cuerpo F.*

1. *Si E y L son extensiones de K tales que E/K y L/K son finitas, entonces EL/K es finita.*

2. *Sea E/K una extensión finita y L/K una extensión arbitraria. Entonces LE/L es finita.*

Dem. Para la primer parte, aplicando el teorema 2.18 sabemos que existen $u_1, \ldots, u_m \in E$ y $v_1, \ldots, v_n \in L$ elementos algebraicos sobre K tales que $E = K(u_1, \ldots, u_m)$ y $L = K(v_1, \ldots, v_n)$. Luego

$$EL = K(u_1, \ldots, u_m)K(v_1, \ldots, v_n) = K(u_1, \ldots, u_m, v_1, \ldots, v_n).$$

Entonces el teorema 2.18 implica que EL/K es finita.

Para la segunda, como E/K es finita, entonces existe un subconjunto finito S formado por elementos algebraicos sobre K tal que $E = K(S)$. Dada $L \supset K$ una extensión arbitraria, es $LE = LK(S) = L(S)$ siendo los elementos de S algebraicos sobre L; luego $LE/L = L(S)/L$ es finitamente generada por elementos algebraicos y por lo tanto es finita. $\square$

Importante. Para simplificar la teoría, de ahora en adelante trabajaremos siempre dentro del cuerpo de números complejos $\mathbb{C}$. Luego cuando escribamos "sea K un cuerpo ..." implícitamente estaremos asumiendo que K es un subcuerpo $\mathbb{C}$. En particular esto implica $\operatorname{car} K = 0$ y $\mathbb{Q} \subset K$.

2.3. Extensiones finitas en $\mathbb{C}$

Empezamos probando algunas propiedades de los polinomios con coeficientes en un cuerpo.

Proposición 2.23. *Sea K un cuerpo y $f, g \in K[X]$. Si F/K es una extensión arbitraria, entonces el máximo comun divisor de f y g en $F[X]$ coincide con el máximo comun divisor de f y g en $K[X]$.*

[2]Intuitivamente parece cierto, pero es difícil de probar que $\mathbb{Q}(S)/\mathbb{Q}$ que es infinita

Dem. Sean d_K y d_F los máximos comunes divisores de f y g en $K[X]$ y $F[X]$, respectivamente. Como d_K divide a f y g en $F[X]$, entonces d_K divide a d_F en $F[X]$. Por otro lado sabemos que existen $p, q \in K[X]$ tales que $d_K = pf + qg \in K[X]$; luego, como d_F divide a f y g en $F[X]$, entonces d_F divide a d_K en $F[X]$. Al ser ambos mónicos se deduce $d_K = d_F$. $\square$

Observación 2.24. La proposición anterior permite escribir al máximo común divisor de $f, g \in K[X]$ mediante $\text{mcd}(f, g)$ sin hacer referencia al cuerpo K.

Definición 2.25. Si $f = a_n X^n + \cdots + a_2 x^2 + a_1 x + a_0 \in K[X]$, se define la *derivada*[3] de f mediante $f' = n a_n X^{n-1} + \cdots + 2a_2 x + a_1$. Es fácil de probar que valen las propiedades usuales de la derivada de funciones:

$$(af + g)' = af' + g', \qquad (fg)' = f'g + fg' \text{ (regla de Leibniz)}, \qquad \forall f, g \in K[X],\ a \in K.$$

Proposición 2.26. *Si $f \in K[X]$, entonces f tiene una raíz múltiple en $\mathbb{C}$ si y solo si* $\text{mcd}(f, f') \neq 1$.

Dem. Si existen F extensión de K, $u \in F$ y $g \in F[X]$ tales que $f = g(X-u)^2 \in F[X]$, entonces $f' = g'(X-u)^2 + 2g(X-u)$; luego $X - u$ divide a f y f' en $F[X]$ y por lo tanto $\text{mcd}(f, f') \neq 1$.
Supongamos $\text{mcd}(f, f') \neq 1$. Sea u una raíz de $\text{mcd}(f, f')$ en alguna extensión F de K. Luego $X - u$ divide a f y f' en $F[X]$. Si $h \in F[X]$ verifica $f = h(X-u) \in F[X]$, entonces $f' = h'(X-u) + h$ y por lo tanto $X - u$ divide a h; luego $(X-u)^2$ divide a f. $\square$

Observación 2.27. Sea K un cuerpo y $f \in K[X]$. Entonces $f' = 0$ si y solo si f es constante[4].

Proposición 2.28. *Sea K un cuerpo y $f \in K[X]$ un polinomio irreducible. Entonces f tiene solo raíces simples.*

Dem. Si f tuviese una raíz múltiple, sería $\text{mcd}(f, f') \neq 1$ y como f es irreducible esto implicaría que f divide a f'. Pero como el grado de f' es menor que el de f, la única posibilidad es $f' = 0$. Pero esto último nos dice que f tiene que ser constante, lo cual no es posible si f es irreducible. $\square$

A continuación probaremos que en el caso complejo toda extensión finita es simple. Este resultado se conoce como el *teorema del elemento primitivo.*

Lema 2.29. *Sean K un cuerpo y $u, v \in \mathbb{C}$ elementos algebraicos sobre K. Entonces existe $w \in \mathbb{C}$ tal que $K(u, v) = K(w)$.*

Dem. Sean $f, g \in K[X]$ los polinomios irreducibles de u y v, respectivamente. Sean $u = u_1, u_2, \ldots, u_m \in \mathbb{C}$ las raíces de f y $v = v_1, v_2, \ldots, v_n \in \mathbb{C}$ las raíces de g. La proposición anterior implica que estas raíces son simples, luego

$$f = (X-u)(X-u_2)\cdots(X-u_m), \qquad g = (X-v)(X-v_2)\cdots(X-v_n). \tag{2}$$

Consideremos los siguientes números complejos

$$\frac{u_i - u}{v - v_j}, \quad \forall i = 1, \ldots, m,\ j = 2, \ldots, n.$$

Elegimos $z \in \mathbb{Q}$ que sea distinto de los números anteriores. Sea $w = u + zv$. Probaremos $K(u, v) = K(w)$.

[3]En los números complejos se define la derivada de una función de la misma forma que en $\mathbb{R}$ y tiene propiedades similares. En particular en los polinomios coincide con la fórmula que dimos.

[4]Esta afirmación no es cierta en cuerpos de característica positiva.

Como es $w = u+zv$ entonces es claro que vale $K(w) \subset K(u,v)$. Luego solo nos resta probar $K(u,v) \subset K(w)$. Consideremos $h = f(w - zX) \in K(w)[X]$, siendo f el polinomio irreducible de u considerado antes. Evaluando en v obtenemos $h(v) = f(w - zv) = f(u) = 0$, luego $X - v$ divide a h en $\mathbb{C}[X]$. Como claramente $X - v$ divide a g (el polinomio irreducible de v), deducimos que $X - v$ divide a $d = \mathrm{mcd}(h, g)$ en $\mathbb{C}[X]$.
Probaremos que vale $d = X - v$. Para esto, como d divide a $g = (X - v)(X - v_2)\cdots(X - v_n)$, alcanza con probar que $v_2, \ldots, v_n$ no son raíces de d.
Supongamos razonando por el absurdo que existe $j \geq 2$ tal que $d(v_j) = 0$. Entonces v_j tiene que ser raíz de h, y por lo tanto $f(w - zv_j) = 0$. Luego $w - zv_j$ tiene que ser una de las raíces de f que son $u_1, u_2, \ldots, u_m$. Entonces existe $i \geq 1$ tal que

$$w - zv_j = u_i \quad \Rightarrow \quad u + zv - zv_j = u_i \quad \Rightarrow \quad z = \frac{u_i - u}{v - v_j},$$

contradiciendo nuestra elección de z. Luego $\mathrm{mcd}(h, g) = X - v$. Pero como $h, g \in K(w)[X]$, deducimos $X - v \in K(w)[X]$; luego $v \in K(w)$. Finalmente al ser $u = w - zv$ concluímos que u también está en $K(w)$. Entonces probamos que u y v están en $K(w)$ lo cual implica $K(u,v) \subset K(w)$. □

Teorema 2.30 (Teorema del elemento primitivo)**.** *Si F/K es una extensión finita, entonces existe $u \in F$ tal que $F = K(u)$.*

Dem. Como F/K es finita, entonces existen $u_1, \ldots, u_n \in F$ algebraicos sobre K tales que $F = K(u_1, \ldots, u_n)$. Consideremos la torre

$$F = K(u_1, \ldots, u_n) \supset K(u_1, \ldots, u_{n-1}) \supset \cdots \supset K(u_1, u_2, u_3) \supset K(u_1, u_2) \supset K(u_1) \supset K.$$

Aplicando el lema anterior obtenemos que existe $w_2 \in \mathbb{C}$ tal que $K(u_1, u_2) = K(w_2)$. Luego $K(u_1, u_2, u_3) = K(u_1, u_2)(u_3) = K(w_2)(u_3) = K(w_2, u_3)$. Aplicando de nuevo el lema obtenemos que existe $w_3 \in \mathbb{C}$ tal que $K(w_2, u_3) = K(w_3)$ y por lo tanto $K(u_1, u_2, u_3) = K(w_3)$. Entonces $K(u_1, u_2, u_3, u_4) = K(w_3, u_4)$ y seguimos repitiendo el procedimiento hasta obtener $F = K(u_1, \ldots, u_n) = K(u)$, para cierto $u \in \mathbb{C}$. □

Observación 2.31. Para que valga el teorema del elemento primitivo solo se requiere característica cero, pero hay que fundamentar mejor la prueba.

2.4. Morfismos entre extensiones

Recordar que si K y F son dos cuerpos, entonces un morfismo de cuerpos $\varphi : K \to F$ es simplemente un morfismo de anillos. Un morfismo de cuerpos siempre es inyectivo. En general abreviaremos "morfismo de cuerpos" en "morfismo". Un isomorfismo es un morfismo biyectivo. Un *automorfismo* es un isomorfismo de un cuerpo en sí mismo.

Definición 2.32. Sean F y E dos extensiones de un mismo cuerpo K. Un morfismo $\sigma : F \to E$ se dice que es un *K-morfismo* si $\sigma|_K = \mathrm{id}$. Esto se suele representar mediante el siguiente diagrama

$$\begin{tikzcd} F \arrow[rr, "\sigma"] \arrow[dr, dash] & & E \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Las definiciones de *K-isomorfismo* y *K-automorfismo* son las naturales.

Observación 2.33. 1. Como estamos considerando los cuerpos los contenidos en $\mathbb{C}$, entonces todo morfismo es un $\mathbb{Q}$-morfismo.

2. Todo K-morfismo es un operador K-lineal. Luego si F es una extensión finita de K y $\sigma : F \to F$ es un K-morfismo, entonces σ es un K-automorfismo (por ser K-lineal e inyectivo).

Proposición 2.34. *Sean F/K y E/K extensiones, $\sigma : F \to E$ un K-morfismo. Si $f \in K[X]$, entonces σ lleva raíces de f en F en raíces de f en E. Luego si $E = F$, entonces σ permuta las raíces de f en F.*

Dem. Si $f(u) = 0$, entonces $0 = \sigma\big(f(u)\big) = f\big(\sigma(u)\big)$. Luego si $E = F$ y R es el conjunto de las raíces de f en F, entonces $\sigma(R) \subset R$ y como σ es inyectivo y R es finito se deduce que $\sigma|_R : R \to R$ es biyectivo. $\square$

Proposición 2.35. *Sea K un cuerpo y $f \in K[X]$ un polinomio irreducible. Si $u, v \in \mathbb{C}$ son raíces de f, entonces existe un único K-isomorfismo $\sigma : K(u) \to K(v)$ tal que $\sigma(u) = v$.*

Dem. La unicidad es inmediata: si existe un tal isomorfismo σ, entonces tiene que estar definido por $\sigma\left(\sum_{i=0}^{n} a_i u^i\right) = \sum_{i=0}^{n} a_i v^i$, para todo $a_0, \ldots, a_n \in K$ y todo $n \in \mathbb{N}$.
Para la existencia podemos suponer que f es mónico, luego $f = \operatorname{Irr}_K(u) = \operatorname{Irr}_K(v)$. Entonces σ queda definido por la composición de los siguientes K-isomorfismos

$$K(u) = K[u] \simeq \frac{K[X]}{\langle \operatorname{Irr}_K(u) \rangle} = \frac{K[X]}{\langle f \rangle} = \frac{K[X]}{\langle \operatorname{Irr}_K(v) \rangle} \simeq K[v] = K(v). \quad \square$$

Proposición 2.36. *Sea $u \in \mathbb{C}$ algebraico sobre K y F/K una extensión arbitraria.*

1. *El mapa $\sigma \mapsto \sigma(u)$ define una correspondencia uno a uno entre los morfismos*

$$\begin{tikzcd} K(u) \arrow[rr, "\sigma"] & & F \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

y las raíces de $\operatorname{Irr}_K(u)$ *en F.*

2. *Vale*
$$\#\{\sigma : K(u) \to F : \ \sigma \text{ es un } K\text{-morfismo}\} \le [K(u) : K]. \tag{3}$$
Además, vale el igual en (3) *si y solo si F contiene a todas las raíces de* $\operatorname{Irr}_K(u)$.

Dem. Sea $f = \operatorname{Irr}_K(u)$. Como u es una raíz de f en $K(u)$, entonces la proposición 2.34 implica que si $\sigma : K(u) \to F$ es un K-morfismo, entonces $\sigma(u)$ es una raíz de f en F. Recíprocamente, si $v \in F$ es una raíz de f, entonces la proposición 2.35 implica que existe un K-morfismo $\alpha : K(u) \to K(v)$ tal que $\alpha(u) = v$. Componiendo este morfismo con la inclusión $K(v) \hookrightarrow F$ obtenemos un K-morfismo $\sigma : K(u) \to F$ tal que $\sigma(u) = v$. Como todo K-morfismo de $K(u)$ en F queda determinado por su valor en u, entonces deducimos que la correspondencia $\sigma \mapsto \sigma(u)$ es biyectiva.

La desigualdad (3) se deduce de lo siguiente

$$\#\{\sigma : K(u) \to F : \ \sigma \text{ es un } K\text{-morfismo}\} = \#\{\text{raíces de } f \text{ en } F\} \le \#\{\text{raíces de } f\} \le \operatorname{gr} f = [K(u) : K].$$

Observar que vale el igual en (3) si y solo si $\#\{\text{raíces de } f \text{ en } F\} = \operatorname{gr} f$. Como f es irreducible entonces tiene solo raíces simples y por lo tanto $\#\{\text{raíces de } f\} = \operatorname{gr} f$. Luego $\#\{\text{raíces de } f \text{ en } F\} = \operatorname{gr} f$ si y solo si $\#\{\text{raíces de } f \text{ en } F\} = \#\{\text{raíces de } f\}$, y esto ocurre si y solo si todas las raíces de f están en F. $\square$

Ejemplo 2.37. Consideremos el polinomio $f = X^4 - 2 \in \mathbb{Q}[X]$. El criterio de Eisenstein implica que f es irreducible en $\mathbb{Q}[X]$. Notar que f tiene raíces $\pm w$ y $\pm wi$, siendo $w = \sqrt[4]{2} \in \mathbb{R}$. Consideremos $\mathbb{Q}(w)$ y $F = \mathbb{Q}(w,i)$. Como $\pm w, \pm wi \in F$ y $[\mathbb{Q}(w) : \mathbb{Q}] = \operatorname{gr} f = 4$, entonces sabemos que hay exactamente 4 morfismos $\sigma_1, \sigma_2, \sigma_3, \sigma_4 : \mathbb{Q}(w) \to F$ que quedan determinados por

$$\sigma_1(w) = w, \quad \sigma_2(w) = -w, \quad \sigma_3(w) = wi, \quad \sigma_4(w) = -wi.$$

Notar que σ_1 es simplemente la inclusión $\mathbb{Q}(w) \hookrightarrow \mathbb{Q}(w,i) = F$. Vamos a dar una descripción explícita de estos morfismos. Como f es irreducible en $\mathbb{Q}[X]$, entonces $\operatorname{Irr}_{\mathbb{Q}}(w) = f$ y por lo tanto $[\mathbb{Q}(w) : \mathbb{Q}] = 4$ y $\mathcal{B} = \{1, w, w^2, w^3\}$ es una base de $\mathbb{Q}(w)$. En esa base es

$$\begin{aligned}
\sigma_1\left(a + bw + cw^2 + dw^3\right) &= a + bw + cw^2 + dw^3,\\
\sigma_2\left(a + bw + cw^2 + dw^3\right) &= a - bw + cw^2 - dw^3,\\
\sigma_3\left(a + bw + cw^2 + dw^3\right) &= a + bwi - cw^2 - dw^3 i,\\
\sigma_4\left(a + bw + cw^2 + dw^3\right) &= a - bw - cw^2 + dw^3 i,
\end{aligned}$$

para todo $a, b, c, d \in \mathbb{Q}$.

Morfismo $K[X] \to F[X]$ inducido por un morfismo $K \to F$. Si $\sigma : K \to F$ es un morfismo de cuerpos, entonces podemos definir un mapa $K[X] \to F[X]$ que a cada $f = \sum_{i=0}^n a_i X^i \in K[X]$ le hace corresponder $\sigma f \in F[X]$ definido por $\sigma f = \sum_{i=0}^n \sigma(a_i) X^i$. Es fácil de probar que vale

$$\sigma 1 = 1, \qquad \sigma(f+g) = \sigma f + \sigma g, \qquad \sigma(f \cdot g) = \sigma f \cdot \sigma g, \qquad \forall f, g \in K[X].$$

Además es claro que $\sigma f = 0$ implica $f = 0$. Luego $f \mapsto \sigma f$ es un morfismo de anillos inyectivo. En particular obtenemos $K[X] \simeq \sigma(K)[X] \subset F[X]$. Notar que $f(u) = 0$ en K implica $\sigma f\big(\sigma(u)\big) = 0$ en F.

El siguiente resultado es una generalización de la proposición 2.36.

Proposición 2.38. *Sean $\sigma : K \to F$ un morfismo de cuerpos y $u \in \mathbb{C}$ algebraico sobre K. Consideremos $f = \operatorname{Irr}_K(u) \in K[X]$. Entonces:*

1. *Si σf tiene alguna raíz v en F, entonces existe un morfismo $\tau : K(u) \to F$ tal que $\tau|_K = \sigma$ y $\tau(u) = v$.*

$$\begin{tikzcd}
K(u) \arrow[r, "\tau"] & F \\
K \arrow[u, dash] \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

2. *El mapa $\tau \mapsto \tau(u)$ define una correspondencia uno a uno entre*

$$\{\tau : K(u) \to F : \ \tau \text{ morfismo y } \tau|_K = \sigma\} \leftrightarrow \{\text{raíces de } \sigma f \text{ en } F\}.$$

Dem. (1). Sea $v \in F$ una raíz de $\sigma f \in F[X]$. El morfismo de cuerpos $\sigma : K \to F$ induce un isomorfismo de anillos $K[X] \to \sigma(K)[X]$ definido por $g \mapsto \sigma g$. Luego, como $f \in K[X]$ es mónico e irreducible, entonces $\sigma f \in \sigma(K)[X]$ es mónico e irreducible y por lo tanto $\sigma f = \operatorname{Irr}_{\sigma(K)}(v) \in \sigma(K)[X]$.
El isomorfismo $K[X] \to \sigma(K)[X]$ compuesto con la proyección canónica $\sigma(K)[X] \to \sigma(K)[X]/\langle \sigma f \rangle$ define un morfismo de anillos sobreyectivo $K[X] \to \sigma(K)[X]/\langle \sigma f \rangle$, mediante $g \mapsto \overline{\sigma g}$.
Sea $g \in K[X]$. Notar que $\overline{\sigma g} = \overline{0}$ en $\sigma(K)[X]/\langle \sigma f \rangle$ si y solo si σf divide a σg en $\sigma(K)[X]$ lo cual equivale a que f divide a g en $K[X]$. Luego el núcleo del morfismo sobreyectivo $K[X] \to \sigma(K)[X]/\langle \sigma f \rangle$ es el ideal generado

por f y por lo tanto aplicando la proposición 1.2 obtenemos un isomorfismo $K[X]/\langle f\rangle \to \sigma(K)[X]/\langle \sigma f\rangle$ definido por $\overline{g} \mapsto \overline{\sigma g}$. Luego podemos definir un isomorfismo $\hat{\sigma} : K(u) \to \sigma(K)(v)$ mediante

$$K(u) = K[u] \simeq \frac{K[X]}{\langle f\rangle} \simeq \frac{\sigma(K)[X]}{\langle \sigma f\rangle} \simeq \sigma(K)[v] = \sigma(K)(v).$$

Explícitamente $\hat{\sigma}\left(\sum_{i=0}^n a_i u^i\right) = \sum_{i=0}^n \sigma(a_i) v^i$, para todo $a_0, \dots, a_n \in K$ y todo $n \in \mathbb{N}$. Finalmente si definimos $\tau : K(u) \to F$ como la composición $K(u) \xrightarrow{\hat{\sigma}} \sigma(K)(v) \hookrightarrow F$, entonces $\tau|_K = \sigma$ y $\tau(u) = v$.

(2). Si $\tau : K(u) \to F$ es un morfismo que verifica $\tau|_K = \sigma$, entonces $0 = \tau\big(f(u)\big) = \tau f\big(\tau(u)\big) = \sigma f\big(\tau(u)\big)$, luego $\tau(u)$ es raíz de σf. Como $K(u)$ está generado por K y u, es claro que el mapa $\tau \mapsto \tau(u)$ es inyectivo; la sobreyectividad de este mapa es la tesis de la parte (1). $\square$

Observación 2.39. Las dos proposiciones anteriores nos permiten, al menos en teoría, hallar todos los K-automorfismos de F, cuando F/K es una extensión finita. Para eso escribimos $F = K(u_1, \dots, u_n)$ siendo $u_1, \dots, u_n \in F$ elementos algebraicos sobre K y consideramos la torre

$$F = K(u_1, \dots, u_n) \supset \cdots \supset K(u_1, u_2) \supset K(u_1) \supset K.$$

Aplicando la proposición 2.36 hallamos todos los K-morfismos $K(u_1) \to F$. Luego aplicando la proposición 2.38 hallamos todas las extensiones posibles de cada uno de estos morfismos a $K(u_1, u_2) \to F$. Y así seguimos aplicando reiteradamente la proposición 2.38 hasta obtener K-morfismos de $F = K(u_1, \dots, u_n)$ en F. Como F/K es finita, entonces los K-morfismos $F \to F$ son automáticamente K-automorfismos. Notar además que si $\sigma : F \to F$ es un K-automorfismo, entonces σ es una extensión de su restricción a $K(u_1, \dots, u_{n-1})$, que es un K-morfismo de $K(u_1, \dots, u_{n-1})$ a F. Siguiendo con ese razonamiento se deduce que todo K-automorfismo de F se puede obtener mediante la serie de extensiones descrita anteriormente.

Ejemplo 2.40. Consideremos de nuevo el polinomio irreducible $f = X^4 - 2 \in \mathbb{Q}[X]$ que tiene raíces $\pm w$ y $\pm wi$, siendo $w = \sqrt[4]{2} \in \mathbb{R}$. En el ejemplo 2.37 vimos que si $F = \mathbb{Q}(w, i)$, entonces hay exactamente 4 morfismos $\sigma_1, \sigma_2, \sigma_3, \sigma_4 : \mathbb{Q}(w) \to F$ que quedan determinados por

$$\sigma_1(w) = w, \quad \sigma_2(w) = -w, \quad \sigma_3(w) = wi, \quad \sigma_4(w) = -wi.$$

Observar que $F = \mathbb{Q}(w)(i)$ es una extensión simple de $\mathbb{Q}(w)$. Consideremos $\operatorname{Irr}_{\mathbb{Q}}(i) = X^2 + 1$. Como es $\mathbb{Q}(w) \subset \mathbb{R}$ y $i \notin \mathbb{R}$, entonces $X^2 + 1$ es irreducible en $\mathbb{Q}(w)$ y por lo tanto $\operatorname{Irr}_{\mathbb{Q}(w)}(i) = X^2 + 1$. Como $X^2 + 1 \in \mathbb{Q}[X]$, entonces $\sigma_l(X^2 + 1) = X^2 + 1$ para cada morfismo σ_l. Notar que las raíces de $X^2 + 1$ son $\pm i \in F$ luego cada morfismo $\sigma_l : \mathbb{Q}(w) \to F$ da lugar a dos morfismos $\alpha_l, \beta_l : \mathbb{Q}(w)(i) \to F$ caracterizados por $\alpha_l|_{\mathbb{Q}(w)} = \alpha_l|_{\mathbb{Q}(w)} = \sigma_l$, $\alpha_l(i) = i$ y $\beta_l(i) = -i$. Diagramáticamente es

$$\begin{tikzcd} \mathbb{Q}(w)(i) \arrow[r, "\alpha_l"] & F \\ \mathbb{Q}(w) \arrow[u, dash] \arrow[ur, "\sigma_l"'] & \end{tikzcd}, \qquad \begin{tikzcd} \mathbb{Q}(w)(i) \arrow[r, "\beta_l"] & F \\ \mathbb{Q}(w) \arrow[u, dash] \arrow[ur, "\sigma_l"'] & \end{tikzcd}$$

Luego existen 8 automorfismos $\alpha_l, \beta_l : F \to F$, $l = 1, 2, 3, 4$, caracterizados por las condiciones anteriores. Hallando una $\mathbb{Q}$-base de $F = \mathbb{Q}(w, i)$ se pueden obtener fórmulas explícitas para estos morfismos, razonando como en el ejemplo 2.37.

3. Teoría de Galois

En este capítulo trabajaremos siempre dentro de $\mathbb{C}$. Todo lo que haremos vale también para cuerpos arbitrarios de característica cero. En característica positiva aparecen ciertas dificultades que obligan a imponer más condiciones para obtener el mismo tipo de resultados.

3.1. El grupo de Galois

Sea F un cuerpo. El conjunto $\operatorname{Aut}(F) = \{\sigma : F \to F|\ \sigma \text{ es un isomorfismo de cuerpos}\}$ es un subgrupo de $\operatorname{Biy}(F)$. El *grupo de Galois* de una extensión F/K es

$$\operatorname{Gal}(F/K) := \{\sigma \in \operatorname{Aut}(F) :\ \sigma|_K = \mathrm{id}\}.$$

Notar que es $\operatorname{Gal}(F/K) = \operatorname{Aut}(F) \cap \operatorname{GL}_K(F)$, siendo $\operatorname{GL}_K(F) = \{\varphi : F \to F|\ \varphi \text{ isomorfismo } K\text{-lineal}\}$. Esto implica que $\operatorname{Gal}(F/K)$ es un subgrupo de $\operatorname{Aut}(F)$ y por lo tanto $\operatorname{Gal}(F/K)$ es un grupo.

Aplicando la proposición 2.36 se obtiene el grupo de Galois de una extensión algebraica simple.

Proposición 3.1. *Sea $u \in \mathbb{C}$ algebraico sobre K y $f = \operatorname{Irr}_K(u)$. Entonces el mapa $\sigma \mapsto \sigma(u)$ define una correspondencia uno a uno entre $\operatorname{Gal}(K(u)/K)$ y las raíces de f en $K(u)$. Luego $\operatorname{Gal}(K(u)/K)$ es finito y*

$$|\operatorname{Gal}(K(u)/K)| = \#\{\textit{raíces de } f \textit{ en } K(u)\} \le [K(u) : K].$$

Además vale $|\operatorname{Gal}(K(u)/K)| = [K(u) : K]$ si y solo si todas las raíces (complejas) de f están en $K(u)$. □

Ejemplos 3.2. A continuación se determinan los grupos de Galois de algunas extensiones simples.

- $\mathbb{C}/\mathbb{R}$. Como $\mathbb{C} = \mathbb{R}(i)$ y $\operatorname{Irr}_{\mathbb{R}}(i) = X^2 + 1$ tiene raíces $\pm i \in \mathbb{C}$, entonces vale $|\operatorname{Gal}(\mathbb{C}/\mathbb{R})| = [\mathbb{C} : \mathbb{R}] = 2$; luego $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\} = C_2$. El morfismo σ queda caracterizado por $\sigma|_{\mathbb{R}} = \mathrm{id}$ y $\sigma(i) = -i$, luego σ es la *conjugación*: $\sigma(z) = \overline{z}$, para todo $z \in \mathbb{C}$.
- $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$. Es $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{2}\right) = X^2 - 2$ y sus raíces son $\pm\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$. Luego $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}\right) = \{\mathrm{id}, \sigma\}$, con $\sigma\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$, para todo $a, b \in \mathbb{Q}$.
- $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$. Es $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[3]{2}\right) = X^3 - 2$ que tiene raíces $\sqrt[3]{2},\ \mu\sqrt[3]{2},\ \mu^2\sqrt[3]{2}$, siendo $\mu = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Como la única raíz de $X^3 - 2$ que está en $\mathbb{Q}\left(\sqrt[3]{2}\right)$ es $\sqrt[3]{2}$, se deduce $\left|\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)\right| = 1$. Luego $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right) = \{\mathrm{id}\}$.
- $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$. Es $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[4]{2}\right) = X^4 - 2$ que tiene raíces $\pm\sqrt[4]{2},\ \pm i\sqrt[4]{2}$. Como las raíces de de $X^4 - 2$ que están en $\mathbb{Q}\left(\sqrt[4]{2}\right)$ son $\pm\sqrt[4]{2}$, se deduce $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\right) = \{\mathrm{id}, \sigma\}$, con $\sigma\left(\sqrt[4]{2}\right) = -\sqrt[4]{2}$.
- $\mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}$. En el ejemplo 2.40 vimos que este grupo tiene orden 8 y se puede describir mediante $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}\right) = \{\alpha_l, \beta_l :\ l = 1, 2, 3, 4\}$. Los morfismos α_l, β_l fueron hallados en el ejemplo 2.40.

El siguiente resultado muestra que el grupo de Galois de una extensión finita es un grupo finito, cuyo orden es menor o igual que el grado de la extensión.

Teorema 3.3. *Sea F/K una extensión finita. Entonces $\operatorname{Gal}(F/K)$ es finito y $|\operatorname{Gal}(F/K)| \le [F : K]$.*

Dem. El teorema 2.30 implica que existe $u \in F$ algebraico sobre K tal que $F = K(u)$. Luego aplicando la proposición anterior obtenemos

$$|\operatorname{Gal}(F/K)| = |\operatorname{Gal}(K(u)/K)| \le [K(u) : K] = [F : K]. \quad \square$$

3.2. Extensiones normales

Empezamos con algunas definiciones.

Sea K un cuerpo y $f \in K[X]$ un polinomio no constante. Decimos que f *se escinde* en $K[X]$ si f se puede escribir como producto de polinomios de grado uno en $K[X]$, *i.e.* si existen $a, u_1, \ldots, u_n \in K$ tales que $f = a(X - u_1) \cdots (X - u_n)$. Si en la descomposición anterior agrupamos los factores repetidos, entonces obtenemos $f = a(X - v_1)^{n_1} \cdots (X - v_k)^{n_k}$, siendo $v_1, \ldots, v_k$ las raíces distintas y $n_i \geq 1$, para todo i.

Observaciones 3.4.

1. Para abreviar, diremos "f se escinde en K", en vez de "f se escinde en $K[X]$".
2. Que $f \in K[X]$ se escinda en K equivale a que todas las raíces complejas de f estén en K.
3. El teorema fundamental del álgebra nos dice que en $\mathbb{C}$ todo polinomio de grado positivo se escinde.
4. Si $f \in K[X]$ es un polinomio de grado positivo, entonces f siempre escinde en $\mathbb{C}$, pero no necesariamente en K.

Sea K un cuerpo. El *cuerpo de descomposición* de $f \in K[X] \setminus K$ es $K(u_1, \ldots, u_m)$, siendo $u_1, \ldots, u_m \in \mathbb{C}$ las raíces de f en $\mathbb{C}$. Es el menor subcuerpo de $\mathbb{C}$ que contiene a K, en el cual f se escinde.

Ejemplo 3.5.

1. El polinomio $X^2 - 2 \in \mathbb{Q}[X]$ tiene raíces $\pm\sqrt{2}$, luego su cuerpo de descomposición es $\mathbb{Q}\left(\sqrt{2}, -\sqrt{2}\right) = \mathbb{Q}\left(\sqrt{2}\right)$.
2. Las raíces de $X^3 - 2 \in \mathbb{Q}[X]$ son $\sqrt[3]{2}$, $w\sqrt[3]{2}$ y $w^2\sqrt[3]{2}$, siendo $1 \neq w \in \mathbb{C}$ tal que $w^3 = 1$. Luego el cuerpo de descomposición de $X^3 - 2$ es $\mathbb{Q}\left(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}\right) = \mathbb{Q}\left(\sqrt[3]{2}, w\right)$.

Proposición 3.6. *Sea K un cuerpo y $f \in K[X]$ de grado $n \geq 1$. Si F es el cuerpo de descomposición de f, entonces $[F : K] \leq n!$.*

Dem. Sea $F = K(u_1, \ldots, u_m)$, siendo $u_1, \ldots, u_m$ las raíces distintas de f en $\mathbb{C}$.

Como $f \in K[X]$ y $f(u_1) = 0$, entonces $\operatorname{Irr}_K(u_1)$ divide a f y por lo tanto

$$[K(u_1) : K] \leq \operatorname{gr} f = n.$$

Como $u_1 \in K(u_1)$ y $f(u_1) = 0$, entonces existen $g_1 \in K(u_1)[X]$ y $n_1 \geq 1$ tales que $f = (X - u_1)^{n_1} g_1$ y $g_1(u_1) \neq 0$. Luego es $0 = f(u_2) = (u_2 - u_1)^{n_1} g_1(u_2)$. Como $u_1, \ldots, u_m$ son distintos, deducimos $g_1(u_2) = 0$. Luego

$$[K(u_1, u_2) : K(u_1)] = [K(u_1)(u_2) : K(u_1)] \leq \operatorname{gr} g_1 \leq n - 1.$$

Siguiendo con ese razonamiento terminamos probando que valen

$$[K(u_1) : K] \leq n,\ [K(u_1, u_2) : K(u_1)] \leq n - 1,\ \cdots,\ [K(u_1, \ldots, u_{m-1}, u_m) : K(u_1, \ldots, u_{m-1})] \leq n - (m - 1).$$

Luego $[K(u_1, \ldots, u_n) : K] \leq n(n-1) \cdots (n - m + 1) \leq n!$. □

En la proposición anterior la cota $n!$ puede alcanzarse o no, como lo muestran los siguientes ejemplos.

Ejemplos 3.7.

1. Si $f = X^4 - X^2 - 2 \in \mathbb{Q}[X]$, entonces sus raíces son $\pm\sqrt{2}$ y $\pm i$. Luego el cuerpo de descomposición de f es $\mathbb{Q}\left(\sqrt{2}, i\right)$. Consideremos la torre

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\left(\sqrt{2}, i\right)$$

Como $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{2}\right) = X^2 - 2$, entonces $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$. Observar $\operatorname{Irr}_{\mathbb{Q}}(i) = X^2 + 1$, como sus raíces son $\pm i$ que no están en $\mathbb{Q}\left(\sqrt{2}\right)$, entonces $\operatorname{Irr}_{\mathbb{Q}(\sqrt{2})}(i) = X^2 + 1$, luego $\left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = \left[\mathbb{Q}\left(\sqrt{2}\right)(i) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$. Entonces $\left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\right] = 4 = \operatorname{gr} f$.

2. El cuerpo de descomposición de $f = X^3 - 2 \in \mathbb{Q}[X]$ es $\mathbb{Q}\left(\sqrt[3]{2}, w\right)$, siendo $w \in \mathbb{C}$ tal que $w^3 = 1$, $w \neq 1$. El criterio de Eisenstein implica que el polinomio $X^3 - 2$ es irreducible en $\mathbb{Q}[X]$, luego $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[3]{2}\right) = X^3 - 2$. Notar que de la factorización $X^3 - 1 = (X-1)(X^2+X+1)$, deducimos que w es una de las raíces de $X^2 + X + 1$, que son $\frac{-1 \pm i\sqrt{3}}{2}$. Como $w \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$, deducimos $\operatorname{Irr}_{\mathbb{Q}(\sqrt[3]{2})}(w) = \operatorname{Irr}_{\mathbb{Q}}(w) = X^2 + X + 1$. Luego $\left[\mathbb{Q}\left(\sqrt[3]{2}, w\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}, w\right) : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 2 \times 3 = 6 = (\operatorname{gr} f)!$.

El cuerpo de descomposición se puede definir para toda familia de polinomios. Lo veremos cuando la familia es finita, que es el caso que nos interesa. Sea K un cuerpo y $f_1, \ldots, f_n \in K[X]$ polinomios no constantes. El *cuerpo de descomposición* de $f_1, \ldots, f_n$ es el subcuerpo de $\mathbb{C}$ generado por K y las raíces complejas de estos polinomios. Es la menor extensión de K en la cual cada cada f_i se escinde. Notar que el cuerpo de descomposición de la familia $f_1, \ldots, f_n$ coincide con el cuerpo de descomposición del polinomio $f = f_1 \cdots f_n$.

Una extensión F/K se dice *normal*[5] si F es el cuerpo de descomposición de algún polinomio $f \in K[X]$.

Observaciones 3.8.

1. Si F/K es normal, entonces F/K es finita (proposición 3.6).
2. Si F/K es normal y $K \subset E \subset F$ es un cuerpo intermedio, entonces F/E es normal. Esto se debe a que si F es el cuerpo de descomposición de $f \in K[X]$, entonces F también es el cuerpo de descomposición de f pensado en $E[X]$.

Proposición 3.9. *Sea F/K una extensión normal. Si $\sigma : F \to \mathbb{C}$ es un K-morfismo, entonces $\sigma(F) = F$.*

Dem. Sea $f \in K[X]$ tal que F es el cuerpo de descomposición de f. Sean $u_1, \ldots u_n \in \mathbb{C}$ las raíces de f, luego $F = K(u_1, \ldots, u_n)$. Si $z \in F$ entonces existen $f, g \in K(X_1, \ldots, X_n)$ tales que $z = \frac{f(u_1,\ldots,u_n)}{g(u_1,\ldots,u_n)}$. Como vale $\sigma|_K = \mathrm{id}$, entonces $\sigma(z) = \frac{f\left(\sigma(u_1),\ldots,\sigma(u_n)\right)}{g\left(\sigma(u_1),\ldots,\sigma(u_n)\right)}$. Pero además $u_1, \ldots u_n \in \mathbb{C}$ son las raíces de $f \in K[X]$, luego σ las permuta y por lo tanto $\{\sigma(u_1), \ldots, \sigma(u_n)\} = \{u_1, \ldots u_n\}$. Eso implica $\sigma(z) \in K(u_1, \ldots, u_n) = F$. Luego $\sigma(F) \subset F$, pero como F es una extensión finita de K y σ es K-lineal e inyectivo, deducimos $\sigma(F) = F$. $\square$

Observación 3.10. De la proposición anterior se deduce que si F/K es una extensión normal, entonces hay una correspondencia uno a uno

$$\{\sigma : F \to \mathbb{C} |\ \sigma \text{ es un } K\text{-morfismo}\} \leftrightarrow \{\sigma : F \to F |\ \sigma \text{ es un } K\text{-automorfismo}\} = \operatorname{Gal}(F/K).$$

La correspondencia está dada para un lado por la proposición anterior y para el otro es componer con la inclusión $F \hookrightarrow \mathbb{C}$. Además usamos que todo K-morfismo de F en F es automáticamente un K-automorfismo.

Lema 3.11. *Sea $\sigma : K \to F$ un morfismo de cuerpos. Si un polinomio $f \in K[X]$ tiene solo raíces simples (en $\mathbb{C}$), entonces $\sigma f \in F[X]$ también tiene solo raíces simples.*

Dem. Como $f \in K[X]$ tiene solo raíces simples, entonces $\operatorname{mcd}(f, f') = 1$ y por lo tanto existen $g, h \in K[X]$ tales que $gf + hf' = 1$. Aplicando σ obtenemos $\sigma(g)\sigma(f) + \sigma(h)\sigma(f') = 1$. Notar que vale $\sigma(f') = \sigma(f)'$, luego es $\sigma(g)\sigma(f) + \sigma(h)\sigma(f)' = 1$ lo cual implica $\operatorname{mcd}\left(\sigma(f), \sigma(f)'\right) = 1$ y por lo tanto σf tiene solo raíces simples. $\square$

Teorema 3.12. *Sea F/K una extensión finita. Entonces*

$$\#\{\sigma : F \to \mathbb{C} |\ \sigma \textit{ es un } K\textit{-morfismo}\} = [F : K].$$

[5] Esta es la definición de extensión normal finita. También se definen extensiones normales infinitas, pero no las necesitaremos.

Dem. Como F/K es finita, entonces existen $u_1, \dots, u_n \in F$ elementos algebraicos sobre K tales que $F = K(u_1, \dots, u_n)$. Consideremos la raíz u_1. Sea $f_1 = \mathrm{Irr}_K(u_1) \in K[X]$. Como f_1 es irreducible, entonces f_1 tiene solo raíces simples (en $\mathbb{C}$). Luego aplicando la proposición 2.36 obtenemos

$$\#\{\sigma : K(u_1) \to \mathbb{C} : \ \sigma \text{ es un } K\text{-morfismo}\} = [K(u_1) : K].$$

Consideremos ahora la raíz u_2 y sea $f_2 = \mathrm{Irr}_{K(u_1)}(u_2) \in K(u_1)[X]$.
Sea $\alpha : K(u_1) \to \mathbb{C}$ un K-morfismo cualquiera. La irreducibilidad implica que f_2 tiene solo raíces simples, luego del lema 3.11 se deduce que $\alpha f_2 \in \mathbb{C}[X]$ también tiene solo raíces simples. Además f_2 y αf_2 tienen el mismo grado. Luego aplicando la proposición 2.38 obtenemos

$$\begin{aligned} &\#\{\beta : K(u_1, u_2) \to \mathbb{C} : \ \beta \text{ es morfismo y } \beta|_{K(u_1)} = \alpha\} \\ &= \#\{\text{raíces de } \alpha f_2 \text{ en } \mathbb{C}\} = \mathrm{gr}\,(\alpha f_2) = \mathrm{gr}\,(f_2) = [K(u_1, u_2) : K(u_1)]. \end{aligned}$$

Notar que todo morfismo $\beta : K(u_1, u_2) \to \mathbb{C}$ que verifique $\beta|_{K(u_1)} = \alpha$ es también un K-morfismo. Diagramáticamente la construcción que hicimos es la siguiente

$$\begin{tikzcd} K(u_1) \arrow[r, dotted, "\alpha"] \arrow[d, dash] & F \\ K \arrow[ur, dash] & \end{tikzcd} \quad \Rightarrow \quad \begin{tikzcd} K(u_1, u_2) \arrow[dr, dotted, "\beta"] \arrow[d, dash] & \\ K(u_1) \arrow[r, "\alpha"] \arrow[d, dash] & F \\ K \arrow[ur, dash] & \end{tikzcd} \quad \Rightarrow \quad \begin{tikzcd} K(u_1, u_2) \arrow[r, "\beta"] \arrow[d, dash] & F \\ K \arrow[ur, dash] & \end{tikzcd} .$$

Por otro lado todo K-morfismo $K(u_1, u_2) \to \mathbb{C}$ es una extensión de su restricción a $K(u_1)$,

$$\begin{tikzcd} K(u_1, u_2) \arrow[dr, "\beta"] \arrow[d, dash] & \\ K(u_1) \arrow[r, "\beta|_{K(u_1)}"] \arrow[d, dash] & F \\ K \arrow[ur, dash] & \end{tikzcd} .$$

Luego todo K-morfismo $K(u_1, u_2) \to \mathbb{C}$ se obtiene mediante la construcción anterior. Entonces, como cada K-morfismo α se puede extender a un K-morfismo β, y tenemos $[K(u_1) : K]$ morfismos α y $[K(u_1, u_2) : K(u_1)]$ morfismos β (por cada α), deducimos

$$\#\{\sigma : K(u_1, u_2) \to \mathbb{C} : \ \sigma \text{ es un } K\text{-morfismo}\} = [K(u_1, u_2) : K(u_1)]\,[K(u_1) : K] = [K(u_1, u_2) : K].$$

Luego seguimos aplicando el razonamiento anterior en cada paso de la torre

$$K \subset K(u_1) \subset K(u_1, u_2) \subset K(u_1, u_2, u_3) \subset \cdots \subset K(u_1, \dots, u_n) = F$$

hasta obtener

$$\#\{\sigma : K(u_1, \dots, u_n) \to \mathbb{C} |\ \sigma \text{ es un } K\text{-morfismo}\} = [K(u_1, \dots, u_n) : K].$$

Como es $F = K(u_1, \dots, u_n)$, entonces esta última igualdad equivale a la tesis. $\square$

Combinando el teorema anterior y la observación 3.10 obtenemos el siguiente.

Teorema 3.13. *Sea F/K una extensión normal. Entonces* $|\mathrm{Gal}(F/K)| = [F : K]$. $\square$

3.3. El teorema de Artin

Sea F un cuerpo. Si H es un subgrupo de $\mathrm{Aut}(F)$, entonces H actúa en F mediante $\sigma \cdot x = \sigma(x)$, para todo $\sigma \in G$ y $x \in F$. Sea F^H el conjunto de puntos fijos de F por la acción de H, es decir

$$F^H = \{x \in F : \ \sigma(x) = x, \ \forall \sigma \in H\}$$

Es fácil de probar que F^H es un subcuerpo de F.

Teorema 3.14 (E. Artin)**.** *Sean F un cuerpo, G un subgrupo finito de* $\mathrm{Aut}(F)$ *y* $K = F^G$. *Entonces*

1. *F/K es finita y $[F : K] = |G|$;*
2. $\mathrm{Gal}\,(F/K) = G$*;*
3. $\mathrm{Irr}_K(u) \in K[X]$ *se escinde en $F[X]$, para todo $u \in F$.*

Dem. Consideremos $u \in F$ arbitrario. Sea $\{\sigma(u) : \ \sigma \in G\} = \{u_1, \ldots, u_m\}$, en que $u_1, \ldots, u_m \in F$ son elementos distintos. Notar que $\mathrm{id} \in G$ implica $u \in \{u_1, \ldots, u_m\}$. Consideremos $f = \prod_{i=1}^m \big(X - u_i\big) \in F[X]$.

Si $\alpha \in G$, entonces $\alpha f = \prod_{i=1}^m \big(X - \alpha(u_i)\big)$. Notar $\{\alpha(u_1), \ldots, \alpha(u_m)\} = \{\alpha\sigma(u) : \ \sigma \in G\}$. Como es $\{\alpha\sigma : \ \sigma \in G\} = G$, entonces $\{\alpha(u_1), \ldots, \alpha(u_m)\} = \{u_1, \ldots, u_m\}$. Luego $\alpha f = f$, para todo $\alpha \in G$, y al ser $K = F^G$, deducimos $f \in K[X]$. Como u es raíz de f, entonces u es algebraico sobre K y $\mathrm{Irr}_K(u) \mid f$.

Por otro lado, como $K = F^G$, entonces $\sigma(x) = x$, para todo $x \in K$ y $\sigma \in G$, luego $G \subset \mathrm{Gal}\,(F/K)$. Esto implica que $\sigma(u)$ es raíz de $\mathrm{Irr}_K(u)$ para todo $\sigma \in G$. Luego $\{u_1, \ldots, u_m\}$ son raíces de $\mathrm{Irr}_K(u)$ y como vale $\mathrm{Irr}_K(u) \mid \prod_{i=1}^m \big(X - u_i\big)$, entonces $\mathrm{Irr}_K(u) = \prod_{i=1}^m \big(X - u_i\big)$. Esto prueba la tercer afirmación de la tesis.

De $\mathrm{Irr}_K(u) = \prod_{i=1}^m \big(X - u_i\big)$ deducimos $[K(u) : K] = m \leq |G|$. Luego $[K(u) : K] \leq |G|$, para todo $u \in F$.
Sea $u^* \in F$ tal que $[K(u^*) : K] = \max\{[K(u) : K] : \ u \in F\}$. Probaremos $K(u^*) = F$.
Sea $v \in F$ arbitrario. Como $u^*, v \in F$ son algebraicos sobre K, entonces $K(u^*, v)/K$ es finita, luego el teorema del elemento primitivo implica que existe $w \in F$ tal que $K(u^*, v) = K(w)$. De las inclusiones $K(w) = K(u^*, v) \supset K(u^*) \supset K$ deducimos $[K(w) : K] \geq [K(u^*) : K]$, y como $[K(u^*) : K]$ es máxima, comcluimos $[K(u^*) : K] = [K(w) : K]$ y por lo tanto $K(u^*, v) = K(w) = K(u^*)$, lo cual implica $v \in K(u^*)$. Como $v \in F$ era arbitrario, concluimos $K(u^*) = F$.

Luego $F = K(u^*)$ y por lo tanto F/K es finita y $[F : K] = [K(u^*) : K] \leq |G|$. Como F/K es finita, entonces $\mathrm{Gal}\,(F/K)$ es finito y $|\mathrm{Gal}\,(F/K)\,| \leq [F : K]$. Por otro lado sabemos $G \subset \mathrm{Gal}\,(F/K)$. Así tenemos

$$[F : K] \leq |G| \leq |\mathrm{Gal}\,(F/K)\,| \leq [F : K],$$

luego $[F : K] = |G| = |\mathrm{Gal}\,(F/K)\,|$. Finalmente de $|G| = |\mathrm{Gal}\,(F/K)\,|$ y $G \subset \mathrm{Gal}\,(F/K)$ deducimos $G = \mathrm{Gal}\,(F/K)$. □

Observaciones 3.15. En las hipótesis del teorema de Artin.

1. De las dos primeras parte de la tesis se deduce $[F : K] = |\mathrm{Gal}\,(F/K)\,|$.
2. Sea $u \in F$. En la prueba del teorema mostramos que actuando con $\mathrm{Gal}(F/K)$ en u obtenemos todas las raíces de $\mathrm{Irr}_K(u)$ y vale
$$\mathrm{Irr}_K(u) = \prod_{i=1}^m (X - u_i) \text{ en } F[X].$$
siendo $u_1, \ldots, u_m$ los distintos elementos de la órbita $\{\sigma(u) : \ \sigma \in \mathrm{Gal}(F/K)\}$.

3.4. Extensiones de Galois

Si F/K es una extensión y H es un subgrupo de $\mathrm{Gal}(F/K)$, entonces $H < \mathrm{Aut}(F)$ y por lo tanto podemos considerar F^H que es un subcuerpo de F. Notar que H deja fijos a los elementos de K, luego es $K \subset F^H \subset F$. En particular tomando $H = \mathrm{Gal}(F/K)$ deducimos $K \subset F^{\mathrm{Gal}(F/K)}$.

Decimos que una extensión F/K es *de Galois*[6] si es finita y verifica $F^{\mathrm{Gal}(F/K)} = K$. Notar que F/K finita implica que $\mathrm{Gal}(F/K)$ es un grupo finito de orden menor o igual que $[F : K]$ (teorema 3.3).

Observación 3.16. Dada una extensión finita F/K, son equivalentes:

1. F/K es de Galois.
2. Si $u \in F$ verifica $\sigma(u) = u$, para todo $\sigma \in \mathrm{Gal}(F/K)$, entonces $u \in K$ (es decir $F^{\mathrm{Gal}(F/K)} \subset K$).
3. Si $u \in F \setminus K$, entonces existe $\sigma \in \mathrm{Gal}(F/K)$ tal que $\sigma(u) \neq u$.

Ejemplos 3.17. 1. Si K es un cuerpo arbitrario, entonces K/K es de Galois.

2. Calculando $F^{\mathrm{Gal}(F/K)}$ para los primeros de los ejemplos 3.2, se obtiene:
   a) las extensiones $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ son de Galois;
   b) las extensiones $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$, $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ no son de Galois.

Teorema 3.18. *Sea F/K una extensión de cuerpos. Las siguientes afirmaciones son equivalentes.*

1. *F/K es normal.*
2. *F/K es finita y vale $|\mathrm{Gal}(F/K)| = [F : K]$.*
3. *F/K es de Galois.*
4. *$K = F^H$, siendo H un subgrupo finito de* $\mathrm{Aut}(F)$.
5. *F/K es finita y para todo $u \in F$ se cumple que* $\mathrm{Irr}_K(u)$ *se escinde en* $F[X]$.

Dem. (1) $\Rightarrow$ (2). Esto se deduce de la observación 3.8 y el teorema 3.3.

(2) $\Rightarrow$ (3). Sea $G = \mathrm{Gal}(F/K)$ y $K_0 = F^G$. Como G es finito, entonces el teorema de Artin implica que F/K_0 es finita y $[F : K_0] = |G| = |\mathrm{Gal}(F/K)|$. Luego al ser $F \supset K_0 \supset K$ y $[F : K] = [F : K_0] < \infty$, deducimos $K_0 = K$, es decir, $F^{\mathrm{Gal}(F/K)} = K$.

(3) $\Rightarrow$ (4). Como F/K es de Galois, entonces F/K es finita y $K = F^{\mathrm{Gal}(F/K)}$. Además, como F/K es finita, entonces el teorema 3.3 implica que $\mathrm{Gal}(F/K)$ es finito. Luego $K = F^{\mathrm{Gal}(F/K)}$ con $\mathrm{Gal}(F/K)$ finito.

(4) $\Rightarrow$ (5). Esto es parte de la tesis del teorema de Artin.

[6] La definición de extensión de Galois no requiere que sea finita, pero como las extensiones que nos interesan son las finitas, entonces lo incluimos en la definición para no tener que estarlo repitiendo constantemente.

(5) $\Rightarrow$ (1). Como F/K es finita, entonces existe una cantidad finita de elementos $u_1, \ldots, u_n \in F$ que son algebraicos sobre K, tales que $F = K(u_1, \ldots, u_n)$. Para cada i, sea $f_i = \operatorname{Irr}_K(u_i)$ y consideremos $f = f_1 \cdots f_n \in K[X]$. Como cada f_i se escinde en $F[X]$, entonces F contiene a todas las raíces de f, luego F contiene al cuerpo de descomposición de f sobre K; pero cada u_i es raíz de f, así que tenemos también la inclusión inversa. Luego F es el cuerpo de descomposición de f sobre K. $\square$

Observaciones 3.19.

1. Una forma equivalente de escribir la condición (4) es que F/K es finita, y para todo polinomio irreducible $f \in K[X]$ se cumple que si f tiene una raíz en F, entonces f se escinde en $F[X]$. Esta condición a veces se usa como definición de normalidad.

2. Si F es un cuerpo, G es un subgrupo finito de $\operatorname{Aut}(F)$ y $K = F^G$, entonces F/K es de Galois por el teorema anterior y $\operatorname{Gal}(F/K) = G$ por el teorema de Artin.

Nota 1. Una pregunta natural es por qué definir los conceptos de extensión normal y de extensión de Galois, si al final terminan siendo equivalentes. La razón es que en nuestro caso equivalen porque estamos trabajando en característica cero. En general lo que vale para extensiones finitas es que Galois equivale a normal y separable[7], pero en característica cero la separabilidad es automática.

Combinando la parte (2) del teorema anterior con la proposición 3.1 se obtiene la siguiente caracterización de las extensiones simples de Galois.

Proposición 3.20. *Sea $K(u)$ una extensión algebraica simple de K. Entonces $K(u)/K$ es de Galois si y solo si todas las raíces complejas de $\operatorname{Irr}_K(u)$ están en $K(u)$.* $\square$

Ejemplos 3.21.

1. Consideremos $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$. Las raíces de $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{2}\right) = X^2 - 2$ son $\pm\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$. Luego $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ es de Galois.

2. Consideremos $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$. Las raíces de $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[3]{2}\right) = X^3 - 2$ son $\sqrt[3]{2}$, $w\sqrt[3]{2}$ y $w^2\sqrt[3]{2}$, siendo $w^3 = 1$, $w \neq 1$. Como en $\mathbb{Q}\left(\sqrt[3]{2}\right)$ no están todas las raíces de $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[3]{2}\right)$, entonces $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ no es de Galois.

3.5. El teorema fundamental

Sea F/K una extensión. Notar que valen las siguientes propiedades.

1. Si E es un cuerpo intermedio entre F y K, entonces $\operatorname{Gal}(F/E)$ es un subgrupo de $\operatorname{Gal}(F/K)$.

2. Si H es un subgrupo de $\operatorname{Gal}(F/K)$, entonces F^H es un cuerpo intermedio entre F y K.

Dada una extensión F/K, la *correspondencia de Galois* es la correspondencia entre la familia de cuerpos intermedios entre F y K y la familia de subgrupos de $\operatorname{Gal}(F/K)$ que asocia a cada cuerpo intermedio E el subgrupo $\operatorname{Gal}(F/E)$ y a cada subgrupo H el cuerpo intermedio F^H.

Observación 3.22. Dada F/K, la correspondencia de Galois invierte el orden de inclusión

$$H_1 < H_2 < \operatorname{Gal}(F/K) \quad \Rightarrow \quad F^{H_2} \subset F^{H_1};$$
$$K \subset E_1 \subset E_2 \subset F \quad \Rightarrow \quad \operatorname{Gal}(F/E_2) < \operatorname{Gal}(F/E_1).$$

Notar que vale $F^{\langle \mathrm{id} \rangle} = F$ y $\operatorname{Gal}(F/F) = \langle \mathrm{id} \rangle$.

Para probar el teorema fundamental necesitamos el siguiente resultado, que también interesa por sí mismo.

[7] Una extensión F/K es *separable* si es algebraica y $\operatorname{Irr}_K(u)$ tiene solo raíces simples (en $\mathbb{C}$), para todo $u \in F$.

Lema 3.23. *Sea F/K una extensión. Si E es un cuerpo intermedio entre F y K, y $\sigma \in \mathrm{Gal}(F/K)$, entonces*

$$\mathrm{Gal}\big(F/\sigma(E)\big) = \sigma \mathrm{Gal}(F/E)\sigma^{-1}.$$

Dem. Sea E un cuerpo intermedio y $\sigma \in \mathrm{Gal}(F/K)$. Consideremos $\alpha \in \mathrm{Gal}(F/E)$ y $u = \sigma(v)$ con $v \in E$, arbitrarios. Entonces

$$\sigma\alpha\sigma^{-1}(u) = \sigma\alpha\sigma^{-1}\big(\sigma(v)\big) = \sigma\alpha(v) = \sigma(v) = u.$$

Luego probamos $\sigma\mathrm{Gal}(F/E)\sigma^{-1} \subset \mathrm{Gal}\big(F/\sigma(E)\big)$, para todo cuerpo intermedio E y todo $\sigma \in \mathrm{Gal}(F/K)$. Entonces, dados E y σ, aplicando esa fórmula al cuerpo $\sigma(E)$ y al morfismo σ^{-1}, obtenemos la inclusión $\sigma^{-1}\mathrm{Gal}\big(F/\sigma(E)\big)\sigma \subset \mathrm{Gal}(F/E)$, lo cual implica $\mathrm{Gal}\big(F/\sigma(E)\big) \subset \sigma\mathrm{Gal}(F/E)\sigma^{-1}$, y completa la prueba. □

Teorema 3.24 (Teorema fundamental)**.** *Sea F/K una extensión de Galois. Entonces:*

1. *Las correspondencias definidas por $H \mapsto F^H$ y $E \mapsto \mathrm{Gal}(F/E)$ entre la familia de subgrupos de $\mathrm{Gal}(F/K)$ y la familia de cuerpos intermedios entre F y K son inversas una de la otra.*
2. *Si $H_1 \subset H_2$ son subgrupos de $\mathrm{Gal}(F/K)$, entonces $[H_2 : H_1] = \big[F^{H_1} : F^{H_2}\big]$.*
3. *Si $E \supset L$ son cuerpos intermedios, entonces $[E : L] = [\mathrm{Gal}(F/L) : \mathrm{Gal}(F/E)]$.*
4. *Si E es un cuerpo intermedio, entonces F/E es de Galois. La extensión E/K es de Galois si y solo si $\mathrm{Gal}(F/E) \lhd \mathrm{Gal}(F/K)$. En caso afirmativo el morfismo restricción*

$$\begin{array}{rcl} \mathrm{Gal}(F/K) & \to & \mathrm{Gal}(E/K) \\ \sigma & \mapsto & \sigma|_E \end{array}$$

induce un isomorfismo $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(E/K)$.

Dem. Empezamos observando que la primer afirmación de la parte (4) se deduce directamente de la observación 3.8, dado que una extensión es de Galois si y solo si es normal.

(1). Si H es un subgrupo de $\mathrm{Gal}(F/K)$, entonces el teorema de Artin implica $\mathrm{Gal}\left(F/F^H\right) = H$. Recíprocamente, si E es un cuerpo intermedio, entonces F/E es de Galois y por lo tanto $E = F^{\mathrm{Gal}(F/E)}$.

(2). Si H es un subgrupo de $\mathrm{Gal}(F/K)$, entonces el teorema de Artin implica $\left[F : F^H\right] = |H|$. Luego, dados $H_1 < H_2 < \mathrm{Gal}(F/K)$, usando

$$\left[F : F^{H_2}\right] = \left[F : F^{H_1}\right]\left[F^{H_1} : F^{H_2}\right].$$

deducimos

$$[H_2 : H_1] = \frac{|H_2|}{|H_1|} = \frac{\left[F : F^{H_2}\right]}{\left[F : F^{H_1}\right]} = \left[F^{H_1} : F^{H_2}\right].$$

(3). Esta afirmación se deduce de las dos anteriores.

(4). Sea E un cuerpo intermedio. Notar que ya vimos que F/E es de Galois.

Supongamos que E/K es de Galois. Sea $\sigma \in \mathrm{Gal}(F/K)$. Como E/K es normal y $\sigma|_E : E \to F \hookrightarrow \mathbb{C}$ es un K-morfismo, entonces la proposición 3.9 implica $\sigma(E) = \sigma|_E(E) = E$. Luego vale $\sigma(E) = E$, para todo $\sigma \in \mathrm{Gal}(F/K)$. Esto implica

$$\mathrm{Gal}\big(F/\sigma(E)\big) = \mathrm{Gal}(F/E), \quad \forall \sigma \in \mathrm{Gal}(F/K), \tag{4}$$

lo cual, por el lema 3.23, equivale a

$$\sigma\mathrm{Gal}(F/E)\sigma^{-1} = \mathrm{Gal}(F/E), \quad \forall \sigma \in \mathrm{Gal}(F/K).$$

Luego $\mathrm{Gal}(F/E)$ es normal en $\mathrm{Gal}(F/K)$.

Supongamos ahora que $\mathrm{Gal}(F/E)$ es un subgrupo normal de $\mathrm{Gal}(F/K)$. Por lo que vimos anteriormente esto equivale a la condición (4); luego aplicando la correspondencia de Galois deducimos que vale $\sigma(E) = E$, para todo $\sigma \in \mathrm{Gal}(F/K)$. Esto permite definir un mapa $\Phi : \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$ mediante $\Phi(\sigma) = \sigma|_E$. Notar que Φ es un morfismo de grupos y su núcleo es $\mathrm{Gal}(F/E)$, luego el primer teorema de isomorfismo implica que Φ induce un morfismo inyectivo $\hat{\Phi} : \mathrm{Gal}(F/K)/\mathrm{Gal}(F/E) \to \mathrm{Gal}(E/K)$. Probaremos que $\hat{\Phi}$ es un isomorfismo.
Como $\hat{\Phi}$ es inyectivo, entonces el orden de $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/E)$ divide al orden de $\mathrm{Gal}(E/K)$. Pero por la parte (3) es $[\mathrm{Gal}(F/K) : \mathrm{Gal}(F/E)] = [E : K]$. Luego $[E : K]$ divide a $|\mathrm{Gal}(E/K)|$. Pero como E/K es finita sabemos que vale $|\mathrm{Gal}(E/K)| \leq [E : K]$ (teorema 3.3) y por lo tanto $|\mathrm{Gal}(E/K)| = [E : K]$. Luego $\hat{\Phi}$ es un morfismo inyectivo entre dos grupos finitos del mismo orden y por lo tanto es un isomorfismo. Además probamos $|\mathrm{Gal}(E/K)| = [E : K]$, luego E/K es de Galois. $\square$

3.6. El grupo de Galois de un polinomio

Sea K un cuerpo y $f \in K[X]$ un polinomio. El *grupo de Galois* de f es $\mathrm{Gal}(F/K)$, siendo F el cuerpo de descomposición de f sobre K.

Dado un polinomio $f \in K[X]$, decimos que la ecuación $f(x) = 0$ es *soluble por radicales* si existe una torre de extensiones

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

tales que

1. para cada $i = 1, \ldots, m$ existen $v_i \in K_i$ y $m_i \in \mathbb{Z}^+$ tales que $K_i = K_{i-1}(v_i)$ y $v_i^{m_i} \in K_{i-1}$;
2. el cuerpo K_m contiene un cuerpo de descomposición de f.

Un grupo G se dice *soluble* si existe una torre de subgrupos

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

tal que $G_{i-1} \lhd G_i$ y G_i/G_{i-1} es abeliano, para todo $i = 1, \ldots, n$.

Vale el siguiente resultado.

Teorema 3.25 (Galois, 1832)**.** *Dado $f \in K[X]$, la ecuación $f(x) = 0$ es soluble por radicales si y solo si el grupo de Galois de f es soluble.* $\square$

Si el grado de $f \in K[X]$ es menor o igual que 4, entonces su grupo de Galois es soluble y se puede encontrar una fórmula para obtener las raíces de f a partir de sus coeficientes (como en el caso de la ecuación de segundo grado). Pero si consideramos $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$, entonces se prueba que el grupo de Galois de f es $\mathcal{S}_5$. Este grupo no es soluble (si no el grupo alternado A_5 sería soluble y eso es imposible porque es simple y no abeliano). Luego la ecuación $X^5 - 4X + 2 = 0$ no es soluble por radicales[8].

3.7. Cálculo del grupo de Galois

Ejemplo 3.26. Consideremos la extensión $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}$.

[8]Que la ecuación de grado mayor o igual que cinco no es soluble por radicales fue probado por P. Ruffini en 1799, pero la prueba tenía errores. El primero en probarlo correctamente fue N. Abel en 1824 y se lo conoce como el teorema de Abel-Ruffini.

Notar que $F=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ es el cuerpo de descomposición de $\left(X^2-2\right)\left(X^2-3\right)\in\mathbb{Q}[X]$, luego $F/\mathbb{Q}$ es de Galois. Vamos a hallar $[F:\mathbb{Q}]$. Consideremos la torre $\mathbb{Q}\subset\mathbb{Q}\left(\sqrt{2}\right)\subset F$. Es $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{2}\right)=X^2-2$, luego $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2$. Es $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{3}\right)=X^2-3$ y es un ejercicio el verificar que $\sqrt{3}\notin\mathbb{Q}\left(\sqrt{2}\right)$; luego $\operatorname{Irr}_{\mathbb{Q}(\sqrt{2})}\left(\sqrt{3}\right)=\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{3}\right)=X^2-3$ y por lo tanto $\left[F:\mathbb{Q}\left(\sqrt{2}\right)\right]=2$. Luego $[F:\mathbb{Q}]=\left[F:\mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=4$.

Sea $G=\operatorname{Gal}(F/\mathbb{Q})$. Como $F/\mathbb{Q}$ es de Galois, es $|G|=[F:\mathbb{Q}]=4$; luego $G=C_4$ o $G=C_2\times C_2$.
Como $\mathbb{Q}\left(\sqrt{2}\right)$ y $\mathbb{Q}\left(\sqrt{3}\right)$ son dos cuerpos intermedios, entonces G tiene al menos dos subgrupos propios. Como C_4 tiene solo un subgrupo propio, deducimos que es $G=C_2\times C_2$.

Vamos a hallar los elementos de G. Aplicando la proposición 2.36 sabemos que existen dos $\mathbb{Q}$-morfismos $\sigma,\tau:\mathbb{Q}\left(\sqrt{2}\right)\to F$ tales que $\sigma\left(\sqrt{2}\right)=\sqrt{2}$ y $\tau\left(\sqrt{2}\right)=-\sqrt{2}$. Notar que vale $\operatorname{Irr}_{\mathbb{Q}(\sqrt{2})}\left(\sqrt{3}\right)=\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{3}\right)=X^2-3$, y que este polinomio queda fijo al aplicarle σ o τ. Ahora aplicando la proposición 2.38 podemos extender $\sigma:\mathbb{Q}\left(\sqrt{2}\right)\to F$ a dos morfismos en G caracterizados por $\sqrt{3}\mapsto\pm\sqrt{3}$. Uno de ellos es la identidad y el otro es un morfismo $\alpha\in G$ que verifica $\alpha\left(\sqrt{2}\right)=\sqrt{2}$ y $\alpha\left(\sqrt{3}\right)=-\sqrt{3}$.
Razonando análogamente con $\tau:\mathbb{Q}\left(\sqrt{2}\right)\to F$ obtenemos dos morfismos $\beta,\gamma\in G$ tales que

$$\beta\left(\sqrt{2}\right)=-\sqrt{2},\qquad \beta\left(\sqrt{3}\right)=\sqrt{3},\qquad \gamma\left(\sqrt{2}\right)=-\sqrt{2},\qquad \gamma\left(\sqrt{3}\right)=-\sqrt{3}.$$

Luego $G=\{\mathrm{id},\,\alpha,\,\beta,\,\gamma\}$. Notar que vale que $\alpha^2=\beta^2=\mathrm{id}$ y $\alpha\beta=\beta\alpha=\gamma$, lo cual confirma $G=C_2\times C_2$.

Vanos a hallar una base de F como $\mathbb{Q}$-espacio. Como $\left\{1,\sqrt{2}\right\}$ es una base de $\mathbb{Q}\left(\sqrt{2}\right)$ sobre $\mathbb{Q}$ y $\left\{1,\sqrt{3}\right\}$ es una base de F sobre $\mathbb{Q}\left(\sqrt{2}\right)$, entonces $\mathcal{B}=\left\{1,\sqrt{2},\sqrt{3},\sqrt{6}\right\}$ es una base de F sobre $\mathbb{Q}$. En la base $\mathcal{B}$ los morfismos α, β, γ se expresan mediante:

$$\begin{aligned}
\alpha\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)&=a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6},\\
\beta\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)&=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6},\\
\gamma\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)&=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6},
\end{aligned}$$

para todo $a,b,c,d\in\mathbb{Q}$.

A continuación vamos a hallar todos los cuerpos intermedios entre $\mathbb{Q}$ y F. Los subgrupos propios de G son $\langle\alpha\rangle$, $\langle\beta\rangle$ y $\langle\gamma\rangle$. Luego usando las fórmulas de arriba deducimos que los cuerpos intermedios entre F y $\mathbb{Q}$ son

$$F^{\langle\alpha\rangle}=\mathbb{Q}\left(\sqrt{2}\right),\quad F^{\langle\beta\rangle}=\mathbb{Q}\left(\sqrt{3}\right),\quad F^{\langle\gamma\rangle}=\mathbb{Q}\left(\sqrt{6}\right).$$

Luego la correspondencia de Galois es la siguiente

$$\begin{tikzcd}
 & F=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & & & & \langle\mathrm{id}\rangle \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}\left(\sqrt{2}\right) \arrow[dr, dash, "2"'] & \mathbb{Q}\left(\sqrt{6}\right) \arrow[d, dash, "2"] & \mathbb{Q}\left(\sqrt{3}\right) \arrow[dl, dash, "2"] & \Longleftrightarrow & \langle\alpha\rangle \arrow[dr, dash, "2"'] & \langle\gamma\rangle \arrow[d, dash, "2"] & \langle\beta\rangle \arrow[dl, dash, "2"] \\
 & \mathbb{Q} & & & & G &
\end{tikzcd}$$

En este caso tenemos una forma alternativa de probar lo anterior. Si escribimos $u=\sqrt{3}+\sqrt{2}\in F$, entonces $u^{-1}=\sqrt{3}-\sqrt{2}\in F$; luego es fácil de probar que vale $F=\mathbb{Q}(u)$. Es $\operatorname{Irr}_{\mathbb{Q}}(u)=X^4-10X^2+1$, que tiene

raíces $\pm\sqrt{3}\pm\sqrt{2}\in F$, luego F es el cuerpo de descomposición de $X^4-10X^2+1\in\mathbb{Q}[X]$ y por lo tanto $F/\mathbb{Q}$ es de Galois finita y $|G|=4$.
Las raíces de $\operatorname{Irr}_{\mathbb{Q}}(u)=X^4-10X^2+1$ se pueden describir en función de u mediante

$$u=\sqrt{3}+\sqrt{2},\quad u^{-1}=\sqrt{3}-\sqrt{2},\quad -u=-\sqrt{3}-\sqrt{2},\quad -u^{-1}=-\sqrt{3}+\sqrt{2}.$$

Luego aplicando la proposición 2.36 deducimos $G=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$, quedando estos morfismos determinados por

$$\sigma_1(u)=u,\quad \sigma_2(u)=u^{-1},\quad \sigma_3(u)=-u,\quad \sigma_4(u)=-u^{-1}.$$

Comparando con lo que hicimos al principio, es $\sigma_1=\mathrm{id}$, $\sigma_2=\beta$, $\sigma_3=\gamma$ y $\sigma_4=\alpha$.

Proposición 3.27. *Sea F/K una extensión de Galois con grupo de Galois G. Sean E,L cuerpos intermedios y H,J subgrupos de G. Entonces.*

1. $F^{H\cap J}=F^HF^J$ *y* $F^H\cap F^J=F^{H\vee J}$. *Además, si $H\lhd G$ o $J\lhd G$, es $F^H\cap F^J=F^{HJ}$.*
2. $\operatorname{Gal}^F_{EL}=\operatorname{Gal}(F/E)\cap\operatorname{Gal}(F/L)$ *y* $\operatorname{Gal}^F_{E\cap L}=\operatorname{Gal}(F/E)\vee\operatorname{Gal}(F/L)$. *Además, si E/K o L/K es de Galois, es $\operatorname{Gal}^F_{E\cap L}=\operatorname{Gal}(F/E)\cdot\operatorname{Gal}(F/L)$.*

Dem. (1). De $H\cap J\subset H$ y $H\cap J\subset J$ se deduce $F^{H\cap J}\supset F^H$ y $F^{H\cap J}\supset F^H$, luego

$$F^{H\cap J}\supset F^HF^J.$$

Por otro lado de $F^H\subset F^HF^J$ y $F^J\subset F^HF^J$ se deduce $H\supset\operatorname{Gal}\left(F/F^HF^J\right)$ y $J\supset\operatorname{Gal}\left(F/F^HF^J\right)$, luego

$$H\cap J\supset\operatorname{Gal}\left(F/F^HF^J\right)\qquad\Rightarrow\qquad F^{H\cap J}\subset F^HF^J.$$

Luego probamos la doble inclusión y por lo tanto $F^{H\cap J}=F^HF^J$. La prueba de $F^H\cap F^J=F^{H\vee J}$ es análoga a la anterior y queda como ejercicio. Si $H\lhd G$ o $J\lhd G$, es $H\vee J=HJ$ y por lo tanto $F^H\cap F^J=F^{HJ}$.

(2). Se deduce de la parte anterior, escribiendo $E=F^H$ y $L=F^J$. □

Ejemplo 3.28. Consideremos el polinomio $X^4-2\in\mathbb{Q}[X]$. Sus raíces son $\pm u$ y $\pm iu$, siendo $u=\sqrt[4]{2}$. Luego su cuerpo de descomposición es $F=\mathbb{Q}(u,i)$. Consideremos la extensión $F/\mathbb{Q}$.

Sea $G=\operatorname{Gal}(F/\mathbb{Q})$. Observar que es $\operatorname{Irr}_{\mathbb{Q}}(u)=X^4-2$ y $\operatorname{Irr}_{\mathbb{Q}}(i)=X^2+1$. Como $i\notin\mathbb{Q}(u)$, entonces $\operatorname{Irr}_{\mathbb{Q}(u)}(i)=\operatorname{Irr}_{\mathbb{Q}}(i)=X^2+1$. En base a lo anterior, considerando la torre $F=\mathbb{Q}(u,i)\supset\mathbb{Q}(u)\supset\mathbb{Q}$, deducimos $|G|=[F:\mathbb{Q}]=8$. Ahora de las extensiones intermedias $\mathbb{Q}(u)$ y $\mathbb{Q}(i)$ obtenemos

$$\begin{tikzcd}
 & F=\mathbb{Q}(u,i) \arrow[dl, dash, "2"'] \arrow[dr, dash, "4"] & & & & \langle\mathrm{id}\rangle \arrow[dl, dash, "2"'] \arrow[dr, dash, "4"] & \\
\mathbb{Q}(u) \arrow[dr, dash, "4"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] & \Longrightarrow & H \arrow[dr, dash, "4"'] & & J \arrow[dl, dash, "2"] \\
 & \mathbb{Q} & & & & G &
\end{tikzcd}$$

siendo $H=\operatorname{Gal}(F/\mathbb{Q}(u))$ y $J=\operatorname{Gal}(F/\mathbb{Q}(i))$. Notar que $|H|=2$, $|J|=4$ y $[G:J]=2$, luego $J\lhd G$. Además de $\mathbb{Q}(u)\mathbb{Q}(i)=F$ y $\mathbb{Q}(u)\cap\mathbb{Q}(i)=\mathbb{Q}$, deducimos $H\cap J=\langle\mathrm{id}\rangle$ y $G=HJ$.
La normalidad de J refleja que $\mathbb{Q}(i)/\mathbb{Q}$ es de Galois. Por otro lado $\operatorname{Irr}_{\mathbb{Q}}(u)=X^4-2$ tiene raíces $\pm u$ y $\pm iu$, de las cuales solo $\pm u\in\mathbb{Q}(u)$. Esto implica que $\mathbb{Q}(u)/\mathbb{Q}$ no es de Galois (teorema 3.18) y por lo tanto H no es normal en G. Esto muestra que $G=HJ$ no es abeliano y al tener orden 8 es el diedral D_4 o los cuaternios Q. Los cuaternios no puede ser porque todos sus subgrupos son normales y H no es normal en G, luego $G=D_4$. Veamos de describir G explícitamente.

Consideremos $H = \mathrm{Gal}\,(F/\mathbb{Q}(u))$. Sabemos $|H| = 2$, luego $H = \{\mathrm{id}, \tau\}$. Como $i \notin \mathbb{Q}(u)$, entonces $\mathrm{Irr}_{\mathbb{Q}(u)}(i) = X^2 + 1$ que tiene raíces $\pm i \in F$; luego τ queda caracterizado por $\tau(u) = u$ y $\tau(i) = -i$.

Consideremos $J = \mathrm{Gal}\,(F/\mathbb{Q}(i))$. Sabemos $|J| = 4$, luego $\mathrm{gr}\,\mathrm{Irr}_{\mathbb{Q}(i)}(u) = 4$ y por lo tanto $\mathrm{Irr}_{\mathbb{Q}(i)}(u) = X^4 - 2$. Las raíces de $X^4 - 2$ son $\pm u, \pm ui \in F$, luego $J = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, estando estos automorfismos de F determinados por $\sigma_l(i) = i$, para todo l y

$$\sigma_1(u) = u, \quad \sigma_2(u) = ui, \quad \sigma_3(u) = -u, \quad \sigma_4(u) = -ui.$$

Notar $\sigma_1 = \mathrm{id}$, $\sigma_2^2 = \sigma_3$ y $\sigma_2^3 = \sigma_4$, luego llamando $\sigma = \sigma_2$, es $J = \langle\sigma\rangle = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\} = C_4$. Entonces

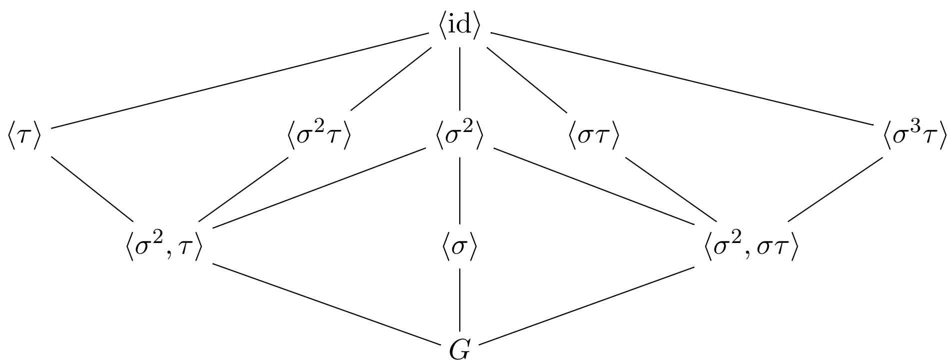
$$G = HJ = \left\{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\right\} = \langle\tau, \sigma\rangle, \qquad \tau(u) = u,\ \tau(i) = -i, \quad \sigma(u) = ui,\ \sigma(i) = i.$$

Operando obtenemos los valores de los elementos de G en los generadores de $F = \mathbb{Q}(u, i)$:

	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
u	ui	$-u$	$-ui$	u	ui	$-u$	$-ui$
i	i	i	i	$-i$	$-i$	$-i$	$-i$

Observar que vale $|\tau| = 2,\ |\sigma| = 4,\ \tau\sigma\tau = \sigma^3$, lo cual caracteriza a D_4. Veremos ahora cómo obtener todos los cuerpos intermedios entre F y $\mathbb{Q}$.

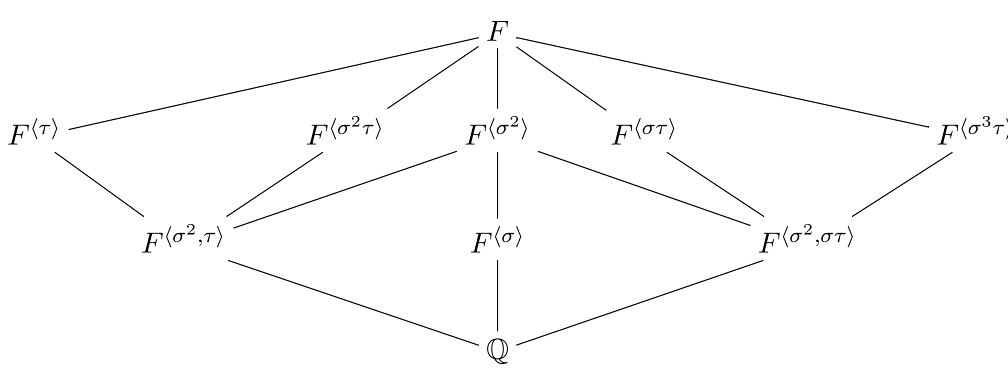
La tabla de subgrupos de G es



En la tabla anterior, contando desde arriba, los subgrupos de la segunda fila tienen orden 2 y los de la tercera tienen orden 4. Explícitamente los subgrupos de orden 4 son

$$\langle\sigma^2, \tau\rangle = \left\{\mathrm{id}, \sigma^2, \tau, \sigma^2\tau\right\}, \qquad \langle\sigma\rangle = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}, \qquad \langle\sigma^2, \sigma\tau\rangle = \left\{\mathrm{id}, \sigma^2, \sigma\tau, \sigma^3\tau\right\}.$$

Aplicando la correspondencia de Galois, obtenemos



Vamos hallar cada uno de estos cuerpos. Por los cálculos anteriores sabemos $F^{\langle\tau\rangle} = \mathbb{Q}(u)$ y $F^{\langle\sigma\rangle} = \mathbb{Q}(i)$.

Una forma de hacerlo es hallando una $\mathbb{Q}$-base de F. Considerando la torre $F \supset \mathbb{Q}(u) \supset \mathbb{Q}$ es fácil de probar que $\{1, u, u^2, u^3, i, ui, u^2i, u^3i\}$ es una base de F como $\mathbb{Q}$-espacio vectorial. Operando en esta base se pueden ir hallando todos los cuerpos intermedios, en forma análoga a como hicimos en el ejemplo 3.26. El problema es que estamos en dimensión 8 y por lo tanto los cálculos son bastante tediosos. En lo que sigue vamos a ver una forma alternativa para hallarlos.

Consideremos $F^{\langle\sigma^2,\tau\rangle} \subset F^{\langle\tau\rangle} = \mathbb{Q}(u)$. De $[\mathbb{Q}(u) : \mathbb{Q}] = 4$, deducimos que $\{1, u, u^2, u^3\}$ es una base de $\mathbb{Q}(u)$ como $\mathbb{Q}$-espacio. Al ser $\sigma^2(u) = -u$ obtenemos $\sigma^2(u^2) = u^2$, luego $u^2 \in F^{\langle\sigma^2,\tau\rangle}$ y por lo tanto $\mathbb{Q}(u^2) \subset F^{\langle\sigma^2,\tau\rangle}$. Como es $u^2 = \sqrt{2}$, entonces $[\mathbb{Q}(u^2) : \mathbb{Q}] = 2$ y como tabién vale $\left[F^{\langle\sigma^2,\tau\rangle} : \mathbb{Q}\right] = 2$, deducimos $F^{\langle\sigma^2,\tau\rangle} = \mathbb{Q}\left(u^2\right)$.

De $\langle\sigma^2,\tau\rangle \cap \langle\sigma\rangle = \langle\sigma^2\rangle$, se deduce $F^{\langle\sigma^2\rangle} = F^{\langle\sigma^2,\tau\rangle}F^{\langle\sigma\rangle} = \mathbb{Q}\left(u^2\right)\mathbb{Q}\left(i\right) = \mathbb{Q}\left(u^2, i\right)$.

Consideremos $F^{\langle\sigma^2,\sigma\tau\rangle} \subset F^{\langle\sigma^2\rangle} = \mathbb{Q}\left(u^2, i\right)$. A partir de la torre $\mathbb{Q}\left(u^2, i\right) \supset \mathbb{Q}(u^2) \supset \mathbb{Q}$ obtenemos que $\{1, u^2, i, u^2i\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}\left(u^2, i\right)$. Evaluando $\sigma\tau$ en esta base encontramos $\sigma\tau\left(u^2i\right) = u^2i$, luego $\mathbb{Q}\left(u^2i\right) \subset F^{\langle\sigma^2,\sigma\tau\rangle}$. Notar $u^2i = i\sqrt{2}$, luego $\operatorname{Irr}_{\mathbb{Q}}(u^2i) = X^2 + 2$ y por lo tanto $\left[\mathbb{Q}\left(u^2i\right) : \mathbb{Q}\right] = 2$. Como también es $[F^{\langle\sigma^2,\sigma\tau\rangle} : \mathbb{Q}] = 2$, deducimos $F^{\langle\sigma^2,\sigma\tau\rangle} = \mathbb{Q}\left(u^2i\right)$.

Consideremos $F^{\langle\sigma^2\tau\rangle}$. Es $\mathbb{Q}(u^2) \subset F^{\langle\sigma^2\tau\rangle} \subset F$ y sabemos $[F : \mathbb{Q}(u^2)] = 4$. Vamos a hallar una $\mathbb{Q}(u^2)$-base de F. Consideremos $F = \mathbb{Q}(u, i) \supset \mathbb{Q}(u) \supset \mathbb{Q}(u^2)$. Sabemos $[F : \mathbb{Q}(u)] = [\mathbb{Q}(u) : \mathbb{Q}(u^2)] = 2$, luego $\{1, i\}$ es una $\mathbb{Q}(u)$-base de F y $\{1, u\}$ es una $\mathbb{Q}(u^2)$-base de $\mathbb{Q}(u)$, por lo tanto $\{1, u, i, ui\}$ es una $\mathbb{Q}(u^2)$-base de F. Evaluando $\sigma^2\tau$ en esta base encontramos $\sigma^2\tau\left(ui\right) = ui$, luego $\mathbb{Q}(ui) \subset F^{\langle\sigma^2\tau\rangle}$. Como $ui \notin \mathbb{Q}(u^2)$, deducimos $[\mathbb{Q}(ui) : \mathbb{Q}(u^2)] = 2$, y como también es $[F^{\langle\sigma^2\tau\rangle} : \mathbb{Q}(u^2)] = 2$, concluimos $F^{\langle\sigma^2\tau\rangle} = \mathbb{Q}\left(ui\right)$.

Solo nos resta identificar $F^{\langle\sigma\tau\rangle}$ y $F^{\langle\sigma^3\tau\rangle}$. Razonando en forma análoga al caso anterior, a partir de la torre $F = \mathbb{Q}(u, i) \supset \mathbb{Q}(u^2, i) \supset \mathbb{Q}(u^2i)$ se deduce que $\{1, u, i, ui\}$ es una $\mathbb{Q}(u^2i)$-base de F. Sea $v = a+bu+ci+dui$, con $a, b, c, d \in \mathbb{Q}(u^2, i)$ un elemento cualquiera de F. Recordar $\mathbb{Q}(u^2, i) = F^{\langle\sigma^2,\sigma\tau\rangle}$, luego $\mathbb{Q}(u^2, i) \subset F^{\langle\sigma\tau\rangle}$ y $\mathbb{Q}(u^2, i) \subset F^{\langle\sigma^3\tau\rangle}$. Entonces

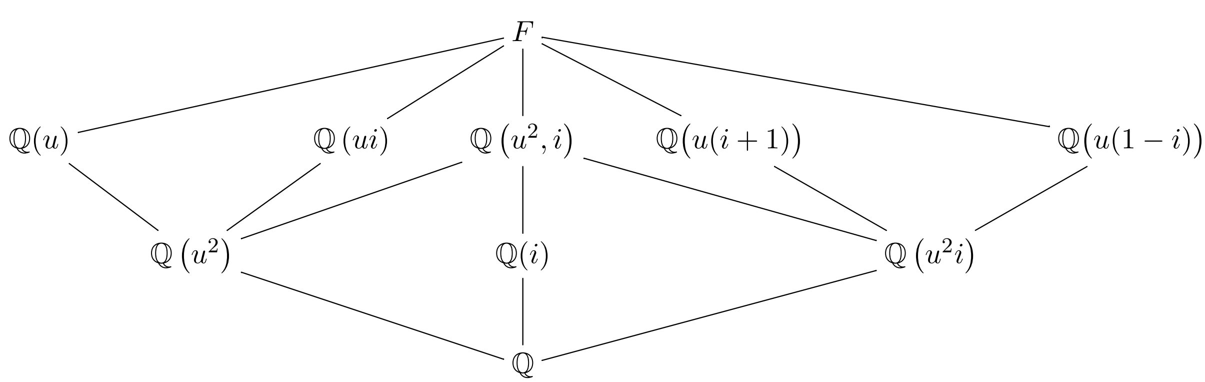
$$\sigma\tau(v) = \sigma\tau(a + bu + ci + dui) = a + bui - ci + du.$$

Luego $v = \sigma\tau(v)$ si y solo si $b = d$ y $c = 0$, lo cual implica $v = a+bu(1+i)$. Luego $F^{\langle\sigma\tau\rangle} = \mathbb{Q}(u^2i)\big(u(1+i)\big) = \mathbb{Q}\big(u^2i, u(1 + i)\big)$. Notar $\big(u(1 + i)\big)^2 = 2u^2i$, luego $u^2i \in \mathbb{Q}\big(u(1 + i)\big)$ y por lo tanto $F^{\langle\sigma\tau\rangle} = \mathbb{Q}\big(u(1 + i)\big)$.
Análogamente,

$$\sigma^3\tau(v) = \sigma^3\tau(a + bu + ci + dui) = a - bui - ci - du.$$

Luego $v = \sigma^3\tau(v)$ si y solo si $b = -d$ y $c = 0$, lo cual implica $v = a+bu(1-i)$. Luego $F^{\langle\sigma^3\tau\rangle} = \mathbb{Q}\big(u^2i, u(1-i)\big)$. Razonando como antes se prueba $u^2i \in \mathbb{Q}\big(u(1 - i)\big)$ y por lo tanto $F^{\langle\sigma^3\tau\rangle} = \mathbb{Q}\big(u(1 - i)\big)$.

Resumiendo, la tabla de cuerpos intermedios es



Terminamos con un par de resultados que permiten ver cómo se relaciona el grupo de Galois con la composición de cuerpos.

Proposición 3.29. *Si F/K es una extensión de Galois y E/K es una extensión arbitraria, entonces FE/E y $F/F \cap E$ son de Galois, y*

$$\mathrm{Gal}(FE/E) \simeq \mathrm{Gal}(F/F \cap E) < \mathrm{Gal}(F/K).$$

Luego $[FE : E] = [F : F \cap E]$. Diagramáticamente,

$$\begin{tikzcd}[column sep=small]
 & FE \arrow[dl, dash] \arrow[dr, dash, "//"] & \\
F \arrow[dr, dash, "//"'] & & E \arrow[dl, dash] \\
 & F \cap E \arrow[d, dash] & \\
 & K &
\end{tikzcd}$$

Dem. Notar que como F/K es de Galois y $F \cap E$ es un cuerpo intermedio, entonces $F/F \cap E$ es de Galois. Al ser F/K de Galois, entonces F es el cuerpo de descomposición de un polinomio $f \in K[X]$, es decir, $F = K(u_1, \ldots, u_n)$, siendo $u_1, \ldots, u_n$ las raíces complejas de f. Luego $FE = K(u_1, \ldots, u_n) \cdot E = E(u_1, \ldots, u_n)$ y por lo tanto FE es el cuerpo de descomposición del mismo f pensado en $E[X]$. Luego FE/E es de Galois.

Sea $\sigma \in \mathrm{Gal}\,(FE/E)$, probaremos que vale $\sigma(F) = F$. El mapa $\sigma|_F : F \to EF \hookrightarrow \mathbb{C}$ es un K-morfismo. Como F/K es de Galois, entonces es normal y por lo tanto la proposición 3.9 implica $\sigma(F) = \sigma|_F(F) = F$. Notar $(\sigma|_F)\,|_{F\cap E} = \sigma|_{F\cap E} = \mathrm{id}$. Luego definimos $\Psi : \mathrm{Gal}(FE/E) \to \mathrm{Gal}(F/F \cap E)$ por $\Psi(\sigma) = \sigma|_F$. Es claro que Ψ es un morfismo; en lo que sigue probaremos que es un isomorfismo.

Si $\sigma \in \mathrm{Gal}\,(FE/E)$ es tal que $\Psi(\sigma) = \mathrm{id}$, entonces es $\sigma|_F = \mathrm{id}$. Como además es $\sigma|_E = \mathrm{id}$, deducimos $\sigma = \mathrm{id}$ (recordar la observación 2.2). Esto nos dice que Ψ es inyectivo.
Sea $H = \mathrm{Im}(\Psi) < \mathrm{Gal}(F/F \cap E)$ y consideramos F^H, que es un cuerpo intemedio entre $F \cap E$ y F. Sea $u \in F$. Notar que vale

$$u \in F^H \quad \Leftrightarrow \quad \tau(u) = u,\ \forall \tau \in H \quad \Leftrightarrow \quad \sigma(u) = u,\ \forall \sigma \in \mathrm{Gal}(FE/E).$$

Como $u \in F \subset FE$ y FE/E es de Galois, entonces la cuenta anterior implica $u \in E$, y por lo tanto $u \in F \cap E$. Luego $F^H = F \cap E$ y por lo tanto $H = \mathrm{Gal}(F/F \cap E)$. Esto prueba que Ψ es sobreyectivo y completa la demostración. $\square$

En la proposición 2.22 probamos que si F/K es finita y E/K es arbitraria, entonces $[FE : E]$ es finita. El siguiente corolario permite afinar este resultado, en el caso en que F/K sea de Galois.

Corolario 3.30. *Si F/K es de Galois y E/K es arbitraria, entonces $[FE : E]$ divide a $[F : K]$.*

Dem. Se deduce de $[F : K] = [F : F \cap E][F \cap E : K] = [FE : E][F \cap E : K]$. $\square$

Si F/K no es de Galois, entonces la afirmación del corolario anterior no es necesariamente cierta, como lo muestra el siguiente ejemplo.

Ejemplo 3.31. Consideremos $E = \mathbb{Q}\left(\sqrt[3]{2}\right)$, $F = \mathbb{Q}\left(w\sqrt[3]{2}\right)$ y $K = \mathbb{Q}$, siendo $w = \frac{-1+i\sqrt{3}}{2}$ (es $w^3 = 1$). El polinomio $X^3 - 2$ es irreducible en $\mathbb{Q}[X]$ y sus raíces son $\sqrt[3]{2}$, $w\sqrt[3]{2}$ y $w^2\sqrt[3]{2}$. Luego $\operatorname{Irr}_{\mathbb{Q}}\left(w\sqrt[3]{2}\right) = X^3 - 2$ y por lo tanto $[F : K] = \left[\mathbb{Q}\left(w\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$.
Por otro lado es $FE = \mathbb{Q}\left(\sqrt[3]{2}, w\sqrt[3]{2}\right) = \mathbb{Q}\left(\sqrt[3]{2}, w\right)$. Como es $w \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$, entonces $\operatorname{Irr}_{\mathbb{Q}\left(\sqrt[3]{2}\right)}(w) = \operatorname{Irr}_{\mathbb{Q}}(w) = X^2+X+1$ y por lo tanto $[FE : E] = \left[\mathbb{Q}\left(\sqrt[3]{2}, w\right) : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = 2$. Luego $[FE : E] = 2$ no divide a $[F : K] = 3$.

Proposición 3.32. *Sean E/K y F/K extensiones de Galois. Entonces.*

1. *La extensión EF/K es de Galois.*
2. *El mapa $\Phi : \operatorname{Gal}(EF/K) \to \operatorname{Gal}(E/K) \times \operatorname{Gal}(F/K)$ definido por $\Phi(\sigma) = (\sigma|_E, \sigma|_F)$ es un monomorfismo de grupos.*
3. *El morfismo Φ es un isomorfismo si y solo si $E \cap F = K$.*

Dem. (1). Como E/K y F/K son de Galois, entonces son normales y por lo tanto existen $f, g \in K[X]$ tales que E es el cuerpo de descomposición de f y F es el cuerpo de descomposición de g. Luego EF es el cuerpo de descomposición de $fg \in K[X]$ y por lo tanto EF/K es de Galois (por ser normal).

(2). Sea $\sigma \in \operatorname{Gal}(EF/K)$. El mapa $\sigma|_E : E \to EF \hookrightarrow \mathbb{C}$ es un K-morfismo y como E/K es normal, entonces $\sigma|_E(E) = E$. Luego $\sigma|_E \in \operatorname{Gal}(E/K)$ y análogamente $\sigma|_F \in \operatorname{Gal}(F/K)$. Esto muestra que la definición de Φ tene sentido. Es claro que Φ es morfismo. Si $\sigma \in \operatorname{Ker}(\Phi)$, entonces $\sigma|E = \mathrm{id}$ y $\sigma|F = \mathrm{id}$, esto implica que $\sigma : EF \to EF$ es la identidad. Luego Φ es inyectivo.

(3). Como Φ es inyectivo, entonces Φ es un isomorfismo si y solo si $[EF : K] = [E : K][F : K]$. Usando la proposición anterior obtenemos $[EF : K] = [EF : F][F : K] = [E : E \cap F][F : K]$. Luego Φ es un isomorfismo si y solo si $[E : E \cap F] = [E : K]$, y al ser $K \subset E \cap F \subset E$, esta última equivale a $E \cap F = K$. $\square$

Referencias

[1] A. Gonçalves, *Introduçao a álgebra*, Projeto Euclides.

[2] T. W. Hungerford, *Algebra*, Springer-Verlag.

[3] S. Lang, *Algebra*, Addison-Wesley, 1993.

[4] J. S. Milne, *Fields and Galois Theory*. Se puede bajar de www.jmilne.org/math/.

[5] I. Stewart, *Galois Theory. Second edition.* Chapman and Halls Mathematics.