NOTAS DE TRABAJO, 16

EXTENSIONES DE CUERPOS

Teoría de Galois

Pascual Jara Martínez

Departamento de Álgebra. Universidad de Granada

Granada, 2001–2018

Primera redacción: 2001.
Segunda redacción: Julio 2014.
Tercera redacción: Septiembre 2016.
Tercera redacción: Septiembre 2017.

Introducción general

This text is a compilation of Extensiones de cuerpos.

Índice general

Parte I

Extensiones de cuerpos

Introducción

Uno de los problemas fundamentales en la Matemática actual es el determinar las raíces de una ecuación polinómica, en una variable, o de sistemas de ecuaciones polinómicas en varias variables. El segundo caso corresponde a la Geometría Algebraica, mientras que el primero es el que vamos a estudiar en este curso.

La teoría clásica trata de determinar las raíces y expresiones de las mismas; fue Kronecker quien cambió el paradigma, después de Kronecker se trata, mas que de determinar las raíces, ver qué relaciones verifican sin necesidad de determinarlas explícitamente. Por esta razón, y ya que los polinomios se supone que tienen coeficientes en un cuerpo, trataremos de trabajar con las raíces considerándolas en un cuerpo extensión finita del cuerpo base.

La teoría pues está dedicada al estudio de cuerpos y sus extensiones, finitas o infinitas. A este respecto tenemos que destacar que hasta el momento las únicas herramientas que tenemos para trabajar con un cuerpo son los espacios vectoriales, la pena es que sólo con espacios vectoriales no podemos distinguir entre cuerpos; esto nos obligará a introducir nuevas herramientas asociadas a extensiones de cuerpos.

Dada una extensión de cuerpos $K \subseteq F$, tenemos que F es un espacio vectorial sobre F y también sobre K. En este segundo caso tenemos información importante que podremos explorar, por ejemplo la dimensión; el valor de la dimensión ya nos da una primera forma de clasificar cuerpos. También F es una K–álgebra, por tanto para cada $x \in F$ tendremos expresiones del tipo $a_n x^n + \cdots + a_1 x + a_0$, con los $a_i \in K$; si $\dim_K(F) < \infty$, entonces existen expresiones $a_n x^n + \cdots + a_1 x + a_0 = 0$ en las que no todos los coeficientes a_i son nulos; esto es, x es una raíz del polinomio $f(X) = a_n X^n + \cdots + a_1 X + a_0$. Puede ser que x sea raíz de un polinomio $f(X)$ incluso cuando $\dim_K(F)$ no sea finita. Esto nos da una clasificación de los elementos de F en términos de K.

Observa los siguientes ejemplos: en la extensión $\mathbb{R} \subseteq \mathbb{C}$ todo elemento de $\mathbb{C}$ es raíz de un polinomio no nulo con coeficientes en $\mathbb{R}$; diremos que los elementos de $\mathbb{C}$ son algebraicos sobre $\mathbb{R}$. En cambio, en la extensión $\mathbb{Q} \subseteq \mathbb{R}$ esto no ocurre, por ejemplo $\pi \in \mathbb{R}$ no es raíz de ningún polinomio no nulo con coeficientes en $\mathbb{Q}$; diremos que π es un elemento trascendente sobre $\mathbb{Q}$. La existencia de elementos algebraicos o trascendentes produce una nueva clasificación de las extensiones de K. Más herramientas irán apareciendo a lo largo del texto.

Capítulo I

Extensiones de cuerpos

Introducción

En el estudio de las estructuras algebraicas, la principal herramienta que hemos utilizado ha sido la de módulos, esto es, hemos utilizado representaciones del anillo y del grupo para obtener propiedades de los mismos. En el caso de cuerpos podemos comprobar que el simple estudio de los espacios vectoriales no es suficiente, pues sólo con espacios vectoriales no podemos distinguir entre cuerpos; los espacios vectoriales tiene la misma estructura sobre todos los cuerpos. Por esta razón, vamos a estudiar homomorfismos entre cuerpos, esto es, subcuerpos y extensiones, para ubicar a cada cuerpo en la clase de todos los cuerpos.

Existen cuerpos que contiene una copia de $\mathbb{Q}$; son aquellos que también contiene una copia de $\mathbb{Z}$: los cuerpos de característica cero. Por otro lado, hay cuerpos, como $\mathbb{F}_2$, que no contienen una copia de $\mathbb{Z}$. En este caso $\mathbb{F}_2$ contiene una copia del grupo aditivo $\mathbb{Z}_2$. Tenemos pues una primera clasificación de cuerpos atendiendo a su característica. El resultado fundamental es que si dos cuerpos no tienen la misma característica no puede existir un homomorfismo entre ellos. Otro resultado, también obvio, es que todo cuerpo finito de característica p tiene exactamente p^r, para $r \in \mathbb{N}$.

El tener la misma característica no garantiza la existencia de un homomorfismo entre dos cuerpos; este es el caso de $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$, ó de $\mathbb{F}_4$ y $\mathbb{F}_8$. Más tarde veremos que, en el caso de cuerpos finitos, dos cuerpos con el mismo número de elementos son isomorfos.

Dados dos cuerpos K y F y un homomorfismo $f : K \longrightarrow F$, tenemos que f es siempre una aplicación inyectiva, y por tanto F es un espacio vectorial sobre K. Cuando $\dim_K(F) < \infty$ tenemos que cada elemento $x \in F$ es raíz de un polinomio no nulo con coeficientes en K; estos elementos son esenciales

en nuestro estudio, y los llamaremos elementos algebraicos sobre K. Puede ocurrir que todos los elementos de F sean algebraicos sobre K y que $\dim_K(F)$ sea infinita.

Si $0 \neq x \in F$ es un elemento algebraico sobre K, entonces el conjunto de los polinomios en $K[X]$ de los que x es una raíz es un ideal principal, ya que $K[X]$ es un DIP, por lo que toda la información sobre x está en el generador de este ideal, sea $f(X)$. Como $f(X)$ es irreducible sobre $K[X]$, ya que tenemos la siguiente situación:

$$\frac{K[X]}{(f(X))} \xrightarrow{eval_x} \mathrm{Im}(eval_x) = K[x] \subseteq F,$$

en donde $K[x]$ es un dominio de integridad. Como $K[X]$ es un DIP, entonces $(f(X))$ es un ideal maximal, y $K[X]$ es un cuerpo. Si $0 \neq x \in F$ no es algebraico sobre K, entonces $f(X) = 0$, y $(f(X)) = 0$ es un ideal primo que no es maximal, y por tanto $K[x]$ no es un cuerpo; éste es el caso de $\mathbb{Q}[\pi] \subseteq \mathbb{R}$. Los elementos que no son algebraicos se llaman trascendentes.

Amén de la introducción ya señalada sobre la teoría de extensiones de cuerpos, en este capítulo veremos dos desarrollos. El primero teórico: veremos que cada cuerpo K está contenido en una extensión $K \subseteq F$ en la que todo elemento de F es algebraico sobre K y F es algebraicamente cerrado, esto es, todo polinomio no constante con coeficientes en F tiene una raíz en F; se dice que F es una clausura algebraica de K.

El segundo desarrollo tiene un aspecto más práctico y trata de un problema clásico: las construcciones con regla y compás. Reduciremos el problema al estudio de las dimensiones de ciertas extensiones finitas de cuerpos que construiremos dentro de $\mathbb{C}$, el cuerpo de los números complejos.

1. Teoría de cuerpos

Si K y F son dos cuerpos y K es un subcuerpo de F, diremos que F es un **cuerpo extensión** de K, y lo representaremos por F/K ó $K \subseteq F$. Llamaremos a F/K una **extensión de cuerpos** de K.

Lema. 1.1.
Si F/K es una extensión de cuerpos, entonces F tiene estructura de espacio vectorial sobre K.

DEMOSTRACIÓN. Tenemos un homomorfismo de anillos $K \hookrightarrow F$, luego todo espacio vectorial sobre F es un espacio vectorial sobre K. □

Si F/K es una extensión de cuerpos, llamamos **grado** de F sobre K a la dimensión de F como espacio vectorial sobre K, lo representamos por $[F : K]$. Cuando $[F : K]$ es finito, decimos que la extensión es **finita**; en otro caso la extensión se llama **infinita**.
Una cadena de subcuerpos de un cuerpo $F = F_m$

$$F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = F,$$

se llama una **torre de cuerpos**, el cuerpo F_0 se llama **cuerpo base**.

Lema. 1.2.
Si $K \subseteq F \subseteq E$ es una torre de cuerpos, son equivalentes:
(a) E/K es una extensión finita.
(b) F/K y E/F son extensiones finitas.

Además en este caso se verifica: $[E : K] = [E : F][F : K]$.

DEMOSTRACIÓN. (a) ⇒ (b). Si E/K es una extensión finita, supongamos que $[E : K] = r$, entonces, ya que F es un K-subespacio vectorial de E, tenemos que $[F : K] \leq r$. Por otro lado, existe una base de E como K-espacio vectorial, sea $\{e_1, \ldots, e_r\}$; estos elementos e_i son un sistema de generadores de E como F-espacio vectorial, y por tanto $[E : F] \leq r$.
(b) ⇒ (a). Supongamos que $[F : K] = n$ y $[E : F] = m$, consideramos bases de F como K-espacio vectorial y de E como F-espacio vectorial $\{f_1, \ldots, f_n\}$ y $\{e_1, \ldots, e_m\}$ respectivamente. Para un elemento $x \in E$ existen $x_1, \ldots, x_m \in F$ verificando:

$$x = \sum_{i=1}^{m} x_i e_i.$$

4161-01.tex

Para cada x_i, $1 \leq i \leq n$, existen $y_{i_1}, \ldots, y_{i_m} \in K$ verificando

$$x_i = \sum_{j=1}^{n} y_{i_j} f_j.$$

Tenemos la expresión de x siguiente:

$$x = \sum_{i=1}^{m} x_i e_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} y_{i_j} f_j \right) e_i = \sum_{i=1}^{m} \sum_{j=1}^{n} y_{i_j} f_j e_i.$$

Como consecuencia $\{f_j e_i \mid 1 \leq j \leq m, 1 \leq i \leq n\}$ es un sistema de generadores de E como K-espacio vectorial. Para comprobar que $[E : K] = [E : F][F : K]$, basta ver que es un sistema linealmente independiente. Supongamos que tenemos una combinación lineal igualada a cero.

$$\sum_{i=1}^{m} \sum_{j=1}^{n} z_{ij} f_j e_i = 0,$$

con $z_{ij} \in K$, entonces tenemos

$$0 = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} z_{ij} f_j \right) e_i,$$

luego $\sum_{j=1}^{n} z_{ij} f_j = 0$, ya que $\{e_1, \ldots, e_n\}$ es una F-base de E. Como $\{f_1, \ldots, f_m\}$ es una K-base de F, tenemos $z_{ij} = 0$ para cada par de índices i, j. □

Corolario. 1.3.
Si $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$ es una torre de cuerpos, siendo F_{i+1}/F_i una extensión finita para $0 \leq i \leq m-1$, entonces F_m/F_0 es una extensión finita y

$$[F_m : F_0] = [F_m : F_{m-1}] \cdots [F_1 : F_0].$$

Este hecho es importante, ya que limita el número de posibles cuerpos intermedios entre dos cuerpos dados $K \subseteq$E. Así, si la extensión es finita, los cuerpos intermedios F han de verificar

$$[E : K] = [E : F][F : K].$$

En particular, $[F : K]$ es un divisor de $[E : K]$, y si $[E : K]$ es un número entero primo, entonces las posibles extensiones intermedias son únicamente K/K y E/K.
Si F/K es una extensión de cuerpos e Y es un subconjunto de F, el **subanillo generado** por K e Y se representa por $K[Y]$, sus elementos son expresiones del tipo

$$\sum \{k_{i_1 \ldots i_r} y_{i_1} \ldots y_{i_r} \mid k_{i_1 \ldots i_r} \in K, y_{i_1}, \ldots, y_{i_r} \in Y\},$$

son polinomios en $y_i \in Y$ con coeficientes en K, y además coincide con la intersección de todos los subanillos de F que contienen a K y a Y. El **subcuerpo generado** por K e Y es el cuerpo de fracciones de $K[Y]$, que se representa por $K(Y)$. Cuando $Y = \{u_1, \ldots, u_r\}$, entonces $K[Y]$ se escribe como $K[u_1, \ldots, u_r]$, y $K(Y)$ como $K(u_1, \ldots, u_r)$.

Lema. 1.4.
Si F/K es una extensión de cuerpos e Y y Z son dos subconjuntos de F, entonces
(1) $K[Y \cup Z] = K[Y][Z] = K[Z][Y]$ *y*
(2) $K(Y \cup Z) = K(Y)(Z) = K(Z)(Y)$.

DEMOSTRACIÓN. Tenemos que $K[Y \cup Z]$ contiene a K, a Y y a Z, luego $K[Y] \subseteq K[Y \cup Z]$ y también $K[Y][Z] \subseteq K[Y \cup Z]$. □

Proposición. 1.5.
Sea F/K una extensión de cuerpos, e Y un subconjunto de F, entonces para cada elemento de $\alpha \in K(Y)$ existe un subconjunto finito $Z \subseteq Y$, tal que $\alpha \in K(Z)$.

DEMOSTRACIÓN. Si $\alpha \in K(Y)$, existen $f(y_1, \ldots, y_r)$ y $0 \neq g(y_1, \ldots, y_r) \in K[Y]$ tales que $\alpha = f(y_1, \ldots, y_r)/g(y_1, \ldots, y_r)$, entonces $\alpha \in K(Z)$, donde $Z = \{y_1, \ldots, y_r\}$. □

Si F/K es una extensión de cuerpos, un elemento $\alpha \in F$ se llama **algebraico** sobre K si existe un polinomio no nulo $f(X) \in K[X]$ tal que $f(\alpha) = 0$. Un elemento $\alpha \in F$ que no es algebraico sobre K se llama **trascendente** sobre K. Si todo elemento de F es algebraico sobre K, entonces la extensión F/K se llama **algebraica**.

Lema. 1.6.
Si F/K es una extensión de cuerpos y $\alpha \in F$, definimos un homomorfismo de anillos

$$h_\alpha : K[X] \longrightarrow F \text{ mediante } h_\alpha(f(X)) = f(\alpha), \text{ para cada } f(X) \in K[X].$$

*h_α se llama **homomorfismo de evaluación** y verifica que un elemento $\alpha \in F$ es algebraico (resp. transcendente) si, y sólo si,* $\mathrm{Ker}(h_\alpha) \neq 0$ *(resp.* $\mathrm{Ker}(h_\alpha) = 0$*).*

DEMOSTRACIÓN. El homomorfismo h_α es el inducido por el morfismo inclusión de K en F, y por el elemento $\alpha \in F$, (propiedad universal del anillo de polinomios).

Caso 1. Si $\alpha \in F$ es algebraico, existe $0 \neq f(X) \in K[X]$ tal que $f(\alpha) = 0$, luego $f(X) \in \mathrm{Ker}(h_\alpha)$. El recíproco es inmediato.
Caso 2. Si $\alpha \in F$ es trascendente, entonces no existe $0 \neq f(X) \in K[X]$ tal que $f(\alpha) = 0$, luego $\mathrm{Ker}(h_\alpha) = 0$. El recíproco es inmediato. □

En general tenemos que $\mathrm{Im}(h_\alpha)$ es el anillo de F generado por K y α, al que representábamos por $K[\alpha]$, por tanto $K[\alpha]$ es un dominio de integridad. Su cuerpo de fracciones es el menor subcuerpo de F que contiene a K y α y se representaba por $K(\alpha)$.

Proposición. 1.7.
Sea F/K una extensión de cuerpos y $\alpha \in F$ un elemento algebraico sobre K, existe un polinomio irreducible $f(X) \in K[X]$ verificando $f(\alpha) = 0$.
Este polinomio $f(X)$ está determinando de forma única, salvo asociados en $K[X]$, y es el polinomio de $K[X]$ de menor grado del que α es una raíz.

DEMOSTRACIÓN. Consideramos el homomorfismo h_α dado en el lema. Ya que $K[X]$ es un dominio euclídeo, en particular es un dominio de ideales principales, y el núcleo de h_α está generado por un polinomio $f(X)$. Ya que α es algebraico sobre K, $f(X)$ es un polinomio no nulo, y tampoco es un polinomio constante. Si $f(X)$ se factoriza en la forma $f(X) = g_1(X)g_2(X)$ con $g_1(X)$, $g_2(X) \in K[X]$, entonces $g_1(\alpha)g_2(\alpha) = 0$, luego $g_1(\alpha) = 0$ ó $g_2(\alpha) = 0$, y tenemos que $g_1(X)$ ó $g_2(X)$ pertenece a $(f(X))$, entonces $g_1(X)$ ó $g_2(X)$ es una unidad en $K[X]$, y $f(X)$ es un polinomio irreducible en $K[X]$. Por otro lado si $g(X)$ es un polinomio de grado mínimo tal que $g(\alpha) = 0$, entonces $g(X) \in (f(X))$, luego $f(X)$ y $g(X)$ son asociados. □

El polinomio $f(X)$ determinado en la proposición anterior verifica:

Corolario. 1.8.
Sea F/K una extensión de cuerpos y $\alpha \in F$ un elemento algebraico sobre K, entonces existe un isomorfismo de cuerpos entre $K[X]/(f(X))$ y $K(\alpha)$. En particular $K[\alpha] = K(\alpha)$.

DEMOSTRACIÓN. Ya que $\mathrm{Ker}(h_\alpha) = (f(X))$, existe un morfismo de anillos de $K[X]/(f(X))$ en F, su imagen es un cuerpo, (ya que por ser $f(X)$ un polinomio irreducible en $K[X]$, el ideal $(f(X))$ es maximal), además contiene a K y contiene a α, y ya que coincide con la imagen de h_α, es el menor subanillo de F que contiene a K y a α. En particular es el menor subcuerpo de F que contiene a K y a α. □

El polinomio determinado en esta proposición podemos suponer que tiene coeficiente líder igual a 1, es un polinomio mónico. Este polinomio está así unívocamente determinado, se llama **polinomio mínimo** ó **polinomio mónico irreducible de** α sobre K, y se representa por $\mathrm{Irr}(\alpha, K, X)$ ó simplemente por $\mathrm{Irr}(\alpha, K)$.

Proposición. 1.9.
Sea F/K una extensión de cuerpos y $\alpha \in F$ un elemento algebraico sobre K. Si $\mathrm{gr}(\mathrm{Irr}(\alpha,K)) = n$, *entonces* $[K(\alpha):K] = n$ *y una base de* $K(\alpha)$ *como* K*-espacio vectorial es* $\{1, \alpha^1, \ldots, \alpha^{n-1}\}$.

Si α es algebraico, llamamos a $n = \mathrm{gr}(\mathrm{Irr}(\alpha,K))$ el **grado** de α sobre K.

DEMOSTRACIÓN. Por el Corolario (1.8.) cada elemento de $K(\alpha)$ es imagen por f_α de un $g(X) \in K[X]$, luego es de la forma $g(\alpha) = b_0 + b_1\alpha + \ldots + b_m\alpha^m$. Si $f(X) = \mathrm{Irr}(\alpha,K)$, tenemos que $g(X) \equiv g_1(X) \pmod{f(X)}$ para algún $g_1(X) \in K[X]$ y $\mathrm{gr}(g_1(X)) = r < n$ con coeficientes $k_0, k_1, \ldots, k_r \in K$, entonces tenemos

$$g(\alpha) = g_1(\alpha) = k_0 + k_1\alpha + \ldots + k_r\alpha^r,$$

y por tanto $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es un sistema de generadores de $K(\alpha)$. Para ver que es una base, supongamos que existen $k_0, k_1, \ldots, k_{n-1} \in K$ tales que $k_0 + k_1\alpha + \ldots + k_{n-1}\alpha^{n-1} = 0$, entonces el polinomio $f_1(X) = k_0 + k_1X + \ldots + k_{n-1}X^{n-1}$ verifica $f_1(\alpha) = 0$, luego $f_1(X) \in \mathrm{Ker}(f_\alpha) = (f(X))$, ya que $\mathrm{gr}(f(X)) = n > n-1 = \mathrm{gr}(f_1(X))$, tenemos $f_1(X) = 0$, y por tanto $k_0 = k_1 = \ldots = k_{n-1} = 0$. □

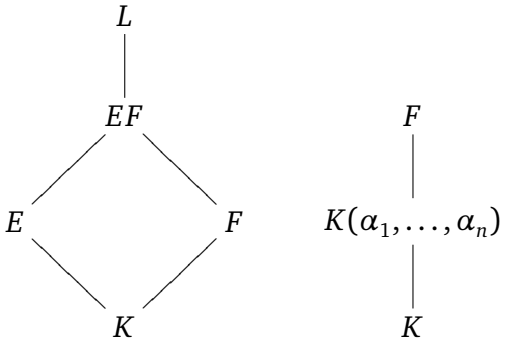
Proposición. 1.10.
Toda extensión finita de cuerpos F/K es una extensión algebraica.

DEMOSTRACIÓN. Basta ver que cada elemento $\alpha \in F$ es algebraico sobre K. Ya que la extensión es finita, $[F:K] = n < \infty$, los elementos $1, \alpha, \ldots, \alpha^n$ no son linealmente independientes, luego existen $k_0, k_1, \ldots, k_n \in K$, no todos nulos, tales que $k_0 + k_1\alpha + \ldots + k_n\alpha^n = 0$, entonces α es raíz del polinomio

$$f(X) = k_0 + k_1X + \ldots + k_nX^n,$$

y α es algebraico sobre K. □

Si E y F son dos subcuerpos de un cuerpo L que contienen un subcuerpo común K, llamamos el **compuesto** de E y F en L, al menor subcuerpo de L que contiene a E y F, lo representamos por EF.



Si F/K es una extensión de cuerpos y $\alpha_1, \ldots, \alpha_n \in F$, el menor subcuerpo de F que contiene a K y a $\alpha_1, \ldots, \alpha_n$ lo representábamos por $K(\alpha_1, \ldots, \alpha_n)$.
Una extensión F/K se llama de **generación finita** sobre K si existen elementos $\alpha_1, \ldots, \alpha_n \in F$ tales que $F = K(\alpha_1, \ldots, \alpha_n)$. Si $n = 1$, la extensión se llama **simple**. Como consecuencia, toda extensión de cuerpos F/K es la composición de todos los subcuerpos de generación finita sobre K.

Lema. 1.11.
Toda extensión finita F/K es una extensión de generación finita.

DEMOSTRACIÓN. Consideramos una base de F como K-espacio vectorial, $\{\alpha_1, \ldots, \alpha_n\}$, entonces $F = K[\alpha_1, \ldots, \alpha_n] = K(\alpha_1, \ldots, \alpha_n)$. □

El recíproco es cierto cuando los generadores son algebricos.

Proposición. 1.12.
Sea $F = K(\alpha_1, \ldots, \alpha_n)$ una extensión de generación finita y cada α_i, $1 \leq i \leq n$, es algebraico sobre K, entonces F/K es una extensión finita.

DEMOSTRACIÓN. Podemos construir una torre de cuerpos

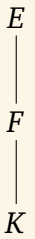
$$K \subseteq K(\alpha_1) \subseteq \ldots \subseteq K(\alpha_1, \ldots, \alpha_n) = F;$$

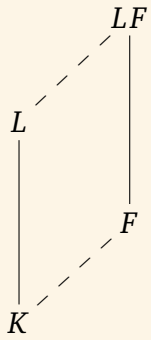
basta ver que $K(\alpha_1)/K$ es una extensión finita. Ya que α_1 es algebraico sobre K, tenemos que $K(\alpha_1) = K[\alpha_1]$ y $[K(\alpha_1) : K] = n$, siendo $n = \text{gr}(\text{Irr}(\alpha_1, K))$. □

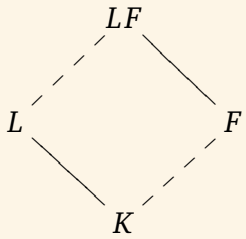
Teorema. 1.13.
Toda extensión generada por elementos algebraicos es una extensión algebraica.

DEMOSTRACIÓN. Supongamos que F/K es una extensión y que F está generado sobre K por elementos algebraicos $\{\alpha_i \mid i \in I\}$. Para cada $\alpha \in F$, por la Proposición (1.5.), existen $i_1, \ldots, i_r \in I$ tales que $\alpha \in K(\alpha_{i_1}, \ldots, \alpha_{i_r})$; por la proposición anterior la extensión de generación finita $K(\alpha_{i_1}, \ldots, \alpha_{i_r})/K$ es algebraica, luego α es algebraico sobre K. □

Teorema. 1.14.
(1) Si $K \subseteq F \subseteq E$ es una torre de cuerpos, son equivalentes:
(a) E/K es una extensión algebraica (resp. finita);
(b) E/F y F/K son extensiones algebraicas (resp. finitas).
(2) Si $K \subseteq L \subseteq E$ y $K \subseteq F \subseteq E$ son dos torres de cuerpos, y L/K es una extensión algebraica (resp. finita), entonces LF/F es una extensión algebraica (resp. finita).
(3) Si $K \subseteq L \subseteq E$ y $K \subseteq F \subseteq E$ son dos torres de cuerpos y L/K, F/K son extensiones algebraicas (resp. finitas), entonces LF/K es una extensión algebraica (resp. finita).

(1)


(2)


(3)


DEMOSTRACIÓN. Caso de extensiones finitas.
(1). Ya fue realizado en el Lema (1.2.)
(2). Si L/K es una extensión finita, en particular es finitamente generada y algebraica. Supongamos que $L = K(u_1, \ldots, u_n)$, entonces $LF = FK(u_1, \ldots, u_n) = F(u_1, \ldots, u_n)$, y ya que cada u_i es algebraico sobre K, y por tanto también sobre F, resulta que LF/F es una extensión finitamente generada por elementos algebraicos, resulta pues, aplicando la Proposición (1.12.) que es una extensión finita.
(3). Si L/K es finita, entonces (2) LF/F es finita, y ya que F/K es finita, por (1) resulta que LF/K es finita.
Caso de extensiones algebraicas.
(1).
(a) $\Leftrightarrow$ (b). Si E/K es una extensión algebraica, entonces es evidente que F/K y E/F son también algebraicas.
(b) $\Leftrightarrow$ (a). Para $\alpha \in E$, existe $f(X) \in F[X]$ no nulo tal que $f(\alpha) = 0$, ya que E/F es una extensión algebraica. Si $f(X) = a_0 + a_1X + \ldots + X^n$, entonces α es un elemento algebraico sobre el cuerpo $K(a_0, a_1, \ldots, a_{n-1})$, y por lo tanto la extensión

$$K(a_0, a_1, \ldots, a_{n-1}, \alpha)/K(a_0, a_1, \ldots, a_{n-1})$$

es finita. Además existe una torre de cuerpos

$$K \subseteq K(a_0) \subseteq K(a_0, a_1) \subseteq \ldots \subseteq K(a_0, a_1, \ldots, a_{n-1}) \subseteq K(a_0, a_1, \ldots, a_{n-1}, \alpha),$$

ya que F/K es una extensión algebraica, tenemos que cada extensión

$$K(a_0, a_1, \ldots, a_{i+1})/K(a_0, a_1, \ldots, a_i)$$

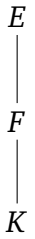
algebraica, y por tanto finita, entonces la extensión $K(a_0, a_1, \ldots, a_{n-1}, \alpha)/K$ es finita, luego algebraica.

(2). Si L/K es una extensión algebraica, para cada $\alpha \in L$ la extensión $K(\alpha)/K$ es finita, entonces aplicando (2) para extensiones finitas, tenemos que $FK(\alpha)/FK$ es una extensión finita, pero $FK(\alpha) = F(\alpha)$, y $FK = F$, luego resulta que $F(\alpha)/F$ es una extensión finita, y por tanto que α es algebraico sobre F. Ya que todo elemento de LF puede escribirse como un polinomio en los elementos de L, con coeficientes en F, $LF = F[L]$. La extensión LF/F es algebraica, ya que está generada por elementos algebraicos.

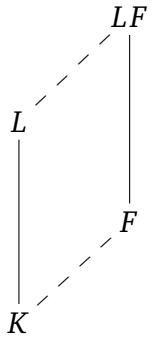
(3). Por (2) resulta que LF/F es algebraica, y como F/K es también algebraica, por (1) tenemos que LF/K es algebraica. □

Una clase de extensiones que verifica las condiciones del teorema se llama una **clase distinguida de extensiones**. Las condiciones del teorema se pueden expresar gráficamente mediante:

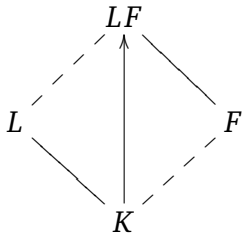
(1)



(2)



(3)



1.1. Ejercicios

Teoría de cuerpos

Ejercicio. 1.15.
Sea F un cuerpo finito de característica p. Demuestra que $|F| = p^n$ para algún entero positivo n.
Ref.: 4161e_001 SOLUCIÓN

Ejercicio. 1.16.
Razona, sabiendo que π y e son trascendentes, cuales de los siguientes números complejos son algebraicos o trascendentes sobre $\mathbb{Q}$.
(1) $\sqrt{7}$.
(2) $\sqrt[3]{3}$.
(3) π^2.
(4) $e^3 + 1$.
(5) $\sqrt{i} + 2$.

Ref.: 4161e_002 SOLUCIÓN

Ejercicio. 1.17.
Sea F/K una extensión de cuerpos y $\alpha \in F$ un elemento algebraico sobre K. Demuestra que los elementos $\alpha + 5$ y α^2 son algebraicos sobre K. En cada uno de los casos, ¿es cierto el recíproco?
Ref.: 4161e_003 SOLUCIÓN

Ejercicio. 1.18.
Sea K un cuerpo, $K[X]$ el anillo de polinomios con coeficientes en K, y $K(X)$ su cuerpo de fracciones. Demuestra que cada elemento de $K[X]$, que no está en K, es trascendente sobre K. Demuestra el resultado análogo para $K(X)$.
Ref.: 4161e_004 SOLUCIÓN

Ejercicio. 1.19.
Demuestra que el polinomio $f(X) = X^3 + 3X + 1$ *es irreducible en* $\mathbb{Q}[X]$. *Si* α *es una raíz de* $f(X)$ *en una extensión de* $\mathbb{Q}$, *calcula* $(1+\alpha)(1+\alpha+\alpha^2)$ *y* $(1+\alpha)/(1+\alpha+\alpha^2)$.
Ref.: 4161e_005 SOLUCIÓN

Ejercicio. 1.20.
Demuestra que el polinomio $f(X) = X^3 + X + 1$ *es irreducible sobre* $\mathbb{F}_2[X]$. *Si* α *es una raíz de* $f(X)$ *en una extensión de* $\mathbb{F}_2$, *calcula todas las potencias de* α.
Ref.: 4161e_006 SOLUCIÓN

Ejercicio. 1.21.
Calcula $\mathrm{Irr}(\alpha, \mathbb{Q})$ *en los siguientes casos:*

(1) $\alpha = 2 + \sqrt{5}$.
(2) $\alpha = \sqrt[4]{5} + \sqrt{5}$.
(3) $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$.

Da en cada caso una $\mathbb{Q}$*-base de* $F = \mathbb{Q}(\alpha)$.
Ref.: 4161e_007 SOLUCIÓN

Ejercicio. 1.22.
Calcula $\mathrm{Irr}(\alpha, \mathbb{Q})$ *en los siguientes casos:*

(1) $\alpha = \beta^2 - 1$, *siendo* β *una raíz del polinomio* $X^3 - 2X - 2$.
(2) $\alpha = \beta^2 + \beta$, *siendo* β *una raíz del polinomio* $X^3 + 3X^2 - 3$.
(3) $\alpha = 1/\beta^2$, *con* β *una raíz del polinomio* $X^4 + X + 1$.

Da en cada caso una $\mathbb{Q}$*-base de* $F = \mathbb{Q}(\alpha)$.
Ref.: 4161e_008 SOLUCIÓN

Ejercicio. 1.23.
Calcula $[F:\mathbb{Q}]$ *en los siguientes casos:*

(1) $F=\mathbb{Q}(\sqrt{7},i)$.
(2) $F=\mathbb{Q}(\sqrt[3]{5},\sqrt{-2})$.
(3) $F=\mathbb{Q}(\sqrt{18},\sqrt[4]{2})$.
(4) $F=\mathbb{Q}(\sqrt{8},3+\sqrt{50})$.
(5) $F=\mathbb{Q}(\sqrt{2},\sqrt{3})$.
(6) $F=\mathbb{Q}(\sqrt{3},\sqrt{-5},\sqrt{7})$.
(7) $F=\mathbb{Q}(\sqrt[3]{2},\beta)$, *donde* $\mathrm{Irr}(\beta,\mathbb{Q})=X^4+6X+2$.

En cada uno de los casos da una $\mathbb{Q}$*-base de* F.
Ref.: 4161e_009 *SOLUCIÓN*

Ejercicio. 1.24.
Razona si el elemento α *genera cada una de las siguientes extensiones de* $\mathbb{Q}$*:*

(1) $\alpha=\sqrt{2}+\sqrt{5}\in\mathbb{Q}(\sqrt{2},\sqrt{5})$.
(2) $\alpha=2+\sqrt[3]{9}\in\mathbb{Q}(\sqrt[3]{3})$.
(3) $\alpha=\frac{\sqrt{2}-1}{1+\sqrt{2}}\in\mathbb{Q}(\sqrt{2})$.
(4) $\alpha=\beta^2+\beta+1\in\mathbb{Q}(\beta)$, *donde* $\mathrm{Irr}(\beta,\mathbb{Q})=X^3+5X-5$.

Ref.: 4161e_010 *SOLUCIÓN*

Ejercicio. 1.25.
Demuestra que si $f(X)$ *es un polinomio irreducible sobre* K *de grado* n *y si* F/K *es una extensión finita de grado primo relativo con* n *entonces* $f(X)$ *es irreducible sobre* F.
Ref.: 4161e_011 *SOLUCIÓN*

Ejercicio. 1.26.
Demuestra que si F/K *es una extensión de grado primo entonces para todo* $\alpha\in F\setminus K$, *se tiene* $F=K(\alpha)$.

Ref.: 4161e_012 SOLUCIÓN

Ejercicio. 1.27.
Demuestra que si $[K(\alpha):K]$ *es impar entonces* $K(\alpha)=K(\alpha^2)$.
Ref.: 4161e_013 SOLUCIÓN

Ejercicio. 1.28.
Sea $F=\mathbb{Q}(u_1,\ldots,u_n)$ *donde* $u_i^2\in\mathbb{Q}$ *para* $i=1,\ldots,n$. *Demuestra que* $\sqrt[3]{2}\notin F$.
Ref.: 4161e_014 SOLUCIÓN

Ejercicio. 1.29.
Demuestra que $\mathbb{Q}(\sqrt{i})=\mathbb{Q}(i,\sqrt{2})$.
Ref.: 4161e_015 SOLUCIÓN

Ejercicio. 1.30.
Prueba que $\mathbb{Q}(\sqrt{2}+i)=\mathbb{Q}(\sqrt{2})(i)=:\mathbb{Q}(\sqrt{2},i)$.
Ref.: 4161e_081 SOLUCIÓN

Ejercicio. 1.31.
Calcula

(1) $\mathrm{Irr}((-2+i\sqrt{3})/2,\mathbb{Q})$ *y*
(2) $\mathrm{Irr}(\sqrt{t+1},\mathbb{F}_3(t))$, *siendo* t *trascendente sobre* $\mathbb{F}_3$.

Ref.: 4161e_016 SOLUCIÓN

Ejercicio. 1.32.
Calcula el polinomio mónico irreducible de $\alpha = \sqrt{t^3+1}$ *sobre* $\mathbb{F}_3(t)$*, donde* t *es trascendente sobre* $\mathbb{F}_3$*.*
Ref.: 4161e_051 SOLUCIÓN

Ejercicio. 1.33.
Demuestra que cualquier dominio de integridad conteniendo a un cuerpo K*, y contenido en una extensión algebraica de* K*, es un cuerpo.*
Ref.: 4161e_017 SOLUCIÓN

Ejercicio. 1.34.
Sea F/K *una extensión de cuerpos. Si* $\alpha \in F$ *es un elemento algebraico sobre* $K(\beta)$ *para algún* $\beta \in F$ *y* α *es trascendente sobre* K *entonces demuestra que* β *es algebraico sobre* $K(\alpha)$*.*
Ref.: 4161e_018 SOLUCIÓN

Ejercicio. 1.35.
Sea F/K *una extensión de cuerpos y* $a \in F$ *un elemento algebraico sobre* K*. ¿Debe necesariamente* $\mathrm{Irr}(a,K)$ *factorizarse en factores lineales en* $K(a)$*?*
Ref.: 4161e_019 SOLUCIÓN

Ejercicio. 1.36.
Sea $f \in K[X]$ *un polinomio irreducible de grado* n*. Sea* $g \in K[X]$ *arbitrario. Demuestra que todo factor irreducible del polinomio* $h(X) = f(g(X))$ *tiene grado divisible por* n*.*
Ref.: 4161e_020 SOLUCIÓN

Ejercicio. 1.37.
Sea K un cuerpo de característica distinta de 2, $f(X) = X^2 + aX + b$ un polinomio irreducible en K. Demuestra que existe un d tal que $d^2 \in K$ y $f(X)$ se factoriza en $K(d)$.
Ref.: 4161e_050 SOLUCIÓN

Ejercicios complementarios

Ejercicio. 1.38.
Sean F_1/K_1 y F_2/K_2 extensiones de cuerpos y $h : K_1 \longrightarrow K_2$ un homomorfismo de cuerpos.

(1) h induce un homomorfismo de $h : K_1[X] \longrightarrow K_2[X]$ mediante $h(X) = X$.
(2) Si h se extiende a un homomorfismo $h' : F_1 \longrightarrow F_2$, para cada polinomio $f(X) \in K_1[X]$, y cada $\alpha \in F_1$ tal que $f(\alpha) = 0$, se tiene que $h'(\alpha)$ es una raíz de $h(f(X))$.
(3) h se extiende a un homomorfismo $h : \dfrac{K_1[X]}{(f(X))} \longrightarrow \dfrac{K_2[X]}{(h(f(X)))}$.
(4) Si $\alpha \in F_1$ es una raíz de $f(X)$ y $f(X) \in K_1[X]$ es irreducible, entonces h se extiende a un homomorfismo $h' : K_1(\alpha) \longrightarrow K_2(f(\alpha))$.

Ref.: 4161e_086 SOLUCIÓN

Ejercicio. 1.39.
Si F/K una extensión de cuerpos y $f(X) \in K[X]$ es un polinomio, se verifica:

(1) Si $h : F/K \longrightarrow F/K$ es un automorfismo y $\alpha \in F$ es una raíz de $f(X)$, entonces $h(\alpha)$ es también una raíz de $f(X)$.
(2) Si $f(X) \in K[X]$ es irreducible y α, β son raíces de $f(X)$, existe un isomorfismo $h : K(\alpha)/K \longrightarrow K(\beta)/K$ que verifica $h(\alpha) = \beta$.

Ref.: 4161e_087 SOLUCIÓN

Ejercicio. 1.40.
Sea $f(X) = X^2 + X + 1 \in \mathbb{F}_5[X]$. Consideramos el anillo cociente $K = \mathbb{F}_5[X]/(X^2 + X + 1)$.

(1) Prueba que K es un cuerpo extensión de $\mathbb{F}_5$.

(2) *Prueba que $f(X)$ no tiene raíces en $\mathbb{F}_5$ pero sí en K.*
(3) *Prueba que $K = \mathbb{F}_5(\alpha)$ siendo α una raíz de $f(X)$ en K.*
(4) *Prueba que $f(X)$ es irreducible en $\mathbb{F}_5$ y reducible en K. Halla una factorización de $f(X)$ en K.*

Ref.: 4161e_021 SOLUCIÓN

Ejercicio. 1.41.
Sea $\mathbb{C}/K$ una extensión de cuerpos, siendo $K = \mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\pi)$ ó $\mathbb{Q}(\sqrt[6]{2})$. Clasifica como algebraico o transcendente sobre K cada uno de los siguientes elementos

(1) $\frac{1+\sqrt{2}}{2}$.
(2) $1+i$.
(3) $\sqrt{2}+\sqrt{3}$.
(4) $\sqrt{1+\sqrt[3]{2}}$.
(5) π^2.
(6) $\sqrt{\pi}$.

Ref.: 4161e_022 SOLUCIÓN

Ejercicio. 1.42.
Se considera la extensión de cuerpos $\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}$.

(1) *Demuestra que cualquier elemento de $\mathbb{Q}(\sqrt{3},\sqrt{5})$ puede expresarse, de forma única, como $a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}$, donde $a,b,c,d \in \mathbb{Q}$.*
(2) *Prueba que $\alpha = \sqrt{3}+\sqrt{5}$ genera la extensión, y calcula* $\mathrm{Irr}(\alpha,\mathbb{Q})$.
(3) *Calcula explícitamente el inverso de $\beta = 1+\sqrt{3}-\sqrt{15}$.*

Ref.: 4161e_023 SOLUCIÓN

Ejercicio. 1.43.
Demuestra que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ es una extensión finita de cuerpos. Halla una base de ella y expresa

(1) $\left(\sqrt[3]{4}+5\sqrt[3]{2}\right)^{-1}$,

(2) $\frac{1+\sqrt[3]{2}+\sqrt[3]{4}}{\sqrt[3]{2}-1}$ y
(3) $\frac{1}{\sqrt[3]{2}+1}+\frac{\sqrt[3]{4}}{2-\sqrt[3]{2}}$,

en función de los elementos de la base hallada.
Ref.: 4161e_024 SOLUCIÓN

Ejercicio. 1.44.
Encuentra una base de la extensión $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. *Expresa en función de dicha base el inverso de* $\sqrt{2+\sqrt{2}}$.
Ref.: 4161e_025 SOLUCIÓN

Ejercicio. 1.45.
Demuestra que $\mathbb{Q}(\sqrt[3]{5},\sqrt{2})/\mathbb{Q}$ *es una extensión finita de cuerpos. Halla una base de ella y expresa* $(\sqrt[3]{5}+\sqrt{2})^{-1}$ *en función de los elementos de la base.*
Ref.: 4161e_026 SOLUCIÓN

Ejercicio. 1.46.
Estudio de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

(1) *Calcula* $\mathrm{Irr}(\sqrt{2}+\sqrt{3},\mathbb{Q})$.
(2) *Demuestra que* $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$. *Deduce que* $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$.
(3) *Demuestra que* $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.
(4) *Describe dos bases diferentes de* $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

Ref.: 4161e_027 SOLUCIÓN

Ejercicio. 1.47.
Sean n y m dos números naturales distintos mayores que 1 y libres de cuadrados.

(1) Demuestra que $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$.
(2) Demuestra que $[\mathbb{Q}(\sqrt{n}, \sqrt{m}) : \mathbb{Q}] = 4$.
(3) Demuestra que $\sqrt{nm} \in \mathbb{Q}(\sqrt{n} + \sqrt{m})$.
(4) Demuestra que $n\sqrt{m} + m\sqrt{n} \in \mathbb{Q}(\sqrt{n} + \sqrt{m})$.
(5) Demuestra que $\sqrt{m}, \sqrt{n} \in \mathbb{Q}(\sqrt{n} + \sqrt{m})$.
(6) Demuestra que $\mathbb{Q}(\sqrt{n}, \sqrt{m}) = \mathbb{Q}(\sqrt{n} + \sqrt{m})$.
(7) Calcula $\mathrm{Irr}(\sqrt{n} + \sqrt{m}, \mathbb{Q})$ e $\mathrm{Irr}(\sqrt{n}, \mathbb{Q}(\sqrt{m}))$.

Ver también el Ejercicio (1.57.)
Ref.: 4161e_028 *SOLUCIÓN*

Ejercicio. 1.48.
Extensiones de $\mathbb{Q}$ de grado 2.

(1) Demuestra que si $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^2 - 2$ e $\mathrm{Irr}(\beta, \mathbb{Q}) = X^2 - 4X + 2$, entonces $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.
(2) Si $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ es una extensión de grado 2 sobre $\mathbb{Q}$, y $f(X) = \mathrm{Irr}(\alpha, \mathbb{Q})$, calcula $\mathrm{Irr}(\beta, \mathbb{Q})$.
(3) Determina el polinomio $\mathrm{Irr}(\sqrt{3} + 3, \mathbb{Q})$.
(4) ¿Es $g(X) = X^7 + 7X + 7$ irreducible sobre $\mathbb{Q}(\sqrt{3})$?
(5) Prueba que si $F/\mathbb{Q}$ es una extensión de grado 2, existe $d \in \mathbb{Q}$ tal que $F = \mathbb{Q}(\alpha)$, para α una raíz de $X^2 - d$.

Ref.: 4161e_029 *SOLUCIÓN*

Ejercicio. 1.49.
Sea α una raíz de $X^3 + 2X + 2 \in \mathbb{Q}[X]$. Demuestra explícitamente (mediante un polinomio) que los elementos siguientes son algebraicos sobre $\mathbb{Q}$. ¿Cuáles son sus grados?

(1) $\alpha + 1$.
(2) α^2.

Ref.: 4161e_030 *SOLUCIÓN*

Ejercicio. 1.50.
Sea E/K una extensión de cuerpos y $\alpha \in E$ un elemento algebraico sobre K. Demuestra, mediante un polinomio, que los elementos $\alpha+1$ y α^2 son algebraicos sobre K. ¿Es cierto que si alguno de esos elementos es algebraico sobre K, entonces lo es α?
Ref.: 4161e_031 SOLUCIÓN

Ejercicio. 1.51.
Sea F/K una extensión de grado $[F:K]=n$.
(1) Para todo $u \in F$ definimos $\lambda_u : F \to F$ como la multiplicación por u, esto es: $\lambda_u(v) = uv$. Demuestra que λ_u es una aplicación K–lineal.
(2) Demuestra que F es isomorfo a un subcuerpo del anillo $\mathscr{M}_n(K)$ de matrices cuadradas $n \times n$ con coeficientes en K.
(3) Razona que $\mathscr{M}_n(K)$ contiene una copia isomorfa de toda extensión F/K de grado n.

Ref.: 4161e_032 SOLUCIÓN

Ejercicio. 1.52.
Sea M_u la matriz de la transformación λ_u definida en el Ejercicio (1.51.). Demuestra que u es raíz del polinomio característico de M_u.
(Observación. Esto da un procedimiento efectivo para determinar una ecuación de grado n del que $u \in F$ sea una raíz). Usa este procedimiento para obtener el polinomio mónico irreducible de $1+\sqrt[3]{2}+\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$.
Ref.: 4161e_033 SOLUCIÓN

Ejercicio. 1.53.
Determina el conjunto de los polinomios mónicos irreducibles sobre $\mathbb{R}$.
Ref.: 4161e_052 SOLUCIÓN

Ejercicio. 1.54.
Sea F/K una extensión. Si $X^n - a \in K[X]$ es irreducible, $\alpha \in F$ es una raíz, y $m \in \mathbb{N}$ un divisor de n, demuestra que el grado de α^m sobre K es n/m. ¿Cuál es el polinomio mónico irreducible de α^m sobre K?
Ref.: 4161e_053 SOLUCIÓN

Ejercicio. 1.55.
Sea F/K una extensión y sean $\alpha, \beta \in F$ algebraicos sobre K de grados, respectivamente n y m.
(1) Demuestra que $K[(\alpha,\beta) : K] \leq n \cdot m$.
(2) Demuestra que si n y m son primos relativos, entonces $[K(\alpha,\beta) : K] = n \cdot m$.
(3) Si n y m son primos relativos y $a, b \in \mathbb{Z}$ mayores que 1. Demuestra que $[\mathbb{Q}(\sqrt[n]{a}, \sqrt[m]{b}) : \mathbb{Q}] = n \cdot m$.
Ref.: 4161e_054 SOLUCIÓN

Ejercicio. 1.56.
Sea p un entero primo positivo. Prueba que existe a lo sumo un número finito de polinomios mónicos irreducibles de grado n en $\mathbb{F}_p$. Describe un método para obtener estos polinomios.
Ref.: 4161e_055 SOLUCIÓN

Ejercicio. 1.57.
Sean $p, q \in \mathbb{Z}$ primos positivos distintos y $F = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Prueba que:
(1) $[F : \mathbb{Q}] = 4$ y $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ es una $\mathbb{Q}$–base de F.
(2) $\mathrm{Irr}(\sqrt{p} + \sqrt{q}) = X^4 - (p+q)X^2 + (p-q)^2$.
(3) $F = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.
(4) $\mathbb{Q}(\sqrt{p}) \neq \mathbb{Q}(\sqrt{q})$.

Ver también el Ejercicio (1.47.).
Ref.: 4161e_056 SOLUCIÓN

Ejercicio. 1.58.
Determina los polinomios mónicos irreducibles sobre $\mathbb{F}_2$ y $\mathbb{F}_3$ de grados 1, 2, 3 y 4. Construye cuerpos finitos de 2, 4, 8, 16, 25 y 27 elementos.
Ref.: 4161e_057 SOLUCIÓN

Ejercicio. 1.59.
Sea K un cuerpo de característica $p \neq 0$, y q una potencia de p. Definimos $K^q = \{a^q \mid a \in K\}$. Prueba que K^q es un cuerpo y que la aplicación $a \mapsto a^q$ es un isomorfismo de K en K^q.
Ref.: 4161e_058 SOLUCIÓN

Ejercicio. 1.60.
Demuestra que existen infinitos polinomios mónicos irreducibles sobre $\mathbb{Q}[X]$.
Ref.: 4161e_059 SOLUCIÓN

Ejercicio. 1.61.
Determina el polinomio mónico irreducible de $\alpha = \sqrt{2} + \sqrt[3]{2}$ sobre $\mathbb{Q}$.
Ref.: 4161e_061 ver Ref.: 203e_56 SOLUCIÓN

Ejercicio. 1.62.
Determina el polinomio mónico irreducible de $\alpha = \sqrt{2} + \sqrt[4]{2}$ sobre $\mathbb{Q}$.
Ref.: 4161e_062 ver Ref.: 203e_57 SOLUCIÓN

Ejercicio. 1.63.
Sean α, β elementos algebraicos no nulos sobre un cuerpo K con polinomios irreducibles $f(X) = \mathrm{Irr}(\alpha, K)$ y $g(X) = \mathrm{Irr}(\beta, K)$, respectivamente. Determina:

(1) El polinomio irreducible de $\gamma = \alpha + \beta$.
(2) El polinomio irreducible de $\gamma = \alpha\beta$.
(3) El polinomio irreducible de $\gamma = 1/\alpha$.

Ref.: 4161e_063 SOLUCIÓN

Ejercicio. 1.64.
Sea F/K una extensión de cuerpos de grado finito y $\sigma : F \longrightarrow F'$ un homomorfismo de cuerpos. Demuestra que $[F : K] = [F^\sigma : K^\sigma]$.
Ref.: 4161e_066 SOLUCIÓN

Ejercicio. 1.65.
Sea F/K una extensión de cuerpos de grado finito. Demuestra que cada endomorfismo de K–álgebras de F deja fijo K y es un automorfismo.
Ref.: 4161e_067 SOLUCIÓN

Ejercicio. 1.66.
Demuestra que todo automorfismo de un cuerpo deja elementalmente fijo al subcuerpo característico.
Ref.: 4161e_068 SOLUCIÓN

Ejercicio. 1.67.
Demostrar que las extensiones $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ no son isomorfas.
Ref.: 4161e_069 SOLUCIÓN

Ejercicio. 1.68.
Demostrar que el polinomio X^4-2X^2-2 es irreducible sobre $\mathbb{Q}[X]$, y encontrar dos pares de raíces que generan extensiones no isomorfas.
Ref.: 4161e_070 SOLUCIÓN

Ejercicio. 1.69.
Encontrar, si es posible, en cada uno de los casos siguientes un elemento α tal que $\mathrm{Irr}(\alpha,K)$ sea el polinomio dado:
(1) X^2-4, siendo $K=\mathbb{R}$.
(2) X^2+1, siendo $K=\mathbb{F}_3$.
(3) X^2+1, siendo $K=\mathbb{F}_5$.
(4) $X^7-3X^6+4X^3-X-1$, siendo $K=\mathbb{R}$.

Ref.: 4161e_071 SOLUCIÓN

Ejercicio. 1.70.
Si α es una raíz del polinomio $X^2+X+1\in\mathbb{Q}[X]$, expresa $3\alpha^2+\dfrac{2}{\alpha+4}$ como un polinomio en α.
Ref.: 4161e_072 SOLUCIÓN

Ejercicio. 1.71.
Sea F/K una extensión de cuerpos y $\alpha\in F$ un elemento algebraico sobre K, se tiene que toda expresión polinómica no nula de α con coeficientes en K es un elemento algebraico sobre K. Prueba el resultado recíproco: si $f(\alpha)$ es una de tales expresiones que es algebraica sobre K, entonces α es algebraico sobre K.
Ref.: 4161e_073 SOLUCIÓN

Ejercicio. 1.72.
Demostrar que $\sqrt[3]{2}+\sqrt{3}$ no es un número racional, pero es algebraico sobre $\mathbb{Q}$. ¿Cuál es su grado?
Ref.: 4161e_074 SOLUCIÓN

Ejercicio. 1.73.
Demostrar que el polinomio X^4-2X^2+9 es irreducible sobre $\mathbb{Q}$.
Ref.: 4161e_075 SOLUCIÓN

Ejercicio. 1.74.
Encuentra el polinomio irreducible de $\alpha=1+2^{\frac{1}{n}}+\cdots+2^{\frac{n-1}{n}}$ sobre $\mathbb{Q}$.
Ref.: 4161e_082 SOLUCIÓN

Ejercicio. 1.75.
Se considera $\alpha=\sqrt{2}+\sqrt{3}+\sqrt{5}\in F=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$.

(1) Prueba que $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}]=8$.
(2) Prueba que $F=\mathbb{Q}(\alpha)$.
(3) Calcula $\mathrm{Irr}(\alpha,\mathbb{Q})$.
(4) Encuentra elementos $\beta\in F$, de grado cuatro sobre Q.

Ref.: 4161e_083 SOLUCIÓN

Ejercicio. 1.76.
Se considera $\alpha=\sqrt{2}+\sqrt[3]{2}\in F=\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$.

(1) Prueba que $F=\mathbb{Q}(\alpha)$.
(2) Calcula $\mathrm{Irr}(\alpha,\mathbb{Q})$.

Se considera ahora la extensión $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$.
(3) Estudia si existe un isomorfismo $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q} \cong \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q}$

Ver también los ejercicios (1.72.) *y* (1.61.).
Ref.: 4161e_084 *SOLUCIÓN*

Ejercicio. 1.77.
Hallar $\mathrm{Irr}(u+v, \mathbb{Q})$ *para*
(1) $u = \sqrt{2}$, $v = \sqrt[3]{3}$
(2) $u = i$, $v = \sqrt{2}$
(3) $u = \sqrt[3]{5}$, $v = \sqrt[5]{7}$

Ref.: 4161e_088 *SOLUCIÓN*

Ejercicio. 1.78.
Consideramos $\mathbb{Z} \subseteq \mathbb{Q}$ *y* $f(X) \in \mathbb{Z}[X]$ *un polinomio de grado positivo.*
(1) Si $f(X) \in \mathbb{Z}[X]$ *es irreducible, prueba que* $f(X)$ *es irreducible sobre* $\mathbb{Q}$.
(2) Si $f(X) \in \mathbb{Z}[X]$ *es irreducible, entonces* $F = \dfrac{\mathbb{Q}[X]}{(f(X))}$ *es un cuerpo y tenemos inclusiones* $\mathbb{Z} \subseteq Q \subseteq F$.
(3) Si llamamos $x = X + (f(X)) \in F$, *prueba que* x *es una raíz de* $f(X) \in F[X]$.

Ref.: 4161e_089 *SOLUCIÓN*

Ejercicio. 1.79.
Describe los elementos del cuerpo $\dfrac{\mathbb{F}_2[X]}{(X^3+X+1)}$, *completando las tablas de la suma y el producto.*

Ref.: 4161e_090 *SOLUCIÓN*

Ejercicio. 1.80.
Calcula el polinomio mónico irreducible de $\alpha = \sqrt{t^2+1}$ *sobre* $\mathbb{F}_3(t)$.
Ref.: 4161e_091 SOLUCIÓN

Ejercicio. 1.81.
Se considera $f(X) = X^4+X+1 \in \mathbb{F}_2[X]$ *y el cuerpo* $\mathbb{F}_{16} = \dfrac{\mathbb{F}_2[X]}{(X^4+X+1)}$. *Sea* $\alpha = \overline{X} = X+(X^4+X+1) \in \mathbb{F}_{16}$.

(1) *Prueba que* α *es una raíz de* X^4+X+1 *en* $\mathbb{F}_{16}$.
(2) *Prueba que el orden de* α *en* $\mathbb{F}_{16}^\times = \mathbb{F}_{16} \setminus \{0\}$ *es 15.*
(3) *Observa que* α^3 *es un elemento de orden 5 y que* α^5 *es un elemento de orden 3. Haz un listado de todos los elementos de orden 3 y de todos los elementos de orden 5.*
(4) *En* $\mathbb{F}_{16}^\times$ *hay pues ocho elementos de orden 15. Cualquiera de ellos es un elemento primitivo. Determina un elemento primitivo* $\beta \in \mathbb{F}_{16}$ *que no sea raíz de* $f(X) = X^4+X+1$.
(5) *El polinomio* $g(X) = X^4+X^3+X^2+X+1 \in \mathbb{F}_2[X]$ *es un polinomio irreducible, si* γ *es una raíz de* $g(X)$, *entonces* γ *es elemento de orden 5.*
(6) *Observa que* $\mathbb{F}_{16} = \mathbb{F}_2(\alpha) = \mathbb{F}_2(\beta) = \mathbb{F}_2(\gamma)$, *y* $\mathbb{F}_{16}^\times = \langle\alpha\rangle = \langle\beta\rangle \neq \langle\gamma\rangle$
(7) *Los elementos de* $\mathbb{F}_{16}^\times$ *se clasifican por sus polinomios irreducibles. Completa el siguiente cuadro:*

Polinomio irreducible	*Raíces*
$X-1$	
X^2+X+1	
X^4+X+1	
X^4+X^3+1	
$X^4+X^3+X^2+X+1$	

Ref.: 4161e_092 SOLUCIÓN

Ejercicio. 1.82.
Se considera α *una raíz del polinomio* $X^6-3X^3-6 \in \mathbb{Q}[X]$. *Determina el grado* $[\mathbb{Q}(\alpha^2+1):\mathbb{Q}]$.
Ref.: 4161e_093 SOLUCIÓN

Ejercicio. 1.83.
Sea $f \in K[X]$ un polinomio irreducible de grado n y F/K una extensión de grado m. Sea $d = \mathrm{mcd}\{n,m\}$ y $g \in F[X]$ un factor irreducible de f. Prueba que
(1) $\frac{n}{d}$ divide a $\mathrm{gr}(g)$ y
(2) f tiene como máximo d factories irreducibles en F.

Ref.: 4161e_094 *SOLUCIÓN*

Ejercicio. 1.84.
Se considera F_1 (resp. F_2) el subcuerpo de $\mathbb{R}$ (resp. $\mathbb{C}$) de todos los elementos algebraicos sobre $\mathbb{Q}$.
(1) Prueba que $F_i/\mathbb{Q}$ es una extensión algebraica.
(2) Prueba que $[F_2 : F_1] = 2$.

Ref.: 4161e_095 *SOLUCIÓN*

2. Clausura algebraica

Teorema. 2.1. (Teorema de Kronecker)
Sea K un cuerpo y $f(X) \in K[X]$ un polinomio no constante, existe una extensión F/K en la que $f(X)$ tiene al menos una raíz.

DEMOSTRACIÓN. Si $f(X) \in K[X]$ es un polinomio no constante con coeficientes en un cuerpo K, vamos a determinar una extensión F/K en la que $f(X)$ tenga una raíz. Si $g(X)$ es un factor irreducible, en $K[X]$, de $f(X)$, entonces toda raíz de $g(X)$ es una raíz de $f(X)$, podemos entonces considerar que $f(X)$ es un polinomio irreducible. Consideramos la proyección canónica $\pi : K[X] \longrightarrow K[X]/(f(X))$, por ser $f(X)$ irreducible, $E = K[X]/(f(X))$ es un cuerpo, llamamos $\alpha = \pi(X)$ y tenemos que α es raíz del polinomio $\pi(f(X)) = f^{\pi}(X)$, ya que

$$f^{\pi}(\alpha) = f^{\pi}(\pi(X)) = \pi(f(X)) = 0.$$

Consideramos el conjunto $S = E \backslash \pi(K)$, y llamamos F a la unión disjunta de K y S, es claro que F es biyectivo con E. En E definimos dos operaciones de forma que la aplicación $\omega : F \longrightarrow E$ sea isomorfismo de cuerpos y $\omega_{|K} = \pi_{|K}$ y $\omega_{|S} = \mathrm{id}_S$. Tenemos pues una extensión de cuerpos F/K. En F el polinomio $f(X)$ tiene una raíz α, ya que $\omega(f(\alpha)) = f^{\pi}(\alpha) = 0$, y por ser ω un isomorfismo, $f(\alpha) = 0$. □

Corolario. 2.2.
Sea K un cuerpo y $f_1(X), \ldots, f_n(X) \in K[X]$ polinomios no constantes, existe una extensión F/K en la que cada $f_i(X)$, $1 \leq i \leq n$, tiene al menos una raíz.

DEMOSTRACIÓN. Si $n = 1$, el resultado es cierto. Si el resultado es cierto para $i \geq 1$, entonces existe un cuerpo E extensión de K tal que $f_1(X), \ldots, f_i(X)$ tienen al menos una raíz en E, consideramos $f_{i+1}(X) \in K[X] \subseteq E[X]$, existe un cuerpo F extensión de E tal que $f_{i+1}(X)$ tiene al menos una raíz en F. Es claro que $f_1(X), \ldots, f_i(X)$ también tienen al menos una raíz en F. Por inducción se obtiene el resultado. □

Sea K un cuerpo, y $f(X) \in K[X]$ un polinomio no constante. $f(X)$ se dice que **descompone en** K si admite una expresión como un producto de un elemento de K y polinomios de $K[X]$ de grado igual a 1.

$$f(X) = a(X - \alpha_1) \ldots (X - \alpha_n); \quad a, \alpha_1, \ldots, \alpha_n \in K.$$

4161-03.tex

Lema. 2.3.
Sea K un cuerpo, son equivalentes:

(a) Todo polinomio no constante $f(X) \in K[X]$ tiene al menos una raíz en K.
(b) Todo polinomio no constante $f(X) \in K[X]$ descompone en K.
(c) Los polinomios no constantes irreducibles en $K[X]$ son de grado uno.
(d) K no tiene extensiones algebraicas propias.
(e) No existen extensiones algebraicas F/K con $F \neq K$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si $f(X) \in K[X]$ es un polinomio no constante, entonces existe una raíz $\alpha_1 \in K$, y por tanto $f(X) = (X-\alpha_1)f_1(X)$, con $f_1(X) \in K[X]$; si $f_1(X)$ no es constante, existe una raíz $\alpha_2 \in K$ tal que $f_1(X) = (X-\alpha_2)f_2(X)$, con $f_2(X) \in K[X]$, y así seguimos hasta que $f_n(X)$ sea un polinomio constante, entonces $f(X)$ admite la expresión $f(X) = (X-\alpha_1)\dots(X-\alpha_n)f_n(X)$, con $f_n(X) \in K$.
(b) $\Rightarrow$ (c). Si $f(X) \in K[X]$ es un polinomio no constante e irreducible y $\mathrm{gr}(f(X)) = n$, entonces $f(X)$ admite la expresión $f(X) = a(X-\alpha_1)\dots(X-\alpha_n)$, con $a, \alpha_1, \dots, \alpha_n \in K$, lo que implica que $n = 1$.
(c) $\Rightarrow$ (d). Si F/K es una extensión algebraica de K y existe $\alpha \in F \setminus K$, entonces $f(X) = \mathrm{Irr}(\alpha, K)$ es un polinomio irreducible de grado mayor que 1, lo que es una contradicción, entonces necesariamente $F = K$.
(d) $\Rightarrow$ (a). Si $f(X) \in K[X]$ es un polinomio no constante, entonces existe una extensión F/K en la que $f(X)$ tiene al menos una raíz α, entonces $K(\alpha)/K$ es una extensión algebraica de K, y por la hipótesis $K(\alpha) = K$, luego $\alpha \in K$ y $f(X)$ tiene una raíz en K. □

Un cuerpo verificando las condiciones del lema se llama un cuerpo **algebraicamente cerrado**.

Vamos a ver que cada cuerpo K está contenido en un cuerpo algebraicamente cerrado; y que para cada cuerpo K podemos elegir una extensión algebraica F/K en la que F es un cuerpo algebraicamente cerrado.

Teorema. 2.4. (Teorema de Steinitz)
Si K es un cuerpo, existe un cuerpo algebraicamente cerrado F extensión de K.

DEMOSTRACIÓN. [Artin] Dado un polinomio $f(X) \in K[X]$ no constante, le asociamos la indeterminada X_f. Llamamos S al conjunto de todas estas indeterminadas, y construimos el anillo $K[S]$. El ideal generado por todos los polinomios de la forma $f(X_f)$ no es el anillo total, ya que si esto ocurriese, existiría una combinación

$$g_1(S)f_1(X_{f_1}) + \dots + g_r(S)f_r(X_{f_r}) = 1, \tag{I.1}$$

con $g_1(S),\dots,g_r(S) \in K[S]$. En este caso, si consideramos el subconjunto de S formado por las indeterminadas $X_i = X_{f_i}$, $1 \le i \le r$, las indeterminadas que aparecen en los polinomios $g_i(S)$, $1 \le i \le r$ y una extensión F/K en la que cada $f_i(X)$ tenga al menos una raíz α_i, $1 \le i \le r$, al hacer la evaluación del anillo $K[S]$ que aplica X_i en α_i, $1 \le i \le r$, y las demás indeterminadas a cero, entonces el primer miembro de la expresión (I.1) se aplica en cero, y el segundo se mantiene en 1, lo que es una contradicción.

Llamamos $\mathfrak{m}$ a un ideal maximal de $K[S]$ que contiene al ideal anterior, tenemos que $K[S]/\mathfrak{m}$ es un cuerpo, y existe un homomorfismo sobreyectivo de anillos $\varphi : K[S] \longrightarrow K[S]/\mathfrak{m}$.

Dado un polinomio no constante $f(X) \in K[X]$, el polinomio $\varphi(f(X))$ tiene una raíz en $K[S]/\mathfrak{m}$. Tenemos que si identificamos K con su imagen por φ, entonces $E_1 = K[S]/\mathfrak{m}$ es una extensión de K en la que cada polinomio no constante tiene al menos una raíz.

Podemos construir ahora una extensión E_2 de E_1 en la que todo polinomio no constante con coeficientes en E_1 tenga al menos una raíz. Este proceso se puede continuar. Se obtiene así una torre de cuerpos

$$K \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n \subseteq \cdots,$$

en la que cada polinomio no constante con coeficientes en E_n tiene al menos una raíz en E_{n+1}. Si llamamos $F = \cup\{E_n \mid n \in \mathbb{N}^*\}$, resulta que F es un cuerpo algebraicamente cerrado que es extensión de K. □

Corolario. 2.5.
Si K es un cuerpo, existe una extensión de K que es algebraica y algebraicamente cerrada.

DEMOSTRACIÓN. Por el teorema de Steinitz, existe una extensión F/K, con F algebraicamente cerrado. Llamamos E a $\{\alpha \in F \mid \alpha \text{ es algebraico sobre } K\}$; es un cuerpo intermedio. Falta ver que es algebraicamente cerrado, para ello, supongamos $f(X) \in E[X]$ un polinomio no constante, $f(X)$ tiene al menos una raíz en F, llamémosla α, entonces α es un elemento algebraico sobre E, y también sobre K, luego α pertenece a E y E es un cuerpo algebraicamente cerrado. □

Una extensión de cuerpos F/K se llama una **clausura algebraica** de K si
(I) es una extensión algebraica y
(II) F es un cuerpo algebraicamente cerrado.

Como consecuencia del corolario, todo cuerpo K tiene al menos una clausura algebraica. Más tarde veremos que las clausuras algebraicas verifican una cierta unicidad.

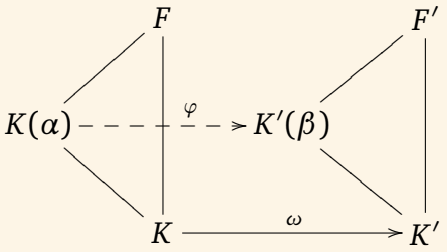
Vamos a estudiar propiedades elementales de homomorfismos de cuerpos para aplicarlos al estudio de la clausura algebraica.

Si F/K y F'/K' son extensiones de cuerpos y $\omega : K \cong K'$ es un isomorfismo de cuerpos, un homomorfismo de anillos $\varphi : F \longrightarrow F'$ se llama un **homomorfismo de cuerpos sobre** ω si $\varphi(k) = \omega(k)$ para todo $k \in K$. Cuando $\omega = 1_K$, en vez de homomorfismo de cuerpos sobre 1_K usamos **homomorfismo de cuerpos sobre** K, y se representa por $\varphi : F/K \longrightarrow F'/K$.

Lema. 2.6.
Sea $\varphi : F/K \longrightarrow F/K$ un homomorfismo de cuerpos sobre K, si F/K es una extensión algebraica, entonces φ es un automorfismo.

DEMOSTRACIÓN. Basta probar que φ es sobreyectivo. Dado $\alpha \in F$, llamamos $f(X) = \mathrm{Irr}(\alpha, K)$; si E es el subcuerpo de F generado sobre K por todas las raíces de $f(X)$ en F, resulta que E es una extensión finita de K ya que está generada por un número finito de elementos algebraicos sobre K. Además la imagen por φ de una raíz de $f(X)$ es también una raíz de $f(X)$, ya que $f(X)$ es invariante por φ. Como consecuencia $\varphi(E) \subseteq E$, y por ser E una extensión finita y ser la K-dimensión de E y de $\varphi(E)$ iguales, tenemos que $\varphi(E) = E$. Existe entonces $\beta \in E \subseteq F$ tal que $\varphi(\beta) = \alpha$, y por tanto φ es sobreyectiva. □

Proposición. 2.7.
Sea $\omega : K \cong K'$ un isomorfismo de cuerpos, F/K y F'/K' extensiones de cuerpos, $\alpha \in F$ un elemento algebraico sobre K con $f(X) = \mathrm{Irr}(\alpha, K)$. Llamamos $f^{\omega}(X)$ a la imagen de $f(X)$ por el isomorfismo $\omega : K[X] \cong K'[X]$ inducido por ω. Entonces para cada $\beta \in F'$ tal que $f^{\omega}(\beta) = 0$ existe un único isomorfismo de cuerpos $\varphi : K(\alpha) \cong K'(\beta)$ sobre ω tal que $\varphi(\alpha) = \beta$.



DEMOSTRACIÓN. Ya que $f^{\omega}(X)$ es imagen de $f(X)$ por un isomorfismo y $f(X)$ era irreducible, también $f^{\omega}(X)$ es irreducible en $K'[X]$. Luego si $f^{\omega}(\beta) = 0$, tenemos que $f^{\omega}(X) = \mathrm{Irr}(\beta, K')$, entonces tenemos $K'(\beta) \cong K'[X]/(f^{\omega}(X))$, y por tanto

$$K(\alpha) \cong K[X]/(f(X)) \cong K'[X]/(f^{\omega}(X)) \cong K'(\beta).$$

$$\alpha \mapsto X + (f(X)) \mapsto X + (f^{\omega}(X)) \mapsto \beta$$

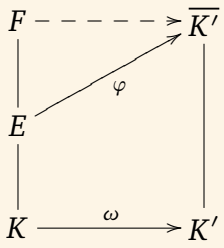
La unicidad de φ se deduce de que $\varphi(\alpha) = \beta$ y de que $\varphi_{|K} = \omega$. □

Corolario. 2.8.
En la situación anterior, si F' es algebraicamente cerrado, existen exactamente r extensiones de ω a $K(\alpha)$, donde r es el número de raíces distintas de $f(X)$.

DEMOSTRACIÓN. Es claro que para cada raíz β de $f^{\omega}(X)$ existe un homomorfismo de $K(\alpha)$ en F' que extiende a ω , y que cada homomorfismo está asociado a una raíz de β por la proposición anterior, además dos raíces distintas determinan homomorfismos distintos, por tanto tenemos el resultado. □

Procedamos ahora a estudiar las propiedades de la clausura algebraica de un cuerpo K respecto a homomorfismos sobre K.

Lema. 2.9.
Sean $\omega : K \cong K'$ un isomorfismo de cuerpos, $K \subseteq E \subseteq F$ una torre de extensiones algebraicas y $\overline{K'}$ una clausura algebraica de K', entonces cualquier homomorfismo de cuerpos $\varphi : E/K \longrightarrow \overline{K'}/K'$ sobre ω se puede extender a un homomorfismo $\psi : F/K \longrightarrow \overline{K'}/K'$ sobre ω.



DEMOSTRACIÓN. Llamamos

$$\Gamma = \{(E_i, \psi_i) \mid E_i \text{ cuerpo}, E \subseteq E_i \subseteq F, \psi_i : E_i \longrightarrow \overline{K'} \text{ sobre } \omega, \text{ y } \psi_{i|E} = \varphi\}.$$

Ya que $(E, \varphi) \in \Gamma$, tenemos que $\Gamma \neq \emptyset$. En Γ consideramos la relación de orden "$\leq$" definida por $(E_i, \psi_i) \leq (E_j, \psi_j)$ si $E_i \subseteq E_j$ y $\psi_{j|E_i} = \psi_i$. Γ es entonces un conjunto inductivo, (cada cadena ascendente de elementos de Γ tiene una cota superior en Γ). Aplicando el lema de Zorn, existe en Γ un elemento maximal, lo llamamos (E_0, ψ_0). Si $E_0 \neq F$, entonces existe $\alpha \in F \setminus E_0$. Sea $f(X) = \text{Irr}(\alpha, E_0)$, su imagen por ψ_0 es $f^{\psi_0}(X) \in \overline{K'}[X]$, luego tiene en $\overline{K'}$ una raíz β. Aplicando la Proposición (2.7.) existe un isomorfismo $\psi : E_0(\alpha) \cong \psi_0(E_0)(\beta)$ sobre ψ_0 siendo $\psi(\alpha) = \beta$, entonces $\psi_{|E} = \varphi$, y por tanto ψ extiende a φ, luego $(E_0(\alpha), \psi) \in \Gamma$, lo que es una contradicción, ya que $(E_0, \psi_0) < (E_0(\alpha), \psi)$ y (E_0, ψ_0) es un elemento maximal de Γ. □

Corolario. 2.10.
Si K es un cuerpo y K', K'' son dos clausuras algebraicas de K, existe un isomorfismo $\varphi : K'/K \longrightarrow K''/K$ sobre K.

DEMOSTRACIÓN. Tenemos que K'/K es una extensión algebraica y K''/K es una clausura algebraica, luego existe un homomorfismo $\varphi : K'/K \longrightarrow K''/K$ sobre K. Aplicando el lema (2.6.) se obtiene que φ es un isomorfismo. □

Como la clausura algebraica es única salvo isomorfismo, la representamos por $\overline{K}$.
Si K es un cuerpo con clausura algebraica $\overline{K}$, y E, F son dos cuerpos intermedios, $K \subseteq E, F \subseteq \overline{K}$. Decimos que E y F son K**–conjugados** si existe un isomorfismo $\varphi : \overline{K}/K \longrightarrow \overline{K}/K$ tal que $\varphi(E) = F$. Dos elementos $\alpha, \beta \in \overline{K}$ decimos que son K**–conjugados** si existe un isomorfismo $\varphi : \overline{K}/K \longrightarrow \overline{K}/K$ tal que $\varphi(\alpha) = \beta$.

Lema. 2.11.
Sea K un cuerpo, $\overline{K}$ una clausura algebraica de K, y $\alpha, \beta \in \overline{K}$, son equivalentes:
(a) α y β son K-conjugados;
(b) $\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$;
(c) Existe un isomorfismo $\eta : K(\alpha) \longrightarrow K(\beta)$ sobre K tal que $\eta(\alpha) = \beta$;
(d) Existe un homomorfismo $\psi : K(\alpha) \longrightarrow \overline{K}$ sobre K tal que $\psi(\alpha) = \beta$.

DEMOSTRACIÓN. (a) ⇒ (b). Existe un isomorfismo $\varphi : \overline{K}/K \longrightarrow \overline{K}/K$ tal que $\varphi(\alpha) = \beta$, para $f(X) = \mathrm{Irr}(\alpha, K)$ tenemos $0 = \varphi(f(\alpha)) = f(\varphi(\alpha)) = f(\beta)$, luego $\mathrm{Irr}(\beta, K) \mid f(X)$, ya que $f(X)$ es mónico irreducible, resulta que $\mathrm{Irr}(\beta, K) = f(X) = \mathrm{Irr}(\alpha, K)$.
(b) ⇒ (c). Si $\mathrm{Irr}(\alpha, K) = f(X) = \mathrm{Irr}(\beta, K)$, entonces existe un isomorfismo η

$$K(\alpha) \xrightarrow{\cong} \frac{K[X]}{(f(X))} \xrightarrow{\cong} K(\beta)$$

$$\alpha \longmapsto X + (f(X)) \longmapsto \beta$$

(c) ⇒ (d). Si existe un isomorfismo $\eta : K(\alpha)/K \longrightarrow K(\beta)/K$ tal que $\eta(\alpha) = \beta$, ya que $K(\beta) \subseteq \overline{K}$, η se prolonga a un homomorfismo $\psi : K(\alpha)/K \longrightarrow \overline{K}/K$, entonces $\psi(\alpha) = \beta$.
(d) ⇒ (a). Si existe $\psi : K(\alpha)/K \longrightarrow \overline{K}/K$ tal que $\psi(\alpha) = \beta$, es posible extender ψ a un homomorfismo $\varphi : \overline{K}/K \longrightarrow \overline{K}/K$, ya que $\overline{K}/K$ es algebraica, resulta que φ es un isomorfismo, luego α y β son K-conjugados. □

Dos notas sobre cardinalidad de conjuntos y cuerpos.

Observación. 2.12.

(1) Si K es un cuerpo finito, entonces K no puede ser algebraicamente cerrado, ya que si K tiene p elementos, todos sus elementos verifican $x^p = x$ (ó equivalentemente $x^{p-1} = 1$), luego el polinomio $X^p - X + 1$ no tiene raíces en K. Como consecuencia todos los cuerpos algebraicamente cerrados tienen cardinal infinito.

(2) Si F/K es una extensión algebraica, entonces conocemos una cota para el cardinal de F, esta es $\text{card}(K[X])\,\text{card}(\mathbb{N})$, ya que F está contenido en la unión de los conjuntos formados por las raíces de todos los polinomios con coeficientes en K. Entonces si $\text{card}(K)$ es finito, tenemos que $\text{card}(K[X]) = \aleph_0 = \text{card}(\mathbb{N})$, luego $\text{card}(F) \leq \aleph_0$. Si $\text{card}(K)$ es infinito, entonces $\text{card}(F) = \text{card}(K)$.

Teorema de Steinitz

Este último resultado nos permite desarrollar una demostración alternativa del Teorema de Steinitz.

Lema. 2.13.
Sea K un cuerpo con cardinal α, y $\beta \geq \alpha$ un cardinal infinito; si F/K una extensión algebraica, entonces $\text{card}(F) \leq \beta$.

DEMOSTRACIÓN. Como $\text{card}(K) \leq \beta$, se tiene $\text{card}(K[X]) \leq \beta$. Por otro lado, como cada polinomio tiene un número finito de raíces, el cardinal del conjunto de cualquier extensión algebraica F/K está acotado por $\beta \cdot \text{card}(\mathbb{N}) = \beta$; esto es, $\text{card}(F) \leq \beta$. □

Teorema. 2.14. (Teorema de Steinitz)
Dado un cuerpo K, existe una extensión algebraica F/K en la que F es algebraicamente cerrado.

DEMOSTRACIÓN. Supongamos que $\text{card}(K) = \alpha$, y sea $\beta > \alpha$ un nuevo cardinal. Consideramos un conjunto C de cardinal 2^β con dos elementos distinguidos: 0 y 1. Para cada cuerpo F con $\text{card}(F) < \beta$ existe una aplicación inyectiva $\nu : F \longrightarrow C$ tal que $\nu(0) = 0$ y $\nu(1) = 1$. A $\text{Im}(\nu)$ podemos dar estructura de cuerpo mediante la biyección $\nu : F \longrightarrow \text{Im}(\nu)$; llamamos a $\text{Im}(\nu)$ un "subcuerpo" de C.

En el conjunto de los subcuerpos de C definimos un orden parcial mediante $F_1 \leq F_2$ si $F_1 \subseteq F_2$ es un homomorfismo de cuerpos y la extensión F_2/F_1 es algebraica. Dada una cadena de subcuerpos $\{F_i \mid i \in \mathbb{I}\}$, con un primer elemento F_0, consideramos $F' = \cup_i F_i$; es claro que F' es un subcuerpo de C, y para cada $x \in F'$ existe $i \in \mathbb{I}$ tal que $x \in F_i$, como tenemos una torre finita de extensiones

algebraicas: $F_0 \subseteq \cdots \subseteq F_n$, se tiene que x es algebraico sobre F_0. Por tanto F'/F_0 es una extensión algebraica. Aplicando el lema de Zorn tenemos que cada subcuerpo F de C está contenido en uno maximal F' tal que la extensión F'/F es algebrica.

En particular, existe un subcuerpo maximal F de C que contiene a K y tal que la extensión F/K es algebraica, por tanto $\text{card}(F) < \beta$, y se tiene $F \subsetneq C$. Falta ver que F es algebraicamente cerrado; si existe $F(\alpha)/F$ algebraica propia, como $\text{card}(F(\alpha)) < \beta$, podemos meter $F(\alpha)$ en C extendiendo a F, y llegaríamos a que F no es maximal, lo que es una contradicción. □

2.1. Ejercicios

Clausura algebraica

Ejercicio. 2.15.
Sea E/K una extensión algebraica tal que para cualquier extensión finita F/K existe un K-homomorfismo $\sigma : F/K \to E/K$. Demuestra que entonces E es una clausura algebraica de K.
Ref.: 4161e_043 SOLUCIÓN

Ejercicio. 2.16.
Sea F/K una extensión algebraica con la propiedad de que cada polinomio no constante con coeficientes en K descompone en F (factoriza en factores lineales). Demuestra que F es un cuerpo algebraicamente cerrado.
Ref.: 4161e_044 SOLUCIÓN

Ejercicio. 2.17.
Demuestra que la clausura algebraica de $\mathbb{Q}$ no es una extensión finita de $\mathbb{Q}$.
Ref.: 4161e_045 SOLUCIÓN

Ejercicio. 2.18.
Prueba que la clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ es numerable.
Ref.: 4161e_078 SOLUCIÓN

Ejercicio. 2.19.
Sea $K \subseteq E \subseteq F$ una torre de cuerpos. Demuestra que F es una clausura algebraica de K si, y sólo si, F es una clausura algebraica de E y E/K es algebraica.
Ref.: 4161e_046 SOLUCIÓN

Ejercicio. 2.20.
Demuestra que existe una clausura algebraica de $\mathbb{Q}(\sqrt{2})$ que lo es también de $\mathbb{Q}(\sqrt{7})$. Deduce que cualquier clausura algebraica de $\mathbb{Q}(\sqrt{2})$ es isomorfa a cualquier clausura algebraica de $\mathbb{Q}(\sqrt{7})$.
Ref.: 4161e_047 SOLUCIÓN

Ejercicio. 2.21.
Demuestra que las extensiones $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{5})$ de $\mathbb{Q}$ tienen clausuras algebraicas isomorfas.
Ref.: 4161e_048 SOLUCIÓN

Ejercicio. 2.22.
Sea $\overline{K}$ una clausura algebraica de K. Demuestra que toda extensión algebraica de K es K–isomorfa a una subextensión de $\overline{K}$.
Ref.: 4161e_049 SOLUCIÓN

Ejercicio. 2.23.
Sea F/K una extensión con F algebraicamente cerrado. Si llamamos

$$E = \{\alpha \in F \mid \alpha \text{ es algebraico sobre } K\},$$

demuestra que E es una clausura algebraica de K.
Ref.: 4161e_060 SOLUCIÓN

Ejercicio. 2.24.
Construir un subcuerpo $K \subsetneq \mathbb{R}$ tal que $\overline{K} = \mathbb{C}$.
Ref.: 4161e_080 SOLUCIÓN

Ejercicio. 2.25.
Prueba que ningún cuerpo algebraicamente cerrado es de cardinal finito.
Ref.: 4161e_079 SOLUCIÓN

Ejercicios propuestos que involucran a capítulos posteriores
Cuerpos finitos.

Ejercicio. 2.26.
Si $K = \mathbb{F}_p = \mathbb{Z}_p$, con $p \in \mathbb{Z}$ primo, y $E/\mathbb{F}_p$ es una clausura algebraica, tenemos varias torres de cuerpos:

$$\mathbb{F}_p \subseteq \cdots \subseteq \mathbb{F}_{p^t} \subseteq \mathbb{F}_{p^s} \subseteq \cdots \subseteq E.$$

(1) Observa que $\mathbb{F}_{p^2} \neq \mathbb{Z}_{p^2}$, ya que el segundo no es un dominio de integridad.
(2) Prueba que si $\mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^s}$, entonces $t|s$.
(3) Utilizando que, salvo isomorfismo, sólo existe un cuerpo con p^n elementos, prueba que $E = \cup_n \mathbb{F}_{p^n}$.

Ref.: 4161e_085 SOLUCIÓN

En una extensión finita F/K de cuerpos finitos, un elemento $\alpha \in F$ es una **raíz primitiva** para la extensión si α genera el grupo multiplicativo $F^\times = F \setminus \{0\}$, en particular $F = K(\alpha)$.

Ejercicio. 2.27.
Encuentra una raíz primitiva β de $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$.
Nota. Observa que $x = [X]$ no es una raíz primitiva, ya que $x^5 = 1$.
Ref.: 4161e_064 SOLUCIÓN

Ejercicio. 2.28.
Sea K una extensión de $\mathbb{F}_2$ de grado $n > 1$, y $f(X) \in \mathbb{F}_2[X]$ un polinomio no constante.

(1) Prueba que si $\alpha \in K$ es una raíz de $f(X)$, entonces $\{\alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \ldots, \alpha^{2^{n-1}}\}$ son raíces de $f(X)$ en K.

(2) *Prueba que, en general,* $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \ldots, \alpha^{2^{n-1}}\}$ *no son todas las raíces de* $f(X)$ *en* K.
(3) *Prueba que si* β *es una raíz primitiva de* K, *que es raíz de* $f(X)$, *entonces el grado de* $f(X)$ *es mayor o gual que* n.

Ref.: 4161e_065 *SOLUCIÓN*

Ejercicio. 2.29.
Si $\sqrt[n]{a}$ *es una raíz del polinomio* $X^n - a$,

(1) *Determina* $\mathrm{Irr}(\sqrt{2}, \mathbb{F}_3)$ *e* $\mathrm{Irr}(\sqrt[4]{2}, \mathbb{F}_3)$.
(2) *Determina* $\mathrm{Irr}(\sqrt{2} + \sqrt[4]{2}, \mathbb{F}_3)$ *e* $\mathrm{Irr}(\sqrt{2} + \sqrt[4]{2}, \mathbb{Q})$.

Ref.: 4161e_096 *SOLUCIÓN*

3. Construcciones con regla y compás

Las construcciones geométricas han sido desde la antigüedad una fuente de problemas amén de una forma amena de entretenerse y pasar el tiempo. Con la regla y el compás es posible construir un gran número de figuras en el plano, por ejemplo todo el mundo recuerda como en la escuela se construían perpendiculares a una recta dada pasando por un punto exterior, se bisecaba un ángulo ó se construía un hexágono regular. (Es conveniente señalar que la regla únicamente sirve para trazar rectas y no para medir.)

La construcción de polígonos regulares de n lados es el problema que mayor atractivo ha tenido. La construcción para $n = 3, 4, 5$ ó 6 es bien conocida; sin embargo, como más adelante veremos, la construcción para $n = 7$ es imposible.

Existen otros problemas relativos a las construcciones con regla y compás, que son también insolubles, y que ya fueron estudiados por los sabios griegos, estos son:

- la trisección del ángulo,
- la duplicación del cubo y
- la cuadratura del círculo.

Todos estos problemas tienen como justificación práctica la medición de tierras, la arquitectura ó simplemente el pasar de forma agradable el tiempo en las largas noches de invierno, y al no encontrar solución con regla y compás se impulsó el desarrollo de nuevas herramientas de dibujo, y también sirvieron para desarrollar la matemática.

El problema que nos ocupa ahora, es el de estudiar la posibilidad o la imposibilidad de hacer ciertas construcciones geométricas con regla y compás; por ejemplo, el determinar si un polígono regular de p lados, con p primo, es construíble con regla y compás[1]. Es de señalar que la importancia de la construcción con regla y compás de polígonos regulares es puramente teórica, ya que en la práctica los errores aportados por los instrumentos junto con el número de operaciones que es necesario realizar hacen que sea impensable la construcción explícita en la mayor parte de los casos.

El problema de las construcciones con regla y compás es el siguiente: dado un conjunto de puntos $X = \{P_1, \ldots, P_n\}$ en el plano euclídeo $\mathbb{E}$, definimos nuevos conjuntos de puntos X_i de forma recursiva mediante;

$$X_1 = X,$$

para un número natural $i \geq 1$; supuesto que tenemos X_i, definimos:

(1) R_i el conjunto de puntos que son intersección de rectas que contienen al menos dos puntos de X_i,

(2) CR_i el conjunto de puntos intersección de rectas que contienen al menos dos puntos de X_i y circunferencias con centro puntos de X_i y radios iguales a segmentos determinados por puntos de X_i,

4161-02.tex

[1] Esto fue hecho por Gauss (a la edad de 19 años), para conmemorar esto en Gottingen existe una estatua en su honor con pedestal en forma de polígono de 17 lados, (17 es el número de lados del primero de los polígonos, con gran número de lados, para los que Gauss descubrió una construcción con regla y compás).

(3) C_i el conjunto de puntos intersección de las circunferencias descritas anteriormente.

Finalmente definimos X_{i+1} como la unión de X_i, R_i, CR_i y C_i.
Un punto $P \in \mathbb{E}$ se llama **construíble** (con regla y compás) a partir de $X = \{P_1, \ldots, P_n\}$ si pertenece al conjunto $C(X) = \cup\{X_i \mid i \in \mathbb{N}\}$.

Formulación algebraica

Para evitar trivialidades consideramos $n \geq 2$, y elegimos un sistema de coordenadas de $\mathbb{E}$ de forma que P_1 y P_2 tengan de coordenadas $(0,0)$ y $(1,0)$ respectivamente. A cada punto $P \in \mathbb{E}$ de coordenadas (x,y) le asociamos el número complejo $x+iy$, y por tanto identificamos el plano $\mathbb{E}$ con el conjunto $\mathbb{C}$ de los números complejos. Así el conjunto $X = \{P_1, \ldots, P_n\}$ se identifica con el conjunto $X = \{z_1, \ldots, z_n\}$ de números complejos, siendo $z_1 = 0$, y $z_2 = 1$. Los números complejos que corresponden a los elementos del conjunto $C(X)$ se llaman, por extensión, **números complejos construíbles** a partir de $z_1, \ldots, z_n$, y lo representamos también por $C(X)$.

Lema. 3.1.
Con las notaciones anteriores, $C(X)$ es el subcuerpo más pequeño de $\mathbb{C}$ que contiene a los números complejos $z_1, \ldots, z_n$, y es cerrado para tomar raíces cuadradas y conjugados.

DEMOSTRACIÓN. $C(X)$ es cerrado para la suma. Si $z, z' \in C(X)$, entonces $z+z'$ se obtiene como la intersección de las circunferencias centradas en z y en z' y de radios los módulos de z' y de z respectivamente, luego $z+z' \in C(X)$.

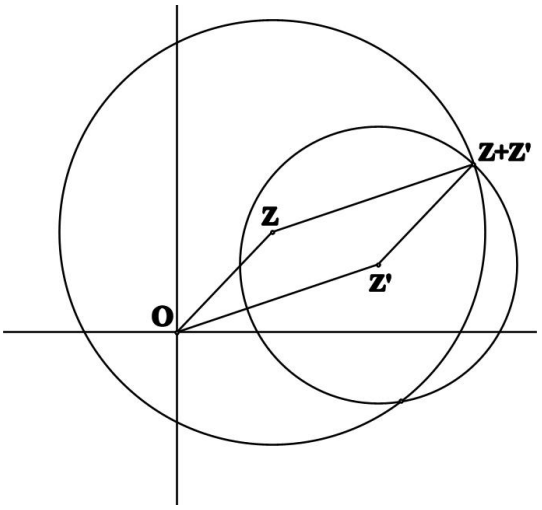


Figura I.1: Suma

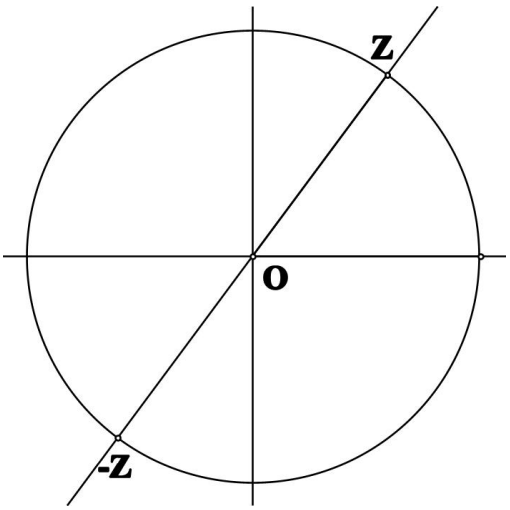


Figura I.2: Opuesto

$C(X)$ es cerrado para tomar opuestos. Si $z \in C(X)$, entonces $-z$ se obtiene como la intersección de la recta que pasa por 0 y z y la circunferencia de radio el módulo de z.

$C(X)$ es cerrado para el producto. Si $z, z' \in C(X)$, entonces escribiéndolos en forma polar tenemos $z = re^{i\theta}$ y $z' = r'e^{i\theta'}$.

(1). Construimos $A \in C(X)$ como la intersección de la circunferencia, centrada en O y de radio el módulo de z, y el eje real.

(2). Construimos B como la intersección de la recta que pasa por 0 y z' con la misma circunferencia.

(3). Construimos C como la intersección de la circunferencia anterior y la circunferencia con centro z y radio el módulo de $B-A$. De esta forma tenemos que el ángulo $\angle AOB$ es igual al ángulo $\angle zOC$, por tanto tenemos que C es un elemento de $C(X)$ de argumento $\theta + \theta'$.

Para comprobar que el producto $zz' \in C(X)$, basta encontrar en $C(X)$ un elemento cuyo módulo sea rr'.

(4). Podemos construir un punto en el eje imaginario el punto ir, y trazar la recta $1, ir$.

(5). Trazamos una paralela a esta recta que pase por el punto r'; esta nueva recta corta al eje imaginario en irr'. Por tanto existe en $C(X)$ un punto cuyo módulo es rr'. Trazamos la circunferencia con centro en 0 y radio rr', su intersección con la recta OC es el punto pedido.

$C(X)$ es cerrado para tomar inversos de elementos no nulos. Si $0 \neq z \in C(X)$, consideramos la circunferencia con centro en 0 y radio el módulo de z; esta circunferencia corta el eje real en r, el módulo de z. Consideramos la circunferencia con centro en r y radio el módulo de $z-r$, la otra intersección con la circunferencia anterior determina un elemento z' de $C(X)$ con argumento $-\theta$. Para ver que podemos construir un elemento de $C(X)$ de módulo r^{-1}, consideramos el punto i y la recta i, r; construimos una recta paralela a ella que pasa por el punto 1; su intersección con el eje imaginario es el punto ir^{-1}; tenemos pues el resultado.

$C(X)$ es cerrado para tomar raíces cuadradas. Sea $z \in C(X)$, si la forma polar de z es $re^{i\theta}$, entonces $1+r$ puede ser construido y también $(1+r)/2$, consideramos la circunferencia con centro $(1+r)/2$

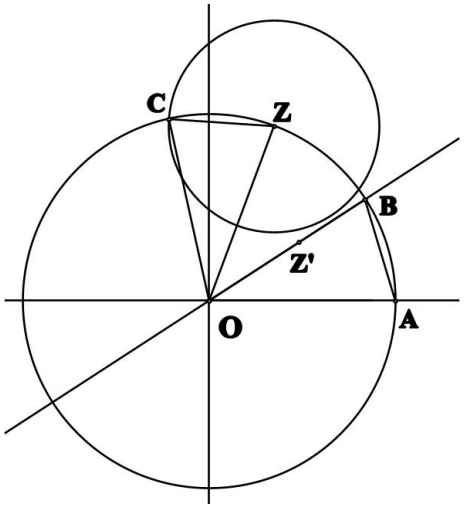


Figura I.3: Argumento

y radio $(1+r)/2$, la intersección de esta circunferencia con la recta paralela al eje imaginario que pasa por el punto 1, determina un punto B, y el módulo de $B-1$ es $\sqrt{r}$. La demostración de este hecho es por semejanza de triángulos. Falta comprobar que podemos construir un elemento de $C(X)$ con argumento $\theta/2$, consideramos $z+r$, tenemos que $z+r$ tiene argumento $\theta/2$.

$C(X)$ es cerrado para tomar conjugados. Si $z \in C(X)$, ya sabemos que existe un elemento de $C(X)$ con argumento $-\theta$, así pues la construcción de $\overline{z}$ es inmediata.

Si K es un subcuerpo de $\mathbb{C}$ que contiene a $z_1, \ldots, z_n$ y es cerrado para tomar raíces cuadradas y conjugados, entonces $-1 \in K$, luego $i = \sqrt{-1} \in K$, y por ser un cuerpo contiene a todos los números complejos de la forma $p+iq$, con $p, q \in \mathbb{Q}$. Una recta que pase por dos puntos de K tiene una ecuación

$$aX + bY + c = 0, \text{ con } a, b, c \in \mathbb{R} \cap K.$$

Una circunferencia con centro un punto de K y radio la distancia entre dos puntos de K, (éste en un número real que pertenece a K), tiene una ecuación

$$X^2 + Y^2 + dX + eY + f = 0, \text{ con } d, e, f \in \mathbb{R} \cap K.$$

Los puntos intersección de dos rectas (de K) tienen coordenadas en $\mathbb{R} \cap K$ (son las soluciones al sistema

$$\begin{cases} a_1X + b_1Y + c_1 = 0 \\ a_2X + b_2Y + c_2 = 0. \end{cases}$$

Los puntos intersección de una recta y una circunferencia (de K) tienen también coordenadas en $\mathbb{R} \cap K$ (son soluciones reales al sistema

$$\begin{cases} X^2 + Y^2 + dX + eY + f = 0 \\ aX + bY + c = 0, \end{cases}$$

que se expresan en función de los coeficientes y raíces cuadradas de los mismos). Los puntos intersección de dos circunferencias (de K) tienen también coordenadas en $\mathbb{R} \cap K$. Entonces, ya que se

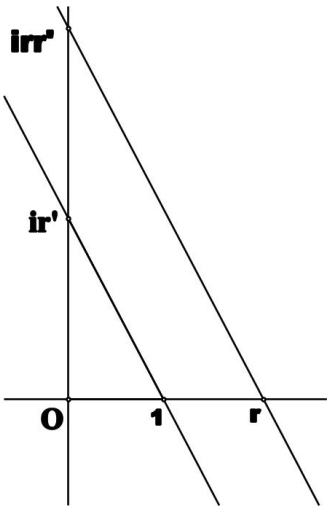


Figura I.4: Módulo

verifica $X \subseteq K$, también $X_i \subseteq K$, $i \in \mathbb{N}$, y por tanto $C(X) \subseteq K$. Como consecuencia $C(X)$ es el menor subcuerpo de $\mathbb{C}$ que contiene a K y es cerrado para raíces cuadradas y conjugados. □

Una propiedad del cuerpo $C(X)$, que se desprende de la demostración, es que $C(X)$ contiene todos los números complejos de la forma $p + iq$, con $p, q \in \mathbb{Q}$, y por tanto $C(X)$ es un subconjunto denso de $\mathbb{C}$, para la topología usual.

Teorema. 3.2.
Si $z_1, \ldots, z_n \in \mathbb{C}$ y llamamos $K = \mathbb{Q}(z_1, \ldots, z_n, \overline{z}_1, \ldots, \overline{z}_n)$, entonces para un número complejo z son equivalentes:

(a) $z \in C(z_1, \ldots, z_n)$;
(b) Existe una torre de cuerpos $K \subseteq K(u_1) \subseteq \cdots \subseteq K(u_1, \ldots, u_r)$ tal que $u_i \in \mathbb{C}$, $1 \leq i \leq r$, $z \in K(u_1, \ldots, u_r)$ y $u_i^2 \in K(u_1, \ldots, u_{i-1})$.

DEMOSTRACIÓN. (a) ⇒ (b). Llamamos H al conjunto de los números complejos que verifican la condición (b). Si $z, z' \in H$ con $z \in K(u_1, \ldots, u_r)$ y $z' \in K(v_1, \ldots, v_s)$, entonces $z + z'$, zz', $z^{-1} \in K(u_1, \ldots, u_r, v_1, \ldots, v_s)$, y tenemos una torre de cuerpos

$$K \subseteq K(u_1) \subseteq \cdots \subseteq K(u_1, \ldots, u_r) \subseteq K(u_1, \ldots, u_r, v_1) \subseteq \cdots \subseteq K(u_1, \ldots, u_r, v_1, \ldots, v_s)$$

que verifica la condición (b). Entonces H es un subcuerpo de $\mathbb{C}$.
Si se verifica que $z \in K(u_1, \ldots, u_r)$, entonces $\sqrt{z} \in K(u_1, \ldots, u_r, \sqrt{z}z)$, y por tanto $\sqrt{z} \in H$.
Es cierto que el conjugado de K es igual a K, y se verifica que el conjugado de $K(u_1, \ldots, u_r)$ es $K(\overline{u}_1, \ldots, \overline{u}_r)$, luego el conjugado de cada elemento de H pertenece a H.

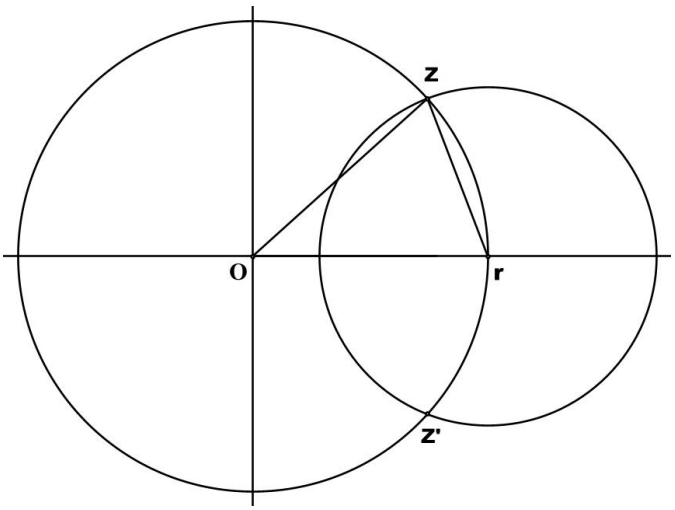


Figura I.5: Argumento

Por tanto H contiene a $C(z_1,\dots,z_n)$; por la minimalidad de este subcuerpo, ya que siempre tenemos $C(z_1,\dots,z_n)\subseteq H$, se verifica $H=C(z_1,\dots,z_n)$.
(b) $\Rightarrow$ (a). Es inmediato que $K=\mathbb{Q}(z_1,\dots,z_n,\overline{z}_1,\dots,\overline{z}_n)\subseteq C(z_1,\dots,z_n)$, y si $z\in K(u_1,\dots,u_r)$ con $u_i^2\in K(u_1,\dots,u_{i-1})$; por inducción tenemos que $u_i\in C(z_1,\dots,z_n)$, y por tanto $z\in K(u_1,\dots,u_r)\subseteq C(z_1,\dots,z_n)$. □

Corolario. 3.3.
Si $z\in C(z_1,\dots,z_n)$, entonces z es algebraico sobre $K=\mathbb{Q}(z_1,\dots,z_n,\overline{z}_1,\dots,\overline{z}_n)$ y su grado es 2^s para algún $s\in\mathbb{N}$.

DEMOSTRACIÓN. Como $z\in C(z_1,\dots,z_n)$, existe una torre $K\subset K(u_1)\subset\cdots\subset K(u_1,\dots,u_r)$, con $u_i\in\mathbb{C}$ y $u_i^2\in K(u_1,\dots,u_{i-1})$, $1\le i\le r$, para la que $z\in K(u_1,\dots,u_r)$, entonces $[K(u_1,\dots,u_r):K]=2^r$, ya que $K\subseteq K(z)\subseteq K(u_1,\dots,u_r)$, tenemos que $[K(z):K]$ es un divisor de 2^r, luego es de la forma 2^s. □

El recíproco de este resultado no es cierto, como más adelante comprobaremos.

Aplicaciones.

Proposición. 3.4.
No es posible dividir un ángulo, arbitrario, en tres ángulos iguales con regla y compás.

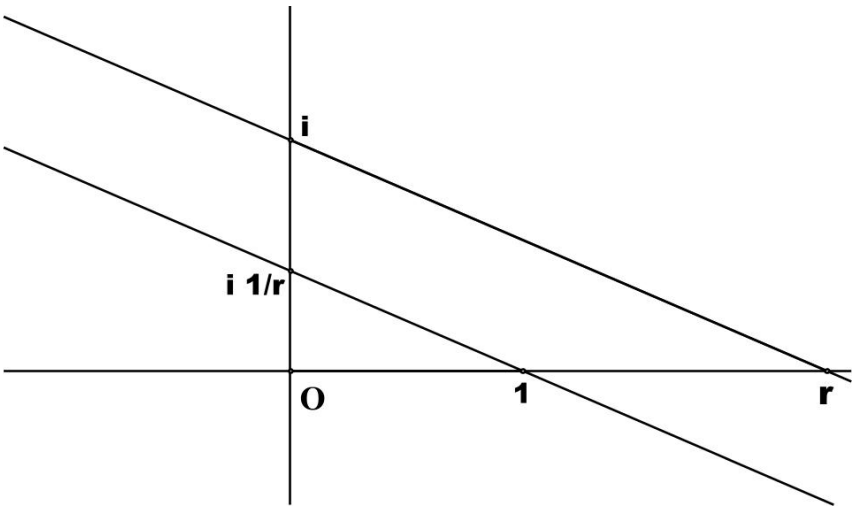


Figura I.6: Módulo

DEMOSTRACIÓN. Consideramos el ángulo de $\theta = 60^o$, ó equivalentemente los puntos del plano complejo $z_0 = 0$, $z_1 = 1$ y $z_2 = \cos(\theta) + i\,\mathrm{sen}(\theta) = 1/2 + i/2$. Dividir θ en tres ángulos iguales es determinar el punto $z_3 = \cos(\theta/3) + i\,\mathrm{sen}(\theta/3)$, y hacerlo con regla y compás es equivalente a que $z_3 \in C(z_0, z_1, z_2)$. Si esto ocurre, entonces las componentes de z_3 también pertenecen a $C(z_0, z_1, z_2)$, y por tanto tienen grado una potencia de dos sobre el cuerpo $K = \mathbb{Q}(z_0, z_1, z_2, \overline{z}_0, \overline{z}_1, \overline{z}_2) = \mathbb{Q}(0, 1, 1/2 + i\sqrt{3}, 1/2 - i\sqrt{3}) = \mathbb{Q}(\sqrt{-3})$, ya que $[K : \mathbb{Q}] = 2$, el grado de las componentes reales de z_3 sobre $\mathbb{Q}$ es también igual a una potencia de 2. Sin embargo de las relaciones

$$\mathrm{sen}(\alpha + \beta) = \mathrm{sen}(\alpha)\cos(\beta) + \cos(\alpha)\,\mathrm{sen}(\beta)$$

y

$$\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \mathrm{sen}(\alpha)\,\mathrm{sen}\,\beta),$$

se obtiene que $\cos(\theta) = 4\cos^3(\theta/3) - 3\cos(\theta/3)$, tenemos la relación

$$1/2 = 4\cos^3(\theta/3) - 3\cos(\theta/3),$$

y por tanto $\cos(\theta/3)$ es raíz del polinomio $4X^3 - 3X - 1/2$, que es irreducible sobre $\mathbb{Q}$, por tanto el polinomio mónico irreducible de $\cos(\theta/3)$ sobre $\mathbb{Q}$ es $4X^3 - 3X - 1/2$, y su grado es igual a 3, que no es una potencia de 2. Tenemos que $\cos(\theta/3)$ no es construíble sobre $\{z_0, z_1, z_2\}$. □

Proposición. 3.5.
No es posible duplicar un cubo, de lado uno, con regla y compás.

DEMOSTRACIÓN. Duplicar el cubo de lado igual a 1 exige construir un segmento de longitud $\sqrt[3]{2}$, ó equivalentemente probar que 2 es construíble sobre el conjunto $\{0, 1\}$, lo que implica que el grado

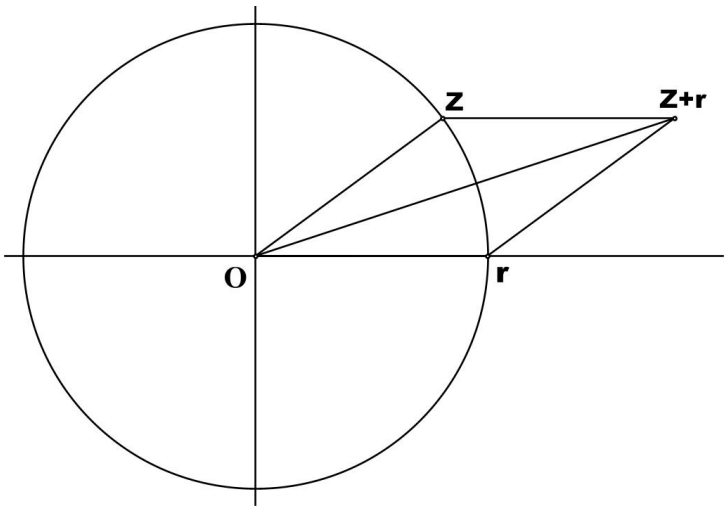


Figura I.7: Argumento

de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ sea una potencia de 2, pero el polinomio X^3-2 es irreducible en $\mathbb{Q}$, y por tanto el grado de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ es igual a 3. □

Proposición. 3.6.
No es posible construir un cuadrado, con regla y compás, con el mismo área que un círculo arbitrario dado.

DEMOSTRACIÓN. Si consideramos el círculo de radio 1, construir un cuadrado con área igual al área del círculo es equivalente a probar que π es un número construíble sobre el conjunto $\{0,1\}$, como consecuencia tiene grado una potencia de 2 sobre $\mathbb{Q}$, en particular es un elemento algebraico sobre $\mathbb{Q}$, pero es bien conocido (Teorema de Lindemann, 1882) que π no es algebraico sobre $\mathbb{Q}$. □

Polígonos regulares.

El otro problema clásico relativo a construcciones con regla y compás es el de la construcción de polígonos regulares. Vamos a estudiar un caso particular, cuando el número de lados es igual a un número primo p. Construir con regla y compás un polígono de p lados es equivalente a construir el número complejo $z=\cos(2\pi/p)+i\,\mathrm{sen}(2\pi/p)$. Este número z verifica $z^p=1$, luego es raíz del polinomio $X^p-1=(X-1)(X^{p-1}+\cdots+X+1)$, entonces z es raíz del polinomio $X^{p-1}+\cdots+X+1$. Este polinomio es irreducible en $\mathbb{Q}$, y por tanto el grado de z sobre $\mathbb{Q}$ es $p-1$. Por los resultados estudiados anteriormente, una condición necesaria para poder construir el polígono de p lados es que $p-1$ sea una potencia de 2, ó equivalentemente que p sea de la forma 2^s+1.

Como consecuencia los polígonos regulares de 7, 11, 13, 19, 23, 29, 31, 37, 39, 41, 43, 47, 49, 51, 53, 59, 61, 67, 71, 73, 79, ...lados no pueden ser construidos con regla y compás. Una condición

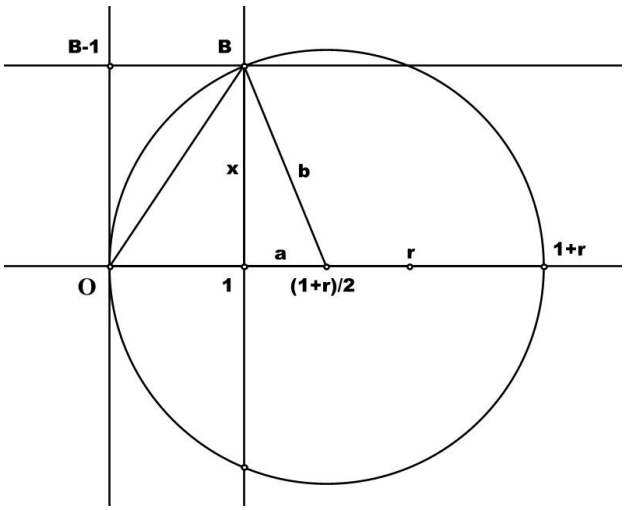


Figura I.8: Módulo

necesaria para que 2^s+1 sea primo es que s sea de la forma 2^t, para algún $t \in \mathbb{N}$, ya que si $s = uv$ con u impar, para cualquier entero positivo impar se verifica

$$X^u + 1 = (X+1)(X^{u-1} - X^{u-2} + \cdots + (-1)^i X^i + \cdots - X + 1),$$

y por tanto 2^s+1 tiene la factorización

$$2^s + 1 = 2^{uv} + 1 = (2^v+1)(2^{(u-1)v} - 2^{(u-2)v} + (-1)^i 2^{iv} + \cdots - 2^v + 1).$$

Entonces los números primos p para los que puede ser posible construir un polígono regular con regla y compás son de la forma $2^{2^t}+1$. Estos primos se llaman **primos de Fermat** porque este matemático los estudió. Fermat conjeturó que para todo $t \geq 0$, $2^{2^t}+1$ es un primo. Esto ocurre para los primeros valores:

t :	0	1	2	3	4
$F_t = 2^{2^t}+1$:	3	5	17	257	65537

Pero el siguiente número $F_5 = 2^{2^5}+1 = 4294967297 = 641 \times 6700417$ no es primo. (La demostración más corta es la siguiente: El número $641 = 5^4 + 2^4 = 5 \times 2^7 + 1$ divide a los dos números siguientes: $a = 5^4 \times 2^{28} + 2^{32}$ y $b = 5^4 \times 2^{28} - 1$ y por tanto divide a su diferencia $a - b = 2^{32} + 1 = F_5$.)

Queda abierta la cuestión de si F_t es primo para algún valor de t mayor que 5. Se ha demostrado que F_t es primo si, y sólo si, F_t divide a $3^{(F_t-1)/2}$. Utilizando este criterio (y efectuando los cálculos por ordenador) se ha demostrado que F_t es compuesto para todo $5 \leq t \leq 22$.

Más adelante, cuando desarrollemos la teoría de Galois, veremos que esta condición también es suficiente. Pero ahora vamos a analizar un poco más esta construcción. Es curioso que históricamente se demostró antes la suficiencia de esta condición que su necesidad. (Teorema de Gauss—Wantzel.)

Si se puede construir un polígono de n lados con regla y compás, es también posible construir polígonos de $2n$, 2^2n, ... lados, ya que con regla y compás podemos hacer la bisección de un ángulo, y también polígonos de m lados, para m un divisor de n. Como consecuencia se pueden construir con regla y compás polígonos regulares de 3, 4, 5, 6, 8 y 10 lados.

Vamos a estudiar la construcción de un polígono regular de 10 lados, y como consecuencia de uno de 5 lados. Consideramos el plano complejo, los puntos 0 y 1, y la circunferencia de radio 1. Sea $z \in \mathbb{C}$ un número complejo tal que el segmento 1, z es un lado del polígono, con centro en z y radio el módulo de $1-z$ construimos una circunferencia, que corta al eje real en el punto 1 y en el punto x. Los triángulos 0, 1, z y z, x, 1 son semejantes, ya que el ángulo $z,0,1$ es de 36^o y los ángulos $0,z,1$ y $z,1,0$ son de 72^o. Así mismo, al ser el triángulo $z,x,1$ isósceles, y ser el ángulo $x,1,z$ de 72^o, tenemos que el ángulo $x,z,1$ es de 36^o, y los triángulos son semejantes como ya habíamos anunciado. Entonces se verifica $\dfrac{1}{x} = \dfrac{x}{1-x}$, que da lugar a la igualdad $x^2+x-1=0$, y que tiene por raíz real positiva a $x = \dfrac{\sqrt{5}-1}{2}$. Entonces x puede ser construido con regla y compás a partir del conjunto $\{0,1\}$.

Como nota histórica, el número x era llamado por los pitagóricos el **número de oro** ó la **razón áurea**. En el Renacimiento se llegó a considerar al rectángulo que tiene x como proporción entre sus lados es el *rectángulo más bello*.

Polígonos regulares de n lados, con n compuesto

Hasta ahora hemos estudiado sólo las construcciones de polígonos regulares de n lados cuando n es primo. El caso general se reduce a éste por las observaciones siguientes:

Si $n = mq$ y el polígono regular de n lados es construíble, y $P_0P_1\cdots P_{n-1}$ son los vértices. El polígono regular de m lados está formado por los vértices $P_0P_q\cdots P_{q(m-1)}$, y por tanto es construíble. Así por ejemplo, el polígono más fácil de construir es el hexágono regular, y el triángulo equilátero se obtiene uniendo los vértices alternos del hexágono (Hay dos de tales triángulos, formando una estrella de David).

Por otra parte, supongamos que $\text{mcd}\{m,n\} = 1$ y que el polígono regular de m lados y el polígono regular de n lados son construíbles. Existen $r,s \in \mathbb{N}$ tales que $sn - rm = 1$ y dividiendo por mn

$$\frac{1}{mn} = \frac{s}{m} - \frac{r}{n}$$

Así que para construir la mn-ésima parte de la circunferencia, tomamos a partir de un punto de la circunferencia s lados del polígono regular de m lados y r lados del polígono regular de n lados. Su diferencia es el lado del polígono regular de mn lados. Euclides en *Elementos* IV.16 procede de manera ligeramente distinta: $\dfrac{1}{15} = \dfrac{1}{2}\left(\dfrac{1}{3} - \dfrac{1}{5}\right)$, así que a partir de un punto A de la circunferencia construye un vértice del pentágono regular B y un vértice del triángulo equilátero, sea C. Biseca el arco BC, sea E el punto medio y cada uno de los segmentos BE y BC es un lado del pentadecágono regular.

Naturalmente, si el polígono regular de m lados es construíble, también lo es el polígono regular de $2m$ lados: Basta bisecar cada uno de los ángulos centrales del polígono regular de m lados, y la bisectriz de un ángulo es construíble con regla y compás.

Estas tres observaciones demuestran la mitad del siguiente teorema:

Teorema. 3.7. (Teorema de Gauss-Wantzel, [17, p. 274])
Un polígono regular de n lados es construíble con regla y compás si, y sólo si, $n = 2^e p_1 \cdots p_s$ *donde* $e \geq 0$ *y los* p_i *son primos de Fermat distintos.*

DEMOSTRACIÓN. Si el polígono regular de n lados es construíble con regla y compás, entonces $\varphi(n)$ es una potencia de dos, por tanto cada factor primo p de n verifica $\varphi(p) = p-1$ es una potencia de dos: es un primo de Fermat. Si el exponente de p en n es e, entonces $p^{e-1}(p-1) = \varphi(p^e) = 2^s$, de donde se deduce que $e = 1$ ó $p = 2$, y por tanto $n = 2^e p_1 \cdots p_s$ donde $e \geq 0$ y los p_i son primos de Fermat distintos.
Si $n = 2^e p_1 \cdots p_s$ donde $e \geq 0$ y los p_i son primos de Fermat distintos, y ξ es una raíz n–ésima primitiva de la unidad, entonces $[\mathbb{Q}(\xi) : Q] = \varphi(n)$ es una potencia de 2, y en consecuencia ξ es un número complejo construíble. □

Construcciones algebraicas explícitas

Hasta finales del siglo XVIII no se conocían más polígonos regulares constructibles que los expuestos en los *Elementos*. Pero el 30 de Marzo de 1796 el joven Gauss (tenía 19 años) escribe en su diario que había hallado "el principio sobre el que se basa la división de la circunferencia y en particular la división de la misma en 17 partes". En otras palabras, había demostrado que el polígono regular de 17 lados es construíble. Posteriormente decía que este descubrimiento le había influido con fuerza para dedicar su vida a las matemáticas.
Vamos a describir directamente la construcción del pentágono y del heptadecágono regular. Como dice Jacob Steiner, haremos nuestras construcciones "simplemente por medio del lenguaje". Es decir, no nos interesa realizar explícitamente las construcciones geométricas más elegantes, sino asegurarnos de que esas construcciones son realmente posibles.
La construcción del pentágono regular equivale a la de la raíz quinta de la unidad $\xi = \cos(2\pi/5) + i\,\mathrm{sen}(2\pi/5)$. Sabemos que ξ es raíz del polinomio $\Phi_5 = X^4+X^3+X^2+X+1$. Sea $\alpha = \xi+\xi^{-1} = \xi+\xi^4$. Un poco de manipulación muestra que α es raíz de $X^2+X-1 \in \mathbb{Q}[X]$ y ξ es raíz de $X^2-\alpha X+1 \in \mathbb{Q}(\alpha)[X]$. Tenemos la torre de extensiones cuadráticas

$$\mathbb{Q}(\xi) \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$$

Por el Teorema (3.7.) ξ es construíble.
En [17, p. 222-223] se describe en detalle la construcción del heptadecágono regular. Resumiéndola, definimos sucesivamente los números

$$\begin{aligned}
\xi &= \cos(2\pi/17) + i\,\mathrm{sen}(2\pi/17)\\
\gamma &= \xi + \xi^{-1} = \xi + \xi^{16}\\
\beta &= \xi + \xi^{-1} + \xi^4 + \xi^{-4}\\
\alpha &= \xi + \xi^{-1} + \xi^4 + \xi^{-4} + \xi^9 + \xi^{-9} + \xi^2 + \xi^{-2}
\end{aligned}$$

y formamos la torre

$$\mathbb{Q}(\xi) \supset \mathbb{Q}(\gamma) \supset \mathbb{Q}(\beta) \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$$

donde cada paso es una extensión cuadrática, ya que se verifican las siguientes ecuaciones cuadráticas:

$$\begin{aligned} \xi^2 - \gamma\xi + 1 &= 0 \\ \gamma^2 - \beta\gamma - (\beta^3 - 6\beta + 3)/2 &= 0 \\ \beta^2 - \alpha\beta - 1 &= 0 \\ \alpha^2 + \alpha - 4 &= 0 \end{aligned}$$

Recientemente se ha publicado una construcción algebraica explícita del polígono regular de 257 lados, donde los cálculos se han realizado con ayuda del programa de ordenador *MAPLE V*.

Construcciones geométricas explícitas. Curiosidades

Cada una de las construcciones algebraicas anteriores se pueden trasladar paso a paso a una construcción geométrica, pero como ya hemos dicho, dicha construcción no será ni la más corta ni la más elegante de todas las posibles. Además de las construcciones expuestas en los *Elementos*, Ptolomeo y Richmond (1893) dieron construcciones del pentágono regular más sencillas que las de Euclides. Richmond (1909) también describe una construcción sencilla del heptadecágono regular.

Richelot y Schwendenwein construyeron en 1832 el polígono regular de 257 lados y J. Hermes invirtió diez años sobre el de 65537 lados; depositó su trabajo en una gran caja que aún se encuentra en la Universidad de Gottingen.

3.1. Ejercicios

Construcciones con regla y compás

Ejercicio. 3.8.
Demuestra que $u = \sqrt{1+\sqrt{2}-\sqrt{3}} + \sqrt[4]{5+\sqrt{6}}$ *es un número construible.*
Ref.: 4161e_034 SOLUCIÓN

Ejercicio. 3.9.
Demuestra la imposibilidad de construir con regla y compás:
(1) Un ángulo de $1°$.
(2) Un 9-gono regular.
(3) La trisección de un ángulo cuyo coseno sea 2/3.
(4) El radio de una esfera cuyo volumen sea la suma de los volúmenes de dos esferas de radios construibles.
(5) Un triángulo isósceles dados su perímetro y su área.

Ref.: 4161e_035 SOLUCIÓN

Ejercicio. 3.10.
Determina los enteros $n \in \mathbb{N}$ *tales que el ángulo de* n *grados es construible con regla y compás.*
Ref.: 4161e_036 SOLUCIÓN

Ejercicio. 3.11.
Sea θ *un ángulo tal que* $\cos(\theta) = 11/16$. *Demuestra que* θ *sí puede trisecarse con regla y compás.*
Ref.: 4161e_037 SOLUCIÓN

Ejercicio. 3.12.
Encuentra un ángulo α que no pueda construirse con regla y compás, pero que, supuesto que está construido, sí pueda trisecarse con regla y compás.
Ref.: 4161e_038 SOLUCIÓN

Ejercicio. 3.13.
Sean n y m enteros positivos y $M = \mathrm{mcm}\{n,m\}$, demuestra que los polígonos regulares de n y m lados son construíbles con regla y compás si, y sólo si, lo es el de M lados.
Ref.: 4161e_039 SOLUCIÓN

Ejercicio. 3.14.
¿Es posible construir con regla y compás el radio de un círculo cuyo área sea igual a la suma de las áreas de dos círculos de radios conocidos?
Ref.: 4161e_040 SOLUCIÓN

Ejercicio. 3.15.
¿Es posible "cuadrar el triángulo"? (Es decir, dado un triángulo arbitrario, ¿es posible construir con regla y compás el lado de un cuadrado que tenga la misma área?)
Ref.: 4161e_042 SOLUCIÓN

Ejercicio. 3.16.
Sea $F/\mathbb{R}$ una extensión de cuerpos y P,S dos puntos del plano euclídeo cuyas coordenadas pertenecen a F. Demostrar que:
(1) La línea recta que pasa por P y S tiene una ecuación de la forma $aX+bY+c=0$ con $a,b,c \in F$.
(2) La circunferencia con centro P y radio el segmento PS tiene una ecuación de la forma $X^2+Y^2+aX+bY+c=0$, con $a,b,c \in F$.

Ref.: 4161e_076 SOLUCIÓN

Ejercicio. 3.17.
Sean c y d números reales construibles. Demostrar que:

(1) $c+d$ y $c-d$ son construibles.
(2) Si $d \neq 0$, entonces c/d es construible.
(3) cd es construible.
(4) Los números reales construibles forman un subcuerpo de $\mathbb{R}$.
(5) Si c es construible, entonces también lo es $\sqrt{c}$.

Ref.: 4161e_077 SOLUCIÓN

4. La cúbica y Tartaglia

Polinomios cuadráticos

Vamos a trabajar con polinomios $f(X) \in K[X]$, con coeficientes en un cuerpo, y sus raíces. Veamos el caso en el que $K = \mathbb{Q}$.
A la hora de calcular las raíces de $f(X) \in \mathbb{Q}[X]$, si $f(X)$ es de grado dos, conocemos un procedimiento que nos da explícitamente las mismas. Sea, por ejemplo, $f(X) = X^2 + bX + c$; en este caso las raíces de $f(X)$ son

$$\alpha_1 = \frac{-b + \sqrt{-b^2 - 4c}}{2} \text{ y } \alpha_2 = \frac{-b - \sqrt{-b^2 - 4c}}{2}.$$

Una forma de llegar a esta fórmula es mediante el método de completación de cuadrados.

$$X^2 + bX + c = X^2 + 2\tfrac{b}{2}X + \left(\tfrac{b}{2}\right)^2 - \left(\tfrac{b}{2}\right)^2 + c$$

$$= (X + \tfrac{b}{2})^2 - (\tfrac{b}{2} - 4c).$$

Si α es una raíz, se tiene $\alpha = -\frac{b}{2} \pm \sqrt{\left(\frac{b}{2} - 4c\right)} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$.

Polinomios cúbicos

En el caso de polinomios de grado tres podemos seguir un método similar. Dado $f(X) = X^3 + bX^2 + cX + d \in \mathbb{Q}[X]$, desarrollando por Taylor en $a \in \mathbb{Q}$, resulta

$$f(X) = f(a) + Df(a)(X - a) + \frac{D^2 f(a)}{2!}(X - a)^2 + \frac{D^3 f(a)}{3!}(X - a)^3.$$

Si tomamos a tal que $D^2 f(a) = 0$, tendremos un nuevo polinomio en el que el coeficiente de X^2 es nulo. Este cambio podemos hacerlo, si $b \neq 0$, directamente mediante $X \mapsto Y - \frac{b}{3}$. En este caso se tiene

$$\begin{aligned} X^3 + bX^2 + cX + d &= \left(Y - \tfrac{b}{3}\right)^3 + b\left(Y - \tfrac{b}{3}\right)^2 + c\left(Y - \tfrac{b}{3}\right) + d \\ &= Y^3 + \left(c - \tfrac{b^2}{3}\right)Y + \tfrac{1}{27}\left(2b^3 - 9bc + 27d\right) \\ &= Y^3 + pY + q. \end{aligned}$$

en donde $p = \frac{1}{3}\left(3c - b^2\right)$, y $q = \frac{1}{27}\left(2b^3 - 9bc + 27d\right)$.
Hemos reducido el problema a considerar un polinomio de grado tres de la forma $X^3 + pX + q \in \mathbb{Q}[X]$. Supongamos que $X = u + v$; desarrollando se tiene

$$X^3 + pX + q = (u + v)^3 + p(u + v) + q = u^3 + 3uv(u + v) + v^3 + p(u + v) + q.$$

4161-04.tex

Como consecuencia $u^3+v^3+q=0$ y $3uv+p=0$, y por tanto $u^3v^3=-\left(\frac{p}{3}\right)^3$. Entonces u^3 y v^3 son raíces del polinomio de grado dos $X^2+qX-\left(\frac{p}{3}\right)^3$, y se tiene:

$$u^3=\frac{-q+\sqrt{\Delta^2}}{2} \quad \text{y} \quad v^3=\frac{-q-\sqrt{\Delta^2}}{2}.$$

Donde Δ^2 es el **discriminante** del polinomio de grado dos anterior, esto es, $\Delta^2=q^2+4\left(\frac{p}{3}\right)^3$.
Caso 1: $\Delta^2=0$.
Si $\Delta^2=0$, $q^2=-4\left(\frac{p}{3}\right)^3$, entonces $u^3=\frac{-q}{2}=v^3$. Si $u=\sqrt[3]{\frac{-q}{2}}$, es real, como $uv=\frac{-p}{3}$, entonces v también es real, luego $v=u$. Si u es complejo no real, sea $u=\omega\sqrt[3]{\frac{-q}{2}}$, entonces v es complejo no real, y es de la forma $\omega^2\sqrt[3]{\frac{-q}{2}}$. Las raíces del polinomio de grado tres son:

$$\begin{aligned}
\alpha_1&=\sqrt[3]{\tfrac{-q}{2}}+\sqrt[3]{\tfrac{-q}{2}}=2\sqrt[3]{\tfrac{-q}{2}}=2\sqrt{\tfrac{-p}{3}},\\
\alpha_2&=\omega\sqrt[3]{\tfrac{-q}{2}}+\omega^2\sqrt[3]{\tfrac{-q}{2}}=-\sqrt[3]{\tfrac{-q}{2}}=\sqrt{\tfrac{-p}{3}},\\
\alpha_3&=\omega^2\sqrt[3]{\tfrac{-q}{2}}+\omega\sqrt[3]{\tfrac{-q}{2}}=-\sqrt[3]{\tfrac{-q}{2}}=\sqrt{\tfrac{-p}{3}}.
\end{aligned}$$

Como $\frac{3q^2}{2p^2}=\frac{-p}{3}$, la anterior expresión es:

$$\begin{aligned}
\alpha_1&=\tfrac{3q}{p},\\
\alpha_2&=\tfrac{-3q}{2p},\\
\alpha_3&=\tfrac{-3q}{2p}.
\end{aligned}$$

Tenemos que el polinomio tiene tres raíces reales: una simple y otra doble.
Caso 2: $\Delta^2>0$.
Si $\Delta^2>0$, consideramos $u=\sqrt[3]{\frac{-q+\sqrt{\Delta^2}}{2}}$ real, y por tanto $v=\sqrt[3]{\frac{-q-\sqrt{\Delta^2}}{2}}$, ya que se tiene

$$uv=\sqrt[3]{\frac{-q+\sqrt{\Delta^2}}{2}}\sqrt[3]{\frac{-q-\sqrt{\Delta^2}}{2}}=\sqrt[3]{\left(\frac{-p}{3}\right)^3}=\frac{-p}{3}.$$

Si tomamos la raíz cúbica $\omega^h\sqrt[3]{\frac{-q+\sqrt{\Delta^2}}{2}}$, entonces la componente v es de la forma $\omega^k\sqrt[3]{\frac{-q-\sqrt{\Delta^2}}{2}}$, y se verifica

$$\frac{-p}{3}=\omega^h\sqrt[3]{\frac{-q+\sqrt{\Delta^2}}{2}}\,\omega^k\sqrt[3]{\frac{-q-\sqrt{\Delta^2}}{2}}=\omega^{h+k}\frac{-p}{3},$$

de donde $h+k\equiv 0 \pmod 3$. Como consecuencia las raíces del polinomio de grado tres son:

$$\begin{aligned}
\alpha_1&=\sqrt[3]{\tfrac{-q+\sqrt{\Delta^2}}{2}}+\sqrt[3]{\tfrac{-q-\sqrt{\Delta^2}}{2}},\\
\alpha_2&=\omega\sqrt[3]{\tfrac{-q+\sqrt{\Delta^2}}{2}}+\omega^2\sqrt[3]{\tfrac{-q-\sqrt{\Delta^2}}{2}},\\
\alpha_3&=\omega^2\sqrt[3]{\tfrac{-q+\sqrt{\Delta^2}}{2}}+\omega\sqrt[3]{\tfrac{-q-\sqrt{\Delta^2}}{2}}.
\end{aligned}$$

Tenemos una raíz real, α_1, y dos complejas no reales, α_2 y α_3.

Caso 3 $\Delta^2 < 0$.

Si $\Delta^2 < 0$, entonces $u = \sqrt[3]{\frac{-q+\sqrt{\Delta^2}}{2}}$ es complejo no real, y v es también complejo no real por ser $uv = \frac{-p}{3}$. Tenemos entonces $v = \frac{-p}{3|u|^2}\overline{u}$, siendo $\frac{-p}{3|u|^2} \in \mathbb{R}$. Por otro lado, una de las raíces es real, sea $u+v \in \mathbb{R}$, entonces $u+v = u + \frac{-p}{3|u|^2}\overline{u} \in \mathbb{R}$, y se tiene $\frac{-p}{3|u|^2} = 1$; en particular $v = \overline{u}$. Una de las raíces es $u+\overline{u}$. El resto de las raíces se obtienen como $\omega^h u + \omega^k \overline{u}$, y por ser $\omega^h u + \omega^k \overline{u} = \frac{-p}{3} = u\overline{u}$, con $0 \le h, k < 3$, entonces $h + k \equiv 0 \pmod 3$. Las raíces son

$$\begin{aligned} \alpha_1 &= u + \overline{u}, \\ \alpha_2 &= \omega u + \omega^2 \overline{u} = \omega u + \overline{\omega u}, \\ \alpha_3 &= \omega^2 u + \omega \overline{u} = \omega^2 u + \overline{\omega^2 u}. \end{aligned}$$

En este caso las tres raíces son reales, ya que cada una es una suma de un número complejo y su conjugado.

Es importante señalar, en este caso, que de los seis valores: u, ωu, $\omega^2 u$, $\overline{u}$, $\omega\overline{u}$, $\omega^2\overline{u}$, solo hay tres parejas (los conjugados) cuya suma es un número real, y éstas son las raíces del polinomio.

Polinomios de grado mayor

El siguiente paso es encontrar fórmulas que permitan calcular las raíces de un polinomio de grado cuatro. El método ideado por Ferrari consiste en reducir a un polinomio de grado tres, calculando sus raíces y construyendo las raíces del polinomio original. Más adelante vernos un método diferente.

El caso de grado dos se debe a matemáticos de la antigüedad: babilonios, griegos, etc. El caso de grado tres se debe a Tartaglia, y la fórmula encontrada se llama la **fórmula de Cardano**. El caso de grado cuatro se debe a Ferrari, discípulo de Cardano.

Para polinomios de grado cinco no conocemos una fórmula que nos dé las raíces en función de los coeficientes del polinomio, y a esto se dedicaron los esfuerzos de los matemáticos en los siglos XVI, XVII y XVIII. La solución final del problema pasa, como ya hemos comentado, por determinar propiedades de las raíces y no por dar fórmulas explícitas, en términos de radicales, de las mismas; formulas que, por otro lado, vamos a probar que no existen en el caso general.

La cuártica

Dado un polinomio $f(X) = X^4 + bX^3 + cX^2 + dX + e \in \mathbb{Q}[X]$, vamos a hallar sus raices mediante el uso de radicales de los coeficientes. Primero reducimos a un polinomio del tipo $X^4 + pXr + qX + r \in \mathbb{Q}[X]$. Para hacer esto simplemente hacemos el desarrollo de Taylor de $f(X)$ en un punto $a \in \mathbb{Q}$:

$$f(X) = f(a) + \frac{Df(a)}{1}(X-a) + \frac{D^2 f(a)}{2}(X-a) + \frac{D^3 f(a)}{3!}(X-a)^3 + \frac{D^4 f(a)}{4!}(X-a)^4,$$

y elegimos a de forma que $D^3 f(a) = 0$, por tanto a será una raíz del polinomio $D^3 f(X) = 24X + 6b$, esto es, $a = \frac{-b}{4}$. Si hacemos el cambio $X \mapsto Y + \frac{b}{4}$, obtenemos un polinomio, en Y, con el coeficiente de grado 3 igual a cero. Podemos suponer entonces que $f(X) = X^4 + pX^2 + qX + r$.
A continuación vamos a expresar $f(X)$ como una diferencia de cuadrados. Para ello escribimos:

$$f(X) = X^4 + pX^2 + qX + r = (X^2 + \frac{p}{2} + a)^2 - \left(2aX^2 - qX + (a^2 + pa + \frac{p^2}{4} - r)\right)$$

Tomamos a de forma que $2aX^2 - qX + (a^2 + pa + \frac{p^2}{4} - r)$ sea un cuadrado; esto ocurre si el discriminate del polinomio $2aX^2 - qX + (a^2 + pa + \frac{p^2}{4} - r)$ es igual a cero, esto es, si

$$q^2 + 4 \times 2a(a^2 + pa + \frac{p^2}{4} - r) = 0;$$

como es un polinomio en a de grado 3, basta tomar a como una de sus raíces reales. A continuación observamos que, fijado a en ese valor, el polinomio $2aX^2 - qX + (a^2 + pa + \frac{p^2}{4} - r)$ tiene una raíz doble, y ésta es: $\alpha = \frac{q}{4a}$.
Como consecuencia, se tiene:

$$f(X) = \left(X^2 + \frac{p}{2} + a\right)^2 - 2a\left(X - \frac{q}{4a}\right)^2.$$

por tanto es la suma por la diferencia, esto es,

$$f(X) = \left(X^2 + \frac{p}{2} + a + \sqrt{2a}(X - \frac{q}{4a})\right)\left(X^2 + \frac{p}{2} + a - \sqrt{2a}(X - \frac{q}{4a})\right).$$

Para calcular las raíces de $f(X)$ basta calcular las raíces de estos dos polinomios cuadráticos en el cuerpo $\mathbb{Q}(\sqrt{2}\sqrt{a})$.

4.1. Cuestiones

En las siguientes cuestiones responde "VERDADERO" ó "FALSO" y haz un breve razonamiento para justificar la respuesta.

(1) ☐ El conjunto de los elementos no nulos de un cuerpo es un grupo cíclico para el producto. (Ref.: 4161q_001)

(2) ☐ Todo cuerpo infinito tiene característica cero. (Ref.: 4161q_002)

(3) ☐ El polígono regular de 9 lados es construible con regla y compás. (Ref.: 4161q_003)

(4) ☐ Sea F/K una extensión finita de cuerpos y $\alpha, \beta \in F$; si $[K(\alpha) : K] = a$ y $[K(\beta) : K] = b$ en enteros primos relativos, entonces $[K(\alpha, \beta) : K] = ab$. (Ref.: 4161q_004)

(5) ☐ Si t es un elemento trascendente sobre un cuerpo K, entonces $t+1$ es también trascendente sobre K. (Ref.: 4161q_005)

(6) ☐ Para toda extensión F/K y $\alpha, \beta \in F$,elementos arbitrarios siempre existe un automorfismo $\varphi \in \mathrm{Aut}(F/K)$ tal que $\varphi(\alpha) = \beta$. (Ref.: 4161q_006)

(7) ☐ $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt{5})$ son $\mathbb{Q}$–espacios vectoriales isomorfos, pero no son cuerpos isomorfos. (Ref.: 4161q_007)

(8) ☐ Para toda extensión F/K y para todo $\varphi \in \mathrm{Aut}(F/K)$ el conjunto $F^{\varphi} = \{x \in F \mid \varphi(x) = x\}$ es un cuerpo. (Ref.: 4161q_008)

(9) ☐ Para todo entero primo positivo p existe un torre de cuerpos $\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq F_{p^3} \subseteq \cdots$ (Ref.: 4161q_009)

(10) ☐ Si F es un cuerpo en el que todo polinomio de grado dos es reducible, entonces F es un cuerpo algebraicamente cerrado. (Ref.: 4161q_010)

(11) ☐ Sea K un cuerpo y α, β elementos algebraicos sobre K. Si $K(\alpha)/K \cong K(\beta)/K$, entonces $\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$. (Ref.: 4161q_011)

(12) ☐ Si K es un cuerpo de característica cero en el que todo polinomio de grado mayor ó igual que 3 es reducible, entonces la extensión $\overline{K}/K$ es siempre de grado 1 ó 2. (Ref.: 4161q_012)

(13) ☐ Toda extensión finita de un cuerpo es una extensión algebraica. (Ref.: 4161q_013)

(14) ☐ Toda extensión algebraica de un cuerpo es una extensión finita. (Ref.: 4161q_014)

(15) ☐ Si $K \subseteq F \subseteq E$ es una torre de cuerpos y E/K es finita, entonces F/K es finita. (Ref.: 4161q_015)

4161-99.tex

(16) ☐ Algunos ángulos se pueden trisecar con regla y compás. (Ref.: 4161q_016)

(17) ☐ La clausura algebraica de $\mathbb{Q}$ es $\mathbb{C}$. (Ref.: 4161q_018)

(18) ☐ Ningún cuerpo finito es algebraicamente cerrado. (Ref.: 4161q_019)

Capítulo II

Extensiones de Galois finitas

Introducción

Vamos a fijar el tipo de extensiones que serán objeto de nuestro estudios; éstas son las extensiones finitas que son normales y separables, a las que llamaremos extensiones de Galois.

Una extensión F/K es **normal** si F es el cuerpo de descomposición de un polinomio $f(X) \in K[X]$; la propiedad importante de este tipo de extensiones es que si $g(X) \in K[X]$ un polinomio que tiene una raíz en F, entonces $g(X)$ descompone completamente en F. Las extensiones separables F/K se caracterizan por ser invariantes por automorfismos de clausuras algebraicas de K. Otra propiedad importante es que para cada extension intermedia $K \subseteq E \subseteq F$ todo homomorfismo $\sigma : E/K \longrightarrow F/K$ se puede extender a un automorfismo de F/K.

5. Cuerpos de descomposición. Extensiones normales

Sea K un cuerpo y E/K una extensión de cuerpos. Un polinomio $f(X) \in K[X]$ **descompone** en E si en $E[X]$ se factoriza como un producto de polinomios lineales, esto es;

$$f(X) = a(X-\alpha_1)\cdots(X-\alpha_n), \text{ con } a \in K \text{ y } \alpha_1,\ldots,\alpha_n \in E.$$

Llamamos **cuerpo de descomposición** de $f(X)$ sobre K a un cuerpo E extensión de K en el que $f(X)$ descompone, y verifica la propiedad de que $f(X)$ no descompone en ningún subcuerpo intermedio F, tal que $K \subseteq F \subseteq E$.

Consecuencias inmediatas de la definición son:

(1) Si E es un cuerpo de descomposición de $f(X) \in K[X]$, entonces $E = K(\alpha_1,\ldots,\alpha_n)$, donde $\alpha_1,\ldots,\alpha_n$ son las raíces de $f(X)$. Entonces E/K es una extensión finita, y su grado está acotado por $n!$, donde n es el grado de $f(X)$.

(2) Todo polinomio $f(X) \in K[X]$ tiene un cuerpo de descomposición sobre K. Para probar esto basta considerar una clausura algebraica $\overline{K}$ de K, la descomposición de $f(X)$ en $\overline{K}$: $f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ y definir $E = K(\alpha_1,\ldots,\alpha_n)$. Evidentemente E es un cuerpo de descomposición de $f(X)$ sobre K.

Lema. 5.1.
Sea K un cuerpo, $f(X) \in K[X]$ un polinomio y E_1/K, E_2/K dos cuerpos de descomposición de $f(X)$ sobre K, entonces existe un isomorfismo $\sigma : E_1/K \longrightarrow E_2/K$.

Para cada elemento $a \in E_1$, escribimos a^σ para representar a $\sigma(a)$, su imagen por σ; y de forma similar, escribimos E_1^σ para representar a $\sigma(E_1)$.

DEMOSTRACIÓN. Llamamos $\overline{K}$ a una clausura algebraica de E_2, entonces $\overline{K}$ es también una clausura algebraica de K, ya que E_2/K es una extensión finita. Existe pues un homomorfismo $\sigma : E_1/K \longrightarrow \overline{K}/K$. Si la factorización de $f(X)$ en E_1 es $f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$, y la factorización en E_2/K es $f(X) = a(X-\beta_1)\cdots(X-\beta_n)$, entonces $p^\sigma(X) = f(X)$ implica que los conjuntos $\{\beta_1,\ldots,\beta_n\}$ y $\{\alpha_1^\sigma,\ldots,\alpha_n^\sigma\}$ son iguales. Entonces $E_1^\sigma = K(\alpha_1^\sigma,\ldots,\alpha_n^\sigma)$. Pero E_2 es un cuerpo de descomposición de $f(X)$ sobre K y está contenido en $\overline{K}$, luego la factorización de $f(X)$ en $\overline{K}$ es también la factorización de $f(X)$ en E_2, y por tanto tenemos

$$f(X) = a(X-\alpha_1^\sigma)\cdots(X-\alpha_n^\sigma) \in E_2[X],$$

lo que implica que $\alpha_1^\sigma,\ldots,\alpha_n^\sigma \in E_2$. Como consecuencia $E_1^\sigma \subseteq E_2$, y ya que $E_2 = K(\alpha_1^\sigma,\ldots,\alpha_n^\sigma)$, tenemos que $E_1^\sigma = E_2$. □

4162-01.tex

Sea K un cuerpo, una extensión E/K se llama **normal** si E es el cuerpo de descomposición de un polinomio $f(X) \in K[X]$.

Es de destacar que las extensiones normales no son una **clase distinguida** de extensiones, ya que si $K \subseteq F \subseteq E$ es una torre de cuerpos y E/K es una extensión normal, no necesariamente F/K es una extensión normal. Un ejemplo de que esto es así lo proporciona el polinomio $f(X) = X^5 - 2 \in \mathbb{Q}[X]$. Su cuerpo de descomposición es $\mathbb{Q}(\sqrt[5]{2}, \xi)$, donde ξ es una raíz quinta de la unidad distinta de 1. Si tomamos $K = \mathbb{Q}$ y $E = \mathbb{Q}(\sqrt[5]{2}, \xi)$, entonces E/K es una extensión normal. Sin embargo, el cuerpo intermedio $F = \mathbb{Q}(\sqrt[5]{2})$ no es normal sobre K.

Ocurre sin embargo que si $K \subseteq F \subseteq E$ es una torre de cuerpos y E/K es una extensión normal, entonces E/F también lo es.

Las extensiones normales pueden ser fácilmente caracterizadas mediante las condiciones equivalentes siguientes:

Teorema. 5.2.
Sea K un cuerpo y E/K una extensión finita, son equivalentes:

(a) E/K es una extensión normal.
(b) Para cada $\sigma : E/K \longrightarrow \overline{K}/K$, donde $\overline{K}$ es una clausura algebraica de K que contiene a E, se tiene $E^\sigma = E$.
(c) Todo polinomio irreducible $f(X) \in K[X]$ con una raíz en E descompone en E.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Supongamos que E es el cuerpo de descomposición sobre K de un polinomio $g(X) \in K[X]$, entonces $E = K(\alpha_1, \ldots, \alpha_n)$, donde $\alpha_1, \ldots, \alpha_n$ son las raíces de $g(X)$. Si $\overline{K}$ es una clausura algebraica de E, entonces para cualquier homomorfismo $\sigma : E/K \longrightarrow \overline{K}/K$ tenemos que α_i^σ es raíz de $g(X)$ en $\overline{K}$, y por tanto $\alpha_i^\sigma \in \{\alpha_1, \ldots, \alpha_n\}$, entonces $\{\alpha_1, \ldots, \alpha_n\} = \{\alpha_1^\sigma, \ldots, \alpha_n^\sigma\}$, y por tanto $E^\sigma = E$.

(b) $\Rightarrow$ (c). Supongamos que $f(X) \in K[X]$ tiene una raíz en E, y que las raíces de $f(X)$ en $\overline{K}$ son $\beta_1, \ldots, \beta_m$, con $\beta_1 \in E$. Definimos $\sigma : K(\beta_1)/K \longrightarrow K(\beta_i)/K$, $1 \leq i \leq m$, mediante $\sigma(\beta_1) = \beta_i$. Componiendo con la inclusión, tenemos un homomorfismo $\sigma : K(\beta_1)/K \longrightarrow \overline{K}/K$, y podemos extender σ a un homomorfismo $\overline{\sigma} : E/K \longrightarrow \overline{K}/K$. Aplicando que E/K es una extensión normal, se verifica $E^{\overline{\sigma}} = E$, y por tanto $\beta_i = \sigma(\beta_1) = \overline{\sigma}(\beta_1) \in \overline{\sigma}(E) = E$.

(c) $\Rightarrow$ (a). Por ser F/K finita, supongamos que $E = K(\alpha_1, \ldots, \alpha_n)$. Para cada α_i, $1 \leq i \leq n$, llamamos $g_i(X) = \mathrm{Irr}(\alpha_i, K)$, y $g(X) = g_1(X) \cdots g_n(X)$. Ya que cada $g_i(X)$ es irreducible y tiene una raíz en E, resulta que $g_i(X)$ se descompone en E, luego $g(X)$ descompone en E y no existe ningún cuerpo intermedio propio en el que descomponga, por tanto E es el cuerpo de descomposición de $g(X)$ sobre K. □

La propiedad (b) se puede también enunciar de la siguiente forma:

Para cada $\sigma : \overline{K}/K \longrightarrow \overline{K}/K$, donde $\overline{K}$ es una clausura algebraica de K que contiene a E, se tiene $E^\sigma = E$.

Las siguientes son propiedades inmediatas que verifican las extensiones normales:

Lema. 5.3.
Sean $K \subseteq E \subseteq L$ y $K \subseteq F \subseteq L$ dos torres de cuerpos con E/K y F/K extensiones finitas. Se verifica:
(1) Si E/K y F/K son extensiones normales, entonces EF/K también lo es.
(2) Si E/K y F/K son extensiones normales, entonces $E \cap F/K$ también lo es.
(3) Si E/K es una extensión normal, entonces EF/F también lo es.

DEMOSTRACIÓN. Consideramos una clausura algebraica de K que contenga a E y a F.
(1). Sea $\sigma : EF/K \longrightarrow \overline{K}/K$ un homomorfismo, entonces $\sigma_{|E} : E/K \longrightarrow \overline{K}/K$ y $\sigma_{|F} : F/K \longrightarrow \overline{K}/K$, por tanto $E^\sigma = E$ y $F^\sigma = F$, entonces $(EF)^\sigma = E^\sigma F^\sigma = EF$.
(2). Sean $\sigma : E \cap F/K \longrightarrow \overline{K}/K$ un homomorfismo, entonces extendemos σ hasta $\overline{K}$, obteniendo un homomorfismo $\overline{\sigma} : \overline{K}/K \longrightarrow \overline{K}/K$, entonces $E^{\overline{\sigma}} = E$ y $F^{\overline{\sigma}} = F$, y es claro que $(E \cap F)^\sigma = (E \cap F)^{\overline{\sigma}} \subseteq E^{\overline{\sigma}} \cap F^{\overline{\sigma}}$. Por otro lado, si $y \in E^{\overline{\sigma}} \cap F^{\overline{\sigma}}$, existen $e \in E$ y $f \in F$ tales que $\overline{\sigma}(e) = y = \overline{\sigma}(f)$, por ser $\overline{\sigma}$ inyectiva se tiene $e = f \in E \cap F$, luego $y \in (E \cap F)^{\overline{\sigma}} = (E \cap F)^\sigma$.
(3). Supongamos que $\sigma : EF/F \longrightarrow \overline{K}/F$, entonces σ también es un homomorfismo sobre K, y por tanto $E^\sigma = E$, de donde $(EF)^\sigma = E^\sigma F^\sigma = EF$. □

Lema. 5.4.
Sea $K \subseteq F \subseteq E$ una torre de extensiones finitas con E/K una extensión normal, entonces todo homomorfismo $\sigma : F/K \longrightarrow E/K$ se puede extender a un automorfismo $\overline{\sigma} : E/K \longrightarrow E/K$.

DEMOSTRACIÓN. Consideramos una clausura algebraica $\overline{K}$ de K que contiene a E, y prolongamos σ hasta, $\sigma : F/K \longrightarrow \overline{K}/K$. Por ser E/K algebraica (es finita) existe una extensión de σ hasta E, $\overline{\sigma} : E/K \longrightarrow \overline{K}/K$. Ya que E/K es una extensión normal, tenemos $E^{\overline{\sigma}} = E$, luego resulta que $\overline{\sigma}$ es la extensión de σ buscada. □

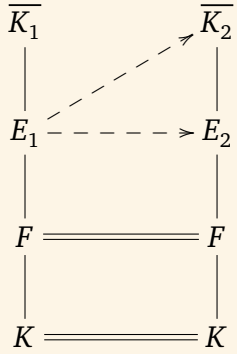
Teorema. 5.5.
Si F/K es una extensión finita, entonces existe una extensión normal E/K verificando:
(1) $F \subseteq E$.
(2) Para cada extensión normal H/K con $F \subseteq H \subseteq E$ se tiene $H = E$.

DEMOSTRACIÓN. Como la extensión F/K es finita, supongamos $F = K(\alpha_1, \ldots, \alpha_n)$. Para cada α_i, $1 \leq i \leq n$, llamamos $g_i(X) = \mathrm{Irr}(\alpha_i, K)$, y $g(X) = g_1(X) \cdots g_n(X)$. Si $\overline{K}$ es una clausura algebraica de K que contiene a todos los α_i, $1 \leq i \leq n$, llamamos $E = K(\{\alpha_j / j \in J\})$, donde $\{\alpha_j / j \in J\}$ es el conjunto de todas las raíces de $g(X)$ en $\overline{K}$. El cuerpo E es un cuerpo de descomposición de $g(X)$ sobre K, luego E/K es una extensión normal, y es claro que $F \subseteq E$. Supongamos ahora que H/K es una extensión normal y que $F \subseteq H \subseteq E$, entonces cada $g_i(X)$, $1 \leq i \leq n$, descompone en H y por tanto $g(X)$ descompone en H, pero E es un cuerpo de descomposición de $g(X)$, luego $H = E$. □

Si F/K es una extensión finita, una extensión E/K verificando las condiciones del teorema se llama una **clausura normal** de F sobre K.

Vamos a probar que la clausura normal tiene una cierta unicidad.

Proposición. 5.6.
Sea F/K una extensión finita y E_1/K, E_2/K clausuras normales de F sobre K, existe un F-isomorfismo $\sigma : E_1/F \longrightarrow E_2/F$.



DEMOSTRACIÓN. Ya que la extensión E_i/F, $1 \leq i \leq 2$, es finita, consideramos una clausura algebraica $\overline{K}_i$ de K que contenga a E_i. Por la construcción del teorema, E_i es el cuerpo de descomposición en $\overline{K_i}$ de un polinomio $g(X) \in K[X]$. Prolongamos la identidad en F hasta $\overline{K}_2$ y por ser E_1/F finita, podemos extenderla hasta un homomorfismo $\sigma : E_1/K \longrightarrow \overline{K}_2/K$. La imagen E_1^σ de E_1 contiene a F y es un cuerpo de descomposición de $g(X)$ contenido en $\overline{K}_2$, entonces $E_1^\sigma = E_2$, y tenemos el F-isomorfismo pedido. □

Una consecuencia importante de esta proposición es que dada una extensión finita F/K, toda clausura normal E de F sobre K es una extensión finita de K.

Si volvemos al ejemplo de $\mathbb{Q}(\sqrt[5]{2}, \xi_5)$, recordemos que $\mathbb{Q}(\sqrt[5]{2}, \xi_5)/\mathbb{Q}$ es una extensión normal y que $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ no lo es. Podemos caracterizar las subextensiones normales de una extensión normal mediante el siguiente teorema.

Teorema. 5.7.
Sea $K \subseteq F \subseteq E$ una torre de extensiones finitas y E/K una extensión normal. Son equivalentes:

(a) F/K es una extensión normal.
(b) Para cada homomorfismo $\sigma : E/K \longrightarrow E/K$ se tiene $F^\sigma = F$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Dado un homomorfismo $\sigma : E/K \longrightarrow E/K$, consideramos su prolongación a una clausura algebraica de K que contenga a E, y su restricción a F, tenemos así un homomorfismo $\sigma_{|F} : F/K \longrightarrow \overline{K}/K$, ya que F/K es normal tenemos $F^\sigma = F$.

(b) $\Rightarrow$ (a). Consideramos un homomorfismo $\sigma : F/K \longrightarrow \overline{K}/K$, por ser E/K finita podemos extenderlo hasta E. Supongamos que $\overline{\sigma} : E/K \longrightarrow \overline{K}/K$ es una extensión de σ. Ya que E/K es una extensión normal, $E^{\overline{\sigma}} = E$, y por tanto podemos suponer que $\overline{\sigma} : E/K \longrightarrow E/K$, aplicando (b), se tiene $F = F^{\overline{\sigma}} = F^\sigma$. □

5.1. Ejercicios

Cuerpos de descomposición

Ejercicio. 5.8.
Razona que existe un isomorfismo $\sigma : \mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(i\sqrt[4]{2})$ *tal que* $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$.
Ref.: 4162e_001 SOLUCIÓN

Ejercicio. 5.9.
Razona que no existe ningún homomorfismo de cuerpos $\sigma : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{3})$.
Ref.: 4162e_002 SOLUCIÓN

Ejercicio. 5.10.
Demuestra que los cuerpos $\mathbb{Q}(i)$ *y* $\mathbb{Q}(\sqrt{2})$ *no son isomorfos.*
Ref.: 4162e_003 SOLUCIÓN

Ejercicio. 5.11.
Determina todos los homomorfismos de cuerpos $\mathbb{Q}(\sqrt{2}, i) \to \mathbb{C}$ *que existan. Halla sus imágenes.*
Ref.: 4162e_004 SOLUCIÓN

Ejercicio. 5.12.
Sea α *una raíz del polinomio* $f(X) = X^6 + X^3 + 1 \in \mathbb{Q}[X]$. *Determina todos los homomorfismos de cuerpos* $\mathbb{Q}(\alpha) \to \mathbb{C}$ *que existan. Halla sus imágenes. (Pista:* $f(X)$ *divide al polinomio* $X^9 - 1$*).*
Ref.: 4162e_005 SOLUCIÓN

Ejercicio. 5.13.
Demuestra que el polinomio X^4-2X^2-2 es irreducible sobre $\mathbb{Q}$. Encuentra dos pares de raíces que generen extensiones no isomorfas.
Ref.: 4162e_006 SOLUCIÓN

Ejercicio. 5.14.
Demuestra que el cuerpo de descomposición de un polinomio de grado n está generado por $n-1$ de sus raíces.
Ref.: 4162e_007 SOLUCIÓN

Ejercicio. 5.15.
Calcula el grado del cuerpo de descomposición de X^6+1 sobre $\mathbb{F}_2$.
Ref.: 4162e_008 SOLUCIÓN

Ejercicio. 5.16.
Calcula el grado de los cuerpos de descomposición de los siguientes polinomios sobre $\mathbb{Q}$:
(1) X^2-2,
(2) X^2-1,
(3) X^2+X+1,
(4) X^3-X^2-X-2,
(5) X^4-1,
(6) X^4+1,
(7) X^4+2,
(8) X^4+4,
(9) X^4-7,
(10) X^5-2,
(11) $(X^2-2)(X^3-2)$,
(12) $X^4+X^3-4X^2-5X-5$,
(13) X^6-1,
(14) X^6+1,

(15) X^6-3,
(16) X^6+3.

Ref.: 4162e_009 SOLUCIÓN

Ejercicio. 5.17.
Calcula el grado de los cuerpos de descomposición de los siguientes polinomios sobre $\mathbb{Q}$*:*
(1) X^3-2.
(2) X^4-7.
(3) $(X^2-2)(X^2-5)$.

Ref.: 4162e_010 SOLUCIÓN

Ejercicio. 5.18.
Demuestra que el cuerpo de descomposición del polinomio X^n-1 *sobre* $\mathbb{Q}$ *es una extensión simple de* $\mathbb{Q}$*. Determina un elemento que genere la extensión (elemento primitivo).*
Ref.: 4162e_011 SOLUCIÓN

Ejercicio. 5.19.
Sea p *un entero primo positivo.*
(1) *Determina el cuerpo de descomposición* F *del polinomio* $X^{p^8}-1$ *sobre el cuerpo* $K=\mathbb{F}_p$*. Calcula el grado* $[F:K]$.
(2) *Determina el cuerpo de descomposición* F *del polinomio* $X^{p^8}-X$ *sobre el cuerpo* $K=\mathbb{F}_p$*. Calcula el grado* $[F:K]$.

Ref.: 4162e_012 SOLUCIÓN

Ejercicio. 5.20.
Sea K un cuerpo y $f(X) \in K[X]$ un polinomio de grado n que se expresa $f(X) = f_1(X)\cdots f_t(X)$, siendo cada $f_i(X) \in K[X]$ un polinomio irreducible de grado d_i, y $f_i(X) \nmid f_j(X)$, si $i \neq j$. Da una cota, que se alcance, del grado de la extensión $K(f(X))/K$.
Ref.: 4162e_093 SOLUCIÓN

Ejercicio. 5.21.
Sea K un cuerpo y $f(X) \in K[X]$ un polinomio de grado n. Prueba que si el grado del $K(f)/K$ es igual a $n!$, entonces $f(X)$ es irreducible.
Ref.: 4162e_094 SOLUCIÓN

Ejercicio. 5.22.
Sea $f(X) \in K[X]$ y E su cuerpo de descomposición. Pon ejemplos de polinomios para los cuales se tengan las relaciones
(1) $[E:K] \lneq \mathrm{gr}(f(X))$.
(2) $[E:K] = \mathrm{gr}(f(X))$.
(3) $[E:K] \gneq \mathrm{gr}(f(X))$.

Si $f(X)$ es irreducible. ¿Es cierta siempre alguna de las relaciones anteriores?.
Ref.: 4162e_116 SOLUCIÓN

Ejercicio. 5.23.
Sea $K \subseteq E \subseteq F$ una torre de cuerpos y supongamos que $\alpha_1, \ldots, \alpha_r$ son algunas de las raíces de $f(X) \in K[X]$ y $E = K(\alpha_1, \ldots, \alpha_r)$. Demuestra que F es el cuerpo de descomposición de $f(X)$ sobre K si, y sólo si, F es el cuerpo de descomposición de $f(X)$ sobre E.
Ref.: 4162e_117 SOLUCIÓN

Extensiones normales

Ejercicio. 5.24.
Demuestra que toda extensión de grado 2 es normal.
Ref.: 4162e_013 SOLUCIÓN

Ejercicio. 5.25.
Consideramos la torre de cuerpos $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$.

(1) Demuestra que las extensiones $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ *y* $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *son normales.*
(2) Demuestra que la extensión $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ *no es normal.*

Ref.: 4162e_014 SOLUCIÓN

Ejercicio. 5.26.
Dada una torre de cuerpos $K \subseteq F \subseteq E$, *sabemos que si las extensiones* E/F *y* F/K *son algebraicas, también lo es la extensión* E/K, *y viceversa. En cambio, para extensiones normales este resultado no se verifica.*

(1) Si la extensión E/K *es normal, no necesariamente la extensión* F/K *es normal. Puedes considerar el ejemplo siguiente:* $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt[3]{2})$ *y* $E = \mathbb{Q}(\omega, \sqrt[3]{2})$, *donde* ω *es una raíz cúbica primitiva de la unidad. Justifica este hecho. Observa que si* E/K *es normal, siempre* E/F *es normal.*
(2) Si las extensiones E/F *y* F/K *son normales, no siempre la extensión* E/K *es normal. Puedes considerar el siguiente ejemplo:* $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{2})$ *y* $E = \mathbb{Q}\left(\sqrt{\sqrt{2}}\right) = \mathbb{Q}(\sqrt[4]{2})$. *Estudia por qué no es normal.*

Ref.: 4162e_095 SOLUCIÓN

Ejercicio. 5.27.
Estudia si la extensión $F/\mathbb{Q}$ *es normal para* F *cada uno de los siguientes cuerpos:*

(1) $\mathbb{Q}(\sqrt{5})$,
(2) $\mathbb{Q}(\sqrt[3]{5})$,
(3) $\mathbb{Q}(\sqrt{5}, \sqrt[3]{5})$,

(4) $\mathbb{Q}(\sqrt{2},\sqrt{5})$,
(5) $\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$,
(6) $\mathbb{Q}(\sqrt[3]{2},\sqrt{-5})$,
(7) $\mathbb{Q}(\sqrt[4]{4})$,
(8) $\mathbb{Q}(\sqrt[4]{8})$,
(9) $\mathbb{Q}(\sqrt[6]{27})$,
(10) $\mathbb{Q}(\sqrt[8]{16})$,
(11) $\mathbb{Q}(\sqrt{a_1},\sqrt{a_2},\ldots,\sqrt{a_r})$.

Ref.: 4162e_015 SOLUCIÓN

Ejercicio. 5.28.
Estudia la normalidad de las siguientes extensiones:

(1) $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$.
(2) $\mathbb{Q}(\sqrt[3]{-7})/\mathbb{Q}$.
(3) $\mathbb{Q}(\sqrt[3]{7},\sqrt{3})/\mathbb{Q}$.
(4) $\mathbb{Q}(\sqrt{3})(\sqrt{-7})/\mathbb{Q}(\sqrt{3})$.

Ref.: 4162e_016 SOLUCIÓN

Ejercicio. 5.29.
Calcula la clausura normal de cada una de las siguientes extensiones:

(1) $\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q}$,
(2) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$,
(3) $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$,
(4) $\mathbb{Q}(\sqrt{5},\sqrt[3]{5})/\mathbb{Q}$,
(5) $\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})/\mathbb{Q}$,
(6) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$.

Ref.: 4162e_017 SOLUCIÓN

Ejercicio. 5.30.
Determina todas las extensiones de grado 3 de $\mathbb{F}_2$. Estudia la normalidad de cada una de ellas. Encuentra un isomorfismo explícito entre aquellas que sean isomorfas.
Ref.: 4162e_019 SOLUCIÓN

Un polinomio $f(X) \in K[X]$ es **normal** si su cuerpo de descomposición está generado por una de sus raíces.

Ejercicio. 5.31.
Demuestra que todo polinomio $f \in K[X]$ irreducible de grado 2 es normal.
Ref.: 4162e_020 SOLUCIÓN

Ejercicio. 5.32.
Demuestra que $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ con p primo es un polinomio normal.
Ref.: 4162e_021 SOLUCIÓN

Ejercicio. 5.33.
Sea α una raíz del polinomio $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$. Demuestra que $\alpha^2 - 2$ es otra raíz de f. ¿Es $f(X)$ normal?
Ref.: 4162e_022 SOLUCIÓN

Ejercicio. 5.34.
¿Es la extensión $\mathbb{Q}\left(\sqrt{2+\sqrt{-5}}\right)/\mathbb{Q}$ normal?
Ref.: 4162e_100 SOLUCIÓN

Ejercicio. 5.35.
Sea E/K una extensión (finita) verificando que todo elemento $\alpha \in E$ está contenido en un subcuerpo intermedio F_α que es normal sobre K. Demuestra que E/K es una extensión normal.
Ref.: 4162e_118 SOLUCIÓN

Ejercicio. 5.36.
Prueba que toda extensión F/K generada por elementos de grado dos es una extensión normal.
Ref.: 4162e_135 SOLUCIÓN

Ejercicio. 5.37.
Sea E/K una extensión normal y $f(X) \in K[X]$ un polinomio (mónico) irreducible. Si $f(X)$ se factoriza en E como producto de dos polinomios (mónicos) irreducibles $f_1(X)$ y $f_2(X)$. Demuestra que existe un homomorfismo $\sigma : E/K \longrightarrow E/K$ tal que $f_1^\sigma(X) = f_2(X)$.
Ref.: 4162e_119 SOLUCIÓN

Ejercicio. 5.38.
Sea E/K una extensión, demuestra que son equivalenes:
(a) La extensión E/K es normal.
(b) Cada polinomio irreducible $f(X) \in K[X]$ factoriza en $E[X]$ como un producto de polinomios irreducibles, todos del mismo grado.

Ref.: 4162e_120 SOLUCIÓN

Ejercicio. 5.39.
Sea $a \in \mathbb{Q}$ y n un número entero positivo impar tal que $\sqrt[n]{a} \in \mathbb{R}\backslash\mathbb{Q}$. Demuestra que la extensión $\mathbb{Q}(\sqrt[n]{a})/\mathbb{Q}$ no es normal.
Ref.: 4162e_121 SOLUCIÓN

Ejercicio. 5.40.
Si $f(X) \in K[X]$ es un polinomio de grado n y E/K es su cuerpo de descomposición, prueba que $[E:K] | n!$
Ref.: 4162e_134 SOLUCIÓN

Ejercicio. 5.41.
Sea $K \subseteq F$ una extensión normal finita y $f(X) \in K[X]$ un polinomio irreducible. Si $f = gh$ es una factorización en $F[X]$, con g, h polinomios mónicos irreducibles, demuestra que existe un automorfismo $\sigma \in \mathrm{Aut}(F/K)$ tal que $\sigma(g) = h$.
Ref.: 4162e_123 SOLUCIÓN

Ejercicio. 5.42.
Sea $f \in \mathbb{Q}[X]$ un polinomio irreducible de grado impar mayor que uno.
(1) Prueba que f tiene al menos una raíz real.
(2) Si α es la única raíz real de f, prueba que $\mathbb{Q}(\alpha)/\mathbb{Q}$ no es una extensión normal.
Ref.: 4162e_141 SOLUCIÓN

6. Extensiones separables. Cuerpos perfectos

Sea K un cuerpo, ya conocemos que existe un único homomorfismo del anillo $\mathbb{Z}$ de los números enteros en K, la imagen de este homomorfismo es un subanillo de K; es el subanillo S de K generado por el elemento 1. Ya que $S \subseteq K$, tenemos que S es un DI, y su cuerpo de fracciones es un subcuerpo de K, llamémoslo C. Este subcuerpo C tiene una propiedad muy interesante: C está contenido en cada subcuerpo de K, es más, C es la intersección de todos los subcuerpos de K. Así pues para cada cuerpo K el cuerpo C está completamente determinado, y se le suele llamar el **subcuerpo característico** o el **subcuerpo primo** de K.

Además, ya que C es el cuerpo de fracciones de un cociente de $\mathbb{Z}$, que es DI, tenemos que C ha de ser isomorfo a $\mathbb{Q}$, el cuerpo de los números racionales, ó a $\mathbb{Z}_p$, el cuerpo de las clases de resto módulo p, para algún número entero primo p. Recordemos que la **característica** de un anillo R es el menor entero positivo n que verificaba $n1 = 0$, en caso de no existir este número entero positivo, la característica de R era igual a cero; ó equivalentemente, la característica de un anillo R es el entero positivo ó nulo que genera el núcleo del único homomorfismo existente de $\mathbb{Z}$ en R. Podemos pues enunciar el siguiente resultado, cuya demostración es inmediata.

Lema. 6.1.
Sea K un cuerpo, la característica de K es cero si, y sólo si, su cuerpo característico es isomorfo a $\mathbb{Q}$, y es p, un número entero primo positivo, si su cuerpo característico es $\mathbb{F}_p$.

Sea $f(X) \in K[X]$ un polinomio no constante, y sea F/K un cuerpo de descomposición de $f(X)$. En F el polinomio $f(X)$ se factoriza en la forma

$$f(X) = (X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r},$$

siendo $\alpha_1, \ldots, \alpha_r$ las raíces de $f(X)$ en F, todas distintas, y los m_i las multiplicidades de la raíces, $m_i \geq 1$, $1 \leq i \leq r$.

Si E/K es otro cuerpo de descomposición de $f(X)$, y $f(X)$ se factoriza E en la forma

$$f(X) = (X - \beta_1)^{n_1} \cdots (X - \beta_s)^{n_s},$$

con $\beta_1, \ldots, \beta_s$ las raíces de $f(X)$ en E, todas distintas, y los n_j verificando $n_j \geq 1$, $1 \leq j \leq s$, entonces existe un isomorfismo de F/K en E/K que aplica biyectivamente el conjunto $\{\alpha_1, \ldots, \alpha_r\}$ en el conjunto $\{\beta_1, \ldots, \beta_s\}$. Luego $r = s$ y además existe una permutación $\sigma \in S_r$ que verifica $m_i = n_{\sigma(i)}$, $1 \leq i \leq r$. Como consecuencia la multiplicidad de las raíces de un polinomio no depende del cuerpo en el que éste descomponga, sino que depende única y exclusivamente de él mismo y del cuerpo K en el que están sus coeficientes.

Vamos a estudiar la multiplicidad de las raíces de un polinomio no constante $f(X) \in K[X]$. Recordemos el siguiente resultado, en donde $Df(X)$ es la derivada de $f(X)$ con respecto a X.

4162-02.tex

Lema. 6.2.
Sea $f(X)$ un polinomio con $Df(X) \neq 0$ y con coeficientes en un cuerpo K, son equivalentes:
(a) Todas las raíces de $f(X)$ son simples.
(b) $f(X)$ y $Df(X)$ son primos relativos.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si todas las raíces de $f(X)$ son simples, en un cuerpo de descomposición F de $f(X)$ tenemos que $f(X)$ tiene la expresión siguiente:

$$f(X) = a(X-\alpha_1)\cdots(X-\alpha_r),$$

con todos los α_i distintos. Si calculamos $Df(X)$ tenemos

$$Df(X) = a\sum_{i=1}^{r}(X-\alpha_1)\cdots(X-\alpha_{i-1})(X-\alpha_{i+1})\cdots(X-\alpha_r).$$

Como para cada i, $1 \leq i \leq r$, se tiene $(X-\alpha_i) \nmid Df(X)$, y $Df(X) \neq 0$, tenemos que $f(X)$ y $Df(X)$ son primos relativos.
(b) $\Rightarrow$ (a). Llamamos $d(X)$ al máximo común divisor de $f(X)$ y $Df(X)$. Tomamos F un cuerpo de descomposición de $f(X)$ y $\alpha \in F$ una raíz de multiplicidad m, mayor ó igual que 2. En $F[X]$ tenemos $f(X) = (X-\alpha)^m g(X)$, con $g(X) \in F[X]$. Por tanto $Df(X) = (X-\alpha)^m Dg(X) + m(X-\alpha)^{m-1}g(X)$, y $X-\alpha$ divide a $f(X)$ y a $Df(X)$, en $F[X]$, por lo tanto no son primos relativos en $F[X]$, y tampoco lo son en $K[X]$. □

Consecuencia de este hecho es:

Corolario. 6.3.
(1) Si K es un cuerpo de característica cero, entonces todo polinomio no constante e irreducible tiene todas sus raíces simples.
(2) Si K es un cuerpo de característica $p(\neq 0)$, entonces un polinomio no constante e irreducible $f(X)$ tiene raíces múltiples si, y sólo si, $Df(X) = 0$.
En el segundo caso el polinomio $f(X)$ es de la forma $g(X^p)$ para algún polinomio $g(X) \in K[X]$.

DEMOSTRACIÓN. (1). Por ser $f(X)$ irreducible tenemos que $f(X)$ y $Df(X)$ son primos relativos, ya que $f(X)$ no puede dividir a $Df(X)$ por ser de grado menor, por tanto las raíces de $f(X)$ son todas simples.
(2). ($\Rightarrow$). Si $Df(X) \neq 0$, entonces $f(X)$ y $Df(X)$ son primos relativos, y por tanto todas las raíces de $f(X)$ son simples.

($\Leftarrow$). Si $Df(X) = 0$, entonces toda raíz de $f(X)$ es también raíz de su derivada, y por tanto es una raíz múltiple.
Si $Df(X) = 0$ y $f(X) = a_0 + a_1X + \cdots + a_nX^n$, entonces para cada índice $0 \leq i \leq n$, se tiene $ia_i = 0$, en particular para cada i verificando $0 \leq i \leq n$ y $p \nmid i$ se tiene $a_i = 0$, luego $f(X) = a_0 + a_pX^p + \cdots + a_{p^r}X^{p^r} = a_0 + a_p(X^p) + \cdots + a_{p^r}(X^p)^r$. □

No podemos asegurar que todos los polinomios irreducibles, al igual que en caso de característica cero, tengan raíces simples, pues puede ocurrir que la derivada sea igual a cero. Un ejemplo de que es posible encontrar un polinomio irreducible con raíces múltiples es el siguiente:

Ejemplo. 6.4.
Sea K un cuerpo de característica $p(\neq 0)$, y T una indeterminada sobre K. Consideramos el anillo de polinomios $K[T]$ y su cuerpo de fracciones $K(T)$. En el anillo $K(T)[X]$ el polinomio $f(X) = X^p - T$ es irreducible (aplicar el criterio de Eisenstein) y su derivada es cero. Si $F/K(T)$ es un cuerpo de descomposición de $f(X)$, y $\beta \in F$ es una raíz, se verifica

$$0 = f(\beta) = \beta^p - T,$$

entonces, en $K(T)(\beta)[X]$ se tiene $f(X) = X^p - T = X^p - \beta^p = (X - \beta)^p$. Como consecuencia, $f(X)$ tiene raíces múltiples.

Vamos a buscar condiciones, sobre el cuerpo K, para que todos los polinomios irreducibles tengan todas sus raíces simples. Para ello introducimos el **endomorfismo de Frobenius**. Si K es un cuerpo de característica $p(\neq 0)$, definimos $\phi : K \longrightarrow K$ mediante $\phi(x) = x^p$, para cada $x \in K$. Así definido ϕ es un homomorfismo de cuerpos; además si K es finito, entonces ϕ es un automorfismo. Este endomorfismo nos va a permitir dar una caracterización de los cuerpos que andamos buscando.

Teorema. 6.5.
Sea K un cuerpo de característica $p(\neq 0)$, son equivalentes:

(a) Todo polinomio irreducible no constante $f(X) \in K[X]$ tiene todas sus raíces simples.
(b) El endomorfismo de Frobenius es un automorfismo.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Dado $a \in K$ consideramos el polinomio $f(X) = X^p - a \in K[X]$. Si α es una raíz de $f(X)$ en un cuerpo de descomposición F/K, entonces en $F[X]$ tenemos la siguiente expresión para $f(X)$:

$$f(X) = (X - \alpha)^p,$$

y por tanto cada factor irreducible, sobre K, de $f(X)$ tiene también una única raíz, posiblemente con multiplicidad ≥ 1. Aplicando (a), resulta que el único factor irreducible de $f(X)$ en $K[X]$ es $X - \alpha$. Luego $\alpha \in K$ y $a = \alpha^p$, así pues el endomorfismo de Frobenius es sobreyectivo y por tanto un automorfismo.

(b) $\Rightarrow$ (a). Supongamos que $f(X) \in K[X]$ es irreducible y no constante, si $Df(X) = 0$, entonces existe $g(X) \in K[X]$ tal que $f(X) = g(X^p)$, supongamos que $g(X) = b_0 + b_1X + \cdots + b_rX^r$, entonces para cada b_i, $0 \leq i \leq r$, existe c_i tal que $c_i^p = b_i$, y tenemos pues $f(X) = c_0^p + c_i^p(X^p) + \cdots + c_r^p(X^p)^r = (c_0 + c_1X + \cdots + c_rX^r)^p$, lo que es una contradicción. Así pues $Df(X) \neq 0$ y $f(X)$ tiene todas sus raíces simples. □

Los cuerpos que verifican las condiciones equivalentes del teorema se llaman **cuerpos perfectos**. Es claro, de los comentarios anteriores, que todo cuerpo de característica cero es perfecto y que también lo es todo cuerpo finito; no lo es en cambio la extensión de un cuerpo de característica p por un elemento trascendente, como nos muestra el Ejemplo (6.4.).

Sea K un cuerpo, un polinomio $f(X) \in K[X]$ es un **polinomio separable** sobre K si sus factores irreducibles, sobre K, tienen todas sus raíces simples.

Sea F/K una extensión de cuerpos, un elemento algebraico $\alpha \in F$ es un **elemento separable** sobre K si el polinomio $\mathrm{Irr}(\alpha, K)$ es separable.

Una extensión algebraica F/K es una **extensión separable** si cada elemento de F es separable sobre K. (*Más adelante veremos que una extensión F/K es separable si está generada por elementos separables.*)

Observa que el polinomio $X^p - T^p \in K(T)[X]$ es separable, pero $X^p - T^p \in K(T^p)[X]$ no es separable, cuando T es una indeterminada sobre K.

Consecuencia inmediata de estas definiciones es que un cuerpo es perfecto si, y sólo si, todo polinomio es separable.

Las extensiones separables permiten caracterizar a los cuerpos perfectos.

Proposición. 6.6.
Sea K un cuerpo, son equivalentes:

(a) K es un cuerpo perfecto.
(b) Toda extensión algebraica de K es separable.
(c) Toda extensión finita de K es separable.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si F/K es una extensión algebraica, para cada $\alpha \in F$ tenemos que $\mathrm{Irr}(\alpha, K)$ es un polinomio separable sobre K, luego α es un elemento separable sobre K, y por tanto F/K es separable.

(b) $\Rightarrow$ (c). Es evidente, ya que cada extensión finita es algebraica.

(c) $\Rightarrow$ (a). Si $f(X) \in K[X]$ es un polinomio irreducible no constante, consideramos un cuerpo de descomposición de $f(X)$ sobre K, entonces F/K es una extensión finita y por tanto separable. Como consecuencia cada raíz de $f(X)$ es separable sobre K, y $f(X)$ es pues un polinomio separable. □

Como consecuencia todo cuerpo algebraicamente cerrado es un cuerpo perfecto.

Proposición. 6.7.
Sea $K \subseteq F \subseteq E$ una torre de cuerpos, siendo E/K una extensión algebraica y separable, entonces E/F y F/K son extensiones separables.

DEMOSTRACIÓN. F/K es separable ya que cada elemento $\alpha \in F$ es también un elemento de E, y por tanto es separable sobre K. Para probar que E/F es una extensión separable, consideremos un elemento $\beta \in E$, entonces se verifica $\mathrm{Irr}(\beta, F) | \mathrm{Irr}(\beta, K)$, ya que $\mathrm{Irr}(\beta, K)$ es separable, resulta que $\mathrm{Irr}(\beta, F)$ también lo es. Luego β es separable sobre F. □

Teorema. 6.8.
Todo cuerpo, extensión algebraica de un cuerpo perfecto, es un cuerpo perfecto.

DEMOSTRACIÓN. Supongamos que K es un cuerpo perfecto y F/K es una extensión algebraica, para cada extensión algebraica E/F tenemos que E/K es una extensión algebraica, y por tanto es separable, como consecuencia E/F es una extensión separable, y por tanto F es un cuerpo perfecto. □

Para seguir nuestro estudio de las extensiones separables necesitamos nuevos elementos en la teoría; en particular, estamos interesados en caracterizar las extensiones separables finitas en términos del número de automorfismos de la extensión.

6.1. Ejercicios

Extensiones separables. Cuerpos perfectos

Ejercicio. 6.9.
Sea K un cuerpo.

(1) Prueba que para cualquier familia de subcuerpos $\{K_i \mid i \in I\}$ se tiene que $\cap_i K_i$ es un subcuerpo de K.
(2) Para cada elemento $\alpha \in K$, la intersección de todos los subcuerpos de K que contienen a α es el menor subcuerpo de K que contiene a α, lo representamos por $\langle\alpha\rangle$.
*(3) Llamamos **subcuerpo caraterístico** o **subcuerpo de primo** de K al menor subcuerpo de K que contiene a 1. Existe una única aplicación de anillos $f : \mathbb{Z} \longrightarrow K$, si $n\mathbb{Z} = \mathrm{Ker}(f)$, $n \in \mathbb{Z}^{\geq 0}$, decimos que n es la característica de K; la característica de K es 0 o un número primo, y el subcuerpo de primo de K es $\mathbb{Q}$, si la característica es 0, ó $\mathbb{Z}_p$, si la característica es $p \neq 0$.*
(4) El subcuerpo primo queda fijo para todo endomorfismo de K.
*(5) Si la característica de K es $p \neq 0$, entonces $\phi_p : K \longrightarrow K$, definido $\phi_p(x) = x^p$, se llama el **endomorfismo de Frobenius**, y tiene como conjunto de elementos fijos los elementos del subcuerpo primo.*
(6) Al considerar $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, prueba que $\phi_2(\alpha) = \alpha + 1$.

Ref.: 4162e_018 SOLUCIÓN

Ejercicio. 6.10.
Demuestra que sobre un cuerpo de característica $p \neq 0$ el polinomio $X^p - a$ ó es irreducible ó es una potencia de un polinomio lineal.
Ref.: 4162e_023 SOLUCIÓN

Ejercicio. 6.11.
Estudia si los siguientes elementos son separables:

(1) $\sqrt[4]{23}$ sobre $\mathbb{Q}$.
(2) $\sqrt[8]{2}$ sobre $\mathbb{Q}(\sqrt{2})$,
(3) $\sqrt[7]{5}$ sobre $\mathbb{F}_7$,
(4) La indeterminada t sobre $\mathbb{F}_p(t^p)$, con p un entero primo positivo.

Ref.: 4162e_024 SOLUCIÓN

Ejercicio. 6.12.
Sea F/K una extensión finita con $m = [F : K]$ y $\mathrm{car}(K) = p \neq 0$ tales que $p \nmid m$. Demuestra que la extensión F/K es separable.
Ref.: 4162e_025 SOLUCIÓN

Ejercicio. 6.13.
Demuestra que una extensión no separable de un cuerpo de característica p tiene grado mayor o igual a p.
Ref.: 4162e_026 SOLUCIÓN

Ejercicio. 6.14.
Sea $a \in \mathbb{F}_p$ un elemento distinto de cero y $f(X) = X^p - X + a \in \mathbb{F}_p[X]$. Demuestra que si α es una raíz de $f(X)$ entonces también lo es $\alpha + 1$. ¿Es $f(X)$ separable?
Ref.: 4162e_027 SOLUCIÓN

Ejercicio. 6.15.
Sea K un cuerpo de característica $p \neq 0$ y α un elemento algebraico sobre K. Demuestra que:

(1) Existe un $n \geq 0$ tal que α es separable sobre $K(\alpha^{p^n})$.
(2) α es separable sobre K si, y sólo si, $K(\alpha) = K(\alpha^p) = K(\alpha^{p^2}) = \cdots$

Ref.: 4162e_028 SOLUCIÓN

Ejercicio. 6.16.
Sea K un cuerpo de característica $p \neq 0$. Si un elemento α de una extensión de K es separable sobre $K(\alpha^p)$, demuestra que $\alpha \in K(\alpha^p)$.
Ref.: 4162e_114 SOLUCIÓN

Ejercicio. 6.17.
Sea K un cuerpo de característica $p \neq 0$, F/K una extensión de cuerpos, y $K_0 = \{a \in F \mid a^{p^r} \in K$, para algún $r \geq 0\}$. Demuestra que:

(1) K_0 es un subcuerpo de F.
(2) Si F es perfecto, entonces también lo es K_0.
(3) Todo automorfismo de F/K deja fijo a K_0 elemento a elemento.

Podemos aplicar este mismo ejercicio al caso del subcuerpo característico de K.
Ref.: 4162e_029 SOLUCIÓN

Ejercicio. 6.18.
Sea K un cuerpo de característica 2. Demuestra que cualquier extensión separable de grado dos sobre K puede generarse por una raíz de un polinomio $X^2 + X + a$, con $0 \neq a \in K$. Recíprocamente, un polinomio del tipo anterior es separable sobre K. Además si u es una raíz del polinomio anterior, también lo es $u+1$. Demostrar que los automorfismos de $K(u)/K$ son la identidad y σ, con $\sigma(b+cu) = b + c + cu$, para $b, c \in K$.
Ref.: 4162e_030 SOLUCIÓN

Ejercicio. 6.19.
Sea K un cuerpo de característica 2. Demuestra que cualquier elemento u, no separable de grado dos sobre K, es raíz de un polinomio de la forma $X^2 + a$ con $a \in K$ un elemento que no es un cuadrado en K. Recíprocamente, demuestra que cualquier polinomio del tipo anterior no es separable sobre K.
Ref.: 4162e_031 SOLUCIÓN

Ejercicio. 6.20.
Sea K un cuerpo de característica 2, y F/K una extensión separable de grado 2. Prueba que existe $\alpha \in F$ tal que $F = K(\alpha)$ y $\alpha^2 + \alpha \in K$.
Ref.: 4162e_101 SOLUCIÓN

Ejercicio. 6.21.
Sea K un cuerpo de característica distinta de 2.

(1) Demuestra que toda extensión de grado dos sobre K es separable y puede ser generada por una raíz del polinomio $X^2 - a$, con $a \in K$ un elemento que no es un cuadrado en K.
(2) Recíprocamente, si u es una raíz del polinomio anterior, entonces $K(u)/K$ es separable.
(3) Demuestra que cualquier automorfismo sobre K es la identidad ó el definido por $\varphi(b + \alpha c) = b - \alpha c$, para $b, c \in K$.
(4) Encuentra los automorfismos de $K(u)/K$.

Ref.: 4162e_032 *SOLUCIÓN*

Ejercicio. 6.22.
Sea K un cuerpo de característica $p \neq 0$, y $a, b \in K$. Si se considera el polinomio $f(X) = X^p - b^{p-1}X - a$, prueba que $f(X)$ es irreducible ó $f(X)$ descompone en K.
Ref.: 4162e_098 *SOLUCIÓN*

Ejercicio. 6.23.
Demuestra que un cuerpo de característica $p \neq 0$ puede tener n raíces distintas n–ésimas de la unidad si, y sólo si, p no divide a n.
Ref.: 4162e_113 *SOLUCIÓN*

Ejercicio. 6.24.
Sea K un cuerpo de característica $p \neq 0$ y t una indeterminada sobre K. Prueba que el polinomio $X^p - t^p \in K(t^p)[X]$ es irreducible.
Ref.: 4162e_124 *SOLUCIÓN*

Ejercicio. 6.25.
Estudiar si son ó no ciertas las siguientes afirmaciones:

(1) $\sqrt[3]{-1}$ *es separable sobre* $\mathbb{F}_9$.
(2) $\sqrt[3]{-1}$ *es separable sobre* $\mathbb{F}_{49}$.
(3) $\sqrt[7]{5}$ *es separable sobre* $\mathbb{F}_{7^7}$.
(4) t *es separable sobre* $\mathbb{F}_{p^2}(t^p)$, *siendo* p *un número entero primo positivo y* t *una indeterminada sobre* $\mathbb{F}_{p^2}$.

Ref.: 4162e_115 SOLUCIÓN

7. Automorfismos de extensiones de cuerpos

En el estudio de las extensiones de cuerpos F/K una herramienta fundamental van a ser los automorfismos. Su uso es debido a R. Dedekind, quién pasó de considerar la teoría basada en el estudio de raíces de polinomios, debida esencialmente a E. Galois, a estudiar las extensiones mediante los homomorfismos a una clausura algebraica de K.

Aquí vamos a considerar dos extensiones F/K y E/K de un cuerpo K. Para cada homomorfismo de cuerpos $\sigma : F/K \longrightarrow E/K$ tenemos que $\sigma : F \longrightarrow E$ es un homomorfismo de K–espacios vectoriales. Si llamamos $\mathrm{Hom}(F/K, E/K)$ al conjunto de los homomorfismos de cuerpos de F/K a E/K, existe una inclusión $\mathrm{Hom}(F/K, E/K) \subseteq \mathrm{Hom}_K(F, E)$, donde $\mathrm{Hom}_K(F, E)$ es el conjunto de los homomorfismos K–lineales de F a E. Es claro que podemos dar a $\mathrm{Hom}_K(F, E)$ estructura de E–espacio vectorial si definimos para $e \in E$ y para cada $\varphi \in \mathrm{Hom}_K(F, E)$

$$(e\varphi)(f) = e(\varphi(f)), \text{ para cada } f \in F.$$

Ahora podemos estudiar la dependencia o independencia lineal, sobre E, de los elementos del espacio vectorial $\mathrm{Hom}(F/K, E/K)$. El primer resultado que estudiamos es debido a Dedekind y caracteriza los conjuntos de elementos de $\mathrm{Hom}(F/K, E/K)$ que son linealmente independientes (sobre E).

Lema. 7.1. (Lema de independencia de Dedekind)
Sean F/K y E/K dos extensiones de cuerpos, cada familia de elementos de $\mathrm{Hom}(F/K, E/K)$ *es E–linealmente independiente en* $\mathrm{Hom}_K(F, E)$*, (sobre E), si y sólo, si todos sus elementos son distintos.*

DEMOSTRACIÓN. ($\Rightarrow$). Es inmediato.

($\Leftarrow$). Sea $\{\sigma_i \mid i \in I\}$ una familia de elementos distintos dos a dos de $\mathrm{Hom}(F/K, E/K)$. Si la familia consta de un sólo elemento σ_1, es claro que $\{\sigma_1\}$ es linealmente independiente. Supongamos ahora que cada subconjunto de menos de n elementos de la familia es linealmente independiente, y consideremos el conjunto $\{\sigma_1, \ldots, \sigma_n\} \subseteq \{\sigma_i \mid i \in I\}$, si $e_1\sigma_1 + \cdots + e_n\sigma_n$ es una combinación igual a cero con coeficientes $e_i \in E$, $1 \leq i \leq n$, entonces para cada $x \in F$ se puede escribir

$$e_1\sigma_1(x) + \cdots + e_n\sigma_n(x) = 0. \tag{II.1}$$

Ya que $\sigma_1 \neq \sigma_n$, existe $y \in F$ tal que $\sigma_1(y) \neq \sigma_n(y)$, por tanto podemos suponer $\sigma_n(y) \neq 0$. Consideramos las siguientes identidades

$$0 = e_1\sigma_1(xy) + \cdots + e_n\sigma_n(xy) = e_1\sigma_1(x)\sigma_1(y) + \cdots + e_n\sigma_n(x)\sigma_n(y).$$

Tenemos entonces

$$0 = e_1\sigma_1(x)\sigma_1(y)\sigma_n(y)^{-1} + \cdots + e_{n-1}\sigma_{n-1}(x)\sigma_{n-1}(y)\sigma_n(y)^{-1} + e_n\sigma_n(x). \tag{II.2}$$

4162-03.tex

La diferencia entre (II.1) y (II.2) es:

$$0 = [e_1 - e_1\sigma_1(y)\sigma_n(y)^{-1}]\sigma_1(x) + \cdots + [e_{n-1} - e_{n-1}\sigma_{n-1}(y)\sigma_n(g)^{-1}]\sigma_{n-1}(y).$$

Ya que es válido para cada $x \in F$, tenemos

$$0 = [e_1 - e_1\sigma_1(y)\sigma_n(y)^{-1}]\sigma_1 + \cdots + [e_{n-1} - e_{n-1}\sigma_{n-1}(y)\sigma_n(y)^{-1}]\sigma_{n-1},$$

que es una combinación lineal de $n-1$ miembros distintos de la familia, entonces todos los coeficientes son nulos, en particular

$$0 = e_1 - e_1\sigma_1(y)\sigma_n(y)^{-1} = e_1(1 - \sigma_1(y)\sigma_n(y)^{-1}),$$

esto es cierto si, y sólo si, $e_1 = 0$ ó $\sigma_1(y) = \sigma_n(y)$. La segunda posibilidad está en contra de la hipótesis, luego necesariamente $e_1 = 0$, y por tanto tenemos

$$e_2\sigma_2 + \cdots + e_n\sigma_n = 0,$$

que es otra vez una combinación lineal de $n-1$ miembros distintos de la familia, entonces todos los coeficientes son nulos, y tenemos el resultado. □

Podemos ahora contar los elementos de $\mathrm{Hom}(F/K, E/K)$ y relacionar este número con el grado de la extensión. En particular tenemos:

Corolario. 7.2.
En la situación anterior, si F/K es una extensión finita de grado $[F : K] = n$, entonces se verifica: $|\mathrm{Hom}(F/K, E/K)| \leq n$.

DEMOSTRACIÓN. Supongamos que en $\mathrm{Hom}(F/K, E/K)$ existen más de n elementos. Sean $\sigma_0, \ldots, \sigma_n$ elementos distintos de $\mathrm{Hom}(F/K, E/K)$. Si existe una combinación lineal con coeficientes en E igual a cero, por ejemplo

$$e_0\sigma_0 + e_1\sigma_1 + \cdots + e_n\sigma_n = 0,$$

para una base $\{f_1, \ldots, f_n\}$ de F como K–espacio vectorial se verifica:

$$\begin{cases} e_0\sigma_0(f_1) + e_1\sigma_1(f_1) + \cdots + e_n\sigma_n(f_1) = 0 \\ \vdots \\ e_0\sigma_0(f_n) + e_1\sigma_1(f_n) + \cdots + e_n\sigma_n(f_n) = 0 \end{cases}$$

y $e_0, e_1, \ldots, e_n$ es una solución del sistema

$$\begin{cases} X_0\sigma_0(f_1) + X_1\sigma_1(f_1) + \cdots + X_n\sigma_n(f_1) = 0 \\ \vdots \\ X_0\sigma_0(f_n) + X_1\sigma_1(f_n) + \cdots + X_n\sigma_n(f_n) = 0 \end{cases}$$

que tiene n ecuaciones y $n+1$ incógnitas. Por ser homogéneo, es compatible indeterminado y existe al menos una solución no trivial. Existen $e_0, e_1, \ldots, e_n \in E$, no todos nulos, que son una solución del sistema. Se verifica $e_0\sigma_0 + \cdots + e_n\sigma_n = 0$ y éstos no son linealmente independientes, por lo tanto no son distintos y necesariamente $|\mathrm{Hom}(F/K, E/K)|$ es menor o igual que n. □

Corolario. 7.3.
Si F/K es una extensión finita entonces $|\mathrm{Aut}(F/K)| \leq [F : K]$.

Vamos a contar ahora el número de homomorfismos de cuerpos de una extensión finita F/K a una clausura algebraica $\overline{K}$ de K.

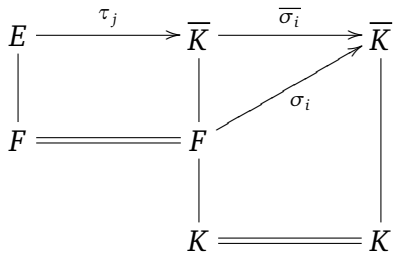
Proposición. 7.4.
Si $K \subseteq F \subseteq E$ es una torre de extensiones finitas de cuerpos y $\overline{K}$ es una clausura algebraica de K que contiene a E, se verifica:

$$|\mathrm{Hom}(E/F, \overline{K}/F)| \cdot |\mathrm{Hom}(F/K, \overline{K}/K)| = |\mathrm{Hom}(E/K, \overline{K}/K)|.$$

DEMOSTRACIÓN. Sean $\mathrm{Hom}(E/F, \overline{K}/F) = \{\tau_1, \ldots, \tau_t\}$ y $\mathrm{Hom}(F/K, \overline{K}/K) = \{\sigma_1, \ldots, \sigma_s\}$, para cada σ_i, $1 \leq i \leq s$, existe una extensión de σ_i a $\overline{K}$, a la que llamaremos $\overline{\sigma_i}$; cada $\overline{\sigma_i}$ es un automorfismo. Podemos definir entonces homomorfismos de E/K a $\overline{K}/K$ mediante $\overline{\sigma_i}\tau_j$, para $1 \leq i \leq s$, $1 \leq j \leq t$. Vamos a ver que si $i \neq h$ y $j \neq k$, entonces $\overline{\sigma_i}\tau_j \neq \overline{\sigma_h}\tau_k$. Supongamos que $\overline{\sigma_i}\tau_j = \overline{\sigma_h}\tau_k$, entonces para cada $f \in F$ se verifica:

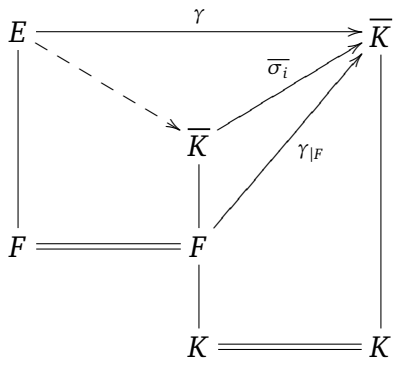
$$\sigma_i(f) = \overline{\sigma_i}\tau_j(f) = \overline{\sigma_h}\tau_k(f) = \sigma_h(f),$$

luego $\overline{\sigma_i} = \overline{\sigma_h}$. Tenemos pues $\overline{\sigma_i}\tau_j = \overline{\sigma_i}\tau_k$ y, ya que $\overline{\sigma_i}$ es un automorfismo, se verifica $\tau_j = \tau_k$.



Falta probar que todo homomorfismo de E/K a $\overline{K}/K$ es de esta forma. Sea $\gamma \in \mathrm{Hom}(E/K, \overline{K}/K)$, si $\gamma = \overline{\sigma_i}\tau_j$, se debe verificar $\tau_j = (\overline{\sigma_i})^{-1}\gamma$, y éste debe ser un homomorfismo de E/F a $\overline{K}/F$. Vamos a

ver cómo definimos σ_i. Ya que para cada $f \in F$ se ha de verificar $f = \tau_j(f) = (\overline{\sigma_i})^{-1}\gamma(f)$, tenemos que $\gamma(f) = \overline{\sigma_i}(f)$, podemos tomar $\sigma_i = \gamma_{|F}$, con esta elección el resultado es inmediato.

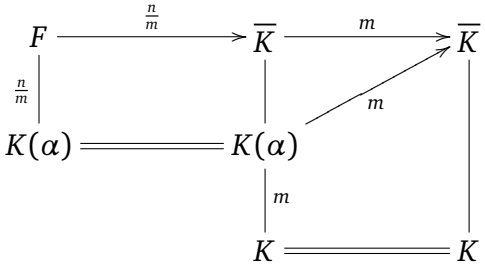


□

En particular, si F/K es una extensión finita, el número de elementos de $\mathrm{Hom}(F/K, \overline{K}/K)$ nos permite dar una condición necesaria y suficiente sobre la separabilidad de la extensión. Así tenemos:

Lema. 7.5.
Sea F/K una extensión finita y $\overline{K}$ una clausura algebraica de K que contiene a F, son equivalentes:
(a) F/K es separable.
(b) $|\mathrm{Hom}(F/K, \overline{K}/K)| = [F : K]$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Ya conocemos que $|\mathrm{Hom}(F/K, \overline{K}/K)| \leq [F : K]$. Si la extensión F/K es separable y $[F : K] = 1$, el resultado es cierto. Supongamos que también es cierto para toda extensión L/K de grado menor que n, y sea $[F : K] = n$. Consideramos $\alpha \in F \setminus K$, y llamamos $f(X) = \mathrm{Irr}(\alpha, K)$, con $\mathrm{gr}(f(X)) = m > 1$. Tenemos una torre de cuerpos $K \subseteq K(\alpha) \subseteq F$ y $[F : K(\alpha)] = n/m < n$. Ya que $\overline{K}$ es también una clausura algebraica de $K(\alpha)$, podemos aplicar la hipótesis de inducción, y por tanto $|\mathrm{Hom}(F/K(\alpha), \overline{K}/K(\alpha))| = n/m$. Por otro lado, ya que α es separable sobre K, el polinomio $f(X)$ tiene exactamente m raíces, y como consecuencia existen m homomorfismos de $K(\alpha)/K$ en $\overline{K}/K$, ya que la imagen de α ha de ser una raíz de $f(X)$ y para cada raíz de $f(X)$ tenemos un homomorfismo; así pues $|\mathrm{Hom}(K(\alpha)/K, \overline{K}/K)| = m$. Aplicando la Proposición (7.4.) tenemos $|\mathrm{Hom}(F/K, \overline{K}/K)| = m(n/m) = n$.



(b) $\Rightarrow$ (a). Si F/K es una extensión finita de grado n no es separable entonces existe $\alpha \in F$ tal que $f(X) = \mathrm{Irr}(\alpha, F)$ no es separable sobre K, y por tanto el número de raíces distintas m_0 de $f(X)$ es menor que $m = \mathrm{gr}(f(X))$ y $|\mathrm{Hom}(K(\alpha)/K, \overline{K}/K)| = m_0 < m$. Tenemos $|\mathrm{Hom}(F/K(\alpha), \overline{K}/K(\alpha))| \leq [F : K(\alpha)] = n/m$, luego

$$\begin{aligned} n &= |\mathrm{Hom}(F/K, \overline{K}/K)| \\ &= |\mathrm{Hom}(F/K(\alpha), \overline{K}/K)| \cdot |\mathrm{Hom}(K(\alpha)/K, \overline{K}/K)| \\ &< (n/m)m = n, \end{aligned}$$

lo que es una contradicción. □

Corolario. 7.6.
Sea $K \subseteq F \subseteq E$ una torre de extensiones finitas, son equivalentes:

(a) E/K es separable.
(b) E/F y F/K son separables.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Ya fue probado.
(b) $\Rightarrow$ (a). Consideramos una clausura algebraica $\overline{K}$ de K que contenga a E. Por ser F/K separable tenemos $|\mathrm{Hom}(F/K, \overline{K}/K)| = [F : K]$. Por ser E/F separable tenemos $|\mathrm{Hom}(E/F, \overline{K}/F)| = [E : F]$. Juntando ambos resultados tenemos:

$$\begin{aligned} [E : K] &= [E : F][F : K] \\ &= |\mathrm{Hom}(E/F, \overline{K}/K)| \cdot |\mathrm{Hom}(F/K, \overline{K}/K)| \\ &= |\mathrm{Hom}(E/K, \overline{K}/K)|, \end{aligned}$$

entonces E/K es una extensión separable. □

Como consecuencia, para cada extensión F/K, y cada elemento $\alpha \in F$ se tiene α es separable sobre K si, y sólo si, la extensión $K(\alpha)/K$ es separable, y en general tenemos el siguiente corolario.

Corolario. 7.7.
Una extensión algebraica $F = K(\alpha_1, \ldots, \alpha_n)$ es separable si, y sólo si, los elementos $\alpha_1, \ldots, \alpha_n$ son separables sobre K.

Siguiendo con la relación existente entre el grado de una extensión y el número de automorfismos, tenemos que siguiente resultado.

Teorema. 7.8. (Teorema de Artin)
Sea E un cuerpo y $G \subseteq \mathrm{Aut}(E)$ un grupo finito de automorfismos de E, entonces el conjunto

$$E^G = \{e \in E \mid \ \sigma(e) = e \text{ para todo } \sigma \in G\}$$

es un subcuerpo de E y verifica $[E : E^G] = |G|$.

DEMOSTRACIÓN. Es fácil probar que E^G es un subcuerpo de E. Para probar la igualdad procedemos como sigue: ya que $G \subseteq \mathrm{Hom}(E/E^G, E/E^G)$, si E/E^G es finita se verifica

$$|G| \leq |\mathrm{Hom}(E/E^G, E/E^G)| \leq [E : E^G],$$

y si E/E^G no es finita, es claro que $|G| \leq [E : E^G]$. Falta pues probar la otra desigualdad. Supongamos que $G = \{\sigma_1, \ldots, \sigma_n\}$ son los elementos de G. Si $e_0, e_1, \ldots, e_n \in E$ son *linealmente independientes sobre el cuerpo E^G*, entonces el sistema homogéneo

$$\begin{cases} \sigma_1(e_0)X_0 + \cdots + \sigma_1(e_n)X_n = 0 \\ \vdots \\ \sigma_n(e_0)X_0 + \cdots + \sigma_n(e_n)X_n = 0, \end{cases}$$

tiene n ecuaciones y $n+1$ incógnitas, por lo tanto es compatible indeterminado y tiene *solución no trivial en E*. Supongamos que tenemos una solución *con el menor número de términos no nulos*; ya que podemos ordenar los elementos $e_0, e_1, \ldots, e_n$ según queramos, podemos suponer que la solución es $s_0, s_1, \ldots, s_n$ con $s_0, s_1, \ldots, s_t$ no nulos y $s_{t+1} = \cdots = s_n = 0$. Se verifica:

$$\begin{cases} \sigma_1(e_0)s_0 + \cdots + \sigma_1(e_n)s_n = 0 \\ \vdots \\ \sigma_n(e_0)s_0 + \cdots + \sigma_n(e_n)s_n = 0, \end{cases} \qquad (*1)$$

si aplicamos un elemento $\sigma \in G$ a estas expresiones, tenemos

$$\begin{cases} \sigma\sigma_1(e_0)\sigma(s_0) + \cdots + \sigma\sigma_1(e_n)\sigma(s_n) = 0 \\ \vdots \\ \sigma\sigma_n(e_0)\sigma(s_0) + \cdots + \sigma\sigma_n(e_n)\sigma(s_n) = 0, \end{cases}$$

y ya que $\sigma\sigma_i$, para $1 \leq i \leq n$, recorre todos los elementos de G, tenemos

$$\begin{cases} \sigma_1(e_0)\sigma(s_0) + \cdots + \sigma_1(e_n)\sigma(s_n) = 0 \\ \vdots \\ \sigma_n(e_0)\sigma(s_0) + \cdots + \sigma_n(e_n)\sigma(s_n) = 0, \end{cases} \qquad (*2)$$

Multiplicamos (*1) por $\sigma(s_0)$ y restamos (*2) multiplicado por s_0, obtenemos

$$\begin{cases} \sum_{i=0}^{n}[\sigma_1(e_i)s_i\sigma(s_0)-\sigma_1(e_i)\sigma(s_i)s_0]=0 \\ \vdots \\ \sum_{i=0}^{n}[\sigma_n(e_i)s_i\sigma(s_0)-\sigma_n(e_i)\sigma(s_i)s_0]=0 \end{cases}$$

Agrupando los elementos tenemos

$$\begin{cases} \sum_{i=0}^{n}\sigma_1(e_i)[s_i\sigma(s_0)-\sigma(s_i)s_0]=0 \\ \vdots \\ \sum_{i=0}^{n}\sigma_n(e_i)[s_i\sigma(s_0)-\sigma(s_i)s_0]=0 \end{cases}$$

Por lo tanto, si llamamos $\bar{s}_i = s_i\sigma(s_0)-\sigma(s_i)s_0$, $1 \leq i \leq t$, resulta que $\bar{s}_0 = 0 = \bar{s}_{t+1} = \cdots = \bar{s}_n$, $\bar{s}_1, \ldots, \bar{s}_t$, es también una solución al sistema y tiene un elemento menos no nulo. Tenemos una solución $\overline{s_0}, \ldots, \overline{s_n}$ para cada uno de los $\sigma \in G$. Si todas fuesen iguales a cero, entonces $\sigma(s_i/s_0) = s_i/s_0$ para cada $\sigma \in G$, llegamos a que $s_i/s_0 \in E^G$; supongamos ahora que $\mathrm{id}_E = \sigma_1$, entonces, en (*1), la primera expresión es:

$$e_0s_0 + e_1s_1 + \cdots + e_ts_t = 0,$$

de donde se deduce que

$$e_0 = -(s_1/s_0)e_1 - \cdots - (s_t/s_0)e_t,$$

y e_0 es una combinación lineal, con coeficientes en E^G, de $e_1, \ldots, e_t$, lo que es una contradicción.
Al obtener una solución del sistema con menos elementos nulos, llegamos a una contradicción con la elección de la solución $s_0, s_1, \ldots, s_n$. Como consecuencia no pueden existir $n+1$ elementos en E, linealmente independientes sobre E^G, por tanto $[E : E^G] \leq n = |G|$. Entonces $|G| = [E : E^G]$. □

7.1. Ejercicios

Automorfismos de extensiones

Ejercicio. 7.9.
Sea K un cuerpo de característica cero, y G el grupo de automorfismos generado por $\eta : K(X) \to K(X)$, definido $\eta(X) = X + 1$. Demuestra que G es un grupo cíclico infinito, calcula el cuerpo fijo F de $K(X)$ bajo G, y calcula $[K(X) : F]$.
Ref.: 4162e_033 SOLUCIÓN

Ejercicio. 7.10.
Si K es un cuerpo perfecto, demuestra que el cuerpo fijo de K bajo todos los automorfismos de K es perfecto.
Ver el Ejercicio (6.17.).
Ref.: 4162e_034 SOLUCIÓN

Ejercicio. 7.11.
Sea E/K una de las siguientes extensiones de cuerpos:
(1) $K = \mathbb{Q}(t)$, $E = \mathbb{Q}(t, i)$
(2) $K = \mathbb{Q}(t^2)$, $E = \mathbb{Q}(t, i)$ *donde t es transcendente sobre $\mathbb{Q}$ e $i^2 = -1$.*

Calcula $G = \mathrm{Aut}(E/K)$, el grupo de automorfismos de E/K; determina el cuerpo fijo F bajo los automorfismos de G y calcula el grado $[E : F]$.
Ref.: 4162e_035 SOLUCIÓN

Ejercicio. 7.12.
Sea E un cuerpo con infinitos elementos, G un grupo finito de automorfismos de E y F el cuerpo fijo por G. Razona que F es necesariamente infinito.
Ref.: 4162e_036 SOLUCIÓN

Ejercicio. 7.13.
Calcula los grupos de automorfismos $\mathrm{Aut}(E/\mathbb{Q})$ *y* $\mathrm{Aut}(F/\mathbb{Q})$, *para* $E=\mathbb{Q}(\omega,\sqrt[3]{2})$ *y* $F=\mathbb{Q}(\omega,\sqrt[3]{2},\sqrt[3]{5})$.
Ref.: 4162e_037 SOLUCIÓN

Ejercicio. 7.14.
Para las siguientes extensiones de $\mathbb{Q}$ *y los siguientes* $\mathbb{Q}$*–automorfismos, calcula los cuerpos fijos.*

(1) $E=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$, $\quad\sigma_1:\sqrt{2}\mapsto-\sqrt{2};\ \sqrt{3}\mapsto\sqrt{3};\ \sqrt{5}\mapsto\sqrt{5}$.
(2) $E=\mathbb{Q}(\sqrt{2},\sqrt{-2})$ $\quad\sigma_2:\sqrt{2}\mapsto\sqrt{2};\ \sqrt{-2}\mapsto-\sqrt{-2}$.
(3) $E=\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$, $\quad\sigma_3:\sqrt{2}\mapsto-\sqrt{2};\ \sqrt[3]{2}\mapsto\sqrt[3]{2}$.
(4) $E=\mathbb{Q}(\omega,\sqrt[3]{2})$, $\quad\sigma_4:\sqrt[3]{2}\mapsto\omega\sqrt[3]{2};\ \omega\mapsto\omega$.

Ref.: 4162e_038 SOLUCIÓN

Ejercicio. 7.15.
Sea K *un cuerpo, y considera los automorfismos de* $K(X)/K$,

$$\sigma_1:X\mapsto 1-X \quad y \quad \sigma_2:X\mapsto 1/X.$$

(1) *Demuestra que el grado de* $K(X)$ *sobre* $F=K(X)^H$, *el cuerpo fijo de* $H=\langle\sigma_1,\sigma_2\rangle$, *es 6.*
(2) *Comprueba que* $\alpha=(X^2-X+1)^3/(X^2-X)^2$ *pertenece a* F *y usa este hecho para encontrar un polinomio con coeficientes en* F *del que* X *sea raíz.*

Ref.: 4162e_039 SOLUCIÓN

Ejercicio. 7.16.
Sea K *un cuerpo y* t *un elemento trascendente sobre* K. *Determina*

$$\left[K(t):K\left(\frac{t^2}{t-1}\right)\right] \quad y \quad \mathrm{Aut}\left(K(t)/K\left(\frac{t^2}{t-1}\right)\right).$$

Ref.: 4162e_083 SOLUCIÓN

Ejercicio. 7.17.
Sean $f, g \in K[X]$ polinomios primos relativos, no constantes. Demuestra que se verifica:

(1) X es algebraico sobre $K(f/g)$.
(2) $[K(X) : K(f/g)] = \max\{\text{grad}(f), \text{grad}(g)\}$.
(3) Si $E \neq K$ es un cuerpo intermedio, $K \subseteq E \subseteq K(X)$, entonces $[K(X) : E]$ es finito.
(4) El homomorfismo $\varphi : K(X) \longrightarrow K(X)$, definido $\varphi(X) = f/g$, con $f, g \in K[X]$ no constantes primos relativos, es un K–automorfismo si, y sólo si, $\max\{\text{grad}(f), \text{grad}(g)\} = 1$.
(5) $\text{Aut}(K(X)/K)$ está formado por todos los K–automorfismos inducidos por $X \mapsto \dfrac{aX+b}{cX+d}$, con $a, b, c, d \in K$ y $ad - bc \neq 0$.

Ref.: 4162e_109 SOLUCIÓN

Ejercicio. 7.18.
Sea E un cuerpo y $\{\varphi_1, \ldots, \varphi_n\}$ un conjunto de n automorfismos distintos de E. Llamamos $K = \{e \in E \mid \varphi_i(e) = e, 1 \leq i \leq n\}$. Demuestra que $[E : K] \geq n$
Ref.: 4162e_110 SOLUCIÓN

Ejercicio. 7.19.
Sea E/K una extensión de cuerpos (algebraica y normal) y $f \in K[X]$ un polinomio irreducible. Si $f = f_1 f_2$ es una factorización en dos irreducibles en $E[X]$,

(1) Prueba que existe un automorfismo $\sigma : E/K \longrightarrow E/K$ tal que $f_1^\sigma = f_2$, y por tanto $f_2^\sigma = f_1$.
(2) Considera el polinomio $f = X^4 - 2 = \mathbb{Q}[X]$, y el cuerpo $E = \mathbb{Q}(\sqrt{2})$. En E/K tenemos la factorización en irreducibles $f = X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2}) = f_1 f_2$. Describe σ en este caso.
(3) Justifica que $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ son extensiones normales y que $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no lo es.
(4) Determina la clausura normal $F/\mathbb{Q}$ de $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.
(5) Calcula el grupo $\text{Aut}(F/\mathbb{Q})$, y los automorfismos que dejan fijo a $\mathbb{Q}(\sqrt{2})$.

Nota: Ver también los ejercicios (5.37.) y (5.26.)
Ref.: 4162e_139 SOLUCIÓN

Grados de separabilidad e inseparabilidad. Extensiones puramente separables

Ejercicio. 7.20.
Sea F/K una extensión algebraica. Definimos

$$F_s = \{\alpha \in F \mid \alpha \text{ es separable sobre } K\}.$$

Demuestra que F_s/K es una extensión separable.
Ref.: 4162e_075 SOLUCIÓN

Ejercicio. 7.21.
Sea F/K una extensión algebraica. Se llama ***grado de separabilidad*** *de F/K a $[F_s : K]$, y se representa por $[F : K]_s$.*
Demuestra que $[F : K]_s$ es igual al cardinal de $\mathrm{Hom}(F/K, \overline{K}/K)$.
Ref.: 4162e_076 SOLUCIÓN

Ejercicio. 7.22.
Sea $F(K$ una extensión algebraica. Se llama ***grado de inseparabilidad*** *de F/K a $[F : F_s]$, y se representa por $[F : K]_i$.*
Sea $K \subseteq F \subseteq E$ una torre de extensiones algebraicas, demuestra que se verifica:

$$[E : F]_s[F : K]_s = [E : K]_s.$$
$$[E : F]_i[F : K]_i = [E : K]_i.$$

Ref.: 4162e_077 SOLUCIÓN

Ejercicio. 7.23.
Sea $f(X) \in K[X]$ un polinomio irreducible sobre K, y F el cuerpo de descomposición de $f(X)$ sobre K. Si α es una raíz de $f(X)$, prueba que la multiplicidad de α, y por tanto de todas las demás raíces de $f(X)$, es $[K(\alpha) : K]_i$.
Ref.: 4162e_078 SOLUCIÓN

Ejercicio. 7.24.
Sea F/K una extensión algebraica; un elemento $\alpha \in F$ es ***puramente inseparable*** *sobre K si* $\mathrm{Irr}(\alpha.K)$ *es una potencia de un polinomio lineal en $F[X]$, esto es,* $\mathrm{Irr}(\alpha, K) = (X-\alpha)^n$
Demuestra que un elemento $\alpha \in F$ es separable y puramente inseparable sobre K si, y sólo si, $\alpha \in K$.
Ref.: 4162e_079 SOLUCIÓN

Ejercicio. 7.25.
Una extensión algebraica F/K es ***puramente inseparable*** *si todo elemento de F es puramente inseparable sobre K.*
Si K es un cuerpo de característica $p \neq 0$, para cada extensión algebraica F/K son equivalentes:
(a) F/K es puramente inseparable.
(b) Para cada $\alpha \in F$ se tiene que $\mathrm{Irr}(\alpha, K)$ *es de la forma $X^{p^n} - a \in K[X]$.*
(c) Si $\alpha \in F$, existe $n \in \mathbb{N}$ tal que $\alpha^{p^n} \in K$.
(d) Los únicos elementos de F separables sobre K son los elementos de K.
(e) F está generado sobre K por un conjunto de elementos puramente inseparables.

Ref.: 4162e_080 SOLUCIÓN

Ejercicio. 7.26.
Demuestra que si K un cuerpo de característica $p \neq 0$ y F/K una extensión algebraica finita puramente inseparable, entonces $[F : K] = p^n$, para algún $n \in \mathbb{N}$.
Ref.: 4162e_081 SOLUCIÓN

Ejercicio. 7.27.
Sea K un cuerpo de característica $p \neq 0$ y F/K una extensión algebraica; definimos

$$F_i = \{\alpha \in F \mid \alpha \text{ es puramente inseparable sobre } K\}.$$

Demuestra que:
(1) F_s/K es una extensión separable.

(2) F/F_s *es una extensión puramente inseparable.*
(3) F_i/K *es una extensión puramente inseparable.*
(4) $F_s \cap F_i = K$.
(5) F/F_i *es separable si, y sólo si,* $F = F_s F_i$.

Ref.: 4162e_082 *SOLUCIÓN*

8. Extensiones finitas de Galois

Supongamos que E es un cuerpo y $G \subseteq \mathrm{Aut}(E)$ es un grupo de automorfismos de E. Para cada subgrupo $H \subseteq G$ definimos:

$$E^H = \{x \in E \mid \sigma(x) = x \text{ para todo } \sigma \in H\}.$$

Y para cada subcuerpo $F \subseteq E$ definimos:

$$G^F = \{\sigma \in H \mid \sigma(x) = x \text{ para todo } x \in F\}.$$

Ya conocemos que E^H es un subcuerpo de E, y es fácil probar que G^F es un subgrupo de G. Llamamos a E^H el **cuerpo fijo** de H y a G^F se llama el **subgrupo de los F-automorfismos** de E en G.
Si llamamos $\mathscr{K}(E)$ al conjunto de los subcuerpos de E y $\mathscr{G}(G)$ al conjunto de los subgrupos de G. En cada uno de estos conjuntos consideramos la relación de orden, definida por la inclusión conjuntista. Existen dos aplicaciones

$$G^{(-)} : \mathscr{K}(E) \longrightarrow \mathscr{G}(G); F \mapsto G^F$$
$$E^{(-)} : \mathscr{G}(G) \longrightarrow \mathscr{K}(E); H \mapsto E^H,$$

que verifican las siguientes propiedades.

Lema. 8.1.
En la situación anterior se tiene:
(1) Si $F_1 \subseteq F_2$, entonces $G^{F_1} \supseteq G^{F_2}$, para cualesquiera $F_1, F_2 \in \mathscr{K}(E)$.
(1′) Si $H_1 \subseteq H_2$, entonces $E^{H_1} \supseteq E^{H_2}$, para cualesquiera $H_1, H_2 \in \mathscr{G}(G)$.
(2) $F \subseteq E^{(G^F)}$ para cada $F \in \mathscr{K}(E)$.
(2′) $H \subseteq G^{(E^H)}$ para cada $H \in \mathscr{G}(G)$.
(3) $E^{(G^{(E^H)})} = E^H$, para cada $H \in \mathscr{G}(G)$.
(3′) $G^{(E^{(G^F)})} = G^F$, para cada $F \in \mathscr{K}(E)$.

DEMOSTRACIÓN. (1). Si $F_1 \subseteq F_2$, para $x \in G^{F_2}$, se tiene que para cada $\sigma \in F_2$, entonces $\sigma(x) = x$, luego en particular, para cada $\sigma \in F_1$, se tiene $\sigma(x) = x$, y por tanto $x \in G^{F_1}$.
(2). Si $x \in F$, entonces para cada $\sigma \in G^F$ se tiene $\sigma(x) = x$, y esto ocurre si, y sólo si, $x \in E^{(G^F)}$.
(3). Aplicando (2) tenemos $E^H \subseteq E^{(G^{(E^H)})}$. También aplicando (2′) tenemos $H \subseteq G^{(E^H)}$, luego por (1′) se tiene la inclusión $E^{(G^{(E^H)})} \subseteq E^H$; juntando ambas obtenemos la igualdad. □

Las aplicaciones $E^{(-)}$ y $G^{(-)}$ se dice que definen una **conexión de Galois** entre $\mathscr{K}(E)$ y $\mathscr{G}(G)$.
Vamos a buscar condiciones sobre subcuerpos F de E y subgrupos H de G para que se verifiquen las propiedades siguientes:

4162-04.tex

(C-1) $G^{E^H} = H$.
(C-2) $E^{G^F} = F$.

Existe una biyección entre los subcuerpos que verifican **(C-2)** y los subgrupos que verifican **(C-1)** dada por $F \mapsto G^F$, y su inversa está definida por $H \mapsto E^H$. Además los subcuerpos que verifican **(C-2)** forman un subretículo de $\mathscr{K}(E)$ y los subgrupos que verifican **(C-1)** forman un subretículo de $\mathscr{G}(G)$. Para determinar estos subcuerpos y subgrupos necesitamos antes algunas definiciones.

Veamos ahora el caso de extensiones finitas.
Una extensión finita de cuerpos E/K se llama una **extensión de Galois** si existe un subgrupo $G \subseteq \mathrm{Aut}(E)$ tal que $K = E^G$. Una extensión de Galois E/K se puede caracterizar mediante propiedades intrínsecas a E/K.

Teorema. 8.2. (Caracterización de extensiones de Galois)
Sea E/K una extensión finita, son equivalentes:
(a) E/K es una extensión de Galois.
(b) E/K es una extensión normal y separable.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Sea E/K una extensión de Galois con $K = E^G$ para un subgrupo $G \subseteq \mathrm{Aut}(E)$.
Recordemos que una extensión E/K es separable si, y sólo si, $|\mathrm{Hom}(E/K, \overline{K}/K))| = [E : K]$. Por el Lema de Artin tenemos $[E : K] = [E : E^G] = |G|$, y sabemos que $|\mathrm{Aut}(E/K)| \leq [E : K]$; ya que $G \subseteq \mathrm{Aut}(E/K)$ se tiene $[E : K] = |G| \leq |\mathrm{Aut}(E/K)| \leq [E : K]$.
Cada elemento de $\mathrm{Aut}(E/K)$ se prolonga a un homomorfismo hasta $\overline{K}/K$, y por tanto

$$|\mathrm{Hom}(E/K, \overline{K}/K)| \geq |G| = [E : K],$$

la otra desigualdad se deduce, por ejemplo, del corolario al lema de Dedekind. Como consecuencia E/K es separable.
Dado un morfismo $\sigma : E/K \longrightarrow \overline{K}/K$, ya que σ proviene de un automorfismo de E/K, tenemos que $E^\sigma = E$, y E/K es una extensión normal.
(b) $\Rightarrow$ (a). Si suponemos que E/K es una extensión normal y separable y $[E : K] = n$; por ser separable tenemos $|\mathrm{Hom}(E/K, \overline{K}/K)| = n$; y por ser normal E/K, tenemos que $E^\sigma = E$, para cada $\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$, y restringiendo el codominio obtenemos: $|\mathrm{Hom}(E/K, E/K)| = n$; por ser E/K una extensión algebraica $\mathrm{Hom}(E/K, E/K) = \mathrm{Aut}(E/K)$, y se tiene $|\mathrm{Aut}(E/K)| = n$. Si llamamos $G = \mathrm{Aut}(E/K)$ y $F = E^G$, se tiene $K \subseteq F \subseteq E$; por el teorema de Artin, $[E : F] = |G| = n$ y $F = K$, esto es, E/K es una extensión de Galois. □

Corolario. 8.3.
Sea $K \subseteq F \subseteq E$ una torre de extensiones finitas, si E/K es una extensión de Galois, entonces E/F es una extensión de Galois.

Más adelante veremos una condición necesaria y suficiente para que la extensión F/K sea también una extensión de Galois. En general F/K no es una extensión de Galois, como el siguiente ejemplo prueba.

Ejemplo. 8.4.
Se considera las extensiones $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$, donde ω es una raíz cúbica primitiva de la unidad. La extensión $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ es de Galois, y también lo es $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})$, pero la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es de Galois.

El siguiente resultado nos proporciona otra caracterización interesante de las extensiones finitas de Galois.

Teorema. 8.5.
Sea E/K una extensión finita, son equivalentes:
(a) E/K es una extensión de Galois.
(b) E es el cuerpo de descomposición de un polinomio separable sobre K.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Ya que E/K es una extensión normal, resulta que E es el cuerpo de descomposición de un polinomio $f(X) \in K[X]$, ya que E/K es una extensión separable, resulta que $f(X)$ es separable sobre K.
(b) $\Rightarrow$ (a). Si E es el cuerpo de descomposición de un polinomio $f(X) \in K[X]$, separable sobre K, entonces E/K es una extensión normal, además por ser $f(X)$ separable sobre K, resulta que E/K es una extensión separable. □

Como consecuencia tenemos un método fácil de construir extensiones de Galois. Así, si K es un cuerpo perfecto, para cada polinomio irreducible $f(X)$, su cuerpo de descomposición es una extensión de Galois. En particular, $\mathbb{Q}(\sqrt[5]{2}, \xi)/\mathbb{Q}$, el cuerpo de descomposición de $f(X) = X^5 - 2$, es una extensión de Galois de $\mathbb{Q}$.
Si E/K es una extensión finita de Galois, llamamos **grupo de Galois** de E/K al grupo

$$\mathrm{Aut}(E/K) = \{\sigma \in \mathrm{Aut}(E) \mid \ \sigma(x) = x, \text{ para cada } x \in K\},$$

y se representa por $\mathrm{Gal}(E/K)$.

Proposición. 8.6.
Sea E/K una extensión finita de Galois con grupo de Galois $G = \mathrm{Gal}(E/K)$, se verifica:
(1) $K = E^G$.
(2) G es el único subgrupo de $\mathrm{Aut}(E)$ tal que $K = E^G$.

DEMOSTRACIÓN. (1). Es claro de la definición.
(2). Si $H \subseteq \mathrm{Aut}(E)$ verifica $K = E^H$, entonces $H \subseteq G$. Por el teorema de Artin $|H| = [E : E^H] = [E : K] = |G|$, y por tanto $H = G$. □

Corolario. 8.7.
Si E/K una extensión finita, son equivalentes:
(a) E/K es una extensión de Galois.
(b) $K = E^G$, para $G = \mathrm{Aut}(E/K) \subseteq \mathrm{Aut}(E)$.

Teorema. 8.8. (Teorema Fundamental de la Teoría de Galois)
Sea E/K una extensión finita de Galois con grupo de Galois $G = \mathrm{Gal}(E/K)$. Llamamos $\mathscr{K}(E/K)$ al retículo de las extensiones F/K con $K \subseteq F \subseteq E$. Consideramos la conexión de Galois entre $\mathscr{K}(E/K)$ y $\mathscr{G}(G)$ definida

$$H \mapsto E^H,$$
$$F \mapsto G^F.$$

La conexión de Galois establece una biyección, que invierte el orden, entre $\mathscr{K}(E/K)$ y $\mathscr{G}(\mathrm{Gal}(E/K))$.

DEMOSTRACIÓN. Dada una sub–extensión F/K de E/K, ya que E/K es normal y separable, también E/F es normal y separable, y por tanto de Galois. Consideramos

$$G^F = \{\sigma \in \mathrm{Gal}(E/K) \mid \sigma(x) = x, \text{ para cada } x \in F\},$$

este grupo es precisamente $\mathrm{Gal}(E/F)$, que por el Corolario (8.7.) está unívocamente determinado. Se tiene que $F = E^{\mathrm{Gal}(E/F)}$.
Dado un subgrupo $H \subseteq G = \mathrm{Gal}(E/K)$, tenemos que E^H es un subcuerpo de E, y que E/E^H es una extensión de Galois, ya que es normal y separable; su grupo de Galois, $\mathrm{Gal}(E/E^H)$, es precisamente H debido a la Proposición (8.6.). Tenemos pues la biyección anunciada.

$$F \mapsto \mathrm{Gal}(E/F) \mapsto F = E^{\mathrm{Gal}(E/F)}.$$
$$H \mapsto \quad E^H \quad \mapsto H = \mathrm{Gal}(E/E^H).$$

□

Veamos algunas consecuencias de la conexión de Galois en una extensión de Galois.

Observación. 8.9.
Sea E/K una extensión de Galois.
(1) Si F/K es una extensión intermedia, $K \subseteq F \subseteq E$, y si $\mathrm{Gal}(E/F) = H$, entonces se verifica:

$$[E : F] = |H|.$$

$$[F : K] = \frac{[E : K]}{[E : F]} = \frac{|G|}{|H|} = (G : H).$$

(2) Ya que la conexión de Galois es un homomorfismo de retículos que invierte el orden, para F_1/K, F_2/K extensiones intermedias, se verifica:

$$\mathrm{Gal}(E/F_1F_2) = \mathrm{Gal}(E/F_1) \cap \mathrm{Gal}(E/F_2).$$

$$\mathrm{Gal}(E/(F_1 \cap F_2)) = \mathrm{Gal}(E/F_1) \vee \mathrm{Gal}(E/F_2).$$

Teorema. 8.10.
Sea E/K una extensión de Galois, y sea $G = \mathrm{Gal}(E/K)$. Si H_1, H_2 son los subgrupos de G que corresponden a los cuerpos intermedios F_1 y F_2 respectivamente. Son equivalentes:

(a) H_1 y H_2 son subgrupos de G conjugados.
(b) F_1 y F_2 son cuerpos conjugados; existe $\sigma \in \mathrm{Gal}(E/K)$ tal que $F_1 = \sigma(F_2)$.

Como consecuencia si F es un cuerpo intermedio, son equivalentes:

(a) F/K es una extensión de Galois.
(b) $\mathrm{Gal}(E/F)$ es un subgrupo normal de G.

Además en este caso existe un isomorfismo $\mathrm{Gal}(F/K) \cong G/\mathrm{Gal}(E/F)$.

DEMOSTRACIÓN. Por definición $H_i = \{\sigma \in \mathrm{Gal}(E/K) \mid \ \sigma(x) = x \text{ para todo } x \in F_i\} = \mathrm{Gal}(E/F_i)$, $1 \leq i \leq 2$.
(a) $\Rightarrow$ (b). Si H_1 y H_2 son conjugados, entonces existe $\sigma \in G$ tal que $H_1 = \sigma H_2 \sigma^{-1}$, ó equivalentemente $H_2 = \sigma^{-1} H_1 \sigma$.
Para $x \in F_2$ y $h \in H_1$ se tiene $x = \sigma^{-1} h \sigma(x)$, por tanto $\sigma(x) = h\sigma(x)$, y tenemos que $\sigma(x) \in F_1$, luego $\sigma(F_2) \subseteq F_1$. De forma análoga $\sigma^{-1}(F_1) \subseteq F_2$. En consecuencia, $F_1 = \sigma(F_2)$.
(b) $\Rightarrow$ (a). Supongamos que $F_1 = \sigma(F_2)$ para $\sigma \in \mathrm{Gal}(E/K)$.
Para $h \in H_1$ y $x \in F_2$ tenemos $h(\sigma(x)) = \sigma(x)$, luego $\sigma^{-1} h \sigma(x) = x$, y por tanto $\sigma^{-1} h \sigma \in H_2$; luego $\sigma^{-1} H_1 \sigma \subseteq H_2$. De forma análoga $\sigma H_2 \sigma^{-1} \subseteq H_1$. En consecuencia, $H_1 = \sigma H_2 \sigma^{-1}$. □
Para probar la segunda parte veamos algunos pequeños hechos para un cuerpo intermedio $K \subseteq F \subseteq E$.

Hecho 1 La extensión F/K es siempre separable, y es de Galois si, y sólo si, es normal, esto es; para cada morfismo $\sigma : F/K \longrightarrow \overline{K}/K$, se tiene $\sigma(F) = F$.

F/K es de Galois si, y sólo si, $\sigma(F) = F$ para cada $\sigma : F/K \longrightarrow \overline{K}/K$.

Hecho 2. Supongamos que $\overline{K}$ es una clausura algebraica de K que contiene a E, todo homomorfismo $\sigma : F/K \longrightarrow \overline{K}/K$ se puede extender a un homomorfismo $\overline{\sigma} : E/K \longrightarrow \overline{K}/K$, y ya que E/K es una extensión normal, tenemos $\overline{\sigma}(E) = E$, y por tanto $\sigma(F) \subseteq E$, esto es, todo homomorfismo $\sigma : F/K \longrightarrow \overline{K}/K$ tiene su imagen en E. Por el Hecho 1, la extensión F/K es de Galois si, y sólo si, $\sigma(F) = F$ para cada homomorfismo $\sigma : F/K \longrightarrow E/K$.

F/K es de Galois si, y sólo si, $\sigma(F) = F$ para cada $\sigma : F/K \longrightarrow E/K$.

Hecho 3. Ya que cada homomorfismo $\sigma : F/K \longrightarrow E/K$ se puede extender a un automorfismo de E/K, resulta que F/K es una extensión de Galois si, y sólo si, $\sigma(F) = F$ para cada $\sigma \in \mathrm{Gal}(E/K)$.

F/K es de Galois si, y sólo si, $\sigma(F) = F$ para cada $\sigma \in \mathrm{Gal}(E/K)$.

(a) $\Rightarrow$ (b). Si F/K es una extensión de Galois, $\sigma(F) = F$ para cada $\sigma \in \mathrm{Gal}(E/K)$, ver (Hecho 2). Aplicando la primera parte tenemos $\sigma\,\mathrm{Gal}(E/F)\sigma^{-1} = \mathrm{Gal}(E/F)$, y por tanto $\mathrm{Gal}(E/F)$ es un subgrupo normal de $\mathrm{Gal}(E/K)$.
(b) $\Rightarrow$ (a). Si suponemos que $\mathrm{Gal}(E/F)$ es un subgrupo normal de $\mathrm{Gal}(E/K)$, entonces por la primera parte, resulta que para cada $\sigma \in \mathrm{Gal}(E/F)$ se tiene $\sigma(F) = F$, luego F/K es una extensión de Galois. Si $\mathrm{Gal}(E/F)$ es un subgrupo normal de $\mathrm{Gal}(E/K)$, definimos una aplicación

$$\nu : \mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(F/K)$$

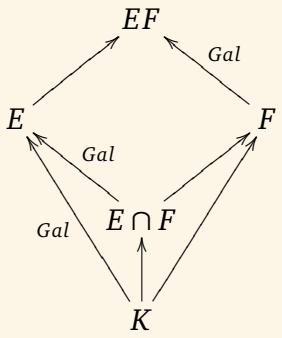
mediante $\nu(\sigma) = \sigma_{|F}$; esto es posible hacerlo por el Hecho 2. Es fácil probar que ν es un homomorfismo de grupos. Es claro que ν es sobreyectivo, Hecho 3. Falta calcular su núcleo, es claro que se tienen las equivalencias:

$$\nu(\sigma) = 1 \Leftrightarrow \sigma_{|F} = 1 \Leftrightarrow \sigma \in \mathrm{Gal}(E/F),$$

luego $\mathrm{Ker}(\nu) = \mathrm{Gal}(E/F)$, y por tanto tenemos el resultado: $\mathrm{Gal}(F/K) \cong \dfrac{\mathrm{Gal}(E/K)}{\mathrm{Gal}(E/F)}$. □

Veamos el comportamiento de las extensiones de Galois con respecto a la composición de cuerpos.

Proposición. 8.11.
Sean $E/K, F/K$ extensiones finitas, siendo E/K una extensión de Galois. Se verifica:
(1) EF/F es una extensión de Galois.
(2) Los grupos de Galois son isomorfos: $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/E\cap F)$.
(3) $[EF:K] = \dfrac{[E:K][F:K]}{[E:E\cap F]}$.



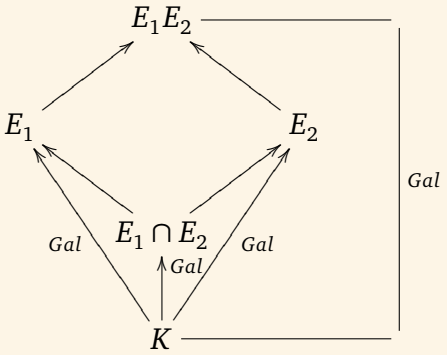
DEMOSTRACIÓN. (1). Como E es el cuerpo de descomposición de un polinomio separable sobre K, también EF es el cuerpo de descomposición de un polinomio separable sobre F, por tanto EF/F es una extensión de de Galois.
(2). Definimos $\theta : \mathrm{Gal}(EF/F) \longrightarrow \mathrm{Gal}(E/K)$ mediante: $\theta(\sigma) = \sigma_{|E}$. Si $\sigma_{|E} = 1$, entonces $\theta(e) = e$ para cada $e \in E$, y se tiene $\sigma = 1$, luego θ es inyectiva.
Llamamos $H = \mathrm{Im}(\theta)$. Es claro que $E\cap F \subseteq E^H$. Por otro lado, $E^H F \subseteq EF$ queda fijo por cada $\sigma \in \mathrm{Gal}(EF/F)$, y se tiene $E^H F = F$, esto es, $E^H \subseteq F$, y por tanto $E^H \subseteq E\cap F \subseteq E^H$, de donde $E\cap F = E^H$, y se tiene $\mathrm{Im}(\theta) = \mathrm{Gal}(E/E\cap F)$.
(3). Es inmediato, ya que $\dfrac{[E:K]}{[E\cap F:K]} = |\mathrm{Gal}(E/E\cap F)| = |\mathrm{Gal}(EF/F))| = \dfrac{[EF:K]}{[F:K]}$. □

Proposición. 8.12.
Sean $E_1/K, E_2/K$ subextensiones finitas de Galois de una extensión E/K. Se verifica:
(1) $E_1 \cap E_2/K$ es una extensión de Galois y su grupo de Galois es

$$\mathrm{Gal}(E_1 \cap E_2/K) \cong \frac{\mathrm{Gal}(E_1/K)}{\mathrm{Gal}(E_1/E_1 \cap E_2)}.$$

(2) E_1E_2/K es una extensión de Galois, y su grupo de Galois es

$$\mathrm{Gal}(E_1E_2/K) \cong \{(\sigma,\tau) \in \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K) \mid \ \sigma_{|E_1\cap E_2} = \tau_{|E_1\cap E_2}\} = H.$$



DEMOSTRACIÓN. (1). Basta ver que $E_1 \cap E_2/K$ es normal. Dado $f(X) \in K[X]$ irreducible con raíz en $E_1 \cap E_2$, esta raíz está en E_i, luego todas están en E_i, y por tanto en $E_1 \cap E_2$. El resto es consecuencia de la correspondencia de Galois.

(2). Cada E_i es el cuerpo de descomposición de un polinomio separable $f_i(X) \in K[X]$, entonces E_1E_2 es el cuerpo de descomposición de $f_1(X)f_2(X)$ y por tanto es una extensión normal.

Definimos $\theta : \mathrm{Gal}(E_1E_2/K) \longrightarrow \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K)$ mediante $\theta(\sigma) = (\sigma_{|E_1}, \sigma_{|E_2})$.

El núcleo de θ es trivial, tenemos $\mathrm{Ker}(\theta) = \{\sigma \in \mathrm{Gal}(E_1E_2/K) \mid \ \sigma_{|E_1} = 1, \sigma_{|E_2} = 1\}$, esto es, σ fija a E_1 y a E_2, luego $\sigma = 1$. La imagen de θ está contenida en el subgrupo H del enunciado, ya que $(\sigma_{|E_1})_{|E_1\cap E_2} = \sigma_{|E_1\cap E_2} = (\sigma_{|E_2})_{|E_1\cap E_2}$. Vamos a contar los elementos de H. Dado $\sigma \in \mathrm{Gal}(E_1/K)$ tenemos exactamente $|\mathrm{Gal}(E_2/E_1 \cap E_2)|$ elementos de la forma (σ,τ) en H, donde τ es un elemento de $\mathrm{Gal}(E_2/E_1 \cap E_2)$ que verifica $\sigma_{|E_1\cap E_2} = \tau_{|E_1\cap E_2}$. Como consecuencia se tiene:

$$|H| = |\mathrm{Gal}(E_1/K)| \cdot |\mathrm{Gal}(E_2/E_1 \cap E_2)| = [E_1 : K]\frac{[E_2 : K]}{[E_1 \cap E_2 : K]} = \frac{[E_1 : K][E_2 : K]}{[E_1 \cap E_2 : K]} = [E_1E_2 : K].$$

Entonces $\mathrm{Gal}(E_1E_2/K) \cong \mathrm{Im}(\theta) = H$. □

Corolario. 8.13.
Sean $E_1/K, E_2/K$ extensiones finitas de Galois tales que $E_1 \cap E_2 = K$, entonces

$$\mathrm{Gal}(E_1E_2/K) \cong \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K).$$

Podemos probar también el recíproco de este último resultado.

Proposición. 8.14.
Si E/K es una extensión finita de Galois y $\mathrm{Gal}(E/K) = H_1 \times H_2$, entonces

$$E = E^{H_1}E^{H_2}, \text{ y } E^{H_1} \cap E^{H_2} = K.$$

DEMOSTRACIÓN. Es consecuencia de la correspondencia de Galois. Ver la observación (8.9.2) en la página 111. □

Dada una extensión finita separable F/K, tenemos que

(1) F está contenido en una extensión de Galois E/K; basta considerar el cuerpo de descomposición de los polinomios irreducibles de un sistema de generadores de F/K.
(2) Existe una subextensión $K \subseteq F \subseteq F' \subseteq E$ tal que F'/K es de Galois y es minimal entre las subextensiones de Galois de E/K que contienen a F. En efecto, F' puede construirse como la intersección de todas las subextensiones de Galois de E/K que contienen a F ya que sólo hay un número finito de ellas. Llamamos a F' la **clausura de Galois** de F/K.

8.1. Ejercicios

Extensiones finitas de Galois

Ejercicio. 8.15.
Comprueba que las siguientes extensiones son de Galois. Encuentra los grupos de Galois y los retículos de subgrupos y subcuerpos y determina la correspondencia de Galois para cada una de ellas:
(1) $\mathbb{Q}(i,\sqrt[4]{5})/\mathbb{Q}$,
(2) $\mathbb{Q}(i,\sqrt[4]{5})/\mathbb{Q}(i)$,
(3) $\mathbb{Q}(\sqrt{2},\sqrt[3]{5},\omega)/\mathbb{Q}$, *donde* $\omega^2+\omega+1=0$.
(4) $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$, *donde* $\omega^2+\omega+1=0$.
(5) $\mathbb{Q}(\sqrt[6]{2},\xi)/\mathbb{Q}$, *con* $\xi=\xi_6$, *una raíz sexta primitiva de la unidad.*
(6) $E/\mathbb{F}_2$ *donde* E *es el cuerpo de descomposición del polinomio* X^3+X+1 *sobre* $\mathbb{F}_2$.

Ref.: 4162e_043 SOLUCIÓN

Ejercicio. 8.16.
Sea $E=\mathbb{Q}(\sqrt{2+\sqrt{2}})$. *Demuestra que* $E/\mathbb{Q}$ *es de Galois y que* $\mathrm{Gal}(E/\mathbb{Q})\cong\mathbb{Z}_4$.
Ref.: 4162e_049 SOLUCIÓN

Ejercicio. 8.17.
Determina el grupo de Galois de $E/\mathbb{Q}$ *donde* E *es el cuerpo de descomposición del polinomio* X^4-14X^2+9.
Ref.: 4162e_048 SOLUCIÓN

Ejercicio. 8.18.
Calcular el grupo $\mathrm{Aut}(F/\mathbb{Q})$, *siendo* $F=\mathbb{Q}(\sqrt{2},\omega)$, *donde* ω *es una raíz cúbica primitiva de la unidad.*
Ref.: 4162e_111 SOLUCIÓN

Ejercicio. 8.19.
Sea $F=\mathbb{Q}(\sqrt{2},\sqrt{3})$. Comprueba que la extensión $F/\mathbb{Q}$ es de Galois y determina $G=\mathrm{Gal}(F/\mathbb{Q})$ y el retículo de cuerpos intermedios.
Ref.: 4162e_060 SOLUCIÓN

Ejercicio. 8.20.
Determina el grupo de Galois de $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}$, el cuerpo de descomposición del polinomio $(X^2-2)(X^2-3)(X^2-5)$ sobre $\mathbb{Q}$. Determina todos los subcuerpos de dicho cuerpo.
Ref.: 4162e_047 SOLUCIÓN

Ejercicio. 8.21.
Sea $\mathbb{Q}(f)$ el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f=(X^2-2X-1)(X^2-2X-7)$. Determina el grupo $\mathrm{Gal}(f/\mathbb{Q})=\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$, y todos los cuerpos intermedios de la extensión.
Ref.: 4162e_068 SOLUCIÓN

Ejercicio. 8.22.
Se considera $\xi_5=e^{2\pi i/5}$ una raíz quinta primitiva de la unidad sobre $\mathbb{Q}$.
(1) Razona que $[\mathbb{Q}(\xi_5):\mathbb{Q}]=4$.
(2) Prueba que $\cos(2\pi/5), i\,sen(2\pi/5)\in\mathbb{Q}(\xi_5)$.
(3) Determina $[\mathbb{Q}(\cos(2\pi/5)):\mathbb{Q}]$.
(4) Determina el retículo de subgrupos de $\mathrm{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$ y los cuerpos asociados.

Ref.: 4162e_084 SOLUCIÓN

Ejercicio. 8.23.
Se considera $\xi_7=e^{2\pi i/7}$ una raíz séptima primitiva de la unidad sobre $\mathbb{Q}$.

(1) *Razona que* $[\mathbb{Q}(\xi_7):\mathbb{Q}]=6$.
(2) *Prueba que* $\cos(2\pi/7), i\,sen(2\pi/7)\in\mathbb{Q}(\xi_7)$.
(3) *Determina* $[\mathbb{Q}(\cos(2\pi/7)):\mathbb{Q}]$.
(4) *Determina* $[\mathbb{Q}(i\,sen(2\pi/7)):\mathbb{Q}]$.
(5) *Determina el retículo de subgrupos de* $\mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q})$ *y los cuerpos asociados.*

Ref.: 4162e_085 SOLUCIÓN

Ejercicio. 8.24.
Prueba que no existe ninguna extensión de Galois $K/\mathbb{Q}$ *con grupo de Galois* C_4 *tal que* $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{3})\subseteq K$.
Ref.: 4162e_091 SOLUCIÓN

Ejercicio. 8.25.
Sea $\mathbb{Q}\subseteq L\subseteq\mathbb{C}$ *una torre de cuerpos.*
(1) *Si* $L/\mathbb{Q}$ *es una extensión de Galois (finita), entonces para cada* $\alpha\in L$ *se tiene* $\overline{\alpha}\in L$ *(el conjugado complejo).*
(2) *Si* $L/\mathbb{Q}$ *es una extensión de Galois, prueba que* $\sigma: L/\mathbb{Q}\longrightarrow L/\mathbb{Q}$, *definido* $\sigma(\alpha)=\overline{\alpha}$ *tiene orden 1 ó 2.*

Ref.: 4162e_090 SOLUCIÓN

Ejercicio. 8.26.
Sea $K\subseteq\mathbb{C}$ *un cuerpo, y* σ *el automorfismo de conjugación en* $\mathbb{C}$. *Prueba que se verifica:*
(1) $\mathbb{Q}\subseteq K$.
(2) *Si* $L/\mathbb{Q}$ *es una extensión finita de Galois, para cada* $\alpha\in K$ *se tiene* $\sigma(\alpha)=\overline{\alpha}\in K$.
(3) $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ *tiene orden 1 ó 2.*
(4) *Si* $\sigma\in\mathrm{Aut}(K/\mathbb{Q})$, *entonces* $\mathrm{ord}(\sigma)=2$ *si, y sólo si,* $K\not\subseteq\mathbb{R}$.
(5) *Si* $\sigma\in\mathrm{Aut}(K/\mathbb{Q})$, *entonces* $[K^\sigma:K]=1$ *ó 2 según que* $K\subseteq\mathbb{R}$ *ó* $K\not\subseteq\mathbb{R}$.

Ref.: 4162e_092 SOLUCIÓN

Ejercicio. 8.27.
Demuestra que el grupo de Galois del cuerpo de descomposición de X^6+3 sobre $\mathbb{Q}$ es isomorfo al grupo diédrico D_3. Determina los retículos de subgrupos y de cuerpos intermedios.
Ref.: 4162e_051 SOLUCIÓN

Ejercicio. 8.28. (Extensiones Bicuadráticas)
Sea K un cuerpo de característica $\neq 2$. Si $F=K(\sqrt{D_1},\sqrt{D_2})$ donde $D_1,D_2\in K$ tienen la propiedad de que D_1, D_2 y D_1D_2 no son cuadrados en K. Demuestra que F/K es una extensión de Galois con grupo de Galois isomorfo al grupo de Klein. Recíprocamente, demuestra que cualquier extensión de Galois con grupo de Galois isomorfo al de Klein es del tipo antes descrito.
*Las extensiones de la forma anterior se llaman **extensiones bicuadráticas**.*
Ref.: 4162e_066 SOLUCIÓN

Ejercicio. 8.29.
Dados $a,b\in\mathbb{Z}$ libres de cuadrados, prueba que $\mathbb{Q}(\sqrt{a},\sqrt{b})=\mathbb{Q}(\sqrt{a}+\sqrt{b})$.
Ref.: 4162e_086 SOLUCIÓN

Ejercicio. 8.30.
*Sea $f(X)=X^4+bX^2+c\in\mathbb{Q}[X]$ un polinomio **bicuadrático** irreducible.*
(1) Prueba que $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ es isomorfo a V, C_4 ó D_4.
(2) Se considera $n,m\in\mathbb{Q}$ tales que n,m,nm no son cuadrados. Prueba que $\mathrm{Gal}(\mathbb{Q}(\sqrt{n},\sqrt{m})/\mathbb{Q})$ es isomorfo a V.
(3) Determina el polinomio $\mathrm{Irr}(\sqrt{n}+\sqrt{m},\mathbb{Q})$, y prueba que es un polinomio bicuadrático.
(4) (Opcional)Prueba que si $\mathrm{Gal}(F/\mathbb{Q})\cong V$, entonces existen n,m, como en (1) tales que $F=\mathbb{Q}(\sqrt{n},\sqrt{m})$.
(5) Da ejemplos de polinomios bicuadráticos $f_i\in\mathbb{Q}[X]$ tales que $\mathrm{Gal}(\mathbb{Q}(f_1)/\mathbb{Q})\cong V$, $\mathrm{Gal}(\mathbb{Q}(f_2)/\mathbb{Q})\cong C_4$, y $\mathrm{Gal}(\mathbb{Q}(f_3)/\mathbb{Q})\cong D_4$.
(6) Prueba que si $\sqrt{c}\in\mathbb{Q}$, entonces $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})\cong V$.
(7) Prueba que si $\sqrt{b^2-4c}\sqrt{c}\in\mathbb{Q}$, entonces $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})\cong C_4$. (Estos dos casos son excluyentes, ya que $\sqrt{b^2-4c}\notin\mathbb{Q}$.)
Ref.: 4162e_132 SOLUCIÓN

Extensiones finitas de Galois. Ccuerpos de característica p

Ejercicio. 8.31.
Sea K un cuerpo de característica $p \neq 0$. Sea $a \in K$ tal que para todo $b \in K$ se tiene $b^p - b \neq a$. Determina E el cuerpo de descomposición de $f = X^p - X - a$ sobre K y $G = \mathrm{Gal}(E/K)$.
(Pista: Sea α una raíz de f. ¿Cuánto vale $f(\alpha + 1)$?)
Ref.: 4162e_054 SOLUCIÓN

Ejercicio. 8.32.
Prueba que existe un cuerpo K y un polinomio $f(X) \in K[X]$ tal que el cuerpo de descomposición de $f(X)$ sobre K no es una extensión de Galois.
Ver también los Ejercicios (10.25.) *y* (10.14.).
Ref.: 4162e_089 SOLUCIÓN

Ejercicio. 8.33.
Se considera el cuerpo $\mathbb{F}_2(Y)$ y el subcuerpo $\mathbb{F}_2(Y^2 + Y)$. Prueba que la extensión $\mathbb{F}_2(Y)/\mathbb{F}_2(Y^2 + Y)$ es de Galois.
Ref.: 4162e_104 SOLUCIÓN

Ejercicio. 8.34.
Sean $K = \mathbb{F}_2$ y $E = K(\alpha_1, \alpha_2, \alpha_3)$, con α_i, $1 \leq i \leq 3$, raíces del polinomio $X^3 + X + 1$. Calcular $\mathrm{Gal}(E/K)$.
Ref.: 4162e_107 SOLUCIÓN

Extensiones finitas de Galois. Grupos de orden mayor

Ejercicio. 8.35.
Estudia el grupo de Galois del polinomio X^4-3 *sobre* $\mathbb{Q}$.
Ref.: 4162e_136 SOLUCIÓN

Ejercicio. 8.36.
Demuestra que $f(X)=X^4-2X^2-2$ *es irreducible sobre* $\mathbb{Q}$ *y que las raíces de esta cuártica son*

$$\alpha_1=\sqrt{1+\sqrt{3}},\quad \alpha_2=\sqrt{1-\sqrt{3}},\quad \alpha_3=-\sqrt{1+\sqrt{3}},\quad y\quad \alpha_4=-\sqrt{1-\sqrt{3}}.$$

Sean $K_1=\mathbb{Q}(\alpha_1)$, $K_2=\mathbb{Q}(\alpha_2)$, *y* $K=\mathbb{Q}(\sqrt{3})$.

(1) *Demuestra que* $K_1\neq K_2$ *y que* $K_1\cap K_2=\mathbb{Q}(\sqrt{3})=K$.
(2) *Demuestra que* K_1/K, K_2/K *y* K_1K_2/K *son de Galois, con* $\mathrm{Gal}(K_1K_2/K)$ *isomorfo al grupo de Klein.*
(3) *Describe explícitamente sus elementos. Determinar todos sus subgrupos y sus correspondientes subcuerpos fijos.*
(4) *Demuestra que el cuerpo de descomposición de* X^4-2X^2-2 *sobre* $\mathbb{Q}$ *es de grado* 8, *con grupo de Galois isomorfo al diédrico* D_4.

Ref.: 4162e_067 SOLUCIÓN

Ejercicio. 8.37.
Demuestra que el grupo de Galois del cuerpo de descomposición de X^6-3 *sobre* $\mathbb{Q}$ *es isomorfo al grupo diédrico* D_6. *Determina los retículos de subgrupos y de cuerpos intermedios.*
Ref.: 4162e_050 SOLUCIÓN

Ejercicio. 8.38.
Sea $\zeta=e^{2\pi i/20}$ *una raíz vigésima primitiva de la unidad y sea* $E=\mathbb{Q}(\zeta)$. *Razona que* $E/\mathbb{Q}$ *es de Galois. Calcula* $\mathrm{Irr}(\zeta,\mathbb{Q})$ *y demuestra que* $\mathrm{Gal}(E/\mathbb{Q})\cong\mathbb{Z}_4\times\mathbb{Z}_2$. *Determina los retículos de subgrupos y de cuerpos intermedios.*
Ref.: 4162e_052 SOLUCIÓN

Ejercicio. 8.39.
Sea E/K una extensión de Galois con grupo $G \cong \mathbb{Z}_{12} \times \mathbb{Z}_2$.

(1) ¿Cuántos cuerpos intermedios F existen tales que $[F : K] = 4$?
(2) ¿Cuántos tales que $[F : K] = 6$?
(3) ¿Y cuántos tales que $\mathrm{Gal}(E/F) \cong \mathbb{Z}_4$?
(4) ¿Y cuántos tales que $\mathrm{Gal}(F/K) \cong \mathbb{Z}_4$?

Ref.: 4162e_069 SOLUCIÓN

Ejercicio. 8.40.
Prueba que existe una extensión $K/\mathbb{Q}$ de grado cuatro que no tiene subcuerpos intermedios.
Ref.: 4162e_087 SOLUCIÓN

Ejercicio. 8.41.
Comprueba que la extensión $\mathbb{Q}(\sqrt[6]{2}, \xi)/\mathbb{Q}$, con $\xi = \xi_6$, una raíz sexta primitiva de la unidad, es de Galois; encuentra el grupo de Galois y los retículos de subgrupos y subcuerpos y determina la correspondencia de Galois..
Ref.: 4162e_137 SOLUCIÓN

Ejercicio. 8.42.
Describe una clausura normal $E/\mathbb{Q}$ de $\mathbb{Q}(\sqrt{2} + \sqrt[3]{2})/\mathbb{Q}$. Calcula el grupo de Galois $\mathrm{Gal}(E/\mathbb{Q})$ y los retículos de subgrupos y subcuerpos.
Ref.: 4162e_046 SOLUCIÓN

Ejercicio. 8.43.
Da un ejemplo de una extensión de Galois E/K con grado $[E:K]=20$ de tal forma que tenga un cuerpo intermedio F tal que F/K no sea de Galois.
Ref.: 4162e_053 SOLUCIÓN

Ejercicio. 8.44.
Sea $E=\mathbb{Q}(\sqrt[8]{2},i)$.

(1) *Demuestra que la extensión $E/\mathbb{Q}$ es de Galois y determina* $\mathrm{Gal}(E/\mathbb{Q})$.
(2) *Sean $F_1=\mathbb{Q}(i)$, $F_2=\mathbb{Q}(\sqrt{2})$ y $F_3=\mathbb{Q}(\sqrt{-2})$. Demuestra que* $\mathrm{Gal}(E/F_1)\cong C_8$, $\mathrm{Gal}(E/F_2)\cong D_4$ y $\mathrm{Gal}(E/F_3)\cong D_4$.
(3) *Determina todos los cuerpos intermedios $\mathbb{Q}\subseteq F\subseteq E$ para los que $F/\mathbb{Q}$ es una extensión de Galois.*

Ref.: 4162e_044 SOLUCIÓN

Ejercicio. 8.45.
Sea ζ una raíz octava primitiva de la unidad.

(1) *Razona que $\mathbb{Q}(\sqrt[8]{3},\zeta)/\mathbb{Q}$, es una extensión de Galois y calcula su grupo de Galois.*
(2) *Determina* $\mathrm{Gal}(\mathbb{Q}(\sqrt[8]{3},\zeta)/\mathbb{Q}(i))$, *el retículo de sus subgrupos y el retículo de subcuerpos de la extensión $\mathbb{Q}(\sqrt[8]{3},\zeta)/\mathbb{Q}(i)$.*

Ref.: 4162e_045 SOLUCIÓN

Ejercicio. 8.46.
Sea $K=\mathbb{Q}(\omega)$, siendo ω una raíz cúbica primitiva de la unidad. Prueba que no existen extensiones de Galois $E/\mathbb{Q}$ tales que $K\subseteq E$ y $\mathrm{Gal}(E/\mathbb{Q})\cong Q$, *el grupo cuaternio de 8 elementos.*
Ref.: 4162e_097 SOLUCIÓN

Los siguientes ejercicios proporcionan un ejemplo de una extensión de Galois E/K con grupo de Galois G isomorfo al grupo cuaternio Q_2.

Ejercicio. 8.47.
Sea $\alpha = (2+\sqrt{2})(3+\sqrt{3})$ *y* $F = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

(1) Comprueba que $\alpha \in F = \mathbb{Q}(\sqrt{2},\sqrt{3})$. *Deduce que los conjugados de* α *también están en* $\mathbb{Q}(\sqrt{2},\sqrt{3})$.
(2) Determina el subgrupo de G *que deja fijo a* α. *Deduce que* $\mathbb{Q}(\alpha) = F = \mathbb{Q}(\sqrt{2},\sqrt{3})$, *y concluye que tanto los conjugados de* α *como los generadores* $\sqrt{2},\sqrt{3}$ *se pueden expresar como polinomios en* α.

Ref.: 4162e_061 SOLUCIÓN

Ejercicio. 8.48.
Sea $\beta = \sqrt{\alpha} = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ *y sea* $E = \mathbb{Q}(\beta)$.

(1) Demuestra que $\beta \notin \mathbb{Q}(\alpha)$; *(pista: utilizar normas).*
(2) Calcula los conjugados de β *sobre* $\mathbb{Q}$.
(3) Comprueba que para cualquier γ, *conjugado de* β *sobre* $\mathbb{Q}$, *se tiene* $\gamma\beta \in \mathbb{Q}(\alpha)$. *Deduce que* $E/\mathbb{Q}$ *es una extensión de Galois. Calcula* $|\mathrm{Gal}(E/\mathbb{Q})|$.

Ref.: 4162e_062 SOLUCIÓN

Ejercicio. 8.49.
Sea $\gamma = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$ *y* $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ *el automorfismo definido por* $\sigma(\beta) = \gamma$.

(1) Demuestra que $\sigma(\beta^2) = \gamma^2$. *Concluye que* $\sigma(\sqrt{2}) = -\sqrt{2}$ *y que* $\sigma(\sqrt{3}) = \sqrt{3}$
(2) Demuestra que $\sigma(\beta\gamma) = -\beta\gamma$. *Deduce que* $\sigma(\gamma) = -\beta$.
(3) Demuestra que el orden de σ *es 4. Determina el cuerpo fijo bajo* σ.

Ref.: 4162e_063 SOLUCIÓN

Ejercicio. 8.50.
Sea $\delta = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$ *y* $\tau \in \mathrm{Gal}(E/\mathbb{Q})$ *el automorfismo definido por* $\tau(\beta) = \delta$.

(1) Demuestra que $\tau(\beta^2) = \delta^2$. *Concluye que* $\tau(\sqrt{2}) = \sqrt{2}$ *y que* $\tau(\sqrt{3}) = -\sqrt{3}$

(2) Demuestra que $\tau(\beta\delta) = -\beta\delta$. Deduce que $\tau(\delta) = -\beta$.
(3) Demuestra que el orden de τ es 4. Determina el cuerpo fijo bajo τ.

Ref.: 4162e_064 SOLUCIÓN

Ejercicio. 8.51.
Demuestra que $\sigma^2 = \tau^2$ y que $\sigma\tau = \tau\sigma^3$. Concluye que $\mathrm{Gal}(E/\mathbb{Q}) = \langle\sigma, \tau\rangle \cong Q_2$.
Ref.: 4162e_065 SOLUCIÓN

Extensiones finitas de Galois. Otras construcciones

Ejercicio. 8.52.
Sea E/K una extensión de Galois de grado $[E : K] = p^n$ con p primo. Razona que para todo $i \leq n$ existe por lo menos un cuerpo intermedio F tal que $[F : K] = p^i$.
Ref.: 4162e_055 SOLUCIÓN

Ejercicio. 8.53.
Suponemos conocido que π y e son números trascendentes. Sea $K(f)$ el cuerpo de descomposición del polinomio $f = X^3 + \pi X + 6$ sobre el cuerpo $K = \mathbb{Q}(\pi)$. Demuestra que $[K(f) : K] = 6$. Demuestra que $K(f)$ es isomorfo al cuerpo de descomposición de $g = X^3 + eX + 6$ sobre $\mathbb{Q}(e)$, mediante el isomorfismo $\mathbb{Q}(\pi) \cong \mathbb{Q}(e)$ que lleva π a e..
Ref.: 4162e_070 SOLUCIÓN

Ejercicio. 8.54.
Sea $f \in K[X]$ un polinomio irreducible y separable de grado n. Sea $K(f)$ el cuerpo de descomposición, $\alpha \in K(f)$ una raíz de f y F/K cualquier extensión de Galois tal que $K \subseteq F \subseteq K(f)$. Demuestra que

(1) $f = f_1 \cdots f_m$ donde los $f_i \in F[X]$ son irreducibles sobre F,
(2) todos los f_i son de grado $d = [F(\alpha) : F]$, y $m = \frac{n}{d} = [K(\alpha) \cap F : K]$.

(Pista: Demuestra primero que la factorización de f sobre F es la misma que sobre $F \cap K(\alpha)$. Si $H = G^F \subseteq G = \mathrm{Gal}(K(f)/K)$ entonces los factores de f sobre F corresponden a las órbitas bajo H de las raíces de f.)
Ref.: 4162e_071 SOLUCIÓN

Ejercicio. 8.55.
Sea $f \in K[X]$ irreducible de grado primo p. Demuestra que para cada extensión de Galois E/K se tiene que f es irreducible sobre E o descompone en factores lineales sobre E.
Ref.: 4162e_072 SOLUCIÓN

Ejercicio. 8.56.
Sea E/K una extensión finita y F_1, F_2 dos cuerpos intermedios. Demuestra:
(1) Si F_1/K de Galois, entonces F_1F_2/F_2 es de Galois y $\mathrm{Gal}(F_1F_2/F_2) \cong \mathrm{Gal}(F_1/F_1 \bigcap F_2)$.
(2) Si F_1/K y F_2/K son de Galois entonces F_1F_2/K es de Galois. Además si $F_1 \bigcap F_2 = K$, entonces $\mathrm{Gal}(F_1F_2/K) \cong \mathrm{Gal}(F_1/K) \times \mathrm{Gal}(F_2/K)$.
(3) Si F_1/K y F_1F_2/K son de Galois y $F_1 \bigcap F_2 = K$, entonces

$$\mathrm{Gal}(F_1F_2/K) \cong \mathrm{Gal}(F_1F_2/F_1) \rtimes \mathrm{Gal}(F_1F_2/F_2).$$

Ref.: 4162e_058 SOLUCIÓN

Si G es un grupo, $H, N \subseteq G$ subgrupos de forma que $N \lhd G$ es normal, $NH = G$ y $N \cap H = \{1\}$, entonces G es el producto semidirecto de N y H, esto es, existe un homomorfismo $\theta : H \longrightarrow \mathrm{Aut}(N)$, y la multiplicación en $G = N \rtimes H$ está dada por $(n_1, h_1)(n_2, h_2) = (n_1 n_2^{h_1}, h_1 h_2)$.

Ejercicio. 8.57.
Se considera el producto semidirecto $G = D_4 \rtimes \mathbb{Z}_2$, siendo $D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = \sigma\tau\sigma\tau = 1 \rangle$ y $\theta(1)(\sigma) = \sigma^3$, $\theta(1)(\tau) = \tau\sigma$. Observa que G es un grupo de orden 16. Supongamos que G es el grupo de Galois de una extensión E/K.

(1) Determina el retículo de subgrupos de $D_4 \rtimes \mathbb{Z}_2$.
(2) Determina los subgrupos normales de G.

Ref.: 4162e_129 SOLUCIÓN

Si G es un grupo, $H, N \subseteq G$ subgrupos de forma que $N \lhd G$ es normal, $NH = G$ y $N \cap H = \{1\}$, entonces G es el **producto semidirecto** de N y H, esto es, existe un homomorfismo $\theta : H \longrightarrow \mathrm{Aut}(N)$, y la multiplicación en $G = N \rtimes_\theta H$ está dada por $(n_1, h_1)(n_2, h_2) = (n_1\theta(h_1)(n_2), h_1h_2) = (n_1 n_2^{h_1}, h_1h_2)$.

Ejercicio. 8.58.
Se considera el producto semidirecto $G = \mathbb{Z}_8 \rtimes_\theta \mathbb{Z}_2$, siendo $\theta(1)(1) = 3$. Observa que G es un grupo de orden 16. Supongamos que G es el grupo de Galois de una extensión E/K.
(1) ¿Cuántos cuerpos intermedios F/K, con $K \subseteq F \subseteq E$, existen de grado 8? ¿Cuántos con grupo de Galois $\mathrm{Gal}(F/K)$ isomorfo a $\mathbb{Z}_8$?
(2) ¿Cuántos cuerpos intermedios F/K, con $K \subseteq F \subseteq E$, existen de grado 4? ¿Cuántos con grupo de Galois $\mathrm{Gal}(E/F)$ isomorfo a $\mathbb{Z}_4$? y ¿cuántos con grupo de Galois isomorfo al grupo de Klein?
(3) ¿Cuántos cuerpos intermedios F/K, con $K \subseteq F \subseteq E$, existen de grado 2? ¿Cuántos con grupo de Galois $\mathrm{Gal}(E/F)$ isomorfo a $\mathbb{Z}_8$?
(4) (Opcional). Determina el retículo de subgrupos de $\mathbb{Z}_8 \rtimes_\theta \mathbb{Z}_2$.

Ref.: 4162e_130 SOLUCIÓN

Extensiones finitas de Galois. Aplicaciones

Ejercicio. 8.59.
Sea E/K una extensión de Galois de grado n. Para cada $\alpha \in E$
(1) Demuestra que el polinomio $f(X) = \prod\{(X - \sigma(\alpha)) \mid \sigma \in \mathrm{Gal}(E/K)\}$ pertenece a $K[X]$.
(2) Demuestra que $f(X) = \mathrm{Irr}(\alpha, K)$ si, y sólo si, $E = K(\alpha)$.

Ref.: 4162e_108 SOLUCIÓN

Ejercicio. 8.60.
Sea E/K una extensión de Galois de grado finito n, y sea $\mathrm{Gal}(E/K) = \{\sigma_1, \ldots, \sigma_n\}$. Para cada subconjunto $\{\alpha_1, \ldots, \alpha_n\} \subseteq E$, prueba que son equivalentes:

(a) $\{\alpha_1, \ldots, \alpha_n\}$ es una K–base de E.
(b) La matriz $(\sigma_i(\alpha_j))_{ij}$ tiene determinante no nulo.

Ref.: 4162e_122 SOLUCIÓN

Ejercicio. 8.61.
Sea E/K una extensión de Galois, F un cuerpo intermedio y $H \subseteq \mathrm{Gal}(E/K)$ el subgrupo de los automorfismos de E/K que aplican F en sí mismo. Demuestra que H es el normalizador de $\mathrm{Gal}(E/F)$ en $\mathrm{Gal}(E/K)$ y describe el grupo cociente $H/\mathrm{Gal}(E/F)$.
Ref.: 4162e_057 SOLUCIÓN

Ejercicio. 8.62.
Sea $K = \mathbb{Q}(\omega)$, siendo ω una raíz cúbica primitiva de la unidad. Prueba que no existen extensiones de Galois $E/\mathbb{Q}$ tales que $K \subseteq E$ y $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_4$.
Ref.: 4162e_096 SOLUCIÓN

Sea $f \in K[X]$ un polinomio sin raíces múltiples; se dice que $G \subseteq \mathrm{Gal}(f/K)$ **actúa transitivamente** sobre las raíces de f si dadas dos raíces cualesquiera α y β de f, existe $\varphi \in G$ tal que $\varphi(\alpha) = \beta$.

Ejercicio. 8.63.
Sea $f \in K[X]$ un polinomio no constante sin raíces múltiples y $G = \mathrm{Gal}(f/K)$. Prueba que son equivalentes:

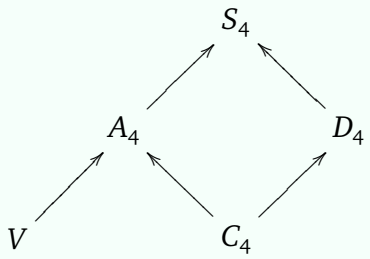
(a) $f(X)$ es irreducible.
(b) G actúa transitivamente sobre las raíces de f.

Ref.: 4162e_128 SOLUCIÓN

Ejercicio. 8.64.
Prueba que los subgrupos transitivos de S_4 son los subgrupos siguientes:

(1) S_4, que es normal.
(2) A_4, que es normal.
(3) $D_4 = \langle (1234), (13) \rangle$, y todos sus conjugados.
(4) $C_4 = \langle (1234) \rangle$, y todos sus conjugados.
(5) $V = \{1, (12)(34), (13)(24), (14)(24)\}$, que es normal.

El retículo de los subgrupos transitivos de S_4 es:



Como consecuencia, si $f(X) \in \mathbb{Q}[X]$ es un polinomio irreducible de grado cuatro, el grupo de Galois de $\mathbb{Q}(f)/\mathbb{Q}$ es isomorfo a uno de éstos.
Ref.: 4162e_131 SOLUCIÓN

Ejercicio. 8.65.
Se considera una extensión de Galois E/K, con grupo de Galois $G = \mathrm{Gal}(E/K)$. Para cada $a \in E$, con $f(X) = \mathrm{Irr}(a, K)$, prueba que los siguientes conjuntos son iguales:

$$\{\varphi(a) \mid \varphi \in G\} = \{x \in E \mid f(x) = 0\}.$$

Ref.: 4162e_138 SOLUCIÓN

Ejercicio. 8.66.
Sea E/K una extensión finita de Galois y $\alpha \in E \setminus K$. Vamos a determinar el polinomio irreducible de α sobre K.

Consideramos todos los conjugados de α, esto es, el conjunto $C = \{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(E/K)\}$, en el que no hay elementos repetidos ya que es un conjunto, y definimos $f(X) = \prod_{\beta \in C}(X - \beta)$. Entonces α es una raíz de $f(X)$.

(1) Prueba que $f(X) \in K[X]$.
(2) Prueba que $f(X)$ es irreducible sobre K. Como consecuencia $f(X) = \mathrm{Irr}(\alpha, K)$.
(3) Considera extensión $\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})/\mathbb{Q}$, prueba que es una extensión de Galois.
(4) Determina $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})/\mathbb{Q})$ e $\mathrm{Irr}(\sqrt[3]{3} + \sqrt{-3}, \mathbb{Q})$.
(5) Considera la clausura normal $E/\mathbb{Q}$ de $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, que es una extensión de Galois; describe E.
(6) Determina $\mathrm{Gal}(E/\mathbb{Q})$ e $\mathrm{Irr}(i + \sqrt{2} + \sqrt{-2}, \mathbb{Q})$.

Ref.: 4162e_140 *SOLUCIÓN*

Ejercicio. 8.67.
Sea E/K una extensión de Galois de grado n con grupo de Galois G y $\alpha \in E$ un elemento. Se define $f(X) = \prod_{\sigma \in G}(X - \sigma(\alpha)) \in E[X]$.

(1) Prueba que $f(X) \in K[X]$.
(2) Prueba que son equivalentes:
  (a) f es irreducible sobre K.
  (b) $E = K(\alpha)$.

Ref.: 4162e_142 *SOLUCIÓN*

9. La ecuación general de grado n

Se trata ahora de construir una extensión de cuerpos de Galois E/L cuyo grupo de Galois sea isomorfo a S_n, y como consecuencia, una extensión de Galois E/E^G, para cada grupo finito $G \subseteq S_n$. Ya que para cada grupo finito G existe un n tal que G es isomorfo a un subgrupo de S_n, tenemos una forma de construir una extensión de Galois con grupo de Galois isomorfos a un grupo finito dado G.
Sea $L = K(X_1, \ldots, X_n)$ el cuerpo de fracciones sobre las indeterminadas $X_1, \ldots, X_n$.

Proposición. 9.1.
Sea $f_n \in K(X_1, \ldots, X_n)[Y]$ el polinomio definido por:

$$f_n = Y^n - X_1 Y^{n-1} + \cdots + (-1)^{n-1} X_{n-1} Y + (-1)^n X_n$$

Si E es el cuerpo de descomposición de f_n sobre $L = K(X_1, \ldots, X_n)$, entonces $\mathrm{Gal}(E/L) \cong S_n$.

Para hacer la demostración, primero consideramos la aplicación

$$S_n \xrightarrow{\varphi} \mathrm{Aut}(K(X_1, \ldots, X_n)/K); \quad \sigma \mapsto \varphi_\sigma; \quad \varphi_\sigma(X_i) = X_{\sigma(i)}$$

Es claro que φ es un monomorfismo de grupos. Si $\Omega = \mathrm{Im}(\varphi)$ es la imagen de φ, y $F = K(X_1, \ldots, X_n)^\Omega$, el cuerpo de los elementos que quedan fijos por Ω, por el Teorema de Artin, se verifica:

$$[K(X_1, \ldots, X_n) : K(X_1, \ldots, X_n)^\Omega] = |\Omega| = n!$$

Lema. 9.2.
Si $e_1, \ldots, e_n$ son los polinomios simétricos elementales en las indeterminadas $X_1, \ldots, X_n$, resulta que $K(e_1 \ldots, e_n) = K(X_1, \ldots, X_n)^\Omega$.

DEMOSTRACIÓN. Tenemos que $K(e_1, \ldots, e_n) \subseteq K(X_1, \ldots, X_n)^\Omega \subseteq K(X_1, \ldots, X_n)$. Para ver que son iguales basta ver que $[K(X_1, \ldots, X_n) : K(e_1, \ldots, e_n)] \leq n!$
Consideramos el polinomio $f = Y^n + \sum_{i=1}^n (-1)^i e_i Y^{n-i}$. Es claro que $f = \prod_{i=1}^n (Y - X_i)$, y por tanto $K(X_1, \ldots, X_n) = K(e_1, \ldots, e_n)(X_1, \ldots, X_n)$ es el cuerpo de descomposición de f, que como tiene grado n sobre $K(e_1, \ldots, e_n)$ se tiene que $[K(X_1, \ldots, X_n) : K(e_1, \ldots, e_n)] \leq n!$ □

4162-05.tex

Lema. 9.3.
Existe un isomorfismo $\nu : E/K \longrightarrow K(X_1,\dots,X_n)/K$ tal que $\nu(K(X_1,\dots,X_n)) = K(e_1,\dots,e_n)$, donde E es el cuerpo de descomposición de f_n sobre $L = K(X_1,\dots,X_n)$.

DEMOSTRACIÓN. El isomorfismo $\eta : K[X_1,\dots,X_n] \longrightarrow K[e_1,\dots,e_n]$, definido $X_i \mapsto e_i$, se puede extender a los cuerpos de fracciones: $\eta : K(X_1,\dots,X_n) \longrightarrow K(e_1,\dots,e_n)$. Se verifica:

$$\begin{aligned}\eta f_n(Y) &= \eta(Y^n + \textstyle\sum(-1)^i X_i Y^{n-i}) \\ &= Y^n + \textstyle\sum(-1)^i e_i Y^{n-i} \\ &= f(Y).\end{aligned}$$

Como E es el cuerpo de descomposición de f_n y $L = K(X_1,\dots,X_n)$ es el cuerpo de descomposición de f, existe un isomorfismo

$$\nu : E/K \longrightarrow L/K,$$

que extiende η.

$$\begin{array}{ccc} E = K(X_1,\dots,X_n)(f_n) & \xrightarrow[\nu]{\cong} & K(e_1,\dots,e_n)(f) = K(X_1,\dots,X_n) = L \\ \Big| & & \Big| \\ L = K(X_1,\dots,X_n) & \xrightarrow[\eta]{\cong} & K(e_1,\dots,e_n) \end{array}$$

□

DEMOSTRACIÓN. [de la Proposición] Existe un homomorfismo de grupos:

$$\mathrm{Gal}(E/L) \longrightarrow \mathrm{Gal}(L/K(e_1,\dots,e_n)); \quad \varphi \mapsto \nu\varphi\nu^{-1},$$

y ambos grupos son isomorfos. Pero $\mathrm{Gal}(L/K(e_1,\dots,e_n))$ tiene $n!$ elementos, y por tanto $\mathrm{Gal}(E/L) \cong S_n$. □

Una de las aplicaciones de los resultados de esta sección es el siguiente teorema.
Sea $f \in K[X]$ un polinomio no constante, y E su cuerpo de descomposición; la ecuación $f(X) = 0$ es **soluble por radicales** si el grupo de Galois de la extensión E/K es un grupo soluble.

Teorema. 9.4. (Teorema de Abel–Ruffini)
Si K es un cuerpo de característica cero y $n > 4$ un entero positivo, entonces la ecuación general de grado n sobre K no es soluble por radicales sobre el cuerpo $K(X_1,\dots,X_n)$.

9.1. Ejercicios

La ecuación general de grado n

Ejercicio. 9.5.
Demuestra que para todo grupo finito G existe una extensión de Galois E/K con grupo de Galois isomorfo a G.
Ref.: 4162e_059 SOLUCIÓN

10. Elementos primitivos

Sea F/K una extensión de cuerpos, un elemento $\alpha \in F$ se llama **primitivo**, para la extensión F/K, si $F = K(\alpha)$. Una extensión F/K es una extensión **simple** si existe $\alpha \in F$ tal que $F = K(\alpha)$.

Teorema. 10.1. (Teorema de Steinitz)
Sea F/K una extensión finita, son equivalentes:
(a) F/K tiene un elemento primitivo.
(b) Existe un número finito de cuerpos intermedios.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Sea $F = K(\alpha)$ y $K \subseteq L \subseteq F$ un cuerpo intermedio. Llamamos $f = \mathrm{Irr}(\alpha, K)$ y $g = \mathrm{Irr}(\alpha, L)$. Entonces $g \,|\, f$, esto es, g divide a f. Llamamos L' al cuerpo generado por los coeficientes de g; se verifica:

$$\left.\begin{array}{l} K \subseteq L' \subseteq L \\ g = \mathrm{Irr}(\alpha, L') \\ F = K(\alpha) = L(\alpha) = L'(\alpha) \\ [F : L] = \mathrm{gr}(g) = [F : L'] \end{array}\right\} \Rightarrow L = L'$$

Entonces el número de cuerpos intermedios está limitado por el número de factores mónicos de $\mathrm{Irr}(\alpha, K)$ en $F[X]$, y por tanto es finito.
(b) $\Rightarrow$ (a). Si K es un cuerpo finito, entonces F es también un cuerpo finito y está generado por un elemento (un generador del grupo multiplicativo).
Si K es un cuerpo infinito, haciendo inducción sobre el número de generadores de F, basta analizar el caso en que $F = K(\alpha, \beta)$. Consideramos los subcuerpos de la forma $K(\alpha + a\beta)$, con $a \in K$. Como sólo hay un número finito de cuerpos intermedios, existen $a, b \in K$, $a \neq b$, tales que $K(\alpha + a\beta) = K(\alpha + b\beta)$. Se verifica:

$$\begin{array}{l} \beta = (a-b)^{-1}(\alpha + a\beta - (\alpha + b\beta)) \in K(\alpha + a\beta) = K(\alpha + b\beta) \\ \alpha = \alpha + a\beta - a\beta \in K(\alpha + a\beta) \end{array}$$

entonces $K(\alpha, \beta) = K(\alpha + a\beta)$, por lo tanto $\alpha + a\beta$ es un elemento primitivo. □

Corolario. 10.2.
Sea F/K una subextensión de una extensión de Galois finita, entonces F/K es una extensión simple.

4162-06.tex

DEMOSTRACIÓN. Si $K \subseteq F \subseteq E$ y E/K es de Galois, los subcuerpos intermedios entre F y K corresponden a los subgrupos de $\mathrm{Gal}(E/K)$ que contienen a $\mathrm{Gal}(E/F)$, y por tanto son un número finito. □

Corolario. 10.3.
Sea F/K una extensión separable finita, entonces existe un elemento primitivo.

DEMOSTRACIÓN. Consideramos una clausura normal E/K, entonces E/K es una extensión de Galois. Por el corolario anterior tenemos que F/K es una extensión simple. □

Sea E/K una extensión de Galois con grupo de Galois $G = \{\varphi_1, \ldots, \varphi_n\}$, si $\alpha \in E$ es un elemento primitivo y llamamos $\alpha_i = \varphi_i(\alpha)$ a los distintos conjugados de α, resulta que

$$\mathrm{Irr}(\alpha, K) = \prod_i (X - \alpha_i).$$

En consecuencia, todos los α_i son distintos y podemos utilizar esto como una caracterización de elementos primitivos.

Teorema. 10.4.
Sea E/K una extensión de Galois y $\alpha \in E$ un elemento de E. Son equivalentes:
(a) α es primitivo.
(b) Todos los conjugados de α son distintos.

DEMOSTRACIÓN. (b) $\Rightarrow$ (a). Si $\mathrm{Gal}(E/K) = \{\varphi_1, \ldots, \varphi_n\}$, el grado del polinomio $\mathrm{Irr}(\alpha, K)$ es n, y por tanto $E = K(\alpha)$. □

Bases normales

En general, si α es un elemento primitivo de una extensión de Galois E/K, no podemos asegurar que el conjunto $\{\varphi_1(\alpha), \ldots, \varphi_n(\alpha)\}$ sea linealmente independiente sobre K. Cuando este conjunto es linealmente independiente decimos que es una **base normal**.

Teorema. 10.5. (Teorema de la base normal)
Cada extensión de Galois finita tiene una base normal.

La demostración de este resultado es diferente según sea K un cuerpo finito o infinito.

Caso en el que K es un cuerpo infinito.

Lema. 10.6.
Sea F/K una extensión finita y separable de grado n, $\overline{K}/K$ una clausura algebraica de K, $\varphi_1,\dots,\varphi_n : F/K \longrightarrow \overline{K}/K$ homomorfismos distintos, y $a_1,\dots,a_n \in F$. Son equivalentes:
(a) Los elementos $a_1,\dots,a_n \in F$ forman una base.
(b) $\det(\varphi_i(a_j))_{ij} \neq 0$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Consideramos el sistema de ecuaciones lineales en $\overline{K}$

$$\left.\sum_{i=1}^{n} \varphi_i(a_j)X_i = 0\right\}_{j=1,\dots,n}$$

Por el lema de independencia de Dedekind los $\varphi_1,\dots,\varphi_n$ son linealmente independientes, entonces si $a_1,\dots,a_n$ es una base, la única solución del sistema es la trivial, y como consecuencia $\det(\varphi_i(a_j))_{ij} \neq 0$.
(b) $\Rightarrow$ (a). Si $\det(\varphi_i(a_j))_{ij} = 0$, existen $x_1,\dots,x_n \in K$, no todos nulos, tales que $x_1a_1+\cdots+x_na_n = 0$. Se verifica:

$$\left.\sum_{i=1}^{n} \varphi_j(a_i)x_i = 0\right\}_{j=1,\dots,n}$$

y por tanto el sistema $\left.\sum_{i=1}^{n} \varphi_j(a_i)X_i = 0\right\}_{j=1,\dots,n}$ tiene una solución no trivial, lo que es una contradicción. □

Proposición. 10.7. (Independencia algebraica de automorfismos)
Sea E/K una extensión de Galois finita, con K un cuerpo infinito. Si $\mathrm{Gal}(E/K) = \{\varphi_1,\dots,\varphi_n\}$ y $f \in K[X_1,\dots,X_n]$ verifica $f(\varphi_1(a),\dots,\varphi_n(a)) = 0$ para cada $a \in E$, entonces $f = 0$.

DEMOSTRACIÓN. Consideramos una K base de E, por ejemplo $\{a_1,\dots,a_n\}$ y definimos el polinomio

$$g(Y_1,\dots,Y_n) = f\left(\sum_{i=1}^{n} Y_i\varphi_1(a_i),\dots,\sum_{i=1}^{n} Y_i\varphi_n(a_i)\right) = f\left(\varphi_1\left(\sum_{i=1}^{n} Y_ia_i\right),\dots,\varphi_n\left(\sum_{i=1}^{n} Y_ia_i\right)\right)$$

Se verifica $g(b_1,\dots,b_n) = 0$ cuando $b_1,\dots,b_n \in K$, y como K es infinito, se verifica $g = 0$.

Como $a_1,\dots,a_n$ es una K–base, resulta $\det(\varphi_i(a_j))_{ij} \neq 0$, y por tanto la matriz $(\varphi_i(a_j))_{ij}$ es una matriz invertible; sea $(b_{ij})_{ij}$ la matriz inversa. si definimos

$$X_j = \sum_{i=1}^{n} \varphi_j(a_i) Y_i, \qquad j = 1,\dots,n,$$

entonces

$$Y_j = \sum_{i=1}^{n} b_{ij} X_i, \qquad j = 1,\dots,n.$$

Y resulta que $f(X_1,\dots,X_n) = g\left(\sum_{i=1}^n b_{i1}X_i,\dots,\sum_{i=1}^n b_{in}X_i\right) = 0$ □

DEMOSTRACIÓN. [del teorema.]
Sea $\mathrm{Gal}(E/K) = \{\varphi_1,\dots,\varphi_n\}$. Consideramos indeterminadas $X_i = X_{\varphi_i}$ y el polinomio

$$f(X_1,\dots,X_n) = \det(X_{\varphi_i^{-1}\varphi_j})_{ij}.$$

Es claro que $f(X_1,\dots,X_n)$ no es el polinomio cero; basta sustituir X_1 por 1 y las demás indeterminadas por 0 y obtenemos un número distinto de cero.
Como K es un cuerpo infinito, existe un $x \in K$ tal que el sustituir X_i por $\varphi_i(x)$ el resultado es no nulo (para todo $i = 1,\dots,n$). Ver Proposición (10.7.). Tenemos pues $\det(\varphi_i^{-1}\varphi_j(x))_{ij} \neq 0$.
Si los $\varphi_1(x)$, …, $\varphi_n(x)$ son linealmente dependientes, entonces existen k_1, …, $k_n \in K$, no todos nulos, tales que $k_1\varphi_1(x) + \cdots + k_n\varphi_n(x) = 0$. Aplicando φ_i^{-1}, para $i = 1,\dots,n$, tenemos que k_1, …, k_n es una solución no trivial de un sistema homogéneo de n ecuaciones con coeficientes $\varphi_i^{-1}\varphi_j(x)$ y determinante no nulo, lo que es una contradicción. □

Caso en el que K es un cuerpo finito.

DEMOSTRACIÓN. [del teorema.]
Consideramos la extensión de Galois E/K, entonces E es también un cuerpo finito. El grupo $\mathrm{Gal}(E/K)$ es cíclico generado por φ, el automorfismo de Frobenius, ver Teorema (12.4.). Si K tiene $q = p^m$ elementos, entonces φ está definido $\varphi(z) = z^q$, para cada $z \in E$.
Si $[E:K] = n$, entonces $\varphi^n = 1$ y los elementos $1, \varphi, \dots, \varphi^{n-1}$ son todos distintos, y por el Teorema de independencia de Dedekind, son linealmente independientes sobre E, en particular sobre K; esto significa que φ no anula a ningún polinomio, no nulo de grado menor que n, por lo que el polinomio de menor grado al que anula φ es $X^n - 1$.
Como aplicación lineal φ tiene un único factor invariante: $X^n - 1$, y uno o varios divisores elementales. Existe $\alpha \in E$ tal que $\{\alpha, \varphi(\alpha), \dots, \varphi^{n-1}(\alpha)\}$ es una base de E sobre K. □

Ejemplos de cálculo de bases normales

Ejemplo. 10.8. (Cálculo de bases normales)
Consideramos la extensión $\mathbb{F}_8/\mathbb{F}_2$, siendo $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$, y el endomorfismo $\varphi : \mathbb{F}_8/\mathbb{F}_2 \longrightarrow \mathbb{F}_8/\mathbb{F}_2$, definido $\varphi(z) = z^2$, para cada $z \in \mathbb{F}_8$.

Observa que si $x = \overline{X}$, se tiene $\varphi(a_0 + a_1x + a_2x^2) = a_0^2 + a_1^2x^2 + a_2^2x^4 = a_0 + a_2x + (a_1 + a_2)x^2$, esto es, φ está definido por la matriz $A = \begin{pmatrix} 1\,0\,0 \\ 0\,0\,1 \\ 0\,1\,1 \end{pmatrix}$.

Se tiene $A^2 = \begin{pmatrix} 1\,0\,0 \\ 0\,1\,1 \\ 0\,1\,0 \end{pmatrix}$, $A^3 = 1$. Como consecuencia $A^3 - 1 = 0$, y A es raíz del polinomio $X^3 - 1$.

Podríamos pensar que A debe ser una raíz del polinomio $X^2 + X - 1$, pero ésto no ocurre, ya que las matrices cuadradas 3×3 forman un anillo no conmutativo. En efecto, se tiene:

$$A^2 + A + 1 = \begin{pmatrix} 1\,0\,0 \\ 0\,0\,0 \\ 0\,0\,0 \end{pmatrix} \neq 0.$$

El grupo de Galois es $\mathrm{Gal}(\mathbb{F}_8/\mathbb{F}_2) = \langle\varphi\rangle \cong C_3$.

Para determinar un elemento primitivo, primero observa que el polinomio característico de A es $X^3-1 = (X-1)(X^2+X+1)$, y por lo tanto tiene un vectores propio $v_1 = (1,0,0)$, y un bloque generado por $v_2 = (0,0,1)$ y $v_3 = (0,1,1)$, siendo $\varphi(v_2) = v_3$. Por lo tanto, aunque x^2 es un elemento primitivo, no define una base normal. Se tiene también que, x es un elemento primitivo, pero tampoco define una base normal.

Un elemento primitivo, que proporciona una base normal, es $\alpha = 1 + x + x^2$, que define la base

$$\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\} = \{1 + x + x^2, 1 + x, 1 + x^2\},$$

en la base $\{1, x, x^2\}$.

Ejemplo. 10.9. (Cálculo de bases normales)

Consideramos la extensión $\mathbb{F}_{64}/\mathbb{F}_4$, siendo $\mathbb{F}_{64} = \mathbb{F}_4[X]/(X^3+X+1)$, y el endomorfismo de Frobenius $\varphi : \mathbb{F}_{64}/\mathbb{F}_4 \longrightarrow \mathbb{F}_{64}/\mathbb{F}_4$, definido $\varphi(z) = z^4$, para cada $z \in \mathbb{F}_{64}$. Supongamos que $\mathbb{F}_4 = \{0, 1, a, a+1\}$, entonces φ está definido $\varphi(a_0 + a_1x + a_2x^2) = a_0^4 + a_1^4x^4 + a_2^4x^8 = a_0 + (a_1 + a_2)x + a_1x^2$, esto es, φ está definido por la matriz $A = \begin{pmatrix} 1\,0\,0 \\ 0\,1\,1 \\ 0\,1\,0 \end{pmatrix}$, y se tiene $A^2 = \begin{pmatrix} 1\,0\,0 \\ 0\,0\,1 \\ 0\,1\,1 \end{pmatrix}$, $A^3 = 1$. Como consecuencia $A^3 - 1 = 0$, pero observa que también en este caso se tiene $A^2 + A + 1 = \begin{pmatrix} 1\,0\,0 \\ 0\,0\,0 \\ 0\,0\,0 \end{pmatrix}$.

El grupo de Galois $\mathrm{Gal}(\mathbb{F}_{64}/\mathbb{F}_4) = \langle\varphi\rangle \cong C_3$. En este caso también x es un elemento primitivo, pero $\{x, \varphi(x), \varphi^2(x)\}$ no es una base.

En general, para calcular un elemento primitivo que genere una base normal, consideramos un elemento genérico $\alpha = a_0 + a_1x + a_2x^2$, calculamos $\varphi(\alpha)$ y $\varphi^2(\alpha)$, y vemos las condiciones necesarias

para que α, $\varphi(\alpha)$ y $\varphi^2(\alpha)$ sean linealmente independientes.

$$\begin{aligned}\alpha &= a_0 + a_1 x + a_2 x^2,\\ \varphi(\alpha) &= a_0 + (a_1 + a_2)x + a_1 x^2,\\ \varphi^2(\alpha) &= a_0 + a_2 x + (a_1 + a_2)x^2.\end{aligned}$$

El determinante de la matriz de coeficientes es: $a_0(a_1^2 + a_1 a_2 + a_2^2)$. Éste es no nulo, por ejemplo, si $\alpha = 1 + x$.

10.1. Ejercicios

Elementos primitivos

Ejercicio. 10.10.
Halla elementos primitivos para las siguientes extensiones:

(1) $\mathbb{Q}(\sqrt{2},\sqrt[3]{3})/\mathbb{Q}$,
(2) $\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}$,
(3) $\mathbb{Q}(\sqrt{2},\sqrt[3]{3},\sqrt[5]{5})/\mathbb{Q}$,
(4) $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

Ref.: 4162e_040 SOLUCIÓN

Ejercicio. 10.11.
Determinar un elemento primitivo del cuerpo de descomposición, sobre $\mathbb{Q}$*, del polinomio* X^5-2.
Ref.: 4162e_105 SOLUCIÓN

Ejercicio. 10.12.
Se considera la extensión $F=\mathbb{Q}(\sqrt{2},\sqrt{3},\alpha)/\mathbb{Q}$*, donde* $\alpha^2=(2+\sqrt{2})(3+\sqrt{3})$.

(1) Prueba que $F=\mathbb{Q}(\alpha)$*, esto es, que* α *es un elemento primitivo para la extensión.*
(2) Determina $\mathrm{Irr}(\alpha,\mathbb{Q})$ *y su cuerpo de descomposición* E *sobre* $\mathbb{Q}$.
(3) Calcula $\mathrm{Gal}(E/\mathbb{Q})$*; comprueba que es isomorfo a* Q_2.

Relacionar con el Ejercicio (8.47.).
Ref.: 4162e_133 SOLUCIÓN

Ejercicio. 10.13.
Sea F/K *una extensión de cuerpos y* $\alpha,\beta\in F$ *elementos algebraicos sobre* K*. Prueba que si* α *es separable sobre* K*, entonces existe* $\gamma\in F$ *tal que* $K(\alpha,\beta)=K(\gamma)$.
Ref.: 4162e_125 SOLUCIÓN

Ejercicio. 10.14.
Sea F/K una extensión separable de grado n (¡no necesariamente de Galois!). Demuestra que $\alpha \in F$ es primitivo si, y sólo si, tiene n conjugados en cualquier clausura algebraica de K que contenga a F.
Ref.: 4162e_041 SOLUCIÓN

Ejercicio. 10.15.
Sea K un cuerpo y $K(\alpha,\beta)/K$ una extensión algebraica. Si α es separable, prueba que $K(\alpha,\beta)/K$ es una extensión simple (tiene un elemento primitivo).
Ref.: 4162e_099 SOLUCIÓN

Ejercicio. 10.16.
Sea K un cuerpo, y α un elemento algebraico sobre K. Prueba que la extensión $K(\alpha)/K$ tiene un número finito de cuerpos intermedios.
Ref.: 4162e_126 SOLUCIÓN

Ejercicio. 10.17.
Determina un elemento primitivo $\alpha \in \mathbb{Q}(\sqrt[3]{3},\omega)/\mathbb{Q}$, donde ω es una raíz cúbica primitiva de la unidad, de forma que $\{\varphi(\alpha) \mid \varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{3},\omega)\mathbb{Q})\}$ sea una base normal.
Ref.: 4162e_073 SOLUCIÓN

Ejercicio. 10.18.
Sea E/K una extensión de Galois de grado n y $\alpha \in E$. Demuestra que el polinomio

$$f(X) = \prod_{\sigma \in \mathrm{Gal}(E/K)} (X - \sigma(\alpha))$$

pertenece a $K[X]$, y que es irreducible si, y sólo si, $E = K(\alpha)$.
Ref.: 4162e_056 SOLUCIÓN

Ejercicio. 10.19.
Sea K un cuerpo, $\overline{K}$ una clausura algebraica de K, y $\sigma \in \mathrm{Aut}(\overline{K}/K)$ (σ no es necesariamente sobreyectivo). Si $F = \overline{K}^{\sigma}$, y $F \subseteq E \subseteq \overline{K}$ verifica que E/F es una extensión finita, entonces que E/F es una extensión de Galois con grupo de Galois cíclico.
Ref.: 4162e_074 SOLUCIÓN

Ejercicio. 10.20.
Dada la extensión $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, determina un elemento primitivo α tal que $\{\varphi(\alpha) \mid \varphi \in \mathrm{Gal}(E/\mathbb{Q})\}$ sea una base normal.
Ref.: 4162e_103 SOLUCIÓN

Ejercicio. 10.21.
Determina la matriz del endomorfismo de Frobenius, respecto a la base $\{1, x, x^2, \ldots\}$, en cada una de las extensiones, siendo x la clase de X:

(1) $\mathbb{F}_9/\mathbb{F}_3$,
(2) $\mathbb{F}_{27}/\mathbb{F}_3$,
(3) $\mathbb{F}_{729}/\mathbb{F}_3$,
(4) $\mathbb{F}_{729}/\mathbb{F}_9$,
(5) $\mathbb{F}_{729}/\mathbb{F}_{27}$.

Calcula para cada una de las extensiones un elemento primitivo.
Ref.: 4162e_102 SOLUCIÓN

Ejercicio. 10.22.
Sea K un cuerpo de característica p y $F = K(\alpha, \beta)$ con $\alpha^p, \beta^p \in K$ y $[F : K] = p^2$. Demuestra que:

(1) F/K no es simple.
(2) Existe un número infinito de cuerpos intermedios en la extensión F/K.

Ver también el Ejercicio (10.25.)
Ref.: 4162e_042 SOLUCIÓN

Ejercicio. 10.23.
Prueba que existen extensiones de cuerpos F/K y elementos $\alpha, \beta \in F$ algebraicos sobre K, tales que $K(\alpha, \beta)$ no es de la forma $K(\gamma)$, para un $\gamma \in K(\alpha, \beta)$, esto es, la extensión $K(\alpha, \beta)/K$ no es una ***extensión simple****.*
Ref.: 4162e_127 *SOLUCIÓN*

Ejercicio. 10.24.
Sea K un cuerpo de característica $p \neq 0$. Si s, t son indeterminadas sobre K,
(1) Demuestra que $[K(s,t) : K(s^p, t^p)] = p^2$.
(2) Si K es infinito, demuestra que hay infinitas extensiones intermedias $K(s^p, t^p) \subseteq E \subseteq K(s,t)$.

Ref.: 4162e_112 *SOLUCIÓN*

Ejercicio. 10.25.
Ejemplo de una extensión finita con un número infinito de cuerpos intermedios.
Ver también el Ejercicio (10.22.)
Ref.: 4162e_088 *SOLUCIÓN*

11. El cuerpo de los números complejos es algebraicamente cerrado

El cuerpo $\mathbb{C}$ de los números complejos se define como $\mathbb{C} = \mathbb{R}(i)$. Cada número complejo se escribe, de forma única como $z = a + bi$, con $a, b \in \mathbb{R}$, y si llamamos $|z| = \sqrt{a^2 + b^2}$ al módulo de z, entonces $z = |z|(c + di)$, con $c + di$ un número complejo de módulo uno.
Todo número complejo de módulo uno $c + di$ se puede escribir como $c + di = \cos\theta + i\text{sen}\theta$, donde $0 \leq \theta < 2\pi$, que abreviadamente representamos por $e^{i\theta}$.
La multiplicación de $e^{i\theta}$ por $e^{i\tau}$ es $e^{i(\theta+\tau)}$, y como el módulo es multiplicativo, para dos números complejos $z_1 = m_1 e^{i\theta}$ y $z_2 = m_2 e^{i\tau}$, la multiplicación es: $z_1 z_2 = m_1 m_2 e^{i(\theta+\tau)}$. En consecuencia es fácil determinar la raíz cuadrada de un número complejo $z = me^{i\theta}$; ésta es: $\sqrt{z} = \sqrt{m}e^{i\frac{\theta}{2}}$.

Lema. 11.1.
$\mathbb{C}$ *no tiene extensiones de grado 2.*

DEMOSTRACIÓN. Dada una extensión $F/\mathbb{C}$ de grado 2, sea $\alpha \in F$ de grado 2 sobre $\mathbb{C}$, con polinomio mónico irreducible $X^2 + bX + c$, entonces

$$X^2 + bX + c = \left(X + \frac{b}{2}\right)^2 - \left(\frac{b}{2} - c\right),$$

por tanto $F = \mathbb{C}(\alpha) = \mathbb{C}(\beta)$, donde β es raíz de un polinomio del tipo $X^2 - d$, y por tanto un elemento de $\mathbb{C}$, lo que es una contradicción. □

Veamos ahora que $\mathbb{R}$ no tiene extensiones propias de grado impar.

Lema. 11.2.
$\mathbb{R}$ *no tiene extensiones propias de grado impar.*

DEMOSTRACIÓN. Sea $F/\mathbb{R}$ una extensión propia de grado impar, entonces existe $\alpha \in F$ con $f(X) = \text{Irr}(\alpha, \mathbb{R})$ de grado impar. Sea $f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, y tomamos $c > \max\{|a_i| \mid i = 0, l \ldots, a_{n-1}\} \cup \{1\}$. Se tiene:

$$f(-nc) = (-nc)^n + \sum_{i=0}^{n-1} a_i(-nc)^i < (-nc)^n + \sum_{i=0}^{n-1} c(nc)^i \leq (-nc)^n + nc(nc)^{n-1} = 0,$$
$$f(nc) = (nc)^n + \sum_{i=0}^{n-1} a_i(nc)^i > (nc)^n - \sum_{i=0}^{n-1} c(nc)^i \geq (nc)^n - nc(nc)^{n-1} = 0.$$

4162-07.tex

Como consecuencia del teorema de Bolzano, resulta que $f(X)$ tiene una raíz en el intervalo $(-nc, nc)$, lo que es una contradicción. □

Teorema. 11.3.
$\mathbb{C}$ *es algebraicamente cerrado.*

DEMOSTRACIÓN. Sea $F/\mathbb{C}$ una extensión finita de $\mathbb{C}$; tomamos $\alpha \in F \setminus \mathbb{C}$ y $f(X) = \mathrm{Irr}(\alpha, \mathbb{C})$. Si E es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{C}$, entonces también E es el cuerpo de descomposición del polinomio $(X^2+1)f(X)$ sobre $\mathbb{R}$, y por tanto $E/\mathbb{R}$ es una extensión de Galois. Sea $G = \mathrm{Gal}(E/\mathbb{R})$ su grupo de Galois $2^m h$ su orden, siendo h un entero impar.

Sea $H \subseteq G$ un 2–subgrupo de Sylow de G, entonces $E^H/\mathbb{R}$ es una extensión, posiblemente no es de Galois, pero es de grado h, que es impar. Entonces $h = 1$, y G es un 2–grupo. Todo 2–grupo es soluble, y por lo tanto tiene una serie de composición, en este caso con factores de composición de orden 2, y como la extensión $E/\mathbb{R}$ tiene una torre de subcuerpos: $\mathbb{R} = F_0 \subseteq \mathbb{C} = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m = E$; en particular $F_2/\mathbb{C}$ sería una extensión de grado 2, lo que es una contradicción. Tenemos entonces $F = \mathbb{C}$, y $\mathbb{C}$ es algebraicamente cerrado. □

11.1. Ejercicios

El cuerpo de los números complejos es algebraicamente cerrado

Ejercicio. 11.4.
Probar que $\mathbb{C}$ es algebraicamente cerrado.
Ref.: 4162e_106 *SOLUCIÓN*

11.2. Cuestiones

En las siguientes cuestiones responde "VERDADERO" ó "FALSO" y haz un breve razonamiento para justificar la respuesta.

(1) ☐ Un cuerpo K es perfecto si, y sólo si, es finito o contiene una copia de $\mathbb{Q}$. (Ref.: 4162q_001)

(2) ☐ Si E/K y F/K son extensiones de Galois, entonces $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(F/K)$ si, y sólo si, $E \cong F$. (Ref.: 4162q_002)

(3) ☐ Sea F/K una extensión de cuerpos y $f \in K[X]$. Si f es separable sobre F, entonces es separable sobre K. (Ref.: 4162q_003)

(4) ☐ Sea F/K una extensión de cuerpos y $f \in K[X]$. Si f es separable sobre K, entonces es separable sobre F. (Ref.: 4162q_004)

(5) ☐ Si E/K es una extensión de Galois, entonces E/K tiene un elemento primitivo si, y sólo si, $\mathrm{Gal}(E/K)$ es un grupo simple. (Ref.: 4162q_005)

(6) ☐ Si F/K es una extensión de grado 2 existe un automorfismo $\sigma : F/K \longrightarrow F/K$ cuyo cuerpo fijo es K. (Ref.: 4162q_006)

(7) ☐ Si F/K es una extensión de grado 2, con K un cuerpo perfecto, existe un automorfismo $\sigma : F/K \longrightarrow F/K$ cuyo cuerpo fijo es K. (Ref.: 4162q_007)

(8) ☐ Toda extensión finita y separable está contenida en una extensión de Galois. (Ref.: 4162q_009)

(9) ☐ Toda extensión finita y normal F/K está contenida en una extensión de Galois E/K, con $F \subseteq E$. (Ref.: 4162q_010)

(10) ☐ Si E/K una extensión finita de Galois, y F un cuerpo intermedio: $K \subseteq F \subseteq E$, entonces F/K es una extensión de Galois. (Ref.: 4162q_011)

(11) ☐ Si $f(X) = X^n - a \in \mathbb{Q}[X]$, $a \neq 0$, y $\xi = \xi_n$ una raíz n–ésima primitiva de la unidad, el cuerpo de descomposición de f sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt[n]{a}, \xi_n)$. (Ref.: 4162q_012)

(12) ☐ La extensión $\mathbb{Q}(\sqrt[3]{3}, i)$ es de Galois. (Ref.: 4162q_013)

(13) ☐ Si $K \subseteq F \subseteq E$ es una torre de cuerpos y E/K es de Galois, entonces F/K es de Galois. (Ref.: 4162q_016)

(14) ☐ Si $K \subseteq F \subseteq E$ es una torre de cuerpos y E/K es de Galois, entonces E/F es de Galois. (Ref.: 4162q_017)

4162-99.tex

(15) ☐ Como $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$, se que $|\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})| = 4$. (Ref.: 4162q_018)

(16) ☐ Se tiene que $|\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})| = 2$ aunque $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. (Ref.: 4162q_019)

(17) ☐ El cuerpo $\mathbb{Q}(\sqrt[6]{2})$ tiene sólo tres conjugados sobre $\mathbb{Q}$. (Ref.: 4162q_020)

(18) ☐ El grupo $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ tiene orden 3. (Ref.: 4162q_022)

(19) ☐ Toda extensión E/K de grado 2 es de Galois. (Ref.: 4162q_023)

(20) ☐ Para todo α, elemento algebraico sobre $\mathbb{Q}$ de grado m, existen exactamente m automorfismos $\mathbb{Q}(\alpha)/\mathbb{Q} \longrightarrow \mathbb{Q}(\alpha)/\mathbb{Q}$. (Ref.: 4162q_024)

(21) ☐ Para todo α, elemento algebraico sobre $\mathbb{Q}$, si $F/\mathbb{Q}$ es una extensión normal, entonces $F(\alpha)/\mathbb{Q}(\alpha)$ es también una extensión normal. . (Ref.: 4162q_025)

(22) ☐ Si F/K es una extensión de Galois se verifica que para cada extensión intermedia $K \subseteq L \subseteq F$ la extensión L/K es de Galois si, y solo si, cada subgrupo de $\mathrm{Gal}(F/K)$ es un subgrupo normal. (Ref.: 4162q_026)

(23) ☐ Si K es un cuerpo perfecto, todo polinomio irreducible de grado n tiene n raíces distintas en una clausura algebraica de K. (Ref.: 4162q_027)

(24) ☐ Toda extensión F/K de grado primo p es de Galois. (Ref.: 4162q_029)

(25) ☐ Toda extensión E/K de grado 3 es normal. (Ref.: 4162q_030)

(26) ☐ Toda extensión E/K de grado 2 es normal. (Ref.: 4162q_031)

(27) ☐ Si $K \subseteq F \subseteq E$ es una torre de cuerpos y $\mathrm{Gal}(E/K)$ es un grupo abeliano, entonces F/K y E/F son extensiones de Galois. (Ref.: 4162q_032)

(28) ☐ Si $K \subseteq F \subseteq E$ es una torre de cuerpos, F/K y E/F son extensiones de Galois si, y sólo si, E/K es una extensión de Galois. (Ref.: 4162q_033)

(29) ☐ Si F/K es una extensión y $\mathrm{Aut}(F/K)$ es finito, entonces F/K es una extensión finita. (Ref.: 4162q_034)

(30) ☐ La extensión F/K, con $K = \mathbb{C}(T_n^3 \mid n \in \mathbb{N})$ y $F = \mathbb{C}(T_n \mid n \in \mathbb{N})$, no es finita, pero es algebraica, por lo que cada subextensión finitamente generada sobre K es finita. (Ref.: 4162q_035)

(31) ☐ Sean X e Y indeterminadas sobre $\mathbb{C}$. La extensión $\mathbb{C}(X,Y)/\mathbb{C}(X^3,Y^3)$ tiene grupo de Galois $C_3 \times C_3$. (Ref.: 4162q_036)

(32) ☐ La extensión $\mathbb{Q}(X,Y,\omega)/\mathbb{Q}(X^3,Y^3)$ tiene grupo de Galois $C_2 \times C_3 \times C_3$, donde ω es una raíz cúbica primitiva de la unidad. (Ref.: 4162q_037)

(33) ☐ Si F/K es una extensión finita y separable y $|\mathrm{Hom}(F/K, \overline{K}/K)| = [F : K]$, entonces la extensión F/K es de Galois. (Ref.: 4162q_038)

(34) ☐ Si F/K es una extensión finita normal, entonces F/E es una extensión normal para cada subcuerpo $K \subseteq E \subseteq F$. (Ref.: 4162q_055)

(35) ☐ Si $K \subseteq K(a)$ es una extensión finita normal simple, entonces $\mathrm{Aut}(K(a)/K)$ es un grupo simple. (Ref.: 4162q_056)

(36) ☐ Para una indeterminada X la extensión $\mathbb{F}_5(X^{10}) \subseteq \mathbb{F}_5(X)$ es separable. (Ref.: 4162q_057)

(37) ☐ Todo polinomio irreducible de grado n sobre un cuerpo perfecto K tiene siempre n raíces distintas en $\overline{K}$. (Ref.: 4162q_058)

(38) ☐ Todo cuerpo K tiene una extensión algebraica $K \subseteq F$ que es un cuerpo perfecto. (Ref.: 4162q_059)

(39) ☐ Para cada extensión normal $K \subseteq F \subseteq \overline{K}$ cada homomorfismo $\sigma : F \longrightarrow \overline{K}$ define un automorfismo de F/K. (Ref.: 4162q_060)

(40) ☐ Toda extensión finita de un cuerpo K es separable sobre K. (Ref.: 4162q_061)

(41) ☐ Dado un cuerpo K y un automorfismo de cuerpos $f : K \longrightarrow K$, el conjunto de todos los elementos de K que quedan fijos por f forma un cuerpo. (Ref.: 4162q_063)

(42) ☐ Sean $a, b \in F$, donde $F \subseteq \overline{K}$ es un cuerpo de descomposición sobre K, esto es, $K \subseteq F$ es normal. Entonces existe un automorfismo de F/K que lleva a a b si, y sólo si, $\mathrm{Irr}(a, K) = \mathrm{Irr}(b, K)$. (Ref.: 4162q_064)

(43) ☐ Todo polinomio de grado n sobre un cuerpo perfecto K tiene siempre n raíces distintas en $\overline{K}$. (Ref.: 4162q_065)

(44) ☐ El polinomio $X^4+1 \in K[X]$ es siempre separable sea cual sea el cuerpo K. (Ref.: 4162q_066)

Capítulo III

Extensiones especiales

Introducción

Introducción.

4163-00.tex

12. Cuerpos finitos

Vamos a estudiar en esta lección cuerpos que tienen un número finitos de elementos, los llamaremos **cuerpos finitos** o **cuerpos de Galois**. Si el cuerpo F es finito, su característica, $\text{car}(F)$, no es cero, por lo tanto $\text{car}(F)$ es igual a un número primo positivo, si suponemos que es p, el cuerpo característico K de F es isomorfo a $\mathbb{F}_p = \mathbb{Z}_p$, y lo que es más importante, F es un espacio vectorial de dimensión finita sobre $\mathbb{F}_p$, por lo tanto el número de elementos de F es una potencia de p.

Lema. 12.1.
Si F es un cuerpo finito de característica p que tiene q elementos, existe un número entero positivo n tal que $q = p^n$.

DEMOSTRACIÓN. Tenemos que $F/\mathbb{F}_p$ es una extensión finita de cuerpos, si suponemos que $[F : \mathbb{F}_p] = n$, entonces el número de elementos de F es p^n. □

Vamos a estudiar el grupo multiplicativo de un cuerpo finito.

Lema. 12.2.
Sea F un cuerpo, no necesariamente finito, y G un subgrupo finito del grupo multiplicativo $F^\times$ de F, entonces G es un grupo cíclico. En particular, el grupo multiplicativo de todos los elementos no nulos de un cuerpo finito es un grupo cíclico.

DEMOSTRACIÓN. Ya que G es un grupo abeliano finito, será isomorfo a un producto directo $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$, donde n_i divide a n_{i+1}, $1 \leq i < r$. Para cada $a_i \in \mathbb{Z}_{n_i}$ tenemos $a_i^{n_i} = 1 = a_i^{n_r}$, y todo elemento de G es raíz del polinomio $X^{n_r} - 1$. Como consecuencia el número de elementos de G está acotado superiormente por n_r; sin embargo el número de elementos de G sabemos que es $n_1 \dots n_r$, por lo tanto $|G| = n_r$ y G es un grupo cíclico.
El caso del cuerpo finito es inmediato. □

Vamos ahora a probar que para cada entero primo positivo p y cada número entero positivo n existe salvo isomorfismo un único, cuerpo F con p^n elementos.

4163-01.tex

Teorema. 12.3. (Teorema de Moore)
Sea p un entero positivo primo y n un entero positivo, existe un cuerpo finito F con $q = p^n$ elementos. Este cuerpo F puede ser construido como el cuerpo de descomposición del polinomio $X^q - X$ sobre $\mathbb{F}_p$. Además todo cuerpo finito de q elementos es isomorfo, sobre $\mathbb{F}_p$, a F.

DEMOSTRACIÓN. Consideramos el polinomio $X^q - X$ sobre $\mathbb{F}_p$, su cuerpo de descomposición F tiene característica p y contiene a todas las raíces de $X^q - X$; supongamos que α y β son raíces, entonces

$$\begin{aligned}(\alpha+\beta)^q &= \alpha^q + \beta^q = \alpha + \beta,\\ (\alpha\beta)^q &= \alpha^q\beta^q = \alpha\beta,\\ 1^q &= 1;\end{aligned}$$

y las raíces de $X^q - X$ forman un subanillo de F. Además, si $\alpha \neq 0$ es una raíz, se verifica

$$(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1},$$

luego las raíces forman un subcuerpo de F. Como la derivada del polinomio es:

$$D(X^q - X) = qX^{q-1} - 1 = -1,$$

resulta que las raíces de $X^q - X$ son simples, y por tanto tenemos un cuerpo de q elementos; contenido en F en el que el polinomio $X^q - X$ descompone, entonces coincide con F y F tiene q elementos.
Supongamos ahora que tenemos un cuerpo F con q elementos; el grupo multiplicativo $F^\times$ es cíclico de orden $q-1$, entonces para cada elemento $\alpha \in F^\times$ se tiene $\alpha^{q-1} = 1$, por lo tanto para cada $\alpha \in F$ se tiene $\alpha^q = \alpha$, y cada elemento de F es raíz del polinomio $X^q - X$; el número de raíces distintas de este polinomio es q, entonces F es el cuerpo de descomposición del polinomio $X^q - X$ sobre $\mathbb{F}_p$, y por lo tanto todos los cuerpos de q elementos son isomorfos sobre $\mathbb{F}_p$. □

Existe una notación estándar para el cuerpo finito de q elementos, ésta es $\mathbb{F}_q$, y se llama el **cuerpo de Galois** de q elementos. Recordar que q es de la forma p^n, siendo p y n números enteros positivos y p además primo.
Vamos a estudiar la extensión $\mathbb{F}_q/\mathbb{F}_p$, identificar sus automorfismos, y ver que es una extensión de Galois con grupo de Galois cíclico.

Teorema. 12.4.
En la situación anterior para p, n y $q = p^n$, tenemos:
(1) $\mathbb{F}_q/\mathbb{F}_p$ es una extensión de Galois.
(2) $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ es un grupo cíclico de orden n generado por el automorfismo de Frobenius.

DEMOSTRACIÓN. (1). Ya que $\mathbb{F}_p$ es un cuerpo finito entonces es perfecto, y por lo tanto toda extensión finita de $\mathbb{F}_p$ es separable; en particular $\mathbb{F}_q/\mathbb{F}_p$ es una extensión separable. Ya que $\mathbb{F}_q$ es el cuerpo de descomposición del polinomio $X^q - X$, resulta que la extensión $\mathbb{F}_q/\mathbb{F}_p$ es normal. Entonces $\mathbb{F}_q/\mathbb{F}_p$ es una extensión de Galois.
(2). Tenemos $[\mathbb{F}_q : \mathbb{F}_p] = n$, y por tanto $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = n$. Si consideramos ϕ el automorfismo de Frobenius, tenemos que $\phi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ ya que para $a \in \mathbb{F}_p$ tenemos que $\phi(a) = a^p = a$. Las potencias de ϕ también pertenecen a $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, para $0 \leq i < n$ y $\alpha \in \mathbb{F}_q$ tenemos por inducción:

$$\phi^i(\alpha) = \phi\phi^{i-1}(\alpha) = \phi(\phi^{i-1}(\alpha)) = \phi(\alpha^{p^{i-1}}) = (\alpha^{p^{i-1}})^p = \alpha^{p^i}.$$

Vamos ahora a ver $\phi^0, \phi, \ldots, \phi^{n-1}$ son todos distintos. Supongamos que $\phi^i = 1$, para $0 \leq i < n$, entonces para cada $\alpha \in \mathbb{F}_q$ tenemos:

$$\alpha = 1(\alpha) = \phi^i(\alpha) = \alpha^{p^i},$$

y por tanto todo elemento de $\mathbb{F}_q$ es raíz del polinomio $X^{p^i} - X$, como consecuencia $\mathbb{F}_q$ tiene como máximo p^i elementos, lo que es una contradicción. □

Corolario. 12.5.
Con las notaciones anteriores son equivalentes:
(a) $\alpha^{p^r} = \alpha$, *para cada* $\alpha \in \mathbb{F}_{p^n}$.
(b) $n|r$.

DEMOSTRACIÓN. (a) ⇒ (b). Si se verifica (a), entonces $\phi^r = 1$, y por tanto $n|r$, ya que el orden de $\phi \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es n.
(b) ⇒ (a). Si $n|r$, entonces $\phi^r = 1$ y se verifica (a). □

Proposición. 12.6.
Sea $q = p^n$. *Los subcuerpos de* $\mathbb{F}_q$ *están determinados por los divisores de n, esto es; los subcuerpos de* $\mathbb{F}_q$ *son de la forma* $\mathbb{F}_{p^m}$, *para* $m|n$. *Además, para cada entero positivo r son equivalentes:*
(a) $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^r}$.
(b) $m|r$.

En particular, la extensión $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^r}$ *es de Galois con grupo de Galois cíclico de orden* r/m *y generado por* ϕ^m.

DEMOSTRACIÓN. Es claro que todo subcuerpo de $\mathbb{F}_{p^n}$ es de la forma $\mathbb{F}_{p^m}$ con $m \leq n$, y además tenemos

$$n = [\mathbb{F}_{p^n} : \mathbb{F}] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]m,$$

por lo tanto $m|n$, y en particular $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \frac{n}{m}$.

(a) $\Rightarrow$ (b). Si $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^r}$, entonces $m|r$, es como en el caso anterior.

(b) $\Rightarrow$ (a). Si $m|r$, entonces supongamos que $r = md$. Por ser $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ un grupo cíclico de orden r generado por el automorfismo de Frobenius ϕ, existe un único subgrupo H de orden d, que es cíclico y está generado por ϕ^m. En la conexión de Galois H corresponde a un subcuerpo $\mathbb{E} = (\mathbb{F}_{p^r})^H$, que está determinado por $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{E}) = H$; ya que H es un subgrupo normal de $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$, tenemos que $\mathbb{E}/\mathbb{F}_p$ es una extensión de Galois y $\mathrm{Gal}(\mathbb{E}/\mathbb{F}_p) \cong \mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)/\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{E})$ tiene orden $r/d = m$, luego $\mathbb{E} = \mathbb{F}_{p^m}$; por lo tanto $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^r}$ y $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_{p^m})$ es cíclico de orden r/m generado por ϕ^m. □

Corolario. 12.7.
Si p es un número entero primo positivo y n, m números enteros positivos, son equivalentes:
(a) $m|n$.
(b) $p^m - 1 | p^n - 1$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si $m|n$, entonces $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, y por tanto $\mathbb{F}_{p^m}^\times \subseteq \mathbb{F}_{p^n}^\times$, luego $p^m - 1 | p^n - 1$.

(b) $\Rightarrow$ (a). Supongamos que $p^m - 1 | p^n - 1$; para una descomposición $n = cm + r$ de n, con $0 \leq r < m$, tenemos

$$p^n = p^{cm} p^r,$$

luego

$$p^n - p^r = p^r(p^{cm} - 1);$$

por la implicación (a)$\Rightarrow$(b), aplicada a $m|cm$, tenemos:

$$p^m - 1 | p^{cm} - 1,$$

y por tanto

$$\begin{array}{lll} p^n - p^r \equiv 0 & \pmod{p^m - 1}, & \\ p^n \equiv p^r & \pmod{p^m - 1}, & \\ p^n - 1 \equiv p^r - 1 & \pmod{p^m - 1}, & \text{y tenemos que} \\ p^r - 1 \equiv 0 & \pmod{p^m - 1}, & \text{lo que implica} \\ p^m - 1 \,|\, p^r - 1, & & \end{array}$$

pero $0 \leq r < m$, luego necesariamente $r = 0$ y $n = cm$, esto es, $m|n$. □

Teorema. 12.8.
Para cualquier cuerpo finito $\mathbb{F}$ y cualquier número entero positivo m existe un polinomio irreducible $f(X) \in \mathbb{F}[X]$ de grado m.

DEMOSTRACIÓN. Supongamos que $\mathbb{F} = \mathbb{F}_q$, $q = p^n$, para m existe una extensión $\mathbb{F}_{q^m}/\mathbb{F}_q$ de grado m, tenemos que $\mathbb{F}_{q^m} = \mathbb{F}_{p^{nm}}$. El grupo multiplicativo $\mathbb{F}_{q^m}$ es cíclico; sea α un generador; si α es de grado r sobre $\mathbb{F}_q$, entonces $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = r$, luego $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$, y por tanto α verifica $\alpha^{q^r} = \alpha$, luego $\alpha^{q^r-1} = 1$ y $q^m - 1 | q^r - 1$, entonces $m|r$ y $m = r$; tenemos pues $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Si tomamos el polinomio irreducible de α sobre $\mathbb{F}_q$, $\mathrm{Irr}(\alpha, \mathbb{F}_q)$, entonces $\mathrm{Irr}(\alpha, \mathbb{F}_q)$ tiene grado m. □

Opcional. Teorema de Wedderburn

El último resultado que vamos a estudiar relativo a cuerpos finitos es el **Teorema de Wedderburn** (1905) que caracteriza los anillos de división finitos como cuerpos finitos.

Teorema. 12.9.
Todo anillo de división finito es conmutativo.

DEMOSTRACIÓN. [Witt, 1931] Supongamos que F es un anillo de división finito, si $\alpha \in F$, llamamos

$$C(\alpha) = \{x \in F \mid \ x\alpha = \alpha x\}$$

al centralizador de α en F, y

$$\mathrm{Cen}(F) = \{x \in F \mid \ \alpha x = x\alpha \text{ para cada } \alpha \in F\} = \cap\{C(\alpha) \mid \ \alpha \in F\}$$

al centro de F. Tenemos que $\mathrm{Cen}(F)$ es un anillo finito, y además es un cuerpo; si $x \in \mathrm{Cen}(F)$, entonces $x^{-1} \in \mathrm{Cen}(F)$:

$$\alpha x^{-1} = x^{-1}x\alpha x^{-1} = x^{-1}\alpha x x^{-1} = x^{-1}\alpha, \text{ para cada } \alpha \in F.$$

Entonces $\mathrm{Cen}(F)$ es un cuerpo finito, supongamos que tenga $q = p^n$ elementos; ya que F es un espacio vectorial sobre $\mathrm{Cen}(F)$, y es finito, su dimensión es finita, supongamos que $\dim_{\mathrm{Cen}(F)}(F) = m$, entonces F tiene q^m elementos. También $C(\alpha)$ es un espacio vectorial sobre $\mathrm{Cen}(F)$, y por tanto el número de elementos de $C(\alpha)$ es un número de la forma q^{m_α}, para $m_\alpha = \dim_{\mathrm{Cen}(F)}(C(\alpha))$, $m_\alpha \leq m$, para cada $\alpha \in F$.
Si $m = 1$, entonces $\mathrm{Cen}(F) = F$ y F es conmutativo. Si $m \neq 1$, entonces procedemos como sigue:

El número de elementos no nulos de $\mathrm{Cen}(F)$ y $C(\alpha)$ son respectivamente $q-1$ y $q^{m_\alpha}-1$, y $\mathrm{Cen}(F)^\times$, $C(\alpha)^\times$ son subgrupos de $F^\times$, por lo tanto $q-1|q^m-1$ y $q^{m_\alpha}-1|q^m-1$, luego $m_\alpha|m$.
Consideramos ahora la relación de conjugación en $F^\times$, la fórmula de las clases se puede escribir

$$q^m-1=(q-1)+\sum\{[F^\times:C(\alpha_i)^\times]\mid\ 1\le i\le r\},$$

donde los α_i son representantes de las distintas clases de conjugación de $F^\times$ no contenidas en $\mathrm{Cen}(F)^\times$, los $[F^\times:C(\alpha_i)^\times]$ son mayores que 1, los $C(\alpha_i)^\times$ son los normalizadores de los α_i, y r es mayor que 1, ya que $n\neq 1$. Tenemos

$$[F^\times:C(\alpha_i)^\times]=(q^m-1)/(q^{m_{\alpha_\iota}}-1),$$

entonces

$$q^m-1=(q-1)+\sum\{(q^m-1)/(q^{m_{\alpha_i}}-1)\mid\ 1\le i\le r\},$$

donde ahora los m_{α_i} verifican $m_{\alpha_i}|m$ y $m_{\alpha_i}\neq m$.
Si consideramos los polinomios ciclotómicos tenemos:

$$X^m-1=\prod\{\Phi_d(X)\mid\ d|m\},$$

entonces

$$(X^m-1)/(X^d-1)=\prod\{\Phi_e(X)\mid\ e|m,\ \text{y } e\nmid d\};$$

si $d\neq m$, entonces $\Phi_m(X)$ es un factor de $(X^m-1)/(X^d-1)$, y se verifica cuando tomamos $d=m_{\alpha_i}$ que

$$\Phi_m(q)\qquad\text{divide a}\qquad(q^m-1)/(q^{m_{\alpha_i}}-1),$$

y entonces

$$\Phi_m(q)\qquad\text{divide a}\qquad\sum\{(q^m-1)/(q^{m_{\alpha_i}}-1)\mid\ 1\le i\le r\},$$

y ya que $\Phi_m(q)$ divide a q^m-1, llegamos a que $\Phi_m(q)$ divide a $q-1$. Si consideramos estas relaciones en el cuerpo $\mathbb{C}$ de los números complejos, tenemos que

$$\Phi_m(q)=\prod\{q-\xi\mid\ \xi\text{ es una raíz }m\text{-ésima primitiva de la unidad en }\mathbb{C}\},$$

ya que $m\neq 1$, para cada ξ tenemos que $|q-\xi|>q-1$, y por tanto $|\Phi_m(q)|>q-1$, lo que es una contradicción con el hecho de que $\Phi_m(q)|q-1$. Como consecuencia no puede ser $m\neq 1$ y tenemos que F es conmutativo. □

Opcional. Cuerpos finitos. Logaritmo discreto

Dado un cuerpo finito $\mathbb{F}_q$, sabemos que existe un polinomio mónico irreducible $f(X)\in\mathbb{F}_p[X]$ tal que $\mathbb{F}_q\cong\frac{\mathbb{F}_p[X]}{(f)}$. Además, sabemos que existe un elemento primitivo $\alpha\in\mathbb{F}_q$ tal que $\mathbb{F}_q=\mathbb{F}_p(\alpha)$. Sin embargo, estamos más interesados en un generador ξ del grupo multipicativo $\mathbb{F}_q^\times$. este elemento ξ tendrá asociado un polinomio mónico irreducible $g(X)=\mathrm{Irr}(\xi,\mathbb{F}_p)$.
El primer problema con el que nos encontramos es el de determinar ξ y/o $g(X)$.

Problema. 12.10.
Da un algoritmo que, en tiempo polinomial dependiendo de p^n, encuentre un elemento primitivo de $\mathbb{F}_{p^n}$.[1]

Supongamos que tenemos ξ y $g(X)$; vamos a ver cómo hacer la aritmética de $\mathbb{F}_q$ de forma más efectiva.

Dado $\alpha \in \mathbb{F}_q^\times$, existe $e \in \mathbb{Z}_{q-1}$ tal que $\alpha = \xi^e$; esto nos permite definir una aplicación biyectiva $\rho : \mathbb{Z}_{q-1} \longrightarrow \mathbb{F}_q^\times$ mediante $\rho(m) = \xi^m$, que evidentemente lleva sumas a productos: es un antilogaritmo. De esta forma tenemos controlado el producto en $\mathbb{F}_q^\times$.

Para controlar el producto en $\mathbb{F}_q$, necesitamos el elemento $0 \in \mathbb{F}_q$, para lo que agregamos un elemento nuevo, $*$, a $\mathbb{Z}_{q-1}$, y extendemos la suma a $\mathbb{Z}_{q-1} \cup \{*\}$ definiendo $* = * + * = m + * = * + m$, para cada $m \in \mathbb{Z}_{q-1}$. De esta forma $\rho : \mathbb{Z}_{q-1} \cup \{*\} \longrightarrow \mathbb{F}_q$ es un homomorfismo biyectivo que lleva sumas en $\mathbb{Z}_{q-1} \cup \{*\}$ a productos en $\mathbb{F}_q$. La tabla del producto en $\mathbb{F}_q$ tendrá un análogo en la tabla de la suma en $\mathbb{Z}_{q-1} \cup \{*\}$.

Para controlar la suma en $\mathbb{F}_q$, definimos una nueva aplicación $\zeta : \mathbb{Z}_{q-1} \cup \{*\} \longrightarrow \mathbb{Z}_{q-1} \cup \{*\}$, a la que llamamos logaritmo de Zech, y que está definida por la relación $\xi^{\zeta(m)} = \xi^m + 1$ en $\mathbb{F}_q$. Observa que ζ es una biyección y que nos permite controlar la suma den $\mathbb{F}_q$, ya que se tiene:

$$\xi^i + \xi^j = (\xi^{i-j} + 1)\xi^j = \xi^{\zeta(i-j)}\xi^j.$$

Veamos cómo construir, en un ejemplo, las tablas antes mencionadas.

Supongamos que $\mathbb{F}_q = \dfrac{\mathbb{F}_p[X]}{(g(X))}$, siendo $g(X) \in \mathbb{F}_p[X]$ irreducible de grado n.

Se tiene $\rho(1) = \xi$, y para cada $m \in \mathbb{Z}_{q-1}$ se ha definido $\rho(m) = \xi^m$, que se expresa en la forma $f_m(\xi)$, donde $f_m(X)$ es el resto de la división de X^m or $g(X)$. Para simplificar representamos a $f_m(X)$ por $\rho(m)(X)$. Dados $s, t \in \mathbb{Z}_{q-1}$ tendremos los restos $\rho(s)(X)$ y $\rho(t)(X)$, que son polinomios de grados menor que n. La multiplicación en $\mathbb{F}_q^\times$ de ξ^s y ξ^t es $\xi^s\xi^t = \xi^{s+t}$, que se representa por el polinomio que es el resto de la división de X^{s+t} por $g(X)$; la representación de éste es $\rho(s+t)(X)$, y lo representamos también como $\rho(s)(X) \star \rho(t)(X)$. Podemos entonces construir la multiplicación en $\mathbb{F}_q^\times$ en la forma obvia a partir de la tabla de la suma en $\mathbb{Z}_{q-1}$. Por ejemplo, se tiene $\rho(m+1)(X) = \rho(1)(X) \star \rho(m)(X)$. A continuación podemos extender a la multiplicación en todo $\mathbb{F}_q$ y a la suma en $\mathbb{Z}_{q-1} \cup \{*\}$.

La construcción de la tabla de ζ es más o menos directa a partir de la definición.

Veamos un ejemplo con $p = 2$, $q = 16$ y $g(X) = X^4 + X + 1$. Si ξ una raíz de $g(X) = X^4 + X + 1 \in \mathbb{F}_2$,

[1] V. Shoup. Searching form primitive roots in finite fields. Math. Comp. **58** (1992), 369–380.

tenemos:

i	$\rho(i)$	$\zeta(i)$	i	$\rho(i)$	$\zeta(i)$
1	ξ	4	9	$\xi^3+\xi$	7
2	ξ^2	8	10	$\xi^2+\xi+1$	5
3	ξ^3	14	11	$\xi^3+\xi^2+\xi$	12
4	$\xi+1$	1	12	$\xi^3+\xi^2+\xi+1$	11
5	$\xi^2+\xi$	10	13	$\xi^3+\xi^2+1$	6
6	$\xi^3+\xi^2$	13	14	ξ^3+1	3
7	$\xi^3+\xi+1$	9	0	1	$*$
8	ξ^2+1	2	$*$	0	0

Observa que ξ es un generador del grupo multiplicativo $\mathbb{F}_q^\times$, ya que en la columna $\rho(i)$ aparecen todos los elementos de $\mathbb{F}_q^\times$.

12.1. Ejercicios

Cuerpos finitos

Ejercicio. 12.11. (Pequeño teorema de Fermat)
Sea p un entero primo positivo. Demuestra que $n^p \equiv n \pmod{p}$, para cada número entero positivo n.
Ref.: 4163e_083 SOLUCIÓN

Ejercicio. 12.12.
Identificar los grupos $\mathbb{F}_4^+$ y $\mathbb{F}_4^\times$.
Ref.: 4163e_001 SOLUCIÓN

Ejercicio. 12.13.
Escribe las tablas de sumar y multiplicar para $\mathbb{F}_4$ y $\mathbb{Z}_4$ y compararlas.
Ref.: 4163e_002 SOLUCIÓN

Ejercicio. 12.14.
Construir cuerpos con 4, 8 y 16 elementos. Da generadores de los correspondientes grupos multiplicativos.
Ref.: 4163e_003 SOLUCIÓN

Ejercicio. 12.15.
Construye una extensión de grado cinco sobre $\mathbb{F}_3$.
Ref.: 4163e_004 SOLUCIÓN

Ejercicio. 12.16.
Sea p un primo y $n \geq 1$.
(1) ¿Cuántos elementos α de $\mathbb{F}_{p^n}$ son generadores del grupo $\mathbb{F}_{p^n}^\times$? (Esto es, verifican $\mathbb{F}_{p^n}^\times = \langle\alpha\rangle$).
(2) ¿Cuantos elementos de $\mathbb{F}_{p^n}$ son primitivos (generadores del grupo multiplicativo) para la extensión $\mathbb{F}_{p^n}/\mathbb{F}_p$?

Ref.: 4163e_005 SOLUCIÓN

Ejercicio. 12.17.
Hallar una raíz decimotercera de 3 en el cuerpo $\mathbb{F}_{13}$.
Ref.: 4163e_006 SOLUCIÓN

Ejercicio. 12.18.
Para cada entero primo positivo p, llamamos $\mathscr{P}_{p,n}$ al número de polinomios mónicos irreducibles de grado n sobre $\mathbb{F}_p$.
(1) Prueba que $p^m = \sum\{j\mathscr{P}_{p,j} \mid j|m\}$.
(2) Si m es primo, prueba que se tiene $\mathscr{P}_{p,m} = \dfrac{p^m - p}{m}$.
(3) Determina el número de polinomios mónicos irreducibles de grado 3 sobre el cuerpo $\mathbb{F}_3$.
(4) Determina el número de polinomios mónicos irreducibles de grado 6 sobre el cuerpo $\mathbb{F}_3$.

Ref.: 4163e_007 SOLUCIÓN

Ejercicio. 12.19.
Descompón, en factores irreducibles sobre $\mathbb{F}_3[X]$, los siguientes polinomios:
(1) $X^9 - X$,
(2) $X^{27} - X$.

Ref.: 4163e_008 SOLUCIÓN

Ejercicio. 12.20.
Descompón el polinomio $X^{16}-X$ en los cuerpos $\mathbb{F}_4$ y $\mathbb{F}_8$.
Ref.: 4163e_009 SOLUCIÓN

Ejercicio. 12.21.
Si F es un cuerpo finito, demuestra que para cada entero positivo n existe un polinomio irreducible de grado n en $F[X]$. (Similar al resultado de teoría).
Ref.: 4163e_010 SOLUCIÓN

Ejercicio. 12.22.
Da un isomorfismo explícito entre los cuerpos de descomposición de X^3-X+1 y X^3-X-1 sobre $\mathbb{F}_3$.
Ref.: 4163e_011 SOLUCIÓN

Ejercicio. 12.23.
Sea F un cuerpo finito.

(1) Demuestra que el producto de todos los elementos no nulos de F vale -1.
*(2) Deduce el **teorema de Wilson**: Un número $n \in \mathbb{N}$, $n > 1$, es primo si, y sólo si, $(n-1)! \equiv -1$ (mód n).*

Ref.: 4163e_012 SOLUCIÓN

Ejercicio. 12.24.
Demuestra que todo elemento de $\mathbb{F}_p$ tiene exactamente una raíz p-ésima. Demuestra la misma propiedad para F_{p^n}.
Ref.: 4163e_013 SOLUCIÓN

Ejercicio. 12.25.
Sea p un primo. Describe los enteros n tales que existen un cuerpo finito $\mathbb{F}_n$ y un elemento $\alpha \in \mathbb{F}_n$ con $\alpha \neq 1$ pero $\alpha^p = 1$.
Ref.: 4163e_014 SOLUCIÓN

Ejercicio. 12.26.
Sean p, q enteros primos positivos. Determina el número de polinomios mónicos irreducibles de grado q en $\mathbb{F}_p[X]$.
Ref.: 4163e_015 SOLUCIÓN

Ejercicio. 12.27.
Sea p primo impar.
(1) Demuestra que exactamente la mitad de los elementos de $\mathbb{F}_p^\times$ son cuadrados y que si $u, v \in \mathbb{F}_p$ no son cuadrados, entonces uv es un cuadrado.
(2) Demuestra lo mismo que en el apartado anterior para cualquier cuerpo finito de orden impar.
(3) Demuestra que en un cuerpo finito de orden par todo elemento es un cuadrado.

Ref.: 4163e_016 SOLUCIÓN

Ejercicio. 12.28.
Demuestra que en un cuerpo finito todo elemento es suma de dos cuadrados.
Ref.: 4163e_017 SOLUCIÓN

Ejercicio. 12.29. (Extensiones Bicuadráticas)
Sea K un cuerpo de característica $p \neq 2$, y sea $F = K(\sqrt{d_1}, \sqrt{d_2})$ con $d_1, d_2 \in K$ dos elementos con la propiedad de que d_1, d_2 y $d_1 d_2$ no son cuadrados en K. La extensión $K(\sqrt{d_1}, \sqrt{d_2})/K$ se llama una ***extensión bicuadrática*** *de K. Ver el ejercicio (8.28.).*

Si K es un cuerpo finito, prueba que no existe ninguna extensión bicuadrática F/K.
Ref.: 4163e_019 SOLUCIÓN

Ejercicio. 12.30.
Demuestra que el polinomio irreducible $X^4+1 \in \mathbb{Z}[X]$ es reducible módulo cualquier primo p.
Ref.: 4163e_020 SOLUCIÓN

Ejercicio. 12.31.
Sea $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ una extensión bicuadrática, con $d_1, d_2 \in \mathbb{Z}$ tales que $d_1, d_2, d_1 d_2$ no son cuadrados en $\mathbb{Z}$ y $\theta = a + b\sqrt{d_1} + c\sqrt{d_2} + d\sqrt{d_1 d_2}$, $a, b, c, d \in \mathbb{Z}$. Demuestra que $\mathrm{Irr}(\theta, \mathbb{Q})$ es reducible módulo cualquier primo p.
En particular demuestra que el polinomio $x^4 - 10x^2 + 1$ es irreducible sobre $\mathbb{Z}[X]$ pero es reducible módulo cualquier primo p.
Ref.: 4163e_021 SOLUCIÓN

Ejercicio. 12.32. (F_p no tiene extensiones bicuadráticas)
Demuestra que uno de 2, 3 ó 6 es un cuadrado en $\mathbb{F}_p$, para cualquier primo p. Concluir que el polinomio $x^6 - 11x^4 + 36x^2 - 36 = (x^2-2)(x^2-3)(x^2-6)$ tiene una raíz módulo p, para cualquier primo p pero no tiene una raíz en $\mathbb{Z}$.
Ver Ejercicio (12.29.).
Ref.: 4163e_022 SOLUCIÓN

Ejercicio. 12.33.
Si p es un primo, demuestra que cualquier elemento algebraico sobre $\mathbb{F}_p$ está en algún $\mathbb{F}_{p^n}$ y deducir que la clausura algebraica de $\mathbb{F}_p$ es la union (dirigida) de los $\mathbb{F}_{p^n}$ con $n \geq 1$.
Ref.: 4163e_025 SOLUCIÓN

Ejercicio. 12.34.
Demostrar que $X^p - X - a$ con $a \neq 0$ es irreducible en $\mathbb{F}_p$ y que sobre $\mathbb{F}_{p^n}$ es irreducible si, y solo si, no tiene factores lineales.
Ver también Ejercicio (15.19.).
Ref.: 4163e_026 SOLUCIÓN

Ejercicio. 12.35.
Sea p un primo y sea $q = p^n$. Razonar que $f = X^q - X \in \mathbb{F}_p[X]$ tiene factores de grado n, pero no de grado superior.
Ref.: 4163e_028 SOLUCIÓN

Ejercicio. 12.36.
Sea $q = p^n$ una potencia de un entero primo positivo.

(1) *Demuestra que un polinomio irreducible de grado r sobre $\mathbb{F}_q$ es un factor de $X^{q^n} - X$ si, y sólo si, $r|n$.*
(2) *Deduce que $X^{q^n} - X = \prod_i f_i(X)$, donde f_i varía sobre todos los polinomios irreducibles cuyo grado divide a n.*
(3) *Demuestra que si t_r es el número de tales polinomios, entonces $\sum r t_r = q^n$, y deduce una fórmula para t_r en términos de q, r y la función de Möbius.*

Ref.: 4163e_029 SOLUCIÓN

Ejercicio. 12.37.
Sea $\mathfrak{p}$ un ideal primo no nulo del anillo $\mathbb{Z}[i]$ de los enteros de Gauss. Demuestra que $\mathbb{Z}[i]/\mathfrak{p}$ es un cuerpo finito. Demuestra además que los únicos cuerpos que pueden aparecer son de orden p ó p^2 donde p es un primo. Describe el anillo cociente por los ideales (7), $(2+i)$ (5). ¿Cuáles de ellos son cuerpos?
Ref.: 4163e_030 SOLUCIÓN

Ejercicio. 12.38.
Sea F un cuerpo finito y sea $n \geq 1$. Demuestra que existe un polinomio irreducible sobre F de grado n con el coeficiente de X distinto de cero.
Pista: Considera la ecuación para un u^{-1}.
Ref.: 4163e_031 SOLUCIÓN

Ejercicio. 12.39.
Factoriza en irreducibles los siguientes polinomios:
(1) X^8+X^7+X+1 *en* $\mathbb{F}_2[X]$.
(2) $X^{11}+X^{10}+X^7+X^6+X^5+X^4+X^3+X+1$ *en* $\mathbb{F}_2[X]$ *y en* $\mathbb{F}_4[X]$.
(3) $X^8+X^6-3X^4-3X^3+8X^2+2X-5$ *en* $\mathbb{F}_5[X]$.

Ref.: 4163e_032 SOLUCIÓN

Ejercicio. 12.40.
Un polinomio irreducible $f \in \mathbb{F}_q[X]$ se llama ***primitivo*** *si para una raíz α de f se verifica que $\mathbb{F}_q(\alpha)^\times = \langle\alpha\rangle$.*
(1) Demuestra que X^4+X+1 y X^4+X^3+1 son polinomios primitivos sobre $\mathbb{F}_2$, mientras que $X^4+X^3+X^2+X+1$ no es primitivo sobre $\mathbb{F}_2$.
(2) Determina todos los polinomios mónicos primitivos de grado cinco sobre $\mathbb{F}_2$ y los de grado tres sobre $\mathbb{F}_3$.
(3) Enuncia una condición suficiente para que un polinomio mónico irreducible de $\mathbb{F}_q[X]$ sea primitivo.

Ref.: 4163e_033 SOLUCIÓN

Ejercicio. 12.41.
Sea $f \in \mathbb{F}_p[X]$ irreducible de grado m. Demuestra que si α es una raíz, los elementos $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}$ son todos distintos y que son todas las raíces de f.
Ref.: 4163e_034 SOLUCIÓN

Ejercicio. 12.42.
Sea p un entero primo positivo y $q = p^n$. Demuestra que si $f(X) \in \mathbb{F}_q$ es un polinomio irreducible de grado r, para cada $m \in \mathbb{N}^*$ son equivalentes:
(a) $f(X)$ es un factor de $X^{q^m} - X$.
(b) $r|m$.

Deduce que

$$X^{q^m} - X = \prod\{f(X) \in \mathbb{F}_q[X] \mid f(X) \text{ es un polinomio mónico irreducible cuyo grado divide a } m\}.$$

Ref.: 4163e_082 SOLUCIÓN

Ejercicio. 12.43. (Criterio de Euler)
Demuestra que para todo $m \in \mathbb{Z}$, verificando $m \not\equiv 0 \pmod{p}$, son equivalentes:
(a) La congruencia $X^2 \equiv m \pmod{p}$ tiene solución.
(b) $m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Ref.: 4163e_084 SOLUCIÓN

Ejercicio. 12.44.
Suma de elementos de un cuerpo finito.
(1) Sea G un grupo y $\eta : G \longrightarrow F^\times$ un homomorfismo de grupos no trivial. Prueba que se verifica $\sum\{\eta(g) \mid g \in G\} = 0$.
(2) Sea $K = \mathbb{F}_q$, donde $q = p^n$, demuestra que para cada número entero positivo m se verifica que

$$S(m) = \sum\{\alpha^m \mid \alpha \in \mathbb{F}_q\} = \begin{cases} -1 & si\ (q-1)|m. \\ 0 & en\ otro\ caso. \end{cases}$$

Ref.: 4163e_085 SOLUCIÓN

Ejercicio. 12.45.
Sobre $\mathbb{F}_{11}$ halla raíces

(1) cuadradas primitivas de la unidad.
(2) quintas primitivas de la unidad.
(3) décimas primitivas de la unidad.

Ref.: 4163e_027 SOLUCIÓN

Ejercicio. 12.46.
Sea p un entero primo positivo

(1) Si p es un entero primo impar y $m > 0$, entonces el grupo multiplicativo de la unidades de $\mathbb{Z}_{p^m}$ es cíclico de orden $p^{m-1}(p-1)$.
(2) Comprueba que (1) es cierto si $p = 2$ y $m = 1$ ó 2.
(3) Si $m \geq 3$, entonces el grupo de las unidades $\mathbb{Z}_{2^m}$ es isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{m-2}}$.

Ref.: 4163e_088 SOLUCIÓN

Ejercicio. 12.47.
Sea $F = \mathbb{F}_q$ un cuerpo finito y $E = \overline{\mathbb{F}_q}$ su clausura algebraica. Prueba que para todo automorfismo $\sigma : E/F \longrightarrow E/F$ de orden finito se tiene $\sigma = id_E$.

Ref.: 4163e_103 SOLUCIÓN

Ejercicio. 12.48.
Sea $F/\mathbb{F}_{1024}$ una extensión de grado 2.

(1) Prueba que existe un único automorfismo $\sigma \in \mathrm{Gal}(F/\mathbb{F}_{1024})$ cuyo cuerpo fijo es $\mathbb{F}_{1024}$.
(2) Prueba que σ tiene orden 2.
(3) Determina cuántos elementos de F verifican la relación $\sigma(x) = x^{-1}$.

Ref.: 4163e_117 SOLUCIÓN

Ejercicio. 12.49. (Pequeño teorema de Fermat)
Para cada entero primo positivo p y cada potencia positiva $q = p^e$, prueba que $x^{q-1} = 1$ para todo $x \in \mathbb{F}_q$, o equivalentemente $x^q \equiv x \pmod{q}$ para cada entero $x \in \mathbb{Z}$.
Ref.: 4163e_102 SOLUCIÓN

Ejercicio. 12.50.
Se considera el cuerpo finito $\mathbb{F}_q$ y $f \in \mathbb{F}_q[X]$ un polinomio no constante de grado d. Prueba que son equivalentes:
(1) f es irreducible.
(2) f y $X^{p^t} - X$ son primos relativos para cada $t < d$.

Prueba que la condición (b) no puede sustituirse por $f \nmid X^{q^t} - X$ para cada $t < d$.
Ref.: 4163e_104 SOLUCIÓN

Ejercicio. 12.51.
Se considera el cuerpo finito $\mathbb{F}_q$ y $f \in \mathbb{F}_q[X]$ un polinomio libre de cuadrados. Prueba que existe $n \in \mathbb{N}$ tal que $f \mid X^{q^n} - X$.
Ref.: 4163e_105 SOLUCIÓN

Ejercicio. 12.52.
Se considera el cuerpo $\mathbb{F}_{2^n}$, siendo $0 \neq n \in \mathbb{N}$; sabemos que $\mathbb{F}_{2^n}^\times \cong \mathbb{Z}_{2^n-1}$,y que por tanto el número de generadores es $\varphi(2^n - 1)$. Por otro lado, $\mathrm{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2) = \langle \phi \rangle$ es el grupo cíclico generado por el automorfismo de Frobenius.
(1) Dado $\alpha \in \mathbb{F}_{2^n}$, prueba que $\mathrm{grad}(\mathrm{Irr}(\alpha, \mathbb{F}_2))$ divide a n.
(2) Dado $\alpha \in \mathbb{F}_{2^n}^\times$, prueba que existe $0 \neq e \in \mathbb{N}$ tal que $\alpha^{2^e} = \alpha$, y que si e es el menor de los que verifican esta condición, entonces $\mathrm{Irr}(\alpha, \mathbb{F}_2) = \prod_{i=0}^{e-1}(X - \alpha^{2^i})$, por lo que $e = \mathrm{grad}(\mathrm{Irr}(\alpha, \mathbb{F}_2))$.
(3) Recíprocamente, si $\mathrm{Irr}(\alpha, \mathbb{F}_2)$ tiene grado $m \geq 1$, entonces m es el menor entero positivo que verifica $\alpha^{2^m} = \alpha$.

Ref.: 4163e_106 SOLUCIÓN

Ejercicio. 12.53.
Cuerpos con nueve elementos.

(1) *Construye todos los cuerpos de nueve elementos que se obtienen a partir de los polinomios mónicos irreducibles de grado dos sobre* $\mathbb{F}_3[x]$. *Llama a estos polinomios* f_i, *para* $i = 1, 2, \ldots$
(2) *Construye isomorfismos entre los cuerpos de nueve elementos* $\frac{\mathbb{F}_3[X]}{(f_i)}$.

Ref.: 4163e_107 SOLUCIÓN

El siguiente ejercicio nos asegura la existencia de polinomios irreducibles sobre cuerpos finitos. Además nos permite determinar el grado del polinomio irreducible de una raíz n–ésima primitiva de la unidad sobre $\mathbb{F}_2$.

Ejercicio. 12.54.
Sea t *el orden de 2 módulo* n.

(1) *Prueba que cada raíz* n*–ésima de la unidad sobre* $\mathbb{F}_2$ *pertenece a* $\mathbb{F}_{2^t}$.
(2) *Prueba que cada raíz* n*–ésima primitiva de la unidad sobre* $\mathbb{F}_2$ *genera la extensión* $\mathbb{F}_{2^t}/\mathbb{F}_2$.
(3) *Prueba que si* ξ *es una raíz* n*–ésima primitiva de la unidad sobre* $\mathbb{F}_2$ *entonces* $\mathrm{Irr}(\xi, \mathbb{F}_2)$ *tiene grado* t.
(4) *¿Es este resultado válido para un primo* $p \neq 2$*?*

Ref.: 4163e_118 SOLUCIÓN

Ejercicio. 12.55.
Determina un polinomio irreducible el de grado 15 sobre $\mathbb{F}_2$.

Ref.: 4163e_119 SOLUCIÓN

Ejercicio. 12.56.
Sea F *un cuerpo finito y* $0 \neq \alpha \in F$. *Prueba que existen elementos* $a, b \in F$ *tales que* $1 + a^2 - \alpha b^2 = 0$

Ref.: 4163e_111 SOLUCIÓN

Ejercicio. 12.57.
Sea p un entero primo positivo impar. Determina el grado del cuerpo de descomposición sobre $\mathbb{F}_p$ del polinomio $(X^2-1)(X^2-2)\cdots(X^2-(p-1))$.
Ref.: 4163e_114 *SOLUCIÓN*

Ejercicio. 12.58.
Sea p un entero primo positivo, $p>3$. Vamos a estudiar los posibles valores del grado del cuerpo de descomposición, sobre $\mathbb{F}_p$, del polinomio $(X^3-1)(X^3-2)\cdots(X^3-(p-1))$.

(1) Estudia la aplicación $\nu:\mathbb{F}_p^\times\longrightarrow\mathbb{F}_p^\times$ definida $\nu(x)=x^3$, y caracteriza cuando es sobreyectiva, y cuando no lo es, en términos de raíces cúbicas de la unidad.
(2) Determina los posibles valores del grado sobre $\mathbb{F}_p$ del cuerpo de descomposición.
(3) Determina para que valores de p el cuerpo de descomposición sobre $\mathbb{F}_p$ tiene grado 2.
(4) Determina para que valores de p el cuerpo de descomposición sobre $\mathbb{F}_p$ tiene grado 3.

Ref.: 4163e_115 *SOLUCIÓN*

Ejercicio. 12.59.
Si $f\in\mathbb{F}_{p^k}$ es irreducible de grado d, son equivalentes:

(a) f es irreducible en $\mathbb{F}_{p^{km}}$.
(b) $mcd\{d,m\}=1$.

Ref.: 4163e_116 *SOLUCIÓN*

13. Extensiones ciclotómicas. Raíces de la unidad

Supongamos que K es un cuerpo y $\overline{K}$ una clausura algebraica; las raíces, en $\overline{K}$, del polinomio X^n-1 se llaman **raíces n–ésimas de la unidad** sobre K. Tenemos que las raíces de la unidad son todas distintas si, y sólo si, $f(X)=X^n-1$ es primo con su derivada, y ya que ésta es $Df(X)=nX^{n-1}$, resulta que esto ocurre si, y sólo si, la característica de K no divide a n; en particular, si la característica de K es cero.

Cuando $\mathrm{car}(K)=p\neq 0$, si $n=mp^r$, con $p\nmid m$, entonces $X^n-1=(X^m-1)^{p^r}$, y en este caso existen únicamente m raíces n–ésimas distintas de la unidad, todas de multiplicidad p^r. *Así pues, en lo que sigue, vamos a suponer que la característica de K es cero o no divide a n y que, por lo tanto, existen n raíces n–ésimas distintas de la unidad.*

Proposición. 13.1.
Para cada cuerpo K las raíces n-ésimas de la unidad forman un subgrupo cíclico de orden n del grupo multiplicativo de $\overline{K}$.

DEMOSTRACIÓN. Primero veamos que las raíces n–ésimas de la unidad forman un subgrupo. Para esto, sean ξ y ζ dos raíces n–ésimas de la unidad, se verifica:

$$(\xi\zeta)^n=\xi^n\zeta^n=1.$$

Vamos ahora a ver que este grupo es cíclico; tomamos m el menor entero positivo tal que $\xi^m=1$, para cada raíz n-ésima de la unidad, entonces $m\leq n$ y $m\,|\,n$; el polinomio X^m-1 tiene m raíces, en $\overline{K}$. Como las raíces n–ésimas de la unidad son también raíces de este polinomio, tenemos $n\leq m$. Como consecuencia $n=m$. □

Utilizando este hecho, definimos una **raíz n–ésima primitiva de la unidad** como una raíz n–ésima de la unidad que genera el grupo de las raíces n–ésimas de la unidad, esto es; su orden es precisamente n.

Cada raíz de la unidad es una raíz primitiva de la unidad para algún entero, más explícitamente:

Lema. 13.2.
Sea ξ una raíz n–ésima primitiva de la unidad sobre un cuerpo K, para cada divisor entero positivo d de n, $\xi^{n/d}$ es una raíz d-ésima primitiva de la unidad sobre K.

4163-02.tex

DEMOSTRACIÓN. Tenemos que $\xi^{n/d}$ es una raíz d-ésima de la unidad ya que $(\xi^{n/d})^d = 1$, además $\xi^{n/d}$ tiene orden d, luego es una raíz d-ésima primitiva de la unidad. □

Recordemos la definición de φ, la **función tociente de Euler**. Para cada número entero n, tenemos que $\varphi(n)$ es igual al número de enteros positivos menores ó iguales que n y primos relativos con n.

- Si consideramos el grupo cíclico $\mathbb{Z}_n$, entonces $\varphi(n)$ es el número de generadores de $\mathbb{Z}_n$.
- Si n y m son números enteros positivos primos relativos, entonces $\varphi(nm) = \varphi(n)\varphi(m)$. La demostración de este hecho se basa, por ejemplo, en contar el número de generadores del grupo cíclico $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$. Un generador es un par (a, b), donde a es un generador de $\mathbb{Z}_n$ y b es un generador de Z_m.
- Para cada número entero positivo primo p se tiene $\varphi(p^e) = (p-1)p^{e-1}$.
- Ya que cada número entero positivo n, que se puede expresar en la forma $n = p_1^{e_1} \cdots p_r^{e_r}$ con $p_1, \ldots, p_r$ enteros positivos primos y distintos dos a dos, tenemos

$$\varphi(n) = \varphi(p_1^{e_1} \cdots p_r^{e_r}) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}) = \prod_i (p_i - 1)p_i^{e_i - 1}.$$

- Se tiene $n = \sum\{\varphi(d) \mid \ d \mid n\}$. Vamos a hacer la demostración. Para cada entero positivo n definimos $\Phi(n) = \sum\{\varphi(d) \mid \ d|n\}$. Si n y m son primos relativos, entonces $\Phi(n)\Phi(m) = \Phi(nm)$. La demostración se hace teniendo en cuenta que cada divisor de nm es de la forma $d_1 d_2$, con $d_1|n$ y $d_2|m$. También podemos probar que $\Phi(p^e) = p^e$, y como consecuencia $\Phi(n) = n$. Ya que se tiene:

$$\Phi(p^e) = \sum_{f \le e} \varphi(p^f) = \sum_{f \le e} (p-1)p^{f-1} = 1 + (p-1)(1 + \cdots + p^{e-1}) = p^e.$$

Llamamos una **extensión ciclotómica** de K a un cuerpo de descomposición, sobre K, de un polinomio del tipo $X^n - 1$. Ya que cada raíz n-ésima primitiva de la unidad genera a las restantes, tenemos que cada extensión ciclotómica es una extensión simple generada por una raíz primitiva.

Teorema. 13.3.
Sea n un entero positivo, K un cuerpo y F/K una extensión ciclotómica, cuerpo de descomposición del polinomio $X^n - 1$. Se verifica:

(1) F/K es una extensión de Galois.
(2) $\mathrm{Gal}(F/K)$ es isomorfo a un subgrupo del grupo multiplicativo de las unidades de $\mathbb{Z}_n$, por lo tanto su orden es un divisor de $\varphi(n)$.

DEMOSTRACIÓN. (1). Tenemos que F/K es una extensión normal, ya que F es el cuerpo de descomposición del polinomio $X^n - 1$ sobre K, y por hipótesis, como vimos al inicio de esta sección, $\mathrm{car}(K) = 0$ ó no divide a n; resulta que $X^n - 1$ es un polinomio con todas sus raíces simples, luego la extensión es separable. Entonces F/K es una extensión de Galois.

(2). Supongamos $\sigma \in \mathrm{Gal}(F/K)$; ya que $F = K(\xi)$, para ξ una raíz n–ésima primitiva de la unidad, tenemos que σ está determinado por $\sigma(\xi)$. Supongamos que

$$\sigma(\xi) = \xi^i, \qquad 1 \leq i < n,$$

y que

$$\sigma^{-1}(\xi) = \xi^j, \qquad 1 \leq j < n,$$

tenemos

$$\xi = \sigma^{-1}\sigma(\xi) = \sigma^{-1}(\xi^i) = \sigma^{-1}(\xi)^i = \xi^{ji},$$

y por tanto $ji \equiv 1 \pmod{n}$. Entonces i es invertible módulo n, y existe una aplicación de $\mathrm{Gal}(F/K)$ en el grupo $\mathbb{Z}_n^\times$ de las unidades de $\mathbb{Z}_n$, definida:

$$\eta : \mathrm{Gal}(F/K) \longrightarrow \mathbb{Z}_n^\times, \quad \eta(\sigma) = i, \text{ tal que } \sigma(\xi) = \xi^i.$$

η es un homomorfismo de grupos, ya que si $\tau \in \mathrm{Gal}(F/K)$ está definida por $\tau(\xi) = \xi^k$, entonces

$$\tau\sigma(\xi) = \tau(\xi^i) = \tau(\xi)^i = \xi^{ki} = \xi^{ik},$$

luego $\eta(\sigma\tau) = ik = \eta(\sigma)\eta(\tau)$.
Tenemos que η es una aplicación inyectiva. Si $\sigma \in \mathrm{Ker}(\eta)$ se tiene $\sigma(\xi) = \xi^i = \xi$, luego $\sigma = \mathrm{id}_F$. Como consecuencia, $\mathrm{Gal}(F/K)$ es isomorfo a $\mathrm{Im}(\eta) \subseteq \mathbb{Z}_n^\times$. Ya que el orden de $\mathbb{Z}_n^\times$ es $\varphi(n)$, resulta que $|\mathrm{Gal}(F/K)|$ divide a $\varphi(n)$. □

Para cada número entero positivo n y cada cuerpo K, si F/K es el cuerpo de descomposición de $X^n - 1$, se define el ***n*–ésimo polinomio ciclotómico** sobre K como el polinomio

$$\Phi_n(X) = (X - \xi_1)\cdots(X - \xi_r),$$

donde $\xi_1, \ldots, \xi_r$ son las raíces n-ésimas primitivas de la unidad en F.

Proposición. 13.4.
En la situación anterior se tiene:
(1) $X^n - 1 = \prod\{\Phi_d(X) \mid d|n\}$.
(2) Los coeficientes de $\Phi_n(X)$ *pertenecen al cuerpo característico de* K. *Además, si* $\mathrm{car}(K) = 0$, *entonces los coeficientes de* $\Phi_n(X)$ *pertenecen a* $\mathbb{Z}$.
(3) El grado de $\Phi_n(X)$ *es* $\varphi(n)$.

DEMOSTRACIÓN. (1). Sea $\xi \in F$ una raíz n–ésima primitiva de la unidad; el grupo de las raíces n–ésimas de la unidad contiene al grupo de las raíces d-ésimas de la unidad para cada divisor d de n; además una raíz n-ésima de la unidad ξ es una raíz d-ésima primitiva de la unidad si, y sólo si, el orden de ξ es d, y entonces

$$\Phi_d(X) = \prod\{X - \xi \mid \xi \text{ es una raíz } n\text{–ésima de la unidad y } \mathrm{ord}(\xi) = d\}.$$

Entonces

$$\begin{aligned} X^n-1 &= \prod\{(X-\xi) \mid \xi \text{ es una raíz } n\text{-ésima de la unidad}\} \\ &= \prod\left\{\prod\{(X-\xi) \mid \xi \text{ es una raíz } n\text{–ésima de la unidad y } \operatorname{ord}(\xi)=d\} \mid d|n\right\} \\ &= \prod\{\Phi_d(X) \mid d|n\}. \end{aligned}$$

(2). Hacemos inducción sobre n. Para $n=1$ tenemos $\Phi_1(X)=X-1$ es un polinomio sobre el cuerpo característico. Supongamos ahora que el resultado es cierto para cada $k<n$, llamamos

$$f(X)=\prod\{\Phi_d(X) \mid d|n,\ d\neq n\}.$$

Cada $\Phi_d(X)$ es un polinomio sobre el cuerpo característico de K, y por tanto también lo es $f(X)$. Tenemos, por (1), que $X^n-1=f(X)\Phi_n(X)$, y $\Phi_n(X)$ es un polinomio sobre el cuerpo característico de K. Para probar esto hacemos la división con resto en el cuerpo característico, tenemos $X^n-1=f(X)c(X)+r(X)$, si hacemos la división con resto en $F[X]$, tenemos $X^n-1=f(X)\Phi_n(X)$, luego $r(X)=0$, y por tanto en el cuerpo característico se tiene $X^n-1=f(X)c(X)$, luego $\Phi_n(X)=c(X)$ y pertenece al cuerpo característico. Si $\operatorname{car}(K)=0$, y tomamos el cuerpo característico igual a $\mathbb{Q}$, entonces haciendo el mismo razonamiento, ahora para $\mathbb{Z}$, tenemos que $\Phi_n(X)$ pertenece a $\mathbb{Z}[X]$.
(3). Ya que $\Phi_n(X)=(X-\xi_1)\cdots(X-\xi_r)$, siendo $\xi_1,\ldots,\xi_r$ las raíces primitivas n–ésimas de la unidad en F, fijada una de ellas, por ejemplo ξ_1, las demás se pueden escribir en la forma ξ_1^i, para $1\leq i<n$, con i primo relativo con n, luego existen $\varphi(n)$, y el grado de $\Phi_n(X)$ es $\varphi(n)$. □

Con estos resultados obtenemos un método para construir los polinomios ciclotómicos de forma fácil. De la expresión $X^n-1=\prod\{\Phi_d(X) \mid d|n\}$ obtenemos

$$\Phi_n(X)=\frac{X^n-1}{\prod\{\Phi_d(X) \mid d|n,\ d\neq n\}}.$$

Definimos la **función de Moebius** sobre enteros positivos de la siguiente forma:

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

Se verifica:

$$\varphi(n)=\sum\{d\ \mu(n/d) \mid d|n\}.$$

La demostración se puede hacer aplicando que $\varphi(nm)=\varphi(n)\varphi(m)$ si n y m son primos relativos y probando el resultado para $n=p^e$, siendo p un entero positivo primo.
Aplicando la función de Moebius al cálculo de polinomios ciclotómicos, obtenemos la siguiente expresión:

$$\Phi_n(X)=\prod\{(X^d-1)^{\mu(n/d)} \mid d|n\}.$$

Podemos estudiar más propiedades de los polinomios ciclotómicos. Por ejemplo al estudiarlos sobre $\mathbb{Q}$ resulta:

Teorema. 13.5.
Para cada entero positivo n el polinomio $\Phi_n(X)$ es irreducible sobre $\mathbb{Q}$.

DEMOSTRACIÓN. Sea ξ una raíz n–ésima primitiva de la unidad y $f(X) = \mathrm{Irr}(\xi, K)$; vamos a relacionarlo con $\Phi_n(X)$.
Tenemos $f(X)|\Phi_n(X)$ y $f(X)|X^n-1$, entonces $X^n-1 = f(X)g(X)$, en $\mathbb{Q}[X]$. Ya que $f(X)$ es mónico, también $g(X)$ lo es; aplicando el Lema de Gauss tenemos que $f(X)$ y $g(X)$ tienen coeficientes en $\mathbb{Z}$.
Para cada entero primo positivo p que no divide a n tenemos que $f(\xi^p) = 0$, ya que si $f(\xi^p) \neq 0$, entonces $g(\xi^p) = 0$, y por tanto $f(X) \mid g(X^p)$, entonces $g(X^p) = f(X)r(X)$, por un razonamiento análogo al anterior tenemos que $r(X)$ tiene coeficientes en $\mathbb{Z}$. Si reducimos módulo p, aplicando que para cada $\alpha \in \mathbb{Z}_p$ se verifica $\alpha^p = \alpha$, tenemos $\overline{f}(X)\overline{r}(X) = \overline{g(X^p)} = \overline{g}(X)^p$, y por tanto $\overline{f}(X)$ y $\overline{g}(X)$ no son primos relativos en $\mathbb{Z}_p[X]$. Entonces existen raíces comunes de $\overline{f}(X)$ y de $\overline{g}(X)$, esto es, $\overline{X^n-1}$ tiene raíces múltiples, pero al derivar tenemos $\overline{n}X^{n-1}$, que no es cero y no tiene factores comunes con $\overline{X^n-1}$, por lo cual, llegamos a una contradicción. Como consecuencia ξ^p es raíz de $f(X)$.
Vamos a comprobar que toda raíz n–ésima primitiva de la unidad se puede escribir en la forma ξ^p, para algún entero primo positivo que no divide a n. Consideramos los primeros enteros positivos primos $p_1, \ldots, p_{\varphi(n)-1}$ que no dividen a n y verifican $p_i \not\equiv p_j \pmod{n}$, si $i \neq j$. Entonces $\xi, \xi^{p_1}, \ldots, \xi^{p_{\varphi(n)-1}}$ son raíces n–ésimas primitivas distintas de la unidad; por lo anterior, $f(X)$ tiene $\varphi(n)$ raíces como mínimo, por lo tanto $\mathrm{gr}(f(X)) \geq \varphi(n) = \mathrm{gr}(\Phi_n(X))$, entonces $\Phi_n(X) = f(X)$, y $\Phi_n(X)$ es irreducible. □

Este resultado no es necesariamente cierto si el cuerpo tiene característica $p \neq 0$, esto es, puede que $\Phi_n(X)$ no sea un polinomio irreducible.

Ejemplo. 13.6.
Tomamos $p = 11$, $n = 12$, el polinomio ciclotómico Φ_{12} es reducible:

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

Tomamos $p = 13$, $n = 12$, el polinomio ciclotómico Φ_{12} es reducible:

$$\Phi_{12}(X) = X^4 - X^2 + 1 = (X - 2)(x + 2)(x - 6)(X + 6).$$

13.1. Ejercicios

Extensiones ciclotómicas

Ejercicio. 13.7.
Calcular los polinomios ciclotómicos $\phi_n(X)$ sobre $\mathbb{Q}$, para $n = 3, 8, 10, 12, 14, 16, 18, 20, 24, 34, 50$.
Ref.: 4163e_035 SOLUCIÓN

Ejercicio. 13.8.
Determinar los polinomios ciclotómicos siguientes:
(1) $\phi_3(X)$ sobre $\mathbb{F}_2$.
(2) $\phi_8(X)$ sobre $\mathbb{F}_3$.

Ref.: 4163e_046 SOLUCIÓN

Ejercicio. 13.9.
Sea $n > 2$ y sea ζ una raíz n-ésima primitiva de la unidad sobre $\mathbb{Q}$. Demuestra que
(1) $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(n)/2$, donde $\varphi(n)$ es el valor de la función de Euler en n,
(2) $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\zeta) \cap \mathbb{R}$.

Ref.: 4163e_036 SOLUCIÓN

Ejercicio. 13.10.
*Sea φ la **función tociente de Euler**.*
(1) Demuestra que $\varphi(n)$ es par para todo $n \geq 2$.
(2) Determina todos los $n \geq 0$ tales que $\varphi(n) = 2$.
(3) Determina todos los pares de enteros positivos n y p tales que p es primo y $\varphi(n) = n/p$.

Ref.: 4163e_037 SOLUCIÓN

Ejercicio. 13.11.
Determinar los enteros n para los que una raíz n-ésima primitiva de la unidad tiene grado 2 sobre $\mathbb{Q}$.
Ref.: 4163e_038 SOLUCIÓN

Ejercicio. 13.12.
Sea K un cuerpo de característica cero y $n > 1$ un número impar. Demostrar que si K contiene una raíz n-ésima primitiva de la unidad, también contiene una raíz $2n$-ésima primitiva de la unidad.
Ref.: 4163e_039 SOLUCIÓN

Ejercicio. 13.13.
Demostrar que el cuerpo $\mathbb{F}_{13}$ contiene todas las raíces decimosegundas de la unidad. Calcular $\phi_{12}(X)$ y factorizarlo en irreducibles en $\mathbb{F}_{13}$. (Obsérvese que no es irreducible).
Ref.: 4163e_043 SOLUCIÓN

Ejercicio. 13.14.
Determina el grupo de Galois de las extensión de $\mathbb{F}_p$ por las raíces n–ésimas de la unidad en los siguientes casos (ver el ejercicio (15.17.)):
(1) $p = 7, \quad n = 5.$
(2) $p = 11, \quad n = 12.$
(3) $p = 13, \quad n = 12.$
(4) $p = 7, \quad n = 28.$
(5) $p = 5^2, \quad n = 6.$

Ref.: 4163e_072 SOLUCIÓN

Ejercicio. 13.15.
Sea $\mathbb{F}_q$ el cuerpo con $q = p^n$, p primo, y sea m un entero positivo primo relativo con q; llamamos E al cuerpo de descomposición de $X^m - 1$ sobre $\mathbb{F}_q$, demuestra que $[E : \mathbb{F}_q] = r$ es el menor entero positivo que verifica $m|q^r - 1$.
Ref.: 4163e_078 SOLUCIÓN

Ejercicio. 13.16.
Calcular $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, los retículos de subgrupos y de subcuerpos intermedios, para ζ una raíz 7^a, 12^a, 17^a, 18^a, 20^a y 24^aprimitiva de la unidad.
Ref.: 4163e_044 SOLUCIÓN

Ejercicio. 13.17.
Sea $E = \mathbb{Q}(\zeta)$ con $\zeta = e^{\frac{2\pi}{5}} = \cos(\frac{2\pi}{5}) + i\mathrm{sen}(\frac{2\pi}{5})$, una raíz quinta primitiva de la unidad.

(1) Demuestra que $E/\mathbb{Q}$ es de grado 4 con grupo de Galois cíclico generado por el automorfismo que lleva ζ en ζ^2.
(2) Demuestra que E tiene un único subcuerpo K con $\mathbb{Q} \subseteq K \subseteq E$ y $[K : \mathbb{Q}] = 2$. Verifica que $\alpha = \zeta + \zeta^4$ y $\beta = \zeta^2 + \zeta^3$ forman una $\mathbb{Q}$-base de K.
(3) Determina los polinomios $\mathrm{Irr}(\alpha, \mathbb{Q})$ e $\mathrm{Irr}(\beta, \mathbb{Q})$.

Ref.: 4163e_045 SOLUCIÓN

Ejercicio. 13.18.
Sean ζ_n y ζ_m raíces n-ésima y m-ésima primitivas de la unidad respectivamente. Demostrar

(1) $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_k)$, con $k = mcm\{n, m\}$ y ζ_k una raíz k-ésima primitiva de la unidad.
(2) Si $mcd\{n, m\} = 1$, entonces $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$
(3) Si $n|m$, entonces $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$
(4) Si n es impar, entonces $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$.

Ref.: 4163e_047 SOLUCIÓN

Ejercicio. 13.19.
Sea ζ una raíz décimo tercera primitiva de la unidad. Calcular un elemento primitivo para cada una de las extensiones intermedias de $\mathbb{Q}(\zeta)/\mathbb{Q}$
Ref.: 4163e_048 SOLUCIÓN

Ejercicio. 13.20.
Sea ζ una raíz del polinomio $X^2-5X+1 \in \mathbb{F}_{11}[X]$ en alguna clausura algebraica.
(1) Demuestra que ζ es una raíz primitiva decimosegunda de la unidad sobre $\mathbb{F}_{11}$.
(2) Descompón en factores primos el polinomio ciclotómico $\phi_{12}(X)$ sobre $\mathbb{F}_{11}$.

Ref.: 4163e_049 SOLUCIÓN

Ejercicio. 13.21.
Sea K el cuerpo de descomposición de todos los polinomios de grado 4 en $\mathbb{Q}[X]$. ¿Para qué valores de $n \in \mathbb{N}$ la n–ésima raíz primitiva de la unidad ζ_n pertenece a K?
Ref.: 4163e_069 SOLUCIÓN

Ejercicio. 13.22.
Sea $K/\mathbb{Q}$ una extensión finita, demuestra que existe un número finito de raíces de la unidad contenidas en K.
Ref.: 4163e_086 SOLUCIÓN

Ejercicio. 13.23.
Determina qué raíces de la unidad pertenecen a las siguientes extensiones de $\mathbb{Q}$.
(1) $\mathbb{Q}(i)/\mathbb{Q}$.

(2) $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$.
(3) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.
(4) $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$.
(5) $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.
(6) $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$.

Ref.: 4163e_087 SOLUCIÓN

Ejercicio. 13.24.
Sea $\mathbb{Q}$ el cuerpo de de los números racionales.

(1) *Determina el polinomio ciclotómico $\phi_{27}(X)$ sobre $\mathbb{Q}$.*
(2) *Determina el grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_{27})/\mathbb{Q}$, donde ζ_{27} es una raíz 27–ésima primitiva de la unidad.*
(3) *Determina el retículo de subcuerpos intermedios.*

Ref.: 4163e_040 SOLUCIÓN

Ejercicio. 13.25.
Sea p un entero positivo primo, y ζ_p una raíz p–ésima primitiva de la unidad. Se considera $E = \mathbb{Q}(\zeta_p)$ y el grupo de Galois $G = \mathrm{Gal}(E/\mathbb{Q})$. Prueba que se tiene:

$$\sum\{\sigma(\xi) \mid \sigma \in G\} = \begin{cases} p-1 & \text{si } \xi \text{ no es una raíz } p\text{–ésima primitiva de la unidad,} \\ -1 & \text{si } \xi \text{ es una raíz } p\text{–ésima primitiva de la unidad.} \end{cases}$$

Ref.: 4163e_041 SOLUCIÓN

Ejercicio. 13.26.
Comprueba las siguientes propiedades de los polinomios ciclotómicos:

(1) *Si p es un entero primo y k es un entero positivo, entonces*

$$\phi_{p^k}(X) = \phi_p(X^{p^{k-1}}).$$

(2) *Si* $n = p_1^{e_1} \dots p_k^{e_k}$, *con los* p_i *enteros positivos primos distintos, y* $e_i > 0$, *entonces*

$$\phi_n(X) = \phi_{p_1 \dots p_k}(X^{p_1^{e_1-1} \cdots p_k^{e_k-1}}).$$

(3) *Si* n *es impar, entonces* $\phi_{2n}(X) = \phi_n(-X)$.
(4) *Si* p *es primo y no divide a* n, *entonces*

$$\phi_{pn}(X) = \frac{\phi_n(X^p)}{\phi_n(X)}.$$

(5) $\phi_n(1) = \begin{cases} p & \text{si } n = p^k, k > 0, \\ 1 & \text{en otro caso.} \end{cases}$

Ref.: 4163e_089 SOLUCIÓN

Ejercicio. 13.27.
Para $n \geq 2$ *prueba que se verifica la relación siguiente para polinomios ciclotómicos:*

$$\phi_n(X) = X^{\varphi(n)} \phi_n(X^{-1}).$$

esto es, $\phi_n(X)$ *es un polinomio recíproco.*
Ref.: 4163e_042 SOLUCIÓN

Ejercicio. 13.28.
Función totiente de Euler.

(1) *Prueba que si* $p = 2^k + 1$, *con* $k \in \mathbb{N}$, *es un entero primo positivo, entonces* k *es una potencia de dos. Estos números primos se llaman* ***primos de Fermat****.*
(2) *Prueba que* $\varphi(n)$ *es una potencia de 2 si, y sólo si,* $n = 2^s p_1 \dots p_t$, *con* $s \in \mathbb{N}$, *y los* p_i *primos de Fermat, distintos dos a dos.*

Ref.: 4163e_096 SOLUCIÓN

Ejercicio. 13.29.
Estudia si $\sqrt{7} \in \mathbb{Q}(\xi_{49})$.
Ref.: 4163e_108 *SOLUCIÓN*

Ejercicio. 13.30.
Se considera $\xi = \xi_{14}$, *una raíz primitiva décimo cuarta de la unidad, sobre* $\mathbb{Q}$.

(1) *Calcula el polinomio ciclotómico* $\phi_{14}(X)$, *y describe los elementos de* $\mathbb{Q}(\xi)/\mathbb{Q}$. *En particular queremos conocer el grado de esta extensión.*
(2) *Calcula el grupo* $G = \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, *y el retículo de subgrupos.*
(3) *Da un generador* σ *del grupo* G; *sólo tienes que dar la imagen de* ξ.
(4) *Observa que la extensión* $\mathbb{Q}(\xi)/\mathbb{Q}(\xi) \cap \mathbb{R}$ *es de grado 2, y que por tanto corresponde a un subgrupo* N *de* G *de orden 2 e índice 3, generado por* σ^3.
(5) *Comprueba que* $\mathbb{Q}(\xi) \cap \mathbb{R} = \mathbb{Q}(\xi + \xi^{-1})$. *Estamos interesados en calcular* $\mathrm{Irr}(\xi + \xi^{-1}, \mathbb{Q})$; *da un método para calcularlo. Entre otras formas puedes calcularlo: (1) resolviendo un sistema de ecuaciones lineales haciendo uso de las potencias, (2) directamente utilizando los conjugados, ó (3) haciendo uso de la resultante.*
(6) *A partir del subgrupo* H, *de orden 3, de* G, *determina el cuerpo intermedio* $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\xi)$ *tal que* $[\mathbb{Q}(\xi) : F] = 2$, *y da un generador* θ *de la extensión* $F/\mathbb{Q}$. *Calcula el polinomio irreducible* $\mathrm{Irr}(\theta, \mathbb{Q})$.

Ref.: 4163e_112 *SOLUCIÓN*

Ejercicio. 13.31.
Se considera $\xi = \xi_{15}$, *una raíz primitiva décimo quinta de la unidad, sobre* $\mathbb{Q}$.

(1) *Calcula el polinomio ciclotómico* $\phi_{15}(X)$, *y describe los elementos de* $\mathbb{Q}(\xi)/\mathbb{Q}$. *En particular queremos conocer el grado de esta extensión.*
(2) *Calcula el grupo* $G = \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, *y el retículo de subgrupos.*
(3) *Da un sistema de generadores* $\{\sigma\tau\}$ *del grupo* G; *sólo tienes que dar la imagen de* ξ. *(Tomaremos* σ *de orden 4 y* τ *de orden 2.)*
(4) *Observa que la extensión* $\mathbb{Q}(\xi)/\mathbb{Q}(\xi) \cap \mathbb{R}$ *es de grado 2, y que por tanto corresponde a un subgrupo* N *de* G *de orden 2 e índice 4, en este caso será* $\langle\tau\rangle$.
(5) *Comprueba que* $\mathbb{Q}(\xi) \cap \mathbb{R} = \mathbb{Q}(\xi + \xi^{-1})$, *y calcula* $\mathrm{Irr}(\xi + \xi^{-1}, \mathbb{Q})$.
(6) *Determina todos los cuerpos intermedios* $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\xi)$, *y da un generador para cada extensión* $F/\mathbb{Q}$.

(7) *Describe la correspondencia de Galois entre los retículos de subgrupos de G y de las extensiones intermedias.*

Ref.: 4163e_113 SOLUCIÓN

Ejercicio. 13.32.
Sea p un entero primo positivo y $\xi = \xi_p$ una raíz p–ésima primitiva de la unidad. Llamamos $E = \mathbb{Q}(\xi)$.

(1) *Prueba que existen extensiones intermedias $\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq E$ tales que $[E : F_2] = [F_1 : \mathbb{Q}] = 2$.*
(2) *Determina $\alpha_2 \in E$ tal que $F_2 = \mathbb{Q}(\alpha_2)$.*
(3) *Determina $\alpha_1 \in E$ tal que $F_1 = \mathbb{Q}(\alpha_1)$.*

Ref.: 4163e_120 SOLUCIÓN

Construcciones con regla y compás

Ejercicio. 13.33.
Enumerar los polígonos regulares de 100 *lados o menos que son contructibles con regla y compás.*
Ref.: 4163e_050 SOLUCIÓN

Ejercicio. 13.34.
Sea $\zeta = \zeta_{17}$ una raíz 17ª primitiva de la unidad sobre $\mathbb{Q}$. Determinar explícitamente la sucesión de raíces cuadradas que generan el cuerpo $\mathbb{Q}(\zeta + \zeta^{-1})$.
Ref.: 4163e_051 SOLUCIÓN

14. Norma y traza

En lo que sigue vamos a considerar extensiones finitas y separables.
Sea F/K una extensión finita y separable con $[F:K]=n$, llamamos $\overline{K}$ a una clausura algebraica de K que contiene a F. Ya que la extensión F/K es separable, existen exactamente n homomorfismos de F a $\overline{K}$ sobre K,

$$\mathrm{Hom}(F/K,\overline{K}/K)=\{\sigma_1,\dots,\sigma_n\}.$$

Para $\alpha\in F$ se define la **norma de α relativa a F/K**, y se representa por $N_{F/K}(\alpha)$, como

$$N_{F/K}(\alpha)=\prod\{\sigma_i(\alpha)\mid\ 1\le i\le n\},$$

y se define la **traza de α relativa a F/K**, y se representa por $T_{F/K}(\alpha)$, como

$$T_{F/K}(\alpha)=\sum\{\sigma_i(\alpha)\mid\ 1\le i\le n\}.$$

La norma y la traza son elementos de $\overline{K}$, y pertenecen a F cuando F/K es una extensión normal.

Proposición. 14.1.
Si F/K es una extensión de Galois (finita), entonces para cada $\alpha\in F$ tenemos $N_{F/K}(\alpha)$, $T_{F/K}(\alpha)\in F$.

DEMOSTRACIÓN. Ya que la extensión es de Galois, en particular es normal, y por tanto los homomorfismos de F en $\overline{K}$ sobre K tienen sus imágenes en F. Podemos suponer que $\{\sigma_1,\dots,\sigma_n\}=\mathrm{Aut}(F/K)=\mathrm{Gal}(F/K)$, entonces para cada i se tiene $\sigma_i(\alpha)\in F$, y tenemos el resultado. □

Recopilamos en el siguiente resultado las propiedades de norma y traza.

Proposición. 14.2.
Sea F/K una extensión finita y separable de grado n, $a\in K$ y $\alpha,\beta\in F$. Se verifica:

(1) $N_{F/K}(\alpha\beta)=N_{F/K}(\alpha)N_{F/K}(\beta)$.	*(1')* $T_{F/K}(\alpha+\beta)=T_{F/K}(\alpha)+T_{F/K}(\beta)$.
(2) $N_{F/K}(a)=a^n$.	*(2')* $T_{F/K}(a)=na$.
(3) $N_{F/K}(\alpha)\in K$.	*(3')* $T_{F/K}(\alpha)\in K$.
(4) $N_{F/K}(a\alpha)=a^nN_{F/K}(\alpha)$.	*(4')* $T_{F/K}(a\alpha)=naT_{F/K}(\alpha)$.

4163-03.tex

DEMOSTRACIÓN. (1). Tenemos

$$\begin{aligned} N_{F/K}(\alpha\beta) &= \prod\{\sigma_i(\alpha\beta) \mid 1 \le i \le n\} \\ &= \prod\{\sigma_i(\alpha)\sigma_i(\beta) \mid 1 \le i \le n\} \\ &= \prod\{\sigma_i(\alpha) \mid 1 \le i \le n\} \prod\{\sigma_i(\beta) \mid 1 \le i \le n\} \\ &= N_{F/K}(\alpha) N_{F/K}(\beta). \end{aligned}$$

(1'). Para $T_{F/K}$ se hace de forma similar.

(2). Tenemos

$$N_{F/K}(a) = \prod\{\sigma_i(a) \mid 1 \le i \le n\} = \prod\{a \mid 1 \le i \le n\} = a^n.$$

(2'). Para $T_{F/K}$ se hace de forma similar.

(3). Para la extensión finita y separable F/K vamos a suponer que $F = K(\alpha_1, \dots, \alpha_r)$. Si llamamos $f_i(X) = \mathrm{Irr}(\alpha_i, K)$ y $f(X) = f_1(X) \dots f_r(X)$, resulta que existe un cuerpo de descomposición E de $f(X)$ sobre K que contiene a F, está contenido en $\overline{K}$ y tal que la extensión E/K es de Galois.

Los homomorfismos $\sigma_i : F/K \longrightarrow \overline{K}/K$ se pueden extender a homomorfismos $\overline{\sigma_i} : E/K \longrightarrow \overline{K}/K$, y ya que E/K es una extensión normal tenemos además que $E^{\overline{\sigma_i}} = E$, y por tanto $\overline{\sigma_i} \in \mathrm{Gal}(E/K)$.

Si consideramos el subgrupo $H = \mathrm{Gal}(E/F)$ que corresponde al subcuerpo F, entonces $(G : H) = [F : K] = n$. Ya que para $i \neq j$ se tiene $\overline{\sigma_i}_{|F} \neq \overline{\sigma_j}_{|F}$, entonces $\overline{\sigma_i}H \neq \overline{\sigma_j}H$ y por tanto las clases a la izquierda de H en G son $\{\overline{\sigma_1}H, \dots, \overline{\sigma_n}H\}$. Para cada $\tau \in \mathrm{Gal}(E/K)$ y cada i, $1 \le i \le n$, existen un $\omega(i)$, $1 \le \omega(i) \le n$ y $\tau_i \in H$ tales que $\tau\,\overline{\sigma_i} = \overline{\sigma_{\omega(i)}}\tau_i$, entonces cuando restringimos a F se verifica la igualdad siguiente: $\tau\sigma_i = \sigma_{\omega(i)}$. Fijado τ, tenemos que ω define una permutación del conjunto $\{1, \dots, n\}$. Después de establecer estos hechos, para cada $\alpha \in F$ se verifica:

$$\begin{aligned} \tau(N_{F/K}(\alpha)) &= \tau(\prod\{\sigma_i(\alpha) \mid 1 \le i \le n\}) \\ &= \prod\{\tau\sigma_i(\alpha) \mid 1 \le i \le n\} \\ &= \prod\{\sigma_{\omega(i)}(\alpha) \mid 1 \le i \le n\} \\ &= N_{F/K}(\alpha). \end{aligned}$$

(3'). Para $T_{F/K}$ se hace de forma similar.

(4). $N_{F/K}(a\alpha) = \prod\{\sigma_i(a\alpha) \mid 1 \le i \le n\} = \prod\{a\sigma_i(\alpha) \mid 1 \le i \le n\} = a^n N_{F/K}(\alpha)$.

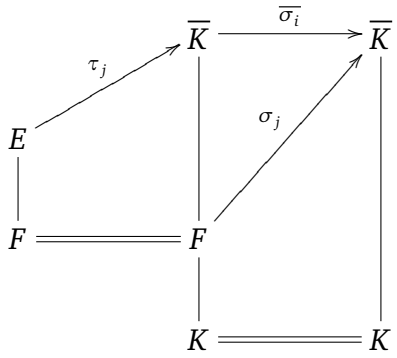
(4'). Para $T_{F/K}$ se hace de forma similar. □

Vamos a estudiar ahora la norma y la traza en torres de extensiones de cuerpos, obtendremos las llamadas fórmulas de transitividad.

Proposición. 14.3.
Sea $K \subseteq F \subseteq E$ una torre de cuerpos, y E/K una extensión finita y separable, entonces para cada $\alpha \in E$ se verifica:

(1) $N_{F/K}(N_{E/F}(\alpha)) = N_{E/K}(\alpha)$.
(2) $T_{F/K}(T_{E/F}(\alpha)) = T_{E/K}(\alpha)$.

DEMOSTRACIÓN. (1). Supongamos que $\overline{K}$ es una clausura algebraica de K que contiene a E, supongamos que $[E:F]=m$ y que $[F:K]=n$. Llamamos $\tau_1,\dots,\tau_m$ a los homomorfismos (distintos) de E en $\overline{K}$ sobre F y $\sigma_1,\dots,\sigma_n$ a los homomorfismos (distintos) de F en $\overline{K}$ sobre K.



Definimos

$$\varphi_{ij}: E \longrightarrow \overline{K}, \qquad \varphi_{ij}=\overline{\sigma_i}\,\tau_j, \text{ para } i,j \text{ verificando } 1\le i\le n, 1\le j\le m.$$

Estos son todos los homomorfismos (distintos) de E en $\overline{K}$ sobre K. Para cada $\alpha\in E$ se verifica:

$$\begin{aligned} N_{E/K}(\alpha) &= \prod\{\varphi_{ij}(\alpha) \mid 1\le i\le n, 1\le j\le m\} \\ &= \prod\{\sigma_i\tau_j(\alpha) \mid 1\le i\le n, 1\le j\le m\} \\ &= \prod\{\sigma_i(\prod\{\tau_j(\alpha) \mid 1\le j\le m\}) \mid 1\le i\le n\} \\ &= \prod\{\sigma_i(N_{E/F}(\alpha)) \mid 1\le i\le n\} \\ &= N_{F/K}(N_{E/F}(\alpha)). \end{aligned}$$

(2). Para la traza se hace de forma similar. □

Corolario. 14.4.
Sea $K\subseteq F\subseteq E$ una torre de cuerpos, y E/K una extensión finita y separable, entonces para cada $\alpha\in F$ se verifica:
(1) $N_{E/K}(\alpha)=(N_{F/K}(\alpha))^{[E:F]}$.
(2) $T_{E/K}(\alpha)=[E:F]T_{F/K}(\alpha)$.

DEMOSTRACIÓN. (1). Tenemos:

$$N_{E/K}(\alpha)=N_{F/K}(N_{E/F}(\alpha))=N_{F/K}(\alpha^{[E:F]})=(N_{F/K}(\alpha))^{[E:F]}.$$

(2). Para la traza se hace de forma similar. □

El cálculo de la norma y de la traza de un elemento algebraico puede hacerse de forma sencilla si conocemos su polinomio mónico irreducible como prueba el siguiente lema.

Proposición. 14.5.
Sea F/K una extensión finita y separable de grado n, para $\alpha \in F$, si

$$\mathrm{Irr}(\alpha, K) = X^r + a_{r-1}X^{r-1} + \ldots + a_1 X + a_0,$$

entonces tenemos:
(1) $N_{F/K}(\alpha) = (-1)^n (a_0)^{n/r}$.
(2) $T_{F/K}(\alpha) = -(n/r)a_{r-1}$.

DEMOSTRACIÓN. Ya que el grado de $\mathrm{Irr}(\alpha, K)$ es r, resulta que $[K(\alpha) : K] = r$, entonces $[F : K(\alpha)] = n/r$.
(1). Aplicando el Corolario (14.4.) a la torre de cuerpos $K \subseteq K(\alpha) \subseteq F$, tenemos:

$$\begin{aligned} N_{F/K}(\alpha) = (N_{K(\alpha)/K}(\alpha))^{[F:K(\alpha)]} &= N_{K(\alpha)/K}(\alpha))^{n/r} \\ = \left(\prod\{\alpha_i \mid 1 \le i \le r\}\right)^{n/r} = ((-1)^r a_0)^{n/r} &= (-1)^n a_0^{n/r}. \end{aligned}$$

(donde $\alpha_1, \ldots, \alpha_r$ son las raíces de $\mathrm{Irr}(\alpha, K)$ en $\overline{K}$).
(2). Para la traza se hace de forma similar. □

Otro resultado de interés, ahora sobre la traza, es el siguiente:

Proposición. 14.6.
Sea F/K una extensión finita y separable, entonces existe $\alpha \in F$ tal que $T_{F/K}(\alpha) \neq 0$.

DEMOSTRACIÓN. Si $\sigma_1, \ldots, \sigma_n$ son los homomorfismos distintos de F en $\overline{K}$ sobre K y no existe ningún $\alpha \in F$ tal que $T_{F/K}(\alpha) \neq 0$, entonces se verifica $\sum\{\sigma_i \mid 1 \le i \le n\} = 0$, lo que contradice el lema de independencia de Dedekind. □

Utilizando la traza podemos dar una caracterización fácil de bases para extensiones separables.

Lema. 14.7.
Sea F/K una extensión finita y separable de grado n. Para $\alpha_1, \ldots, \alpha_n \in F$ son equivalentes:
(a) $\{\alpha_1, \ldots, \alpha_n\}$ *es una base de F como espacio vectorial sobre K.*

(b) Los elementos siguientes elementos son linealmente independientes sobre F

$$\begin{aligned}\beta_1 &= (\sigma_1(\alpha_1),\dots,\sigma_1(\alpha_n))\\ &\vdots\\ \beta_n &= (\sigma_n(\alpha_1),\dots,\sigma_n(\alpha_n)).\end{aligned}$$

(c) El determinante de la matriz $(T_{F/K}(\alpha_i\alpha_j))_{ij}$ *es no nulo.*

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Siguiendo con las notaciones precedentes, consideramos el sistema de ecuaciones lineales

$$\sigma_1(\alpha_j)X_1+\cdots+\sigma_n(\alpha_j)X_n=0\Big\}_{j=1,\dots,n}$$

Si $\{\alpha_1,\dots,\alpha_n\}$ es una base, el sistema únicamente admite la solución trivial, ya que si $(x_1,\dots,x_n)$ es una solución, entonces obtenemos una combinación de los homomorfismos σ_i;

$$\sigma_1 x_1+\cdots\sigma_n x_n=0,$$

lo que, por el lema de independencia de Dedekind, implica que $x_1=\cdots=x_n=0$. Entonces ha de ser el sistema compatible determinado, y por tanto el determinante de la matriz del sistema es no nulo; $\det\big(\sigma_i(\alpha_j)\big)_{ij}\neq 0$.

(b) $\Rightarrow$ (a). Supongamos que $\{\alpha_1,\dots,\alpha_n\}$ no es una base, entonces no son linealmente independientes, y existen elementos $a_i\in K$, $1\leq i\leq n$, no todos nulos, tales que

$$a_1\alpha_1+\cdots+a_n\alpha_n=0,$$

entonces

$$a_1\sigma_i(\alpha_1)+\cdots+a_n\sigma_i(\alpha_n)=0, \text{para todo } i \text{ tal que } 1\leq i\leq n.$$

Entonces el sistema tiene solución no trivial, y por tanto el determinante de la matriz del sistema es nulo; $\det\big(\sigma_i(\alpha_j)\big)_{ij}=0$.

Queda por último relacionar los dos determinantes, el de (b) y el de (c). Se verifica

$$T_{F/K}(\alpha_i\alpha_j)=\sum\{\sigma_k(\alpha_i)\sigma_k(\alpha_j)\mid 1\leq k\leq n\};$$

este es el elemento (i,j) del producto de las matrices $(\sigma_k(\alpha_i))^t_{ki}\ \big(\sigma_k(\alpha_j)\big)_{kj}$. Por lo tanto tenemos

$$\det\big(T_{F/K}(\alpha_i\alpha_j)\big)_{ij}=\big[\det(\sigma_k(\alpha_i))_{ki}\big]^2,$$

y $\det\big(T_{F/K}(\alpha_i\alpha_j)\big)_{ij}\neq 0$ si, y sólo si, $\det(\sigma_k(\alpha_i))_{ki}\neq 0$, si, y sólo si, $\{\alpha_1,\dots,\alpha_n\}$ es una base de F. □

A la luz de este resultado, dada una extensión finita y separable F/K, se define una aplicación $T:F\times F\longrightarrow K$ mediante $T(\alpha,\beta)=T_{F/K}(\alpha\beta)$.

Proposición. 14.8.
Sea F/K una extensión finita y separable, entonces

$$T : F \times F \longrightarrow K, \text{ definida } T(\alpha,\beta) = T_{F/K}(\alpha\beta),$$

es una forma bilineal simétrica no degenerada sobre F con valores en K.

DEMOSTRACIÓN. Vamos a probar que es bilineal:

$$\begin{aligned} T(\alpha+\alpha',\beta) &= T_{F/K}((\alpha+\alpha')\beta) = T_{F/K}(\alpha\beta+\alpha'\beta) \\ &= T_{F/K}(\alpha\beta) + T_{F/K}(\alpha'\beta) = T(\alpha,\beta) + T(\alpha',\beta). \\ T(a\alpha,\beta) &= T_{F/K}(a\alpha\beta) = aT_{F/K}(\alpha\beta) \\ &= aT(\alpha,\beta), \end{aligned}$$

para cualesquiera α ,α', $\beta \in F$ y $a \in K$. De forma análoga se puede probar que es lineal en la segunda variable.

Evidentemente es simétrica.

Vamos a probar que es no degenerada, para esto utilizamos el Lema (14.7.). □

El determinante $\det\left(T_{F/K}(\alpha_i\alpha_j)\right)_{ij}$ es de interés en el estudio de extensiones finitas y separables de cuerpos, por cuanto sirve para caracterizar bases. Vamos a llamarlo el **discriminante de la extensión** relativo a la base $\{\alpha_1,\ldots,\alpha_n\}$. El primer problema que nos podemos plantear es cómo cambia el discriminante ante un cambio de base, esto lo resolvemos fácilmente mediante el siguiente lema.

Proposición. 14.9.
Sea F/K una extensión finita y separable de grado n, si $\{\alpha_1,\ldots,\alpha_n\}$ y $\{\beta_1,\ldots,\beta_n\}$ son dos bases de F, como espacio vectorial sobre K, con matriz de cambio de base A, entonces se tiene

$$\det\left(T_{F/K}(\alpha_i\alpha_j)\right)_{ij} = [\det(A)]^2 \det\left(T_{F/K}(\beta_i\beta_j)\right)_{ij}.$$

DEMOSTRACIÓN. Hacer como ejercicio. □

Como consecuencia, si en la situación anterior existe una base con discriminante no nulo, éste es no nulo para cada base. Una extensión F/K diremos que **tiene discriminante no nulo** si existe una base que tiene discriminante no nulo.

Proposición. 14.10.
Sea F/K una extensión finita y separable de grado n, entonces el discriminante de la extensión es no nulo.

Finalmente vamos a estudiar un discriminante de una extensión simple $K(\alpha)/K$, y ver que está relacionado con el discriminante del polinomio irreducible $\mathrm{Irr}(\alpha, K)$.

Teorema. 14.11.
Sea $K(\alpha)/K$ una extensión finita y separable de grado n. El discriminante de la extensión $K(\alpha)/K$ relativo a la base $\{1, \alpha, \dots, \alpha^{n-1}\}$ coincide con el discriminante de $\mathrm{Irr}(\alpha, K)$.

DEMOSTRACIÓN. Supongamos que $\alpha_1 = \alpha$, $\alpha_2, \dots, \alpha_n$ son las raíces de $\mathrm{Irr}(\alpha, K)$ en una clausura algebraica de K. Consideramos la base $\{1, \alpha, \dots, \alpha^{n-1}\}$; los homomorfismos de $K(\alpha)$ en $\overline{K}$ sobre K están definidos por las imágenes de α y son precisamente

$$\{\sigma_1, \dots, \sigma_n \mid \text{ definidos } \sigma_i(\alpha) = \alpha_i,\ 1 \le i \le n\}.$$

Se verifica:

$$\det\left(\sigma_i(\alpha^j)\right)_{ij} = \det\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix} = \prod\{\alpha_i - \alpha_h \mid\ 1 \le i, h \le n\}. \qquad \begin{cases} 1 \le i \le n, \\ 0 \le j \le n-1. \end{cases}$$

entonces

$$\det\left(T_{F/K}(\alpha^k \alpha^j)\right)_{kj} = \left[\det\left(\sigma_i(\alpha^j)\right)_{ij}\right]^2 = \mathrm{Discr}(\mathrm{Irr}(\alpha, K)). \qquad \begin{cases} 1 \le i \le n, \\ 0 \le k, j \le n-1. \end{cases}$$

□

14.1. Ejercicios

Norma y traza

Ejercicio. 14.12.
Sea $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. *Calcula* $N_{E/\mathbb{Q}}(\alpha)$ *y* $T_{E/\mathbb{Q}}(\alpha)$ *para*

(1) $\alpha = \sqrt{2}$,
(2) $\alpha = \sqrt{2} + \sqrt{3}$,
(3) $\alpha = \sqrt{6}$,
(4) $\alpha = 2$.

Ref.: 4163e_052 SOLUCIÓN

Ejercicio. 14.13.
Sea $E = \mathbb{Q}(\zeta)$ *con* ζ *una raíz quinta primitiva de la unidad y* $\beta = \zeta + \zeta^{-1}$. *Calcular*

(1) $N_{E/\mathbb{Q}}(\beta)$,
(2) $T_{E/\mathbb{Q}}(\beta)$,
(3) $N_{E/\mathbb{Q}(\beta)}(\zeta)$,
(4) $T_{E/\mathbb{Q}(\beta)}(\zeta)$.

Ref.: 4163e_053 SOLUCIÓN

Ejercicio. 14.14.
Sea K *un cuerpo finito y* F/K *una extensión finita. Demuestra que* $N_{F/K}$ *y* $T_{F/K}$ *son aplicaciones sobreyectivas de* F *en* K.
Ref.: 4163e_054 SOLUCIÓN

Ejercicio. 14.15.
Sea K *un cuerpo finito y* F/K *una extensión finita. Calcula el núcleo de*

$$N_{F/K} : F^\times \longrightarrow K^\times.$$

Ref.: 4163e_055 SOLUCIÓN

Ejercicio. 14.16.
Sea F/K una extensión cíclica de grado n, con grupo de Galois $G = \langle\sigma\rangle$. Si $\beta \in F$ es un elemento de norma uno, encontrar todas las soluciones $\beta = x/\sigma(x)$.
Ref.: 4163e_056 SOLUCIÓN

Ejercicio. 14.17.
Sea ζ una raíz n-ésima primitiva de la unidad y sea $F = \mathbb{Q}(\zeta)$.

(1) Si ξ es una raíz p^r–ésima primitiva de la unidad, determina $\varphi_{p^r}(X) = \mathrm{Irr}(\xi, \mathbb{Q})$.
(2) Si $n = p^r$, donde $r \geq 1$, es una potencia de primo, demostrar que $N_{F/\mathbb{Q}}(1-\zeta) = p$.
(3) Si $p^2 | n$, se tiene $\varphi_n(X) = \varphi_{n/p}(X^p)$; si $p | n$ y $p^2 \nmid n$, entonces $\varphi_n(X) | \varphi_{n/p}(X^p)$ es un factor propio.
(4) Da una fórmula para al cálculo del $\varphi_{p_1 \cdots p_t}(X)$, siendo los p_i enteros positivos primos distintos dos a dos.
(5) Si n es divisible, por al menos dos primos distintos, demostrar que $N_{F/\mathbb{Q}}(1-\zeta) = 1$.

Ref.: 4163e_057 SOLUCIÓN

Ejercicio. 14.18.
Sea ξ una raíz q–ésima de la unidad, siendo $q = p^n$, con p primo y $n \in \mathbb{N} \setminus \{0\}$. Si $K = \mathbb{Q}(\xi)$, calcula $N_{K/\mathbb{Q}}(1-\xi)$.
Ref.: 4163e_068 SOLUCIÓN

Ejercicio. 14.19.
Si $F = K(u)$ es una extensión separable de K y $f(x) = \mathrm{Irr}(u, K)$ con $\mathrm{grad}(f(x)) = n$, demuestra que el discriminante de la base $\{1, u, \ldots, u^{n-1}\}$ de F/K viene dado por

$$(-1)^{\frac{n(n-1)}{2}} N_{F/K}(Df(u))$$

Ref.: 4163e_090 SOLUCIÓN

Ejercicio. 14.20.
Sea F una extensión separable finita de K y sea $\{u_1,\dots,u_n\}$ una base de F sobre K. Para $u\in F$, sea $\varphi_u : F\to F$ el K-homomorfismo de espacios vectoriales dado por

$$uu_i=\sum_{j=1}^{n} a_{ij}u_j$$

$a_{ij}\in K$, $i=1,\dots,n$. Sea $A=(a_{ij})$. Demostrar que $N_{F/K}(u)=|A|$ y $T_{F/K}(u)=Traza(A)$
Ref.: 4163e_091 SOLUCIÓN

Ejercicio. 14.21.
Sea F es una extensión separable y finita de K. Si σ es un isomorfismo de F en algún cuerpo $\sigma(F)$ y $u\in F$ entonces

$$N_{\sigma(F)/\sigma(K)}(\sigma(u))=\sigma(N_{F/K}(u)) \quad y \quad T_{\sigma(F)/\sigma(K)}(\sigma(u))=\sigma(T_{F/K}(u)).$$

Ref.: 4163e_092 SOLUCIÓN

Ejercicio. 14.22.
Demuestra que el polinomio $X^{2^n}+X+1$ es reducible sobre $\mathbb{F}_2$, para $n\geq 3$.
Ref.: 4163e_023 SOLUCIÓN

Ejercicio. 14.23.
Demuestra que $X^{p^n}-X+1$ es irreducible sobre $\mathbb{F}_p$ sólo si $n=1$ o $n=p=2$.

(Nótese que si α es una raíz, también lo es $\alpha+a$ para cualquier $a \in \mathbb{F}_{p^n}$. Demuestra que esto implica que $\mathbb{F}_p(\alpha)$ contiene a $\mathbb{F}_{p^n}$ y que $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p$.)

Ref.: 4163e_024 SOLUCIÓN

Extensiones cíclicas, norma y traza.

Ejercicio. 14.24.
Sea E/K una extensión cíclica de grado n, con $\mathrm{Gal}(E/K) = \langle\tau\rangle$. Sea F un cuerpo intermedio con $[F : K] = m$ y $n = tm$. Si existe $a \in K$ tal que $a^t = N_{E/K}(\alpha)$, para algún $\alpha \in E$, prueba que existe $\beta \in F$ tal que $c = N_{F/K}(\beta)$.

Ref.: 4163e_075 SOLUCIÓN

Ejercicio. 14.25.
Sea K un cuerpo contiene p raíces distintas p-ésimas de la unidad, p es un entero positivo primo. Sea F/K una extensión cíclica de grado $p^n > 1$. Demuestra que si existe un torre $E \supset F \supset K$ donde E/K es cíclica de grado p^{n+1}, para cada raíz p–ésima primitiva de la unidad ζ entonces existe un $\alpha \in F$ tal que $N_{F/K}(\alpha) = \zeta$.

Ref.: 4163e_058 SOLUCIÓN

Ejercicio. 14.26.
Demostrar que si $F = \mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ y $m < 0$, entonces no existe ninguna extensión cuártica cíclica $E/\mathbb{Q}$ con $E \supset F \supset \mathbb{Q}$.

Ref.: 4163e_059 SOLUCIÓN

Ejercicio. 14.27.
Con las mismas notaciones que en el ejercicio (14.25.), sea $\mathrm{Gal}(F/K) = \langle\sigma\rangle$. Supongamos que existe un elemento $\alpha \in F$ tal que $N_{F/K}(\alpha) = \zeta$. Demostrar que

(1) *Existe un elemento* $\beta \in F$ *tal que* $\sigma(\beta) = \alpha^p \beta$.
(2) $X^p - k\beta \in F[X]$ *es irreducible para cada* $k \in K \setminus \{0\}$. *En particular,* β *no es una* p*-ésima potencia en* F.
(3) *Si* $E = F(\gamma)$ *con* $\gamma^p = \beta$, *entonces* E/K *es cíclica de grado* p^{n+1}.
(4) *Si* $K \subseteq F \subseteq E$ *es una extensión cíclica de grado* p^{n+1}, *existe* $k \in K \setminus \{0\}$ *tal que* E *es el cuerpo de descomposición de* $X^p - k\beta$ *sobre* F.

Ref.: 4163e_060 SOLUCIÓN

Ejercicio. 14.28.
Nótese que los Ejercicios (14.25.) *y* (14.27.) *implican el siguiente*

Teorema. *Si* K *contiene* p *raíces* p*-ésimas distintas de la unidad* (p *primo*) *y si* F/K *es cíclica de grado* $p^n > 1$, *entonces* E *puede sumergirse en una extensión cíclica de grado* p^{n+1} *sobre* K *si, y sólo si, una raíz* p*-ésima primitiva de la unidad* ζ *es la norma de algún elemento de* F.

Utilizar este teorema para demostrar que si la característica de K *es distinta de* 2 *y* $F = K(\sqrt{c}) \neq K$, *entonces* F/K *puede sumergirse en una extensión cuártica cíclica de* K *si, y sólo si,* c *es la suma de dos cuadrados de elementos de* K.

Ref.: 4163e_061 SOLUCIÓN

Ejercicio. 14.29.
Sea F/K *una extensión cíclica de grado* p^n, *y* $\zeta \in K$ *una raíz* p^m*–ésima primitiva de la unidad,* $n > m \geq 1$. *Son equivalentes:*

(a) $\zeta \in N_{F/K}(F^\times)$.
(b) *Existe una torre* $K \subseteq F \subseteq E$ *tal que* E/K *es cíclica de grado* p^{n+m}.

Ref.: 4163e_076 SOLUCIÓN

Ejercicio. 14.30.
Sea F/K *una extensión cíclica de grado* p^n, *y* ξ *una raíz* p^m*–ésima primitiva de la unidad. Son equivalentes:*

(a) Existe $\alpha \in F$ tal que $N_{F/K}(\alpha) = \xi$.
(b) Existe una extensión $E \supseteq F \supseteq K$ tal que E/K es cíclica y $[E : F] = p^m$.

Ref.: 4163e_074 SOLUCIÓN

Ejercicio. 14.31.
Determina el grupo de Galois de la extensión $\mathbb{Q}(\omega, \sqrt[5]{3})/\mathbb{Q}$, donde $\omega \neq -1$ es una raíz de $X^5 + 1$. Construye una serie de composición de G, si la hay, y la torre de subextensiones asociada.
Nota: Posibles grupos: S_5, A_5, $F_{20} = \langle (12345), (1243) \rangle$, $D_5 = \langle (12345), (14)(23) \rangle$, $C_5 = \langle (12345) \rangle$.
Ref.: 4163e_100 SOLUCIÓN

15. Extensiones cíclicas y radicales

Extensiones cíclicas

Una extensión E/K se llama

- **cíclica** si es de Galois y su grupo de Galois es cíclico, y
- **abeliana** si su grupo de Galois es un grupo abeliano.

Teorema. 15.1. (Teorema 90 de Hilbert)
Sea E/K una extensión cíclica de grado n con grupo $G = \mathrm{Gal}(E/K) = \langle\sigma\rangle$ y sea $\beta \in E$. Son equivalentes:

(a) $N_{E/K}(\beta) = 1$;
(b) Existe $0 \neq \alpha \in E$ tal que $\beta = \alpha/\sigma(\alpha)$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Supongamos $N_{E/K}(\beta) = 1$, lo que implica $\beta \neq 0$. Los automorfismos $1, \sigma, \ldots, \sigma^{n-1}$ son distintos y por tanto linealmente independendientes sobre E. Luego la aplicación

$$\tau = 1 + \beta\sigma + (\beta\sigma(\beta))\sigma^2 + \cdots + (\beta\sigma(\beta)\ldots\sigma^{n-2}(\beta))\sigma^{n-1}$$

no es la aplicación cero. Por tanto existe $\theta \in E$ tal que $\tau(\theta) \neq 0$; llamamos $\alpha = \tau(\theta)$, y calculamos:

$$\sigma(\alpha) = \sigma(\tau(\theta)) = \sigma(\theta) + \sigma(\beta)\sigma^2(\theta) + \cdots + (\sigma(\beta)\ldots\sigma^{n-1}(\beta))\sigma^n(\theta)$$

Multiplicando por β, y teniendo en cuenta que $\sigma^n = 1$ y que $\beta\sigma(\beta)\cdots\sigma^{n-1}(\beta) = 1$, nos queda $\beta\sigma(\alpha) = \alpha$.
(b) $\Rightarrow$ (a). Si $\beta = \alpha/\sigma(\alpha)$, obtenemos:

$$N_{E/K}(\beta) = \frac{N_{E/K}(\alpha)}{N_{E/K}(\sigma(\alpha))} = 1$$

□

Teorema. 15.2. (Teorema de Lagrange)
Sea K un cuerpo, n un entero positivo que es primo con la característica de K, si ésta es no nula, y supongamos que existe una raíz n-ésima primitiva de la unidad ξ en K. Se verifica:

4163-04.tex

(1) Si E/K es una extensión cíclica de grado n, entonces existe $\alpha \in E$ tal que $E = K(\alpha)$ e $\mathrm{Irr}(\alpha, K) = X^n - a$ para algún $a \in K$.
(2) A la inversa, sea $a \in K$. Si α es una raíz de $X^n - a$, entonces $K(\alpha)/K$ es una extensión cíclica de grado d, con $d|n$ y $\alpha^d \in K$.

DEMOSTRACIÓN. (1). Sea $G = \mathrm{Gal}(E/K) = \langle\sigma\rangle$, y sea $\xi \in K$ una raíz n-ésima primitiva de la unidad, entonces $N_{E/K}(\xi^{-1}) = \xi^{-n} = 1$. Por el teorema 90 de Hilbert, existe $\alpha \in E$ tal que $\sigma(\alpha) = \xi\alpha$. Por inducción sobre i, se verifica $\sigma^i(\alpha) = \xi^i\alpha$. Luego los elementos $\xi^i\alpha$ son los n conjugados distintos de α, por lo que $[K(\alpha) : K] \geq n$, y como $K(\alpha) \subseteq E$, tenemos que $E = K(\alpha)$. Además, $\sigma(\alpha^n) = \sigma(\alpha)^n = (\xi\alpha)^n = \alpha^n$, luego $a = \alpha^n$ es fijo bajo σ y todas sus potencias, por lo que $a \in K$.
(2). Sea α una raíz de $X^n - a \in K[X]$, y sea $\xi \in K$ la raíz n–ésima primitiva de la unidad en K. Entonces $\xi^i\alpha$ también es raíz del mismo polinomio y todas estas raíces son distintas. Luego $K(\alpha)$ es el cuerpo de descomposición sobre K del polinomio $X^n - a$, y por tanto $K(\alpha)/K$ es una extensión de Galois. Sea $G = \mathrm{Gal}(K(\alpha)/K)$, para todo $\sigma \in G$, se tiene que $\sigma(\alpha)$ también es raíz de $X^n - a$. Luego $\sigma(\alpha) = \omega_\sigma\alpha$, siendo ω_σ una raíz de la unidad (no necesariamente primitiva). La aplicación $\sigma \mapsto \omega_\sigma$ es obviamente un monomorfismo de G en el grupo de las raíces n-ésimas de la unidad, y como éste es un grupo cíclico de orden n, entonces G es un grupo cíclico de orden d, un divisor de n. Sea $G = \langle\sigma\rangle$. Entonces ω_σ es una raíz d-ésima primitiva de la unidad, y $\sigma(\alpha^d) = (\omega_\sigma\alpha)^d = \alpha^d$, luego $\alpha^d \in K$ ya que es fijo bajo $G = \mathrm{Gal}(K(\alpha)/K)$. □

Teorema. 15.3. (Teorema 90 de Hilbert, forma aditiva)
Sea K un cuerpo y E/K una extensión cíclica de grado n con grupo $G = \mathrm{Gal}(E/K) = \langle\sigma\rangle$ y sea $\beta \in E$. Son equivalentes:
(a) $T_{E/K}(\beta) = 0$;
(b) Existe $\alpha \in E$ tal que $\beta = \alpha - \sigma(\alpha)$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Sea $T_{E/K}(\beta) = 0$. Existe $\theta \in E$ tal que $T_{E/K}(\theta) \neq 0$. Sea

$$\alpha = \frac{1}{T_{E/K}(\theta)}(\beta\sigma(\theta) + (\beta + \sigma(\beta))\sigma^2(\theta) + \cdots + (\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta))\sigma^{n-1}(\theta))$$

Calculando se ve que $\sigma(\alpha) = \alpha - \beta$.
(b) $\Rightarrow$ (a). A la inversa, sea $\beta = \alpha - \sigma(\alpha)$. Calculemos:

$$T_{E/K}(\beta) = T_{E/K}(\alpha) - T_{E/K}(\sigma(\alpha)) = 0.$$

□

Teorema. 15.4. (Teorema de Artin–Schreier)
Sea K un cuerpo de característica p. Se verifica:

(1) Si E/K es una extensión cíclica de grado p, entonces existe $\alpha \in E$ tal que $E = K(\alpha)$ y $\mathrm{Irr}(\alpha, K) = X^p - X - a$ para algún $a \in K$.

(2) A la inversa, para $a \in K$ el polinomio $X^p - X - a$ tiene una raíz en K, en cuyo caso todas las raíces están en K, o es irreducible; en este caso, si α es una raíz, la extensión $K(\alpha)/K$ es cíclica de grado p.

DEMOSTRACIÓN. (1). $T_{E/K}(-1) = p(-1) = 0$. Por el teorema 90 existe $\alpha \in E$ tal que $-1 = \alpha - \sigma(\alpha)$, esto es, $\sigma(\alpha) = \alpha + 1$. Luego para todo i, se verifica $\sigma^i(\alpha) = \alpha + i$ y α tiene p conjugados distintos. Entonces, por el teorema del grado, $[K(\alpha) : K] = p$ y $E = K(\alpha)$. Calculamos:

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Luego $a = \alpha^p - \alpha$ es fijo bajo σ y todas sus potencias, y está en el cuerpo fijo bajo G que es K. Luego α es raíz de $X^p - X - a \in K[X]$ que tiene que ser irreducible (razonando sobre el grado).

(2). Si α es una raíz de $f = X^p - X - a$, entonces $\alpha + i$ también lo es para todo i. Luego f tiene p raíces distintas. Si una raíz está en K, todas están en K. Supongamos que no hay ninguna raíz en K y que f es reducible. Sea $f = g \cdot h$ con $g, h \in K[X]$ no triviales. Como $d = \mathrm{gr}(g) < \mathrm{gr}(f) = p$, entonces g será el producto de d factores de la forma $(X - (\alpha + i))$. El coeficiente de X^{d-1} es de la forma $-d\alpha + j$ para algún entero j. Pero $d \neq 0$, luego α está en K, lo que es una contradicción.

Sabemos ahora que si α no está en K, entonces f es irreducible. Por el mismo razonamiento que antes todas las raíces de f están en $K(\alpha)$ que es por tanto una extensión normal de K. Como $\alpha + 1$ es también una raíz de f, existe un $\sigma \in \mathrm{Gal}(K(\alpha)/K)$ tal que $\sigma(\alpha) = \alpha + 1$. Las potencias de σ nos dan todas las demás raíces: $\sigma^i(\alpha) = \alpha + i$. Luego $\langle\sigma\rangle$ tiene orden p y por tanto $\mathrm{Gal}(K(\alpha)/K) = \langle\sigma\rangle$. □

Como consecuencia de estos resultados, tenemos caracterizadas las extensiones cíclicas en todos los casos.

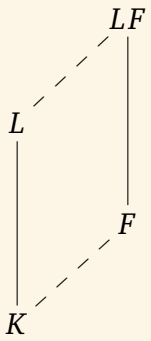
Extensiones solubles y radicales

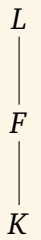
Una extensión finita y separable F/K se llama

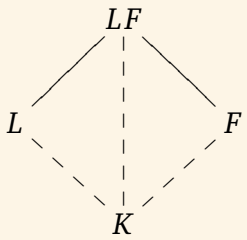
- **soluble** si existe una extensión de Galois finita E/K con grupo $G = \mathrm{Gal}(E/K)$ soluble tal que $K \subseteq F \subseteq E$.

La anterior definición es equivalente a decir que la clausura normal de F/K tiene grupo de Galois soluble.
La siguiente proposición no es necesaria para la demostración del Teorema (15.8.), del cual se deduce inmediatamente.

Proposición. 15.5.
(1) Sea F/K una extensión soluble, y sea L/K una extensión arbitraria. Entonces FL/L es una extensión soluble.
(2) Sea $L \supseteq F \supseteq K$ una torre de extensiones separables y finitas. Entonces L/K es soluble si y sólo si L/F y F/K son solubles.
(3) Sean F/K y L/K extensiones solubles. Entonces FL/K es soluble.

(1)


(2)


(3)


Una extensión finita y separable

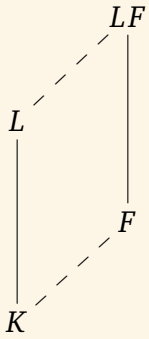
- F/K se llama **soluble por radicales** si existe una torre de extensiones finitas

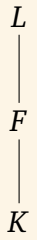
$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_m = E \tag{III.1}$$

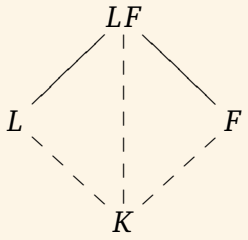
tal que $F \subseteq E$ y que cada paso E_{i+1}/E_i es de uno de los tipos siguientes:

(1) $E_{i+1} = E_i(\xi)$ con ξ raíz de la unidad.
(2) $E_{i+1} = E_i(\alpha)$ con α raíz de un polinomio $X^n - a \in E_i[X]$ y n primo relativo con $\mathrm{car}(K)$, si ésta es no nula, y existe $\xi \in E_i$ raíz n–ésima primitiva de la unidad.
(3) $E_{i+1} = E_i(\alpha)$ con α raíz de un polinomio $X^p - X - a \in E_i[X]$ y $p = \mathrm{car}(K)$.

Proposición. 15.6.
(1) Sea F/K una extensión soluble por radicales, y sea L/K una extensión arbitraria. Entonces FL/L es una extensión soluble por radicales.
(2) Sea $L \supseteq F \supseteq K$ una torre de extensiones separable y finitas. Entonces L/K es soluble por radicales si, y sólo si, L/F y F/K son solubles por radicales.
(3) Sean F/K y L/K extensiones solubles por radicales. Entonces FL/K es soluble por radicales.

(1)


(2)


(3)


DEMOSTRACIÓN. (1). Sea

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_m = E$$

la torre de extensiones del tipo (III.1) con $F \subseteq E$. Definimos una nueva torre:

$$L = E_0' \subseteq E_1' \subseteq E_2' \subseteq \cdots \subseteq E_m' = E'$$

siendo $E_i' = E_i L$. Es evidente que $E_0' = KL = L$, que $E_m' = EL > FL$ y que si $E_{i+1} = E_i(\alpha)$, entonces $E_{i+1}' = E_i'(\alpha)$ es del mismo tipo. Luego la extensión FL/L es soluble por radicales.
(2). Sea L/K soluble por radicales. El mismo cuerpo E que contiene a L también contiene a F. Luego F/K es soluble por radicales. Por otra parte, aplicamos el punto anterior a las extensiones L/K (que es soluble por radicales por hipótesis) y L/F. Nos queda que $L = LF/F$ es soluble por radicales.
A la inversa, sean L/F y F/K solubles por radicales. Sea E el cuerpo que contiene a F y que permite la torre (III.1). La extensión LE/E es soluble por radicales por el punto anterior. Sea

$$E = E_m \subseteq E_{m+1} \subseteq E_{m+2} \subseteq \cdots \subseteq E_n = LE$$

la torre que verifica las condiciones de (III.1). Pegamos ambas torres y obtenemos la torre:

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n = LE \supseteq L,$$

donde cada paso es de uno de los tipos permitidos. Luego L/K es radical.
(3). Es consecuencia inmediata de los dos puntos anteriores. □

Corolario. 15.7.
Sea F/K una extensión separable y finita. Entonces F/K es soluble por radicales si, y sólo si, existe una torre

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_m = L \supseteq F$$

donde cada paso es de uno de los tipos descritos en (III.1)*, y además la extensión L/K es de Galois.*

DEMOSTRACIÓN. Sólo hay que demostrar la última propiedad. Sea F/K soluble por radicales, y sea

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_m = E$$

la torre que lo muestra. Para todo $\sigma : E/K \longrightarrow \overline{K}/K$ (clausura algebraica de K), la torre

$$K = E_0 \subseteq \sigma(E_1) \subseteq \sigma(E_2) \subseteq \cdots \subseteq \sigma(E_m) = \sigma(E)$$

tiene cada paso del mismo tipo, ya que $\sigma(E_{i+1}) = \sigma(E_i)(\sigma(\alpha))$. Luego $\sigma(E)/K$ es soluble por radicales. Sea $L = \prod_\sigma \sigma(E)$. Por el tercer punto de la proposición anterior, L posee una torre del tipo buscado. Además, L/K es la clausura normal de E/K y por tanto es de Galois. □

Teorema. 15.8. (Teorema de Galois)
Sea F/K una extensión separable y finita. son equivalentes:

(a) F/K es soluble por radicales;
(b) F/K es soluble.

DEMOSTRACIÓN. (b) ⇒ (a). Sea F/K soluble. Sea E/K una extensión de Galois con grupo soluble tal que $E \supseteq F$, y sea m el producto de todos los primos que dividen al orden de $\mathrm{Gal}(E/K)$. Sea ξ una raíz m-ésima primitiva de la unidad. Llamamos $L = K(\xi)$. La extensión EL/L es de Galois con grupo isomorfo a un subgrupo de $\mathrm{Gal}(E/K)$, luego también soluble. Tomamos una serie de composición:

$$\mathrm{Gal}(EL/L) = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1.$$

Cada cociente G_i/G_{i+1} es cíclico de orden primo divisor de $|G_0|$. Por la correspondencia de Galois, obtenemos una torre de cuerpos:

$$K \subset L = L_0 \subset L_1 \subset \cdots \subset L_n = EL \supset F,$$

donde cada eslabón es una extensión de Galois con grupo $\mathrm{Gal}(L_{i+1}/L_i) \cong G_i/G_{i+1}$ cíclico de orden primo, y $L_i \supseteq L$ contiene todas las raíces de la unidad necesarias. Aplicando los Teoremas (15.2.)

o (15.4.) según sea el primo, vemos que cada extensión es de uno de los tipos definidos en (III.1). Luego F/K es soluble por radicales.

(a) $\Rightarrow$ (b). Sea ahora F/K soluble por radicales. Por el corolario anterior, existe una extensión de Galois E/K tal que $F \subseteq E$ y que existe una torre

$$K = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_m = E,$$

donde cada eslabón es de uno de los tipos descritos en (III.1). Igual que antes, sea m el producto de todos los primos que dividen a $|\mathrm{Gal}(E/K)|$ y sea ξ una raíz m-ésima primitiva de la unidad. Llamamos $L = K(\xi)$. L/K es de Galois con grupo abeliano y EL/L también es de Galois. Llamamos $L_i = E_i L$. Obtenemos la torre

$$L = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_m = EL,$$

donde cada paso es de uno de los tipos requeridos. Por la correspondencia de Galois, le corresponde una serie de subgrupos:

$$\mathrm{Gal}(EL/L) = G_0 \rhd G_1 \rhd G_2 \rhd \cdots G_m = 1,$$

donde cada cociente $G_i/G_{i+1} \cong \mathrm{Gal}(L_{i+1}/L_i)$ es abeliano para el primer tipo de (III.1) y cíclico para cada uno de los otros por los Teoremas (15.2.) y (15.4.). Luego $\mathrm{Gal}(EL/L)$ es soluble. Como $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(EL/K)/\mathrm{Gal}(EL/L)$ es abeliano, el grupo $\mathrm{Gal}(EL/K)$ es soluble y la extensión F/K es soluble, ya que $F \subset EL$. □

15.1. Ejercicios

Extensiones cíclicas y radicales

Ejercicio. 15.9.
Sea F un cuerpo de característica distinta de 2. Dar una condición necesaria y suficiente sobre elementos $\alpha, \beta \in F$ para que $F(\sqrt{\alpha}) = F(\sqrt{\beta})$. Usar esta condición para determinar si $\mathbb{Q}(\sqrt{1-\sqrt{2}}) = \mathbb{Q}(i, \sqrt{2})$.
Ref.: 4163e_062 SOLUCIÓN

Ejercicio. 15.10.
Sea $F = \mathbb{Q}(\sqrt[n]{a})$, con $a \in \mathbb{Q}$, $a \geq 0$ tal que que $[F : \mathbb{Q}] = n$. Sea E cualquier subcuerpo de F tal que $[E : \mathbb{Q}] = d$. Demostrar que $E = \mathbb{Q}(\sqrt[d]{a})$.
Nota: considerar $N_{F/E}(\sqrt[n]{a}) \in E$.
Ref.: 4163e_063 SOLUCIÓN

Ejercicio. 15.11.
Sea F como en el Ejercicio (15.10.). Demostrar que si n es impar entonces F no tiene extensiones intermedias de Galois sobre $\mathbb{Q}$ y que si n es par, la única extensión intermedia de F que es de Galois sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{a})$.
Ref.: 4163e_064 SOLUCIÓN

Ejercicio. 15.12.
Sea L la clausura de Galois del cuerpo F en los dos ejercicios anteriores. Demostrar que $[L : \mathbb{Q}] = n\varphi(n)$ ó $\frac{n\varphi(n)}{2}$.
Nota: $\mathbb{Q}(\zeta_n) \cap F$ es una extensión de Galois sobre $\mathbb{Q}$.
Ref.: 4163e_065 SOLUCIÓN

Ejercicio. 15.13.
Sea $\zeta \in K$ una raíz n–ésima primitiva de la unidad y $\mathrm{car}(K) \nmid n$. Sea F/K una extensión cíclica con $[F:K] = d \mid n$. Prueba:

(1) Se tiene $F = K(\sqrt[n]{a})$, para $a \in K$.
(2) Sea $\mathrm{Gal}(F/K) = \langle \sigma \rangle$, grupo cíclico de orden d, se tiene $\sigma(\alpha) = \xi\alpha$, para ξ una raíz d–ésima primitiva de la unidad.
(3) Si $F = K(\sqrt[n]{a}) = K(\sqrt[n]{b})$, entonces $\dfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \left(\dfrac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}\right)^j$, para j entero primo relativo con d. Como consecuencia $\sqrt[n]{a}/\sqrt[n]{b}^j \in K$.
(4) $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$ si, y sólo si, a y b generan el mismo subgrupo de $K^\times/K^{\times n}$ si, y sólo si, existen $h,k \in \mathbb{N}$ y $c,d \in K$ tal que $a = b^h c^n$ y $b = a^k d^n$.

Ref.: 4163e_077 SOLUCIÓN

Ejercicio. 15.14.
Sean p,q,r enteros primos positivos con $q \neq r$. Sean $\sqrt[p]{q}$ y $\sqrt[p]{r}$ las raíces de los polinomios $X^p - q$ y $X^p - r$. Demuestra que $\mathbb{Q}(\sqrt[p]{q}) \neq \mathbb{Q}(\sqrt[p]{r})$.
Ref.: 4163e_066 SOLUCIÓN

Ejercicio. 15.15.
Sea K un subcuerpo de $\mathbb{R}$, $a \in K$ y $\alpha = \sqrt[n]{a}$ una raíz n-ésima real de a. Demuestra que:

(1) Si $n = p$ es primo, entonces $[K(\alpha):K]$ es 1 ó p.
(2) Si $K(\alpha)/K$ es de Galois entonces $[K(\alpha):K] \leq 2$.

Ref.: 4163e_067 SOLUCIÓN

Ejercicio. 15.16.
Se considera el polinomio $(X^{14}-1)(X^{15}-2) \in \mathbb{Q}[X]$.

(1) Prueba que $\mathbb{Q}(\xi_{14}) \cap \mathbb{Q}(\xi_{15}) = \mathbb{Q}$.

(2) *Prueba que* $\mathbb{Q}(\sqrt[15]{2}) \cap \mathbb{Q}(\xi_{15}) = \mathbb{Q}$.
(3) *Si* E *es el cuerpo de descomposición determina el grado de la extensión* $E/\mathbb{Q}$.

Ref.: 4163e_070 SOLUCIÓN

Ejercicio. 15.17.
Sea p *un entero primo positivo. Determina el grupo de Galois de la extensión de* $\mathbb{F}_p$ *por las raíces* n*–ésimas de la unidad, siendo* $p \nmid n$.

Pista.

(1) *Si* $\xi_0, \xi_1, \ldots, \xi_{n-1}$ *son la raíces* n*–ésimas de la unidad, prueba que* $\mathbb{F}_p(\xi_0, \xi_1, \ldots, \xi_{n-1})/\mathbb{F}_p$ *está generado por una de las raíces* ξ*; cada uno de los generadores se llama una* ***raíz*** n***–ésima primitiva de la unidad*** *sobre* $\mathbb{F}_p$.
(2) *Tenemos que el grupo de las raíces* n*–ésimas de la unidad,* $\{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$*, es un subgrupo del grupo multiplicativo de* $\mathbb{F}_p(\xi) = \mathbb{F}_{p^s}$. *Para determinar el grupo de Galois hay que averiguar el valor de* s*; el grado de la extensión* $\mathbb{F}_p(\xi)/\mathbb{F}_p$ *es igual a* s*, y por lo tanto el grupo de Galois pedido es el grupo cíclico de orden* s.
(3) *Como* $\xi \in \mathbb{F}_p(\xi) = \mathbb{F}_{p^s}$*, se verifica* $X^n - 1 \mid X^{p^s-1} - 1$*, por lo tanto* $n \mid p^s - 1$. *Para terminar, solo queda probar que* s *es el menor entero positivo que verifica* $n \mid p^s - 1$

Ref.: 4163e_071 SOLUCIÓN

Ejercicio. 15.18.
Sea K *un cuerpo. Si* $K(\alpha)/K$, $K(\beta)/K$ *son extensiones de Galois abelianas, entonces* $K(\alpha+\beta)/K$ *es una extensión de Galois abeliana.*
Ref.: 4163e_073 SOLUCIÓN

Ejercicio. 15.19.
Demostrar que $f(X) = X^p - X - a \in \mathbb{F}_p[X]$, $a \neq 0$, *es irreducible sobre* $\mathbb{F}_p$ *o descompone completamente.*
Demostrar que $f(X) \in \mathbb{F}_{p^n}[X]$ *es irreducible sobre* $\mathbb{F}_{p^n}$ *si, y sólo si, no tiene factores lineales.*

Ver también Ejercicio (12.34.).
Ref.: 4163e_079 *SOLUCIÓN*

Ejercicio. 15.20.
Sea K un cuerpo que no contiene una raíz cuarta primitiva de la unidad. Para $\alpha \in K \setminus K^2$ se define $F = K(\sqrt{\alpha})$, y para $\beta \in F \setminus F^2$ se define $E = F(\sqrt{\beta})$.
Si $N_{F/K}(\beta) \equiv \alpha \pmod{F^\times 2}$, prueba que se verifica:
(1) α es una suma de dos cuadrados de K.
(2) La extensión E/K es una extensión cíclica

Ref.: 4163e_018 *SOLUCIÓN*

Ejercicio. 15.21.
Sea F un cuerpo extensión separable de K de grado n. Demostrar que un elemento de F es primitivo si, y sólo si, tiene n conjugados en una clausura algebraica de K conteniendo a F.
Ref.: 4163e_093 *SOLUCIÓN*

Ejercicio. 15.22.
Hallar un elemento primitivo sobre $\mathbb{Q}$ para
(1) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$.
(2) $\mathbb{Q}(i, \sqrt{2})$.
(3) $\mathbb{Q}(\sqrt[3]{5}, \sqrt[5]{7})$.

Ref.: 4163e_094 *SOLUCIÓN*

Ejercicio. 15.23.
Sean $n_1,\dots,n_t \in \mathbb{Z}$ positivos mayores que 1, libres de cuadrados y primos relativos dos a dos, entonces $\dim(\mathbb{Q}(\sqrt{n_1},\dots,\sqrt{n_t})) = 2^t$.
Ref.: 4163e_081 SOLUCIÓN

Ejercicio. 15.24.
Sean $p_1,\dots,p_t$ son enteros primos positivos distintos dos a dos. Prueba que
(1) $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_t})/\mathbb{Q}) \cong \mathbb{Z}_2^t$.
(2) $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_t}) = \mathbb{Q}(\sqrt{p_1}+\cdots+\sqrt{p_t})$.

Ref.: 4163e_080 SOLUCIÓN

Ejercicio. 15.25.
Demostrar que $\mathbb{Q}(\sqrt[4]{5},i)$ es una extensión cíclica de $\mathbb{Q}(i)$ y encontrar un generador de $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{5},i)/\mathbb{Q})$.
Ref.: 4163e_095 SOLUCIÓN

Ejercicio. 15.26.
Prueba que la extensión $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ es cíclica de grado cuatro.
Compara con el Ejercicio (12.45.).
Ref.: 4163e_097 SOLUCIÓN

Ejercicio. 15.27.
Se considera la sucesión $\{\alpha_n\}_n$, definida:

$$\alpha_0 = 0,$$
$$\alpha_{n+1} = \sqrt{2+\alpha_n} \text{ para todo } n \in \mathbb{N}.$$

Prueba que la extensión $\mathbb{Q}(\alpha_n)/\mathbb{Q}$ es una extensión cíclica de grado 2^n.
Ref.: 4163e_098 *SOLUCIÓN*

Ejercicio. 15.28.
Prueba que existe un cuerpo K, que no es algebraicamente cerrado, tal que toda extensión finita algebraica F/K es una extensión cíclica de grado una potencia de 2.
Ref.: 4163e_109 *SOLUCIÓN*

Ejercicio. 15.29.
Prueba que existe un cuerpo K, que no es algebraicamente cerrado, tal que toda extensión finita algebraica es de orden una potencia de 3.
Ref.: 4163e_110 *SOLUCIÓN*

Ejercicio. 15.30.
Sea $f(X) \in K[X]$ un polinomio irreducible separable y F el cuerpo de descomposición de $f(X)$. Prueba que si $\mathrm{Gal}(F/K)$ es un grupo cíclico, entonces $F = K(\alpha)$, esto es, F/K es una extensión simple.
Ref.: 4163e_099 *SOLUCIÓN*

Ejercicio. 15.31.
Sea $F = K(\alpha)/K$ una extensión finita separable. Si $f(X) = \mathrm{Irr}(\alpha, K)$ y llamamos $Df(X)$ a su derivada, sea $\frac{f(X)}{X-\alpha} = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} \in F[X]$. Prueba que la base dual de $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es

$$\left\{\frac{b_0}{Df(\alpha)}, \ldots, \frac{b_{n-1}}{Df(\alpha)}\right\}.$$

Ref.: 4163e_101 *SOLUCIÓN*

15.2. Cuestiones

En las siguientes cuestiones responde "VERDADERO" ó "FALSO" y haz un breve razonamiento para justificar la respuesta.

(1) ☐ Si K es un cuerpo de característica $p \neq 0$ que tiene n raíces n–ésimas distintas de la unidad, entonces n no es múltiplo de p. (Ref.: 4163q_001)

(2) ☐ Si K es un cuerpo de característica $p \neq 0$, para cada entero positivo n siempre existe una extensión F/K que contiene n raíces n–ésimas distintas de la unidad. (Ref.: 4163q_002)

(3) ☐ Si $E = \mathbb{Q}(i, \sqrt[4]{5})$, entonces $N_{E/\mathbb{Q}}(i\sqrt[4]{5}) = 25$. (Ref.: 4163q_003)

(4) ☐ Si la extensión $K(\sqrt[n]{a})/K$ es de Galois, entonces es cíclica. (Ref.: 4163q_004)

(5) ☐ Si $\mathbb{F}$ un cuerpo finito, todo polinomio sobre $\mathbb{F}$ es soluble por radicales sobre $\mathbb{F}$. (Ref.: 4163q_005)

(6) ☐ $\mathbb{F}_{27}$ tiene un único subcuerpo propio. (Ref.: 4163q_006)

(7) ☐ Sea $K \subseteq F \subseteq E$ una torre de cuerpos, si E/K es una extensión abeliana, tiene grupo de Galois abeliano, entonces F/K es una extensión de Galois. (Ref.: 4163q_000)

(8) ☐ Existe una extensión ciclotómica $E/\mathbb{Q}$ con grupo de Galois isomorfo a S_3. (Ref.: 4163q_008)

(9) ☐ Toda extensión ciclotómica de $\mathbb{Q}$ es cíclica. (Ref.: 4163q_009)

(10) ☐ El grupo de Galois, sobre $\mathbb{Q}$, del polinomio $X^{36}-1$ es abeliano de orden 12. (Ref.: 4163q_010)

(11) ☐ El grupo de Galois, sobre $\mathbb{Q}$, del polinomio $X^{36}-1$ es cíclico de orden 12. (Ref.: 4163q_011)

(12) ☐ Existe una extensión $K/\mathbb{F}_3$ con grupo de Galois isomorfo a S_3. (Ref.: 4163q_012)

(13) ☐ Si $\xi = \xi_{13}$ es una raíz decimosexta primitiva de la unidad, entonces $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\sqrt[3]{2})$. (Ref.: 4163q_013)

(14) ☐ Si $\mathbb{F}_{p^n}$ y $\mathbb{F}_{p^m}$ son cuerpos finitos tales que $n \leq m$, entonces $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$. (Ref.: 4163q_014)

(15) ☐ Si $K/\mathbb{F}_2$ es una extensión finita, para todo $0 \neq \alpha \in K$ se tiene $N_{K/\mathbb{F}_2}(\alpha) = 1$. (Ref.: 4163q_015)

(16) ☐ Si $\phi_{10} \in \mathbb{Q}[X]$ es el polinomio ciclotómico, entonces $\phi_{10} = X^4 - X^3 - X^2 - X - 1$. (Ref.: 4163q_016)

4163-99.tex

(17) ☐ La extensión $\mathbb{F}_{81}/\mathbb{F}_3 = \mathbb{F}_{3^4}/\mathbb{F}_3$ tiene un exactamente 4 cuerpos intermedios. (Ref.: 4163q_017)

(18) ☐ Si $\xi = \xi_n$ es una raíz n–ésima primitiva de la unidad, se tiene $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong C_{n-1}$ si, y sólo si, n es un entero positivo primo. (Ref.: 4163q_018)

(19) ☐ Existe una extensión ciclotómica $E/\mathbb{Q}$ con grupo de Galois C_7. (Ref.: 4163q_019)

(20) ☐ Todas las extensiones ciclotómicas no triviales E de $\mathbb{Q}$ contienen un cuerpo real F de grado $\dfrac{[E:\mathbb{Q}]}{2}$. (Ref.: 4163q_020)

(21) ☐ Para toda extensión ciclotómica no trivial $E/\mathbb{Q}$ se tiene $[E : E \cap \mathbb{R}] = 2$. (Ref.: 4163q_021)

(22) ☐ El grupo de Galois, sobre $\mathbb{Q}$, del polinomio $X^{36}-1$ es isomorfo a $C_4 \times C_3$. (Ref.: 4163q_022)

(23) ☐ Sea p un entero primo positivo; si ξ es una raíz p^t–ésima primitiva de la unidad en $\mathbb{F}_p$, entonces $\xi \in \mathbb{F}_p$. (Ref.: 4163q_023)

(24) ☐ Si p es un entero primo positivo y $\xi \in \mathbb{F}_{p^t}$, entonces ξ es una raíz p^t–ésima de la unidad. (Ref.: 4163q_024)

(25) ☐ Sea p un entero primo positivo; todo elemento de $\mathbb{F}_{p^t}$ es una raíz de la unidad. (Ref.: 4163q_025)

(26) ☐ El grupo de Galois $\mathrm{Gal}(X^{27}-1/\mathbb{Q})$ es isomorfo a C_{18}. (Ref.: 4163q_026)

(27) ☐ El grupo de Galois $\mathrm{Gal}(X^{27}-1/\mathbb{Q})$ es isomorfo al cíclico C_{26}. (Ref.: 4163q_027)

(28) ☐ Si p es un entero primo positivo, toda extensión finita $F/\mathbb{F}_p$ es normal. (Ref.: 4163q_028)

(29) ☐ Si p es un entero positivo y K es un cuerpo de característica p, toda extensión finita F/K es de Galois. (Ref.: 4163q_029)

(30) ☐ Sea p un entero primo positivo, y K un cuerpo de característica p. Si F_1/K y F_2/K son extensiones finitas del mismo grado, ¿existe un isomorfismo $F_1/K \cong F_2/K$ sobre K. (Ref.: 4163q_030)

(31) ☐ Si $f \in \mathbb{Q}[X]$ es un polinomio irreducible de grado p, siendo p un entero primo positivo, entonces $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathbb{Z}_p$. (Ref.: 4163q_031)

(32) ☐ Si $X^4-a \in \mathbb{Q}[X]$ es un polinomio irreducible, entonces $\mathrm{Gal}(X^4-a/\mathbb{Q}) \cong D_4$. (Ref.: 4163q_032)

(33) ☐ Si p un entero primo positivo impar, y ξ_{2p} es una raíz $2p$–ésima primitiva de la unidad, entonces $[\mathbb{Q}(\xi_{2p}) : \mathbb{Q}] = 2p-1$. (Ref.: 4163q_033)

(34) ☐ Si $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\xi)$ es una torre de cuerpos y ξ una raíz de la unidad, entonces $K/\mathbb{Q}$ es una extensión de Galois. (Ref.: 4163q_034)

(35) ☐ Sea p un entero primo positivo; todo elemento no nulo de $\mathbb{F}_{p^t}$ es una raíz de la unidad. (Ref.: 4163q_035)

(36) ☐ Si E/K es una extensión de Galois soluble y $K \subseteq F \subseteq E$ es un cuerpo intermedio, entonces F/K es una extension de Galois soluble. (Ref.: 4163q_036)

(37) ☐ Si ξ_n es una raíz n–ésima primitiva de la unidad, se tiene $\mathbb{Q}(\xi_{12}) \cap \mathbb{Q}(\xi_{18}) = \mathbb{Q}(\xi_6)$. (Ref.: 4163q_037)

(38) ☐ Si ξ_n es una raíz n–ésima primitiva de la unidad, se tiene $\mathbb{Q}(\xi_{12}) \cap \mathbb{Q}(\xi_{18}) = \mathbb{Q}(\xi_{12})$. (Ref.: 4163q_038)

(39) ☐ Para todas extensión simple $K(\alpha)/K$, que es de Galois, se tiene que $\mathrm{Gal}(K(\alpha)/K)$ es un grupo simple. (Ref.: 4163q_039)

(40) ☐ El grupo de Galois de la extensión $\mathbb{F}_{p^t}/\mathbb{F}_{p^s}$, con $s|t$, es un grupo cíclico de orden $\frac{t}{s}$. (Ref.: 4163q_040)

(41) ☐ El grupo de Galois de la extensión $\mathbb{F}_{p^4}/\mathbb{F}_{p^2}$ está generado por φ, el automorfismo de Frobenius $\varphi : \mathbb{F}_{p^4} \longrightarrow \mathbb{F}_{p^4}$, definido $\varphi(x) = x^p$ para cada $x \in \mathbb{F}_{p^4}$. (Ref.: 4163q_041)

(42) ☐ El grupo de Galois de la extensión $\mathbb{F}_{p^4}/\mathbb{F}_p$ está generado por φ, el automorfismo $\varphi : \mathbb{F}_{p^4} \longrightarrow \mathbb{F}_p$, definido $\varphi(x) = x^{p^4}$ para cada $x \in \mathbb{F}_{p^4}$. (Ref.: 4163q_042)

(43) ☐ Para todo cuerpo finito $\mathbb{F}$ de característica p y cada extensión finita $L/\mathbb{F}$, el grado $[L : \mathbb{F}]$ es necesariamente una potencia de p. (Ref.: 4163q_043)

(44) ☐ El grupo de Galois del polinomio ciclotómico ϕ_n sobre $\mathbb{Q}$ es siempre un grupo cíclico de orden $\varphi(n)$. (Ref.: 4163q_044)

(45) ☐ Cada raíz en $\mathbb{C}$ de $\phi_n(X)$ es una raíz n–ésima primitiva de la unidad. (Ref.: 4163q_054)

(46) ☐ Cada raíz en $\mathbb{C}$ de $X^n - 1$ es una raíz n–ésima primitiva de la unidad. (Ref.: 4163q_055)

(47) ☐ El grupo de Galois del cuerpo de descomposición de $\phi_n(X) \in K[X]$ tiene orden $\varphi(n)$. (Ref.: 4163q_053)

(48) ☐ El grupo de Galois de una extensión finita de un cuerpo finito es un grupo soluble. (Ref.: 4163q_065)

Capítulo IV

Grupo de Galois de un polinomio

Introducción

Introducción.

4164-00.tex

16. Grupo de Galois como grupo de permutaciones

Hasta ahora hemos estudiado las extensiones finitas de cuerpos en términos de su grupo de automorfismos. Vamos ahora a aplicar esta teoría al estudio de las soluciones de una ecuación polinómica. Consideramos a lo largo de este tema un polinomio *separable* $f(X)$ con coeficientes en un cuerpo K; si llamamos E al cuerpo de descomposición de $f(X)$ sobre K, la extension E/K es una extensión de Galois.

Supongamos que las raíces de $f(X)$, en una clausura algebraica $\overline{K}$ de K, son $\alpha_1, \ldots, \alpha_n$, el cuerpo de descomposición de f sobre K es $E = E(f/K) = K(\alpha_1, \ldots, \alpha_n)$. Sea $G = \mathrm{Gal}(E/K)$.

Cada $\sigma \in \mathrm{Gal}(E/K)$ está completamente determinado por su acción sobre $\alpha_1, \ldots, \alpha_n$, que son las raíces de $f(X)$, por eso la imagen de un α_i por σ es otra α_j; en consecuencia, cada $\sigma \in \mathrm{Gal}(E/K)$ define una permutación π_σ de $\{1, \ldots, n\}$ mediante

$$\pi_\sigma(i) = j \text{ tal que } \sigma(\alpha_i) = \alpha_j$$

Lema. 16.1.
Existe un homomorfismo inyectivo de grupos de $\mathrm{Gal}(E/K)$ *al grupo simétrico* S_n.

DEMOSTRACIÓN.

$$\alpha_{\pi_{\sigma\tau}(i)} = \sigma\tau(\alpha_i) = \sigma(\alpha_{\pi_\tau(i)}) = \alpha_{\pi_\sigma \pi_\tau(i)}$$

□

Tenemos que $\mathrm{Gal}(E/K)$ es isomorfo a su imagen en S_n. Vamos a llamar a esta imagen $\mathrm{Gal}(f/K)$. La diferencia entre estos dos grupos es que el primero es un grupo de automorfismos y el segundo es un grupo de permutaciones.

Observación. 16.2.
El grupo $\mathrm{Gal}(f/K)$ no está determinado de manera única por la extensión, sino que depende de la numeración elegida para las raíces: Si cambiamos el orden de las raíces, cambiamos $\mathrm{Gal}(f/K)$ por otro grupo, conjugado suyo dentro de S_n. A pesar de ello, para simplificar la notación normalmente identificamos $\sigma \in \mathrm{Gal}(E/K)$ con su imagen en S_n, y pasamos libremente de $\mathrm{Gal}(E/K)$ a $\mathrm{Gal}(f/K)$ y viceversa. En cada caso el contexto dejará claro si σ es un automorfismo o una permutación. Representamos a ambos grupos por la letra G.

Ejemplo. 16.3.
Sea $K = \mathbb{Q}$, $f(X) = X^4 - 5X^2 + 6 = (X^2 - 2)(X^2 - 3)$. Las raíces de $f(X)$ son:

$$\alpha_1 = \sqrt{2}, \quad \alpha_2 = -\sqrt{2}, \quad \alpha_3 = \sqrt{3}, \quad \alpha_4 = -\sqrt{3}.$$

4164-01.tex

El cuerpo de descomposición de f es $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y el grupo de Galois es $G = \mathrm{Gal}(E/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$, donde

$$\sigma_1(\sqrt{2}) = -\sqrt{2}, \quad \sigma_1(\sqrt{3}) = \sqrt{3},$$
$$\sigma_2(\sqrt{2}) = \sqrt{2}, \quad \sigma_2(\sqrt{3}) = -\sqrt{3}.$$

Entonces $\mathrm{Gal}(f/\mathbb{Q}) = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$. Si hubiésemos escogido otra numeración para las raíces, obtendríamos un grupo distinto, pero conjugado del anterior.

Ejemplo. 16.4.
Sea $K = \mathbb{Q}$ y sea $f(X) = X^3 - 2 \in \mathbb{Q}[X]$. Si α es una raíz de $f(X)$ y ω una raíz cúbica primitiva de la unidad. El cuerpo de descomposición de f es $E = \mathbb{Q}(\alpha, \omega)$. Las raíces de $f(X)$ son $\alpha, \omega\alpha, \omega^2\alpha$ y tenemos $[E : \mathbb{Q}] = 6$.

(1) Cualquier permutación de las raíces define un automorfismo, luego $\mathrm{Gal}(f/K) = S_3$.
(2) Sobre $K = \mathbb{Q}(\omega)$ el grupo es $\mathrm{Gal}(f/\mathbb{Q}(\omega)) = A_3$: en este caso las raíces pueden permutarse de forma cíclica y no de otra manera.
(3) Sobre $\mathbb{Q}(\alpha)$, $\mathrm{Gal}(f/\mathbb{Q}(\alpha))$ es cíclico de orden 2: α debe permanecer fija, y podemos intercambiar $\omega\alpha$ y $\omega^2\alpha$.

El primer problema a estudiar es cómo calcular el grupo de Galois de un polinomio. Vamos a obtener propiedades del polinomio $f(X)$ a partir de su grupo de Galois $\mathrm{Gal}(f/K)$, y a la inversa, restricciones para posibles valores del grupo de Galois a partir de propiedades del polinomio.

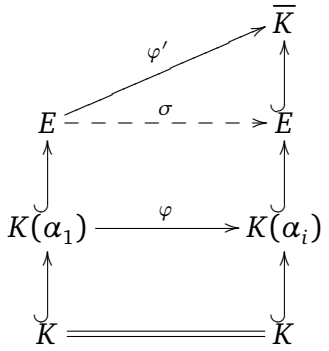
Proposición. 16.5.
Sea $f(X) \in K[X]$ un polinomio de grado n, sin raíces múltiples, y sea $G = \mathrm{Gal}(f/K)$ su grupo de Galois, son equivalentes las siguientes afirmaciones:

(a) $f(X)$ es irreducible;
(b) $\mathrm{Gal}(f/K) \subseteq S_n$ es un subgrupo transitivo.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Supongamos que $E = K(\alpha_1, \ldots, \alpha_n)$ es el cuerpo de descomposición de $f(X)$, cuyas raíces son $\alpha_1, \ldots, \alpha_n$. Dadas dos raíces distintas, por ejemplo α_1 y α_i, existe un isomorfismo

$$\varphi : K(\alpha_1) \xrightarrow{\cong} K(\alpha_i)$$

que induce un homomorfismo φ'



Como E es una extensión normal de K, entonces φ' se factoriza por E, produciendo un automorfismo $\sigma \in \mathrm{Gal}(E/K)$. Es claro que $\sigma(\alpha_1) = \alpha_i$.
(b) $\Rightarrow$ (a). Si G es un subgrupo transitivo de S_n, sea α una raíz de un factor irreducible $g(X)$ de $f(X)$. En caso de ser $g(X)$ un factor propio, existe una raíz β de $f(X)$ que no es raíz de $g(X)$; por hipótesis existe $\sigma \in \mathrm{Gal}(f/K)$ tal que $\sigma(\alpha) = \beta$, obteniéndose que β es una raíz de $g(X)$, lo que es una contradicción. □

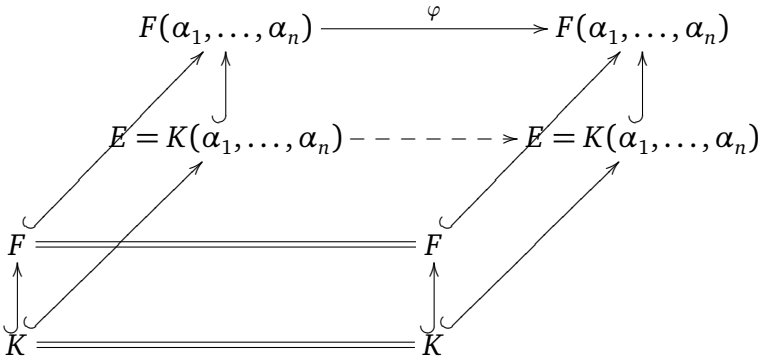
Corolario. 16.6.
Sea $f(X) \in K[X]$ sin raíces múltiples. Sea $f(X) = f_1 \cdots f_r$ la factorización en irreducibles sobre K. Dos ceros α_i, α_j de $f(X)$ son raíces del mismo f_k si, y sólo si, i, j están en la misma órbita bajo $G = \mathrm{Gal}(f/K)$

DEMOSTRACIÓN. Supongamos que i, j están en la misma órbita. Entonces existe $\sigma \in G$ tal que $\sigma(\alpha_i) = \alpha_j$. Luego α_i, α_j son conjugados y por tanto son raíces del mismo polinomio irreducible.
Sean ahora α_i, α_j raíces del mismo polinomio irreducible. Entonces son conjugados. Luego existe $\sigma \in G$ tal que $\sigma(\alpha_i) = \alpha_j$ y $j = \sigma(i)$ está en la órbita que i. □

Sea $f(X) \in K[X]$ un polinomio separable, si F/K es una extensión de cuerpos, entonces el polinomio $f(X)$ es también separable sobre F y tenemos una extensión de Galois $F(\alpha_1, \ldots, \alpha_n)/F$. De cara a relacionar los dos grupos de Galois $\mathrm{Gal}(f/K)$ y $\mathrm{Gal}(f/F)$ tenemos:

Proposición. 16.7. (Teorema de los irracionales naturales)
En la situación anterior, existe un homomorfismo inyectivo de grupos $\mathrm{Gal}(f/F) \hookrightarrow \mathrm{Gal}(f/K)$.

DEMOSTRACIÓN. Consideramos una clausura algebraica $\overline{F}$ de F y supongamos que las raíces α_1, $\ldots$, α_n pertenecen a $\overline{F}$, entonces podemos construir el siguiente diagrama conmutativo, donde $E = K(\alpha_1, \ldots, \alpha_n)$



Dado $\varphi \in \mathrm{Gal}(F(\alpha_1,\ldots,\alpha_n)/F)$, como φ aplica cada α_i en otro α_j, entonces $\varphi(E) \subseteq E$ y por tanto $\varphi_{|E} \in \mathrm{Gal}(E/K)$. Es claro que la aplicación $\varphi \mapsto \varphi_{|E}$ es inyectiva y es un homomorfismo de grupos. □

Corolario. 16.8.
Si $\mathrm{Gal}(f/K)$ *es un grupo simple, para cada extensión* F/K *tenemos que* $\mathrm{Gal}(f/F) = \mathrm{Gal}(f/K)$ *ó es trivial.*

Podemos aplicar este resultado en el caso en el que $\mathrm{Gal}(f/K)$ tiene orden un número primo.

Dentro de los subgrupos de $\mathrm{Gal}(f/K)$ tenemos el subgrupo $\mathrm{Gal}(f/K)\cap A_n$; este subgrupo es de índice, como máximo, dos, por lo tanto es siempre normal. Estamos interesados en calcular el subcuerpo fijo asociado a este subgrupo. Para este fin vamos a recordar la definición de discriminante de un polinomio $f(X)$.

$$\mathrm{Discr}(f(X)) = \prod_{i<j}(\alpha_i-\alpha_j)^2 = \prod_{i\neq j}(-1)^{\frac{n^2-n}{2}}(\alpha_i-\alpha_j),$$

y por tanto, para cada permutación $\pi \in S_n$ tenemos que $\mathrm{Discr}(f(X))$ queda invariante. Como consecuencia $\mathrm{Discr}(f(X))$ es invariante ante los elementos de $\mathrm{Gal}(f/K)$, esto es, $\mathrm{Discr}(f(X)) \in K$. En cambio, si consideramos Δ, la raíz cuadrada de $\mathrm{Discr}(f(X))$,

$$\Delta = \prod_{i<j}(\alpha_i-\alpha_j),$$

veamos que Δ queda fijo ante todo automorfismo en $\mathrm{Gal}(f/K)\cap A_n$.

Teorema. 16.9.
Si $f(X)$ *es un polinomio que no tiene raíces múltiples y* K *es un cuerpo de característica distinta de 2, entonces* $K(\Delta)$ *es el cuerpo fijo asociado a* $\mathrm{Gal}(f/K)\cap A_n$*, o equivalentemente* $\mathrm{Gal}(f/K)\cap A_n = \mathrm{Gal}(f/K(\Delta))$

DEMOSTRACIÓN. Llamamos $G^+ = \mathrm{Gal}(f/K)\cap A_n$ y $F = E^{G^+}$. Para cada $\sigma \in \mathrm{Gal}(f/K)\cap A_n$ tenemos que $\sigma(\Delta) = \Delta$, ya que el número de cambios $\alpha_i-\alpha_j \mapsto \alpha_j-\alpha_i$ es par por lo que no varía el signo del producto. En consecuencia $\Delta \in F$ y por tanto $K(\Delta) \subseteq F$. Si se verifica $[F:K] = (G:G^+) = 1$, entonces $F = K(\Delta) = K$ y tenemos el resultado. En cambio, si $[F:K] = (G:G^+) = 2$, entonces existe una permutación impar $\sigma \in G$ que debe verificar $\sigma(\Delta) = -\Delta$, por lo tanto $\Delta \in K(\Delta)\setminus K$, y tenemos $K(\Delta) = F$. □

Corolario. 16.10.
En la situación anterior, el grupo de Galois de $f(X)$ está incluido en A_n si, y sólo si, $\mathrm{Discr}(f(X))$ *es un cuadrado en K.*

DEMOSTRACIÓN. Si el grupo de Galois de $f(X)$ está incluido en A_n, entonces $G^+ = G$ y tenemos $\Delta \in K$, luego $\mathrm{Discr}(f(X)) = \Delta^2$ es un cuadrado en K. Por otro lado, si $\mathrm{Discr}(f(X))$ es un cuadrado en K, entonces $\Delta \in K$ y por tanto $G^+ = G$, luego $G \subseteq A_n$. □

16.1. Ejercicios

Grupo de Galois como grupo de permutaciones

Ejercicio. 16.11.
Sea K un cuerpo de característica distinta de 2 en el que -1 es un cuadrado. Sea $d \in K$ tal que $\sqrt{d} \notin K$. Demuestra que $\sqrt{d}$ no es cuadrado en $K(\sqrt{d})$.
Ref.: 4164e_030 SOLUCIÓN

Ejercicio. 16.12.
Prueba que $K = \mathbb{Q}(i\sqrt[3]{2}, \sqrt[4]{3})$ es una extensión de Galois de $\mathbb{Q}$.
Ref.: 4164e_019 SOLUCIÓN

Ejercicio. 16.13.
En la Proposición (8.11.) tenemos que si E/K es una extensión finita de Galois, para cada extensión finita F/K se verifica $[EF : K] = \dfrac{[E : K][F : K]}{[E : E \cap F]}$. Da un ejemplo en el que se pruebe que la condición de Galois es necesaria.
Ref.: 4164e_023 SOLUCIÓN

Cúbicas

Ejercicio. 16.14.
Sea K un cuerpo de característica distinta de 2 y $f(X) \in K[X]$ una cúbica con discriminante un cuadrado en K. Demuestra que $f(X)$ ó es irreducible ó se descompone completamenteen K.
Ref.: 4164e_031 SOLUCIÓN

Ejercicio. 16.15.
Demuestra que sobre cualquier cuerpo K, el polinomio X^3-3X+1 es irreducible o descompone completamente.
Ref.: 4164e_006 SOLUCIÓN

Ejercicio. 16.16.
Sea $K\subseteq\mathbb{R}$ y $f(X)\in K[X]$ una cúbica irreducible con discriminante $\Delta^2=\mathrm{Discr}(f(X))$. Demuestra que

(1) Si $f(X)$ tiene tres raíces reales, entonces $\mathrm{Discr}(f(X))>0$.
(2) Si $f(X)$ tiene exactamente una raíz real, entonces $\mathrm{Discr}(f(X))<0$.

El recíproco de este resultado es también cierto ya que una cúbica tiene o una o tres raíces reales y su discriminante o es positivo o es negativo.
En el caso de $K=\mathbb{Q}$ tenemos entonces que si $f(X)$ tiene exactamente una raíz real, entonces $\mathrm{Gal}(f/\mathbb{Q})=S_3$. Por el contrario, si f tiene tres raíces reales, puede ser que $\Delta\in\mathbb{Q}$, y por tanto $\mathrm{Gal}(f/\mathbb{Q})=A_3$ ó $\Delta\notin\mathbb{Q}$, y se tiene $\mathrm{Gal}(f/\mathbb{Q})=S_3$.
Los siguientes ejemplos ilustran los casos posibles:

$f(X)$	$\mathrm{Discr}(f(X))$	$\sqrt{\mathrm{Discr}(f(X))}\in\mathbb{Q}$	$\mathrm{Gal}(f/\mathbb{Q})$
X^3-3X+3	-135	*NO*	S_3, *una sola raíz real*
X^3-5X+3	257	*NO*	S_3, *tres raíces reales*
X^3-3X+1	81	*SI*	A_3, *tres raíces reales*

Ref.: 4164e_008 SOLUCIÓN

Ejercicio. 16.17.
Calcula

(1) $\mathrm{Gal}(X^3-X-1)$ *sobre* $\mathbb{Q}$ *y sobre* $\mathbb{Q}(\sqrt{-23})$.
(2) $\mathrm{Gal}(X^3-10)$ *sobre* $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-3})$ *y* $\mathbb{Q}(\sqrt{2})$.
(3) $\mathrm{Gal}((X^3-2)(X^3-3)(X^2-2))$ *sobre* $\mathbb{Q}(\sqrt{-3})$.
(4) $\mathrm{Gal}((X^3-2)(X^2-3)(X^2-5)(X^2-7))$ *sobre* $\mathbb{Q}$.
(5) $\mathrm{Gal}((X^3-2)(X^2-5))$ *sobre* $\mathbb{Q}$.
(6) $\mathrm{Gal}((X^3-2)(X^2+3))$ *sobre* $\mathbb{Q}$.

Ref.: 4164e_032 SOLUCIÓN

Ejercicio. 16.18.
Sea K un cuerpo finito de característica $\neq 2$ y $f = X^3 + pX + q \in K[X]$ un polinomio irreducible. Demuestra que $-4p^3 - 27q^2$ es un cuadrado en K.
Ref.: 4164e_005 SOLUCIÓN

Ejercicio. 16.19.
Sea α una raíz del polinomio $X^3 + 2X + 1 \in \mathbb{Q}[X]$. Si $K = \mathbb{Q}(\alpha)$, ¿tiene el polinomio $X^3 + X + 1$ una raíz en K?
Ref.: 4164e_028 SOLUCIÓN

Ejercicio. 16.20.
Sea $f(X) \in K[X]$ un polinomio irreducible separable de grado 3 con grupo de Galois S_3 sobre K y raíces $\alpha_1, \alpha_2, \alpha_3 \in F$, siendo F el cuerpo de descomposición de $f(X)$ sobre K. Prueba que los cuerpos intermedios entre K y F son K, $K(\alpha_1)$, $K(\alpha_2)$, $K(\alpha_3)$, $K(\Delta)$, F.
Ref.: 4164e_033 SOLUCIÓN

Cuárticas

Ejercicio. 16.21.
Calcula

(1) $\mathrm{Gal}(X^4 - 5)$ *sobre* $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{5}, i)$, $\mathbb{Q}(i)$.
(2) $\mathrm{Gal}(X^4 + 3X^3 + 3X - 2)$ *sobre* $\mathbb{Q}$.
(3) $\mathrm{Gal}(X^4 + 2X^2 + X + 3)$ *sobre* $\mathbb{Q}$.
(4) $\mathrm{Gal}(X^4 - a)$ *sobre* $\mathbb{Q}$ *con* $a \in \mathbb{Z}$, $a \neq 0, \pm 1$ *y libre de cuadrados.*
(5) $\mathrm{Gal}(X^4 + 2)$ *sobre* $\mathbb{Q}$, $\mathbb{Q}(i)$.

(6) $\mathrm{Gal}(X^4-t)$ *sobre* $\mathbb{C}(t)$, $\mathbb{R}(t)$ *con* t *un elemento transcendente.*
(7) $\mathrm{Gal}(X^4-3X^2+4)$ *sobre* $\mathbb{Q}$.
(8) $\mathrm{Gal}(X^4+5X^2+6)$ *sobre* $\mathbb{Q}$.
(9) $\mathrm{Gal}(X^4+4X^3+6X^2+4X-1)$ *sobre* $\mathbb{Q}$.
(10) $\mathrm{Gal}(X^4-2)(X^2-3)(X^2-5)(X^2-7))$ *sobre* $\mathbb{Q}$.

Ref.: 4164e_001 SOLUCIÓN

Ejercicio. 16.22.
Sea $f(X)$ *una cuártica irreducible y separable sobre un cuerpo* K *y sea* α *una raíz de* f. *Demuestra que no existe ningún cuerpo intermedio entre* K *y* $K(\alpha)$ *si, y sólo si,* $\mathrm{Gal}(f/K)$ *es* S_4 *ó* A_4.
Ref.: 4164e_010 SOLUCIÓN

Ejercicio. 16.23.
Sea $f(X)$ *una cuártica irreducible sobre un cuerpo* $K \subseteq \mathbb{R}$. *Demuestra que si* $f(X)$ *tiene exactamente dos raíces reales entonces* $\mathrm{Gal}(f/K)$ *es* S_4 *ó* A_4.
Ref.: 4164e_011 SOLUCIÓN

Subgrupos transitivos

Ejercicio. 16.24.
Prueba que si $G \subseteq S_n$ *es un subgrupo transitivo, entonces* n *divide a* $|G|$.
Ref.: 4164e_036 SOLUCIÓN

Ejercicio. 16.25.
Prueba que S_n *está generado por el ciclo* $\sigma = (1 \dots n)$ *y la trasposición* $\tau = (12)$.
Ref.: 4164e_037 SOLUCIÓN

Ejercicio. 16.26.
Demuestra que el único subgrupo transitivo de S_n que contiene a una transposición y a un ciclo de orden $n-1$ es S_n.
Ref.: 4164e_003 SOLUCIÓN

Ejercicio. 16.27.
Sea p un entero primo positivo.

(1) Si $G \subseteq S_p$ es un subgrupo (no necesariamente transitivo) que contiene a un elemento de orden p y a una transposición entonces $G = S_p$.
(2) Si p es primo, demuestra que el único subgrupo transitivo de S_p que contiene a una transposición es S_p.

Ref.: 4164e_038 SOLUCIÓN

Ejercicio. 16.28.
Prueba que si $G \subseteq S_n$ es un subgrupo transitivo que está generado por trasposiciones, entonces $G = S_n$.
Ref.: 4164e_039 SOLUCIÓN

Ejercicio. 16.29.
Prueba que si $G \subseteq S_n$ es un subgrupo transitivo y abeliano, entonces $|G| = n$
Ref.: 4164e_040 SOLUCIÓN

Ejercicio. 16.30.
Sea $f \in K[X]$ un polinomio irreducible y separable con cuerpo de descomposición E. Prueba que existe $\varphi \in \mathrm{Gal}(E/K)$ tal que $\varphi(\alpha) \neq \alpha$ para cada raíz α de f.
Ref.: 4164e_041 SOLUCIÓN

Quínticas

Ejercicio. 16.31.
Sea $K \subseteq \mathbb{R}$ y $f(X) \in K[X]$ un polinomio irreducible de grado p primo.

(1) Demuestra que si f tiene exactamente dos raíces no reales, entonces $\mathrm{Gal}(f/K) \cong S_p$.
(2) Calcula el grupo de Galois de $X^5 - 6X + 3$ sobre $\mathbb{Q}$.

Ref.: 4164e_004 SOLUCIÓN

Séxticas

Ejercicio. 16.32.
Encuentra el cuerpo de descomposición F sobre $\mathbb{Q}$ del polinomio $f(X) = X^6 + X^3 + 1$. Demuestra que $\mathrm{Gal}(f/\mathbb{Q})$ es cíclico y que tiene un único subgrupo H de orden tres. Encuentra el cuerpo fijo para H.
Ref.: 4164e_007 SOLUCIÓN

Ejercicio. 16.33.
Consideramos el polinomio $f(X) = X^6 - 2X^3 - 2 \in \mathbb{Q}[X]$, y sea F su cuerpo de descomposición.

(1) Demuestra que f es irreducible sobre $\mathbb{Q}$ y que sus raíces son las tres raíces cúbicas de $1 \pm \sqrt{3}$.
(2) Demuestra que F contiene una raíz cúbica primitiva de la unidad y deduce que contiene a la extensión bicuadrática $L_1 = \mathbb{Q}(i, \sqrt{3})$.
(3) Tomando el producto de dos raíces de f deduce que F contiene a la extensión $L = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})$.
(4) Tomando el cociente de dos raíces reales del polinomio $f(X)$, deduce que los números reales $\sqrt[3]{2+\sqrt{3}}$ y $\sqrt[3]{2-\sqrt{3}}$ están en F. Demuestra que el elemento $\gamma = \sqrt[3]{2+\sqrt{3}} + \sqrt[3]{2-\sqrt{3}} \in F$ es una raíz real de la cúbica $X^3 - 3X - 4$ cuyo discriminante es $-2^2 3^4$ y concluye que la clausura normal de $\mathbb{Q}(\gamma)$ contiene a $\mathbb{Q}(i)$; en particular $\mathbb{Q}(\gamma) \neq \mathbb{Q}(\sqrt[3]{2})$.
(5) Demuestra que $[L : \mathbb{Q}] = 12$ y deduce que $[F : \mathbb{Q}] = 12$ ó 36.
(6) Si suponemos que $[F : \mathbb{Q}] = 12$, demuestra que todo F contiene exactamente tres subextenioens de grado tres sobre $\mathbb{Q}$ lo que es imposible.
(7) Prueba que $F = \mathbb{Q}(\omega, \sqrt[3]{1+\sqrt{3}}, \sqrt[3]{2})$, y describe los elementos de $\mathrm{Gal}(F/\mathbb{Q})$.
(8) Prueba que $G \cong S_3 \times S_3$.

Ref.: 4164e_013 SOLUCIÓN

Ejercicio. 16.34. (Un caso curioso)
Prueba que existen polinomios irreducibles $f(X) \in \mathbb{Q}[X]$ de grado 6 tales que $\mathrm{Gal}(f/\mathbb{Q})$ *es un grupo isomorfo a S_3.*
Ref.: 4164e_017 SOLUCIÓN

Raíces

Ejercicio. 16.35.
Sean α y β raíces de un polinomio irreducible $f(X) \in K[X]$, siendo K un cuerpo perfecto.
(1) Prueba que $[K(\alpha):K] = [K(\beta):K]$.
(2) Prueba que $K(\alpha)/K \cong K(\beta)/K$.
(3) Sea E un cuerpo de descomposición de $f(X)$ sobre K tal que $\alpha, \beta \in E$. ¿Existe siempre un automorfismo $\sigma : E/K \longrightarrow E/K$ tal que $f(\alpha) = \beta$?
(4) ¿Existe siempre $\sigma : E/K \longrightarrow E/K$ tal que $\sigma(\alpha) = \beta$ y $\sigma(\beta) = \alpha$, dejando las demás raíces fijas.
(5) ¿Existe $\sigma : E/K \longrightarrow E/K$, $\sigma \neq id$, tal que $\sigma(\alpha) = \alpha$?

Ref.: 4164e_024 SOLUCIÓN

Ejercicio. 16.36.
Sean α y β raíces de un polinomio irreducible $f(X) \in K[X]$ tal que $\alpha^n \in K$. Prueba que β verifica esta misma relación.
Ref.: 4164e_025 SOLUCIÓN

Ejercicio. 16.37.
Sea K un cuerpo de característica p, y $a \in K$. Prueba que si el polinomio $X^p - a$ no tiene raíces en K, entonces $X^p - a$ es irreducible sobre K.
Ref.: 4164e_026 SOLUCIÓN

Grupo de Galois

Ejercicio. 16.38.
Se consideran $a, b, d \in \mathbb{Z}$ tales que d y $a^2 - db^2$ son libres de cuadrados. Determina el grupo de Galois de la extensión $\mathbb{Q}(\sqrt{a + b\sqrt{d}})/\mathbb{Q}$.
Ref.: 4164e_027 SOLUCIÓN

Ejercicio. 16.39.
Sean $p_1, \ldots, p_t \in \mathbb{Z}$ enteros primos positivos distintos dos a dos. Prueba que se verifica: $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_t})) \cong {\mathbb{Z}_2}^t$.
Ref.: 4164e_018 SOLUCIÓN

Ejercicio. 16.40.
Sea $f(X)$ un polinomio (irreducible) de grado n con grupo de Galois $\mathrm{Gal}(f/\mathbb{Q}) = S_n$. *Si α es una raíz de $f(X)$, y $F = K(\alpha)$, prueba que no existen cuerpos intermedios en la extensión F/K.*
Ver Ejercicio (8.40.).
Ref.: 4164e_021 SOLUCIÓN

Ejercicio. 16.41.
Sea $f(X) \in K[X]$ un polinomio separable y g un factor irreducible de f. ¿Actúa transitivamente $G = \mathrm{Gal}(f/K)$ sobre las raíces de g?
Ref.: 4164e_035 SOLUCIÓN

Ejercicio. 16.42.
Estudia la extensión $\mathbb{Q}(\xi_{37})/\mathbb{Q}$; determina el retículo de subgrupos de $\mathrm{Gal}(\mathbb{Q}(\xi_{37})/\mathbb{Q})$ *y los cuerpos fijos para los subgrupos de orden 2 y 3.*
Ref.: 4164e_051 SOLUCIÓN

Ejercicio. 16.43.
Sea ω una raíz cúbica primitiva de la unidad, y $\xi = \xi_5$ una raíz quinta primitiva de la unidad. Llamamos $E = \mathbb{Q}(\omega, \xi)$.

(1) Prueba que $E/\mathbb{Q}$ es una extensión de Galois, y determina $[E : \mathbb{Q}]$.
(2) Prueba que $\zeta = \omega\xi$ es una raíz décimoquinta primitiva de la unidad, por tanto $E = \mathbb{Q}(\zeta)$.
(3) Determina $G = \mathrm{Gal}(E/\mathbb{Q})$.
(4) Da generadores y relaciones de $G = \mathrm{Gal}(E/\mathbb{Q})$, y una lista de sus elementos.
(5) Da una lista de los subgrupos de G indicando su orden.
(6) ¿Es cierto que $i \in E$?
(7) Tenemos que $\sqrt{-3} \in E$; para demostrar que $\sqrt{5} \in E$, determina el polinomio $\mathrm{Irr}(\xi + \overline{\xi}, \mathbb{Q})$, y prueba que $\mathbb{Q}(\xi + \overline{\xi}) = \mathbb{Q}(\sqrt{5})$.
(8) Si llamamos $\alpha = \xi + \overline{\xi}$, tenemos una torre de cuerpos: $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\xi) \subseteq \mathbb{Q}(\zeta)$ en la que cada extensión es de grado dos. Ya conocemos $\mathrm{Irr}(\alpha, \mathbb{Q})$; determina $\mathrm{Irr}(\xi, \mathbb{Q}(\alpha))$.
(9) Utilizando los apartados anteriores, da una expresión por radicales (de elementos de $\mathbb{Q}$) de ξ.
(10) Para cada subgrupo H de G de orden cuatro determina el cuerpo fijo E^H.

Ref.: 4164e_052 *SOLUCIÓN*

17. Cálculo del grupo de Galois

Vamos a trabajar sobre un cuerpo K de característica distinta de 2 y a utilizar polinomios separables sobre K que no tienen raíces múltiples.

Ecuaciones cuadráticas

Sea $f(X) = X^2 + a_1X + a_0$, su discriminante es $\Delta^2 = a_1^2 - 4a_0$ entonces se verifica:

$$G_p = \mathrm{Gal}(f/K) = \begin{cases} S_2, & \text{si } a_1^2 - 4a_0 \textbf{ no} \text{ es un cuadrado en } K \\ A_2 = \{1\}, & \text{si } a_1^2 - 4a_0 \text{ es un cuadrado en } K \end{cases}$$

En el primer caso, el polinomio es irreducible, y en el segundo es reducible.

Ecuaciones cúbicas

Sea $f(X) = X^3 + a_2X^2 + a_1X + a_0$, su discriminante es

$$\Delta^2 = -4a_2^3a_0 + a_1^2a_2^2 + 18a_0a_1a_2 - 4a_1^3 - 27a_0^2.$$

Puede ocurrir que $f(X)$ sea reducible, en este caso tiene una raíz y por lo tanto existe una factorización $f(X) = (X-\alpha)g(X)$. Como α queda fijo por $\mathrm{Gal}(f/K)$, resulta que $\mathrm{Gal}(f/K) = \mathrm{Gal}(g/K)$ y el problema se reduce al caso cuadrático.
Si el polinomio es irreducible, entonces su grupo de Galois es un subgrupo transitivo de S_3; como únicamente tenemos dos: A_3 y S_3, se verifica:

$$G_p = \mathrm{Gal}(f/K) = \begin{cases} S_3, & \text{si } \Delta^2 \textbf{ no} \text{ es un cuadrado en } K \\ A_3, & \text{si } \Delta^2 \text{ es un cuadrado en } K \end{cases}$$

Ecuaciones cuárticas

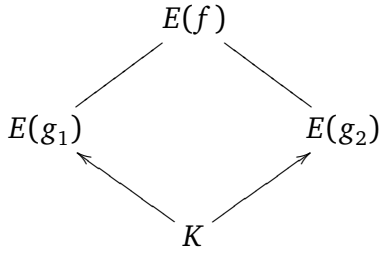
Sea $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$, su discriminante es

$$\begin{aligned} \Delta^2 = &-4a_3^3a_1^3 - 128a_2^2a_0^2 + 16a_2^4a_0 - 4a_2^3a_1^2 - 27a_3^4a_0^2 + 256a_0^3 - 27a_1^4 - 6a_3^2a_1^2a_0 \\ &-192a_3a_1a_0^2 + 18a_3a_1^3a_2 + 144a_2a_3^2a_0^2 + a_2^2a_3^2a_1^2 - 4a_2^3a_3^2a_0 + 144a_0a_1^2a_2 \\ &-80a_3a_1a_2^2a_0 + 18a_3^3a_1a_2a_0. \end{aligned}$$

Puede ocurrir que $f(X)$ sea reducible. Se presentan dos casos:

4164-02.tex

Caso 1. $f(X)$ tiene una raíz, en este caso $f(X) = (X-\alpha)g(X)$, y como α queda fijo por $\mathrm{Gal}(f/K)$, resulta que $\mathrm{Gal}(f/K) = \mathrm{Gal}(g/K)$ y el problema se reduce al caso cúbico.
Caso 2. Si $f(X) = g_1(X)g_2(X)$, con $g_i(X)$ irreducibles de grado dos, tenemos la siguiente situación

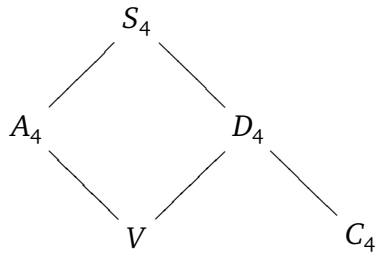


Como $E(g_1)/K$ y $E(g_2)/K$ son extensiones normales, los grupos $\mathrm{Gal}(f/E(g_1))$ y $\mathrm{Gal}(f/E(g_2))$ son subgrupos normales de $\mathrm{Gal}(f/K)$.
Tenemos que $\mathrm{Gal}(f/K)$ es un subgrupo del grupo $\langle(1\,2),(3\,4)\rangle$. Para ver qué grupo es estudiamos los discriminantes de g_1 y g_2, en efecto tenemos:

$$\langle(1\,2),(3\,4)\rangle \text{ si, y sólo si, } \sqrt{\mathrm{Discr}(g_1)\,\mathrm{Discr}(g_2)} \notin K.$$
$$\langle(1\,2)(3\,4)\rangle \text{ si, y sólo si, } \sqrt{\mathrm{Discr}(g_1)\,\mathrm{Discr}(g_2)} \in K.$$

Si el polinomio es irreducible, entonces su grupo de Galois es un subgrupo transitivo de S_4. En este caso tenemos cinco tipos de subgrupos transitivos:

S_4,	normal en S_4.
A_4,	normal en S_4.
$V = \{1,(12)(34),(13)(24),(14)(23)\}$,	normal en S_4.
$C_4 = \{1,(1234),(13)(24),(1432)\} \cong C_4$,	y sus conjugados en S_4.
$D_4 = V \cup \{(12),(34),(1423),(1324)\} \cong D_4$,	y sus conjugados en S_4.



Podemos suponer $C_4 = \langle(1\,2\,3\,4)\rangle$, $D_4 = \langle(1\,2\,3\,4),(1\,4)\rangle$, $V = \langle(1\,2)(3\,4),(1\,3)(2\,4)\rangle$. Observamos que cuatro de estos tipos contienen al subgrupo V; estudiamos entonces el comportamiento de $\mathrm{Gal}(f/K)$ con respecto a V de la siguiente forma.
Llamamos

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4,$$
$$\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4,$$
$$\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Estos elementos quedan fijos por V y a la inversa, si una permutación deja fijos a todos los β_i, entonces esta permutación pertenece a V.

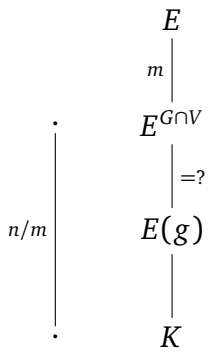
Definimos un nuevo polinomio, la **resolvente cúbica** de $f(X)$,

$$g(X) = (X-\beta_1)(X-\beta_2)(X-\beta_3).$$

Es posible expresar los coeficientes de $g(X)$ en términos de los coeficientes de $f(X)$, ya que son polinomios simétricos en las raíces de $f(X)$. En nuestro caso si $g(X) = X^3 + b_2X^2 + b_1X + b_0$, resulta

$$\begin{cases} b_2 = -a_2 \\ b_1 = a_1a_3 - 4a_0 \\ b_0 = -a_3^2a_0 + 4a_2a_0 - a_1^2 \end{cases}$$

Se verifica pues $\mathrm{Gal}(f/E(g)) = \mathrm{Gal}(f/K) \cap V$. En efecto, si llamamos $G = \mathrm{Gal}(f/K)$, se tiene



en donde $m = |G \cap V|$ y $|G| = n$. Entonces $[E^{G\cap V} : K] = n/m$. Si consideramos el elemento $\beta_1 - \beta_2$ y la acción de S_4 sobre él, su órbita es:

$$\beta_1-\beta_2,\ (1\,2\,3)(\beta_1-\beta_2),\ (1\,3\,2)(\beta_1-\beta_2),\ (1\,2)(\beta_1-\beta_2),\ (1\,3)(\beta_1-\beta_2),\ (2\,3)(\beta_1-\beta_2).$$

En este caso

$$\{1, (1\,2\,3), (1\,3\,2), (1\,2), (1\,3), (2\,3)\}$$

es un conjunto de representantes de clases a la izquierda de V en S_4. Tenemos

- $\mathrm{Stab}_{S_4}(\beta_1-\beta_2) = V$, entonces $\mathrm{Stab}_G(\beta_1-\beta_2) = G \cap V$.
- La órbita de $\beta_1-\beta_2$ tiene $|\mathrm{Orb}_G(\beta_1-\beta_2)| = [G : \mathrm{Stab}_G(\beta_1-\beta_2)] = [G : G\cap V]$ elementos.
- $\beta_1-\beta_2$ tiene $[G : G\cap V]$ conjugados, y $[E^{G\cap V} : K] \geq [E(g) : K] \geq [G : G\cap V] = [E^{G\cap V} : K]$.

De aquí se deduce que $E^{G\cap V} = E(g)$, y por lo tanto $G \cap V = \mathrm{Gal}(f/E(g))$.
En consecuencia, tenemos los isomorfismos:

$$\mathrm{Gal}(E(g)/K) \cong \frac{\mathrm{Gal}(E/K)}{\mathrm{Gal}(E/E(g))} \cong \frac{\mathrm{Gal}(f/K)}{\mathrm{Gal}(f/K)\cap V} \cong \frac{G}{G\cap V}. \tag{IV.1}$$

Resulta que $g(X)$ y $f(X)$ tienen el mismo discriminante, lo que nos permite determinar fácilmente el grupo de Galois de $g(X)$, y a partir de éste calcular el grupo de Galois de $f(X)$.
Podemos entonces enunciar y demostrar el siguiente resultado.

Teorema. 17.1.
Sea $f(X)$ un polinomio irreducible de grado 4 con resolvente cúbica $g(X)$. Se verifica
(1) Si $g(X)$ es irreducible y Δ^2 no es un cuadrado en K, entonces $\mathrm{Gal}(g/K) = S_3$, y $\mathrm{Gal}(f/K) \cong S_4$;
(2) Si $g(X)$ es irreducible y Δ^2 es un cuadrado en K, entonces $\mathrm{Gal}(g/K) = A_3$, y $\mathrm{Gal}(f/K) \cong A_4$;
(3) Si $g(X)$ tiene tres raíces en K, entonces $\mathrm{Gal}(g/K) = 1$, y $\mathrm{Gal}(f/K) \cong V$;
(4) Si $g(X)$ tiene una única raíz en K, entonces $\mathrm{Gal}(g/K) \cong C_2$, y $\mathrm{Gal}(f/K)$ es isomorfo a C_4 ó a D_4.

DEMOSTRACIÓN. Del isomorfismo (IV.1) obtenemos la igualdad siguiente:

$$|\mathrm{Gal}(f/K)| = |\mathrm{Gal}(g/K)| \cdot |\mathrm{Gal}(f/K) \cap V| \tag{IV.2}$$

(1). Tenemos $\mathrm{Gal}(g/K) \cong S_3$, entonces de (IV.2) se deduce que $|\mathrm{Gal}(f/K)|$ es un múltiplo de 6, y por tanto $\mathrm{Gal}(f/K) \cong S_4$ ó A_4. Si $\mathrm{Gal}(f/K) = A_4$, entonces $\mathrm{Gal}(f/K) \cap V = V$ y tenemos

$$|\mathrm{Gal}(f/K)| = |\mathrm{Gal}(g/K)| \cdot |\mathrm{Gal}(f/K) \cap V| = 6 \times 4 = 24.$$

(2). Tenemos $\mathrm{Gal}(g/K) \cong A_3$, entonces de (IV.2) obtenemos que $|\mathrm{Gal}(f/K)|$ es un múltiplo de 3, y por tanto $\mathrm{Gal}(f/K) \cong S_4$ ó A_4. Pero como

$$|\mathrm{Gal}(f/K)| = |\mathrm{Gal}(g/K)| \cdot |\mathrm{Gal}(f/K) \cap V| \leq 3 \times 4 = 12$$

se obtiene $\mathrm{Gal}(f/K) = A_4$.
(3). Tenemos $\mathrm{Gal}(g/K) = \{1\}$, entonces de (IV.2) obtenemos $\mathrm{Gal}(f/K) \subseteq V$, y por tanto $\mathrm{Gal}(f/K) = V$.
(4). Tenemos $\mathrm{Gal}(g/K) \cong C_2$, y por tanto $\mathrm{Gal}(f/K)$ tiene orden 2 $|\mathrm{Gal}(f/K) \cap V|$. Los posibles valores para $|\mathrm{Gal}(f/K) \cap V|$ son 2 ó 4, siendo entonces $|\mathrm{Gal}(f/K)|$ igual a 4 u 8. Vamos a buscar un criterio que permita discernir cual es el caso en cada ocasión. Tenemos en este caso que $E(g) = K(\sqrt{\mathrm{Discr}(f)})$.
Si $\mathrm{Gal}(f/K) \cong C_4$, entonces $|\mathrm{Gal}(f/E(g))| = |\mathrm{Gal}(f/K) \cap V| = 2$ y por tanto $[E : E(g)] = 2$, lo que implica que $f(X)$ es reducible en $E(g)$.
Si $\mathrm{Gal}(f/K) \cong D_4$, entonces $|\mathrm{Gal}(f/E(g))| = |\mathrm{Gal}(f/K) \cap V| = 4$ y por tanto $\mathrm{Gal}(f/K) \cap V = V$; como V actúa transitivamente sobre las raíces, resulta que $\mathrm{Gal}(f/E(g))$ actúa transitivamente sobre las raíces de f, y por tanto $f(X)$ es irreducible sobre $E(g)$. □

Vamos a buscar un criterio sencillo para discriminar entre los grupos D_4 y C_4.

Proposición. 17.2.
Sea $f(X) \in K[X]$ un polinomio irreducible con resolvente cúbica $g(X)$ y $\mathrm{Gal}(g/K) = C_2$. Si $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, es la única raíz de g que hay en K, son equivalentes:

(a) $\mathrm{Gal}(f/K) = C_4$.
(b) $\alpha_1+\alpha_3, \alpha_1\alpha_3, \alpha_2+\alpha_4, \alpha_2\alpha_4 \in K(\sqrt{\mathrm{Discr}(f)})$.
(c) *El polinomio* $h = (X^2+a_3X+(a_2-\beta_2))(X^2-\beta_2X+a_0)$ *tiene todas sus raíces en* $K(\sqrt{\mathrm{Discr}(f)})$.
(d) $\sqrt{a_3^2-4(a_2-\beta_2)}, \sqrt{\beta_2^2-4a_0} \in K(\sqrt{\mathrm{Discr}(f)})$.

DEMOSTRACIÓN. Estudiamos el comportamiento del elemento (13)(24). Construimos el polinomio

$$(X-(\alpha_1+\alpha_3))\big(X-(\alpha_2+\alpha_4)\big)(X-\alpha_1\alpha_3)\big(X-\alpha_2\alpha_4\big).$$

Observa que para cualquier cuerpo $F \supseteq K$ se tiene: $\mathrm{Gal}(f/F) \subset \langle (1\,3)(2\,4)\rangle$ si, y sólo si, las cuatro raíces de este polinomio están en F. Calculando los coeficientes de los productos de los dos primeros factores y los dos últimos, nos queda que es precisamente el polinomio h del enunciado. Finalmente, los dos factores cuadráticos formados tienen sus coeficientes en K y descompondrán en factores lineales en F si, y sólo si, las raíces cuadradas de sus discriminantes pertenecen a F. □

Ejemplo. 17.3.
Cálculo del grupo de Galois de polinomios bicuadráticos. Sea $f(X) = X^4+aX^2+b \in K[X]$ irreducible sobre K. Tenemos:

(1) Resolvente cúbica: $g(X) = X^3-aX^2-4bX+4ab = (X-a)(X^2-4b)$
(2) $K(\sqrt{\mathrm{Discr}(f)}) = K(\sqrt{b})$.

Entonces $\mathrm{Gal}(f/K) = V$ si, y sólo si, $\mathrm{Gal}(g/K) = \{1\}$, si, y sólo si, $\sqrt{b} \in K$. En otro caso, $\mathrm{Gal}(g/K) = C_2$; en la Proposición (17.2.) los dos elementos del último apartado son:

$$\sqrt{0-4(a-a)} = 0, \qquad \sqrt{a^2-4b}$$

El primer elemento siempre pertenece a K, y el segundo nunca pertenece a K, porque en otro caso $f(X)$ sería reducible. Luego $\sqrt{a^2-4b} \in K(\sqrt{b})$ si, y sólo si, $\sqrt{b(a^2-4b)} \in K$. En resumen:

$$\begin{cases} \sqrt{b} \in K \Rightarrow & \mathrm{Gal}(f/K) = V, \\ \sqrt{b} \notin K \begin{cases} \sqrt{b(a^2-4b)} \in K \Rightarrow & \mathrm{Gal}(f/K) = C_4, \\ \sqrt{b(a^2-4b)} \notin K \Rightarrow & \mathrm{Gal}(f/K) = D_4. \end{cases} \end{cases}$$

Ejemplo. 17.4.
Cálculo del grupo de Galois de los polinomios recíprocos. Sea $f(X) = X^4+aX^3+bX^2+aX+1 \in K[X]$ irreducible sobre K. Tenemos:

(1) Resolvente cúbica: $g(X) = X^3-bX^2+(a^2-4)X+(-2a^2+4b) = (X-2)(X^2+(2-b)X+(a^2-2b)$.
(2) El discriminante del segundo factor es: $(2-b)^2-4(a^2-2b) = (2+b)^2-4a^2 = (2+b+2a)(2+b-2a)$.

(3) Los discriminantes cuadráticos de la Proposición (17.2.) son: $a^2-4(b-2)=a^2-4b+8$ y $2^2-4=0$.

Análogamente al ejemplo anterior, el segundo elemento siempre pertenece a K y la raíz cuadrada del primero nunca pertenece a K porque en otro caso $f(X)$ sería reducible con factorización:

$$f(X)=\left(X^2+\frac{a+\sqrt{a^2-4(b-2)}}{2}X+1\right)\left(X^2+\frac{a-\sqrt{a^2-4(b-2)}}{2}X+1\right).$$

Finalmente, analizamos qué ocurre cuando $\sqrt{a^2-4(b-2)}\in K(\sqrt{(2+b)^2-4a^2})$; en este caso tenemos: $\sqrt{(a^2-4(b-2))((2+b)^2-4a^2)}\in K$. Observa que si $\alpha,\beta\in K$, y $\sqrt{\alpha}\in K(\sqrt{\beta})$, existen $a,b\in K$ tales que $\sqrt{\alpha}=a+b\sqrt{\beta}$, y se tiene $\sqrt{\alpha\beta}=(\alpha+b^2\beta-a^2)/2b\in K$. Como consecuencia, los distintos caso son:

$$\begin{cases}\sqrt{(2+b)^2-4a^2}\in K\Rightarrow & \mathrm{Gal}(f/K)=V.\\ \\ \sqrt{(2+b)^2-4a^2}\notin K\begin{cases}\sqrt{(a^2-4(b-2))((2+b)^2-4a^2)}\in K\Rightarrow & \mathrm{Gal}(f/K)=C_4.\\ \\ \sqrt{(a^2-4(b-2))((2+b)^2-4a^2)}\notin K\Rightarrow & \mathrm{Gal}(f/K)=D_4.\end{cases}\end{cases}$$

Aplicación de Mathematica

El siguiente es un método alternativo para determinar el grupo de Galois de un polinomio cuadrático.
Si consideramos un polinomio $f(X)\in K[X]$ de grado 4, para calcular su grupo de Galois procedemos como sigue.
Calculamos la descomposición en irreducibles de $f(X)$.

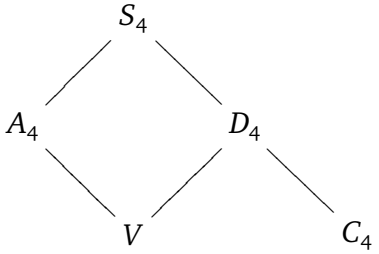
Caso 1. Si $f(X)=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)$, el grupo de Galois es trivial.

Caso 2. Si $f(X)=(X-\alpha_1)(X-\alpha_2)f_1(X)$, el grupo de Galois es C_2.

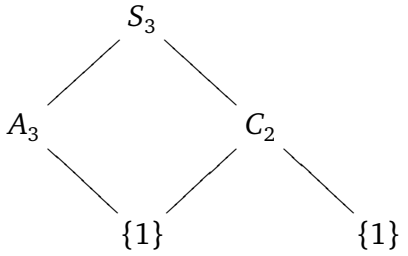
Caso 3. Si $f(X)=(X-\alpha)f_1(X)$, entonces $f_1(X)$ es de grado 3 e irreducible, luego basta calcular el discriminante y comprobar si $\sqrt{\mathrm{Discr}(f_1(X))}\in K$, o equivalentemente $\sqrt{\mathrm{Discr}(f(X))}\in K$.

Caso 4. Si $f(X)=f_1(X)f_2(X)$, ambos de grado 2, el grupo de $f(X)$ es $C_2\times C_2$, si $\sqrt{\mathrm{Discr}(f)}\notin K$ o equivalentemente $\sqrt{\mathrm{Discr}(f_1)\,\mathrm{Discr}(f_2)}\notin K$, y es C_2, si $\sqrt{\mathrm{Discr}(f)}\in K$ o equivalentemente si $\sqrt{\mathrm{Discr}(f_1)\,\mathrm{Discr}(f_2)}\in K$.

Caso 5. $f(X)$ es irreducible, en este caso el grupo de $f(X)$ es un subgrupo transitivo de S_4; es uno de los siguientes:



Tomamos una raíz α_1 de $f(X)$. Al estudiar el polinomio $f(X)$ en $K(\alpha_1)$, su grupo de Galois es uno de los siguientes:



y el polinomio se escribe, como producto de polinomios irreducibles, en una de las siguientes formas, lo que permite identificar el grupo de Galois:

$$\begin{cases} f(X)=(X-\alpha_1)f_1(X) & \begin{cases} \sqrt{\text{Discr}(f)}\notin K \Rightarrow & \text{Gal}(f/K)=S_4. \\ \sqrt{\text{Discr}(f)}\in K \Rightarrow & \text{Gal}(f/K)=A_4. \end{cases} \\ f(X)=(X-\alpha_1)f_1(X)f_2(X) & \Rightarrow \quad \text{Gal}(f/K)=D_4. \\ f(X)=(X-\alpha_1)f_1(X)f_2(X)f_3(X) & \begin{cases} \sqrt{\text{Discr}(f)}\notin K \Rightarrow & \text{Gal}(f/K)=C_4. \\ \sqrt{\text{Discr}(f)}\in K \Rightarrow & \text{Gal}(f/K)=V. \end{cases} \end{cases}$$

Es claro que para poder hacer esto es necesario poder estudiar polinomios en la extensión $K(\alpha_1)$.

Polinomios de grado 5

Sea $f(X)\in K[X]$ un polinomio de grado 5.

Quíntica reducible

Caso 1. $f(X)=(X-\alpha)f_1$, tenemos que $\text{Gal}(f/K)=Gal(f_1/K)$, que es una cuártica ya discutida.

Caso 2. $f(X)=f_1f_2$ con f_i irreducible, $\text{gr}(f_1)=3$, $\text{gr}(f_2)=2$. Si $\alpha_1,\alpha_2,\alpha_3$ son las raíces de $f_1(X)$, y α_4,α_5 las de $f_2(X)$, entonces

(1) $G=\text{Gal}(f/K)$ es un subgrupo de $H=\langle(1\,2\,3),(1\,2),(4\,5)\rangle$.
(2) G actúa transitivamente sobre el conjunto $\{1,2,3\}$ y también sobre el conjunto $\{4,5\}$; entonces $6\mid|G|$.
(3) Como $H\cong S_3\times S_2\cong D_6$, el grupo H es de orden 12 y contiene exactamente tres subgrupos de orden 6. De todos ellos, $S_3=\langle(1\,2\,3),(1\,2)\rangle$ no es transitivo sobre $\{4,5\}$, así que sólo nos quedan tres posibilidades, que podemos distinguir por los discriminantes de f_1 y f_2:

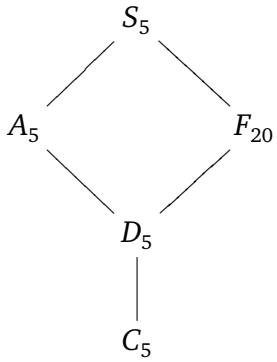
$$\begin{cases} \langle(1\,2\,3),(1\,2)\rangle \cong S_3 & \Rightarrow \text{No puede ocurrir, no es transitivo sobre } \{4,5\} \\ H \cap A_5 = \langle(1\,2\,3),(1\,2)(4\,5)\rangle \cong S_3 & \Rightarrow \sqrt{\text{Discr}(f_1)\,\text{Discr}(f_2)} \in K. \\ H \cong A_3 \times S_2 & \Rightarrow \sqrt{\text{Discr}(f_1)},\ \sqrt{\text{Discr}(f_1)\,\text{Discr}(f_2)} \notin K. \\ \langle(1\,2\,3),(4\,5)\rangle \cong A_3 \times S_2 & \Rightarrow \sqrt{\text{Discr}(f_1)} \in K,\ \sqrt{\text{Discr}(f_1)\,\text{Discr}(f_2)} \notin K. \end{cases}$$

En los dos últimos casos se tiene $\sqrt{\text{Discr}(f_1)\,\text{Discr}(f_2)} \notin K$, y resulta que $G = \text{Gal}(f_1/K) \times \text{Gal}(f_2/K)$.

Quíntica irreducible

El grupo G es un subgrupo transitivo de S_5. Los subgrupos transitivos de S_5 son:

S_5,	normal.
A_5,	normal.
$F_{20} = \langle(1\,2\,3\,4\,5),(1\,2\,4\,3)\rangle = N_{S_5}(C_5)$,	y sus conjugados.
$C_5 = \langle(1\,2\,3\,4\,5)\rangle$,	y sus conjugados.
$D_5 = \langle <(1\,2\,3\,4\,5),(1\,4)(2\,3)> \rangle$,	y sus conjugados.



Para distinguir en este caso buscamos un elemento primitivo para el cuerpo fijo bajo $G \cap F_{20}$. Para ello formamos los elementos:

$$\begin{array}{ll} \gamma_1 & = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_5 + \alpha_5\alpha_1, \\ \gamma_1' = (1\,2\,4\,3)\gamma_1 & = \alpha_2\alpha_4 + \alpha_4\alpha_1 + \alpha_1\alpha_3 + \alpha_3\alpha_5 + \alpha_5\alpha_2, \\ \beta_1 = \frac{1}{4}(\gamma_1 - \gamma_1')^2. & \end{array}$$

Se tiene que β_1 es fijo bajo F_{20}. Consideramos sus conjugados bajo S_5:

$$\beta_1,\ \ \beta_2 = (1\,2\,3)\beta_1,\ \ \beta_3 = (1\,3\,2)\beta_1,\ \ \beta_4 = (1\,2)\beta_1,\ \ \beta_5 = (1\,3)\beta_1,\ \ \beta_6 = (2\,3)\beta_1.$$

y formamos el polinomio $g = \prod_{i=1}^{6}(X - \beta_i)$, al que llamamos la **resolvente séxtica** de la quíntica $f(X)$. Como $\text{Stab}_{S_5}(\beta_1) = F_{20}$, entonces $\text{Gal}(E(g)/K(\beta_1)) \subseteq F_{20}$, y se verifica: el grupo G es un subgrupo de F_{20} si, y sólo si, g tiene una raíz en K. Resumiendo, tenemos una primera tabla de

clasificación:

$\sqrt{\text{Discr}(f)}$	β_i	$\text{Gal}(f/K)$
$\notin K$	$\notin K$	S_5
$\in K$	$\notin K$	A_5
$\notin K$	$\in K$	F_{20}
$\in K$	$\in K$	D_5, C_5

Observa que tenemos el problema de discriminar entre D_5 y C_5.

Los coeficientes de g son polinomios simétricos en los α_i y por tanto se pueden calcular como polinomios en los coeficientes de $f(X)$. En general este cálculo es largo y tedioso y la expresión obtenida bastante grande. Sólo vamos a citarla en un caso sencillo. Sea

$$f(X) = X^5 + aX + b.$$

Entonces $d = \text{Discr}(f) = 4^4a^5 + 5^5b^4$ y la resolvente séxtica es:

$$g(X) = (X^3 - 5aX^2 + 15a^2X + 5a^3)^2 - dX.$$

Encontrando elementos de $\text{Gal}(f/K)$

En las secciones anteriores hemos acotado el grupo $\text{Gal}(f/K)$, es decir, hemos obtenido criterios para que $\text{Gal}(f/K)$ sea un subgrupo de otros grupos conocidos de S_5. En esta sección vamos a acotarlo *por abajo*, o sea, determinaremos condiciones para que $\text{Gal}(f/K)$ contenga elementos (y por tanto subgrupos) de S_5.

Empezamos describiendo un método constructivo general para calcular el grupo de Galois sobre cualquier cuerpo en el que sepamos factorizar polinomios y a partir de él expondremos un método rápido y útil cuando $K = \mathbb{Q}$ y $n = 5$.

Sean $t_1, \ldots, t_n$ indeterminadas en número igual al grado de $f(X)$, y $\alpha_1, \ldots, \alpha_n$ las raíces de $f(X)$. Formamos las extensiones $K' = K(t_1, \ldots, t_n)$ y $E' = K'E = K'(\alpha_1, \ldots, \alpha_n)$.

Lema. 17.5.
La extensión E'/K' *es de Galois, y* $\text{Gal}(E'/K') \cong \text{Gal}(E/K)$.

DEMOSTRACIÓN. Por las propiedades de traslación de las extensiones normales y separables, E'/K' es de Galois y $\text{Gal}(E'/K') \cong \text{Gal}(E/E \cap K')$. Pero $E \cap K' = K$, ya que es una subextensión algebraica de K'/K y K es algebraicamente cerrado en K'. □

Consideramos el elemento $\theta = \alpha_1 t_1 + \cdots + \alpha_n t_n \in E'$. Para todo $\sigma \in S_n$ tenemos

$$\sigma(\theta) = \alpha_{\sigma(1)} t_1 + \cdots + \alpha_{\sigma(n)} t_n = \alpha_1 t_{\sigma^{-1}(1)} + \cdots + \alpha_n t_{\sigma^{-1}(n)}$$

Lema. 17.6.
Sean $\sigma, \tau \in S_n$. Entonces $\sigma(\theta) = \tau(\theta)$ si, y sólo si, $\sigma = \tau$.

DEMOSTRACIÓN. Los polinomios $\sigma(\theta) = \alpha_{\sigma(1)}t_1 + \cdots + \alpha_{\sigma(n)}t_n$ y $\tau(\theta) = \alpha_{\tau(1)}t_1 + \cdots + \alpha_{\tau(n)}t_n$ son iguales si, y sólo si, tienen los mismos coeficientes: $\alpha_{\sigma(i)} = \alpha_{\tau(i)}$ para todo i. Pero esto ocurre si, y sólo si, $\sigma = \tau$. □

Corolario. 17.7.
θ es un elemento primitivo para E'/K'.

Definimos $\Phi_1 = \mathrm{Irr}(\theta, K') \in K'[X]$; su grado es: $\mathrm{gr}(\Phi_1) = [E' : K'] = [E : K] = |\mathrm{Gal}(f/K)|$; el desarrollo de Φ_1 es:

$$\Phi_1 = \prod_{\sigma \in \mathrm{Gal}(f/K)} (X - \sigma(\theta)).$$

Para describir el grupo de Galois $\mathrm{Gal}(f/k)$ hacemos actuar S_n sobre K' mediante $\sigma(h(t_1, \ldots, t_n)) = h(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$.

Teorema. 17.8.
$\mathrm{Gal}(f/K) = \{\tau \in S_n \mid \tau(\Phi_1) = \Phi_1\}$.

DEMOSTRACIÓN. Calculemos:

$$\tau(\Phi_1) = \tau\left(\prod_{\sigma \in \mathrm{Gal}(f/K)} (X - \sigma(\theta)) = \prod_{\sigma \in \mathrm{Gal}(f/K)} (X - \tau\sigma(\theta))\right),$$

así que $\tau(\Phi_1) = \Phi_1$ si, y sólo si, para todo $\sigma \in \mathrm{Gal}(f/K)$ existe $\sigma_1 \in \mathrm{Gal}(f/K)$ tal que $\tau\sigma = \sigma_1$ si, y sólo si, $\tau = \sigma_1\sigma^{-1} \in \mathrm{Gal}(f/K)$. □

Es claro que Φ_1 es un divisor de

$$\Phi = \prod_{\sigma \in S_n} (X - \sigma(\theta)) \in K'. \tag{IV.3}$$

Los coeficientes de Φ son polinomios simétricos en los α_i y conocemos algoritmos para expresarlos como polinomios en los coeficientes de $f(X)$.
Del Teorema (17.8.) podemos extraer un algoritmo general para el cálculo del grupo de Galois de $f(X)$:

(1) Formamos el polinomio Φ.
(2) Descomponemos Φ en factores irreducibles en $K'[X]$. (Existen algoritmos para ello siempre que K sea "calculable", p.e., si $K=\mathbb{Q}$ o cualquier extensión finitamente generada de $\mathbb{Q}$).
(3) Tomamos uno de los factores irreducibles Φ_1 (cualquiera de ellos, sólo se diferencian en el orden de numeración de las raíces). El Teorema (17.8.) nos dice que $\sigma\in \mathrm{Gal}(f/K)$ si, y sólo si, $\sigma(\Phi_1)=\Phi_1$.

Desgraciadamente $\mathrm{gr}(\Phi)=n!$, muy alto para los cálculos prácticos (por ejemplo, si $\mathrm{gr}(f(X))=5$ tendríamos que factorizar un polinomio de grado 120 en seis indeterminadas: $X,t_1,\dots,t_5$). Incluso para grados inferiores es pesado factorizar el polinomio Φ. Por ejemplo, si $f(X)=X^3-3X+1$, el polinomio factoriza como $\Phi=\Phi_1\Phi_2$ siendo:

$$\Phi_1=X^3-3((t_1+t_2+t_3)^2-3(t_1t_2+t_2t_3+t_3t_1))X+((t_1+t_2+t_3)^3-9(t_1^2t_2+t_2^2t_3+t_3^2t_1)),$$
$$\Phi_2=X^3-3((t_1+t_2+t_3)^2-3(t_1t_2+t_2t_3+t_3t_1))X+((t_1+t_2+t_3)^3-9(t_1t_2^2+t_2t_3^2+t_3t_1^2)).$$

Pero si K es el cuerpo de fracciones de un DFU, obtenemos una consecuencia muy útil.

Sean D un dominio de factorización única, K su cuerpo de fracciones, $\mathfrak{p}$ un ideal primo de D. Llamamos $\bar{R}$ al anillo cociente $D/\mathfrak{p}$ (que es un dominio de integridad) y $\bar{K}$ al cuerpo de fracciones de $\bar{D}$. Supongamos que $f(X)$ es mónico y con coeficientes en D. Llamamos $\bar{f}\in\bar{K}$ al polinomio que se obtiene reduciendo los coeficientes de $f(X)$ módulo $\mathfrak{p}$. Suponemos además que $\bar{f}$ no tiene raíces múltiples (con lo que $f(X)$ tampoco las puede tener).

Teorema. 17.9.
Con una numeración adecuada de las raíces,

$$\mathrm{Gal}(\bar{f}/\bar{K})\subseteq \mathrm{Gal}(f/K).$$

DEMOSTRACIÓN. En este caso los coeficientes del polinomio Φ de (IV.3) son polinomios en los a_i y por tanto están en D. Los factores irreducibles sobre K también están en D por el lema de Gauss. Así que $\Phi=\Phi_1\dots\Phi_t$ con $\Phi_i\in D$. Reduciendo módulo $\mathfrak{p}$, obtenemos $\bar{\Phi}=\bar{\Phi}_1\dots\bar{\Phi}_t$ con $\bar{\Phi}_i\in\bar{D}$. Naturalmente, estos $\bar{\Phi}_i$ pueden ser reducibles. Sea Φ_1' un factor irreducible de $\bar{\Phi}_1$. Por el Teorema (17.8.), $\sigma\in\mathrm{Gal}(f/K)$ si, y sólo si, $\sigma(\bar{\Phi}_1)=\bar{\Phi}_1$, mientras que si $\sigma\notin\mathrm{Gal}(f/K)$, $\sigma(\bar{\Phi}_1)=\bar{\Phi}_i$ que no tiene ningún factor en común con $\bar{\Phi}_1$. Por otra parte, para todo $\sigma\in\mathrm{Gal}(\bar{f}/\bar{K})$ tenemos que $\sigma(\Phi_1')=\Phi_1'$ que divide a $\bar{\Phi}_1$. Luego debe verificarse que $\sigma(\bar{\Phi}_1)=\bar{\Phi}_1$ y por tanto $\sigma\in\mathrm{Gal}(f/K)$. □

Para aplicar el teorema anterior, tomamos $D=\mathbb{Z}$, $K=\mathbb{Q}$, $\mathfrak{p}=p\mathbb{Z}$, con p primo, y $\bar{D}=\bar{K}=\mathbb{Z}_p$. Obtenemos:

Corolario. 17.10.
Sea $f(X) \in \mathbb{Z}[X]$ mónico y $p \in \mathbb{Z}$ un primo tales que $p \nmid \mathrm{Discr}(f(X))$. Sea $\bar{f} = \bar{f}_1 \dots \bar{f}_t$ la factorización en factores irreducibles de $\bar{f} \in \mathbb{F}_p[X]$, y sean $n_i = \mathrm{gr}(\bar{f}_i)$. Entonces $\mathrm{Gal}(f/\mathbb{Q})$ *contiene una permutación conjugada con*

$$(1 \dots n_1)(n_1+1 \ \dots \ n_1+n_2)\cdots(n_1+\cdots+n_{t-1}+1 \ \dots \ n_1+\cdots+n_t).$$

DEMOSTRACIÓN. Todo consiste en ver que $\mathrm{Gal}(\bar{f}/\mathbb{F}_p)$ es cíclico y que sus órbitas tienen longitudes $n_1, \dots, n_t$. □

Ejemplo. 17.11.
Sea $f(X) = X^5 - X - 1$.
Reduciendo módulo 2 tenemos, $f(X) \equiv (X^2+X+1)(X^3+X^2+1) \pmod 2$, así que $\mathrm{Gal}(f/\mathbb{Q})$ contiene una permutación del tipo $\sigma = (1\ 2)(3\ 4\ 5)$. Elevando al cubo $\sigma^3 = (1\ 2) \in \mathrm{Gal}(f/\mathbb{Q})$.
Módulo 3 tenemos que $f(X)$ es irreducible. No tiene raíces y si tuviese un factor cuadrático, tendría un factor en común con $X^9 - X = X(X^4+1)(X^4-1)$ que es el producto de todos los polinomios irreducibles de grado 1 y 2 sobre $\mathbb{F}_3$. Pero entonces tendría un factor en común con $X^5 - X$ ó $X^5 + X$, luego un factor en común con -1 ó $2X+1$, que obviamente no tiene. Luego $\mathrm{Gal}(f/\mathbb{Q})$ contiene un 5-ciclo y una transposición y por tanto es S_5.

Ejercicio. 17.12.
Para todo n positivo existen infinitos polinomios $f(X) \in \mathbb{Z}[X]$ con $\mathrm{Gal}(f/\mathbb{Q}) = S_n$.

SOLUCIÓN. Todos los polinomios que vamos a considerar son mónicos. Sea $f_1(X)$ un polinomio de grado n irreducible módulo 2. Sea $f_2(X)$ el producto de un polinomio de grado 2 irreducible módulo 3 con polinomios de grado impar irreducibles módulo 3. Sea $f_3(X)$ el producto de X por un polinomio de grado $n-1$ irreducible módulo 5. Finalmente, sea $f(X) \in \mathbb{Z}[X]$ un polinomio congruente con $f_1(X)$ módulo 2, con $f_2(X)$ módulo 3 y con $f_3(X)$ módulo 5 (hay infinitos de tales polinomios por el teorema chino del resto). Entonces $\mathrm{Gal}(f/\mathbb{Q})$ es transitivo, contiene una transposición y un $(n-1)$-ciclo. Luego es S_n. □

Existen algoritmos muy eficientes para factorizar polinomios módulo p. Por ejemplo, el Corolario (17.10.) es un procedimiento efectivo para determinar los tipos de descomposición en ciclos de algunos elementos de $\mathrm{Gal}(f/\mathbb{Q})$. ¡CUIDADO! Al usar el Corolario (17.10.), no se puede suponer que una permutación particular pertenece a $\mathrm{Gal}(f/\mathbb{Q})$, sino sólo que existe una permutación de ese tipo. Por ejemplo, una factorización puede implicar la existencia de una permutación del tipo $(1\ 2)(3\ 4)$ y otra la existencia de una transposición. No se puede concluir que esta transposición sea $(1\ 2)$ y no $(1\ 3)$ ó $(3\ 4)$ o cualquier otra. La elección de $(1\ 2)(3\ 4)$ para representar la primera permutación fija un orden particular de las raíces, y puede que respecto a este orden la transposición no sea $(1\ 2)$.

Aplicación de Mathematica

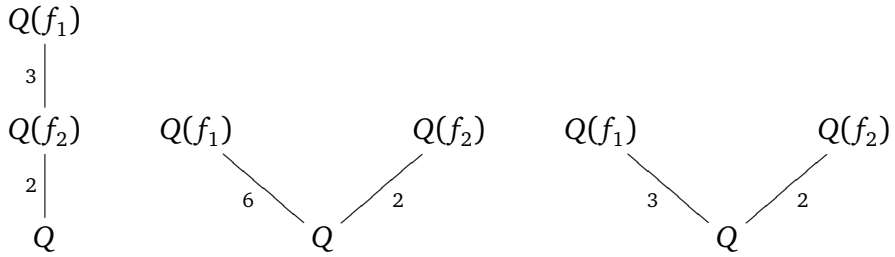
Si consideramos un polinomio $f(X) \in K[X]$ de grado 5, para calcular su grupo de Galois procedemos como sigue.

Calculamos la descomposición en irreducibles de $f(X)$.

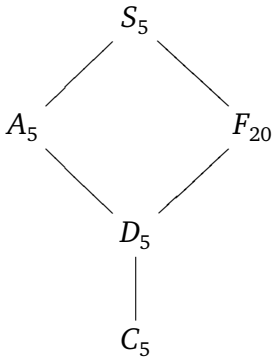
Caso 1. Si $f(X) = (X-\alpha)f_1(X)$, entonces $f_1(X)$ es de grado 4, y podemos aplicar el estudio realizado para la cuártica.

Caso 2. Si $f(X) = f_1(X)f_2(X)$, de grados 3 y 2 respectivamente, ambos irreducibles, el grupo de $f(X)$ es igual a:

$$\left\{\begin{array}{l} \left.\begin{array}{l}\sqrt{\mathrm{Discr}(f)} \in K \text{ y} \\ \sqrt{\mathrm{Discr}(f_1)\mathrm{Discr}(f_2)} \in K\end{array}\right\} \Rightarrow \quad G = S_3 \cong \langle (1\,2\,3), (1\,2)(4\,5)\rangle. \\ \\ \left.\begin{array}{l}\sqrt{\mathrm{Discr}(f_1)} \notin K \text{ y} \\ \sqrt{\mathrm{Discr}(f_1)\mathrm{Discr}(f_2)} \notin K\end{array}\right\} \Rightarrow \quad G = S_3 \times S_2 \cong \langle (1\,2\,3), (1\,2), (4\,5)\rangle. \\ \\ \left.\begin{array}{l}\sqrt{\mathrm{Discr}(f_1)} \in K \text{ y} \\ \sqrt{\mathrm{Discr}(f_1)\mathrm{Discr}(f_2)} \notin K\end{array}\right\} \Rightarrow \quad G = A_3 \times S_2 \cong \langle (1\,2\,3), (4\,5)\rangle. \end{array}\right.$$

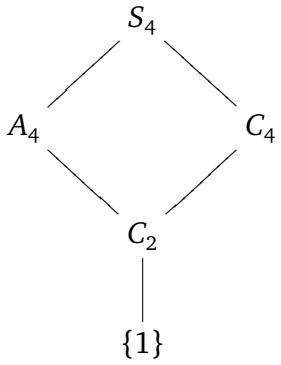


Caso 3. $f(X)$ es irreducible, en este caso el grupo $\mathrm{Gal}(f/K)$ es un subgrupo transitivo de S_5. Luego es uno de los siguientes:



Tomamos una raíz α_1 de $f(X)$. Al estudiar el polinomio $f(X)$ en $K(\alpha_1)$, el grupo de Galois es $\mathrm{Gal}(f/K(\alpha_1))$, y es el subgrupo de S_5 intersección de $\mathrm{Gal}(f/K)$ con el subgrupo que fija el elemento

1. (Es evidente que los subíndices de las raíces pueden cambiar). En cualquier caso el diagrama de los subgrupos transitivos de S_5 se transforma en el siguiente diagrama de subgrupos de S_4.



que corresponde a las siguientes factorizaciones de $f(X)$ en $K(\alpha_1)$.

$$\begin{cases} f(X)=(X-\alpha_1)f_1(X) & \begin{cases} \sqrt{\mathrm{Discr}(f)}\notin K \Rightarrow & \mathrm{Gal}(f/K)=S_5 \text{ ó } F_{20}. \\ \sqrt{\mathrm{Discr}(f)}\in K \Rightarrow & \mathrm{Gal}(f/K)=A_5. \end{cases} \\ \\ \left.\begin{array}{l} f(X)=(X-\alpha_1)f_1(X)f_2(X) \text{ ó} \\ f(X)=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)f_1(X) \end{array}\right\} & \sqrt{\mathrm{Discr}(f)}\in K \text{ (¡siempre!)} \quad \Rightarrow \quad \mathrm{Gal}(f/K)=D_5. \\ \\ f(X)=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)(X-\alpha_5) & \Rightarrow \quad \mathrm{Gal}(f/K)=C_5. \end{cases}$$

Como consecuencia, si en $K(\alpha_1)$ tenemos dos raíces, entonces están todas.

En el caso en que $f(X)=(X-\alpha_1)f_1$ y $\sqrt{\mathrm{Discr}(f)}\notin K$, entonces para dilucidar cuál es el grupo de Galois, S_5 ó F_{20}, consideramos otra raíz α_2 y estudiamos el polinomio $f(X)$ en $K(\alpha_1,\alpha_2)$. Estudiamos la intersección de $\mathrm{Gal}(f/K)$ con el subgrupo $L=S_3(3,4,5)$ que fija $\{1,2\}$; las posibilidades son que esta intersección es trivial ó es L. Tenemos entonces que si $f(X)$ descompone en $K(\alpha_1,\alpha_2)$, su grupo de Galois es F_{20}, y si $f(X)$ no descompone en $K(\alpha_1,\alpha_2)$, su grupo de Galois es S_5.

$$\begin{cases} f(X)=(X-\alpha_1)f_1(X) & \begin{cases} \sqrt{\mathrm{Discr}(f)}\notin K & \begin{cases} \sqrt{\mathrm{Discr}(f)}\notin K(\alpha_1,\alpha_2) & \Rightarrow \quad \mathrm{Gal}(f/K)=S_5. \\ \sqrt{\mathrm{Discr}(f)}\in K(\alpha_1,\alpha_2) & \Rightarrow \quad \mathrm{Gal}(f/K)=F_{20}. \end{cases} \\ \sqrt{\mathrm{Discr}(f)}\in K & \Rightarrow \quad \mathrm{Gal}(f/K)=A_5. \end{cases} \\ \\ \left.\begin{array}{l} f(X)=(X-\alpha_1)f_1(X)f_2(X) \text{ ó} \\ f(X)=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)f_1(X) \end{array}\right\} & \sqrt{\mathrm{Discr}(f)}\in K \text{ (¡siempre!)} \quad \Rightarrow \quad \mathrm{Gal}(f/K)=D_5. \\ \\ f(X)=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)(X-\alpha_5) & \Rightarrow \quad \mathrm{Gal}(f/K)=C_5. \end{cases}$$

Es claro que para poder hacer esto es necesario estudiar polinomios en las extensiones $K(\alpha_1)$ y $K(\alpha_1,\alpha_2)$.

Una consecuencia de este estudio es que el cuerpo de descomposición de un polinomio irreducible de grado 5 está generado por dos raíces si, y sólo si, el grupo de Galois es soluble.

La combinación del estudio de la resolvente séxtica con el tratamiento en Mathematica simplifica el estudio del grupo de Galois y no es necesario estudiar la factorización en la extensión $K(\alpha_1,\alpha_2)$. Un método también efectivo es el estudio módulo varios primos.

17.1. Ejercicios

Cúbica

Ejercicio. 17.13.
Determina un polinomio mónico irreducible f en $\mathbb{Q}$, de grado 3 y tal que $\mathrm{Gal}(f/\mathbb{Q})$ *sea isomorfo a* C_3.
Ref.: 4164e_048 SOLUCIÓN

Cuártica

Ejercicio. 17.14.
Sea $X^4+aX^2+b \in K[X]$ un polinomio irreducible, con K un cuerpo de característica $\neq 2$, y sea G su grupo de Galois. Demuestra que:

(1) si b es un cuadrado en K, entonces $G \cong V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
(2) si b no es un cuadrado en K y $b(a^2-4b)$ si lo es, entonces $G \cong \mathbb{Z}_4$.
(3) si b y $b(a^2-4b)$ no son cuadrados en K, entonces $G \cong D_4$.

Ref.: 4164e_002 SOLUCIÓN

Ejercicio. 17.15.
Determinar el grupo de Galois y el retículo de subcuerpos de la extensión de $\mathbb{Q}$ por el cuerpo de descomposición del polinomio X^4-3X^2+4
Ref.: 4164e_029 SOLUCIÓN

Ejercicio. 17.16.
Estudia el grupo de Galois de X^4-2X^2-2 sobre $\mathbb{Q}$.
Ref.: 4164e_042 SOLUCIÓN

Quíntica

Ejercicio. 17.17.
Sea $f \in \mathbb{Q}[X]$ una quíntica irreducible tal que $G = \mathrm{Gal}(f/\mathbb{Q}) \subseteq S_5$ contiene un ciclo de longitud 3. Prueba que $G = A_5$ ó $G = S_5$.
Ref.: 4164e_045 SOLUCIÓN

Ejercicio. 17.18.
Sea $f \in \mathbb{Q}[X]$ una quíntica irreducible con dos raíces complejas no reales y tres raíces reales. Prueba que $\mathrm{Gal}(f/\mathbb{Q}) = S_5$.
Aplícalo al polinomio $X^5 - 4X + 2 \in \mathbb{Q}[X]$.
Ref.: 4164e_046 SOLUCIÓN

Ejercicio. 17.19.
Sea $f \in K[X]$ un polinomio irreducible y separable de grado cinco, y $E = K(f)$ su cuerpo de descomposición. Si existe $\varphi \in \mathrm{Gal}(E/K)$ que fija tres raíces de f y permuta las otras dos, prueba que $\mathrm{Gal}(E/K) \cong S_5$.
Ref.: 4164e_049 SOLUCIÓN

Séxtica

Ejercicio. 17.20.
Se considera $f = X^6 - 5 \in \mathbb{Q}[X]$. Llamamos $E = \mathbb{Q}(f)$ al cuerpo de descomposición de f sobre $\mathbb{Q}$.

(1) Determina un sistema de generadores de la extensión $E/\mathbb{Q}$.
(2) Determina $[E : \mathbb{Q}]$.
(3) Describe $G = \mathrm{Gal}(E/\mathbb{Q})$ probando que tiene dos elementos, σ y τ de órdenes 6 y 2, respectivamente. ¿A qué grupo es isomorfo G?
(4) Sea $F = \mathbb{Q}(\omega, \sqrt[3]{5}) \subseteq E$. Determina el subgrupo $L = G^F$. Observa que como $F/\mathbb{Q}$ es de Galois, entonces $L \subseteq G$ es un subgrupo normal.
(5) Considera σ^3 y τ, ambos de orden 2, y el subgrupo $H = \langle \sigma^3, \tau \rangle \subseteq G$. ¿Cuál es el orden de H?
(6) Determina el cuerpo fijo de H. ¿Es $H \subseteq G$ un subgrupo normal?
(7) Ya conocemos que G contiene un subgrupo cíclico de orden 6. Prueba que G contiene más subgrupos de orden 6 aunque no sean cíclicos. ¿Cuántos?

(8) Para cada subgrupo del apartado anterior determina el cuerpo fijo.

Ref.: 4164e_050 SOLUCIÓN

Cálculo del grupo de Galois

Ejercicio. 17.21.
Sea $K/\mathbb{Q}$ una extensión de cuerpo de grado 4 que no es de Galois. Prueba que no siempre existe una extensión de Galois $E/\mathbb{Q}$ de grado 8 tal que $\mathbb{Q} \subseteq K \subseteq E$.
Ref.: 4164e_015 SOLUCIÓN

Ejercicio. 17.22.
Sea $f(X) \in \mathbb{Q}$ un polinomio de grado 4 con grupo de Galois, sobre $\mathbb{Q}$, igual a S_4. Si α es una raíz de $f(X)$,
(1) Prueba que $K = \mathbb{Q}(\alpha)/\mathbb{Q}$ tiene grado 4; evidentemente no es de Galois.
(2) Prueba que K no tiene subcuerpos propios (distintos de K y de $\mathbb{Q}$).
(3) Prueba que toda extensión de Galois $E/\mathbb{Q}$ de grado 4 tiene subcuerpos intermedios.

Ref.: 4164e_016 SOLUCIÓN

Ejercicio. 17.23.
Sea $\alpha \in \mathbb{C}$ tal que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Prueba que existe $d \in \mathbb{Q}$ tal que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$.
Ref.: 4164e_022 SOLUCIÓN

Ejercicio. 17.24.
¿Existen elementos $\alpha \in \mathbb{C}$ tales que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^t$, y α no es contruible sobre $\mathbb{Q}$?
Ver Ejercicio (8.40.).
Ref.: 4164e_020 SOLUCIÓN

Ejercicio. 17.25.
Supongamos que $X^p - a \in \mathbb{Q}[X]$ es irreducible. Demostrar que el grupo de Galois de $X^p - a$ sobre $\mathbb{Q}$ es isomorfo al grupo de transformaciones de $\mathbb{Z}_p$ de la forma $y \mapsto ky + \ell$, con $k, \ell \in \mathbb{Z}_p$ y $k \neq 0$.
Ref.: 4164e_034 SOLUCIÓN

Grupo de Galois el simétrico

Ejercicio. 17.26.
Se considera $f \in \mathbb{Q}[X]$, un polinomio de grado seis tal que $\mathrm{Gal}(f/\mathbb{Q}) \cong S_6$. Llamamos $E = \mathbb{Q}(f)$, al cuerpo de descomposición de f.

(1) Determina cuántos cuerpos intermedios $\mathbb{Q} \subseteq F \subseteq E$ existen tales que $[E : F] = 9$.
(2) Prueba que la intersección de los cuerpos F, del apartado anterior, contiene propiamente a $\mathbb{Q}$.
(3) Si $\alpha_1 \in E$ es una raíz de f, prueba que $\mathrm{Gal}(E/\mathbb{Q}(\alpha_1)) \cong S_5$.
(4) Prueba que $\mathbb{Q}(\alpha_1)$ no está contenido en ningún F.
(5) Si $\alpha_1 \neq \alpha_2 \in E$ es otra raíz de f, prueba que $\mathrm{Irr}(\alpha_2, \mathbb{Q}(\alpha_1)$ tiene grado 5.

Ref.: 4164e_043 SOLUCIÓN

Ejercicio. 17.27.
Se considera $f \in \mathbb{Q}[X]$, un polinomio de grado siete tal que $\mathrm{Gal}(f/\mathbb{Q}) \cong S_7$. Llamamos $E = \mathbb{Q}(f)$, al cuerpo de descomposición de f.

(1) Determina cuántos cuerpos intermedios $\mathbb{Q} \subseteq F \subseteq E$ existen tales que $[E : F] = 9$.
(2) Prueba que la intersección de los cuerpos F, del apartado anterior, contiene propiamente a $\mathbb{Q}$.
(3) Si $\alpha_1 \in E$ es una raíz de f, determina a cuántos de los F pertenece α_1.
(4) Si $\alpha_1 \neq \alpha_2 \in E$ es otra raíz de f, prueba que $\mathrm{Irr}(\alpha_2, \mathbb{Q}(\alpha_1))$ tiene grado 6.

Ref.: 4164e_044 SOLUCIÓN

Ejercicio. 17.28.
Sea $f \in \mathbb{Q}[X]$ una quíntica irreducible con grupo de Galois isomorfo a S_5.

(1) Determina cuántas extensiones cuadráticas de $\mathbb{Q}$ existe en $E = Q(f)$.
(2) Describe un generador de cada una de ellas.

Ref.: 4164e_047 *SOLUCIÓN*

18. Resolución de ecuaciones solubles

Consideramos un polinomio soluble $f(X)$ sobre un cuerpo K, esto significa que si E es el cuerpo de descomposición de $f(X)$, entonces el grupo de Galois $G = \mathrm{Gal}(f/K)$ es un grupo soluble. Como consecuencia, existe una serie de composición $\{1\} \subsetneqq H_1 \subsetneqq \cdots \subsetneqq H_t = G$, con factores de composición grupos abelianos simples. Dado el factor H_{i+1}/H_i, la extensión $E^{H_i}/E^{H_{i+1}}$ es una extensión de Galois cíclica de grado un número primo, p. Para cada $\alpha \in E^{H_i} \setminus E^{H_{i+1}}$, se tiene $E^{H_{i+1}} \subsetneqq E^{H_{i+1}}(\alpha) \subseteq E^{H_i}$, por ser p primo, se tiene $E^{H_i} = E^{H_{i+1}}(\alpha)$; si $g(X) = \mathrm{Irr}(\alpha, E^{H_{i+1}})$, entonces $g(X)$ es un polinomio irreducible de grado p con grupo de Galois cíclico. Si probamos que las raíces de $g(X)$ se pueden calcular por radicales sobre $E^{H_{i+1}}$, entonces las raíces de $f(X)$ se podrán calcular por radicales sobre K.

Proposición. 18.1.
Sea K un cuerpo, igual a $\mathbb{Q}$ o a una extensión algebraica de $\mathbb{Q}$, y $f(X)$ un polinomio sobre K, irreducible de grado n con $\mathrm{Gal}(f/K)$ *cíclico. Entonces $f(X)$ es soluble por radicales.*

DEMOSTRACIÓN. Hacemos la demostración por inducción sobre n. Si $n = 1, 2$, el resultado es cierto. Supongamos que es cierto para todo polinomio de grado menor que $n > 2$. Si consideramos una raíz n–ésima primitiva de la unidad ξ, su polinomio irreducible es Φ_n, y ya que su grado es menor que n, tenemos que es soluble por radicales, y ξ se puede calcular mediante radicales.
Consideramos ahora $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$, de grado n con raíces $\alpha_1, \ldots, \alpha_n$, ordenadas de forma que $\mathrm{Gal}(f/K) = \langle(1\ 2\ \ldots\ n)\rangle$, y llamamos $\sigma = (1\ 2\ \ldots\ n)$. Para calcular los α_i, vamos a definir nuevos polinomios;

$$\begin{aligned} f_1(X) &= \alpha_1 + \alpha_2 X + \cdots + \alpha_n X^{n-1} \\ f_2(X) &= \alpha_2 + \alpha_3 X + \cdots + \alpha_1 X^{n-1} \quad = \sigma f_(X) \\ &\vdots \\ f_n(X) &= \alpha_n + \alpha_1 X + \cdots + \alpha_{n-1} X^{n-1} = \sigma^{n-1} f_1(X) \end{aligned}$$

Al evaluar en ξ, una raíz n–ésima de la unidad, no necesariamente primitiva, se tiene:

$$f_2(\xi) = \alpha_2 + \alpha_3\xi + \cdots + \alpha_1\xi^{n-1} = \xi^{-1} f_1(\xi),$$

y en general:

$$\begin{aligned} f_2(\xi) &= \xi^{-1} f_1(\xi) \\ f_3(\xi) &= \xi^{-2} f_(\xi) \\ &\vdots \\ f_n(\xi) &= \xi^{-n+1} f_1(\xi). \end{aligned}$$

4164-03.tex

En consecuencia:

$$(f_1(\xi))^n = (f_2(\xi))^n = \cdots = (f_n(\xi))^n$$

Al considerar éste como un polinomio en ξ, y hacer actuar $\langle\sigma\rangle$, se tiene:

$$\sigma(f_i(\xi))^n = \sigma(\sigma^{i-1}f_1(\xi))^n = (\sigma^i f_1(\xi))^n = (f_{i+1}(\xi))^n = (f_i(\xi))^n,$$

esto es, $(f_i(\xi))^n \in K(\xi)$, ya que K es el cuerpo fijo para $\mathrm{Gal}(f/K)$. Como consecuencia podemos calcular $f_1(\xi),\ldots,f_n(\xi)$ como las raíces n–ésimas de $(f_1(\xi))^n$. Para simplificar, llamamos a este elemento $h(\xi) = (f_1(\xi))^n \in K(\xi)$. Esto podemos hacerlo para cada raíz n–ésima de la unidad.
Sea $\{\xi_j \mid i = 1,\ldots,n\} = \{\xi_1,\ldots,\xi_n\}$ el conjunto de todas las raíces n–ésimas de la unidad; se tiene la relación $\sum_{j=1}^n \xi_j = 0$. Además, para f_1 se verifica:

$$\begin{aligned}\sum_{j=1}^n f_1(\xi_j) &= \sum_{j=1}^n (\alpha_1 + \alpha_2\xi_j + \cdots + a_n\xi_j^{n-1}) \\ &= \sum_{j=1}^n \alpha_1 + \sum_{j=1}^n \alpha_2\xi_j + \cdots + \sum_{j=1}^n \alpha_n\xi_j^{n-1} \\ &= \sum_{j=1}^n \alpha_1 + \alpha_2\sum_{j=1}^n \xi_j + \cdots + \alpha_n\sum_{j=1}^n \xi_j^{n-1} \\ &= n\alpha_1.\end{aligned}$$

En general se tiene:

$$\sum_{j=1}^n f_i(\xi_j) = n\alpha_i.$$

Y como conocemos los valores de $f_i(\xi_j)$, las raíces n–ésimas de $h(\xi_j)$, podemos calcular los valores de los α_i en función de radicales de elementos de $K(\xi)$, y por tanto de K.
El problema que queda por resolver es encontrar el valor de $h(\xi)$. Consideramos representantes de las clases de resto de $G \subseteq S_n$; si éstas son $1,\sigma_2,\ldots,\sigma_t$, entonces tenemos t conjugados de $h(\xi)$:

$$h_1 = h(\xi), \quad h_2 = \sigma_2 h(\xi), \quad \ldots, \quad h_t = \sigma_t h(\xi).$$

Consideramos la ecuación:

$$H = (Y - h_1)(Y - h_2)\ldots(Y - h_t) = 0,$$

que tiene como raíces, en $K(\xi)$, a los h_i. Ya que el polinomio H es invariante por S_n, sus coeficientes son funciones de los coeficientes del polinomio original, y por tanto son elementos de K. Además $h_1 = h(\xi)$ es una raíz de H y pertenece a $K(\xi)$, luego el polinomio tiene una raíz en $K(\xi)$. Una vez calculado $h(\xi)$, el resto es inmediato. □

Resolución de la cúbica

Ejemplo. 18.2.
Sea $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$. Es un polinomio de grado 3 irreducible, ya que no tiene raíces en $\mathbb{Q}$. Para calcular su grupo de Galois basta con calcular su discriminante:

$$\begin{aligned}&\mathrm{Discr}(X^3 + bX + c) = -4b^3 - 27c^2 \\ &\mathrm{Discr}(X^3 - 3X + 1) = 81 \text{ (es un cuadrado en } \mathbb{Q})\end{aligned}$$

Como consecuencia se tiene $\mathrm{Gal}(f/\mathbb{Q}) = A_3$. Las raíces cúbicas de la unidad son: 1, ω y ω^2. En este caso f_1 es:

$$f_1(\xi) = \alpha_1 + \alpha_2\xi + \alpha_3\xi^2,$$

y

$$\begin{aligned} h(\xi) &= (f_1(\xi))^3 = (\alpha_1 + \alpha_2\xi + \alpha_3\xi^2)^3 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\xi(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\xi^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) + 6\alpha_1\alpha_2\alpha_3. \end{aligned}$$

Observa que $h(\xi)$ queda fijo por A_3, y no por S_3. Tenemos que $h(\xi)$ pertenece al cuerpo $K(\xi)$, y el hecho de no ser invariante por S_3 nos dificulta el cálculo de una expresión explícita de $h(\xi)$.
Particularizando para $\xi = 1, \omega, \omega^2$, y utilizando que se obtienen polinomios simétricos en los α_i, veremos que se tiene:

$$\begin{aligned} h(1) &= 0 \\ h(\omega) &= -27\omega \\ h(\omega^2) &= -27\omega^2 \end{aligned}$$

Vamos a ver cómo se calculan estos valores.

(1) La expresión $h(1)$ es fácil, ya que $h(1) = (\alpha_1 + \alpha_2 + \alpha_3)^3 = 0^3 = 0$.
(2) Para $h(\omega)$ tenemos:

$$\begin{aligned} h(\omega) &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) + 6\alpha_1\alpha_2\alpha_3 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 6\alpha_1\alpha_2\alpha_3 + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) \\ &= -3 - 6 + 3B\omega + 3A\omega^2 = -9 + 3B\omega + 3A\omega^2 \end{aligned}$$

En donde hemos aplicado que

$$\begin{aligned} &\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = e_1^3 - 3e_1e_2 + 3e_3 = -3a_0 + 3a_1a_2 - a_2^3 = -3 \\ &\alpha_1\alpha_2\alpha_3 = e_3 = -a_0 = -1 \text{ y definido} \\ &A = \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 \\ &B = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 \end{aligned}$$

(3) En la misma forma, para $h(\omega^2)$ tenemos:

$$\begin{aligned} h(\omega^2) &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\omega^2(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) + 6\alpha_1\alpha_2\alpha_3 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 6\alpha_1\alpha_2\alpha_3 + 3\omega^2(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) \\ &= -3 - 6 + 3A\omega + 3B\omega^2 = -9 + 3A\omega + 3B\omega^2 \end{aligned}$$

La órbita de $h(\omega)$ por S_3 tiene sólo dos elementos, ya que A_3 lo estabiliza, y el índice de A_3 en S_3 es igual a 2; estos son: $h(\omega)$ y $(1\,2)h(\omega)$. Lo mismo ocurre para $h(\omega^2)$. En este caso se verifica:

$$(1\,2)h(\omega) = h(\omega^2) \quad \text{y} \quad (1\,2)h(\omega^2) = h(\omega).$$

Tenemos entonces la ecuación

$$H(Y) = (Y - h(\omega))(Y - h(\omega^2)) = 0,$$

que en $K(\omega)$ tiene dos raíces: $h(\omega)$ y $h(\omega^2) = (1\ 2)h(\omega)$. Desarrollamos y resolvemos esta ecuación:

$$\begin{aligned}&(Y-(-9+3B\omega+3A\omega^2))(Y-(-9+3A\omega+3B\omega^2))\\ &= Y^2+Y(18+3A+3B)+(81+27A+9A^2+27B-9AB+9B^2)\\ &= Y^2+Y(18+3(A+B))+(81+27(A+B)+9(A^2-AB+B^2)\end{aligned}$$

Los elementos

$$\begin{aligned}A &= \alpha_1\alpha_2^2+\alpha_2\alpha_3^2+\alpha_3\alpha_1^2\\ B &= \alpha_1^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1\end{aligned}$$

son fijos por A_3 pero no por S_3, en cambio $A+B$ y A^2-AB+B^2 son invariantes por S_3.

$A+B = e_1e_2-3e_3 = 3a_0-a_1a_2 = 3$ y
$A^2-AB+B^2 = e_1^2e_2^2-3e_2^3-3e_1^3e_3+12e_1e_2e_3-18e_3^2 = -18a_0^2-3a_1^3+12a_0a_1a_2+a_1^2a_2^2-3a_0a_2^3 = 63$

La ecuación se escribe:

$$Y^2+Y(18+3(A+B))+(81+27(A+B)+9(A^2-AB+B^2) = Y^2+27Y+729 = Y^2+27Y+27^2 = 0$$

Como se tiene $(Y-27)(Y^2+27Y+27^2) = Y^3-27^3$, las raíces de $H(Y)$ son: $\omega 27$ y $\omega^2 27$, y por tanto $h(\omega) = 27\omega$ y $h(\omega^2) = 27\omega^2$. Esto es:

$$\begin{cases}h(1) &= (f_1(1))^3 &= (f_2^(1))^3 &= (f_3(1))^3 = 0\\ h(\omega) &= (f_1(\omega))^3 &= (f_2(\omega))^3 &= (f_3(1))^3 = 27\omega\\ h(\omega^2) &= (f_1(\omega^2))^3 &= (f_2(\omega^2))^3 &= (f_3(1))^3 = 27\omega^2\end{cases}$$

y resulta:

$$\begin{cases}f_1(0)=0, & f_2(1)=0, & f_3(1)=0\\ f_1(\omega)=\sqrt[3]{27\omega}, & f_2(\omega)=\omega\sqrt[3]{27\omega}, & f_3(\omega)=\omega^2\sqrt[3]{27\omega}\\ f_1(\omega^2)=\omega^2\sqrt[3]{27\omega^2}, & f_2(\omega^2)=\omega\sqrt[3]{27\omega^2}, & f_3(\omega^2)=\sqrt[3]{27\omega^2}\end{cases}$$

Tenemos entonces, de $\sum_{j=1}^n f_i(\xi_j) = n\alpha_i$, que

$$\begin{cases}f_1(1)+f_1(\omega)+f_1(\omega^2) = 3\alpha_1\\ f_2(1)+f_2(\omega)+f_2(\omega^2) = 3\alpha_2\\ f_3(1)+f_3(\omega)+f_3(\omega^2) = 3\alpha_3\end{cases}$$

en nuestro caso:

$$\begin{cases}0+\sqrt[3]{27\omega}+\omega^2\sqrt[3]{27\omega^2} &= 3\alpha_1\\ 0+\omega\sqrt[3]{27\omega}+\omega\sqrt[3]{27\omega^2} &= 3\alpha_2\\ 0+\omega^2\sqrt[3]{27\omega}+\sqrt[3]{27\omega^2} &= 3\alpha_3\end{cases}$$

Esto es,

$$\begin{cases}\sqrt[3]{\omega} &+\omega^2\sqrt[3]{\omega^2} &= \alpha_1\\ \omega\sqrt[3]{\omega} &+\omega\sqrt[3]{\omega^2} &= \alpha_2\\ \omega^2\sqrt[3]{\omega}+\sqrt[3]{\omega^2} & &= \alpha_3\end{cases}$$

$$\begin{cases} \sqrt[3]{\omega} & +\omega^2\sqrt[3]{\omega^2} = \alpha_1 = \omega^{\frac{1}{3}} + \omega^{\frac{8}{3}} \\ \omega\sqrt[3]{\omega} & +\omega\sqrt[3]{\omega^2} = \alpha_2 = \omega^{\frac{4}{3}} + \omega^{\frac{5}{3}} \\ \omega^2\sqrt[3]{\omega} & +\sqrt[3]{\omega^2} = \alpha_3 = \omega^{\frac{7}{3}} + \omega^{\frac{2}{3}} \end{cases}$$

$$\begin{cases} \alpha_1 = \omega^{\frac{1}{3}} + \omega^{-\frac{1}{3}} \\ \alpha_2 = \omega^{\frac{4}{3}} + \omega^{-\frac{4}{3}} \\ \alpha_3 = \omega^{-\frac{2}{3}} + \omega^{\frac{2}{3}} \end{cases}$$

Ejemplo. 18.3.
Sea $f(X) = X^3 - 3X + 3 \in \mathbb{Q}[X]$. Es un polinomio de grado 3 irreducible, ya que no tiene raíces en $\mathbb{Q}$. Para calcular su grupo de Galois basta con calcular su discriminante:

$$\begin{aligned} &\text{Discr}(X^3 + bX + c) = -4b^3 - 27c^2 \\ &\text{Discr}(X^3 - 3X + 3) = -135 \text{ (no es un cuadrado en } \mathbb{Q}) \end{aligned}$$

Como consecuencia se tiene $\text{Gal}(f/\mathbb{Q}) = S_3$. Una serie de composición de S_3 es $\{1\} \subsetneq A_3 \subsetneq S_3$. Las raíces de $f(X)$ son $\alpha_1, \alpha_2, \alpha_3$, ordenadas de forma que $S_3 = \langle \sigma = (1\ 2\ 3), \tau = (1\ 2) \rangle$. El cuerpo fijo para A_3 es $(\sqrt{\text{Discr}(p)}) = \mathbb{Q}(3\sqrt{-15}) = \mathbb{Q}(\sqrt{-15})$, y tenemos la torre de cuerpos: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-15}) \subseteq E$. Es claro que la extensión $\mathbb{Q}(\sqrt{-15})/\mathbb{Q}$ es cíclica, $\sqrt{-15}$ se obtiene por radicales a partir de elementos de $\mathbb{Q}$. Tenemos pues que estudiar la extensión $E/\mathbb{Q}(\sqrt{-15})$, que es cíclica de grado 3. Observa que E es el cuerpo de descomposición del polinomio $f(X) = X^3 - 3X + 3$ sobre $K = \mathbb{Q}(\sqrt{-15})$, y podemos aplicar el desarrollo del ejemplo anterior.
Las raíces cúbicas de la unidad son: 1, ω y ω^2. En este caso f_1 es:

$$f_1(\xi) = \alpha_1 + \alpha_2\xi + \alpha_3\xi^2,$$

y

$$\begin{aligned} h(\xi) &= (f_1(\xi))^3 = (\alpha_1 + \alpha_2\xi + \alpha_3\xi^2)^3 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\xi(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\xi^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) + 6\alpha_1\alpha_2\alpha_3. \end{aligned}$$

Observa que $h(\xi)$ queda fijo por A_3, y no por S_3. Tenemos que $h(\xi)$ pertenece al cuerpo $K(\xi)$, y el hecho de no ser invariante por S_3 nos dificulta el cálculo de una expresión explícita de $h(\xi)$.
Particularizando para $\xi = 1, \omega, \omega^2$, y utilizando que se obtienen polinomios simétricos en los α_i, se tiene:

$$\begin{aligned} &h(1) = 0 \\ &h(\omega) = \tfrac{27}{2}\left(-3 - \sqrt{5}\right) \\ &h(\omega^2) = \tfrac{27}{2}\left(-3 + \sqrt{5}\right) \end{aligned}$$

Vamos a ver cómo se calculan estos valores.

(1) La expresión $h(1)$ es fácil, ya que $h(1) = (\alpha_1 + \alpha_2 + \alpha_3)^3 = 0^3 = 0$.
(2) Para $h(\omega)$ tenemos:

$$\begin{aligned} h(\omega) &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) + 6\alpha_1\alpha_2\alpha_3 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 6\alpha_1\alpha_2\alpha_3 + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) \\ &= -9 - 18 + 3B\omega + 3A\omega^2 = -27 + 3B\omega + 3A\omega^2 \end{aligned}$$

En donde hemos aplicado que

$$\begin{array}{l}\alpha_1^3+\alpha_2^3+\alpha_3^3 = e_1^3-3e_1e_2+3e_3 = -3a_0+3a_1a_2-a_2^3 = -9\\ \alpha_1\alpha_2\alpha_3 = e_3 = -a_0 = -3 \text{ y definido}\\ A = \alpha_1\alpha_2^2+\alpha_2\alpha_3^2+\alpha_3\alpha_1^2\\ B = \alpha_1^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1\end{array}$$

(3) En la misma forma, para $h(\omega^2)$ tenemos:

$$\begin{aligned}h(\omega^2) &= \alpha_1^3+\alpha_2^3+\alpha_3^3+3\omega^2(\alpha_1^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1)+3\omega(\alpha_1\alpha_2^2+\alpha_2\alpha_3^2+\alpha_3\alpha_1^2)+6\alpha_1\alpha_2\alpha_3\\ &= \alpha_1^3+\alpha_2^3+\alpha_3^3+6\alpha_1\alpha_2\alpha_3+3\omega^2(\alpha_1^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1)+3\omega(\alpha_1\alpha_2^2+\alpha_2\alpha_3^2+\alpha_3\alpha_1^2)\\ &= -9-18+3A\omega+3B\omega^2 = -27+3A\omega+3B\omega^2\end{aligned}$$

La órbita de $h(\omega)$ por S_3 tiene sólo dos elementos, ya que A_3 lo estabiliza, y el índice de A_3 en S_3 es igual a 2; estos son: $h(\omega)$ y $(1\,2)h(\omega)$. Lo mismo ocurre para $h(\omega^2)$. En este caso se verifica:

$$(1\,2)h(\omega) = h(\omega^2) \quad \text{y} \quad (1\,2)h(\omega^2) = h(\omega).$$

Tenemos entonces la ecuación

$$H(Y) = (Y-h(\omega))(Y-h(\omega^2)) = 0,$$

que en $K(\omega)$ tiene dos raíces: $h(\omega)$ y $h(\omega^2) = (1\,2)h(\omega)$. Desarrollamos y resolvemos esta ecuación:

$$\begin{aligned}&(Y-(-27+3B\omega+3A\omega^2))(Y-(-27+3A\omega+3B\omega^2))\\ &= Y^2+Y(54+3A+3B)+(729+81A+9A^2+81B-9AB+9B^2)\\ &= Y^2+Y(54+3(A+B))+(729+81(A+B)+9(A^2-AB+B^2)\end{aligned}$$

Los elementos

$$\begin{array}{l}A = \alpha_1\alpha_2^2+\alpha_2\alpha_3^2+\alpha_3\alpha_1^2\\ B = \alpha_1^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1\end{array}$$

son fijos por A_3, pero on por S_3, en cambio $A+B$ y A^2-AB+B^2 son invariantes por S_3.

$A+B = e_1e_2-3e_3 = 3a_0-a_1a_2 = 9$ y
$A^2-AB+B^2 = e_1^2e_2^2-3e_2^3-3e_1^3e_3+12e_1e_2e_3-18e_3^2 = -18a_0^2-3a_1^3+12a_0a_1a_2+a_1^2a_2^2-3a_0a_2^3 = -81$

La ecuación se escribe:

$$Y^2+Y(54+3(A+B))+(729+81(A+B)+9(A^2-AB+B^2) = Y^2+81Y+729 = Y^2+3^4Y+3^6 = 0$$

Las raíces son: $\frac{27}{2}\left(-3-\sqrt{5}\right)$ y $\frac{27}{2}\left(-3+\sqrt{5}\right)$, y por tanto $h(\omega) = \frac{27}{2}\left(-3-\sqrt{5}\right)$ y $h(\omega^2) = \frac{27}{2}\left(-3+\sqrt{5}\right)$. Esto es:

$$\begin{cases}h(1) &= (f_1(1))^3 &= (f_2(1))^3 &= (f_3(1))^3 = 0\\ h(\omega) &= (f_1(\omega))^3 &= (f_2(\omega))^3 &= (f_3(1))^3 = \frac{27}{2}\left(-3-\sqrt{5}\right)\\ h(\omega^2) &= (f_1(\omega^2))^3 &= (f_2(\omega^2))^3 &= (f_3(1))^3 = \frac{27}{2}\left(-3+\sqrt{5}\right)\end{cases}$$

y resulta:

$$\begin{cases} f_1(0)=0, & f_2(1)=0, & f_3(1)=0 \\ f_1(\omega)=\sqrt[3]{\frac{27}{2}\left(-3-\sqrt{5}\right)}, & f_2(\omega)=\omega\sqrt[3]{\frac{27}{2}\left(-3-\sqrt{5}\right)}, & f_3(\omega)=\omega^2\sqrt[3]{\frac{27}{2}\left(-3-\sqrt{5}\right)} \\ f_1(\omega^2)=\omega^2\sqrt[3]{\frac{27}{2}\left(-3+\sqrt{5}\right)}, & f_2(\omega^2)=\omega\sqrt[3]{\frac{27}{2}\left(-3+\sqrt{5}\right)}, & f_3(\omega^2)=\sqrt[3]{\frac{27}{2}\left(-3+\sqrt{5}\right)} \end{cases}$$

Tenemos entonces, de $\sum_{j=1}^{n} f_i(\xi_j)=n\alpha_i$, que

$$\begin{cases} f_1(1)+f_1(\omega)+f_1(\omega^2)=3\alpha_1 \\ f_2(1)+f_2(\omega)+f_2(\omega^2)=3\alpha_2 \\ f_3(1)+f_3(\omega)+f_3(\omega^2)=3\alpha_3 \end{cases}$$

en nuestro caso:

$$\begin{cases} 0+\sqrt[3]{\frac{27}{2}\left(-3-\sqrt{5}\right)}+\omega^2\sqrt[3]{\frac{27}{2}\left(-3+\sqrt{5}\right)}=3\alpha_1 \\ 0+\omega\sqrt[3]{\frac{27}{2}\left(-3-\sqrt{5}\right)}+\omega\sqrt[3]{\frac{27}{2}\left(-3+\sqrt{5}\right)}=3\alpha_2 \\ 0+\omega^2\sqrt[3]{\frac{27}{2}\left(-3-\sqrt{5}\right)}+\sqrt[3]{\frac{27}{2}\left(-3+\sqrt{5}\right)}=3\alpha_3 \end{cases}$$

Esto es,

$$\begin{cases} \alpha_1=\sqrt[3]{\frac{1}{2}\left(-3-\sqrt{5}\right)}+\omega^2\sqrt[3]{\frac{1}{2}\left(-3+\sqrt{5}\right)} \\ \alpha_2=\omega\sqrt[3]{\frac{1}{2}\left(-3-\sqrt{5}\right)}+\omega\sqrt[3]{\frac{1}{2}\left(-3+\sqrt{5}\right)} \\ \alpha_3=\omega^2\sqrt[3]{\frac{1}{2}\left(-3-\sqrt{5}\right)}+\sqrt[3]{\frac{1}{2}\left(-3+\sqrt{5}\right)} \end{cases}$$

Supongamos que tenemos una extensión cíclica F/K con $\mathrm{Gal}(F/K)=\langle\sigma\rangle$ tal que $\xi\in K$, para una raíz n–ésima primitiva de la unidad, sea $F=K(\alpha,\sigma(\alpha),\ldots,\sigma^{n-1}(\alpha)$, las resolventes de Galois se definen

$$\beta_i=\sum_{j=0}^{n-1}\xi^{-ij}\sigma^j(\alpha),\ i=0,1,\ldots,n-1.$$

Lema. 18.4.
En la situación anterior se verifica:
(1) $\sigma(\beta_i)=\xi^i\beta_i$.
(2) $\sigma^h(\alpha)=\sum_{i=0}^{n-1}\frac{\xi^{ik}}{n}\beta_i\in\sum_{i=0}^{n-1}K\beta_i$.

DEMOSTRACIÓN. (1). Tenemos:

$$\begin{aligned} \sigma(\beta_i) &= \sigma(\textstyle\sum_{j=0}^{n-1}\xi^{-ij}\sigma^j(\alpha)) \\ &= \textstyle\sum_{j=0}^{n-1}\xi^{-ij}\sigma^{j+1}(\alpha) \\ &= \xi^i\textstyle\sum_{j=0}^{n-1}\xi^{-ij-i}\sigma^{j+1}(\alpha) \\ &= \xi^i\textstyle\sum_{j=0}^{n-1}\xi^{-i(j+1)}\sigma^{j+1}(\alpha) \\ &= \xi^i\beta_i. \end{aligned}$$

(2). Tenemos: $\beta_i = \sum_{j=0}^{n-1} \xi^{-ij}\sigma^j(\alpha)$, si multiplicamos por ξ^{ih} se verifica:

$$\begin{aligned}\sum_{i=0}^{n-1} \xi^{ih}\beta_i &= \sum_{i=0}^{n-1} \xi^{ih} \sum_{j=0}^{n-1} \xi^{-ij}\sigma^j(\alpha)\\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \xi^{-ij+ih}\sigma^j(\alpha)\\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \xi^{-i(j-h)}\sigma^j(\alpha)\\ &= \sum_{i=0}^{n-1}\Big(\sum_{j=0}^{n-1} \xi^{-i(j-h)}\Big)\sigma^j(\alpha)\\ &= \sum_{i=0}^{n-1}\sigma^j(\alpha)\\ &= n\sigma^j(\alpha)\end{aligned}$$

ya que si $j-h \neq 0$ se tiene $\sum_{j=0}^{n-1} \xi^{-i(j-h)} = \frac{\xi^{n(j-h)}-1}{\xi^{j-h}-1} = 0$. □

Ejemplo. 18.5.
Consideramos ahora el caso de una cúbica general

$$f = X^3 + a_2X^2 + a_1X + a_0 = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$$

y sea $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ su cuerpo de descomposición.
El discriminante es:

$$\Delta = (-1)^{\frac{3(3-1)}{2}}\begin{vmatrix} 1 & a_2 & a_1 & a_0 & 0\\ 0 & 1 & a_2 & a_1 & a_0\\ 3 & 2a_2 & a_1 & 0 & 0\\ 0 & 3 & 2a_2 & a_1 & 0\\ 0 & 0 & 3 & 2a_2 & a_1\end{vmatrix} \in \mathbb{Q}(a_2, a_1, a_0) = K$$

y $G = \mathrm{Gal}(f/\mathbb{Q}) = S_3$.
Una serie de composición para este grupo es: $S_3 \trianglerighteq A_3 \trianglerighteq \{1\}$, y los cuerpos fijos bajo los grupos de esta serie forman la torre:

$$K \subseteq K(\sqrt{\Delta}) \subseteq E.$$

La primera extensión es cuadrática.
Para aplicar el teorema de Lagrange, extendemos todos los cuerpos adjuntando una raíz cúbica de la unidad $\omega = (-1+\sqrt{-3})/2$. Las raíces α_i pertenecen a $E' = E(\omega)$ que es cíclica de grado tres sobre $K(\sqrt{\Delta}, \omega)$, con grupo generado por $\sigma = (1\,2\,3)$. Formamos las *resolventes de Lagrange*:

$$\begin{aligned}\beta_0 &= \alpha_1 + \alpha_2 + \alpha_3\\ \beta_1 &= \alpha_1 + \omega\sigma(\alpha_1) + \omega^2\sigma^2(\alpha_1) = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3\\ \beta_2 &= \alpha_1 + \omega^2\sigma(\alpha_1) + \omega\sigma^2(\alpha_1) = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3\end{aligned}$$

Sus cubos pertenecen a $K(\sqrt{\Delta}, \omega)$. Teniendo en cuenta que los polinomios simétricos elementales de los α_i son los coeficientes de f, salvo el signo, tenemos:

$$\begin{aligned}\beta_1^3 = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 6\alpha_1\alpha_2\alpha_3 + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2)\\ = (\alpha_1+\alpha_2+\alpha_3)^3 + 3(\omega-1)A + 3(\omega^2-1)B, \quad \text{(IV.4)}\end{aligned}$$

donde

$$A = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1,$$
$$B = \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2$$

Tenemos que

$$A-B = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3) = \sqrt{\Delta} \text{ y}$$
$$A+B = (\sum \alpha_i)(\sum \alpha_i\alpha_j) - 3\alpha_1\alpha_2\alpha_3.$$

Sustituyendo los polinomios simétricos por los coeficientes de f nos queda:

$$\begin{array}{ll} A-B = & \sqrt{\Delta} \qquad A = \frac{1}{2}\left(-a_2a_1 + 3a_0 + \sqrt{\Delta}\right) \\ A+B = & -a_2a_1 + 3a_0 \qquad B = \frac{1}{2}\left(-a_2a_1 + 3a_0 - \sqrt{\Delta}\right). \end{array}$$

Simplificamos ahora IV.4 (Nótese que $\omega - \omega^2 = \sqrt{-3}$):

$$\beta_1^3 = -a_2^3 - \frac{9}{2}(A+B) + \frac{3}{2}(\omega-\omega^2)(A-B) = \frac{-2a_2^3 + 9a_2a_1 - 27a_0}{2} + \frac{3}{2}\sqrt{-3\Delta}$$

Análogamente obtenemos:

$$\beta_2^3 = -a_2^3 - \frac{9}{2}(A+B) + \frac{3}{2}(\omega^2-\omega)(A-B) = \frac{-2a_2^3 + 9a_2a_1 - 27a_0}{2} - \frac{3}{2}\sqrt{-3\Delta}.$$

Tenemos el sistema:

$$\begin{array}{ll} \alpha_1 + \alpha_2 + \alpha_3 = -a_2 & \\ \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 = \beta_1 & = \sqrt[3]{\frac{-2a_2^3+9a_2a_1-27a_0}{2} + \frac{3}{2}\sqrt{-3\Delta}} \\ \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 = \beta_2 & = \sqrt[3]{\frac{-2a_2^3+9a_2a_1-27a_0}{2} - \frac{3}{2}\sqrt{-3\Delta}} \end{array}$$

cuyas soluciones son las raíces de f:

$$\alpha_1 = \frac{1}{3}\left(-a_2 + \sqrt[3]{\frac{-2a_2^3+9a_2a_1-27a_0}{2} + \frac{3}{2}\sqrt{-3\Delta}} + \sqrt[3]{\frac{-2a_2^3+9a_2a_1-27a_0}{2} - \frac{3}{2}\sqrt{-3\Delta}}\right)$$

$$\alpha_2 = \frac{1}{3}\left(-a_2 + \omega^2\sqrt[3]{\frac{-2a_2^3+9a_2a_1-27a_0}{2} + \frac{3}{2}\sqrt{-3\Delta}} + \omega\sqrt[3]{\frac{-2a_2^3+9a_2a_1-27a_0}{2} - \frac{3}{2}\sqrt{-3\Delta}}\right)$$

$$\alpha_3 = \frac{1}{3}\left(-a_2 + \omega\sqrt[3]{\frac{-2a_2^3+9a_2a_1-27a_0}{2} + \frac{3}{2}\sqrt{-3\Delta}} + \omega^2\sqrt[3]{\frac{-2a_2^3+9a_2a_1-27a_0}{2} - \frac{3}{2}\sqrt{-3\Delta}}\right)$$

En el caso particular en que $f = X^3 + aX + b$, es decir cuando $a_2 = 0$, $a_1 = a$, $a_0 = b$, las anteriores expresiones se reducen a las fórmulas de Cardano.

Ejemplo. 18.6. (Fórmula de Tartaglia–Cardano)
Sea $f(X) = X^3 + aX^2 + bX + c \in \mathbb{C}[X]$ un polinomio de grado 3. Primero observa que podemos hacer el desarrollo de $f(X)$, obteniendo:

$$f(X) = f(y) + \frac{f'(y)}{1!}(X-y) + \frac{f^{(2}(y)}{2!}(X-y)^2 + \frac{f^{(3}(y)}{3!}(X-y)^3.$$

Haciendo $f^{(2}(y)=0$, resulta $6y+2a=0$, y tenemos el valor $y=\dfrac{-a}{3}$. De esta forma tenemos un polinomio $(X+\frac{a}{3})^3+f(\frac{-a}{3})(X+\frac{a}{3})+f(\frac{-a}{3})$, y haciendo el cambio de variable $X+\frac{a}{3}\mapsto Y$, tenemos un polinomio de la forma Y^3+bY+c.
Consideremos pues que $f(X)=X^3+bX+c\in\mathbb{C}[X]$. Sea $X=x-y$, desarrollando $f(X)$ tenemos:

$$\begin{aligned} f(x-y) &= (x-y)^3+b(x-y)+c \\ &= x^3-y^3-3xy(x-y)+b(x-y)+c, \end{aligned}$$

que puede resolverse mediante $x^3-y^3+c=0$ y $3xy-b=0$. Como consecuencia, $x^3y^3=\frac{b^3}{27}$, y se tiene $x^3(x^3+c)=\frac{b^3}{27}$, esto es, $(x^3)^2+c(x^3)-\frac{b^3}{27}=0$ de donde $x^3=\dfrac{-c\pm\sqrt{c^2+\frac{4b^3}{27}}}{2}=\dfrac{-c}{2}\pm\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}$.
De la misma forma se tiene $(y^3-c)y^3=\frac{b^3}{27}$, y por tanto, $(y^3)^2-c(y^3)-\frac{b^3}{27}=0$, de donde $y^3=\dfrac{c}{2}\pm\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}$.
Tenemos entonces la raíz

$$\sqrt[3]{\frac{-c}{2}+\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}}-\sqrt[3]{\frac{c}{2}+\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}}.$$

Ejemplo. 18.7. (Fórmula de Ferrari)
Sea $X^4+aX^2+bX+c\in\mathbb{C}[X]$, para cada $u\in\mathbb{C}$ se tiene la relación:

$$\begin{aligned} (X^2+\tfrac{a}{2}+u)^2 &= X^4+\left(\tfrac{a}{2}\right)^2+u^2+aX^2+au+2uX^2 \\ &= -aX^2-bX-c+\left(\tfrac{a}{2}\right)^2+u^2+aX^2+au+2uX^2 \\ &= -bX-c+\left(\tfrac{a}{2}\right)^2+u^2+au+2uX^2 \\ &= \left(\sqrt{2u}X-\tfrac{b}{2\sqrt{2u}}\right)^2-\tfrac{b^2}{8u}-c+\left(\tfrac{a}{2}\right)^2+u^2+au \end{aligned}$$

Se tiene entonces $(X^2+\frac{a}{2}+u)^2=\left(\sqrt{2u}X-\frac{b}{2\sqrt{2u}}\right)^2$ si, y sólo si, $-\frac{b^2}{8u}-c+\left(\frac{a}{2}\right)^2+u^2+au=0$, esto es, tenemos una relación cúbica de u, que podemos determinar siguiendo el proceso del Ejemplo (18.6.).

Resolución de la cuártica

Ejemplo. 18.8.
Consideramos un polinomio general de grado cuatro

$$f:=X^4+a_3X^3+a_2X^2+a_1X+a_0=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4).$$

Sea

$$g=X^3+b_2X^2+b_1X+b_0=(X-\beta_1)(X-\beta_2)(X-\beta_3)$$

la resolvente cúbica. Una serie de composición para el grupo de Galois de f sobre $\mathbb{Q}(a_3,a_2,a_1,a_0)$ es

$$G=S_4\trianglerighteq A_4\trianglerighteq V\trianglerighteq<(13)(24)>\trianglerighteq 1$$

El cuerpo fijo para V es $\mathbb{Q}(\beta_1,\beta_2,\beta_3)$, y las raíces de g pueden construirse por radicales ya que es una cúbica. Tenemos pues que estudiar la extensión $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)/\mathbb{Q}(\beta_1,\beta_2,\beta_3)$, cuyo grupo es V. Para construir las raíces α_i seguimos un proceso que trata simétricamente a los tres subgrupos de orden 2. Consideramos los elementos:

$$\begin{aligned}(\alpha_1+\alpha_2-\alpha_3-\alpha_4)^2&=(\textstyle\sum\alpha_i)^2-4(\beta_1+\beta_2)=a_3^2-4a_2+4\beta_3\\(\alpha_1-\alpha_2+\alpha_3-\alpha_4)^2&=(\textstyle\sum\alpha_i)^2-4(\beta_1+\beta_3)=a_3^2-4a_2+4\beta_2\\(\alpha_1-\alpha_2-\alpha_3+\alpha_4)^2&=(\textstyle\sum\alpha_i)^2-4(\beta_2+\beta_3)=a_3^2-4a_2+4\beta_1\end{aligned}$$

Formamos ahora el sistema:

$$\begin{aligned}\alpha_1+\alpha_2+\alpha_3+\alpha_4&=-a_3\\\alpha_1+\alpha_2-\alpha_3-\alpha_4&=\sqrt{a_3^2-4a_2+4\beta_3}\\\alpha_1-\alpha_2+\alpha_3-\alpha_4&=\sqrt{a_3^2-4a_2+4\beta_2}\\\alpha_1-\alpha_2-\alpha_3+\alpha_4&=\sqrt{a_3^2-4a_2+4\beta_1}\end{aligned}$$

y al resolverlo tenemos las raíces de f:

$$\alpha_1=\tfrac{1}{4}\left(-a_3+\sqrt{a_3^2-4a_2+4\beta_3}+\sqrt{a_3^2-4a_2+4\beta_2}+\sqrt{a_3^2-4a_2+4\beta_1}\right)$$

$$\alpha_2=\tfrac{1}{4}\left(-a_3+\sqrt{a_3^2-4a_2+4\beta_3}-\sqrt{a_3^2-4a_2+4\beta_2}-\sqrt{a_3^2-4a_2+4\beta_1}\right)$$

$$\alpha_3=\tfrac{1}{4}\left(-a_3-\sqrt{a_3^2-4a_2+4\beta_3}+\sqrt{a_3^2-4a_2+4\beta_2}-\sqrt{a_3^2-4a_2+4\beta_1}\right)$$

$$\alpha_4=\tfrac{1}{4}\left(-a_3-\sqrt{a_3^2-4a_2+4\beta_3}-\sqrt{a_3^2-4a_2+4\beta_2}+\sqrt{a_3^2-4a_2+4\beta_1}\right)$$

Observa que no son posibles todas las combinaciones de signos.
Cuando $a_3=0$, tenemos la solución dada por el método de Euler.

18.1. Ejercicios

Resolución de ecuaciones por radicales

Ejercicio. 18.9.
Resolver por radicales sobre $\mathbb{Q}$ *la ecuación* $X^4-2X^3-8X-3=0$.
Ref.: 4164e_009 SOLUCIÓN

Ejercicio. 18.10.
Usar las fórmulas de Cardano para resolver la ecuación $X^3+X^2-2=0$. *En particular demostrar que esa ecuación tiene la raíz real*

$$\frac{1}{3}(\sqrt[3]{26+15\sqrt{3}}+\sqrt[3]{26-15\sqrt{3}}-1)$$

Determinar por la regla de Ruffini directamente las raíces de la ecuación anterior y explicar lo que ocurre, comprobando que

$$\sqrt[3]{26+15\sqrt{3}}=2+\sqrt{3}, \qquad \sqrt[3]{26-15\sqrt{3}}=2-\sqrt{3}.$$

Ref.: 4164e_012 SOLUCIÓN

Ejercicio. 18.11.
Discriminante.
(1) Demostrar que el discriminante del polinomio $f(X)=X^n+aX+b$ *es*

$$\Delta(f)=(-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1}+(-1)^{n+1}(n-1)^{n-1}a^n).$$

(2) Calcular el grupo de Galois de los siguientes polinomios sobre $\mathbb{Q}$*:*
(I) X^5-X-1,
(II) $X^5+20X+16$.

Ref.: 4164e_014 SOLUCIÓN

19. Apéndice: Resolución de polinomios ciclotómicos

Veamos como resolver algunos polinomios ciclotómicos; esto sería parte de la teoría general de resolución de ecuaciones polinómicas, sin embargo las relaciones existentes entre las raíces hacen que la resolución de los polinomios consideramos sea especialmente fácil.

Ejemplo. 19.1.
Se considera

$$f = \Phi_5(X) = X^4 + X^3 + X^2 + X + 1 = \prod_{i=1}^{4}(X - \xi^i)$$

el quinto polinomio ciclotómico. Si las raíces son $\xi_i = \xi^i$. El cuerpo de descomposición es $E = \mathbb{Q}(\xi)$, el discriminante vale $\Delta = 5^3$ y el grupo $G = \mathrm{Gal}(f/\mathbb{Q})$ es cíclico de orden cuatro generado por $\sigma = (1\,2\,4\,3)$. La única serie de composición de G es: $G \trianglerighteq < (1\,4)(2\,3) > \trianglerighteq 1$. La torre de cuerpos que le corresponde es:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq E.$$

Como las extensiones intermedias son de grado 2, ya están en $\mathbb{Q}$ todas las raíces de la unidad necesarias. Formamos las resolventes de Galois:

$$\beta_1 = \xi + (-1)\sigma^2(\xi) = \xi - \xi^4$$
$$\beta_2 = \xi^2 + (-1)\sigma^2(\xi^2) = \xi^2 - \xi^3$$

Calculamos:

$$\beta_1^2 = \xi^2 + \xi^3 - 2,$$
$$\beta_2^2 = \xi^4 + \xi - 2$$

que son raíces del polinomio

$$(X - \beta_1^2)(X - \beta_2^2) = X^2 + 5X + 5.$$

Por otro lado, $\xi + \xi^4$ y $\xi^2 + \xi^3$ son raíces del polinomio:

$$(X - (\xi + \xi^4))(X - (\xi^2 + \xi^3)) = X^2 + X - 1$$

Resolviendo ambos polinomios formamos el sistema:

$$\xi + \xi^4 = \tfrac{-1+\sqrt{5}}{2}$$

$$\xi - \xi^4 = \sqrt{\tfrac{-5+\sqrt{5}}{2}}$$

con lo que llegamos a la expresión final:

$$\xi = \frac{1}{2}\left(\frac{-1+\sqrt{5}}{2} + \sqrt{\frac{-5+\sqrt{5}}{2}}\right).$$

4164-04.tex

Ejemplo. 19.2.
Sea

$$f = \Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = \prod_{i=1}^{6}(X - \xi^i)$$

el séptimo polinomio ciclotómico. Su discriminante vale $\Delta = -7^5$ y el grupo $G = \mathrm{Gal}(f/\mathbb{Q}) =< (1\,3\,2\,6\,4\,5) >$ donde llamamos $\xi_i = \xi^i$. G tiene dos series de composición y podemos resolverlo por cualquiera de ellas:

(1) Tomamos en primer lugar la serie

$$G \trianglerighteq < (1\,2\,4)(3\,6\,5) > \trianglerighteq 1.$$

El grupo intermedio es $G \cap A_6$ por lo que su cuerpo fijo es $F = \mathbb{Q}(\sqrt{-7})$. Nos queda la última extensión. Empezamos adjuntando la raíz cúbica de la unidad $\omega = (-1+\sqrt{-3})/2$. Las resolventes de Lagrange que necesitamos son:

$$\begin{aligned}\beta_0 &= \xi + \xi^2 + \xi^4\\ \beta_1 &= \xi + \omega\xi^2 + \omega^2\xi^4\\ \beta_2 &= \xi + \omega^2\xi^2 + \omega\xi^4\end{aligned}$$

El primero es raíz del polinomio X^2+X+2, luego $\beta_0 = (-1+\sqrt{-7})/2$. Calculando las potencias cúbicas, tenemos:

$$\begin{aligned}\beta_1^3 + \beta_2^3 &= 14\\ (\beta_1^3 - \beta_2^3)^2 &= 224 + 84\omega.\end{aligned}$$

Estableciendo y resolviendo el sistema lineal correspondiente nos queda:

$$\xi = \frac{1}{3}\left(\frac{-1+\sqrt{-7}}{2} + \sqrt[3]{7 + \sqrt{56+21\omega}} + \sqrt[3]{7 - \sqrt{56+21\omega}}\right)$$

Esta expresión se puede simplificar (¿o complicar?) observando que $\sqrt{56+21\omega} = (1+3\omega)\sqrt{-7}$.

(2) La otra serie de composición es la siguiente:

$$G \trianglerighteq < (1\,6)(2\,5)(3\,4) > \trianglerighteq 1.$$

En este caso el cuerpo fijo bajo el grupo intermedio es $\mathbb{Q} \cap F = \mathbb{Q}(\xi + \xi^6)$. Adjuntando la raíz cúbica ω, procedemos en dos pasos: En primer lugar, formamos el sistema

$$\begin{aligned}\xi + \xi^6 &= \xi_1\\ (\xi - \xi^6)^2 &= \beta_1\end{aligned}$$

El grupo cociente actúa sobre ξ_1 y β_1 dándonos tres conjugados. En cada caso formamos las resolventes de Lagrange correspondientes:

$$\begin{aligned}
\gamma_0 &= (\xi+\xi^6)+(\xi^3+\xi^4)+(\xi^2+\xi^5)\\
\gamma_1 &= (\xi+\xi^6)+\omega(\xi^3+\xi^4)+\omega^2(\xi^2+\xi^5)\\
\gamma_2 &= (\xi+\xi^6)+\omega^2(\xi^3+\xi^4)+\omega(\xi^2+\xi^5)
\end{aligned}$$

$$\begin{aligned}
\theta_0 &= (\xi-\xi^6)^2+(\xi^3-\xi^4)^2+(\xi^2-\xi^5)^2\\
\theta_1 &= (\xi-\xi^6)^2+\omega(\xi^3-\xi^4)^2+\omega^2(\xi^2-\xi^5)^2\\
\theta_0 &= (\xi-\xi^6)^2+\omega^2(\xi^3-\xi^4)^2+\omega(\xi^2-\xi^5)^2
\end{aligned}$$

y calculamos:

$$\begin{aligned}
\gamma_0 &= -1 & \theta_0 &= -7\\
\gamma_1^3 &= -7-21\omega & \theta_1^3 &= -7-21\omega\\
\gamma_2^3 &= -7-21\omega^2 & \theta_2^3 &= -7-21\omega^2
\end{aligned}$$

Resolviendo los sucesivos sistemas lineales:

$$\begin{aligned}
\xi+\xi^6 &= \tfrac{1}{3}\left(-1+\sqrt[3]{-7-21\omega}+\sqrt[3]{-7-21\omega^2}\right)\\
\xi-\xi^6 &= \sqrt{\tfrac{1}{3}\left(-7+\sqrt[3]{-7-21\omega}+\sqrt[3]{-7-21\omega^2}\right)}
\end{aligned}$$

$$\xi = \frac{1}{2}\left(\frac{1}{3}\left(-1+\sqrt[3]{-7-21\omega}+\sqrt[3]{-7-21\omega^2}\right)+\sqrt{\frac{1}{3}\left(-7+\sqrt[3]{-7-21\omega}+\sqrt[3]{-7-21\omega^2}\right)}\right)$$

Ejemplo. 19.3.
Consideramos ahora el undécimo polinomio ciclotómico. Sea

$$f=\Phi_{11}=\prod_{i=1}^{10}(X-\xi^i),$$

siendo ξ una raíz undécima primitiva de la unidad. Sea $E=\mathbb{Q}(\xi)$ su cuerpo de descomposición. Numeramos a las raíces como $\xi_i=\xi^i$. El discriminante vale $\Delta=-11^9$ y $G=\mathrm{Gal}(E/\mathbb{Q})=<\sigma\mid \sigma(\xi)=\xi^2>$ es cíclico de orden 10. Tiene dos series de composición. Vamos a usar la siguiente:

$$G\trianglerighteq<\sigma^2>\trianglerighteq 1.$$

El grupo intermedio es cíclico de orden 5. La torre de cuerpos que le corresponde es:

$$\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{-11})\subseteq E.$$

El primer eslabón es una extensión cuadrática que ya está expresada explícitamente, así que nos concentramos en el segundo que es una extensión cíclica de orden 5. Adjuntamos una raíz quinta primitiva de la unidad ξ para poder aplicar el teorema de Lagrange. Formamos las resolventes de Galois siguientes:

$$\begin{aligned}
\beta_1 &= \xi+\xi\sigma^2(\xi)+\xi^2\sigma^4(\xi)+\xi^3\sigma^6(\xi)+\xi^4\sigma^8(\xi) &&= \xi+\xi\xi^4+\xi^2\xi^5+\xi^3\xi^9+\xi^4\xi^3\\
\beta_2 &= \sigma(\xi)+\xi\sigma^3(\xi)+\xi^2\sigma^5(\xi)+\xi^3\sigma^7(\xi)+\xi^4\sigma^9(\xi) &&= \xi^2+\xi\xi^8+\xi^2\xi^{10}+\xi^3\xi^7+\xi^4\xi^6.
\end{aligned}$$

Los elementos β_1^5, β_2^5 son conjugados y pertenecen a $\mathbb{Q}(\sqrt{-11}, \xi)$. Para encontrar su expresión explícita calculamos el polinomio

$$h = (X - \beta_1^5)(X - \beta_2^5) = X^2 - (110\xi^2 + 220\xi + 264)X + (3135\xi^3 - 165\xi^2 + 2035\xi + 1738)$$

y lo resolvemos por radicales. Nos queda:

$$\begin{aligned}\beta_1^5 &= (55\xi^2 + 110\xi + 132) + (10\xi^3 + 40\xi^2 + 20\xi - 7)\sqrt{-11}\\ \beta_2^5 &= (55\xi^2 + 110\xi + 132) - (10\xi^3 + 40\xi^2 + 20\xi - 7)\sqrt{-11}\end{aligned}$$

Para encontrar la expresión explícita para ξ resolvemos el sistema:

$$\begin{aligned}\xi + \xi^4 + \xi^5 + \xi^9 + \xi^3 &= \tfrac{1}{2}\left(-1 + \sqrt{-11}\right)\\ \xi + \xi\xi^4 + \xi^2\xi^5 + \xi^3\xi^9 + \xi^4\xi^3 &= \sqrt[5]{(55\xi^2 + 110\xi + 132) + (10\xi^3 + 40\xi^2 + 20\xi - 7)\sqrt{-11}}\\ \xi + \xi^2\xi^4 + \xi^4\xi^5 + \xi\xi^9 + \xi^3\xi^3 &= \sqrt[5]{(55\xi^4 + 110\xi^2 + 132) + (10\xi + 40\xi^4 + 20\xi^2 - 7)\sqrt{-11}}\\ \xi + \xi^3\xi^4 + \xi\xi^5 + \xi^4\xi^9 + \xi^2\xi^3 &= \sqrt[5]{(55\xi + 110\xi^3 + 132) + (10\xi^4 + 40\xi + 20\xi^3 - 7)\sqrt{-11}}\\ \xi + \xi^4\xi^4 + \xi^3\xi^5 + \xi^2\xi^9 + \xi\xi^3 &= \sqrt[5]{(55\xi^3 + 110\xi^4 + 132) + (10\xi^2 + 40\xi^3 + 20\xi^4 - 7)\sqrt{-11}}\end{aligned}$$

y la suma de todas las ecuaciones dividida por cinco proporciona la expresión buscada. Este es el primer ejemplo de resolución por raíces quínticas que encontramos, y siendo el más sencillo de todos, implica cálculos bastante pesados.

Para acortar la presentación de los cálculos, cuando tengamos una extensión cuadrática, cúbica u otra que hayamos tratado con anterioridad, calcularemos un polinomio cuyas raíces generen dicha extensión, pero no hallaremos expresiones explícitas para ellas.

Ejemplo. 19.4.
Sea

$$f = \Phi_{13} = \prod_{i=1}^{n}(X - \xi^i),$$

siendo ξ una raíz decimotercera primitiva de la unidad. El discriminante vale $\Delta = 13^{11}$. Como antes, numeramos las raíces como $\xi_i = \xi^i$. Sea $E = \mathbb{Q}(\xi)$ el cuerpo de descomposición y sea $G = \mathrm{Gal}(E/\mathbb{Q})$. Sabemos que $G =< \sigma >$, donde $\sigma(\xi) = \xi^2$. Este grupo tiene tres series de composición, de las que escogemos la siguiente:

$$G \trianglerighteq < \sigma^2 > \trianglerighteq < \sigma^6 > \trianglerighteq 1.$$

Los índices de esta serie son 2, 3, 2. Como permutacion de las raíces, σ es un ciclo de longitud 12, luego es impar, mientras que σ^2 es par. Por tanto el segundo grupo de la serie anterior es la intersección de G con A_{13}. Al tercer grupo le corresponde el cuerpo $E \cap F$. En resumen a la serie de composición anterior le corresponde la torre de cuerpos siguiente:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{13}) \subseteq \mathbb{Q}(\xi + \xi^{-1}) \subseteq E.$$

El elemento ξ se obtiene a partir de $\alpha = \xi + \xi^{-1}$ como raíz del polinomio $(X - \xi)(X - \xi^{-1}) = X^2 - \alpha X + 1$. Resolviendo:

$$\xi = \frac{\alpha + \sqrt{\alpha^2 - 4}}{2} \tag{IV.5}$$

La primera extensión ya está expresada por un radical cuadrático, así que sólo nos falta la intermedia. Sea $\omega = (-1+\sqrt{-3})/2$ una raíz cúbica primitiva de la unidad. La adjuntamos y formamos la resolvente de Galois:

$$\beta = \alpha + \omega\sigma^2(\alpha) + \omega^2\sigma^4(\alpha) = (\xi + \xi^{-1}) + \omega(\xi^4 + \xi^{-4}) + \omega^2(\xi^3 + \xi^{-3}).$$

El elemento β^3 pertenece a $\mathbb{Q}(\sqrt{13}, \omega)$. Elevando al cubo y reduciendo los coeficientes nos queda

$$\beta^3 = 13 + \sqrt{13(7+15\omega)} = 13 + (4+3\omega)\sqrt{13}.$$

Por otra parte, calculamos los coeficientes del polinomio:

$$(X - (\alpha + \sigma^2(\alpha) + \sigma^4(\alpha))(X - (\sigma(\alpha) + \sigma^3(\alpha) + \sigma^5(\alpha)) = X^2 + X - 3$$

de donde obtenemos la expresión explícita de sus raíces. Finalmente establecemos el sistema lineal:

$$\begin{array}{ll} \alpha + \sigma^2(\alpha) + \sigma^4(\alpha) & = \frac{1}{2}(-1+\sqrt{13}) \\ \alpha + \omega\sigma^2(\alpha) + \omega^2\sigma^4(\alpha) & = \sqrt[3]{13 + (4+3\omega)\sqrt{13}} \\ \alpha + \omega^2\sigma^2(\alpha) + \omega\sigma^4(\alpha) & = \sqrt[3]{13 + (4+3\omega^2)\sqrt{13}} \end{array}$$

Sumando las ecuaciones de este sistema y dividiendo por tres, obtenemos la expresión explícita para α que sustituida en (IV.5) proporciona la expresión por radicales para ξ.

Ejemplo. 19.5.
Sea el decimoséptimo polinomio ciclotómico:

$$f = \Phi_{16} = \prod_{i=1}^{16}(X - \xi^i),$$

y sea $E = \mathbb{Q}(\xi)$ su cuerpo de descomposición. El grupo $G = \mathrm{Gal}(E/\mathbb{Q})$ es cíclico de orden 16 generado por σ tal que $\sigma(\xi) = \xi^3$. La única serie de composición es:

$$G \trianglerighteq < \sigma^2 > \trianglerighteq < \sigma^4 > \trianglerighteq < \sigma^8 > \trianglerighteq 1$$

Todos los factores de composición son cíclicos de orden 2, así que las raíces de la unidad necesarias son 1 y -1. La torre de cuerpos correspondiente es:

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha) \subseteq E,$$

siendo:

$$\begin{array}{l} \alpha = \xi + \sigma^8(\xi) = \xi + \xi^{16} \\ \beta = \alpha + \sigma^4(\alpha) = \xi + \xi^4 + \xi^{13} + \xi^{16} \\ \gamma = \beta + \sigma^2(\beta) = \xi + \xi^2 + \xi^4 + \xi^8 + \xi^9 + \xi^{13} + \xi^{15} + \xi^{16} \end{array}$$

Obsérvese que $\mathbb{Q}(\gamma)$ debe ser $\mathbb{Q}(\sqrt{17})$ y que $\mathbb{Q}(\alpha) = E \cap F$. Cada uno de los elementos anteriores es raíz del polinomio correspondiente siguiente:

$$\begin{aligned}(X-\xi)(X-\sigma^8(\xi)) &= X^2 - \alpha X + 1\\ (X-\alpha)(X-\sigma^4(\alpha)) &= X^2 - \beta X + \tfrac{1}{2}(-\beta^3 + 6\beta - 3)\\ (X-\beta)(X-\sigma^2(\beta)) &= X^2 - \gamma X - 1\\ (X-\gamma)(X-\sigma(\gamma)) &= X^2 + X - 4\end{aligned}$$

Resolviendo hacia arriba por las fórmulas de Baskhara:

$$\gamma = \tfrac{-1+\sqrt{17}}{2}$$

$$\beta = \tfrac{\gamma+\sqrt{\gamma^2+4}}{2}$$

$$\alpha = \tfrac{\beta+\sqrt{2\beta^3+\beta^2+12\beta-6}}{2}$$

$$\xi = \tfrac{\alpha+\sqrt{\alpha^2-4}}{2}$$

Realizando todas las operaciones obtenemos explícitamente:

$$\alpha = \frac{1}{8}\left(-1+\sqrt{17}+\sqrt{2(17-\sqrt{17})}+2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-\sqrt{2(17+\sqrt{17})}}\right)$$

y a partir de esta expresión podemos obtener una expresión explícita para ξ. Obsérvese la elección de signo de los radicales, que no son todos los posibles como ya se explica antes.

19.1. Ejercicios

Resolución de polinomios ciclotómicos

19.2. Cuestiones

En las siguientes cuestiones responde "VERDADERO" ó "FALSO" y haz un breve razonamiento para justificar la respuesta.

(1) ☐ Si $f(X) \in \mathbb{Q}[X]$ es una cúbica irreducible y $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathbb{Z}_3$, entonces todos los ceros de $f(X) = 0$ son reales. (Ref.: 4164q_001)

(2) ☐ Si $\mathrm{Car}(K) = 0$, entonces $X^8 + aX^6 + bX^4 + cX^2 + d = 0$ es soluble por radicales sobre K. (Ref.: 4164q_002)

(3) ☐ La ecuación $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = 0$ es soluble por radicales sobre $\mathbb{Q}$. (Ref.: 4164q_003)

(4) ☐ Si $f \in \mathbb{Q}[X]$ es una cúbica irreducible con una única raíz real, entonces $\mathrm{Gal}(f/\mathbb{Q}) \cong S_3$. (Ref.: 4164q_004)

(5) ☐ Si $f(X)$ un polinomio sobre $\mathbb{Q}$ con grupo de Galois isomorfo a D_n, entonces $f(X)$ es soluble por radicales. (Ref.: 4164q_005)

(6) ☐ Si $f(X)$ un polinomio sobre $\mathbb{Q}$ con grupo de Galois isomorfo a A_n, entonces $f(X)$ es soluble por radicales. (Ref.: 4164q_006)

(7) ☐ Si F es un cuerpo de característica p todo polinomio irreducible $f(X) \in F[X]$ es soluble por radicales. (Ref.: 4164q_007)

(8) ☐ Si $f(X) \in K[X]$ es un polinomio separable de grado n, $\mathrm{car}(K) \neq 2$, y $\mathrm{Discr}(f(X))$ es un cuadrado en K, entonces $\mathrm{Gal}(f/K) = A_n$. (Ref.: 4164q_008)

(9) ☐ Sea $f \in \mathbb{Q}[X]$ un polinomio irreducible de grado $n \leq 5$ tal que $\mathbb{Q}(f) = \mathbb{Q}(\alpha)$, siendo α una raíz de f. En este caso siempre se tiene $\mathrm{Gal}(f/\mathbb{Q}) \cong C_n$. (Ref.: 4164q_009)

(10) ☐ El grupo de Galois de $\mathbb{Q}(X^5 - 5)/\mathbb{Q}$ es isomorfo a D_5. (Ref.: 4164q_010)

(11) ☐ El grupo de Galois de $\mathbb{Q}(X^5 - 5)/\mathbb{Q}$ es isomorfo a F_{20}. (Ref.: 4164q_011)

(12) ☐ Para el polinomio $f(X) = X^3 - 1 \in \mathbb{Q}[X]$ se verifica que $\mathrm{Gal}(f/\mathbb{Q})$ es un subgrupo transitivo de S_3. (Ref.: 4164q_012)

(13) ☐ Para cada extensión $E/\mathbb{Q}$, cíclica de grado 3 (de Galois), existe un elemento $\alpha \in E$ tal que $E = K(\alpha)$ e $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^3 - a \in \mathbb{Q}[X]$. (Ref.: 4164q_014)

(14) ☐ Recordar que si $f(X)$ es un polinomio en $\mathbb{Q}$ con cuerpo de descomposición E, el grupo de Galois de $f(X)$ es el grupo de la extensión $E/\mathbb{Q}$. El grupo de Galois de $X^4 + 27X^3 - 3X + 6$ sobre $\mathbb{Q}$ tiene orden un múltiplo de 4. (Ref.: 4164q_026)

4164-99.tex

(15) ☐ Las raíces de un polinomio cúbico sobre un cuerpo K de característica cero pueden siempre obtenerse mediante suma, resta, multiplicación, división y extracción de raíces cuadradas a partir de elementos de K. (Ref.: 4164q_051)

(16) ☐ Si K es un cuerpo de característica cero, un polinomio $f(X) \in K[X]$ es soluble por radicales si, y sólo si, su cuerpo de descomposición E en $\overline{K}$ verifica que $\mathrm{Gal}(E/K)$ es un grupo soluble. (Ref.: 4164q_052)

(17) ☐ $\mathrm{Gal}(X^{17} - 5/\mathbb{Q})$ es un grupo soluble. (Ref.: 4164q_062)

Capítulo V

Extensiones trascendentes

Introducción

Introducción.

4165-00.tex

20. Operador dimensión

Dado un conjunto C, consideramos $\mathscr{P}(C)$, el conjunto potencia de C, esto es, el conjunto de todos los subconjuntos de C.

Un **operador dimensión** en C es una aplicación $d : \mathscr{P}(C) \longrightarrow \mathscr{P}(C)$, que verifica las siguientes propiedades, en las que representamos $d(X) = X^d$ para cada $X \subseteq C$:

(I) Para cada $X \subseteq C$ se tiene $X \subseteq X^d$.
(II) Para cada $X \subseteq C$ se tiene $X^d = X^{dd}$.
(III) Si $X \subseteq Y \subseteq C$, entonces $X^d \subseteq Y^d$.
(IV) Para cada $X \subseteq C$ se tiene $X^d = \cup\{Y^d \mid Y \in \mathscr{P}_F(X)\}$, donde $\mathscr{P}_F(X)$ es el conjunto de los subconjuntos finitos de X.
(V) (**Axioma de intercambio**). Para cada $X \subseteq C$, si $y \in (X \cup \{x\})^d \setminus X^d$, entonces $x \in (X \cup \{y\})^d$.

Ejemplo. 20.1.
Para cada conjunto C, la aplicación identidad $\mathrm{id} : \mathscr{P}(C) \longrightarrow \mathscr{P}(C)$, es un operador dimensión.

Ejemplo. 20.2.
Para cada conjunto C, la aplicación $d_C : \mathscr{P}(C) \longrightarrow \mathscr{P}(C)$, definida $d_C(X) = C$, para cada $X \subseteq C$, es un operador dimensión.

Ejemplo. 20.3.
Para cada espacio vectorial V sobre un cuerpo K definimos $g : \mathscr{P}(V) \longrightarrow \mathscr{P}(V)$ mediante $g(X) = KX$, el subespacio vectorial generado por X; se tiene que g es un operador dimension. En este caso (v) se conoce como la **propiedad de intercambio de Steinitz**.

Dado un operador dimensión d en un conjunto C, un subconjunto $X \subseteq C$ se llama:

- un subconjunto d**–libre**, si para todo $x \in X$ se tiene $x \notin (X \setminus \{x\})^b$.
- un subconjunto d**–denso**, si $X^d = C$.
- una d**–base**, si es d–libre y d–denso.

En lo que sigue omitiremos el uso de d el referirnos a estos conceptos.

Ejemplo. 20.4.
Para el operador dimensión id del Ejemplo (20.1.) todo subconjunto de C es libre y el único subconjunto denso es el propio C, por lo tanto C es una base.

Ejemplo. 20.5.
Para el operador d_C del Ejemplo (20.2.) el único subconjunto libre es $\varnothing$, y todos los subconjuntos son densos, por lo tanto $\varnothing$ es una base.

Ejemplo. 20.6.
Para el operador dimensión del Ejemplo (20.3.), un subconjunto es libre si, y sólo si, es linealmente independiente, y es denso si, y sólo si, es un sistema de generadores; por lo tanto las bases son los subconjuntos linealmente independientes que son sistemas de generadores, esto es, las base del espacio vectorial.

4165-01.tex

Ejemplo. 20.7.
Para cada operador dimensión d sobre un conjunto C se tiene que $\varnothing$ es siempre libre y C es siempre denso.

Lema. 20.8.
Sea d un operador dimensión en un conjunto C, se verifica:
(1) Si $X \subseteq Y \subseteq C$ e Y es libre, entonces X es libre.
(2) Si $X \subseteq Y \subseteq C$ y X es denso, entonces Y es libre.
(3) Si $X \subseteq C$, entonces X es denso si, y sólo si, X^d es denso.

Lema. 20.9.
Sea d un operador dimensión en un conjunto C, si $\{X_i \mid i \in I\}$ es una familia dirigida superiormente de subconjuntos libres de C, entonces $\cup_i X_i$ es libre.

DEMOSTRACIÓN. Supongamos que $\cup_i Xi$ no es libre, existe $x \in \cup_i X_i$ tal que $x \in (\cup_i X_i \setminus \{x\})^d$, por tanto existe $F \subseteq \cup_i X_i$, finito, tal que $x \in F^d$, y $F \cup \{x\} \subseteq \cup_i X_i$ es finito, por lo que existe un índice j tal que $F \cup \{x\} \subseteq X_j$, y se tiene $X \subseteq X_j \setminus \{x\}$ y $x \in F^d \subseteq (X_j \setminus \{x\})^d$, por lo que X_j no sería libre, lo que es una contradicción. □

Corolario. 20.10.
Sea d un operador dimensión en un conjunto C, si $X \subseteq C$, y cada subconjunto finito de X es libre, entonces X es libre.

DEMOSTRACIÓN. Tenemos que X es la unión de sus subconjuntos finitos. □

Proposición. 20.11.
Sea d un operador dimensión en un conjunto C, si $X \subseteq C$ es libre y $x \in C \setminus X^d$, entonces $X \cup \{x\}$ es libre.

DEMOSTRACIÓN. Si $X \cup \{x\}$ no es libre, existe $y \in X \cup \{x\}$ tal que $y \in ((X \cup \{x\}) \setminus \{y\})^d$. Ya que $x \notin X^d$, se tiene $x \notin X$. Existen dos casos posibles:
Caso 1. $x = y$, entonces $x \in ((X \cup \{x\}) \setminus \{x\})^d = X^d$, lo que es imposible.
Caso 2. $x \neq y$, entonces $y \in X$, y como X es libre, se tiene $y \notin (X \setminus \{y\})^d$. Se tiene $(X \cup \{x\}) \setminus \{y\} = (X \setminus \{y\}) \cup \{x\}$, y por tanto $y \in ((X \setminus \{y\}) \cup \{x\})^d \setminus (X \setminus \{y\})^d$, y como consecuencia, ver axioma (v), se tiene $x \in ((X \setminus \{y\}) \cup \{y\})^d = X^d$, lo que es una contradicción. □

Proposición. 20.12.
Sea d un operador dimensión en un conjunto C, y $B \subseteq C$ un subconjunto, son equivalentes:
(a) B es una base.
(b) B es minimal en el conjunto de los subconjuntos densos.
(c) B es maximal en el conjunto de los subconjuntos libres.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si B es una base y no es un subconjunto denso minimal, existe un subconjunto denso $D \subsetneq B$, sea $x \in B \setminus D$, entonces $x \notin (B \setminus \{x\})^d \supseteq D^d = C$, lo que es una contradicción.
(b) $\Rightarrow$ (c). Primero veamos que B es libre. Si B no es libre, existe $x \in B$ tal que $x \in (B \setminus \{x\})^d$, entonces $B = (B \setminus \{x\}) \cup \{x\} \subseteq (B \setminus \{x\})^d$, y por tanto $B \setminus \{x\}$ es denso, lo que contradice la minimalidad de B. Veamos ahora que B es maximal entre los subconjuntos libre. Si $B \subsetneq L$, veamos que L no es libre. Tomamos $x \in L \setminus B$, luego $B \subseteq L \setminus \{x\}$, y se tiene que $L \setminus \{x\}$ es denso, por tanto $x \in (L \setminus \{x\})^d$.
(b) $\Rightarrow$ (a). Tenemos que ver que B es denso. Si $B^d \neq C$, sea $x \in C \setminus B^d$; vamos a ver que $B \cup \{x\}$ es libre, lo que es una contradicción. Para $y \in B \cup \{x\}$, si $y \in ((B \cup \{x\}) \setminus \{y\})^d$, estudiamos dos casos:
Caso 1. $x = y$, entonces $x \in ((B \setminus \{x\}) \cup \{x\})^b = B^d$, lo que es una contradicción.
Caso 2. $x \neq y$, entonces $y \in ((B \cup \{x\}) \setminus \{y\})^d = ((B \setminus \{y\}) \cup \{x\})^d$, además $y \notin (B \setminus \{y\})^d$, ya que B es libre. Por el axioma (v) se tiene $x \in ((B \setminus \{y\}) \cup \{y\})^d = B^d$, lo que es una contradicción. Como consecuencia $B \cup \{x\}$ es libre. □

Teorema. 20.13.
Sea d un operador dimensión en un conjunto C, $L \subseteq C$ un subconjunto libre y $D \subseteq C$ un subconjunto denso. Existe un subconjunto $B \subseteq D$ tal que $B \cup L$ es una base y $B \cap L = \emptyset$.

DEMOSTRACIÓN. Llamamos $\Gamma = \{X \subseteq D \mid X \cup L \text{ es libre y } X \cap L = \emptyset\}$. Es claro que $\emptyset \in \Gamma$ y que si $\{X_i \mid i \in I\}$ es una cadena en Γ, por el Lema (20.9.), se tiene que $\cup_i X_i \in \Gamma$, por lo tanto Γ es un conjunto inductivo y existen en Γ elementos maximales. Sea $B \in \Gamma$ maximal.
Por hipótesis $B \cup L$ es libre, veamos que es denso. Supongamos que $B \cup L$ no es denso, entonces $D \nsubseteq (B \cup L)^d$, sea $x \in D \setminus (B \cup L)^d$. Como $B \cup L$ es libre, por la Proposición (20.11.) se tiene que

$B \cup L \cup \{x\}$ es libre. Por tanto, al considerar $B \cup \{x\} \subseteq D$, si probamos que $L \cap (B \cup \{x\}) = \emptyset$, tendremos un elemento de Γ que contradice la maximalidad de B. Es claro que se tiene $L \cap (B \cup \{x\}) = (L \cap B) \cup (L \cap \{x\}) = \emptyset$. □

Corolario. 20.14.
Sea d un operador dimensión en un conjunto C, $L \subseteq C$ un subconjunto libre y $D \subseteq C$ un subconjunto denso tales que $L \subseteq D$, existe una base $B \subseteq C$ verificando $L \subseteq B \subseteq D$.

Corolario. 20.15.
Sea d un operador dimensión en un conjunto C, se verifica:
(1) Cada subconjunto libre está contenido en una base.
(2) Cada subconjunto denso contiene una base.
(3) Existe una base en C.

DEMOSTRACIÓN. Es consecuencia del corolario anterior y de que $\emptyset$ es un subconjunto libre y C un subconjunto denso. □

Teorema. 20.16.
Sea d un operador dimensión en un conjunto C, cada dos bases de C tienen el mismo cardinal.

DEMOSTRACIÓN. Estudiamos dos casos.

Caso 1. Existe una base con cardinal finito.

Sea B una base finita, podemos tomar B con el menor número de elementos, sea E otra base; si $|B| < |E|$, existe $x \in E \setminus B$; por la hipótesis $E \setminus \{x\}$ no es denso, y se tiene $B \nsubseteq (E \setminus \{x\})^d$. Sea $y \in B \setminus (E \setminus \{x\})^d$, entonces $(E \setminus \{x\}) \cup \{y\}$ es libre; vamos a ver que es denso. Se tiene $y \in E^d \setminus (E \setminus \{x\})^d = ((E \setminus \{x\}) \cup \{x\})^d \setminus (E \setminus \{x\})^d$, y por el axioma (v), se tiene que $x \in ((E \setminus \{x\}) \cup \{y\})^d$. Entonces $C = E^d = (E \setminus \{x\}) \cup \{x\})^d \subseteq ((E \setminus \{x\}) \cup \{y\})^d$, y $(E \setminus \{x\}) \cup \{y\}$ es denso. De este forma tenemos una nueva base, $(E \setminus \{x\}) \cup \{y\}$ con los mismos elementos que E, y que tiene en común con B un elemento más que la base E; repitiendo el proceso llegamos a dos bases: $B \subseteq E$ con $|B| < |E|$, lo que es una contradicción.

Caso 2. No existen bases con cardinal finito.

Sean B y E dos bases, ambas infinitas, veamos que $|B| \leq |E|$. Tenemos $E \subseteq B^d$, luego para cada $x \in E$ existe un conjunto finito $B_x \subseteq B$ tal que $x \in (B_x)^d$. Si llamamos $B' = \cup\{B_x \mid x \in E\} \subseteq B$, se tiene $E \subseteq (B')^d$, por lo que B' es un subconjunto denso, y por ser B una base, se tiene $B' = B$; en consecuencia $|B| \leq |E|$. □

Referencia: Bastida, [3].

21. Extensiones trascendentes

Dada una extensión de cuerpos F/K, vamos a introducir un operador dimensión $d = d_K$ en F definido como $d_K(X) =$ clausura algebraica en F de $K(X)$.

Lema. 21.1.
Con la notación anterior, $d = d_K$ es un operador dimensión.

DEMOSTRACIÓN. Vamos a probar el axioma (iv). Dado $X \subseteq F$ y $x \in X^d$, se tiene que x es algebraico sobre $K(X)$, y existen $x_1, \dots, x_t \in X$ tales que x es algebraico sobre $K(x_1, \dots, x_t)$, luego $x \in K(x_1, \dots, x_t)^d$.
Vamos a probar el axioma (v). Dado $X \subseteq F$ y $x, y \in F$ tales que $y \in (X \cup \{x\})^d \setminus X^d$, esto es, y es algebraico sobre $K(X \cup \{x\})$, y por tanto existen $x_1, \dots, x_t \in X$ tales que y es algebraico sobre $K(x_1, \dots, x_t, x)$, y es trascendente sobre $K(X)$. Existe una expresión $\sum_{i=0}^{t} f_i y^i = 0$, con $f_i \in K[x_1, \dots, x_t, x]$, no todos nulos; si $f_i = \sum_{j=0}^{s_i} g_{ij} x^j$, entonces $0 = \sum_i \sum_j g_{ij} x^j y^i$, con los $g_{ij} \in K[x_1, \dots, x_t]$ no todos nulos. Tenemos la expresión $0 = \sum_j \sum_i g_{ij} y^i x^j$, y como no todos los g_{ij} son nulos, tenemos que algún $\sum_i g_{ij} y^i \neq 0$, ya que y es trascendente sobre $K(x_1, \dots, x_t)$. Tenemos entonces que x es algebraico sobre $K(x_1, \dots, x_t, y)$, luego $x \in (X \cup \{y\})^d$. □

Vamos a identificar los subconjuntos libres y densos en una extensión de cuerpos F/K. Recordemos que un subconjunto $X \subseteq F$ es **algebraicamente independiente** si para cada subconjunto finito $\{x_1, \dots, x_t\} \subseteq X$ el homomorfismo $h : K[X_1, \dots, X_t] \longrightarrow F$, definido por $h(X_i) = x_i$ para $i = 1, \dots, t$, tiene núcleo zero.

Proposición. 21.2.
Sea F/K una extensión de cuerpos y $d = d_k$ el operador dimensión en F. Para $X \subseteq F$ se verifica:
(1) $X \subseteq F$ es denso si, y sólo si, $F/K(X)$ es una extensión algebraica.
(2) $X \subseteq F$ es libre si, y sólo si, X es algebraicamente independiente sobre K.

DEMOSTRACIÓN. (1). Tenemos que $X \subseteq F$ es denso si, y sólo si, $X^d = F$ si, y sólo si, $F/K(X)$ es una extensión algebraica.
(2).
($\Rightarrow$). Supongamos que $X \subseteq F$ es algebraicamente dependiente, existen $x_1, \dots, x_t \in X$ y un polinomio no nulo $f \in K[X_1, \dots, X_t]$ tales que $f(x_1, \dots, x_t) = 0$. Supongamos que t es el mínimo, y vamos a

4165-02.tex

probar que $Y = \{x_1, \dots, x_t\}$ no es libre, por lo que tampoco lo será X. Hacemos la demostración por inducción sobre t. Si $t = 1$, entonces x_1 es algebraico sobre K, y se tiene $x_1 \in K(\varnothing) = \varnothing^d$; en este caso $\varnothing = Y \setminus \{x_1\}$. Supongamos que $t > 1$, y que el resultado es cierto para $t-1$, vamos a probar que $x_t \in (Y \setminus \{x_t\})^d$. Escribimos $0 = f(x_1, \dots, x_t) = \sum_{i=0}^{s} f_i x_t^i$, con $f_i = f_i(x_1, \dots, x_{t-1}) \in K[x_1, \dots, x_{t-1}]$. Si $f_i(x_1, \dots, x_{t-1}) = 0$, entonces $f_i(X_1, \dots, X_{t-1}) = 0$, ya que $\{x_1, \dots, x_{t-1}\}$ es algebraicamente independiente, por lo que no todos los $f_i(x_1, \dots, x_{t-1})$ son nulos. Tenemos entonces que x_t es raíz de $0 \neq \sum_i f_i(x_1, \dots, x_{t-1}) X^i \in K(x_1, \dots, x_{t-1})[X]$, y x_t es algebraico sobre $K(x_1, \dots, x_{t-1})$, esto es, $x_t \in (X \setminus \{x_t\})^d$.

($\Leftarrow$). Supongamos que $X \subseteq F$ no es libre, existe un subconjunto finito $Y \subseteq X$ que no es libre. Sea $x \in Y$ tal que $x \in (Y \setminus \{x\})^d$, esto es, x es algebraico sobre $K(Y \setminus \{x\})$. Si llamamos $\{x_1, \dots, x_t\} = Y \setminus \{x\}$, existe una expresión $0 = \sum_{i=0}^{s} f_i(x_1, \dots, x_t) x_i$, con $f_i(x_1, \dots, x_t) \in K[x_1, \dots, x_t]$ no todos nulos. Vamos a ver que Y es algebraicamente dependiente. Hacemos inducción sobre t. Si $t = 0$, entonces x es algebraico sobre K. Supongamos que $t > 0$, y que el resultado es cierto para $t - 1$. De la expresión $0 = \sum_{i=0}^{s} f_i(x_1, \dots, x_{t-1}) x^i$ se obtiene un polinomio no nulo $f = \sum_{i=0}^{s} f_i(X_1, \dots, X_{t-1}) X^i \in K[X_1, \dots, X_{t-1}, X]$ tal que $f(x_1, \dots, x_{t-1}, x) = 0$, y por tanto Y es algebraicamente dependiente.

□

Dada una extensión F/K, una **base de trascendencia** es una base de F para el operador dimensión $d = d_K$, llamamos **grado de trascendencia** de la extensión, y lo representamos por $\operatorname{tgr}(F/K)$ al cardinal de una base de trascendencia.

Proposición. 21.3.
Sea F/K una extensión finitamente generada, se verifica:
(1) $\operatorname{tgr}(F/K)$ *es finita.*
(2) Si B es una base de trascendencia de la extensión F/K, entonces $[F : K(B)]$ es finito.

DEMOSTRACIÓN. (1). Como tenemos $F = K(X)$, para un conjunto finito $X \subseteq F$, entonces $X \subseteq F$ es un subconjunto denso, y por tanto existe una base $B \subseteq X$, que necesariamente es finita.
(2). Como $F = K(X)$ para un conjunto finito $X \subseteq F$, entonces $F = K(B)(X)$, y como $F/K(B)$ es una extensión algebraica finitamente generada, resulta que $F/K(B)$ es finita. □

Corolario. 21.4.
Sea F/K una extensión finitamente generada, $B \subseteq F$ una base de trascendencia, y $X \subseteq F$ un subconjunto tal que $F = K(X)$. Existe $Y \subseteq X$, finito, tal que $F = K(B \cup Y)$ y $B \cap Y = \varnothing$.

DEMOSTRACIÓN. Consideramos la torre de cuerpos $K \subseteq K(B) \subseteq F$, ya conocemos que $[F : K(B)]$ es finito, y para cada $Y \subseteq X \setminus B$, finito, tenemos $K(B) \subseteq K(B)(Y) \subseteq F$, y podemos tomar Y con

$[K(B)(Y) : K(B)]$ máximo. Vamos a probar que $K(B)(Y) = F$. Si existe $x \in F \setminus K(B)(Y)$, podemos tomar $x \in X \setminus B$; si definimos $Y' = Y \cup \{x\}$, es claro que $Y \subseteq X \setminus B$ y $K(B)(Y) \subsetneq K(B)(Y') \subseteq F$, lo que es una contradicción. En consecuencia, $K(B)(Y) = F$, y tenemos el resultado. □

Proposición. 21.5.
Sea $K \subseteq F \subseteq E$ una torre de cuerpos, se verifica:

(1) Si B_F y B_E son bases de trascendencia de las extensiones F/K y E/F, respectivamente, entonces $B_F \cap B_E = \varnothing$ y $B_F \cup B_E$ es una base de trascendencia de la extensión E/K.
(2) $\operatorname{tgr}(E/K) = \operatorname{tgr}(F/K) + \operatorname{tgr}(E/F)$.

DEMOSTRACIÓN. Es claro que $B_F \cap B_E = \varnothing$ y que $B_F \cup B_E$ es algebraicamente independiente. Veamos que $E/K(B_F \cup B_E)$ es algebraico. Por hipótesis tenemos

$$\begin{array}{ccccccc} K & \longrightarrow & K(B_F) & \longrightarrow & F & \qquad F(B_E) & \longrightarrow & E \\ \| & & \| & \searrow & \downarrow & \qquad \| & & \| \\ K & \longrightarrow & K(B_F) & \longrightarrow & K(B_F \cup B_E) & \qquad F(B_E) & & E \end{array}$$

Como $E/F(B_E)$ es algebraica y $F/K(B_F)$ es algebraica, entonces $F(B_E)/K(B_F)(B_E)$ es algebraica, y $F(B_E)/K(B_F \cup B_E)$ es algebraica, entonces $E/K(B_F \cap B_E)$ es algebraica. □

Proposición. 21.6.
Sean $K \subseteq F_1, F_2 \subseteq E$ torres de cuerpos, se verifica:

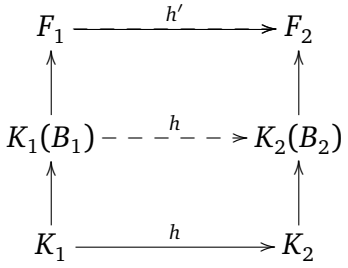
(1) $\operatorname{tgr}(F_1F_2/K) \leq \operatorname{tgr}(F_i/K)$.
(2) $\operatorname{tgr}(F_1F_2/K) \leq \operatorname{tgr}(F_1/K) + \operatorname{tgr}(F_2/K)$.

DEMOSTRACIÓN. Sea B_1 una base de trascendencia de F_1/K, entonces $F_1/K(B_1)$ es algebraica, y también lo es $F_1F_2/K(B_1)F_2 = F_1F_2/F_2(B_1)$, y por tanto B_1 contiene una base de trascendencia B de F_1F_2/F_2. Como consecuencia $\operatorname{tgr}(F_1F_2/K) = |B| \leq |B_1| = \operatorname{tgr}(F_1/K)$. □

Veamos el comportamiento de los homomorfismos en extensiones de cuerpos trascendentes.

Proposición. 21.7.
Sean F_i/K_i extensiones de cuerpos, $i = 1, 2$, con F_i algebraicamente cerrado. Si $\operatorname{tgr}(F_1/K_1) = \operatorname{tgr}(F_2/K_2)$, entonces cada isomorfismo $h : K_1 \longrightarrow K_2$ se extiende a un isomorfismo $h' : F_1 \longrightarrow F_2$.

DEMOSTRACIÓN. Sea B_i una base de trascendencia de F_i/K_i, como existe una biyección $B_1 \cong B_2$, existe un isomorfismo $h : K(B_1) \longrightarrow K(B_2)$. Como $F_i/K(B_i)$ es una extensión algebraica y F_i es algebraicamente cerrado, entonces F_i es una clausura algebraica de K_i, entonces h se puede extender a un isomorfismo $h' : F_1 \longrightarrow F_2$.



□

Corolario. 21.8.
Sea K un cuerpo y $F_1/K, F_2/K$ extensiones de cuerpos con F_i algebraicamente cerrado y $\operatorname{tgr}(F_1/K) = \operatorname{tgr}(F_2(K)$*, existe un isomorfismo $F_1/K \cong F_2/K$.*

Corolario. 21.9.
Sea K un cuerpo y F/K una extensión de cuerpos con F algebraicamente cerrado, entonces todo automorfismo de K se extiende a un automorfismo de F.

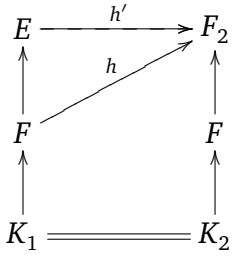
Proposición. 21.10.
Sea F/K una extensión de cuerpos con $\operatorname{tgr}(F/K) < \infty$ *y E/F una extensión con E algebraicamente cerrado. Todo homomorfismo $h : F/K \longrightarrow E/K$ se extiende a un K–automorfismo de E/K.*

DEMOSTRACIÓN. Consideramos $h : F/K \longrightarrow E/K$ y $h(F) \subseteq E$, entonces $\operatorname{tgr}(F/K) = \operatorname{tgr}(h(F)/K)$, y se verifica

$$\operatorname{tgr}(E/K) = \operatorname{tgr}(E/F) + \operatorname{tgr}(F/K) = \operatorname{tgr}(E/h(F)) + \operatorname{tgr}(h(F)/K),$$

y por la igualdad anterior, se tiene $\operatorname{tgr}(E/F) = \operatorname{tgr}(E/h(F))$, y podemos definir un automorfismo h'

que extiende a h.



□

Corolario. 21.11.
Si F/K es una extensión con F algebraicamente cerrado y $\operatorname{tgr}(F/K) < \infty$*, entonces todo endomorfismo de F/K es un isomorfismo.*

Dada una extensión F/K y $B \subseteq F$ un subconjunto finito algebraicamente independiente, tenemos que $K(B)$ es un cuerpo de funciones racionales, y es isomorfo a $K(X)$, el cuerpo de fracciones de $K[X]$, para un conjunto finito de indeterminadas X verificando $|X| = |B|$. Si $X = \{X_1, \ldots, X_t\}$, entonces el grado de trascendencia de $K(X)/K$ es igual a t.

Una extensión trascendente F/K es una extensión trascendente pura (puramente trascendente) si existe una base de trascendencia $B \subseteq F$ tal que $F = K(X)$; en este caso F es el cuerpo de funciones racionales sobre B; por extensión llamamos a B una base trascendente pura.

Teorema. 21.12.
Una extensión F/K es trascendente pura si y solo si F es un cuerpo de funciones racionales sobre K.

Dada una extensión trascendente F/K, siempre existe una extensión trascendente pura $K(B)/K$ verificando $K \subseteq K(B) \subseteq F$, y la extensión $F/K(B)$ es una extensión algebraica.

Existe un problema que es de interés: Si F/K es una extensión trascendente pura, para cada cuerpo intermedio $K \subseteq E \subseteq F$, ¿es la extensión E/K trascendente pura? En este sentido tenemos:

(1) En el caso de $\operatorname{tgr}(F/K) = 1$ el teorema de Lüroth asegura que sí.
(2) Si F/K es una extensión con $\operatorname{tgr}(F/K) = 1$, entonces la extensión es trascendente pura. Teorema de Weber–Igusa.
(3) Si K es algebraicamente cerrado, cada extensión F/K con $\operatorname{tgr}(F/K) = 2$ es una extensión trascendente pura. Teorema de Castelnouvo–Zariski.
(4) Si K no es algebraicamente cerrado, existen extensiones F/K con $\operatorname{tgr}(F/K) > 2$ que no son trascendentes puras.

(5) Si K es algebraicamente cerrado, existen extensiones F/K con $\mathrm{tgr}(F/K) > 2$ que no son trascendentes puras.

Otro problema relativo a extensiones trascendentes puras es el propuesto por Nether. Sea F/K una extensión trascendente pura con $\mathrm{tgr}(F/K) = n$, entonces el grupo simétrico S_n se puede embeber en $\mathrm{Aut}(F/K)$. Es conocido que para $G = S_n$, se tiene $F^{S_n} = K(e_1, \ldots, e_n)$, el cuerpo de funciones racionales sobre $\{e_1, \ldots, e_n\}$, el conjunto de los polinomios simétricos elementales en $\{X_1, \ldots, X_n\}$. El problema es si para cada subgrupo $H \subseteq S_n$ se tiene que F^H/K es una extensión trascendente pura. Swan prueba que si $n = 47$, existe un subgrupo transitivo $H \subseteq S_n$ tal que F^H/K no es trascendente pura.

Referencia: Bastida, [3, p. 219–226].

Capítulo VI

Funciones aritméticas

Introducción

Introducción.

4166-00.tex

22. Funciones aritméticas

Una **función aritmética** es una aplicación $f : \mathbb{N}^* \longrightarrow \mathbb{N}$; una función aritmética f se llama **multiplicativa** si $f(n_1 n_2) = f(n_1)f(n_2)$ cuando n_1 y n_2 son primos relativos.

Lema. 22.1.
Si f es una función multiplicativa, entonces la función definida $F(n) = \sum\{f(d) \mid d \mid n\}$ es una función aritmética multiplicativa.

DEMOSTRACIÓN. Si $n_1, n_2 \in \mathbb{N}$ son primos relativos, entonces cada divisor d de $n_1 n_2$ factoriza en la forma $d = d_1 d_2$, siendo $d_i | n_i$, $i = 1, 2$. Tenemos entonces:

$$F(n_1 n_2) = \sum_{d | n_1 n_2} f(d) = \sum_{d_1 | n_1,\, d_2 | n_2} f(d_1 d_2) = \sum_{d_1 | n_1,\, d_2 | n_2} f(d_1)f(d_2) = \sum_{d_1 | n_1} f(d_1) \sum_{d_2 | n_2} f(f_2) = F(n_1)F(n_2).$$

□

Ejemplo. 22.2. (La función divisor)
Para cada $n \in \mathbb{N}^*$ se define $\delta(n) =$ número de divisores de n; esto es, $\delta(n) = \sum\{1 \mid d | n\}$. Tenemos que δ es una función aritmética multiplicativa.

Tenemos una forma explícita para δ.

Lema. 22.3.
Si $n = p_1^{e_1} \cdots p_t^{e_t}$, siendo los p_i primos distintos dos a dos, y los $e_i \in \mathbb{N}^*$, se tiene $\delta(n) = \prod\{e_i + 1 \mid i = 1, \ldots, t\}$.

Ejemplo. 22.4. (La función de Mersenne)
Para cada $n \in \mathbb{N}^*$ se define $\eta(n) =$ la suma de los divisores de n; esto es, $\eta(n) = \sum\{d \mid d \mid n\}$. Tenemos que η es una función multiplicativa.

Lema. 22.5.
Existe una expresión explícita para η; si $n = p_1^{e_1} \cdots p_t^{e_t}$, siendo los p_i primos distintos dos a dos, y los $e_i \in \mathbb{N}^*$, se tiene $\eta(n) = \prod \left\{ \frac{p_i^{e_i+1}-1}{p_i - 1} \mid i = 1, \ldots, t \right\}$.

4166-01.tex

DEMOSTRACIÓN. Por ser multiplicativa, basta estudiar el caso $n = p^e$; los divisores de p^e son: $1, p, \ldots, p^e$, y su suma es: $1 + p + \cdots + p^e = \frac{p^{e+1}-1}{p-1}$. □

Un número $n \in \mathbb{N}^*$ se llama **perfecto** si $\eta(n) = 2n$. Podemos caracterizar a los números perfectos que son pares.

Proposición. 22.6.
Sea $n \in \mathbb{N}^*$ un número par, son equivalentes:

(a) n es perfecto.
(b) $n = 2^{m-1}(2^m - 1)$, con $2^m - 1$ primo.

DEMOSTRACIÓN. (b) $\Rightarrow$ (a). Si $2^m - 1$ es primo, entonces $\eta(n) = \eta(2^{m-1}(2^m - 1)) = \eta(2^{m-1})\eta(2^m - 1) = (2^m - 1)\frac{(2^m-1)^2-1}{2^m-1} = (2^m - 1)2^m = 2n$.
(a) $\Rightarrow$ (b). Supongamos que n es par y perfecto, escribimos $n = 2^{m-1}h$, con h impar. Se verifica $2n = \eta(n) = \eta(2^{m-1})\eta(h) = (2^m - 1)\eta(h)$, por tanto $(2^m - 1)\eta(h) = 2^m h = (2^m - 1)h + h$, y se tiene $\eta(h) = h + \frac{h}{2^m-1}$. Como $\eta(h) \in \mathbb{N}^*$, se tiene $\frac{h}{2^m-1} \in \mathbb{N}^*$, y los únicos divisores de h son: h y 1, por tanto $\frac{h}{2^m-1} = 1$, y tenemos $h = 2^m - 1$. otra vez por la relación $\eta(h) = h + \frac{h}{2^m-1}$ se tiene que $h = 2^m - 1$ es primo. □

Observa que si $2^m - 1$ es primo y $m > 2$, entonces m es impar. En efecto, si $2 < m = 2h$, se tiene $h \geq 2$, y podemos escribir $2^m - 1 = 2^{2h} - 1 = (2^h - 1)(2^h + 1)$, y ninguno de los factores es igual a 1, lo que es una contradicción. Se tiene la siguiene lista de primos:

m	$2^m - 1$	m	$2^m - 1$
1	1 (no es primo)	6	63 (no es primo)
2	3	7	127
3	7	8	255 (no es primo)
4	15 (no es primo)	9	511 (no es primo)
5	31	10	1023 (no es primo)

El mismo resultado se tiene si $m > 3$ es compuesto impar.

Ejemplo. 22.7. (La función de Moebius)
Para cada $n \in \mathbb{N}^*$ se define

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

Tenemos que μ es una función aritmética multiplicativa.

Lema. 22.8.
Para cada $n \in \mathbb{N}^*$, si se define $F(n) = \sum_{d|n} \mu(d)$, se verifica

$$F(n) = \begin{cases} 1 & si\ n = 1, \\ 0 & si\ n > 1, \end{cases}$$

DEMOSTRACIÓN. Sea $n > 1$, podemos considerar que $n = p^e$, entonces

$$F(p^e) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) = \mu(1) + \mu(p) = 1 - 1 = 0.$$

□

Teorema. 22.9. (Fórmula de inversión de Moebius)
Si f, F son dos funciones aritméticas relacionadas por la fórmula $F(n) = \sum\{f(d) \mid\ d|n\}$, entonces se tiene:

$$f(n) = \sum \left\{ \mu(d) F\left(\frac{n}{d}\right) \mid\ d|n \right\} = \sum \left\{ \mu\left(\frac{n}{d}\right) F(d) \mid\ d|n \right\}.$$

DEMOSTRACIÓN. Tenemos la siguiente relación:

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

Como $d|n$ y $c|\frac{n}{d}$, se tiene $c|n$ y $d|\frac{n}{c}$, y podemos reescribir la expresión anterior como

$$\sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d) f(c) = \sum_{c|n} f(c) \left(\sum_{d|\frac{n}{c}} \mu(c) \right) = \sum_{c|n} f(c) \sum_{d|\frac{n}{c}, d=1} \mu(d) = \sum_{c|d} f(c) \sum_{d|\frac{n}{c}, \frac{n}{c}=1} \mu(d) = f(n).$$

□

Como consecuencia, si f es una función aritmética multiplicativa, entonces $F(n) = \sum\{f(d) \mid\ d|n\}$ también lo es. Por otro lado, la fórmula de inversión de Moebius nos permite probar que cuando F es multiplicativa, también f lo es.

Teorema. 22.10.
Dada una función aritmética f, se define $F(n) = \sum\{f(d) \mid\ d|n\}$, si F es multiplicativa, también f lo es.

DEMOSTRACIÓN. Dados $n_1, n_2 \in \mathbb{N}^*$ primos relativos, dada divisor d de $n_1 n_2$ es de la forma $d_1 d_2$, siendo $d_i | n_i$, entonces

$$\begin{aligned} f(n_1 n_2) &= \sum_{d | n_1 n_2} \mu(d) F\left(\tfrac{n_1 n_2}{d}\right) = \sum_{d_1 | n_1,\, d_2 | n_2} \mu(d_1 d_2) F\left(\tfrac{n_1}{d_1}\, \tfrac{n_2}{d_2}\right) \\ &= \sum_{d_1 | n_1,\, d_2 | n_2} \mu(d_1)\mu(d_2) F\left(\tfrac{n_1}{d_1}\right) F\left(\tfrac{n_2}{d_2}\right) = \sum_{d_1 | n_1} \mu(d_1) F\left(\tfrac{n_1}{d_1}\right) \sum_{d_1 | n_1} \mu(d_1) F\left(\tfrac{n_1}{d_1}\right) \\ &= f(n_1) f(n_2). \end{aligned}$$

□

Ejemplo. 22.11. (La función totiente φ de Euler. La función indicatriz de Euler)
Para cada $n \in \mathbb{N}^*$ se define $\varphi(n) =$ número de naturales menores que n y que son primos con n, o equivalentemente, $\varphi(n) = |\mathbb{Z}_n^\times|$. Tenemos que φ es una función multiplicativa, y si p es primo, se tiene $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$. Como consecuencia, si $n = p_1^{e_1} \cdots p_t^{e_t}$, se tiene $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_t})$.

Lema. 22.12.
Para cada $n \in \mathbb{N}^*$ se verifica $\sum\{\varphi(d) \mid d | n\} = n$.

DEMOSTRACIÓN. Para cada $1 \leq a \leq n$ existe $1 \leq c \leq n$ tal que $\operatorname{mcd}\{a, n\} = c$, y por tanto $\operatorname{mcd}\{\frac{a}{c}, \frac{n}{c}\} = 1$, esto es, $\frac{a}{c}$ es primo relativo con $\frac{n}{c}$. Establecemos una aplicación $\mathbb{Z}_n \longrightarrow \{\text{divisores de } n\}$ mediante $a \mapsto d$ tal que $d = \frac{n}{\operatorname{mcd}\{a,n\}}$. Esta aplicación es sobreyectiva, y dado un divisor d de n con $n = dc$, para cada $1 \leq b \leq d$, se obtiene un elemento bc verificando $1 \leq bc \leq n$; se determinan así $\varphi(d)$ elementos. En consecuencia se tiene $n = \sum_{d | n} \varphi(d)$. □

Tenemos entonces una función aritmética multiplicativa φ, que define una función aritmética (también multiplicativa): $\operatorname{id}(n) = F(n) = \sum_{d | n} \varphi(d)$.

Corolario. 22.13.
En la situación anterior se tiene $\varphi(n) = \sum\{\mu(d)\frac{n}{d} \mid d | n\} = \sum\{d\mu\left(\frac{n}{d}\right) \mid d | n\}$.

DEMOSTRACIÓN. Es consecuencia directa del Lema (22.12.) y de la fórmula de inversión de Moebius. □

Proposición. 22.14.
Sea f una función aritmética multiplicativa, para $n = p_1^{e_1} \cdots p_t^{e_t} > 1$ se tiene:

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1)) \cdots (1 - f(p_t)).$$

DEMOSTRACIÓN. Definimos una función aritmética $g(n) = \sum_{d|n} \mu(d) f(d)$. Como μ y f son multiplicativas, también g, por tanto basta probar el resultado para $n = p^e$, una potencia de un primo. Se tiene:

$$g(p^e) = \sum_{d|p^e} \mu(d) f(d) = \mu(1) f(1) + \mu(p) f(p) + \cdots + \mu(p^e) f(p^e) = \mu(1) f(1) + \mu(p) f(p) 1 - f(p).$$

□

Tenemos entonces las siguiente relaciones:

Corolario. 22.15.
Para $n = p_1^{e_1} \cdots p_t^{e_t} > 1$ se tiene:
(1) Si δ es la función número de divisores, se tiene $\sum_{d|n} \mu(d)\delta(d) = (-1)^t$.
(2) Si η es la función suma de divisores, se tiene $\sum_{d|n} \mu(d)\eta(d) = (-1)^t p_1 \cdots p_t$.
(3) $\sum_{d|n} \frac{\mu(d)}{d} = (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_t}) = \frac{\varphi(n)}{n}$.
(4) $\sum_{d|n} \mu(d) d = (1 - p_1) \cdots (1 - p_t) = (-1)^t \frac{\varphi(n) p_1 \cdots p_t}{n}$.

Teorema de Euler–Fermat

Teorema. 22.16. (Teorema de Euler–Fermat)
Sean a, n enteros positivos primos relativos, entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.

DEMOSTRACIÓN. Tenemos que $\varphi(n)$ es el orden del grupo multiplicativo $\mathbb{Z}_n^\times$; y por ser a primo relativo con n, entonces $a + n\mathbb{Z} \in \mathbb{Z}_n^\times$. □

Ejercicio. 22.17.
Dado un entero primo positivo p, un polinomio irreducible $f \in \mathbb{F}_p[X]$, de grado n, se llama ***primitivo*** *si una raíz α de f es un generador del grupo multiplicativo $\mathbb{F}_{p^n}^\times$.*

(1) Si f es un polinomio irreducible primitivo de grado n, prueba que cada raíz de f es un generador del grupo multiplicativo $\mathbb{F}_{p^n}^\times$.
(2) Determina el número de polinomios irreducibles de grado n sobre $\mathbb{F}_p$.

SOLUCIÓN. (1). Sea f un polinomio irreducible primitivo de grado n, y sean α y β dos raíces. Si α es un generador de $\mathbb{Z}_{p^n}^\times$, entonces $\operatorname{ord}(\alpha) = p^n - 1$; si β no es un generador, existe $h | p^n - 1$, divisor propio, tal que $\beta^h = 1$, por tanto β es raíz del polinomio $X^h - 1$, y como $f | X^h - 1$, también lo es α, lo que es una contradicción.
(2). Supongamos que f es una polinomio irreducible primitivo de grado n, y que α es una raíz de f. Para cada $1 \leq t < n$, primo relativo con n se tiene que α^t es también un generador.
Como el automorfismo de Frobenius es un generador del grupo de Galois de $\mathbb{F}_{p^n}/\mathbb{F}_p$, los conjugados de α son $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$, y por tanto $f(X) = (X-\alpha)\cdots(X-\alpha^{p^{n-1}})$. Por la hipótesis se tiene $f(X) = (X-\alpha)\cdots(X-\alpha^{p^{n-1}})$. Al considerar α^t, su polinomio irreducible es $f_t(X) = (X-\alpha^t)\cdots(X-\alpha^{tp^{n-1}})$. Tenemos entonces que todos los polinomios irreducibles de grado n sobre $\mathbb{F}_p$ son de la forma $f_t(X)$, para algún t.
Para calcular cuántos hay basta dividir por n el número de generadores de $\mathbb{F}_{p^n}^\times$. Como $\mathbb{F}_{p^n}^\times \cong \mathbb{Z}_{p^n-1}$, ya que es cíclico, el número de polinomios irreducibles primitivos de grado n sobre $\mathbb{F}_p$ es:

$$\frac{\varphi(p^n-1)}{n}.$$

□

Ejercicio. 22.18.
Dado un entero primo positivo p, determina cuántos polinomios irreducibles de grado n existen sobre $\mathbb{F}_p$.

SOLUCIÓN. Tenemos que si f es un polinomio irreducible de grado n, entonces f es un factor de $X^{p^n} - X$. Por otro lado, los factores irreducibles de $X^{p^n} - X$ son todos los polinomio irreducibles de grado d, un divisor de n.
Llamamos $P_p(n)$ al número de polinomios irreducibles de grado n sobre $\mathbb{F}_p$, entonces se tiene $p^n = \sum_{d|n} dP_p(d)$. Si consideramos la función aritmética $Q_p(n) = \frac{1}{n}P_p(n)$, se tiene $p^n = \sum_{d|n} Q_p(d)$, y por

la fórmula de inversión de Moebius, resulta $Q_p(n) = \sum_{d|n} \mu(d) p^{\frac{n}{d}}$, y por tanto

$$P_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

□

Producto de convolución de Dirichlet

Dadas dos funciones aritméticas f y g, se define el producto de convolución $f * g$ mediante

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

Observa que el producto de convolución es conmutativo, y la aplicación $\mathbb{1}$, definida $\mathbb{1}(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \neq 1 \end{cases}$, es un elemento neutro.

Lema. 22.19.
El producto de convolución es:
(1) asociativo; $f * (g * h) = (f * g) * h$,
(2) distributivo respecto a la suma: $f * (g + h) = f * g + f * h$

para cualesquiera f, g y h funciones aritméticas.

DEMOSTRACIÓN. (1). Se tiene:

$$\begin{aligned} (f * (g*))(n) &= \textstyle\sum_{d_1 d_2 = n} f(d_1)(g * h)(d_2) \\ &= \textstyle\sum_{d_1 d_2 = n} f(d_1) \sum_{d_3 d_4 = d_2} g(d_3) h(d_4) \\ &= \textstyle\sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3) \\ &= \cdots = ((f * g) * h)(n). \end{aligned}$$

(2). Se tiene:

$$\begin{aligned} (f * (g + h))(n) &= \textstyle\sum_{d_1 d_2 = n} f(d_1)(g + h)(d_2) \\ &= \textstyle\sum_{d_1 d_2 = n} f(d_1)\,(g(d_2) + h(d_2)) \\ &= \textstyle\sum_{d_1 d_2 = n} f(d_1) g(d_2) + \sum_{d_1 d_2 = n} f(d_1) h(d_2)) \\ &= (f * g)(n) + (f * h)(n). \end{aligned}$$

□

Lema. 22.20.
Cuando f es una función aritmética con $f(1) \neq 0$, entonces f tiene un inverso para el producto de convolución.

DEMOSTRACIÓN. Definimos una función aritmética f^{-1} como sigue: $f^{-1}(1) = \frac{1}{f(1)}$. Supongamos que f^{-1} está definida para todo $x < n$ y queremos ver que propiedad verifica $f^{-1}(n)$, para $n > 1$. Supongamos que f^{-1} está definida y que se tiene $f^{-1} * f = \mathbb{1}$, entonces se tiene

$$\sum_{d_1 d_2 = n} f^{-1}(d_1) f(d_2) = \mathbb{1}(n) = 0.$$

Se tiene $f^{-1}(n)f(1) + \sum_{d_1 d_2 = n, d_1 \neq n} f^{-1}(d_1)f(d_2) = 0$, esto es,

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{d_1 d_2 = n, d_1 \neq n} f^{-1}(d_1) f(d_2),$$

lo que permite definir, por recurrencia, el inverso de f. □

Lema. 22.21.
Si f es una función aritmética multiplicativa no nula, entonces $f(1) = 1$.

DEMOSTRACIÓN. Existe n tal que $f(n) \neq 0$, entonces se tiene $f(n) = f(n \cdots 1) = f(n)f(1)$, y por tanto $f(1) = 1$. □

Observación. 22.22.
Como consecuencia, el conjunto de las funciones aritméticas multiplicativas tiene estructura de grupo para el producto de convolución.

La función de Moebius tiene por inversa a la función constante igual a 1, a la representamos simplemente por 1. Es consecuencia del Lema (22.8.).

Prueba de la fórmula de inversión de Moebius.

DEMOSTRACIÓN. Dada una función aritmética f se define una nueva función F mediante $F(n) = \sum_{d|n} f(n)$, entonces $F = 1 * f$, y se tiene $\mu * F = \mu * 1 * f = \mathbb{1} * f = f$. □

Parte entera

Para cada $r \in \mathbb{R}$ se define la **parte entera** de r como el mayor entero menor o igual que r, y se representa por $[r]$. Se verifica $x - [x] \in [0,1[$, o equivalentemente, $[r]$ es el único entero en $]r-1, r]$.
Para cada entero primo positivo p y cada entero m se define $v_p(m)$ como el exponente de la mayor potencia de p que divide a m.

Teorema. 22.23.
Para cada $n \in \mathbb{N}^*$ se tiene $v_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$.

DEMOSTRACIÓN. Tenemos que los múltiplos de p que aparecen en la lista $1, 2, \ldots, n$ son los siguientes: $p, 2p, \ldots, \left[\frac{n}{p}\right]p$. Ahora consideramos la lista $1, 2, \ldots, \left[\frac{n}{p}\right]$; los múltiplos de p que aparecen en la misma son: $p, 2p, \ldots, \left[\frac{[n/p]}{p}\right]p$. Vamos a probar que $\left[\frac{[n/p]}{p}\right] = \left[\frac{n}{p^2}\right]$. En efecto, se tiene:

$$\left[\frac{[n/p]}{p}\right]p^2 \leq \left[\frac{n}{p}\right]p \leq m,$$

por tanto $\left[\frac{[n/p]}{p}\right] \leq \left[\frac{n}{p^2}\right]$. Y también

$$\left[\frac{n}{p^2}\right]p^2 \leq m,$$

por tanto $\left[\frac{n}{p^2}\right]p \leq \left[\frac{n}{p}\right]$, y se tiene $\left[\frac{n}{p^2}\right] \leq \left[\frac{[n/p]}{p}\right]$.
Analizando las listas que se van construyendo, y haciendo inducción tenemos el resultado. □

Teorema. 22.24.
Sean f y F funciones aritméticas tales que $F(n) = \sum_{d|n} f(d)$. Para cualquier $n \in \mathbb{N}^*$ se verifica: $\sum_{i=1}^{n} F(i) = \sum_{j=1}^{n} f(j)\left[\frac{n}{j}\right]$.

DEMOSTRACIÓN. Tememos

$$\sum_{i=1}^{n} F(i) = \sum_{i=1}^{n} \sum_{d|i} f(d) = \sum_{d=1}^{n} f(d)\left[\frac{n}{d}\right],$$

ya que si $1 \leq i \leq n$ y $d|i$, entonces $1 \leq d \leq n$, y el número de éstos d's es $\left[\frac{n}{d}\right]$, que es el número de múltiplos de d que son menores o iguales que n. □

Ejercicio. 22.25.
Sean $n, p \in \mathbb{N}^*$, siendo p primo. Si escribimos n en base p, esto es, $n = a_0 + a_1 p + \cdots + a_t p^t$, con $0 \leq a_i < p$, prueba que la mayor potencia de p qe divise a $n!$ es $\dfrac{m-(a0+\cdots+a_t)}{p-1}$.

SOLUCIÓN. Tenemos que $v_p(n) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$. Observa que

$$\left[\frac{n}{p}\right] = \frac{a_1 p + \cdots + a_t p^t}{p} = a_1 + a_2 p + \cdots + a_t p^{t-1},$$

y en general se tiene

$$\left[\frac{n}{p^i}\right] = a_i + a_{i+1} p + \cdots + a_t p^{t-i}.$$

por tanto se tiene

$$\begin{aligned} v_p(n) &= \textstyle\sum_{i=1}^{\infty} (a_i + a_{i+1} p + \cdots + a_t p^{t-i}) \\ &= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots + a_t(p^{t-1} + \cdots + p + 1) \\ &= a_1 + a_2 \frac{p^2-1}{p-1} + a_3 \tfrac{p^3-1}{p-1} + \cdots + a_t \tfrac{p^t-1}{p-1} \\ &= \frac{a_1(p-1) + a_2(p^2-1) + \cdots + a_t(p^t-1)}{p-1} \\ &= \frac{n-(a_0+a_1+\cdots+a_t)}{p-1}. \end{aligned}$$

□

Ejercicio. 22.26.
Determina la mayor potencia de 5 que divide a 2018!

SOLUCIÓN. Escribimos 2018 en base 5: se tiene $2018 = 1333_{(5}$, por tanto

$$v_5(2018) = \frac{2018-(1+3+3+3)}{4} = 502.$$

□

Ejercicio. 22.27.
Determina la mayor potencia de 2 que divide a 2018!

SOLUCIÓN. Escribimos 2018 en base 2: se tiene $2018 = 11111011010_{(2}$, por tanto

$$v_2(2018) = \frac{2018-(1+1+1+1+1+0+1+1+0+1+0)}{1} = 2010.$$

□

Ejercicio. 22.28.
Determina la mayor potencia de p que divide a $2\times 4\times\cdots\times 2n$.

SOLUCIÓN. Llamamos $m = 2\times 4\times\cdots\times 2n$; se tiene $m = 2^n n!$, entonces $p|m$ si $p|n!$ ó $p|2^n$.
Cuando $p = 2$ se tiene $v_2(m) = n + v_2(n!)$.
Cuando $p \neq 2$, se tiene $v_p(m) = v_p(n!)$. □

Ejercicio. 22.29.
Determina la mayor potencia de p que divide a $1\times 3\times\cdots\times(2n-1)$.

SOLUCIÓN. Llamamos $m = 1\times 3\times\cdots\times(2n-1)$; se tiene $m = \frac{(2n-1)!}{2\times\cdots\times 2(n-1)} = \frac{(2n)!}{2^n n!}$.
Cuando $p = 2$ tenemos $v_2(m) = v_2((2n)!) - n - v_2(n!)$.
Cuando $p \neq 2$ tenemos $v_p(m) = v_p((2n)!) - v_p(n!)$. □

Ejemplo. 22.30.
Consideramos la función definida por $f(n) = 1$, para cada $n \in \mathbb{N}$, entonces $F(n)$ es el número de divisores de n, esto es, $F = \delta$, y se tiene $\sum_{i=1}^{n} \delta(i) = \sum_{j=1}^{n} \left[\frac{n}{j}\right]$.

Ejemplo. 22.31.
Consideramos la función definida por $f(n) = n$, entonces $F(n)$ es la suma de los divisores de n, esto es, $F = \eta$, y se tiene $\sum_{i=1}^{n} \eta(i) = \sum_{j=1}^{n} j\left[\frac{n}{j}\right]$.

Ejercicio. 22.32.
Prueba que el producto de n enteros positivos consecutivos es divisible por $n!$

SOLUCIÓN. Tenemos la siguiente relación:

$$(x+1)\cdots(x+n) = \frac{(x+n)!}{x!} = \frac{(x+n)!}{n!\,x!}n! = \binom{x+n}{n}n!$$

□

Ejercicio. 22.33.
Prueba que para cada $n \in \mathbb{N}^*$ se verifica $\dfrac{\eta(n)}{n} = \sum_{d|n}\frac{1}{d}$.

SOLUCIÓN. Observa que los divisores de n están emparejados en la siguiente forma: $d_1 \sim d_2$ si $d_1 d_2 = n$. Por tanto se tiene que $\sum_{d_1|n}\frac{n}{d_1} = \sum_{d_2|n} d_2 = \eta(n)$, y se tiene

$$\eta(n) = \sum_{d|n} d = \sum_{d|n}\frac{n}{d} = n\sum_{d|n}\frac{1}{d}.$$

□

Bibliografía

[1] E. Artin, *Geometric algebra*, Wiley, 1957.

[2] M. Artin, *Algebra*, Prentice Hall, 1991.

[3] J Bastida, *Field extesions and Galois theory*, Addison–Wesley, 1984. 20, 21

[4] J. A. Beachy and W. D. Blair, *Abstract algebra, 2nd ed.*, Waveland Press, 1996.

[5] H. Cohen, *A course in computational algebraic number theory*, Springer, 1993.

[6] P. M. Cohn, *Algebra I*, John Wiley, 1974.

[7] ———, *Algebra II*, John Wiley, 1977.

[8] ———, *Algebra. vol. 1. 2nd. ed.*, Wiley, 1982.

[9] ———, *Algebra vol. 2. 2nd. ed.*, Wiley, 1989.

[10] ———, *Algebra vol. 3.*, Wiley, 1991.

[11] D. S. Dummit and R. M. Foote, *Abstract algebra. 2nd ed.*, Prentice-Hall, 1999.

[12] ———, *Abstract algebra. 3rd ed.*, Wiley, 2004.

[13] J. D. Fraleigh, *A first course in abstract algebra*, Addison–Wesley, 1967.

[14] L. Gaal, *Classical galois theory*, Univ. Minnesota, 1971.

[15] T. W. Hungerford, *Algebra*, Springer–Verlag, 1974.

[16] N. Jacobson, *Lectures in abstract algebra. III. Theory of fields and Galois theory*, Springer Verlag, 1964.

[17] ———, *Basic algebra i. 2nd. ed.*, Freeman, 1985. 3.7., 3

[18] ———, *Basic algebra II. 2nd ed.*, Freeman, 1989.

[19] I. Kaplansky, *Fields and rings*, Chicago Univ. Press, 1972.

[20] J. P. Lafon, *Algèbre commutative: Languages géometrique et algébrique*, Collection enseignement des sciences, 24, Hermann, Paris, 1977.

[21] S. Lang, *Algebra 3rd. ed.*, Springer, 2002.

[22] S. MacLane and G. Birkhoff, *Algèbre I. Structures fondamentales. II. Les grands théorèmes*, Gauthier–Villar, 1971.

[23] S. MacLane and G. Birkhoff, *Algebra*, Macmillan, 1979.

[24] P. J. McCarthy, *Algebraic extensions of fields*, Chelsea, 1976.

[25] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

[26] L. Rowen, *Graduate Algebra: Commutative view*, Graduate Studies in Mathematics, 73, Graduate Studies in Math., 73. Amer. Math. Soc., 2006.

[27] I. Stewart, *Galois theory*, Chapman and Hall, 1973.

[28] B. L. van der Waerden, *Algebra i*, Frederick Ungar Publ. Co., 1970.

Índice alfabético