EJERCICIOS DE EXTENSIONES DE CUERPOS Y TEORÍA DE GALOIS

José Antonio Cuenca Mira
Departamento de Álgebra Geometría y Topología
Universidad de Málaga

26 de mayo de 2021

Índice general

Prólogo

To know mathematics means to be able to do mathematics: to use mathematical language with some fluency, to do problems, to critize arguments, to find proofs ...

On the Mathematics Curriculum of
the High School

Las páginas que siguen son una recopilación de ejercicios de teoría de cuerpos. Incorporan, corregidas y aumentadas, relaciones previas que fueron utilizadas para complementar la asignatura de *Álgebra Clásica*, que formaba parte del anterior plan de estudios vigente en la Universidad de Málaga. La necesidad de adaptar los ejercicios al contenido de la asignatura de *Teoría de Cuerpos* del plan de estudios actualmente vigente, unido al deseo de corregir algunas erratas que se habían deslizado en las anteriores relaciones, me llevan hoy, a la realización de esta nueva selección. Con el mismo espíritu que antaño, espero que resulte útil como importante material complementario, habida cuenta el papel fundamental que en cualquier proceso de aprendizaje de matemáticas juega el trabajo personal dedicado a la resolución de ejercicios.

El propio origen de estas páginas se manifiesta en algunos de los enunciados que contienen, donde en ciertos lugares se encontrarán referencias a resultados contenidos en las notas, aún provisionales y no disponibles, que desarrollan el contenido del referido curso de *Teoría de Cuerpos*. No obstante, creo que podrían ser también de utilidad a quienes se inician en el estudio de las extensiones de cuerpos y teoría de Galois, o a aquellos profesores que enseñan estos temas. Con ese deseo las pongo a disposición de todos ellos.

Los ejercicios seleccionados pasan los cuatrocientos y tienen procedencia variada, inclyéndose algunos que podrían ser originales. Se usan a veces algunas notaciones habituales. Éste es el caso de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$ para designar al anillo de enteros $\mathbb{Z}$, o a los cuerpos de números racionales, reales o complejos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

Málaga, 5 de mayo de 2020.

José Antonio Cuenca Mira

Capítulo 1

Extensiones de cuerpos

L'álgègre est à proprement parler, l'Analyse des équations*; les diverses théories partielles qu'elle comprend se rattachent toutes, plus ou moins, à cet object principal.*

J.-A. Serret

1.1. Introducción

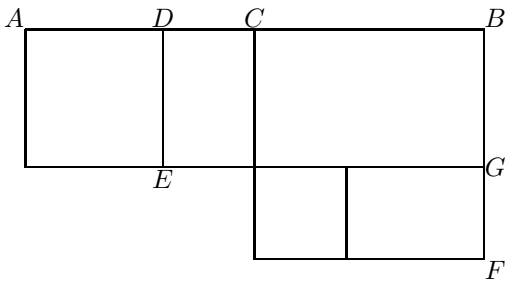
1.1 Mostrar que, para todo entero $n \geq 1$, el conjunto de las raíces n-ésimas de la unidad que hay en un cuerpo dado F constituyen un subgrupo del grupo multiplicativo $F^\star$ del cuerpo F. ¿Cuántas raíces n-ésimas de la unidad hay en F en el caso en que n es un número primo que coincide con la característica de F?

1.2 Sea p un primo positivo. Demostrar que un cuerpo F contiene p raíces p-ésimas de la unidad distintas si y sólo si F contiene alguna raíz de $X^p - 1$ que sea distinta de 1.

1.3 Sea p un primo positivo. Cualquiera de las raíces p-ésimas de la unidad distintas de 1 que pertenecen a un cuerpo $\mathbb{C}$ delos números complejos, ¿genera el subgrupo W_p de todas las raíces p-ésimas de la unidad del cuerpo $\mathbb{C}$?

1.4 Sea C el punto medio del segmento AB de la figura que se da continuación y D el punto del segmento AB elegido de manera que el rectángulo de lados BD y DE tiene área conocida c. Por otra parte, el rectángulo superior de la figura contiene en su parte izquierda un cuadrado de lado AD. La parte

derecha de la figura lo constituye un cuadrado de lado CB, que contiene en su parte inferior izquierda otro cuadrado cuyo lado tiene longitud CD.



Hacer $AD = x$ y elegir de modo adecuado BC para justificar a la manera de Al-Khwarizmi que x es solución de la ecuación de segundo grado $x^2 + c = bx$ (b, $c > 0$) y que

$$x = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

1.5 Sea F un cuerpo de característica distinta de 2, f el polinomio de $F[X]$ siguiente

$$f(X) = X^2 + bX + c,$$

y x una raíz de f contenida en un cuerpo L que contiene a F como subcuerpo. Sean α, $\beta \in F$. Establecer condiciones sobre α y β para que $\alpha + \beta x$ tenga su cuadrado en F y mostrar la existencia de algún α, determinado de forma única, tal que $(\alpha + x)^2 \in F$. A partir de aquí, justificar la validez de la fórmula de resolución de la ecuación de segundo grado.

1.6 Sea q un número racional dado. Mostrar que los números complejos que se escriben en la forma $\alpha + \beta\sqrt{q}$, $(\alpha, \beta \in \mathbb{Q})$ constituyen un subcuerpo de $\mathbb{C}$ y que toda ecuación de segundo grado con coeficientes en $\mathbb{Q}$ tiene sus raíces en un cuerpo de este tipo para un número racional q convenientemente elegido.

1.7 Sea F un cuerpo de característica distinta de 2 y 3 y $f = X^3 + pX + q$, $(p \neq 0)$, un polinomio de $F[X]$. Mostrar que la resolución de la ecuación $f(x) = 0$ puede reducirse a la de una ecuación de grado a lo sumo 2 en y^3 introduciendo una nueva variable y relacionada con x por la igualdad $p/3 = y(y + x)$.

1.8 En las condiciones del ejercicio 1.7 con $F = \mathbb{Q}$, mostrar que un número complejo y, relacionado con una raíz compleja x del polinomio f por la igualdad $p/3 = y(y + x)$, no pertenece necesariamente al menor subcuerpo de $\mathbb{C}$ que contiene a todas las raíces de f.

1.9 Sea F un cuerpo de característica distinta de 2 y L un cuerpo extensión de F que contiene tres raíces x_1, x_2, x_3, distintas o no, del polinomio $f(X) = X^3 - bX + c$, $(b, c \in F)$. Demostrar que para cada dos de ellas, x_i y x_j, $(i \neq j)$, se tiene $x_i^2 + x_j^2 + x_i x_j = b$ y $x_i^2 x_j + x_i x_j^2 = c$.

1.10 Sea el polinomio de tercer grado f con coeficientes en el cuerpo F y definido por la igualdad $f(X) = X^3 + pX + q$. Suponer que L es un cuerpo extensión de F en el que f tiene las tres raíces x_1, x_2 y x_3. Comprobar que si $i \neq j$ entonces

$$(x_i - x_j)^2 = x_k^2 - 4x_i x_j = -3x_k^2 - 4p,$$

siendo $k \neq i, j$. Mostrar que si $\Delta \in F[X_1, X_2, X_3]$ es el polinomio discriminante en tres indeterminadas definido por la igualdad

$$\Delta = \prod_{i<j;\ i,j=1}^{3} (X_i - X_j)^2$$

se tiene entonces

$$\Delta(x_1, x_2, x_3) = -(27q^2 + 4p^3).$$

1.11 Sea F un cuerpo, L un cuerpo extensión de F y f un polinomio mónico del anillo de polinomios $F[X]$ tal que f se descompone como producto de factores lineales de $L[X]$.

1. Determinar el número de factorizaciones en producto de polinomios mónicos de grado 2 que tiene f en $L[X]$, si dicho polinomio tiene grado $n > 1$.
2. Suponer que F tiene característica $\neq 2$ y que f es el polinomio de grado 4

   $$f(X) = X^4 + pX^2 + qX + r, \qquad (p,\, q,\, r \in F).$$

   Considerar una factorización de f como producto de polinomios mónicos de segundo grado del tipo

   $$X^4 + pX^2 + qX + r = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta). \tag{1.1}$$

   A la manera de R. Descartes, identificando coeficientes, mostrar que si α es no nulo entonces α^2 es raíz de una ecuación de tercer grado con coeficientes en F y que los restantes coeficientes de los polinomios que aparecen en la factorización dada quedan completamente determinados por α y los coeficientes p, q, r del polinomio f. Mostrar que la resolución de la ecuación polinómica $f(x) = 0$ se reduce a resolver a lo sumo una ecuación de grado 3 y dos de segundo grado.

1.12 Sea F un cuerpo, f un polinomio mónico de $F[X]$ de grado n, que tiene raíces $x_1, \ldots, x_n$, distintas o no, en un cuerpo L extensión de F. Usar el teorema fundamental de los polinomios simétricos para demostrar que, si $\varphi \in F[X_1, \ldots, X_n]$ es un polinomio simétrico, entonces $\varphi(x_1, \ldots, x_n)$ pertenece a F

1.13 Sea F un cuerpo que contiene alguna raíz cúbica de la unidad $\varepsilon \neq 1$. Sean h_1 y h_2 los polinomios de $F[X_1, X_2, X_3]$ definidos por las igualdades siguientes:

$$h_1 = (X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3, \qquad h_2 = (X_1 + \varepsilon^2 X_2 + \varepsilon X_3)^3.$$

Mostrar que $h_1 \neq h_2$. Demostrar que toda permutación de las indeterminadas X_1, X_2, X_3, o bien deja invariantes a los dos polinomios h_1 y h_2, o transforma uno en el otro.

1.14 Sea f un polinomio mónico de grado n con coeficientes en el cuerpo F y con n raíces $x_1, \ldots, x_n$ en un cuerpo L extensión de F. Sean $h_1, \ldots, , h_k$ polinomios de $F[X_1, \ldots, X_n]$ tales que, para cada $i \in \{1, \ldots, k\}$ y toda permutación σ del conjunto $\{1, \ldots, n\}$, el polinomio h_i^σ obtenido de h_i aplicando σ a cada uno de los subíndices de las indeterminadas pertenece al conjunto $\{h_1, \ldots, h_k\}$. Demostrar que el polinomio

$$\psi(X) = \prod_{i=1}^{k} (X - h_i(x_1, \ldots, x_n))$$

tiene coeficientes en F y tiene por raíces a los elementos $h_i(x_1, \ldots, x_n)$, $(i = 1, \ldots, k)$ del cuerpo L.

1.15 Sea $f \in \mathbb{R}[X]$ un polinomio mónico de tercer grado. Mostrar que f tiene alguna raíz real y que, si x_1, x_2 y x_3 son las raíces de f en $\mathbb{C}$ y $\Delta \in \mathbb{R}[X_1, X_2, X_3]$ denota al polinomio discriminante definido como en la página 17, se tiene entonces que $\Delta(x_1, x_2, x_3)$ es un número real que se anula en caso de que alguna de dichas raíces sea raíz múltiple de f. Justifíquese que para f se presentan únicamente dos posibilidades: (i) f tiene una única raíz real, o (ii) f tiene todas sus ríces reales. Demostrar $\Delta(x_1, x_2, x_3) > 0$ si y sólo si f tiene tres raíces reales distintas.

1.2. Extensiones finitas y algebraicas

2.1 Comprobar que $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\sqrt{5}) = \mathbb{Q}$.

2.2 Sea $\{K_i\}_{i \in \mathcal{A}}$ una familia de subcuerpos de un cuerpo L, todos ellos extensiones de un cuerpo F. Para cada $i \in \mathcal{A}$, sea A_i el subcuerpo de los elementos de K_i que son algebraicos sobre F. Comprobar que el cuerpo de los elementos de $\bigcap K_i$ que son algebraicos sobre F coincide con $\bigcap A_i$.

2.3 Encontrar el polinomio irreducible sobre $\mathbb{Q}$ del número complejo $x = \sqrt{2 - \sqrt{3}}$.

2.4 Sea K/F una extensión de cuerpos de grado n y x un elemento de K tal que $x^3 \in F$. Demostrar:

1. Si n no es divisible por 2 ni por 3 entonces $x \in F$.
2. Si n no es divisible por 3, existe entonces $c \in F$ tal que $x^3 = c^3$.

2.5 Sea $y \in \mathbb{C}$ un número algebraico cuyo polinomio irreducible $\mathrm{irr}(y, X, \mathbb{Q})$ tiene grado 3. Mostrar que si $\mathrm{irr}(y, X, \mathbb{Q}) = X^3 + \alpha X^2 + \beta X + \gamma$ entonces $\mathrm{irr}(-y, X, \mathbb{Q})$ tiene también grado 3 y $\mathrm{irr}(-y, X, \mathbb{Q}) = X^3 - \alpha X^2 + \beta X - \gamma$, siendo en particular $\mathrm{irr}(y, X, \mathbb{Q}) \neq \mathrm{irr}(-y, X, \mathbb{Q})$.

2.6 Sea K/F una extensión de cuerpos y x un elemento de K que es raíz del polinomio $X^8 + 2X^4 + 1$. Demostrar que $[F(x) : F] \leq 4$. ¿Puede darse la desigualdad estricta?

2.7 Sea x un elemento algebraico de la extensión K/F y n un entero estrictamente positivo. Comprobar que

$$[F(x^n) : F] \geq \frac{1}{n}[F(x) : F].$$

2.8 Sea K/F una extensión de cuerpos, L un cuerpo y $g : K \longrightarrow L$ un homomorfismo. Mostrar que $g(K)/g(F)$ es una extensión de cuerpos tal que $[g(K) : g(F)] = [K : F]$. Suponer $L = K$ y g suprayectivo tal que $g(F) \subset F$. Demostrar que si K/F es extensión finita entonces g induce un automorfismo de F.

2.9 Sean K/F y L/F extensiones de cuerpos y $g : K \longrightarrow L$ un isomorfismo de cuerpos tal que $g(F) \subset F$. Si K/F y L/F son extensiones finitas, ¿induce g necesariamente un automorfismo de F?

2.10 Sea K/F una extensión cuadrática. Supóngase $K = F(z)$, donde $z^2 \in F$. Determinar los elementos de K que tienen cuadrado en F.

2.11 Sea K/F una extensión de cuerpos, x un elemento de K y f un polinomio de grado ≥ 1 de $F[X]$ tal que $y = f(x)$ es algebraico. ¿Es x un elemento algebraico de la extensión?

2.12 Determinar el polinomio irreducible de $\sqrt{2} + \sqrt{5}$ sobre $\mathbb{Q}(\sqrt{2})$.

2.13 Sea x una raíz del polinomio X^3+X^2+1 de $\mathbb{Q}[X]$ e y una raíz del polinomio $X^2 + X - 8$. Los números $x + y$ y xy, ¿son algebraicos sobre $\mathbb{Q}$? Determinar el grado de la extensión $\mathbb{Q}(x, y)/\mathbb{Q}$.

2.14 Demostrar que el cuerpo A de los números algebraicos coincide con $(A \cap \mathbb{R})(\mathrm{i})$.

2.15 Sea $u = \sqrt{2}\sqrt[3]{5}$. Demostrar que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(u)$. ¿Será irreducible sobre $\mathbb{Q}$ el polinomio $X^6 - 200$?

2.16 Demostrar que el número complejo $x = \sqrt{2 - \sqrt{5\sqrt{3}}}$ es tal que $\mathbb{Q}(x^2) = \mathbb{Q}(\sqrt[4]{75})$ y que $[\mathbb{Q}(x) : \mathbb{Q}] = 8$. Determinar $\mathrm{irr}(x, X, \mathbb{Q})$.

2.17 Determinar el grado de la extensión $\mathbb{Q}(x)/\mathbb{Q}$ cuando x es un número complejo raíz del polinomio $X^6 - 6X^4 + X^3 + 9X^2 - 1$.

2.18 Sea x un elemento algebraico sobre un cuerpo F cuyo polinomio irreducible tiene grado impar. Demostrar que $F(x) = F(x^2)$.

2.19 Sean m y n enteros positivos primos relativos. Comprobar que, si x e y son números complejos tales que $x^m = 2$, $y^n = 3$, entonces $\mathbb{Q}(x, y) = \mathbb{Q}(xy)$. ¿Cuál es el polinomio irreducible de xy sobre $\mathbb{Q}$?

2.20 Sea K/F una extensión de cuerpos. Supóngase que x e y son elementos de K y a lo menos uno de ellos trascendente sobre F. Mostrar que $x + y$ ó xy son trascendentes sobre F.

2.21 Sea K/F una extensión de cuerpos, t y w elementos de K trascendentes sobre F. Demostrar que w es algebraico sobre $F(t)$ si y sólo si t es algebraico sobre $F(w)$.

2.22 Sea K/F una extensión de cuerpos y $x_1, \ldots, x_n$ elementos algebraicos de la extensión. Demostrar que $F(x_1, \ldots, x_n) = F[x_1, \ldots, x_n]$. Si S es un subconjunto de elementos algebraicos de K, ¿se tiene $F(S) = F[S]$?

2.23 Sea K/F una extensión algebraica de generación finita. Mostrar que existe algún entero $n \geq 1$ y algún ideal un maximal $\mathfrak{m}$ de un anillo de polinomios $F[X_1, \ldots, X_n]$ tal que $K \cong F[X_1, \ldots, X_n]/\mathfrak{m}$.

2.24 Sea F un cuerpo de característica distinta de 2, K/F una extensión de cuerpos y x e y dos elementos de K que no están en F, pero cuyos cuadrados sí lo están. Demostrar que $F(x) = F(y)$ si y sólo si x^2/y^2 es un cuadrado de F.

2.25 Sean p y q primos positivos. Mostrar que $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{q})$ si y sólo si $p = q$.

2.26 Sean x e y dos números complejos para los que se satisfacen las igualdades siguientes:

$$x^3 + 6x^2 + 1 = 0, \qquad y = x^7 + 6x^6 + x^4 + x^3 + 7x^2 + 2.$$

Determinar $[\mathbb{Q}(x) : \mathbb{Q}]$, mostrar que $y \neq 0$ y que $y^{-1} = -(x^2 + x - 31)/26$.

2.27 Dar el grado de la extensión $\mathbb{Q}(x)/\mathbb{Q}$ cuando x es un número complejo que es raíz de $X^4 + 1$, y cuando lo es de $X^6 + X^3 + 1$.

2.28 Sea K/F una extensión de cuerpos, x un elemento de K y f y g polinomios de $F[X]$ tales que $g(x) \neq 0$ y $f(x)/g(x)$ es un elemento algebraico de la extensión que no pertenece a F. ¿Es x un elemento algebraico de la extensión?

2.29 Sea t un elemento trascendente de la extensión K/F. ¿Es $F(t)/F$ necesariamente una extensión totalmente trascendente?

2.30 Sea t un número complejo trascendente, x e y elementos de $\mathbb{C}$ tales que $x^2 = 2t$, $y^2 = 3$. Hágase $K = \mathbb{Q}(t, x, y)$. Determinar $[K : \mathbb{Q}(t)]$. ¿Es $K = \mathbb{Q}(\sqrt{t}, \sqrt{2}, \sqrt{3})$?

2.31 Demostrar que todo subcuerpo de $\mathbb{C}$, que no está contenido en $\mathbb{R}$, es denso en $\mathbb{C}$.

2.32 Sea F un cuerpo de característica distinta de 2, K un cuerpo que es extensión del cuerpo F, x e y elementos de K con sus cuadrados en F, pero con $y \notin F$ y $x \notin F(y)$. Demostrar que $F(x+y) = F(x,y)$ y que el polinomio irreducible de $x+y$ sobre F es del tipo $X^4 + aX^2 + b$.

2.33 Sea F un cuerpo de característica distinta de 2 y K/F una extensión de grado 4. Demostrar la equivalencia de las dos afirmaciones siguientes:

1. La extensión K/F tiene algún cuerpo intermedio distinto de K y de F.
2. Existe algún $x \in K$ tal que $K = F(x)$ con polinomio irreducible sobre F del tipo $X^4 + aX^2 + b$.

2.34 Si $n > 0$ es un entero y z un elemento dado de un anillo A, se dirá que z es una *raíz n-ésima de la unidad* si se satisface la igualdad $z^n = 1$. Sea p un primo positivo y $\varepsilon \neq 1$ un número complejo que es raíz p-ésima de la unidad. Determinar $[\mathbb{Q}(\varepsilon) : \mathbb{Q}]$.

2.35 Sea $p > 0$ un número primo impar. Demostrar que $x = \cos(2\pi/p)$ es un número algebraico y que $[\mathbb{Q}(x) : \mathbb{Q}] = (p-1)/2$.

2.36 Sea p un número primo y x un número complejo que es raíz del polinomio $X^n - p$. Sea m un entero positivo tal que $m \mid n$. Demostrar que $[\mathbb{Q}(x^m) : \mathbb{Q}] = n/m$. Determinar el polinomio $\operatorname{irr}\big(x, X, \mathbb{Q}(x^m)\big)$.

2.37 Sea K un subcuerpo de $\mathbb{C}$ que es extensión finita de grado impar del cuerpo $\mathbb{Q}$. Mostrar que las únicas raíces de la unidad en K son 1 y -1.

2.38 Sea K/F una extensión finita de cuerpos en la que el conjunto de los cuerpos intermedios es totalmente ordenado respecto a la inclusión. Demostrar que K/F es monógena.

2.39 Sea $K = \mathbb{Q}(x)$ donde x es un número complejo para el que se verifica $x^3 - 2x^2 + 4x + 2 = 0$. Expresar $(x^3 + x + 1)(x^2 + x)$ y $(x-3)^{-1}$ en la forma $ax^2 + bx + c$, con $a, b, c \in \mathbb{Q}$.

2.40 Sea K/F una extesión de cuerpos. Supóngase que existe un entero positivo n para el que todo cuerpo intermedio E estrictamente contenido en K es tal que se verifica $[E : F] < n$. Demostrar que K es una extensión finita de F. [Indicación. Comprobar primero que K/F es una extensión algebraica].

2.41 Mostrar que toda extensión algebraica infinita tiene cuerpos intermedios que son extensiones finitas del cuerpo base de grado suficientemente grande.

2.42 Para cada entero $n \geq 1$ sea K_n el subcuerpo de $\mathbb{R}$ definido por la igualdad $K_n = \mathbb{Q}(\sqrt[n]{2})$.

1. Mostrar que $[K_n : \mathbb{Q}] = n$.

2. Comprobar que si $m|n$ entonces $K_m \subset K_n$. Determinar $[K_n : K_m]$.
3. Demostrar que, en el caso en que m y n sean primos relativos, se tiene entonces $K_{mn} = \mathbb{Q}(\sqrt[n]{2}, \sqrt[m]{2})$.

2.43 Sea K/F una extensión de cuerpos, x e y elementos de K algebraicos sobre F. Demostrar que $\mathrm{irr}(x, X, F)$ es irreducible sobre $F(y)$ si y sólo si $\mathrm{irr}(y, X, F)$ es irreducible sobre $F(x)$.

2.44 Sean K y L subcuerpos de un cuerpo común, ambos extensiones de un mismo cuerpo F. Supóngase que K/F es extension algebraica. Demostrar que el mínimo subcuerpo $L \vee K$ que contiene a L y K está formado por las sumas finitas $\sum x_i y_i$, donde los elementos x_i están en K y los y_i en L.

2.45 Sea $\mathcal{C}$ una clase de extensiones de cuerpos. Se dirá que $\mathcal{C}$ es una clase *distinguida* de extensiones si se satisfacen las dos condiciones siguientes: 1) $\mathcal{C}$ es una clase transitiva de extensiones; 2) si F, K, E, Ω son cuerpos, con F subcuerpo de K y E, con éstos últimos siendo subcuerpos de Ω, y si además K/F está en $\mathcal{C}$, entonces el menor subcuepo $K \vee E$ de Ω que contiene a K y E es tal que la extensión $(K \vee E)/E$ también pertenece a $\mathcal{C}$. Demostrar que si $\mathcal{C}$ es una clase distinguida de extensiones, F, K, E, Ω son cuerpos, con K y E subcuerpos de Ω, F subcuerpo de K y E, y si se verifica además que K/F y E/F están en $\mathcal{C}$ entonces también lo está $(K \vee E)/F$.

2.46 Demostrar que, tanto la clase de las extensiones finitas, como la de las extensiones algebraicas, son clases distinguidas de extensiones (Ver el ejercicio 2.45 para la definición de clase distinguida).

2.47 Sea K/F una extensión finita de cuerpos, L un cuerpo que es extensión de K y t un elemento de L que es trascendente sobre K. Demostrar que $K(t)/F(t)$ es también una extensión finita y que se tiene además $[K(t) : F(t)] = [K : F]$.

2.48 Sea K/F una extensión de cuerpos. Demostrar que dicha extensión es algebraica si y sólo si todo subanillo A de K tal que $F \subset A$ es necesariamente un cuerpo.

2.49 Hacer $x_1 = 2$ y definir $x_{n+1} = \sqrt{x_n}$ para todo entero $n > 1$. Demostrar que

$$[\mathbb{Q}(x_{n+1}) : \mathbb{Q}] = 2^n$$

y que el polinomio $X^{2^n} - 2$ es un polinomio irreducible de $\mathbb{Q}[X]$.

2.50 Sea $K = F(X)$ el cuerpo de funciones racionales en una indeterminada sobre el cuerpo F y E un cuerpo intermedio de la extensión K/F. Demostrar que $E \neq F$ si y sólo si K/E es una extensión finita. Determinar el grado de esta extensión cuando $E = F(X^3/(X+1))$.

2.51 Sea K/F una extensión de cuerpos. Supóngase:

1. La unión de cualquier cadena, respecto a la inclusión, de subcuerpos intermedios y distintos de K es distinto de K.

2. Todo cuerpo intermedio y distinto de K es una extensión finita de F.

Demostrar que K es una extensión finita de F.

2.52 Sea K/F una extensión de grado 2, $f \in K[X]$ un polinomio irreducible de grado 3 y x un elemento en un cuerpo extensión de K que es raíz de f. Supóngase que el término constante de f es un elemento de K que no está en F y que el resto de los coeficientes de f están en F. Demostrar que $[F(x) : F] = 6$.

2.53 Comprobar que el polinomio

$$f(X) = 4X^3 - 3X - \frac{-1+\sqrt{5}}{4}$$

es reducible en $\mathbb{Q}(\sqrt{5})[X]$.

2.54 Supongamos que el número complejo x tiene por polinomio irreducible sobre $\mathbb{Q}$ a $X^3 + aX^2 + bX + c$. Demostrar que la condición necesaria y suficiente para que exista algún $y \in \mathbb{Q}(x)$ tal que $y^2 = x$ es que existan $\alpha, \beta, \gamma \in \mathbb{Q}$ tales que

$$a = 2\beta - \alpha^2, \qquad b = \beta^2 - 2\alpha\gamma, \qquad c = -\gamma^2$$

[Indicación: Considerar el polinomio irreducible de y sobre $\mathbb{Q}$].

2.55

1. Mostrar que si u es un número complejo raíz del polinomio X^3+X^2-1 entonces u no tiene ninguna raíz cuadrada en $\mathbb{Q}(u)$.
2. Dar $\sqrt[3]{28} - 3$ como un cuadrado de $\mathbb{Q}(\sqrt[3]{28})$.

2.56 Sea K/F una extensión de cuerpos y S un subconjunto de K que no corta a F. Mostrar la existencia de algún cuerpo intermedio M de la extensión K/F que es maximal respecto a la inclusión en la familia de los subcuerpos de K que contienen a F y no cortan a S. Demostrar que si S es finito entonces K/M es una extensión algebraica.

2.57 Demostrar que, si $m_1, \ldots, m_n$ son enteros positivos primos relativos y ninguno de ellos cuadrado perfecto, entonces se tiene

$$[\mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_n}) : \mathbb{Q}] = 2^n.$$

2.58 Sea t un elemento trascendente sobre el cuerpo F y $K = F(t)$. Escríbase cada elemento no nulo de K como $u = f(t)/g(t)$ donde f y g son polinomios en una indeterminada, con $g \neq 0$, y tales que m.c.d.$(f, g) = 1$. Al máximo de los grados de f y g se llama *grado* de u y se denota por $\deg u$. Demostrar que si X e Y son dos indeterminadas distintas entonces $f(X) - Yg(X)$ es irreducible tanto en $F[X, Y]$ como en $F(Y)[X]$. Demostrar que si $u \notin F$ entonces t es algebraico sobre $F(u)$ y el polinomio irreducible de t sobre $F(u)$ coincide con el único polinomio mónico que puede obtenerse de $f(X) - ug(X)$ multiplicándolo por una constante no nula de $F(u)$. Concluir así que $[F(t) : F(u)] = \deg u$, cuando $u \notin F$ y, en particular, se verifica $F(t) = F(u)$ si y sólo si $u = (at + b)/(ct + d)$, donde $ad - bc \neq 0$.

2.59 Sea K/F una extensión de cuerpos, t y w elementos de K tales que t es trascendente sobre F y w es trascendente sobre $F(t)$. Demostrar que para cualesquiera enteros positivos n y m se tiene entonces $[F(t,w) : F(t^n, w^m)] = nm$.

2.60 Sea F un cuerpo, K y L cuerpos extensiones algebraicas de F que están contenidos como subcuerpos de un mismo cuerpo M. Sea $K \vee L$ el mínimo subcuerpo de M que contiene a K y a L. Establecer la desigualdad $[K \vee L : F] \leq [K : F][L : F]$, caracterizando los casos en que se da la igualdad mediante una propiedad de las bases del F-espacio vectorial K.

2.61 Sean F, K, L, M y $K \vee L$ cuerpos en las condiciones del ejercicio anterior. Supóngase además que K/F y L/F son ambas finitas. Caracterizar los casos en que se da la igualdad $[K \vee L : F] = [K : F][L : F]$ en términos de los polinomios irreducibles de los elementos de los subconjuntos finitos S tales que $K = F(S)$.

1. Demostrar que si $[K \vee L : F] = [K : F][L : F]$, entonces $K \cap L = F$.
2. Mostrar que en el caso en que $[K : F]$ y $[L : F]$ sean primos relativos se verifica entonces $[K \vee L : F] = [K : F][L : F]$.
3. Supóngase que $[M : F] = 4$, $[K : F] = 2 = [L : F]$, $K = F(x)$, $L = F(y)$. Demostrar la equivalencia de las propiedades siguientes: i) $K \neq L$, ii) $K \vee L = M$, iii) $\{1, x, y, xy\}$ es una base del F-espacio vectorial $K \vee L$.

2.62 Sea K/F una extensión algebraica de cuerpos tal que $K = F(x, y)$ con x e y elementos de K tales que $p = \deg \operatorname{irr}(x, X, F)$ y $q = \deg \operatorname{irr}(y, X, F)$ son primos positivos distintos. Mostrar que todo elemento z de K se escribe de manera única en la forma

$$z = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} c_{ij} x^i y^j, \qquad (c_{ij} \in F). \tag{1.2}$$

Demostrar que, si $p < q$ entonces $F(x)$ es el único cuerpo intermedio en la extensión K/F que es extensión de grado p del cuerpo F.

2.63 (Este ejercicio requiere cierta familiaridad con los rudimentos de la teoría de módulos). Sea K un cuerpo y A un subanillo de K. Mostrar que el cuerpo de cocientes F de A puede identificarse a un subcuerpo de K. Supóngase que K es finitamente generado como A-módulo. Descomponiendo K como suma directa de F y un cierto F-subespacio suplementario W, muéstrese que F es finitamente generado como A-módulo. Pruébese la igualdad $A = F$.

1.3. Construcciones con regla y compás

3.1 ¿Es posible construir con regla y compás un triángulo isósceles con vértices en la circunferencia unidad y de superficie unidad?

3.2 ¿Son todos los triángulos isósceles con vértices en la circunferencia unidad y de superficie unidad construibles con regla y compás?

3.3 Sea $\mathcal{A}$ un subconjunto del plano euclídeo con al menos 2 puntos distintos y $\mathbb{Q}(S)$ el subcuerpo de $\mathbb{R}$ asociado a él como en la página 65. Comprobar que el cuerpo $\mathbb{Q}(S)$ es independiente de la unidad de medida elegida.

3.4 Sea $\mathcal{A}$ el conjunto $\{(0,0),(1,0)\}$ de puntos del plano euclídeo y $\mathcal{R}$ un sistema de referencia apropiado para el mismo. Mostrar que si x es alguna de las raíces del polinomio X^4-6X^2+2 entonces el punto de coordenadas $(x,\sqrt{7})$ respecto a $\mathcal{R}$ es construible con regla y compás a partir de $\mathcal{A}$.

3.5 ¿Puede construirse con regla y compás el eneágono regular?

3.6 Demostrar que el ángulo θ puede trisecarse con regla y compás si y sólo si el polinomio

$$f(X)=4X^3-3X-\cos\theta$$

es reducible sobre $\mathbb{Q}(\cos\theta)$.

3.7 Suponer n y m enteros positivos tales que $m \mid n$. Mostrar que si el polígono regular de n lados es construible con regla y compás, entonces también lo es el de m lados.

3.8 Sean n y m enteros positivos primos relativos. Mostrar que, si los polígonos regulares de n y m lados son construibles con regla y compás, entonces el polígono regular de nm lados es también construible con regla y compás.

3.9 La *cisoide de Diocles* es la curva algebraica definida por la ecuación $y^2(1-x)-x^3=0$. Sea P el punto de intersección de la cisoide con la recta $y=2(-x+1)$. Mostrar que la recta que une el punto P al origen de coordenadas corta a la recta $x=1$ en el punto $(1,\sqrt[3]{2})$ y, en consecuencia, determina un segmento que puede tomarse como arista de un cubo doble del cubo unidad.

3.10 Mostrar que, para todo entero $n \geq 2$, el polígono regular de 2^n lados es construible con regla y compás y dar explícitamente la longitud del lado de dichos polígonos cuando se consideran inscritos en la circunferencia unidad. Demostrar que

$$\frac{2}{\pi}=\sqrt{\frac{1}{2}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}}\cdots$$

3.11 ¿Puede construirse con regla y compás el pentágono regular? Estudiar la exactitud de la siguiente construcción geométrica: sea OA un segmento de longitud unidad; trazar la circunferencia unidad de centro O y radio OA; construir el diámetro BB' perpendicular a OA, así como el punto medio I del segmento OB'; trazar la circunferencia de centro I y radio IA; si D es el punto de intersección de dicha circunferencia con el segmento OB, entonces AD es el lado del pentágono regular inscrito en la circunferencia de radio unidad y centro O.

3.12 ¿Puede trisecarse con regla y compás el ángulo $2\pi/5$?

3.13 ¿Es posible la quintisección del ángulo $\pi/3$ con regla y compás?

3.14 Comprobar que el ángulo θ no puede ser trisecado con regla y compás en los casos en que $\cos\theta$ sea un número real trascendente.

3.15 Mostrar que en el caso en que $\cos\theta = -5/6$ el ángulo θ no puede dividirse en cinco partes iguales con regla y compás.

3.16 ¿Cuál es el menor entero estrictamente positivo n para el que el ángulo de n grados puede ser construido con regla y compás?

3.17 Caracterizar los enteros n para los que el ángulo de n grados es construible con regla y compás.

3.18 Mostrar que para el ángulo de 3 grados se satisface la igualdad

$$\cos 3^0 = \frac{1}{8}(\sqrt{3}+1)\sqrt{5+\sqrt{5}} + \frac{1}{16}(\sqrt{6}-\sqrt{2})(\sqrt{5}-1).$$

Dar explícitamente una cadena de subcuerpos como la del teorema 1.3.2 que permita garantizar la constructibilidad con regla y compás del punto $(\cos 3^0, \operatorname{sen} 3^0)$.

3.19 Tómese un cuadrado $OABC$. Supóngase que el lado OB se mueve uniformemente girando alrededor de O y que durante el mismo intervalo de tiempo BC se traslada paralelamente a sí mismo con movimiento uniforme hasta hacer coincidir los segmentos OB y BC con OA. La intersección de los dos segmentos móviles determina en cada instante un punto X. El lugar geomético de los puntos X constituye una curva a la que se denomina *cuadratriz de Hipias.* Dar las ecuaciones en coordenadas polares y en coordenadas cartesianas de dicha curva.

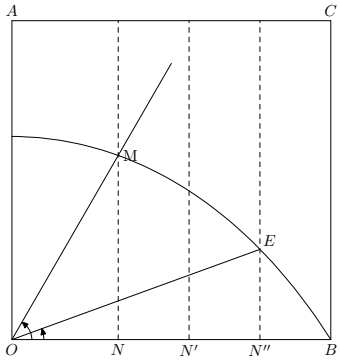


Figura 1.1: Trisección con cuadratriz

Supóngase dado un ángulo agudo en el que uno de sus lados se hace coincidir con OB y el otro está dentro l cuadrado $OABC$. Sea M el punto de intersección del último de los lados del ángulo con la cuadratriz, N la proyección ortogonal del punto M sobre el segmento OB y N'' el punto del segmento OB tal que $N''B = \frac{1}{3}NB$. Comprobar que la paralela a OA trazada desde N'' corta a la cuadratriz en un punto E tal que BOE es el ángulo tercio del ángulo dado. Comprobar que, si el cuadrado $OABC$ tiene lado unidad, entonces el punto Q_0 del segmento OA al que tienden los puntos de la cuadratriz es tal que el segmento OQ_0 es de longitud $\frac{2}{\pi}$, con lo que con auxilio de la cuadratriz puede construirse un cuadrado de igual área que el círculo unidad.

3.20 En la proposición 8 del *Libro de los Lemas,* Arquímedes da la siguiente construcción para trisecar ángulos: Sea $\widehat{ABC}$ un ángulo agudo que se desea trisecar. Con centro en B y radio arbitrario se traza una circunferencia $\mathcal{C}$, la cual corta a la semirrecta BC en el punto Q. Sea R el otro punto de intersección de la recta BC con la circunferencia y P el punto de intersección de la semirrecta BA con $\mathcal{C}$. Trazar una recta que pase por P, que corte a $\mathcal{C}$ en un punto T y a la semirrecta BR en un punto S, de modo que los segmentos ST y TB sean de igual longitud. Justifíquese cada una de las afirmaciones siguientes:

1. $\widehat{BST}$ es el ángulo tercio de $\widehat{ABC}$.

2. La construcción precedente no es una construcción con regla y compás.

3. Es posible trisecar cualquier ángulo con compás y una regla en la que se hayan marcado dos puntos que determinan un segmento de longitud unidad.

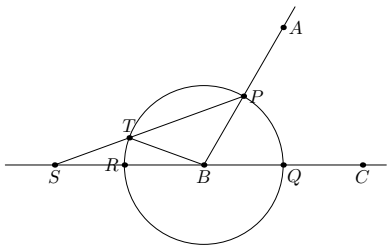


Figura 1.2: Construcción del Libro de los Lemas

3.21 (J. H. Conway) Sea k un número real estrictamente comprendido entre 0 y 1. Supóngase dado un sitema de referencia ortogonal en el plano eucídeo con origen en el punto O. Con radio unidad y haciendo centro en el punto $A = (k, 0)$ se traza una circunferenica cuya intersección con el semieje positivo de ordenadas es un punto B. Construir el punto P del semieje negativo de ordenadas tal que $OP = \frac{1}{3}OB$. Determinar el punto C sobre la recta PA, y el punto D en la intersección de las rectas BC y OA, de manera que $CD = 1$. Demostrar que $AD = 2\sqrt[3]{k}$. Mostrar que es posible construir el punto D con compás y una regla en la que se han hecho dos marcas, pero que hay valores de k para los que dicho punto no puede construirse con regla y compás.

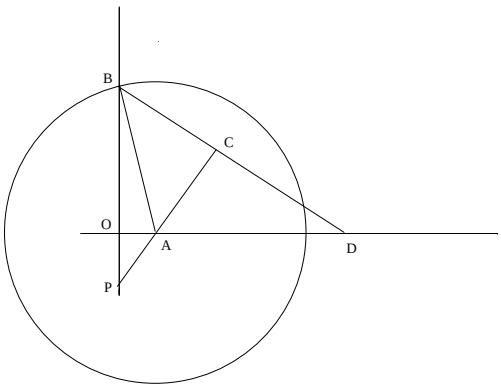


Figura 1.3: Construcción de segmento de longitud $2\sqrt[3]{k}$

3.22 Se define la *espiral de Arquímedes* como el lugar geométrico descrito por un punto que se mueve uniformemente sobre una semirrecta partiendo de su origen mientras ésta gira uniformemente en torno a dicho punto.

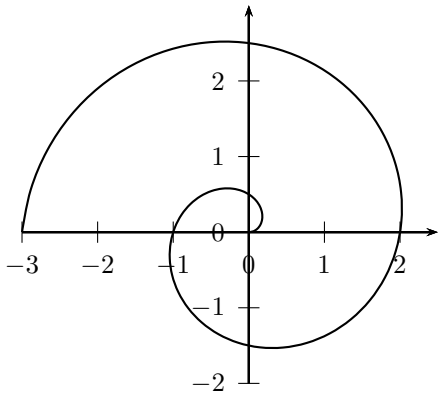


Figura 1.4: Espiral de Arquímedes

¿De qué modo puede utilizarse la espiral de Arquímedes para trisecar ángulos?

3.23 (Pappus). Sea $A\overset{\triangle}{O}H$ un triángulo con $\widehat{OHA}$ ángulo recto y $\widehat{HOA}$ el ángulo a trisecar. Sea a la longitud del segmento OA. Se traza la paralela r a OH que pasa por A. Sea s una recta que corta al segmento HA en el punto B, a la recta r en el punto C y de manera que el segmento BC tiene longitud $2a$. Demostrar que $\widehat{BOH} = \frac{1}{3}\widehat{AOH}$. Justificar por qué la construcción precedente no es una construcción con regla y compás.

3.24 (Descartes). Supóngase dados un segmento de longitud q y una parábola Γ de vértice A, y parámetro p. Sea $C \neq A$ un punto del eje e de la parábola que está a distancia $p/2$ del foco de Γ. Trazar una perpendicular a e que pase por C. Determinar sobre esta recta un punto E cuya distancia a C es $\frac{1}{2}q$ y trazar con centro en E y radio EA una circunferencia. Si $F \neq A$ es punto de intersección de Γ con la circunferencia y si L es su proyección ortogonal sobre e, pruébese que FL y LA son dos medias proporcionales entre segmentos de longitudes $2p$ y q.

3.25 Sea $\mathcal{A}$, S y K_0 como en el teorema 1.3.2. Un número real se dirá $\mathcal{A}$-*construible* si es alguna de las coordenadas de un punto construible con regla y compás a partir de $\mathcal{A}$. Comprobar que el conjunto de los números $\mathcal{A}$-constuibles C constituye un subcuerpo de $\mathbb{R}$ que contiene a K_0 y con la propiedad de que $c \in C$ y $c > 0$ implican $\pm\sqrt{c} \in C$. Comprobar que C es el menor subcuerpo de $\mathbb{R}$ que contiene a K_0 y que goza de dicha propiedad.

3.26 Sea $p \geq 3$ un número primo. Demostrar que, si el polígono regular de p lados es construible con regla y compás, entonces $p = 2^r + 1$, para algún entero $r > 1$.

3.27 Sea $r > 0$ un entero y $p = 2^r + 1$ un primo positivo. Comprobar que p se escribe en la forma $2^{2^n} + 1$ para cierto entero $n \geq 0$. Mostrar que si el polígono regular de p lados es constuible con regla y compás entonces

$p = 2^{2^n} + 1$ para algún entero $n \geq 0$. [A los números $F_n = 2^{2^n} + 1$ se llama *números de Fermat*. P. Fermat conjeturó que todos ellos debían ser primos. Euler mostró que esto no ocurre en el caso de F_5. A día de hoy los únicos números de Fermat que se sabe que son primos son F_0, F_1, F_2, F_3 y F_4].

3.28 Demostrar que el heptágono regular no es construible con regla y compás. ¿Cómo puede utilizarse el teorema 1.3.2 para caracterizar este hecho?

3.29 (Trisección con papiroflexia). Supóngase dada una hoja de papel rectangular de vértices O, A, B y C. Sea $\theta = \widehat{AOD}$ un ángulo agudo de vértice O que está totalmente contenido en la referida hoja de papel. Efectuar dos pliegues sucesivos de una misma anchura arbitraria para obtener dos rectas ℓ_1 y ℓ_2 paralelas al lado OA. Desplegar completamente el papel y volver a plegar de modo que O se lleva sobre un punto O' de la recta ℓ_1 mientras que el punto O_2 de intersección de ℓ_2 con el lado OB de la hoja se lleva a un punto de la semirrecta OD. Si O'_1 es el punto correspondiente a O_1 en el último pliegue, mostrar que entonces $\widehat{DOO'_1} = \frac{1}{3}\theta$.

3.30 Sea θ un ángulo arbitrario y $f(X)$ el polinomio de $\mathbb{R}[X]$ definido por la igualdad siguiente:

$$f(X) = 4X^3 - 3X - \cos\theta.$$

Mostrar que todas las raíces de $f(X)$ están en el intervalo $[-1, 1]$ y, en consecuencia, pueden verse como cosenos de ángulos. ¿Cuáles son estos ángulos?

3.31 Dados un punto P y un subconjunto $\mathcal{A}$ del plano euclídeo con al menos dos puntos distintos, se define la *constructibilidad con regla, compás y trisector de ángulos* de P a partir de $\mathcal{A}$ de modo semejante a como se definió la constructibilidad con regla y compás sin más que añadir entre las posibilidades de constructibilidades atómicas el que P pueda también ser punto de intersección de una recta r que triseca algún ángulo subtendido por dos semirrectas, cada una de las cuales pasa por dos puntos distintos de $\mathcal{A}$, con alguna de las figuras geométricas siguientes: (i) una circunferencia que tiene su centro en un punto de $\mathcal{A}$ y cuyo radio es la distancia existente entre dos puntos de $\mathcal{A}$, (ii) una recta que pasa por dos puntos distintos de $\mathcal{A}$ y que es distinta de r, (iii) una recta distinta de r que triseca algún ángulo subtendido por semirrectas distintas, cada una de las cuales pasa por dos puntos distintos de $\mathcal{A}$. Sea S el conjunto de coordenadas de puntos de $\mathcal{A}$ respecto a un sistema de referencia apropiado para $\mathcal{A}$. Denótese por K_0 al subcuerpo $\mathbb{Q}(S)$. Supóngase que x es algún número complejo raíz del polinomio $f(X) = X^3 - pX + q$ de coeficientes en K_0. Demostrar que si $p > 0$ y $|q\sqrt{27/p^3}| < 2$ entonces x es real y el punto $(x, 0)$ es construible con regla, compás y trisector de ángulos a partir de $\mathcal{A}$. [Indicación. Buscar raíces de f del tipo $2\sqrt{\frac{p}{3}}\cos\frac{\theta}{3}$.]

3.32 Probar la constructibilidad con regla, compás y trisector de ángulos del polígono regular de 7 lados.

3.33 Sea $\mathcal{A}$ un subconjunto de puntos del plano euclídeo, S el subconjunto de las coordenadas de los puntos de $\mathcal{A}$ respecto a un sistema de referencia apropiado. Hágase $K_0 = \mathbb{Q}(S)$. Demostrar que el punto $P = (x, y)$ es construible con regla, compás y trisector de ángulos a partir de $\mathcal{A}$ si y sólo si existe una cadena de subcuerpos de $\mathbb{R}$

$$K_0 \subset K_1 \subset \cdots \subset K_n, \tag{1.3}$$

eventualmente reducida a K_0, y para la que se satisfacen las dos condiciones dadas a continuación:

1. Cada K_i es una extensión cuadrática de K_{i-1} o una extensión cúbica del tipo $K_i = K_{i-1}(u_i)$ donde u_i es raíz de un polinomio $f_i(X) = X^3 - p_i X + q_i$ con coeficientes en K_{i-1} y tal que $p_i > 0$, $|q_i\sqrt{27/p_i^3}| < 2$.
2. $x, y \in K_n$.

3.34 ¿Puede resolverse el problema de la cuadratura del círculo con la ayuda adicional de un trisector de ángulos?

3.35

1. Sea $f(X) = X^3 - pX + q$ un polinomio con coeficientes reales. Demostrar que el polinomio f tiene tres raíces reales distintas si y sólo si $p > 0$ y $|q\sqrt{27/p^3}| < 2$.
2. Sea K/F una extensión de cuerpos de grado 3, con K subcuerpo de $\mathbb{C}$ y F subcuerpo de $\mathbb{R}$. Sea $x \in K$ tal que $x \notin F$. Mostrar que $\mathrm{irr}(x, X, F)$ tiene tres raíces reales distintas si y sólo si existe algún elemento u de K tal que $K = F(u)$, con $\mathrm{irr}(u, X, F) = X^3 - pX + q$ y de manera que para los coeficientes de $\mathrm{irr}(u, X, F)$ se satisfacen las desigualdades $p > 0$ y $|q\sqrt{27/p^3}| < 2$. [Indicación. Considerar el polinomio $f(X - \frac{a}{3})$, siendo a el coeficiente de X^2 en el polinomio $\mathrm{irr}(x, X, F)$].

3.36 ¿De qué manera puede usarse el ejercicio 3.35 para reformular la caracterización de la constructibilidad con regla, compás y trisector de ángulos dada en el ejercicio 3.33?

1.4. Extensión de inmersiones. Consecuencias

4.1 Dar algún número real x, con $x \notin \mathbb{Q}$, para el que se tenga:

1. $\mathbb{Q}(x)$ y $\mathbb{Q}(\mathrm{i}x)$ son isomorfos.
2. $\mathbb{Q}(x)$ y $\mathbb{Q}(\mathrm{i}x)$ no son isomorfos.

4.2 Sea F un subcuerpo de $\mathbb{R}$ y K uno de $\mathbb{C}$. Suponer K una extensión de grado primo p del cuerpo F. Demostrar que, si existe algún $x \in K$ tal que $\mathrm{irr}(x, X, F)$ tiene p raíces reales distintas, entonces esto ocurre para el polinomio irreducible $\mathrm{irr}(y, X, F)$ de todo elemento $y \in K$ que no pertenece a F.

4.3 Mostrar que no es posible la duplicación del cubo con regla, compás y trisector de ángulos.

4.4 Usar inducción para demostrar el teorema 1.4.2 en el caso en que S es un subconjunto finito de K.

4.5 Sea $F = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}(\sqrt[4]{2})$ y $\sigma : F \longrightarrow F$ el automorfismo $\sigma : \alpha+\beta\sqrt{2} \mapsto \alpha - \beta\sqrt{2}$. ¿Puede σ extenderse a un automorfismo de K?

4.6 Mostrar que la identidad es el único automorfismo del cuerpo $\mathbb{R}$ de los número reales.

4.7 Sea K un subcuerpo de $\mathbb{C}$, siendo $K/\mathbb{Q}$ una extensión finita. Mostrar que el conjunto de las inmersiones $\sigma : K \longrightarrow \mathbb{C}$ tales que $\sigma(K) \not\subset \mathbb{R}$ tiene cardinal par.

4.8 Sea a un número racional y x una raíz del polinomio $X^4 + a$. Demostrar que el número de inmersiones de $\mathbb{Q}(x)$ en $\mathbb{C}$ es distinto de 4 si y sólo si se verifica alguna de las dos alternativas siguientes: (i) $-a$ es el cuadrado de un número racional, (ii) $4a$ es potencia cuarta de algún racional.

4.9 Sea K/F una extensión de cuerpos, t un elemento trascendente de la extensión, L un cuerpo y $\sigma : F \longrightarrow L$ una inmersión. Comprobar que el conjunto de las inmersiones $\tau : F(t) \longrightarrow L$ que extienden a σ está en biyección con el conjunto de los elementos de L que son trascendentes sobre $\sigma(F)$.

4.10 Demostrar que todo cuerpo algebraicamente cerrado es infinito.

1.5. Clausura algebraica

5.1 Sea x una raíz del polinomio $X^2 + X + 1$ de $\mathbb{Z}/(2)[X]$. Dar las tablas de sumar y multiplicar del cuerpo $[\mathbb{Z}/(2)](x)$.

5.2 ¿Cuál es el cardinal de la clausura algebraica de un cuerpo finito?

5.3 Mostrar que el cuerpo A de los números algebraicos es una clausura algebraica de $\mathbb{Q}$.

5.4 Sea $x \in \mathbb{C}$ una raíz del polinomio $f(X) = X^3 - 2$ de $\mathbb{Q}[X]$. ¿Es $\mathbb{Q}(x)$ cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$?

5.5 Dar el cuerpo de descomposición de $X^6 + 1$ sobre $\mathbb{Z}/(2)$.

5.6 Mostrar que cualquier extensión algebraica de un cuerpo F puede sumergirse en la clausura algebraica de dicho cuerpo, y que cualquier extensión algebraica de F con la propiedad de contener alguna copia F-isomorfa de cada uno de los cuerpos que son extensión algebraica de F coincide, salvo F-isomorfismos, con la clausura algebraica de F.

5.7 Demostrar que la extensión de cuerpos K/F es algebraica si y sólo si para todo cuerpo intermedio E se verifica que cualquier inmersión de E en sí mismo que induce la identidad sobre F es necesariamente un F-automorfismo de E.

5.8 Sea f el polinomio de $\mathbb{Q}[X]$ definido por la igualdad $f(X) = X^4 - 4X^2 + 1$ y K el cuerpo de descomposición de f sobre $\mathbb{Q}$. Mostrar que $\sqrt{3} \in K$. Determinar el el grado de la extensión $K/\mathbb{Q}$, así como las $\mathbb{Q}$-inmersiones de K en $\mathbb{C}$.

5.9 Sea K/F una extensión de cuerpos, x un elemento algebraico de la extensión y E un cuerpo intermedio. Mostrar que los coeficientes de $\operatorname{irr}(x, X, E)$ son algebraicos sobre F.

5.10 Demostrar que, sobre cualquier cuerpo F, el cuerpo de descomposición del polinomio $f(X) = X^3 - 3X + 1$ coincide con el propio F o es una extensión de grado 3 del mismo. [Indicación: Mostrar que si x es raíz de f entonces $x^2 - 2$ también lo es].

5.11 Si el conjunto de polinomios no constantes $\mathcal{F}$ es finito, ¿puede darse alguna demostración del teorema 1.5.6 que no dependa de ninguna de las equivalencias del axioma de elección?

5.12 Sea K/F una extensión algebraica. Mostrar que para todo polinomio $f(X)$ de $K[X]$ existe siempre algún polinomio no nulo $h \in K[X]$ tal que $fh \in F[X]$.

5.13 Sea F un cuerpo, f y g polinomios de $F[X]$. Suponer f irreducible y g no constante. Mostrar que si $h \in F[X]$ es un factor irreducible del polinomio $f(g(X))$ entonces el grado de f divide al grado de h.

5.14 Sea f un polinomio de grado $n \geq 1$ del anillo de polinomios $F[X]$ y K el cuerpo de descomposición de f sobre F. Sea $f = \prod_{i=1}^{r} p_i^{t_i}$ la factorización de f en polinomios irreducibles de $F[X]$. Demostrar que $[K : F]$ divide a $(\deg p_1)! \cdots (\deg p_r)!$

5.15 Sea K/F una extensión finita de cuerpos cuyo grado n es primo con el grado del polinomio $f(X) \in F[X]$. Demostrar que, si f es irreducible sobre F, lo es también sobre K.

5.16 Sea F un cuerpo, $\bar{F}$ una clausura algebraica de F, y x e y elementos de $\bar{F}$ tales que $[F(x) : F] = n$ y $[F(y) : F] = m$, con n y m primos relativos. Sean $x', y' \in \bar{F}$ tales que x' es raíz de $\operatorname{irr}(x, X, F)$ e y' es raíz de $\operatorname{irr}(y, X, F)$. ¿Existe algún F-automorfismo σ de $\bar{F}$ tal que $\sigma(x) = x'$ y $\sigma(y) = y'$?

5.17 Sea K/F una extensión cuadrática y $f \in F[X]$ un polinomio irreducible de grado 6. Comprobar que f es irreducible en $K[X]$ o se descompone en dicho anillo de polinomios como producto de dos polinomios irreducibles de grado 3.

5.18 Sean n, $m > 0$ enteros primos relativos, F un cuerpo y $X^n - a$ un polinomio irreducible en $F[X]$. Demostrar que $X^n - a^m$ es también irreducible.

5.19 Sea K el cuerpo de descomposición sobre $\mathbb{Q}$ de un polinomio de grado 8 que es reducible sobre $\mathbb{Q}$, pero que no admite raíces en $\mathbb{Q}$. Demostrar que $[K : \mathbb{Q}] \leq 1.440$.

5.20 Sea p un primo positivo y K el cuerpo de descomposición del polinomio $X^p - 2$ sobre $\mathbb{Q}$. Calcular $[K : \mathbb{Q}]$.

5.21 Sea F un cuerpo de característica 2, K un cuerpo que es extensión cuadrática de F. Demostrar que existe algún $a \in F$ de modo que K es cuerpo de descomposición sobre F de algún polinomio irreducible que es del tipo $X^2 - a$ o del tipo $X^2 - X - a$.

5.22 Sea F un cuerpo de característica distinta de 2 y a, b elementos distintos de F. Sea K el cuerpo de descomposición sobre F del polinomio $X^4 - (a+b)X^2 + ab$. Demostrar que $[K : F] = 4$ si y sólo si a, b y ab no son cuadrados en F.

5.23 ¿Existen automorfismos del cuerpo $\mathbb{C}$ de los números complejos distintos de la identidad y la conjugación?

5.24 Comprobar que los únicos automorfismos *continuos* de $\mathbb{C}$ son la identidad y la conjugación

5.25 Sea K/F una extensión algebraica de cuerpos. Demostrar que K es algebraicamente cerrado si y sólo si todo polinomio no constante de $F[X]$ tiene todas sus raíces en K.

5.26 Sea F un cuerpo de cardinal numerable. Mostrar directamente, sin usar el teorema 1.5.4, que F tiene una clausura algebraica.

5.27 Sea F un cuerpo de característica p, con p primo positivo. Considérese el polinomio $f(X) = X^p - X - a$ de $F[X]$.

1. Comprobar que si f tiene alguna raíz en el cuerpo F entonces las tiene todas.
2. Mostrar que, en el caso en que f no tiene ninguna raíz en F, el polinomio f es entonces irreducible en $F[X]$ [Indicación. Suponer la existencia de una factorización $f(X) = g(X)h(X)$ con $r = \deg g < p$, siendo $r \geq 1$, y llegar a una contradicción tras estudiar el coeficiente de X^{r-1} en g.]
3. Mostrar que el cuerpo de descomposición K de f sobre F tiene grado 1 ó p. Dar explícitamente ejemplos de ambas posibilidades.

4. Si x es un número complejo raíz del polinomio $X^p - X - a$ y a es un entero tal que $a \not\equiv 0 \pmod{p}$, demuéstrese que $[\mathbb{Q}(x) : \mathbb{Q}] = p$.

5.28 Sea F un cuerpo de caracterísitica p. Demostrar que el conjunto $A = \{c^p - c : c \in F\}$ es un subgrupo aditivo de F y que el polinomio $X^p - X - a$, $(a \in F)$, es un polinomio irreducible de $F[X]$ si y sólo si $a \notin A$.

5.29 Sea $f(X) = X^p - X - a$ un polinomio con coeficientes en un cuerpo F de característica el primo positivo p. Supóngase K una extensión del cuerpo F y $x \in K$ una raíz de $f(X)$ tal que $x \notin F$. Si $y \in K$ es una raíz del polinomio $X^p - X - ax^{p-1}$, determínese el grado de la extensión $F(x, y)/F$.

5.30 Sea p un primo positivo y F un cuerpo de característica p. Mostrar que el polinomio $X^p - a$ de $F[X]$ es, o bien, irreducible sobre F, o bien, la potencia de un polinomio lineal de $F[X]$.

5.31 Sea F un cuerpo de característica p, Ω una clausura algebraica de F y x un elemento de Ω, que no está en F, tal que $x^p \in F$. Hacer $y_1 = x$. Para cada entero $s > 1$ defínase y_s como el único elemento de Ω para el que se tiene la igualdad $y_s^p = y_{s-1}$. Mostrar que $[F(y_s) : F] = p^s$.

5.32 Sea F un cuerpo, m y n enteros positivos primos relativos. Demostrar que el polinomio $X^{mn} - a$ de $F[X]$ es irreducible si y sólo si los polinomios $X^m - a$ y $X^n - a$ lo son.

5.33 Sea F un cuerpo y $f(X) \in F[X]$ un polinomio de grado n estrictamente mayor que 1. Comprobar que f es irreducible si y sólo si f no tiene raíces en ningún cuerpo K extensión de F tal que $[K : F] \leq n/2$.

5.34 Mostrar que un anillo es dominio de integridad si y sólo si puede sumergirse en un cuerpo algebraicamente cerrado.

5.35 (E. Artin). Sea F un cuerpo y S el conjunto de todos los polinomios no constantes de $F[X]$. Sea $A = F[X_f]_{f \in S}$ el anillo de polinomios con coeficientes en F y cuyo conjunto de indeterminadas tiene una y sólo una indeterminada distinta X_f por cada polinomio $f \in S$. Demostrar que el ideal de A generado por el conjunto $\{f(X_f) : \ f \in S\}$ es distinto de A. Sea $\mathfrak{m}$ un ideal maximal de A que contiene al ideal anterior. Demostrar que $F_1 = A/\mathfrak{m}$ es una extensión de un cuerpo F_0 isomorfo a F en la que todo polinomio no constante de $F_0[X]$ tiene alguna raíz y mostrar a partir de aquí la existencia de alguna clausura algebraica del cuerpo F.

5.36 Sea F un cuerpo, F_0 el subconjunto de $F[X] \times \mathbb{N}$ formado por los elementos $(X - a, 0)$, $a \in F$. Mostrar que F_0 es un cuerpo respecto a la suma y el producto definidos de la manera siguiente

$$\begin{aligned} (X - a, 0) + (X - b, 0) &= (X - (a + b), 0), \\ (X - a, 0)(X - b, 0) &= (X - ab, 0), \end{aligned}$$

y que la aplicación $\theta : F \longrightarrow F_0$ que a cada $a \in F$ asocia $(X - a, 0)$ es un isomorfismo de cuerpos. Sea D el conjunto de las extensiones E de F_0

cuyo conjunto subyacente está contenido en $F[X] \times \mathbb{N}$ y que gozan de la siguiente propiedad: si $(f, n) \in E$ entonces (f, n) es una raíz del polinomio f^θ. Ordenar parcialmente D respecto a la relación de extensión. Demostrar que existe en D algún elemento maximal M y que M es clausura algebraica de F_0. Obtener de aquí la existencia de clausura una algebraica $\bar{F}$ del cuerpo F y de un isomorfismo $\rho : \bar{F} \longrightarrow M$ tal que $\rho(a) = \theta(a)$ para todo $a \in F$.

1.6. Extensiones normales

6.1 Sea K/F una extensión de cuerpos tal que $K = F(S)$ y siendo $[F(x) : F] \leq 2$ para todo $x \in S$. Demostrar que K/F es una extensión normal.

6.2 Sea K/F una extensión de cuerpos y $\{E_i\}_{i\in I}$ una familia de cuerpos intermedios de dicha extensión tal que cada una de las extensiones E_i/F es normal. Demostrar que la intersección $\bigcap_{i\in I} E_i$ es una extensión normal de F.

6.3 Sean F, K y L cuerpos, cada uno de ellos extensión algebraica del precedente. Demostrar que la clausura normal $\mathrm{nc}(L/F)$ de L/F contiene un subcuerpo que contiene a L y que es K-isomorfo a la clausura normal de L/K.

6.4 Sea Ω una clausura algebraica del cuerpo F. Supóngase K un subcuerpo de Ω que es extensión de F y sea $\{N_i\}_{i\in\mathcal{I}}$ la familia de los subcuerpos de Ω que contienen a K y son extensión normal de F. Mostrar que $L = \bigcap_{i\in\mathcal{I}} N_i$ es clausura normal de K.

6.5 Sea K/F una extensión normal y E un cuerpo intermedio de dicha extensión. Demostrar que E/F es normal si y sólo si $\sigma(E) \subset E$ para todo F-automorfismo σ de K.

6.6 Sean L/K y K/F extensiones normales. Supóngase que todo F-automorfismo de K se extiende a un automorfismo de L. Demostrar que la extensión L/F es normal.

6.7 Sean K/F y E/F extensionnes normales con K y E contenidos en un cuerpo Ω que es clausura algebraica del cuerpo F. Si K y E son F-isomorfos, ¿se tiene necesariamente $K = E$?

6.8 Sea K/F una extensión de grado 5 y $f \in F[X]$ un polinomio irreducible de $F[X]$ de grado 5. Suponer que el cuerpo de descomposición de f sobre F tiene grado 120. Demostrar que f es irreducible sobre K o tiene alguna raíz en K. Mostrar que en el caso en que K/F es extensión normal la segunda posibilidad no puede presentarse

6.9 Sea L/F una extensión de cuerpos, x e y elementos algebraicos de L. Supóngase que K (resp. E) es cuerpo de descomposición de $\mathrm{irr}(x, X, F)$ (resp. $\mathrm{irr}(y, X, F)$) contenido en L. Mostrar que si $F(x) \subset F(y)$ entonces $K \subset E$. ¿Se satisface el recíproco?

6.10 Sea F un subcuerpo de $\mathbb{R}$ y K una extensión normal de F de grado primo p. Demostrar que si $p > 2$ entonces K es F-isomorfo a algún subcuerpo de $\mathbb{R}$.

6.11 Demostrar que $\mathbb{Q}(\sqrt{2}, \mathrm{i})$ es una extensión normal de $\mathbb{Q}$ y que cada una de las raíces del polinomio irreducible $X^4 - 2X^2 + 9$ genera a $\mathbb{Q}(\sqrt{2}, \mathrm{i})$ sobre $\mathbb{Q}$.

6.12 Mostrar que el cuerpo generado sobre $\mathbb{Q}$ por alguna de las raíces del polinomio $f(X) = X^3 - X + 1$ *no* es extensión normal de $\mathbb{Q}$.

6.13 Sea K/F una extensión de cuerpos, x e y elementos algebraicos de la extensión. Suponer que $F(y)/F$ es extensión normal y que $F(x) \cap F(y) = F$. Demostrar que $\mathrm{irr}(y, X, F(x)) = \mathrm{irr}(y, X, F)$.

6.14 Sea L/F una extensión de cuerpos, K y E cuerpos intermedios de la extensión tales que $[K : F] = 3 = [E : F]$, $K \neq E$. Si $K \vee E$ es el menor subcuerpo de L que contiene a K y E, mostrar que entonces $[K \vee E : F] = 6$ ó 9 y que se presenta el primer caso si y sólo si existe algún F-automorfismo $\sigma : K \vee E \longrightarrow K \vee E$ tal que $\sigma(K) = E$.

6.15 Sean K/F y L/F extensiones normales y finitas. Comprobar que existe alguna F-inmersión $\sigma : K \longrightarrow L$ si y sólo si hay dos polinomios no constantes f y g de $F[X]$ con $f \mid g$ tal que K es cuerpo de descomposición de f y L cuerpo de descomposición de g.

6.16 ¿Existe algún automorfismo del cuerpo A de los números algebraicos que transforma $\sqrt{2}$ en $-\sqrt{2}$ y $\sqrt{5}$ en $-\sqrt{5}$?

6.17 Sea K/F una extensión algebraica. Demostrar que K/F es una extensión normal si y sólo si para todo $x \in K$ existe algún subcuerpo E de K que contiene a x y que constituye una extensión finita y normal de F.

6.18 Sean K/F y L/K extensiones de cuerpos. Suponer que L/F es cuerpo de descomposición de algún polinomio no constante $f \in F[X]$ con la propiedad de que cada uno de los factores irreducibles de f en $F[X]$ tiene alguna raíz en K. ¿Es necesariamente L/K una clausura normal de K/F?

6.19 Demostrar que la clase de las extensiones normales satisface la segunda de las condiciones exigidas en la definición de clase distinguida de extensiones (ver el ejercicio 2.45).

6.20 Sea Ω una clausura algebraica del cuerpo F, L un cuerpo intermedio de la extensión Ω/F y

$$K = \{x \in \Omega : L \text{ contiene todas las raíces de } \mathrm{irr}(x, X, F)\}.$$

Demostrar que K es un subcuerpo de L y que K/F es una extensión normal.

6.21 Sea $f(X)$ un polinomio irreducible de $\mathbb{Q}[X]$ que tiene raíces reales y no reales y K el subcuerpo de $\mathbb{C}$ que es cuerpo de descomposición de f sobre $\mathbb{Q}$.

1. Demostrar que el grupo de Galois de la extensión $K/\mathbb{Q}$ no es abeliano y comprobar que la hipótesis de irreducibilidad no puede suprimirse.
2. Comprobar que si f tiene una única raíz real entonces la parte real de cada una de sus raíces complejas no reales no puede ser un número racional.

6.22 Sea K/F una extensión normal y $f(X)$ un polinomio irreducible de $F[X]$. Supóngase que g y h son polinomios mónicos irreducibles de $K[X]$ que son factores de f. Demostrar que existe algún F-automorfismo σ de K tal que $g^\sigma = h$. Dar un ejemplo de una extensión que no sea normal y en la que no se tenga un resultado de este tipo.

6.23 Sea K/F una extensión algebraica de cuerpos. Demostrar que la extensión es normal si y sólo si los factores irreducibles en $K[X]$ de cada polinomio irreducible de $F[X]$ tienen el mismo grado.

1.7. Extensiones separables

7.1 Sea a un elemento de una extensión de $\mathbb{Z}/(3)$. Demostrar que el polinomio $X^3 - 2a$ de coeficientes en $(\mathbb{Z}/(3))(a)$ no es separable.

7.2 Sea F un cuerpo de característica distinta de 2 y 3. Mostrar que un polinomio $f \in F[X]$ del tipo $f(X) = 4X^3 - 3X - a$ tiene alguna raíz múltiple en una clausura algebraica de F si y sólo si $a = \pm 1$. Determinar en ambos casos todas las raíces de f. ¿Están dichas raíces en F?

7.3 La hipótesis de ser en el ejercicio 4.2 distintas todas las raíces del polinomio $\mathrm{irr}(x, X, F)$, ¿puede suprimirse?

7.4 Sea F un cuerpo de característica el primo positivo p y f un polinomio de $F[X]$ que tiene alguna raíz múltiple. Demostrar que si p no divide al grado de f entonces f no puede ser irreducible.

7.5 Sea F un cuerpo de característica 2. Demostrar que los cuerpos que son extensión cuadrática y separable de F coinciden con los cuerpos del tipo $F(x)$ para x raíz de un polinomio irreducible de $F[X]$ que se escribe en la forma $X^2 + X + a$.

7.6 Sea m un entero mayor o igual que 2, F un cuerpo de característica cero, $f \neq 0$ un polinomio de $F[X]$ y x una raíz de f en F. Demostrar que x es raíz múltiple de multiplicidad m si y sólo si x es raíz de multiplicidad $m-1$ del polinomio f'.

7.7 Sea F un cuerpo de característica cero. Demostrar que un polinomio mónico f de $F[X]$ es divisible por su derivada formal si y sólo si f es potencia de un polinomio de $F[X]$ del tipo $X - x$.

7.8 Sea K/F una extensión de cuerpos y f y g polinomios irreducibles en $F[X]$. Supóngase que K es cuerpo de descomposición sobre F tanto de f como de g. Mostrar que f es separable sobre F si y sólo si lo es g.

7.9 Sea K un subcuerpo de $\mathbb{C}$, siendo $K/\mathbb{Q}$ una extensión normal y finita de grado impar. Mostrar que K es un subcuerpo de $\mathbb{R}$.

7.10 Sea K/F una extensión normal y separable, $f \in F[X]$ un polinomio de grado primo p, con todas sus raíces en K y alguna de ellas no perteneciendo a F. Sea G el grupo de Galois de la extensión K/F y E un cuerpo intermedio de la extensión K/F, que es extensión finita de F, que contiene al conjunto S de las raíces de f y tal que $[E : F]$ divide a $p-1$. Suponer que el conjunto S de las raíces de f en el cuerpo K goza de las dos propiedades siguientes:

1. Para todo $y \in S$, cuya órbita $Gy = \{\sigma(y) : \ \sigma \in G\}$ es de cardinal estrictamente mayor que 1, se tiene $F(y) = E$.
2. Si S contiene al menos dos elementos distintos que pertenecen a F entonces $E = F$.

Demostrar que f tiene una única raíz en F y las restantes raíces de f en E tienen polinomio irreducible sobre F de un mismo grado $d > 1$, siendo además E cuerpo de descomposición de f sobre F y $[E : F] = d$.

7.11 (Fórmula de Taylor para polinomios). Sea F un cuerpo de característica cero, f un polinomio de $F[X]$ de grado n. Para cada entero positivo k, denótese por $f^{(k)}$ al polinomio obtenido a partir de f aplicándole k veces el operador de derivada formal. Convéngase que $f^{(0)} = f$. Demostrar que para todo $a \in F$ se tiene

$$f(X + a) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} X^k.$$

7.12 Sea F un cuerpo de característica cero y f un polinomio de $F[X]$. Demostrar que las sucesivas derivadas formales de f se anulan en un punto dado a si y sólo si f es un polinomio constante. La hipótesis sobre la característica del cuerpo, ¿puede suprimirse?

7.13 Sea A un anillo no necesariamente conmutativo. Una aplicación $D : A \longrightarrow A$ se dice que es una *derivación* de A si D es un endomomorfismo del grupo abeliano subyacente a A y se tiene además que $D(xy) = D(x)y + xD(y)$ para cualesquiera x, $y \in A$. Si C es un subanillo de A y D se anula en

cada uno de los elementos de C se dice entonces que D es una C-derivación de A. Mostrar que si $1/2 \in C$, entonces una derivación D de A es una C-derivación si y sólo si es C-lineal (i. e. $D(cx) = cD(x)$ para cualesquiera $x, y \in A$ y $c \in C$). Dadas dos derivaciones (resp. C-derivaciones) D_1 y D_2 de A, comprobar que la aplicación $[D_1, D_2]$ definida mediante la igualdad

$$[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$$

es también una derivación (resp. C-derivación) de A. Mostrar que para cada $x \in A$ la aplicación $D_x : A \longrightarrow A$ definida de manera que $D_x : y \mapsto xy - yx$ es una derivación de A. [De las derivaciones D_x se dice que son *derivaciones interiores* de A].

7.14 Sea A un anillo conmutativo y con unidad. Mostrar que el anillo de polinomios $A[X]$ tiene una única A-derivación que transforma X en 0. ¿Cuál es esa A-derivación? Comprobar que para toda A-derivación D de $A[X]$ y todo polinomio f de $A[X]$ se satisface la igualdad

$$D(f) = f'D(X).$$

7.15 Sea F un cuerpo y D una F-derivación de $F[X]$. Mostrar que D se extiende de manera única a una F-derivación de $F(X)$.

7.16 Sea x un elemento algebraico de la extensión de cuerpos K/F. Demostrar que x es separable sobre F si y sólo si la derivación nula es la única F-derivación de $F(x)$.

7.17 Demostrar que no existen extensiones separables de grado de separabilidad numerable.

7.18 Si K/F es una extensión separable, ¿se satisface siempre la igualdad $[K : F]_s = [K : F]$?

7.19 La clausura normal de una extensión separable, ¿es necesariamente separable?

7.20 Demostrar que un cuerpo F de característica p es perfecto si y sólo si su endomorfismo de Frobenius $\varphi : x \mapsto x^p$ es suprayectivo.

7.21 Sea K/F una extensión algebraica de cuerpos. Comprobar que si F es perfecto entonces K también lo es. Demostrar que, en el caso en que K/F es una extensión finita, el cuerpo F es perfecto si y sólo si lo es el cuerpo K.

7.22 Dar un ejemplo de un cuerpo no perfecto y de una extensión algebraica suya que sea cuerpo perfecto

7.23 Sea p un primo positivo y F un cuerpo de característica p. Supóngase que $\varphi : F \longrightarrow F$ es el endomorfismo de Frobenius. Hágase $F_0 = \bigcap_{n \geq 0} \operatorname{Im} \varphi^n$. Compruébese que F_0 es un cuerpo perfecto y que cualquier subcuerpo perfecto de F está contenido en F_0.

7.24 Sea p un primo positivo, F un cuerpo de característica p y K un cuerpo que es extensión de F. Demostrar que para todo elemento x de K que sea algebraico sobre F existe algún entero $n \geq 0$ tal que x^{p^n} es separable sobre F.

7.25 Sea F un cuerpo de característica p, K/F una extensión separable y x un elemento de K tal que $x^n \in F$ para algún entero $n > 0$. Demostrar que existe algún entero m, que divide a n y no es divisible por p, para el que se tiene $x^m \in F$.

7.26 Sea F un cuerpo cuya característica es un primo positivo p. Sea a un elemento no nulo de F y K una extensión de F que es cuerpo de descomposición del polinomio $X^n - a$. Supóngase K/F extensión separable. Sea m el mayor entero positivo que divide a n y que no es divisible por p. Mostrar que K contiene todas las raíces m-ésimas de la unidad.

7.27 Sea F un cuerpo y K un cuerpo de descomposición sobre F de un polinomio irreducible y separable $f \in F[X]$. Supóongase que el grupo de Galois $G(K/F)$ es abeliano. Demostrar que $K = F(x)$ para cualquier raíz $x \in K$ que sea raíz de f.

7.28 Sea F un cuerpo de característica prima p, K/F una extensión de cuerpos y $x \in K$ un elemento algebraico de la extensión. Demostrar que x es separable sobre F si y sólo si $F(x) = F(x^p)$.

7.29 Demostrar que la clase de las extensiones separables es una clase distinguida de extensiones.

7.30 Sea K/F una extensión algebraica. Comprobar que los elementos de K que son separables sobre F constituyen un subcuerpo K_s de K tal que K_s/F es una extensión separable. A K_s se llama *clausura separable* de F en K. Mostrar que para todo cuerpo intermedio E de la extensión K/F tal que E/F sea separable se tiene $E \subset K_s$.

7.31 Demostrar que para todo cuerpo F existe algún cuerpo Ω, que es extensión separable de F y está determinado de manera única salvo F-isomorfismos por la propiedad de que para todo cuerpo K tal que K/F sea separable exista siempre alguna F-inmersión de K en Ω.

7.32 Sea Ω una clausura algebraica de un cuerpo F y Ω_s la clausura separable de F en Ω. Demostrar que se da alguna de las dos alternativas siguientes: (1) $\Omega = \Omega_s$; (2) Ω/Ω_s es una extensión infinita.

7.33 Sea F un cuerpo y f un polinomio mónico irreducible de $F[X]$, de grado estrictamente mayor que 1, que tiene todas sus raíces coincidentes en una clausura algebraica de F. Demostrar que la característica de F es un primo $p > 0$ y que $f(X) = X^{p^n} - a$ para algún $a \in F$ y cierto entero $n \geq 0$.

7.34 Sea K/F una extensión de cuerpos y p un primo estrictamente positivo. Supóngase que F tiene característica p y que x es un elemento algebraico de la extensión. Demostrar la equivalencia de las siguientes afirmaciones:

1. $[F(x) : F]_s = 1$.
2. Existe algún entero $n \geq 0$ tal que $x^{p^n} \in F$.
3. El polinomio irreducible de x sobre F es del tipo $X^{p^n} - a$ para algún entero $n \geq 0$ y $a \in F$.

De un elemento algebraico x para el que se satisfacen las condiciones anteriores se dice que es un elemento *puramente inseparable* de la extensión. Una extensión algebraica se dice que es *puramente inseparable* si lo son cada uno de sus elementos.

7.35 Sea F un cuerpo de característica prima, K/F una extensión algebraica y K_s la clausura separable de F en K. Muéstrese que K/K_s es una extensión puramente inseparable.

7.36 Sea K/F una extensión de cuerpos, x e y elementos algebraicos de K. Suponer que x es separable e y puramente inseparable. Demostrar que $F(x, y) = F(x + y)$.

7.37 Sea F un cuerpo de característica no nula, K/F una extensión algebraica y S es un subconjunto de K tal que $K = F(S)$. Demostrar que la extensión K/F es puramente inseparable si y sólo si cada uno de los elementos de S es puramente inseparable sobre F.

7.38 Comprobar que la clase de las extensiones puramente inseparables es una clase distinguida de extensiones.

7.39 Sea K/F una extensión algebraica monógena y S un subconjunto no vacío de elementos puramente inseparables de la extensión tal que $K = F(S)$. Mostrar que existe algún $x \in S$ tal que $K = F(x)$.

7.40 Sea K/F una extensión de cuerpos y $D : K \longrightarrow K$ una F-derivación. Mostrar que el conjunto E de puntos en los que se anula D constituye un subcuerpo intermedio E de la extensión K/F y que en el caso en que K/F sea algebraica se tiene entonces que K/E es puramente inseparable.

7.41 Sea K/E una extensión normal y E/F una extensión puramente inseparable. Mostrar que K/F es normal.

7.42 Comprobar que para la clausura separable K_s de una extensión finita K/F se satisface la igualdad $[K_s : F] = [K : F]_s$.

7.43 Sea F un cuerpo de característica prima y K/F una extensión algebraica. Comprobar la existencia de un cuerpo intermedio K_i de la extensión K/F tal que K_i/F es puramente inseparable y contiene a cualquier otro cuerpo intermedio E que sea extensión puramente inseparable de F. Mostrar que la intersección de K_i con la clausura separable de F en K coincide con el cuerpo F. Comprobar que K/K_i es una extensión separable si y sólo si el cuerpo K coincide con el menor subcuerpo $K_s \vee K_i$ que contiene a K_s y K_i.

Nota. Del cuerpo K_i se dice que es la clausura inseparable de la extensión K/F.

1.8. Cuerpos finitos

8.1 ¿Puede un cuerpo finito de 27 elementos contener algún subcuerpo de cardinal 9?

8.2 Hallar el polinomio irreducible de una raíz 7-ésima primitiva de la unidad sobre $\mathbb{Z}/(2)$.

8.3 Mostrar que todo cuerpo F cuyo grupo multiplicativo es cíclico es necesariamente finito.

8.4 Sea F un cuerpo finito y p su característica. Usar el teorema de Cauchy para demostrar que el cardinal de F es una potencia de p.

8.5 Sea D un anillo, no necesariamente conmutativo, que no tiene divisores de cero no nulos, ni por la derecha, ni por la izquierda. Suponer que D contiene como subanillo a un cuerpo F y que D tiene dimensión finita como F-espacio vectorial por la izquierda. ¿Es D necesariamente de división?

8.6 Mostrar que todo subgrupo abeliano finito del grupo multiplicativo $D^\star$ de un anillo de división D es cíclico.

8.7 Sea F un cuerpo y $f \neq 0$ un polinomio de $F[X]$. Supóngase que el conjunto de las raíces de f en una clausura algebraica de F constituyen un subcuerpo que es extensión de F. Demostrar que F es finito de cardinal q y que f es divisible por un polinomio del tipo $X^{q^n} - X$.

8.8 Sea G un grupo cíclico finito de orden n. Comprobar que para todo entero positivo d que divide a n existe un único subgrupo de G de orden d. Demostrar que hay exactamente $\varphi(d)$ elementos de G cuyo orden es d, donde $\varphi : \mathbb{N}_> \longrightarrow \mathbb{N}_>$ es la *función φ de Euler* definida por $\varphi(1) = 1$ y siendo, para cada entero $n \geq 2$, $\varphi(n)$ el número de enteros positivos menores que n y primos relativos con él. Mostrar finalmente que

$$\sum_{d|n} \varphi(d) = n.$$

8.9 Sea G un grupo abeliano multiplicativo de orden n con la propiedad de que para todo entero positivo d que divide a n existen a lo más d elementos para los que se satisface la igualdad $x^d = 1$. Generalizar el ejercicio 8.8, demostrando además que G es entonces cíclico.

8.10 ¿Cómo puede usarse el ejercicio precedente para demostrar que si F es un cuerpo entonces todo subgrupo multiplicativo finito G de $F^\star$ es cíclico?

8.11 Sea n un entero estrictamente positivo dado. Demostrar que una clausura algebraica Ω de un cuerpo finito de q elementos F_q contiene un único subcuerpo F_{q^n} de q^n elementos y que $\Omega = \bigcup_{n\geq 1} F_{q^n}$.

8.12 Sea p un primo positivo. Demostrar que el cuerpo de descomposición de $X^p - 1$ sobre cualquier cuerpo F tiene un grado que divide a $p - 1$.

8.13 Sea F un cuerpo finito de q elementos. Demostrar que toda aplicación $\chi : F \longrightarrow F$ está representada por un único polinomio de grado estrictamente menor que q y que dicho polinomio es $f(X) = \sum_{a \in F} \chi(a)\big(1-(X-a)^{q-1}\big)$.

8.14 Sean p y n enteros positivos, con p primo y n dividiendo a $p-1$. Demostrar que la congruencia $x^n \equiv 1 (\text{mód}\, p)$ tiene exactamente n soluciones en $\mathbb{Z}/(p)$.

8.15 ¿Cómo puede generalizarse el ejercicio anterior en el caso de los cuerpos finitos?

8.16 Sea p un primo positivo que es congruente con 3 módulo 4. Demostrar que la congruencia $x^2 \equiv -1 (\text{mód}\, p)$ no tiene soluciones en $\mathbb{Z}/(p)$.

8.17 Demostrar que en un cuerpo finito F todo elemento es suma de dos cuadrados. [Indicación. Considerar separadamente los casos en que F tiene tiene o no característica 2].

8.18 Supóngase que el cuerpo F goza de la propiedad siguiente: si $f \in F[X]$ tiene dos raíces distintas en F entonces su derivada formal f' tiene también alguna raíz en F. Mostrar que F tiene característica cero y que el cuerpo $\mathbb{R}$ de los número reales tiene dicha propiedad.

8.19 Sea F un cuerpo con la misma propiedad que el cuerpo F del ejercicio anterior. Sean a, $b \in F$. Considerando el polinomio

$$f(X) = X^3 - 3(a^2 + b^2)X + 2a^3 - 6ab^2,$$

demostrar que cada suma de cuadrados de elementos de F es un cuadrado en F.

8.20 Para todo entero $r > 0$, se denota por S_r a la suma de las potencias r-ésimas de los elementos de un cuerpo finito dado de q elementos. Demostrar que

$$S_r = \begin{cases} -1 & \text{si } q-1 \mid r \\ 0 & \text{en otros casos} \end{cases}$$

[Indicación. En el caso que $q - 1 \not| r$, tómese un generador z del grupo multiplicativo del cuerpo finito dado].

8.21 Sea F un cuerpo finito de q elementos, p la característica de F y $n \geq 1$ un entero. Supóngase $f_1, \ldots, f_r \in F[X_1, \ldots, X_n]$ tales que $\sum \deg f_j < n$. Sea V el subconjunto de F^n que consta de todas las raíces comunes que tienen los polinomios $f_1, \ldots, f_r$ en F^n. Comprobar que el polinomio $h = \prod_{j=1}^{r}(1 - f_j^{q-1})$ es tal que para todo $x = (x_1, \ldots, x_n) \in F^n$ se tiene

$$h(x) = \begin{cases} 1 & \text{si } x \in V \\ 0 & \text{si } x \notin V \end{cases}$$

Para todo $f \in F[X_1, \ldots, X_n]$, denótese por $S(f)$ a la suma $\sum_{x \in F^n} f(x)$. Demostrar que $S(h)$ es un elemento del cuerpo primo de F que coincide con la clase de $|V|1$ módulo p. Expresando h como combinación lineal de monomios de grado estrictamente menor que $n(q-1)$ y usando el ejercicio precedente, demostrar que $S(h) = 0$ y que, en consecuencia, se obtiene el *teorema de Chevalley-Warning* que asegura que el número de puntos de V es divisible por p.

8.22 Sea F un cuerpo finito. Demostrar que toda forma cuadrática sobre F de a lo menos tres variables se anula en algún punto no nulo y, en particular, toda cónica del plano proyectivo $\mathcal{P}_2(F)$ es no vacía.

8.23 Sea F un cuerpo, Ω una clausura algebraica suya y $f(X)$ un polinomio mónico de $F[X]$ que no tiene raíces múltiples. Demostrar que si las raíces de $f(X)$ constituyen un subcuerpo de Ω entonces F tiene característica p y existe algún entero $r \geq 1$ tal que $f(X) = X^{p^r} - X$.

8.24 Mostrar que el producto de los elementos no nulos de un cuerpo finito coincide con -1.

8.25 (Wilson). Comprobar que si p es un número primo entonces $(p-1)! \equiv -1 (\text{mód}\, p)$.

8.26 ¿Es verdad el recíproco del teorema de Wilson enunciado en el ejercicio anterior.

8.27 Demostrar que si p es un primo positivo impar entonces

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} (\text{mód}\, p).$$

8.28 Sea n un entero positivo y F un cuerpo cuya característica es cero o un primo p distinto de 2 que no divide a $2n+1$. Sea K el cuerpo de descomposición del polinomio $X^{2n+1} - 1$ sobre el cuerpo F. Demostrar que K coincide con el cuerpo de descomposición de $X^{4n+2} - 1$ sobre F. [Indicación. Pruébese que si ε es una raíz $(2n+1)$-ésima primitiva de la unidad, entonces $\eta = -\varepsilon^n$ es una raíz $(4n+2)$-ésima primitiva de la unidad].

8.29 Comprobar que sobre cualquier cuerpo F el polinomio $X^5 - 1$ tiene cuerpo de descomposición de grado 1, 2 ó 4. Sea K/F una extensión de grado 5 para la que existe algún elemento $y \in K$ tal que $y^5 \in F$ y para el que se tiene $K = F(y)$.

1. Mostrar que el cuerpo de descomposición de $\text{irr}(y, X, F)$ es extensión de grado 5, 10 ó 20 del cuerpo F.
2. Demostrar que, si $f \in F[X]$ es un polinomio irreducible de grado 5 que tiene cuerpo de descomposición de grado 120 sobre F, entonces f es también irreducible sobre K.

8.30 Sea p un primo positivo y $s > 0$ un entero. Demostrar que el grupo aditivo de un cuerpo finito F de p^s elementos es isomorfo a una suma directa de s copias de $\mathbb{Z}/(p)$.

8.31 Demostrar que sobre un cuerpo finito polinomios irreducibles del mismo grado tienen el mismo cuerpo de descomposición.

8.32 Sean F_q y $F_{q'}$ cuerpos finitos de cardinales q y q'. Comprobar que $F_{q'}$ tiene un subcuerpo isomorfo a F_q si y sólo si existe un primo positivo p tal que $q = p^d$, $q' = p^n$ con $d|n$.

8.33 Sea F_{q_0} un cuerpo finito de q_0 elementos y Ω una clausura algebraica de F_{q_0}. Sea F_q (resp. $F_{q'}$) un subcuerpo finito de Ω de $q = {q_0}^{n_q}$ (resp. $q' = {q_0}^{n'_q}$) elementos. Demostrar que F_q es un subcuerpo de $F_{q'}$ si y sólo si $n_q \mid n_{q'}$.

8.34 Sea Ω una clausura algebraica de un cuerpo finito F_q. Sea S un subconjunto de número enteros estrictamente positivos con la propiedad de que cada vez que n y m sean elementos de S entonces el mínimo común múltiplo de estos enteros también pertenece a S. Mostrar que entonces

$$\bigcup_{m \in S} F_{q^m} \tag{1.4}$$

es un cuerpo intermedio de la extensión Ω/F_q. Demostrar que cualquier cuerpo intermedio de la extensión Ω/F_q se puede escribir como una unión de este tipo para un cierto suconjunto S convenientemente elegido gozando de la referida propiedad.

8.35 Sea Ω una clausura algebraica de un cuerpo finito F. Demostrar que todo cuerpo intermedio E de la extensión Ω/F que está estrictamente contenido en Ω es tal que $[\Omega : E] = \infty$.

8.36 Sea F un cuerpo de 81 elementos. Determinar el número de raíces distintas que los polinomios $X^{80} - 1$, $X^{81} - 1$ y $X^{88} - 1$ tienen en F.

8.37 Demostrar que $\Phi_n(0) = 1$ para todo entero $n > 1$.

8.38 Calcular $\Phi_{15}(X)$.

8.39 Sean n y p enteros estrictamente positivos, con p primo que no divide a n. Demostrar que si hay algún entero k tal que $p \mid \Phi_n(k)$ entonces $p \equiv 1 (\text{mód}\, n)$. Justificar la existencia de infinitos números primos congruentes con 1 módulo n.

8.40 Sea F un cuerpo finito de q elementos. Demostrar que los factores irreducibles de $X^q - X - 1$ en $F[X]$ tienen todos el mismo grado y que dicho grado coincide con la característica de F.

8.41 Suponer p y n enteros estrictamente positivos, siendo p primo. Demostrar que el polinomio $X^{p^n} - X + 1$ de $(\mathbb{Z}/(p))[X]$ es irreducible si y sólo si $n = 1$ ó $n = 2 = p$.

8.42 Sea F un cuerpo finito de q elementos, $n \geq 1$ un entero y $f(X)$ un polinomio irreducible de $F[X]$. Demostrar que el polinomio $f(X)$ divide a $X^{q^n} - X$ si y sólo si $\deg f$ divide a n.

8.43 Sea F un cuerpo finito de q elementos, K una extensión finita de F y $x \neq 0$ un elemento de K cuyo polinomio irreducible sobre F es $p(X)$. Mostrar que los elementos $x, x^q, \ldots, x^{q^{\deg p-1}}$ son todos distintos y que el conjunto que constituyen coincide con el de las raíces de $p(X)$ en K.

8.44 Sea K/F una extensión finita de un cuerpo finito de q elementos. Sea x un elemento de K que genera al grupo multiplicativo $K^\star$. Demostrar que las restantes raíces del polinomio irreducible de x sobre F generan también a $K^\star$ y que el grado m de éste divide a $\varphi(q^m - 1)$, donde φ es el indicador de Euler.

8.45 Demostrar que el polinomio $X^4 + 1$ es irreducible sobre $\mathbb{Z}$ pero no lo es sobre ningún cuerpo $\mathbb{Z}/(p)$. [Indicación. Comenzar comprobando que para todo primo $p > 2$ el número $p^2 - 1$ es divisible por 8. Utilizar el ejercicio 5.33 en el caso en que $p > 2$.]

8.46 Sea K/F una extensión finita de cuerpos y $K = F(x)$. Supóngase que F contiene alguna raíz primitiva n-ésima de la unidad y que $x^n \in F$. Demostrar que entonces $x^{[K:F]} \in F$.

8.47 Sean p y ℓ dos primos positivos distintos. Demostrar que el polinomio $f(X) = X^p - 1$ se descompone en factores lineales de $F_\ell[X]$ si y sólo si $\ell \equiv 1 (\text{mód}\, p)$.

8.48 Supóngase dado un entero $n \geq 1$. Pruébese que en un cuerpo finito de q elementos F se tiene

$$X^{q^n} - X = \prod_{d|n} \prod_{f_d} f_d(X) \tag{1.5}$$

donde el producto más interno se toma sobre todos los polinomios irreducibles de grado d cuyo coeficiente líder es 1. Por comparación de grados, demuéstrese que

$$q^n = \sum_{d|n} d\psi(d), \tag{1.6}$$

donde $\psi(d)$ es el cardinal del conjunto de los polinomios irreducibles de grado d de $F[X]$.

8.49 Determinar el número de polinomios mónicos irreducibles de grado 3 que hay en $F_{81}[X]$.

8.50 Sea K un cuerpo de característica distinta de 2, n un entero impar mayor o igual que 1 y $\varepsilon \in K$ una raíz n-ésima primitiva de la unidad. Probar que K contiene alguna raíz $2n$-ésima primitiva de la unidad.

8.51 Sea p un primo positivo que no divide al entero positivo n. Demostrar que el polinomio ciclotómico Φ_n es irreducible sobre F_p si y sólo si la clase de p módulo n tiene orden $\varphi(n)$ en el grupo multiplicativo de los elementos inversibles de $\mathbb{Z}/(n)$. [Indicación: Demostrar que, si Φ_n es irreducible y ε es una raíz n-ésima primitiva de la unidad en una clausura algebraica de F_p, entonces el menor entero positivo m para el que se tiene $\varepsilon^{p^m-1} = 1$ coincide con $\varphi(n)$, en el caso en que Φ_n sea irreducible sobre F_p.]

1.9. Teorema del elemento primitivo

9.1 Sea F un cuerpo infinito y K/F una extensión finita y propia del cuerpo F. Demostrar que el grupo $K^\star/F^\star$ es infinito.

9.2 Sea K/F una extensión separable de grado finito n. Demostrar que si $\sigma_1, \ldots, \sigma_n$ son las distintas inmersiones de K en una clausura algebraica de dicho cuerpo que inducen la identidad sobre F y si $x \in K$ es tal que $\sigma_i(x) \neq \sigma_j(x)$ para $i \neq j$, entonces x es un elemento primitivo de la extensión.

9.3 Sea K/F una extensión finita y separable de un cuerpo no perfecto F de característica p. Mostrar que existe algún elemento primitivo de la extensión que no es raíz p-ésima de ningún elemento de K. [Indicación. Sea φ el endomorfismo de Frobenious de K. Estudiar separadamente los casos en que $F \subset \varphi(K)$ y cuando esto no ocurra.

9.4 Sea F un cuerpo de característica p y K/F una extensión de cuerpos monógena y puramente inseparable tal que $[K : F] = p^n$. Mostrar que K/F tiene exactamente $n + 1$ cuerpos intermedios.

9.5 Sea K/F una extensión separable tal que $K \neq F$. Suponer que para todo $x \in K$, con $x \notin F$, el grado de la extensión $F(x)/F$ es un número primo. ¿Es K/F una extensión finita de grado primo?

9.6 Sea K/F una extensión de cuerpos tal que $K = F(x_1, \ldots, x_n)$ y con cada x_i con cuadrado en F. Suponer F de característica distinta de 2 y $[K : F] = 2^n$. Demostrar que $x = x_1 + \cdots + x_n$ es un elemento primitivo de la extensión.

9.7 Sea F un cuerpo de característica p y $F(X, Y)$ el correspondiente cuerpos de funciones racionales en dos indeterminadas. Mostrar que $F(X, Y)/F(X^p, Y^p)$ es una extensión finita de grado p^2 que contiene un número infinito de cuerpos intermedios.

9.8 Sea K/F una extensión algebraica de cuerpos tal que $K = F(x_1, \ldots, x_n, y)$, con cada x_i separable sobre F. Comprobar que la extensión K/F es monógena.

9.9 Sea F un cuerpo y n un entero estrictamente positivo. Demostrar que existe alguna extensión K/F de grado n si y sólo si hay algún polinomio irreducible de $F[X]$ con grado n.

9.10 Sea K/F una extensión algebraica de cuerpos tal que $K = F(x_1, \ldots, x_n, y)$, con cada x_i separable sobre $F(y)$. Comprobar que la extensión K/F es monógena.

9.11 Sea Ω/F una extensión separable. Supóngase que cualquier polinomio irreducible $h \in F[X]$ tiene alguna raíz en Ω. Demostrar que Ω es una clausura algebraica de F.

9.12 Sea K/F una extensión finita y separable de un cuerpo infinito. Supongamos que $x, y \in K$ son tales que $K = F(x, y)$. Sean $f(X)$ y $g(X)$ los polinomios irreducibles de x e y. Supongamos que

$$\begin{aligned} f(X) &= \prod_{i=1}^{n}(X - x_i), \qquad x_1 = x, \\ g(X) &= \prod_{j=1}^{m}(X - y_j), \qquad y_1 = y, \end{aligned}$$

son descomposiciones de f y g en una clausura algebraica de K. Tómese $c \in F$, distinto de cada uno de los elementos $(y_j - y)/(x - x_i)$, $(i \neq 1)$. Sea $z = y + cx$ y $h(X) = g(z - cX)$. Demostrar que el máximo común divisor de f y h en $F(z)[X]$ es $X - x$. Obtener de aquí el teorema del elemento primitivo.

9.13 Sea K/F una extensión separable y $\{K_n\}_{n=0}^{\infty}$ una sucesión estrictamente creciente de subcuerpos de K que son extensiones finitas de F y tales que $K_0 = F$ y $\bigcup_{n=0}^{\infty} K_n = K$. Demostrar que $[K : F]_s = 2^{\aleph_0}$.

Capítulo 2

Teoría de Galois

Modern algebra begins with Évariste Galois. With Galois the character of algebra changed radically. Before Galois, the efforts of algebraists were mainly directed towards the solution of algebraic equations. [$\cdots$] . If one wants to know wherther an equation can be solved by radicals, one has to analyse the structure of its Galois group. After Galois, the efforts of the leading algebraists were mainly directed torwards the investigation of the structure of rings, fields, algebras, and the like.

B. L. van der Waerden

2.1. Teorema fundamental de la teoría de Galois

1.1 Sea $K = \mathbb{Q}(x)$. Determinar los casos en que $K/\mathbb{Q}$ es una extensión de Galois, siendo x:

1. raíz del polinomio $X^2 + bX + c$, $(b, c \in \mathbb{Q})$.
2. raíz del polinomio $X^3 - d$, $(d \in \mathbb{Z}, d > 0)$.

1.2 Sea K/F una extensión de Galois finita. Mostrar que si n es el grado de la extensión entonces el número de cuerpos intermedios no puede ser mayor que 2^n.

1.3 La familia de cuerpos intermedios de una extensión de Galois de grado primo p, ¿tiene cardinal exactamente p?

1.4 Sean $\mathcal{L}$ y $\mathcal{L}'$ conjuntos parcialmente ordenados.

$$\varphi : \mathcal{L} \longrightarrow \mathcal{L}', \qquad \psi : \mathcal{L}' \longrightarrow \mathcal{L}$$

aplicaciones que constituyen una conexión de Galois. Sean a y b elementos cerrados de $\mathcal{L}$ que tienen un ínfimo $a \wedge b$ y tales que $\varphi(a)$ y $\varphi(b)$ tienen un supremo $\varphi(a) \vee \varphi(b)$. Supóngase que los elementos de $\mathcal{L}'$ que son cotas superiores simultáneas de $\varphi(a)$ y $\varphi(b)$ son todos ellos cerrados de la conexión de Galois. Demostrar que

$$\varphi(a \wedge b) = \varphi(a) \vee \varphi(b).$$

1.5 Sea K/F una extensión de Galois de grupo de Galois G. Demostrar que si H_1 y H_2 son subgrupos finitos de G entonces $K^{H_1 \cap H_2} = K^{H_1} \vee K^{H_2}$ y que, si la extensión K/F es además finita, se tiene entonces $G(K/(E_1 \cap E_2)) = G(K/E_1)G(K/E_2)$ para cualesquiera dos subcuerpos intermedios E_1 y E_2 de la extensión K/F.

1.6 Sea K/F una extensión de Galois, G su grupo de Galois y E_1 y E_2 cuerpos intermedios tales que $G(K/E_1) \cap G(K/E_2)$ es un subgrupo finito. Demostrar que $G(K/(E_1 \vee E_2)) = G(K/E_1) \cap G(K/E_2)$. Imponer condiciones sobre los subgrupos H_1 y H_2 del grupo de Galois G que permitan garantizar que $K^{H_1 H_2} = K^{H_1} \cap K^{H_2}$.

1.7 Sea K/F una extensión finita de cuerpos y G un grupo de F-automorfismos de K. Mostrar que G es finito y su orden $|G|$ divide a $[K : F]$. Comprobar que se da la igualdad $|G| = [K : F]$ si y sólo si K/F es de Galois y $G(K/F) = G$.

1.8 Sean p y s enteros positivos con p primo y K/F una extensión de Galois de grado p^s. Suponer que los cuerpos intermedios de la extensión K/F constituyen una cadena

$$F = F_0 \subset F_1 \subset \cdots \subset F_s = K,$$

en la que cada uno de los subcuerpos F_i es extensión de F de grado p^i. Demostrar que el grupo de Galois de la extensión K/F es cíclico.

1.9 Sea K/F una extensión de Galois y G su grupo de Galois. Mostrar que, si H es un grupo para el que existe algún epimorfismo $\theta : G \longrightarrow H$, existe entonces algún cuerpo intermedio E de la extensión K/F que es extensión normal de F tal que $G(E/F) \cong H$

1.10 Sea K/F una extensión de Galois finita de grado $n = rs$, siendo r y s enteros positivos primos relativos. Suponer que K/F tiene cuerpos intermedios E_1 y E_2 que son extensiones de F tales que $[E_1 : F] = r$, $[E_2 : F] = s$.

1. Mostrar que $K = E_1 \vee E_2$ y $E_1 \cap E_2 = F$.
2. Demostrar que si E_1/F y E_2/F son extensiones normales entonces el grupo de Galois G de la extensión K/F es isomorfo a un producto directo de dos subgrupos de G de órdenes respectivos r y s. Mostrar que si $G(K/E_1)$ y $G(K/E_2)$ son conmutativos (resp. cíclicos), entonces el grupo de Galois de la extensión K/F es conmutativo (resp, cíclico)

1.11 Sea $F(X)$ el cuerpo de funciones racionales en una indeterminada con coeficientes en el cuerpo de característica cero F. Mostrar que $F(X)/F(X^2)$ y $F(X)/F(X^2 - X)$ son extensiones cuadráticas y que se tiene además $F(X^2) \cap F(X^2 - X) = F$.

1.12 Sea $f \in \mathbb{R}(X, Y)$ una función racional para la que se tiene $f(-X, Y) = -f(X, Y)$. Demostrar que el cambio de variable $x = \cos t$ reduce la integral $\int f(\operatorname{sen} x, \cos x)\mathrm{d}x$ a una integral de función racional; esto es, existe alguna función racional $g \in \mathbb{R}(X)$ tal que

$$\int f(\operatorname{sen} x, \cos x)\mathrm{d}x = \int g(t)\mathrm{d}t.$$

1.13 Sea K/F una extensión normal y G su grupo de Galois. Si K_i es el cuerpo intermedio de K/F caracterizado como en el ejercicio 1.7.43, demostrar que entonces $K_i = K^G$.

1.14 Sea Ω/F una extensión algebraica de cuerpos. Supóngase que todo polinomio irreducible $h \in F[X]$ tiene alguna raíz en Ω. Demostrar que Ω es una clausura algebraica de F.

1.15 Demostrar que todos los cuerpos intermedios de la extensión $\mathbb{Q}(\sqrt{2}, \mathrm{i})$ son extensiones normales de $\mathbb{Q}$. Dar para cada uno de ellos un polinomio del que sea cuerpo de descomposición sobre $\mathbb{Q}$.

1.16 Dar el cuerpo de descomposición sobre $\mathbb{Q}$ de cada uno de los polinomios siguientes:

$$(X^3 - 1)(X^2 - 3)(X^4 - 1), \quad (X^2 - 3)(X^2 + 1), \quad (X^3 - 2)(X^2 + 3).$$

Dar en cada uno de los casos el grado de las extensiones correspondientes y establecer explícitamente las biyecciones subgrupo-subcuerpo del teorema fundamental de la teoría de Galois.

1.17 Sea $K = \mathbb{Q}(\sqrt{3}, \sqrt{5}, x)$ donde $x^2 = (1 - \sqrt{3})(2 + \sqrt{5})$.

1. Mostrar que x es un elemento primitivo de la extensión $K/\mathbb{Q}$.
2. Determinar el grupo de los $\mathbb{Q}$-automorfismos de K.
3. Demostrar que $K/\mathbb{Q}$ no es una extensión de Galois.

1.18 Suponer que K/F es una extensión de Galois cuyo grupo de Galois G puede darse por generadores y relaciones por

$$G = \langle \xi, \eta, \rho : \ \xi^2 = \eta^2 = \rho^2 = \mathrm{Id},\ \eta\rho = \xi\rho\eta,\ \xi\eta = \eta\xi,\ \xi\rho = \rho\xi \rangle.$$

Mostrar que el grupo G tiene 8 elementos y es isomorfo al grupo diédrico D_4. Dar los enteros n para los que existe algún cuerpo intermedio de grado n sobre F y determinar el número de ellos que son extensión de grado 4 del cuerpo F.

1.19 Sea K/F una extensión de Galois finita, E_1 y E_2 cuerpos intermedios de la extensión tales que el menor subcuerpo $E_1 \vee E_2$ que contiene a E_1 y E_2 coincide con K. Suponer que E_1/F es una extensión normal. Demostrar que la igualdad $F = E_1 \cap E_2$ se da si y sólo si $[K : F] = [K : E_1][K : E_2]$.

1.20 Dar el grupo de Galois del cuerpo de descomposición del polinomio $X^4 - 5$ sobre cada uno de los cuerpos siguientes:

$$\mathbb{Q}, \quad \mathbb{Q}(\sqrt{5}), \quad \mathbb{Q}(\sqrt{-5}), \quad \mathbb{Q}(\mathrm{i}).$$

1.21 Sea z un número algebraico y F un subcuerpo de $\mathbb{C}$. Mostrar que $[F(z) : F] \leq [\mathbb{Q}(z) : \mathbb{Q}]$ y que, en el caso en que $\mathbb{Q}(z)/\mathbb{Q}$ sea normal, también lo es la extensión $F(z)/F$, teniéndose entonces que $[F(z) : F]$ divide a $[\mathbb{Q}(z) : \mathbb{Q}]$.

1.22 Sea K un subcuerpo de $\mathbb{C}$ y $E = K \cap \mathbb{R}$. Demostrar que si $K/\mathbb{Q}$ es una extensión normal entonces $[K : E] \leq 2$. Mostrar que dicha afirmación no se satisface necesariamente en el caso de que $K/\mathbb{Q}$ sea extensión finita no normal.

1.23 Sea K un subcuerpo de $\mathbb{C}$, que es extensión normal de $\mathbb{Q}$, y $E = K \cap \mathbb{R}$. Sea τ el automorfismo de K obtenido por restricción de la conjugación compleja $-$. Demostrar que $E/\mathbb{Q}$ es extensión de Galois si y sólo si τ conmuta con todo $\sigma \in G(K/\mathbb{Q})$.

1.24 Sea F un cuerpo de característica cero y K/F una extensión de grado 3 que no es normal. Sea L una clausura normal de dicha extensión. Demostrar que $[L : F] = 6$ y que L/F es una extensión de Galois. Comprobar la existencia de un único cuerpo intermedio E de la extensión L/F tal que $[E : F] = 2$.

1.25 Sea F un cuerpo finito de q elementos y K/F una extensión finita. Comprobar que la aplicación $\psi : K \longrightarrow K$ dada por $\psi : x \mapsto x^q$ es un F-automorfismo de K y que todo elemento del grupo de Galois $G(K/F)$ es una potencia de ψ. Mostrar, en particular, que los automorfismos de un cuerpo finito son potencia de su automorfismo de Frobenius.

1.26 Sea f el polinomio con coeficientes en $\mathbb{Z}/(2)$ dado por la igualdad siguiente $f(X) = X^6 + X + 1$.

1. Demostrar que $f(X)$ es un polinomio irreducible de $[\mathbb{Z}/(2)][X]$.
2. Sea x una raíz de f en una clausura algebraica de $\mathbb{Z}/(2)$ y $K = (\mathbb{Z}/(2))(x)$. ¿ Es K un cuerpo de descomposición de $f(X)$?
3. Determinar el grado del cuerpo de descomposición de f sobre $\mathbb{Z}/(2)$ y dar el retículo de cuerpos intermedios de dicha extensión.

1.27 Sea Ω una clausura algebraica de un cuerpo finito F. Demostrar que la identidad es el único automorfismo de Ω que tiene orden finito.

1.28 Sea K/F una extensión de Galois finita, p un primo positivo y $s \geq 1$ un entero tal que $p^s|[K : F]$ pero $p^{s+1} \not| [K : F]$. Demostrar que existe una cadena de subcuerpos

$$F = F_0 \subset F_1 \subset \cdots \subset F_{s+1} = K$$

tal que $p \not| [F_1 : F]$ y de manera que para cada $i \in \{1, \ldots, s\}$ la extensión F_{i+1}/F_i es normal de grado p.

1.29 Sea $\mathcal{A}$ un subconjunto del plano euclídeo con a lo menos dos puntos distintos, S el conjunto de las coordenadas de los puntos de $\mathcal{A}$ respecto a un sistema de referencia apropiado para $\mathcal{A}$ y $F = \mathbb{Q}(S)$. Sea $P = (x, y)$ un punto dado del plano cuyas coordenadas están dadas en dicho sistema de referencia. Suponer que x e y pertenecen a un subcuerpo K de $\mathbb{R}$ que es extensión normal de grado potencia de 2 del cuerpo F. Demostrar que P es construible con regla y compás a partir de $\mathcal{A}$. Mostrar que los factores de composición de cada una de las sucesiones de composición del grupo de Galois G de la extensión K/F son todos ellos isomorfos a $\mathbb{Z}/(2)$ (ver el apéndice C para las definiciones). ¿Puede alternativamente utilizarse esto para demostrar la constructibilidad de P?

1.30 Sean $\mathcal{A}$, S, F y $P = (x, y)$ como en el ejercicio anterior. Suponer que x e y pertenecen a un subcuerpo K de $\mathbb{R}$ que es extensión de Galois finita del cuerpo F tal que $[K : F] = 2^s 3^t$, $(s, t \geq 0)$. Si el grupo de Galois G de la extensión K/F tiene algún subgrupo de Sylow normal en G, demostrar que P es entonces construible con regla, compás y trisector de ángulos a partir del conjunto de puntos $\mathcal{A}$

1.31 Sea K/F una extensión de Galois finita de grado n y grupo de Galois G para la que se satisface la siguiente propiedad: para todo primo positivo p que divide a $|G|$, existe algún p-subgrupo de Sylow que es subgrupo normal de G, y el cuerpo intermedio E del correspondiente subgrupo de Sylow es tal que para cada potencia positiva de p que divida a $[E : F]$ existe un único subcuerpo de E/F que tiene por grado dicha potencia de p. Demostrar que G es entonces un grupo cíclico.

1.32 Sea $K = \mathbb{C}(t)$ donde t es trascendente sobre $\mathbb{C}$ y ω un número complejo tal que $\omega^3 = 1$, $\omega \neq 1$. Sean σ y τ los automorfismos de K que dejan fijo cada elemento de $\mathbb{C}$ y para los que se satisfacen las igualdades $\sigma(t) = \omega t$ y $\tau(t) = t^{-1}$. Demostrar que

$$\sigma^3 = \mathrm{Id} = \tau^2, \qquad \tau \circ \sigma = \sigma^{-1} \circ \tau$$

Comprobar que el grupo G de los automorfismos generado por σ y τ tiene orden 6. Demostrar que el cuerpo fijo de G es $\mathbb{C}(u)$, donde $u = t^3 + t^{-3}$.

1.33 Sea K/F una extensión de Galois de grado 4 cuyo grupo de Galois es isomorfo a $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Supóngase F de característica distinta de 2. Demostrar que $K = F(x, y)$, siendo x e y elementos con cuadrados en el cuerpo F.

1.34 Sea K/F una extensión de cuerpos, E_1 y E_2 subcuerpos estrictamente comprendidos entre K y F y tales que K coincide con el menor subcuerpo $E_1 \vee E_2$ que contiene tanto a E_1 como a E_2. Demostrar que si E_1/F es una extensión de Galois entonces también lo es K/E_2, pudiéndose identificar $G(K/E_2)$ con un subgrupo de $G(E_1/F)$. Mostrar que si además K/F es de Galois finita y $E_1 \cap E_2 = F$ entonces $G(K/E_2) \cong G(E_1/F)$.

1.35 Sea K/F una extensión de cuerpos, E_1 y E_2 subcuerpos de K tales que $K = E_1 \vee E_2$. Supóngase que K/E_1 y K/E_2 son de Galois. Demostrar que K/F es también de Galois y que si la extensión K/F es finita y $F = E_1 \cap E_2$ entonces el grupo de Galois G de la extensión K/F es isomorfo a $G(E_1/F) \times G(E_2/F)$.

1.36 Sea F un cuerpo finito y K el cuerpo de descomposición sobre F de un polinomio irreducible de grado 3. Demostrar que el grupo de Galois de la extensión K/F es isomorfo al grupo alternado A_3.

1.37 Sea F un cuerpo que contiene todas las raíces n-ésimas de la unidad y $X^n - a,\ X^n - b$ dos polinomios irreducibles de $F[X]$. Demostrar que estos dos polinomios tienen cuerpos de descomposición F-isomorfos si existe algún entero positivo r primo relativo con n tal que $b = a^r c^n$ para algún $c \in F$.

1.38 Sea F un cuerpo y $F(X)$ el cuerpo de funciones racionales en la indeterminada X. Considérese el conjunto de los automorfismos de $F(X)$ dados por

$$\begin{array}{lll} f(X) \mapsto f(X), & f(X) \mapsto f(1-X), & f(X) \mapsto f\left(\frac{1}{X}\right) \\ f(X) \mapsto f\left(1-\frac{1}{X}\right), & f(X) \mapsto f\left(\frac{1}{1-X}\right), & f(X) \mapsto f\left(\frac{X}{X-1}\right). \end{array}$$

Demostrar que estos automorfismos constituyen un subgrupo G del grupo de todos los automorfismos de $F(X)$ que dejan fijo a cada uno de los elementos de F y que el cuerpo fijo de G coincide con $F(T)$, siendo T el elemento de $F(X)$ definido por la igualdad siguiente:

$$T(X) = \frac{(X^2 - X + 1)^3}{X^2(X-1)^2}.$$

1.39 Sea F un cuerpo y $K = F(X)$ el cuerpo de funciones racionales sobre F. Demostrar que las aplicaciones dadas por

$$f(X) \mapsto f(X), \quad f(X) \mapsto f\left(\frac{1}{1-X}\right), \quad f(X) \mapsto f\left(1-\frac{1}{X}\right)$$

constituyen un subgrupo del grupo de automorfismos del ejercicio anterior. Sea E su cuerpo fijo. Determinar $[K : E]$ y dar un elemento que genere K sobre E y otro que genere E sobre F.

1.40 Sea F un cuerpo de característica prima p y $K = F(t)$ un cuerpo extensión del cuerpo dado con t trascendente sobre F. Sean σ y τ los F-automorfismos de K que actúan sobre t del modo siguiente

$$\sigma : t \mapsto -t \qquad \tau : t \mapsto 1 - t.$$

Demostrar que el subgrupo de los F-automorfismos generado por σ y τ es finito. Determinar el cuerpo fijo del mismo.

1.41 Sea K/F una extensión normal. Mostrar la existencia de un cuerpo intermedio I de la extensión K/F tal que I/F es una extensión puramente inseparable y K/I es extensión separable. Comprobar que, si K_s es la clausura separable de la extensión K/F, entonces $K_s \cap I = F$.

1.42 Sea K/F una extensión normal finita, E_1 y E_2 cuerpos intermedios de la extensión tales que K/E_1 y K/E_2 son extensiones separables. Demostrar que la extesnsión $K/(E_1 \cap E_2)$ es también separable

1.43 Sea $F(t)/F$ una extensión de cuerpos en la que t es trascendente sobre F. Sea G el grupo de Galois de dicha extensión. Demostrar que existe un antihomomorfismo de grupos

$$\varphi : \mathrm{GL}_2(F) \longrightarrow G$$

cuyo dominio $\mathrm{GL}_2(F)$ es el grupo de todas las matrices no singulares 2×2 con coeficientes en F y que está definido del siguiente modo

$$\varphi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{Bmatrix} a & b \\ c & d \end{Bmatrix}.$$

Aquí se denota por

$$\begin{Bmatrix} a & b \\ c & d \end{Bmatrix}$$

al F-automorfismo de $F(t)$ que transforma el elemento t en $\frac{at+b}{ct+d}$. Demostrar que

$$\ker \varphi = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : \quad 0 \neq a \in F \right\} \tag{2.1}$$

y que G es isomorfo al grupo lineal proyectivo general $\mathrm{PGL}_2(F)$.

1.44 Sea F un cuerpo finito con q elementos y $K = F(X)$. Sea G el grupo de los F-automorfismos de K. Demostrar:

1. El orden de G es $q^3 - q$.
2. Mostrar que si
$$U = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}$$
entonces $U \in K^G$. Observando que
$$U = \frac{\left((X^{q(q-1)} \cdots + X^{q-1} + 1)\right)^{q+1}}{(X^q - X)^{q^2-q}}, \tag{2.2}$$
demostrar que $F(U)$ es el cuerpo fijo de G.
3. Sea H_1 el subgrupo de los F-automorfismos de K tales que $X \mapsto aX+b$ con $a \neq 0$ y H_2 el subgrupo de H_1 formado por los F-automorfismos que tansforman X en $X + b$. Comprobar que los cuerpos fijos de H_1 y H_2 son $F(T)$ y $F(Z)$, donde $T = (X^q - X)^{q-1}$ y $Z = X^q - X$.

1.45 Sea F un cuerpo y $\bar{F}$ una clausura algebraica de F. Supóngase que τ es un automorfismo de $\bar{F}$ que deja fijo a cada elemento de F. Sea E el cuerpo fijo del subgrupo generado por τ. Demostrar que cualquier extensión finita de E es cíclica.

1.46 Un cuerpo F se dice cuasi-finito si es perfecto y para cada entero $n > 0$ existe una única extensión de F de grado n contenida en una clausura algebraica $\bar{F}$ de F. Demostrar que si F es un cuerpo cuasi-finito cualquier extensión finita K/F es de Galois y cíclica.

2.2. Teorema fundamental del álgebra

2.1 ¿Cuáles son las extensiones algebraicas del cuerpo $\mathbb{R}$ de los números reales?

2.2 Mostrar que los polinomios irreducibles de $\mathbb{R}[X]$ son a lo sumo de grado 2.

2.3 Sea F un cuerpo perfecto de característica distinta de 2 y Ω un cuerpo algebraicamente cerrado que es extensión de F. Sea S_0 el conjunto de los elementos de Ω que son raíz de algún polinomio irreducible de $F[X]$ de grado impar y L_0 el subcuerpo de Ω dado por la igualdad $L_0 = F(S_0)$. Para cada entero $i > 0$ defínase el subcuerpo $L_i = L_{i-1}(S_i)$ siendo S_i el subconjunto de los elementos de Ω que son raíces cuadradas de elementos de L_{i-1}. Demostrar que

$$L = \bigcup_{i=0}^{\infty} L_i$$

es un subcuerpo de Ω que es clausura algebraica de F.

2.4 (*Lema de d'Alembert*). Sea $f \in \mathbb{C}[X]$ un polinomio no constante. Usar el ejercicio I.7.11 para demostrar que si z_0 es un número complejo tal que $f(z_0) \neq 0$ existe entonces en todo entorno de z_0 algún punto z_1 tal que $|f(z_1)| < |f(z_0)|$.

2.5 Sea $f(X) = \sum_{i=0}^{m} a_i X^i$ un polinomio no constante de grado m con coeficientes en $\mathbb{C}$ y $M > 0$ un número real. Utilizando el ejercicio precedente y observando que para todo $z \in \mathbb{C}$ tal que

$$|z| \geq \text{máx}\left\{1,\ \frac{M + \sum_{i=0}^{m-1} |a_i|}{|a_m|}\right\} \tag{2.3}$$

se tiene $|f(z)| \geq M$, mostrar que f tiene alguna raíz en $\mathbb{C}$ y que consecuentemente $\mathbb{C}$ es algebraicamente cerrado.

2.3. Extensioes ciclotómicas

3.1 Sea $K/\mathbb{Q}$ una extensión finita de grado impar. Mostrar que si ε es una raíz n-ésima primitiva de la unidad contenida en K entonces $n = 1$ ó 2 y que, en consecuencia, 1 y -1 son las únicas raíces de la unidad contenidas en K (ver el ejercicio I.2.37).

3.2 Sea $p > 1$ un número primo y a un racional tal que el polinomio $X^p - a$ es irreducible sobre $\mathbb{Q}$. Demostrar que el grupo de Galois de $X^p - a$ sobre $\mathbb{Q}$ es isomorfo al grupo de las afinidades de la recta vectorial $\mathbb{Z}/(p)$.

3.3 Sea $p > 0$ un primo impar y $\varepsilon \in \mathbb{C}$ una raíz p-ésima primitiva de la unidad. Sea $p - 1 = q_1^{r_1} \cdots q_s^{r_s}$ la factorización de $p - 1$ en producto de potencias de primos. Demostrar que los cuerpos intermedios de la extensión $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ constituyen un conjunto de $(r_1 + 1) \cdots (r_s + 1)$ elementos.

3.4 Sean n y m enteros positivos, x un número real tal que $x^3 = m$ y $K = \mathbb{Q}(\varepsilon)$, siendo ε una raíz n-ésima primitiva de la unidad. Demostrar la equivalencia de las dos afirmaciones siguientes:

1. $x \in \mathbb{Z}$.
2. $x \in K$.

3.5 Sea ε una raíz primitiva n-ésima de la unidad. Determinar los valores de n para los que $\mathbb{Q}(\varepsilon)$ es una extensión cuadrática de $\mathbb{Q}$.

3.6 Sea K una extensión finita del cuerpo $\mathbb{Q}$. Demostrar que K contiene únicamente un número finito de raíces de la unidad.

3.7 Sea F un cuerpo de característica distinta de 2 y n un entero impar ≥ 1. Supóngase que ε es una raíz n-ésima primitiva de la unidad y η es una raíz $2n$-ésima primitiva de la unidad, ambas en en una clausura algebraica Ω de F. Demostrar que $F(\varepsilon) = F(\eta)$.

3.8 Sea p un primo positivo distinto de 2, ε una raíz p-ésima primitiva de la unidad y $K = \mathbb{Q}(\varepsilon)$. Demostrar que en la extensión $K/\mathbb{Q}$ existe un único cuerpo intermedio que es extensión cuadrática de $\mathbb{Q}$ y que dicho cuerpo es real o no, según que p sea de la forma $4n + 1$ ó $4n + 3$.

3.9 Sea ε (resp. η) un número complejo que es raíz n-éima (resp. m-ésima) primitiva de la unidad. Supóngase que n y m son primos relativos. Demostrar que $\mathbb{Q}(\varepsilon) \cap \mathbb{Q}(\eta) = \mathbb{Q}$ y que el menor subcuerpo $\mathbb{Q}(\varepsilon) \vee \mathbb{Q}(\eta)$ que contiene a $\mathbb{Q}(\varepsilon)$ y $\mathbb{Q}(\eta)$ coincide con $\mathbb{Q}(\varepsilon\eta)$

3.10 Sea n un entero mayor o igual que 2 y $K/\mathbb{Q}$ una extensión de grado n. Demostrar que si K contiene una raíz n-ésima primitiva de la unidad entonces n se factoriza en factores primos en la forma $n = 2^{r_1}3^{r_2}$, con $r_1 \geq 1$ y $r_2 \geq 0$.

3.11 Utilizar el ejercicio I.8.39 para demostrar que para todo grupo cíclico finito C existe siempre algún primo positivo p, una raíz p-ésima primitiva de la unidad $\varepsilon \in \mathbb{C}$ y un cuerpo intermedio E de la extensión $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ tal que $G(E/\mathbb{Q}) \cong C$.

3.12 Generalizar la afirmación del ejercicio anterior demostrando que para todo grupo abeliano finito G existe algún subcuerpo E de una extensión ciclotómica $\mathbb{Q}(\varepsilon)$ de $\mathbb{Q}$ tal que $G(E/\mathbb{Q}) \cong G$.

3.13 Sea $\varepsilon \in \mathbb{C}$ una raíz primitiva n-ésima de la unidad. Suponer que m es un entero positivo primo relativo con n. Demostrar que el polinomio $\Phi_m(X)$ es irreducible sobre $\mathbb{Q}(\varepsilon)$.

3.14 Sean p y k enteros estrictamente positivos con p primo y F un cuerpo de característica distinta de p. Mostrar que las raíces primitivas de la unidad de orden p^k de una clausura algebraica $\bar{F}$ de F coinciden con las raíces del polinomio $X^{p^k} - 1$ en $\bar{F}$ que no son raíces p^{k-1}-ésimas de la unidad. Demostrar que el polinomio

$$X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1$$

es irreducible sobre $\mathbb{Q}$.

3.15 Sea $\varepsilon \in \mathbb{C}$ una raíz primitiva n-ésima de la unidad, $m \geq 1$ un entero positivo y $y \in \mathbb{Q}(\varepsilon)$ tal que $y^m \in \mathbb{Q}$. Demostrar que $(\mathbb{Q}(\varepsilon) \cap \mathbb{R})/\mathbb{Q}$ es una extensión normal y que si $y \in \mathbb{Q}(\varepsilon) \cap \mathbb{R}$ entonces $y^2 \in \mathbb{Q}$.

3.16 Sea ε una raíz primitiva n-ésima de la unidad. Mostrar que el polígono regular de n lados es construible con regla y compás si y sólo si $[\mathbb{Q}(\varepsilon) : \mathbb{Q}]$ es potencia de 2.

3.17 (Gauss/Wantzel). Mostrar que el polígono regular de n lados es construible con regla y compás si y sólo si n tiene una factorización en producto de primos del tipo $n = 2^r p_1 \cdots p_s$, siendo $r \geq 0$ y siendo los p_i primos de Fermat distintos dos a a dos.

2.4. Extensiones cíclicas

4.1 Sean F, K y $X^n - a$ como en el lema 2.4.1. Suponer además n primo y a no siendo potencia n-ésima de ningún elemento de F. ¿Es $X^n - a$ polinomio irreducible de $F[X]$?

4.2 Usar los ejercicios I.5.30 y I.7.10 para generalizar el ejercicio anterior, demostrando que si p es primo y $X^p - a$ es un polinomio con coeficientes en el cuerpo F, que no tiene raíces en F, entonces $X^p - a$ es irreducible sobre F.

4.3 Sea $\omega \neq 1$ un número complejo que es raíz cúbica de la unidad, $F = \mathbb{Q}(\omega)$ y K un subcuerpo de $\mathbb{C}$ tal que K/F es extensión de Galois cuyo grupo de Galois es isomorfo a $\mathbb{Z}/6\mathbb{Z}$. Demostrar que existen entonces x, $y \in K$ con $x^2 \in F$, $y^3 \in F(x)$ tales que $K = F(x, y)$.

4.4 Sea K/F una extensión de cuerpos, p un primo positivo y x y β elementos de K tales que $x^p = \beta$. Suponer que F contiene una raíz p-ésima de la unidad $\varepsilon \neq 1$. Demostrar que si σ es un F-automorfsimo de K de orden finito no divisible por p y que deja fijo a β, entonces deja también fijo a x.

4.5 Sea K cuerpo de descomposición sobre el cuerpo F de un polinomio f de grado $n \geq 5$. Sea p un primo positivo y z y β elementos de K tales que $z^p = \beta$. Supóngase que F contiene alguna raíz p-ésima de la unidad $\varepsilon \neq 1$ y que f tiene al menos 5 raíces distintas $x_1, \ldots, x_5$. Mostrar que si el grupo de Galois G de la extensión K/F contiene a los F-automorfismos σ y τ que actúan sobre las raíces $x_1, \ldots, x_n$ de f del modo siguiente

$$\sigma : x_1 \mapsto x_2 \mapsto x_3 \mapsto x_1, \quad \sigma(x_i) = x_i \text{ si } \ i > 3,$$

y

$$\tau : x_3 \mapsto x_4 \mapsto x_5 \mapsto x_3, \quad \sigma(x_i) = x_i \text{ si } \ i \neq 3, 4, , 5,$$

y que si ambos fijan β, entonces dejan fijo también a z.

4.6 Sean n p enteros positivos con $n \geq 5$ y $p \geq 3$ primo, y F un cuerpo que contiene alguna raíz p-ésima de la unidad distinta de 1. Mostrar que si K es cuerpo de descomposición sobre F de un polinomio irreducible y separable $f \in F[X]$ y si el grupo de Galois $G(K/F)$ es isomorfo a S_n entonces K no contiene elementos con potencias p-ésimas en F, salvo aquéllos que están en F.

4.7 Sea F un cuerpo que contiene alguna raíz primitiva n-ésima de la unidad y $X^n - a$, $X^n - b$ dos polinomios irreducibles de $F[X]$. Comprobar que si los cuerpos de descomposición coinciden y F tiene característica cero o un primo que no divide a n, existe entonces algún entero positivo $r < n$, primo relativo con n, tal que $b = a^r c^n$ para algún $c \in F$.

4.8 Sea n un entero estrictamente positivo, p y q primos positivos y $\sqrt[n]{p}$ (resp. $\sqrt[n]{q}$) la raíz n-ésima positiva de p (resp. q). Demostrar que $\mathbb{Q}(\sqrt[n]{p}) = \mathbb{Q}(\sqrt[n]{q})$ si y sólo si $p = q$.

4.9 Sea n un entero estrictamente mayor que 1, P el conjunto de todos los primos positivos y $S = \{x \in \mathbb{R} : x^n \in P\}$. Demostrar que $\mathbb{Q}(S)/\mathbb{Q}$ tiene grado infinito.

4.10 Sea p un primo positivo y F un cuerpo de característica distinta de p, con cuerpo primo P y conteniendo una raíz p-ésima primitiva de la unidad ε. Sea K/F una extensión de cuerpos tal que $K = F(x)$, donde $x \in K$ es tal que $x \notin F$ pero $x^p \in F$. Mostrar que si $y \in K$ no pertenece a F entonces $\text{irr}(y, X, F)$ tiene p raíces distintas $y_0, \ldots, y_{p-1}$ en el cuerpo K y

si $y = y_0 = \sum_{j=0}^{p-1} b_j x^j$, $(b_j \in F)$, entonces, tras una reordenación si fuera necesario, las restantes raíces $y_1, \ldots, y_{p-1}$ de $\mathrm{irr}(y, X, F)$ son

$$y_1 = \sum_{j=0}^{p-1} b_j \varepsilon^j x^j \tag{2.4}$$

$$y_2 = \sum_{j=0}^{p-1} b_j \varepsilon^{2j} x^j \tag{2.5}$$

$$\vdots = \quad \vdots \tag{2.6}$$

$$y_{p-1} = \sum_{j=0}^{p-1} b_j \varepsilon^{(p-1)j} x^j. \tag{2.7}$$

Comprobar que para cada $k \in \{0, \ldots, p-1\}$ se tiene

$$\sum_{i=0}^{p-1} \varepsilon^{-ik} y_i = p b_k x^k$$

y que, en consecuencia, existe algún k_0 tal que $x^{k_0} \in P(\varepsilon, b_{k_0}, y_0, \ldots, y_{p-1})$. Mostrar que existe algún elemento no nulo z en alguna de las rectas vectoriales Fx, $Fx^2, \ldots, Fx^{p-1}$ tal que $K = F(z)$, $z^p \in F$ y pudiéndose escribir

$$y = c_0 + z + \sum_{j=2}^{p-1} c_j z^j,$$

siendo los c_j elementos de F determinados de manera única. Mostrar que tanto x como los c_j están en el subcuerpo $P(\varepsilon, y_0, \ldots, y_{p-1})$.

4.11 Suponer n, F, x y K como en el lema 2.4.1. Demostrar que $[K : F]$ coincide con el menor entero positivo d para el que se tiene $x^d \in F$.

4.12 Dado un primo positivo p, demostrar que el cuerpo de descomposición K de $X^n - p$ sobre $\mathbb{Q}$ es tal que $[K : \mathbb{Q}] = n\varphi(n)$ ó $n\varphi(n)/2$. (Indicación. Sea $x \in \mathbb{R}$ tal que $x^n = p$. Usar los ejercicios 3.15 y 4.11 para demostrar que si $d = [K : \mathbb{Q}(\varepsilon)]$ entonces $d|n$ y $x^{2d} \in \mathbb{Q}$).

4.13 Sea F un cuerpo de característica p, a un elemento de F y f el polinomio de $F[X]$ definido por la igualdad

$$f(X) = X^p - X - a.$$

Mostrar que si K es el cuerpo de descomposición de f sobre F entonces K/F es una extensión cíclica.

4.14 Sea F un cuerpo de característica p, A el subgrupo del grupo aditivo F definido como en el ejercicio I.5.28, Ω una clausura algebraica de F y f y g los siguientes polinomios de $F[X]$:

$$f(X) = X^p - X - a, \qquad g(X) = X^p - X - b, \qquad (a, b \in F).$$

Sean K y E subcuerpos de Ω, el primero de los cuales es cuerpo de descomposición de f sobre F, mientras el segundo lo es del polinomio g. Suponer f irreducible. Demostrar que $K = E$ si y sólo si $a - rb \in A$ para algún $r \in \mathbb{Z}$.

4.15 Sea K/F una extensión de Galois tal que $K = F(x)$, con $x^n \in F$ para algún entero $n > 0$. Sea G su grupo de Galois. Mostrar que el grupo derivado G' es cíclico y que, en el caso que n sea primo, también el grupo G es cíclico.

4.16 Sea K/F una extensión de Galois abeliana, cuyo grupo de Galois G tiene n elementos. Supóngase que F contiene alguna raíz n-ésima primitiva de la unidad. Demostrar que K es cuerpo de descomposición sobre F de un polinomio del tipo

$$(X^{n_1} - a_1)(X^{n_2} - a_2) \cdots (X^{n_s} - a_s).$$

4.17 Sea F un cuerpo de característica el primo positivo p. Sea K/F una extensión cíclica de grado p y σ un automorfsmo generador del grupo de Galois. Demostrar que la aplicación lineal $S : K \longrightarrow K$ dada por $S : u \mapsto u - \sigma(u)$ es nilpotente y, en consecuencia, $\ker S \neq \ker S^2$. Mostrar que, si x está en el núcleo de S^2 y no en el de S, entonces $y = x(\sigma(x) - x)^{-1}$ satisface $\sigma(y) = y + 1$. Obtener de aquí que K es cuerpo de descomposición sobre F de un polinomio irreducible del tipo $X^p - X - a$ (Teorema de Artin y Scrhreier).

2.5. Teoremas de Abel y Galois

5.1 Mostrar que A_4 no es un grupo simple.

5.2 Mostrar que S_4 no tiene elementos de orden 6. Demostrar que todo subgrupo de S_4 de índice 4 es isomorfo al grupo simétrico S_3.

5.3 Mostrar que A_4 no contiene ningún subgrupo de orden 6.

5.4 Sean n y m enteros positivos. Mostrar que si m es impar y mayor o igual que 3 entonces los m-ciclos de S_n generan A_n. Usar esto para demostrar que si p es el mayor primo positivo que es menor o igual que n y S_n actúa sobre un conjunto no vació dado T entonces la órbita de un elemento arbitrario t de T tiene a los menos p elementos o cardinal ≤ 2. (Indicación: Para la segunda parte del ejercicio tomar un p-ciclo arbitrario $\sigma \in S_n$ y considerar la acción inducida del subgrupo generado por σ sobre el conjunto T.)

5.5 Sea G un subgrupo del grupo simétrico S_n. Supóngase que G contiene alguna permutación impar. Demostrar que existe algún subgrupo normal de G cuyo índice es 2.

5.6 Demostrar que si $n \geq 5$ entonces los únicos subgrupos normales de S_n son A_n, $\{\mathrm{Id}\}$ y S_n.

5.7 Mostrar que para todo entero $n \geq 2$ el grupo simétrico S_n tiene un único subgrupo de índice 2.

5.8 Usar el ejercicio 5.6 para comprobar la afirmación del ejercicio 4.6.

5.9 Sea F un cuerpo, f un polinomio irreducible y separable de $F[X]$ de grado n, y K el cuerpo de descomposición de f sobre F. Demostrar que si $[K : F] = n!$ entonces, para cualquier $x \in K$ que sea raíz de f, la extensión $F(x)/F$ no contiene ningún cuerpo intermedio estrictamente comprendido entre F y $F(x)$ que sea extensión normal de F.

5.10 Sea n un entero mayor o igual que 4, N un subgrupo normal de A_n o S_n, que contiene alguna permutación que es producto de dos transposiciones disjuntas. Supóngase que $|N| \leq 4$. Mostrar que N no puede ser de orden 2, y que si $|N| = 4$ entonces $n = 4$ y N es isomorfo al grupo de Klein. ¿Puede darse alguna demostración de este hecho que sea independiente de la simplicidad de los grupos alternados A_n $(n \geq 5)$?

5.11 Determinar el número de elementos de A_5 que tienen órdenes 2, 3 y 5.

5.12 (J. Gallian). Usar el ejercicio anterior para demostrar que A_5 es un grupo simple. [Indicación. Tener en cuenta que si G es un grupo, N un subgrupo normal de G tal que $|G/N| < \infty$, entonces para todo elemento x de G cuyo orden sea finito y primo relativo con $|G/N|$ se tiene necesariamente $x \in N$].

5.13 Sea $\Omega = \{1,\ 2,\ 3, \ldots\}$. Denótese por G_n al subgrupo del grupo de permutaciones de Ω que deja fijo a todo elemento $j > n$. Sea N_n el subgrupo de los elementos de G_n que actúan como permutaciones pares de $\{1, \ldots, n\}$. Hágase $G = \bigcup_{n\geq 1} G_n$ y $N = \bigcup_{n\geq 1} N_n$. Demostrar que G es un subgrupo del grupo de permutaciones de Ω y que $N = \bigcup N_n$ es un subgrupo normal de G cuyo índice es 2. Comprobar que todo subgrupo normal de G distinto de G y de $\{\mathrm{Id}\}$ coincide con N.

5.14 Demostrar que si $n \geq 2$ entonces todo subgrupo H de índice n del grupo simétrico S_n es isomorfo a S_{n-1}. [Indicación. Estudiar separadamente los casos $n < 5$ y $n \geq 5$. En el primero de ellos tener en cuenta el ejercicio 5.2. Si H es un subgrupo de índice n de S_n y $n \geq 5$ considérese el homomorfismo φ de S_n al grupo $S(S_n/H)$ de las permutaciones del conjunto S_n/H, que está definido por $\varphi(\sigma) = \varphi_\sigma$ donde $\varphi_\sigma : S_n/H \longrightarrow S_n/H$ es tal que $\varphi_\sigma(\tau H) = \sigma\tau H$ para cada $\sigma \in S_n$ y $\tau H \in S_n/H$. Téngase ahora en cuenta el resultado del ejercicio 5.6].

2.6. Solubilidad de ecuaciones por radicales

6.1 Sea f un polinomio irreducible con coeficientes en un cuerpo F. Si f tiene alguna raíz en un cuerpo L que es extensión radical de F, ¿es la ecuación polinómica $f(x) = 0$ soluble por radicales?

6.2 Sean K/F y L/K extensiones de cuerpos. Mostrar que si K/F y L/K son extensiones radicales entonces L/F es también una extensión radical. Si L/F es radical, ¿es entonces L/K radical?

6.3 Mostrar que la clase de las extensiones radicales no es una clase distinguida de extensionnes pero que, sin embargo, satisface la condición 2 del ejercicio I.2.45.

6.4 Sea F un cuerpo conteniendo todas las raíces de la unidad, K/F y L/K extensiones de cuerpos. Mostrar que para todo subcuerpo R de L que es extensión radical de F existe siempre alguna extensión radical R' de K que contiene a R y está contenida en L.

6.5 Sea F un cuerpo de característica cero. Demostrar que para todo entero positivo n el polinomio de $F[X]$ dado por la igualdad

$$f(X) = X^{4n} + aX^{3n} + bX^{2n} + cX^n + d$$

tiene grupo de Galois soluble.

6.6 Mostrar que toda extensión finita de un cuerpo finito es una extensión radical.

6.7 Mostrar que si F es un cuerpo finito y $f \in F[X]$ un polinomio no constante, entonces la ecuación $f(x) = 0$ es soluble por radicales, aunque tales radicales pueden ser de orden mayor que el grado del polinomio.

6.8 Sea K cuerpo de descomposición sobre el cuerpo F de un polinomio f de grado $n \geq 5$ y con a lo menos 5 raíces distintas $x_1, \ldots, x_5$. Suponer que F contiene raíces p-ésimas de la unidad distintas de 1 para cada primo p que divide a n y que el grupo de Galois G de la extensión K/F contiene a los F-automorfismos σ y τ del ejercicio 4.5. Demostrar que K/F no puede ser una extensión radical.

6.9 Demostrar que la clase $\mathfrak{S}$ de las extensiones separables K/F cuya clausura normal tiene grupo de Galois sobre F soluble es una clase transitiva de extensiones.

6.10 Sea K/F una extensión finita. Suponer que F tiene característica nula o un primo $p > [K : F]$. Demostrar que K/F está en la clase $\mathfrak{S}$ del ejercicio 6.9 si y sólo si existe alguna extensión radical L de F que contiene a K como cuerpo intermedio.

6.11 Sea K/F una extensión de Galois de un cuerpo F de característica cero que contiene a todas las raíces de la unidadd. Usar el ejercicio 4.10 para demostrar que si el elemento y de K pertenece a alguna extensión radical de F entonces y pertenece también a una extensión radical de F que está contenida en K.

6.12 Sea F un cuerpo f y g polinomios de $F[X]$ con f irreducible de grado primo p. Suponer $1 \leq \deg g < p$ y que existe algún entero $r \geq 1$ tal que f divide a $g(X^r)$. Demostrar que si K es cuerpo de descomposición de f sobre F entonces K/F es una extensión radical.

6.13 Sea K/F una extensión normal de grado 3 y

$$F = F_0 \subset F_1 \subset \cdots \subset F_m = L$$

una torre radical tal que $K \subset L$. Supóngase que el grado $[F_m : F_{m-1}]$ es un número primo p_m y que K no está contenido en F_{m-1}. Demostrar que entonces $p_m = 3$ y F_m/F_{m-1} es una extensión normal.

6.14 Sea $f \in \mathbb{Q}[X]$ un polinomio irreducible de grado 3 que tiene todas sus raíces reales. Sea K el cuerpo de descomposición de f sobre $\mathbb{Q}$. Demostrar que la ecuación $f(x) = 0$ no es resoluble por radicales reales; esto es, no existe ninguna extensión radical R de $\mathbb{Q}$ tal que $K \subset R \subset \mathbb{R}$.

6.15 Sea K/F una extensión de Galois finita. Suponer F de característica distinta de 2. Mostrar que existe entonces algún cuerpo intermedio E de la extensión K/F que es extensión de grado impar de F y tal que K/E es extensión radical que tiene alguna torre radical en la que cada uno de los subcuerpos es extensión cuadrática del precedente.

6.16 Mostrar que si en el ejercicio anterior $K \subset \mathbb{C}$ y $F = \mathbb{Q}$ entonces puede elegirse E siendo un subcuerpo de $\mathbb{R}$ que es extensión de grado impar de $\mathbb{Q}$

6.17 Sea Ω de una clausura algebraica de un cuerpo F_0 de característica cero y S un subconjunto de Ω que contiene todas las raíces de cada uno de los polinomios irreducibles de grado impar del anillo de polinomios $F_0[X]$. Sea $F = F_0(S)$. Demostrar que todo polinomio no nulo de $F[X]$ es tal que la ecuación $f(x) = 0$ es soluble por radicales. ¿Puede siempre resolverse la correspondiente ecuación polinómica utilizando radicales a lo sumo de grado dos?

Los ejercicios siguientes tienen por objetivo caracterizar los subgrupos solubles y transitivos de los grupos simétricos S_p (p primo positivo). Dicha caracterización es importante para resolver el ejercicio 6.23 que trata un bonito resultado de Galois.

6.18 Sea $H \neq \{\mathrm{Id}\}$ un subgrupo normal de un grupo transitivo G de permutaciones del conjunto $\{1, \ldots, n\}$. Comprobar que todas las H-órbitas tienen el mismo número de elementos, y por consiguiente, si $n = p$ es un número primo entonces H es transitivo.

6.19 Sea p un primo positivo y $\mathrm{GA}(\mathbb{Z}/(p))$ el subgrupo del grupo de premutaciones del conjunto $\mathbb{Z}/(p)$ cuyos elementos son las permutaciones de $\mathbb{Z}/(p)$ de la forma $x \mapsto ax + b$, $a \neq 0$. A $\mathrm{GA}(\mathbb{Z}/(p))$ se denomina *grupo afín* de $\mathbb{Z}/(p)$ y a sus elementos *afinidades* de $\mathbb{Z}/(p)$. De las afinidades de $\mathbb{Z}/(p)$ del tipo $x \mapsto x + b$ se dice que son *traslaciones* del grupo afín.

1. Mostrar que el conjunto de las traslaciones distintas de la identidad coincide con el de las únicas permutaciones pertenecientes a $\mathrm{GA}(\mathbb{Z}/(p))$ que no tienen punto fijo y, consiguientemente, son los únicos elementos de $\mathrm{GA}(\mathbb{Z}/(p))$ que son p-ciclos.
2. Comprobar que si un subgrupo del grupo de permutaciones de $\mathbb{Z}/(p)$ contiene alguna traslación distinta de la identidad entonces necesariamente debe contenerlas todas.
3. Demostrar que todo subgrupo H de $\mathrm{GA}(\mathbb{Z}/(p))$ es un grupo soluble.

6.20 Sea G un subgrupo del grupo de permutaciones de $\mathbb{Z}/(p)$. Sea H un subgrupo de $\mathrm{GA}(\mathbb{Z}/(p)$ que contiene al subgrupo de traslaciones y que está contenido en G como subgrupo normal. Demostrar que G es un subgrupo del grupo afín de $\mathbb{Z}/(p)$. [Indicación. Sea $\tau : x \mapsto x + \bar{1}$ y $\eta \in G$. Por el ejercicio anterior, $\eta \circ \tau \circ \eta^{-1} : x \mapsto x + \bar{k}$. Así, $\eta(x + \bar{1}) = \eta(x) + \bar{k}$, de donde se obtiene $\eta : x \mapsto \bar{k}x + b$.]

6.21 Sea p un primo positivo, G un subgrupo del grupo simétrico S_p. Se dirá que G es *permutación isomorfo* a un subgrupo $\bar{G}$ de $\mathrm{GA}(\mathbb{Z}/(p))$ si existen una biyección $b : \{1, \ldots, p\} \longrightarrow \mathbb{Z}/(p)$ y un isomorfismo $\theta : G \longrightarrow \bar{G}$ tales que $b \circ \sigma(i) = \theta(\sigma)(b(i))$ para cualesquiera $\sigma \in G$ y $i \in \{1, \ldots p\}$.

1. Sea H un subgrupo normal de G y $\theta : H \longrightarrow \bar{H}$ un permutación isomorfismo sobre un subgrupo $\bar{H}$ de $\mathrm{GA}(\mathbb{Z}/(p))$. Mostrar que, si H contiene algún p-ciclo, entonces $\bar{H}$ contiene todas las traslaciones y existe algún permutación isomorfismo φ de G sobre un subgrupo de $\mathrm{GA}(\mathbb{Z}/(p))$ tal que $\varphi(h) = \theta(h)$ para todo $h \in H$.
2. Demostrar que si p divide a $|G|$ y $|G| \leq p(p-1)$ entonces G es permutación isomorfo a algún subgrupo de $\mathrm{GA}(\mathbb{Z}/(p))$ que contiene al subgrupo de las traslaciones como subgrupo normal.

6.22 Usar inducción y los ejercicios 6.21 y 6.18 para demostrar que cada subgrupo soluble y transitivo de S_p (p primo) es permutación isomorfo a un subgrupo de $\mathrm{GA}(\mathbb{Z}/(p))$ conteniendo al subgrupo de las traslaciones.

6.23 (Galois). Sea $f(X) \in F[X]$ un polinomio irreducible de grado un primo p, con coeficientes en un cuerpo F de característica cero, y K el cuerpo de descomposición de $f(X)$ sobre F. Demostrar que $f(x) = 0$ es soluble por radicales si y sólo si $K = F(x_i, x_j)$ para cualesquiera dos raíces distintas x_i y x_j de $f(X)$.

2.7. Ejemplo de polinomio de $\mathbb{Q}[X]$ de ecuación insoluble

7.1 Sea ε una raíz octava primitiva de la unidad. Mostrar que $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ es un ejemplo de una extensión de Galois de grado 4 que no contiene ningún 4-ciclo.

7.2 Mostrar que para todo entero $n \geq 5$ existe siempre algún polinomio $f(X) \in \mathbb{Q}[X]$ tal que la ecuación $f(x) = 0$ no es soluble por radicales.

7.3 Sea p un primo mayor que 11. Demostrar que $f(X) = X^5 - pX + p$ es un polinomio de $\mathbb{Q}[X]$ tal que la ecuación $f(x) = 0$ no es soluble por radicales.

7.4 Sea f un polinomio de grado 5 con coeficientes en el cuerpo F y cuyo grupo de Galois es isomorfo al grupo simétrico S_5.

1. Mostrar que si L es el cuerpo de descomposición de f sobre F se tiene entonces que L/F es extensión de Galois, que $[L : F] = 120$ y que f es irreducible sobre F.
2. Utilizar el ejercicio I.8.29 para dar una demostración directa, sin utilizar la insolubilidad de S_5 ni el teorema 2.6.6, de que la ecuación polinómica $f(x) = 0$ no es soluble por radicales.

7.5 (Kronecker). Sea $f(X) \in \mathbb{Q}[X]$ un polinomio irreducible de grado primo e impar p. Mostrar que si $f(x) = 0$ es soluble por radicales entonces el número de raíces reales de $f(X)$ es 1 ó p. [Indicación. Utilizar el ejercicio 6.23].

7.6 ¿Puede utilizarse el ejercicio 7.5 en lugar del lema 2.7.2 para demostrar la proposición 2.7.3?

7.7 Sea p un número primo mayor o igual que 5 y f el polinomio de $\mathbb{Q}[X]$ definnido por la igualdad

$$f(X) = X^p - 4X + 2.$$

Demostrar que la ecuación polinómica $f(x) = 0$ no es soluble por radicacles.

7.8 Sean f y p como en el ejecicio 7.5. Suponer además que $p \equiv 3 (\text{mód } 4)$. Mostrar que las raíces reales de f son 1 ó p dependiendo de que su discriminante sea negativo o positivo.

7.9 Demostrar que para N un entero suficientemente grande, y p un primo positivo dado, la ecuación polinómica correspondiente al polinomio

$$f(X) = X(X - Np^2)(X + Np^2)(X^2 + N^2p^4) + p$$

no puede resolverse por radicales.

7.10 (R. Brauer). Sea k un impar estrictamente mayor que 3, m un entero impar positivo y $n_1 < \cdots < n_{k-2}$ una sucesión estrictamente creciente de $k-2$ números pares. Sean

$$g(X) = (X^2 + m)(X - n_1)(X - n_2)\cdots(X - n_{k-2}), \qquad f(X) = g(X) - 2.$$

Mostrar que la función polinómica $x \mapsto g(x)$ tiene $(k-3)/2$ máximos relativos en $[n_1, n_{k-2}]$ cuyos valores son todos mayores que 2, y $(k-3)/2$ mínimos relativos menores que -2. Demostrar que $f(X)$ tiene $(k-3)$ raíces reales en $[n_1, n_{k-2}]$. Considerando los coeficientes de los términos de f de grados $k-1$ y $k-2$, comprobar que f tiene exactamente $k-2$ raíces reales, en el caso en que se elija m suficientemente grande. Demostrar que, si además k es un primo p, entonces el grupo de Galois de f es S_p.

7.11 Sea G un grupo finito arbitrario. Mostrar que puede elegirse algún primo positivo p tal que S_p contiene algún subgrupo isomorfo a G. Demostrar la existencia de alguna extensión finita $K/\mathbb{Q}$ y un cuerpo intermedio E de dicha extensión tal que K/E es extensión de Galois finita de grupo de Galois isomorfo a G.

Apéndice A

Dcpos y axioma de elección

1.1 Sea S un subconjunto de un conjunto parcialmente ordenado L. Mostrar que si S está bien ordenado entonces S es una cadena y que si $S \neq \emptyset$ es cadena entonces S es dirigido. ¿Qué puede decirse de las afirmaciones recíprocas?

1.2 Sea L un conjunto parcialmente ordenado Supóngase que $\{A_i\}_{i\in I}$ y $\{B_j\}_{j\in J}$ son familias de subconjuntos de L tales que $A_i \cap B_j \neq \emptyset$ para cualesquiera $i \in I$ y $j \in J$. Suponer que existen los supremos de los conjuntos B_j y los ínfimos de los conjuntos A_i, al igual que el ínfimo de $\{\bigvee B_j : \ j \in J\}$ y el supremo de $\{\bigwedge A_i : \ i \in I\}$. Mostrar que

$$\bigvee\{\bigwedge A_i : \ i \in I \} \leq \bigwedge\{\bigvee B_j : \ j \in J\}.$$

1.3 Sea A un subconjunto de un conjunto parcialmente ordenado L. Suponer que A tiene ínfimo en L. Comprobar que

$$\bigcap_{x\in A} \downarrow x = \downarrow \left(\bigwedge A\right).$$

1.4 Justificar los detalles de las afirmaciones hechas respecto a los ejemplos de dcpos dados en este apéndice.

1.5 Un conjunto parcialmente ordenado L se dice que satisface la *condición de cadena ascendente* si cada vez que $x_1, x_2, \ldots$ son elementos de L tales que

$$x_1 \leq x_2 \leq \cdots \leq x_n \leq \cdots,$$

existe entonces algún entero positivo n_0 tal que $x_{n_0} = x_{n_0+1} = x_{n_0+2} = \cdots$. Mostrar que si L es un conjunto parcialmente ordenado que satisface la condición de cadena ascendente entonces los subconjuntos dirigidos de L son los subconjuntos no vacíos de L que tienen un mayor elemento y que L es entonces un dcpo.

1.6 De los conjuntos parcialmente ordenados que se dan a continuación determinar aquéllos que son dcpos.

1. El conjunto $\mathcal{P}(\mathbb{N})$ respecto a la relación de inclusión.
2. La familia de los subconjuntos finitos de $\mathbb{N}$ respecto a la inclusión.
3. La familia de los subconjuntos cofinitos de $\mathbb{N}$ ordenados respecto a la inclusión.
4. El conjunto $\{1/n : n = 1, 2, 3, \ldots\}$ respecto al orden usual $\leq$.
5. El conjunto $\{1/n : n = 1, 2, 3, \ldots\}$ respecto al orden $\geq$.

¿Cuáles son dcpos punteados?

1.7 Un subconjunto I de un conjunto parcialmente ordenado se dice que es un *ideal* si es dirigido y para todo $x \in I$ el subconjunto $\downarrow x$ está contenido en I. Demostrar que un conjunto parcialmente ordenado D es un dcpo si y sólo si todo ideal de D tiene un supremo.

1.8 Sea D un dcpo. Demostrar que las dos afirmaciones siguientes son equivalentes: (i) cada subconjunto de D acotado superiormente tiene un supremo; (ii) todo subconjunto no vacío de D tiene un ínfimo.

1.9 Mostrar que existen subconjuntos S de dcpos que son dcpos respecto al orden inducido por D y que, sin embargo, no son sub-dcpos.

1.10 Sea S un conjunto arbitrario y $\mathcal{W}$ la familia formada por todos los pares $(W, \leq_W)$, donde W es subconjunto de S y $\leq_W$ un buen orden en W. Defínase en $\mathcal{W}$ un orden parcial $\preceq$ del siguiente modo: $W_1 \preceq W_2$ si y sólo si $W_1 \subset W_2$, con el buen orden de W_2 extendiendo al de W_1, y de manera que los elementos de $\complement_{W_2} W_1$ son todos ellos posteriores respecto a $\preceq_{W_2}$ a cada uno de los de W_1. Mostrar que $\mathcal{W}$ tiene elementos maximales respecto al orden parcial $\preceq$. Obtener de aquí que S puede bien ordenarse. Demostrar que el principio de buena ordenación enunciado en la página 288 es equivalente al axioma de elección.

1.11 Una familia no vacía $\mathcal{L}$ de conjuntos se dice que es de *carácter finito* si la condición necesaria y suficiente para que un conjunto X pertenezca a $\mathcal{L}$ es que cada uno de sus subconjuntos finitos esté en L. Demostrar la equivalencia de las afirmaciones siguientes y su equivalencia con el axioma de elección.

1. Todo conjunto ordenado L contiene alguna cadena maximal.
2. Si L es un conjunto ordenado no vacío en el que cualquier subconjunto bien ordenado tiene una cota superior, entonces L tiene algún elemento maximal.
3. *Lema de Teichmuller-Tuckey-Bourbaki.* Toda familia $\mathcal{L}$ de carácter finito de subconjuntos de un conjunto S tiene algún elemento maximal respecto a la inclusión.

[*Indicación.* Para demostrar que 1⇒2 puede procederse de la manera siguiente: Sea $\leq$ el orden parcial en L y $\mathcal{T}$ la familia de los subconjuntos bien ordenados de L respecto a la restricción de $\leq$. Definir en $\mathcal{T}$ un orden parcial $\leq_{\mathcal{T}}$ haciendo $\mathcal{A} \leq_{\mathcal{T}} \mathcal{B}$ si y sólo si $\mathcal{A} \subset \mathcal{B}$ y $\mathcal{A}$ es segmento inicial de $\mathcal{B}$ (i. e. existe $b \in \mathcal{B}$ tal que $\mathcal{A} = \{x \in \mathcal{B} : x \leq b\}$). Sea $\mathcal{M}$ maximal en $\mathcal{T}$ y $N = \bigcup_{R \in \mathcal{M}} R$. Comprobar: (a)$N \in \mathcal{T}$; (b) N es maximal en $\mathcal{T}$; (c) las cotas superiores de N pertenecen a N y son elementos maximales de L.]

Apéndice B

Trascendencia de e y π

2.1 Sea $f(X)$ un polinomio de $\mathbb{Z}[X]$ de grado n. Comprobar que si p, $q \in \mathbb{Z}$, $q \neq 0$ y $f(p/q) \neq 0$, entonces se verifica

$$|f(p/q)| \geq \frac{1}{|q^n|}.$$

2.2 Sean p, $q \in \mathbb{Z}$, $q \neq 0$ tal que $f(p/q) \neq 0$. Supóngase que x es un número real raíz del polinomio $f \in \mathbb{Z}[X]$ y que $x - 1 < p/q < x + 1$ y que $f(p/q) \neq 0$. Comprobar que existe un número real estrictamente positivo M tal que $|f'(y)| < M$ si $x - 1 < y < x + 1$. Usar el teorema del valor medio para demostrar que

$$\left|\frac{p}{q} - x\right| > \frac{1}{M|q|^n}$$

y consecuentemente

$$\left|\frac{p}{q} - x\right| > \frac{1}{q^{n+1}}$$

si $q \geq M$.

2.3 Un *número de Liouville* es un número real del tipo

$$x = \sum_{n=1}^{\infty} \frac{a_n}{10^{n!}},$$

donde los a_n son todos enteros tales que $0 \leq a_n \leq 9$ y un número infinito de ellos siendo no nulos. Considerar los enteros $q_m = 10^{m!}$ y usar el ejercicio anterior para demostrar que los números de Liouville son trascendentes.

2.4 Demostrar que el conjunto de números de Liouville tiene la potencia del continuo.