ÁLGEBRA II

Fernando Chamizo Lorente

3º de Matemáticas. Curso 1996-1997

Versión del 21/1/2002

Índice

Bibliografía:

I. Stewart. "Galois Theory". Ed Chapman and Hall.

A. Clark. "Elementos de Álgebra Abstracta". Ed. Alhambra.

Ideas que subyacen a la Teoría de Galois

De forma poco precisa pero ilustrativa, se puede afirmar que la Teoría de Galois estudia las "simetrías" de las soluciones de ecuaciones algebraicas $x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=0$.

El resultado más conocido de esta teoría, y con el que a veces se la identifica, es que si $n>4$ hay ecuaciones para las que x no se puede despejar a partir de los coeficientes en términos de sumas, restas, multiplicaciones divisiones y radicales, por tanto no existe ninguna fórmula de este tipo que resuelva la ecuación general de grado $n>4$. En realidad este resultado es algunos años anterior al famoso trabajo de Galois y fue probado en 1826 por Abel (Ruffini había obtenido con anterioridad una demostración poco rigurosa). Como veremos, la contribución de Galois fue dar condiciones necesarias y suficientes para la resolubilidad por radicales en términos de un grupo, el grupo de Galois, que refleja las "simetrías" de las soluciones de la ecuación. En la práctica suele ser difícil verificar estas condiciones para una ecuación dada porque el grupo de Galois puede ser muy complicado de calcular, pero desde el punto de vista matemático la relación entre grupos de simetrías y resolución de ecuaciones es muy reveladora, permitiendo perfeccionar y aclarar ideas de Lagrange, Gauss, Ruffini y Abel.

§1. El grupo de Galois.

Descomponiendo el polinomio $P(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=0$ en factores, es fácil comprobar que sus coeficientes se pueden expresar como polinomios simétricos de las raíces $x_1,x_2\ldots,x_n$ (se tiene por ejemplo $a_0=(-1)^nx_1x_2\ldots x_n$ y $-a_{n-1}=x_1+x_2+\ldots+x_n$), por tanto cualquier permutación de las raíces deja invariantes los coeficientes. El grupo de Galois se define como el conjunto formado por las permutaciones que son compatibles con las relaciones algebraicas que pudiera haber entre las raíces. Por ejemplo, las raíces de $x^4+x^3+x^2+x+1$ son $x_1=e^{2\pi i/5}$, $x_2=x_1^2$, $x_3=x_1^3$, $x_4=x_1^4$ y la permutación que intercambia x_1 y x_2 no se incluye en el grupo de Galois porque si x_1 pasa a ser x_2 entonces $x_2=x_1\cdot x_1$ debiera pasar a ser $x_2\cdot x_2=x_4$ y no a x_1. De hecho no es difícil comprobar que sólo hay cuatro permutaciones válidas. Como en general no hay relaciones entre las raíces, el grupo de Galois suele ser el grupo S_n de todas las permutaciones de n letras.

§2. Grupo de Galois y resolución de ecuaciones.

Resolver $P(x)=0$ implica pasar de los coeficientes que son invariantes por todas las "simetrías" (permutaciones) a las raíces que son intercambiadas por ellas. El grupo de Galois mide el número mínimo de simetrías para que una función de las raíces se pueda escribir en términos de los coeficientes. Concretamente, Galois demostró que una función racional (cociente de polinomios) de las raíces se puede escribir como una función racional de los coeficientes si y sólo si es invariante por el grupo de Galois.

En las fórmulas clásicas para resolver las ecuaciones de segundo, tercer y cuarto grado se usan radicales para ir rompiendo poco a poco las simetrías de los coeficientes. Por ejemplo, al resolver $x^2 + bx + c = 0$ aparece $\sqrt{b^2 - 4c}$ que pasa de la función simétrica $b^2 - 4c = (x_1 + x_2)^2 - 4x_1x_2$ a la no simétrica $\sqrt{b^2 - 4c} = \pm(x_1 - x_2)$. Un ejemplo un poco más complicado es la ecuación de tercer grado $x^3 + px + q = 0$ cuya solución viene dada por

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{p}{3} \Big/ \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Obteniéndose las tres raíces a base de elegir los tres posibles valores (complejos) para la raíz cúbica.

Si llamamos x_1, x_2, x_3 a las raíces de la ecuación anterior,

$$x^3 + px + q = (x - x_1)(x - x_2)(x - x_3) \;\Rightarrow\; p = x_1x_2 + x_1x_3 + x_2x_3, \quad q = -x_1x_2x_3.$$

De nuevo, obsérvese que p y q son invariantes por S_3 (en el sentido de que no varían al cambiar x_1, x_2, x_3 por $x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}$ con $\sigma \in S_3$), mientras que algunos cálculos prueban que

$$\frac{q^2}{4} + \frac{p^3}{27} = -\frac{1}{108}(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

y por tanto $\sqrt{q^2/4 + p^3/27}$ sólo es invariante por A_3 (permutaciones pares). Por otra parte

$$-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = \frac{1}{27}(x_1 + \zeta x_2 + \zeta^2 x_3)^3 \quad \text{con } \zeta = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\frac{2\pi}{3}$$

implica que la raíz cúbica de esta expresión no es invariante por nada distinto de la identidad.

La idea fundamental de Galois es que los radicales reducen las simetrías de una forma muy particular que queda fielmente reflejada en la estructura del grupo de Galois.

§3. Radicales, grupos y la ecuación general de grado n.

Supongamos ahora que tenemos una fórmula para resolver la ecuación general de grado n (cuyo grupo de Galois es S_n) y que $r = \sqrt[p]{A}$ es uno de los radicales más interiores (podemos suponer p primo porque $\sqrt[ab]{} = \sqrt[a]{\sqrt[b]{}}$), es decir, A es una función racional de los coeficientes y por tanto simétrica en las raíces $x_1, x_2, \ldots, x_n$; así pues r^p es invariante por S_n. Consideremos el homomorfismo (pruébese que lo es)

$$\begin{aligned}\Phi : S_n &\longrightarrow \big(\mathbb{C} - \{0\}, \cdot\big)\\ \sigma &\longrightarrow r\big(x_{\sigma(1)}, x_{\sigma(2)}, \ldots x_{\sigma(n)}\big)\big/ r(x_1, x_2, \ldots, x_n).\end{aligned}$$

Nótese que $\sigma \in \operatorname{Nuc}\Phi$ si y sólo si r es invariante por σ. Si $\sqrt[p]{}$ ha roto algunas simetrías, hay elementos en la imagen distintos de 1; como además $\big(\Phi(\sigma)\big)^p = 1$ (porque r^p es invariante por S_n), se deduce que la imagen de Φ está formada por las raíces de la unidad de índice p, esto es

$$\operatorname{Im}\Phi = \{1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{p-1}\} \qquad \text{con } \zeta = \cos\frac{2\pi}{p} + i\operatorname{sen}\frac{2\pi}{p}.$$

Como $\operatorname{Im}\Phi$ (con la multiplicación) es isomorfo a $\mathbb{Z}_p$, por el teorema del isomorfismo se tiene

$$S_n\big/\operatorname{Nuc}\Phi \cong \mathbb{Z}_p.$$

Recapitulemos todo lo hecho: Hemos partido de la expresión A que es invariante por $G_0 = S_n$ y hemos demostrado que $\sqrt[p]{A}$ es invariante por $G_1 = \operatorname{Nuc}\Phi$ y que si $G_1 \underset{\neq}{\subset} G_0$ se debe tener $G_0/G_1 \cong \mathbb{Z}_p$. Todo este proceso se puede repetir al añadir un nuevo radical "reduciendo" G_1 a G_2 con $G_1/G_2 \cong \mathbb{Z}_{p'}$ y así sucesivamente hasta llegar a $\{\mathrm{Id}\}$ que corresponde a una expresión que no es invariante por nada y de la que podemos despejar las raíces. Todo esto queda resumido en el siguiente resultado:

Si la ecuación de grado n es soluble por radicales, existe una cadena de grupos

$$G_0 = S_n \supset G_1 \supset G_2 \supset \ldots \supset G_m = \{\mathrm{Id}\}$$

tales que cada uno es subgrupo normal del anterior y $G_{i-1}/G_i \cong \mathbb{Z}_{p_i}$, $1 \le i \le m$.

Para las ecuaciones de grados $n = 2, 3$ y 4, las cadenas son

$$S_2 \supset \{\mathrm{Id}\}, \quad S_3 \supset A_3 \supset \{\mathrm{Id}\}, \quad S_4 \supset A_4 \supset \langle (1,2)(3,4), (2,3)(1,4)\rangle \supset \{\mathrm{Id}\};$$

pero no existe ninguna cadena similar en el caso $n = 5$. La idea es que ésta debiera comenzar por $S_5 \supset A_5$ y como A_5 no tiene ningún subrupo normal no trivial no podemos completar esta cadena, y por tanto no existe una solución con radicales para la ecuación quíntica general. Lo mismo ocurre siempre que $n \ge 5$.

La demostración de que A_5 (y en general A_n) no tiene subgrupos normales no triviales es un poco tediosa pero no excesivamente complicada. Esencialmente, se prueba que si $\sigma \in A_5$, $\sigma \ne \{\mathrm{Id}\}$, entonces $\{\tau^{-1}\sigma\tau \,/\, \tau \in A_5\} = A_5$ y por tanto no existe ningún $\{\mathrm{Id}\} \ne H \underset{\neq}{\subset} A_5$ tal que $\tau^{-1}H\tau = H$ para todo τ.

§4. El teorema de Galois.

A pesar de que una parte de las ideas de la sección anterior están implícitas en el trabajo de Abel sobre la imposibilidad de resolver la quíntica por radicales, fue Galois quien puso de manifiesto la estrecha relación entre la resolubilidad por radicales y la teoría de grupos. Su resultado principal contempla ecuaciones cuyo grupo de Galois no es necesariamente S_n y permite dar una condición necesaria y suficiente para que las raíces de una ecuación se puedan expresar mediante radicales.

Teorema (de Galois): *La ecuación $P(x) = 0$ se puede resolver en términos de sus coeficientes con expresiones obtenidas por composición de funciones racionales y radicales si y sólo si el grupo de Galois, G, tiene una cadena de subgrupos $G = G_0 \supset G_1 \ldots \supset G_{m-1} \supset G_m$ cada uno subgrupo normal del anterior y con G_m el grupo trivial, de modo que $G_{i-1}/G_i \approx \mathbb{Z}_{p_i}$ con p_i primo, $i = 1, 2 \ldots, m$.*

1. Cuerpos y sus extensiones

§1. Definición de cuerpo.

Un sorprendente teorema que demostraremos más adelante implica que la suma, resta, multiplicación y división de raíces de polinomios da lugar a nuevas raíces de polinomios. Así, por ejemplo, como $1+\sqrt{2}$ y $\sqrt{3}-2$ son raíces de polinomios con coeficientes en $\mathbb{Q}$, concretamente de x^2-2x-1 y x^2+4x+1, entonces $(1+\sqrt{2})(\sqrt{3}-2)$ es también raíz de un polinomio con coeficientes en $\mathbb{Q}$, concretamente de $x^4+8x^3-10x^2-8x+1=0$. Esto sugiere que la estructura algebraica natural para estudiar raíces de polinomios es aquella en la que podemos sumar, restar, multiplicar y dividir (salvo por cero), la cual corresponde a la idea intuitiva de cuerpo.

Definición: *Un cuerpo, K es un anillo tal que $K-\{0\}$ es un grupo abeliano con respecto a la multiplicación.*

Para aquellos que tengan problemas para identificar la definición anterior con su significado intuitivo, se recuerdan los conceptos de anillo y de grupo que ya se introdujeron el curso pasado.

Definición: *Un anillo, A, es un conjunto dotado con dos operaciones cerradas, $\oplus$ y $\otimes$ (suma y multiplicación), de modo que se verifican las siguientes propiedades:*

i) A es un grupo abeliano con respecto a $\oplus$.

ii) $\otimes$ es una operación asociativa en A.

iii) Se cumplen las leyes distributivas $(a\oplus b)\otimes c=(a\otimes c)\oplus(b\otimes c)$ y $c\otimes(a\oplus b)=(c\otimes a)\oplus(c\otimes b)$.

Definición: *Un grupo, G, es un conjunto dotado con una operación cerrada, $*$, tal que se verifican las siguientes propiedades:*

i) $*$ es asociativa: $g*(h*f)=(g*h)*f$.

ii) Existe el elemento neutro: $\exists e\in G \,/\, e*g=g*e=g\ \forall g\in G$.

iii) Existe el elemento inverso: $\forall g\in G\ \exists h\in G \,/\, h*g=g*h=e$.

Nota: Si además $*$ es una operación conmutativa ($g*h=h*g$) se dice que el grupo es abeliano o conmutativo.

Obsérvese que intuitivamente un anillo (conmutativo) es un conjunto en el que podemos sumar, restar y multiplicar; mientras que un grupo abeliano es un conjunto en el que podemos sumar y restar (sumar el inverso).

NOTA: En estas notas se usarán las letras K, A y G para designar cuerpos, anillos y grupos respectivamente, sin indicar explícitamente que lo son siempre que ello no dé lugar a confusión. Además, en este curso sólo se considerarán anillos conmutativos y unitarios, es decir, en los que $\otimes$ es una operación conmutativa y tiene elemento neutro.

Es conviente recordar también que en un anillo puede haber elementos con inverso multiplicativo, y se les llama unidades. También es importante recordar que un ideal, I, de un anillo (conmutativo), A, es un subconjunto de A cerrado con respecto a la suma y tal que si a pertenece a A y x pertenece a I, entonces su producto pertenece a I.

Muchas veces se indican los ideales por sus generadores, así $I = (2)$ en $\mathbb{Z}$ son los números pares, y $(2,3)$ son todas las combinaciones lineales enteras de 2 y 3. No es difícil ver que $(2,3) = \mathbb{Z}$. La notación A/I indica las clases de equivalencia módulo el ideal, por ejemplo, $\mathbb{Z}/(2)$ (escrito también $\mathbb{Z}/2\mathbb{Z}$ o a veces $\mathbb{Z}_2$) son las clases de números pares e impares. Estas clases tienen de nuevo estructura de anillo, de hecho en este ejemplo forman un cuerpo.

Veamos algunos ejemplos de cuerpos y anillos:

Ejemplo 1. $\mathbb{Q}$ es un cuerpo.

Ejemplo 2. $\mathbb{Z}$ es una anillo.

Ejemplo 3. $\mathbb{Z}$ es un grupo abeliano con la suma.

Ejemplo 4. $\mathbb{Z}$ no es un grupo con el producto (porque no existe elemento inverso). Su estructura se conoce con el nombre de semigrupo.

Ejemplo 5. $C = \{a+b\sqrt{2} \,/\, a,b \in \mathbb{Z}\}$ es un anillo con respecto a la suma y el producto habituales.

Para comprobarlo, obsérvese que la suma y el producto están bien definidas en C, es decir, $\alpha, \beta \in C \Rightarrow \alpha + \beta \in C$ y $\alpha\beta \in C$. Porque si $\alpha = a + b\sqrt{2}$ y $\beta = c + d\sqrt{2}$ entonces $\alpha + \beta = (a+c) + (b+d)\sqrt{2} \in C$ y $\alpha\beta = (ac + 2bd) + (ad + bc)\sqrt{2} \in C$. Una vez realizadas estas comprobaciones, las propiedades *i)*, *ii)* y *iii)* de la definición de anillo están garantizadas porque se cumplen en $\mathbb{R}$ y $C \subset \mathbb{R}$.

Ejemplo 6. $C' = \{a + b\sqrt{2} \,/\, a,b \in \mathbb{Q}\}$ es un cuerpo con respecto a la suma y el producto habituales. A este cuerpo se le denota con $\mathbb{Q}(\sqrt{2})$ (el porqué de esta notación quedará claro más adelante).

Se puede demostrar que C' es un anillo procediendo como en el ejemplo anterior porque allí no usamos la hipótesis de que a y b eran enteros (sólo que la multiplicación era cerrada para ellos). Así pues sólo falta comprobar que C' es un grupo abeliano con respecto al producto. Obviamente el producto es conmutativo y asociativo (porque C' es un anillo conmutativo) y tiene elemento neutro $1 = 1 + 0\sqrt{2}$. Además como

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in C',$$

también existe elemento inverso.

Ejemplo 7. Si p es primo $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo.

Recuérdese que $\mathbb{Z}/p\mathbb{Z}$ son las clases de congruencia módulo p: $\overline{0}, \overline{1}, \dots, \overline{p-1}$, es decir, todos los posibles restos al dividir por p.

Este cuerpo se suele denotar con $\mathbb{F}_p$. Es un cuerpo con un número finito de elementos. A pesar de que existen otros cuerpos finitos seguramente es demasiado prematuro introducirlos ahora.

Obsérvese que en $\mathbb{F}_p$ se cumple $1+1+1+\overset{p\ \text{veces}}{\cdots\cdots}+1 = 0$. Esta propiedad es tan importante a la hora de clasificar los cuerpos que requiere una definición especial.

DEFINICIÓN: *Diremos que un cuerpo tiene* característica n *si n es el menor número natural tal que* $1+1+\overset{n\ \text{veces}}{\cdots\cdots}+1 = 0$. *Si esta suma fuera siempre distinta de cero se dice que el cuerpo tiene* característica cero.

Así por ejemplo $\mathbb{R}$ y $\mathbb{Q}$ tienen característica cero y $\mathbb{F}_p$ tiene característica p.

Ejemplo 8. Dado un dominio de integridad, $\mathcal{D}$, (esto es, un anillo conmutativo con unidad tal que $ab = 0 \Rightarrow a = 0$ ó $b = 0$), el cuerpo de fracciones de $\mathcal{D}$ es el conjunto de expresiones de la forma r/s con $r, s \in \mathcal{D}$, $s \neq 0$, bajo la relación de equivalencia $r/s \sim t/u \Leftrightarrow ru = ts$. Nótese que $\mathcal{D}$ se puede identificar con los elementos de la forma $r/1$. Intuitivamente, el cuerpo de fracciones de $\mathcal{D}$ es el cuerpo que resulta si permitimos dividir en $\mathcal{D}$. Por ejemplo, el cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.

Ejemplo 9. Si $A \subset \mathbb{C}$ es el anillo $A = \{n+m\sqrt{-2} \,/\, n, m \in \mathbb{Z}\}$, entonces $A/(1+\sqrt{-2})$ es un cuerpo de tres elementos.

Nótese primero que $\overline{n+m\sqrt{-2}} = \overline{n-m} + \overline{m(1+\sqrt{-2})} = \overline{n-m}$, y por tanto basta considerar clases cuyos representantes sean números enteros. Por otra parte, $\overline{n} = \overline{n} + \overline{(1-\sqrt{-2})(1+\sqrt{-2})} = \overline{n-3}$. Así pues $A/(1+\sqrt{-2}) = \{\overline{0}, \overline{1}, \overline{2}\}$ (es fácil comprobar que estas tres clases son distintas). Con ello hemos demostrado que $A/(1+\sqrt{-2})$ es prácticamente idéntico a $\mathbb{F}_3$. En general, si un primo p es suma de un cuadrado y el doble de un cuadrado, digamos $p = n^2 + 2m^2$, se puede demostrar que $A/(n+m\sqrt{-2})$ es "isomorfo" a $\mathbb{F}_p$.

§2. Polinomios.

Un polinomio es una expresión de la forma $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ donde x es una indeterminada y los coeficientes a_i pertenecen a un anillo.

El conjunto de todos los polinomios sobre el anillo A (con coeficientes en A) en la indeterminada x se denota con $A[x]$ y tiene una estructura natural de anillo. Se dice que $A[x]$ es el <u>anillo de polinomios sobre A</u>. Abreviaremos la notación $\big(A[x_1]\big)[x_2]$, $\Big(\big(A[x_1]\big)[x_2]\Big)[x_3]$, etc. escribiendo simplemente $A[x_1, x_2]$, $A[x_1, x_2, x_3]$, etc. Obsérvese que estos anillos corresponden a los polinomios de varias variables.

Definición: *Si $P \in A[x]$, $P = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ con $a_n \neq 0$ diremos que P tiene <u>grado n</u> y se escribe $\operatorname{grad} P = n$ o también $\partial P = n$. Si $P = 0$ escribiremos formalmente $\partial P = -\infty$.*

Proposición 2.1: *Si A es un dominio de integridad, $A[x]$ también lo es. Además si $P, Q \in A[x]$*

$$1)\ \partial(P + Q) \leq \max(\partial P, \partial Q) \qquad 2)\ \partial(PQ) = \partial P + \partial Q.$$

<u>Dem.</u>: Las propiedades 1) y 2) se siguen fácilmente de la definición de grado (ejercicio). Por otra parte si $A[x]$ no fuera un dominio de integridad, entonces existirían P y $Q \in A[x] - \{0\}$ tales que $PQ = 0$ y esto contradice 2). ■

Si A es un dominio de integridad, por la proposición anterior tiene sentido considerar el cuerpo de fracciones que se denota con $A(x)$. Es decir

$$A(x) = \big\{P/Q \,/\, P, Q \in A[x],\ Q \neq 0\big\}.$$

Proposición 2.2: *Si K es un cuerpo, $K[x]$ es un dominio euclídeo. Más concretamente, si $P, Q \in K[x]$ con $Q \neq 0$ entonces existen dos polinomios C y R determinados únicamente tales que*

$$P = QC + R \qquad \textit{con} \quad \partial R < \partial Q.$$

El principal interés de los dominios euclídeos es que se puede definir el máximo común divisor y se tiene el "algoritmo de Euclides" para hallarlo. A pesar de que estos conceptos seguramente son ya conocidos por el lector, los recordamos aquí.

Definición: *Si $P, Q \in K[x]$ se dice que $D \in K[x]$ es un <u>máximo común divisor</u> de P y Q si $D|P$, $D|Q$ y cualquier otro divisor común de P y Q divide a D.*

<u>Nota</u>: Recuérdese que un dominio euclídeo es en particular un dominio de ideales principales (todo ideal se puede generar con un elemento), de modo que el máximo común divisor de P y Q también se puede definir como un generador del ideal (P, Q).

---

* Para una definición más formal véase el libro de A. Clark p.203.

Proposición 2.3 : *Dados dos polinomios en $K[x]$ no simultáneamente nulos, tienen un máximo común divisor y es único salvo unidades. Es decir, si D_1 y D_2 son dos máximos comunes divisores de P y Q entonces $D_1 = kD_2$ con $k \in K - \{0\}$.*

Proposición 2.4 : *Si $P, Q \in K[x] - \{0\}$ y D es su máximo común divisor, entonces existen $A, B \in K[x]$ tales que*

$$D = AP + BQ.$$

La demostración de estas dos últimas proposiciones se basa en el algoritmo de Euclides que consiste en hallar el máximo común divisor aplicando repetidamente el siguiente lema

Lema 2.5 : *Sean $P, Q \in K[x]$ y sean C y R como en la Proposición 2.2. Si D es un máximo común divisor de P y Q entonces también lo es de Q y R.*

DEM.: De $P = QC + R$ se deduce que $S \in K[x]$ es divisor común de P y Q si y sólo si lo es de Q y R. Como los divisores comunes coinciden, también coinciden los máximos comunes divisores. ■

DEM.(de la proposición 2.3):

Dados $P_1 = P$ y $P_2 = Q$ en $K[x]$ con $Q \neq 0$, definamos P_3 como el polinomio R en la Proposición 2.2. Ahora repetimos el proceso para definir P_4 a partir de P_2 y P_3 y así sucesivamente, es decir

$$P_1 = P_2C_1 + P_3, \quad P_2 = P_3C_2 + P_4, \quad P_3 = P_4C_3 + P_5, \quad \ldots$$

Como $\partial P_2 > \partial P_3 > \partial P_4 > \ldots$, el proceso anterior termina con cierto $P_n = 0$ y por tanto $P_{n-2} = P_{n-1}C_{n-2}$. La aplicación repetida del Lemma 2.5 implica que un máximo común divisor de P y Q es también un máximo común divisor de P_{n-1} y 0, y obviamente éste debe ser P_{n-1} o kP_{n-1}. ■

DEM.(de la proposición 2.4):

Como ya indicamos en la demostración de la Proposición 2.3, aplicando el Lema 2.5 se tiene

$$P = QC_1 + P_3, \quad Q = P_3C_2 + P_4, \quad \ldots P_{n-3} = P_{n-2}C_{n-3} + D, \quad P_{n-2} = DC_{n-2} + D.$$

La penúltima igualdad permite escribir D en términos de P_{n-3} y P_{n-2}, concretamente $D = P_{n-3} - P_{n-2}C_{n-3}$; la antepenúltima igualdad permite escribir D en términos de P_{n-4} y P_{n-3}, $D = (1 + C_{n-3}C_{n-4})P_{n-3} - C_{n-3}P_{n-4}$, y así sucesivamente. Iterando este proceso se obtiene finalmente la igualdad que asegura la proposición. ■

Ejemplo . Calcular el máximo común divisor de $P = x^4 + x^3 - 5x^2 + 4x + 3$ y $Q = x^3 - 6x + 9$, y expresarlo de la manera indicada en la Proposición 2.4.

Procedemos con el algoritmo de Euclides:

$$\begin{aligned}x^4+x^3-5x^2+4x+3 &= (x^3-6x+9)(x+1)+x^2+x-6\\ x^3-6x+9 &= (x^2+x-6)(x-1)+x+3\\ x^2+x-6 &= (x+3)(x-2).\end{aligned}$$

Por tanto el máximo común divisor es $x+3$, además

$$\begin{aligned}x+3 &= -(x-1)(x^2+x-6)+x^3-6x+9\\ &= -(x-1)\big(x^4+x^3-5x^2+4x+3-(x+1)(x^3-6x+9)\big)+x^3-6x+9,\end{aligned}$$

de donde $x+3=(1-x)P+x^2Q$.

Nótese que la demostración de la Proposición 2.4 se puede repetir paso por paso en otros dominios euclídeos. Así por ejemplo, en $\mathbb{Z}$, si d es el máximo común divisor de a y b, entonces la ecuación $d=ax+by$ tiene solución con $x,y\in\mathbb{Z}$ (de hecho tiene infinitas).

La demostración de la Proposición 2.4 puede usarse como algoritmo para calcular el inverso en algunos cuerpos definidos como cocientes de anillos por ideales. Para mayor claridad veamos primero un ejemplo en $\mathbb{Z}$.

Ejemplo 1. Hallar el inverso de $\overline{8}$ en $\mathbb{Z}/29\mathbb{Z}$.

Como el máximo común divisor de 29 y 8 es 1, según el análogo de la Proposición 2.4 en $\mathbb{Z}$ se tiene que $1=29n+8m$ se cumple para ciertos $n,m\in\mathbb{Z}$, por tanto $\overline{1}=\overline{8}\cdot\overline{m}$ y $\overline{m}$ es la clase que buscamos. Para calcular m y n se puede proceder usando el algoritmo de Euclides como en la demostración de la Proposición 2.4. Concretamente

$$\begin{aligned}29&=8\cdot 3+5\\ 8&=5\cdot 1+3\\ 5&=3\cdot 1+2\\ 3&=2\cdot 1+1\\ 1&=1\cdot 2+0\end{aligned}\quad\Rightarrow\quad\begin{aligned}&(4^{\text{a}}\text{ ecuación})\ 1=3-2\cdot 1\\ &(3^{\text{a}}\text{ ecuación})\ 1=3-(5-3\cdot 1)\cdot 1=5\cdot(-1)+3\cdot 2\\ &(2^{\text{a}}\text{ ecuación})\ 1=5\cdot(-1)+(8-5\cdot 1)\cdot 2=8\cdot 2+5\cdot(-3)\\ &(1^{\text{a}}\text{ ecuación})\ 1=8\cdot 2-(29-8\cdot 3)\cdot 3=29\cdot(-3)+8\cdot 11.\end{aligned}$$

Así pues podemos tomar $n=-3$ y $m=11$ y se concluye que $\overline{11}$ es el inverso de $\overline{8}$.

Veamos ahora un ejemplo con polinomios. Obsérvese que los razonamientos son análogos a los del ejemplo anterior.

Ejemplo 2. Sean $P=x^4+x^3+x^2+x+x+1$ y $Q=x^2+x+x+1$. Calcular el inverso de $\overline{Q}$ en $\mathbb{Q}[x]/(P)$.

Como comprobaremos inmediatamente con el algoritmo de Euclides, el máximo común divisor de P y Q es 1, así pues $1 = AP + BQ$ para ciertos $A, B \in \mathbb{Q}[x]$ y por tanto $\overline{1} = \overline{BQ}$, con lo cual $\overline{B}$ es el inverso de $\overline{Q}$. Calculemos A y B procediendo como en el ejemplo anterior:

$$\begin{aligned} P &= Q \cdot x^2 + (x+1) \\ Q &= (x+1)\cdot x + 1 \\ x+1 &= 1\cdot(x+1) + 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} &(2^{\underline{a}}\text{ ecuación})\ 1 = Q - x(x+1) \\ &(1^{\underline{a}}\text{ ecuación})\ 1 = Q - x(P - x^2Q) = -xP + (x^3+1)Q. \end{aligned}$$

Por tanto el inverso de $\overline{Q}$ es $\overline{x^3+1}$.

Otra propiedad interesante de los dominios euclídeos es que son de factorización única, es decir, al igual que en $\mathbb{Z}$ todo número se puede descomponer en factores primos, también se cumple

Proposición 2.6 : *Todo polinomio de $K[x]$ se puede descomponer como producto de polinomios ireducibles, además esta descomposición es única salvo el orden de los factores y multiplicación por elementos de $K - \{0\}$.*

<u>Nota</u>: Recuérdese que un polinomio, P, es <u>irreducible</u> si no puede escribirse como $P = QR$ con $\partial Q, \partial R < \partial P$.

<u>Ejemplo</u> . El polinomio $P = x^2 - 6x + 7$ es irreducible en $\mathbb{Q}[x]$ porque no se puede escribir como $a(x-\alpha_1)(x-\alpha_2)$ con $\alpha_1, \alpha_2 \in \mathbb{Q}$; sin embargo P no es irreducible en $\mathbb{Q}(\sqrt{2})[x]$ porque $P = (x - 3 + \sqrt{2})(x - 3 - \sqrt{2})$

En $\mathbb{C}[x]$ la cuestión de irreducibilidad de un polinomio es muy sencilla gracias al siguiente resultado

Teorema 2.7 (Teorema Fundamental del Álgebra): *$P \in \mathbb{C}[x]$ es irreducible $\Leftrightarrow$ $\partial P \le 1$. Equivalentemente, todo polinomio no constante de $\mathbb{C}[x]$ se puede descomponer en factores lineales.*

Si $K \neq \mathbb{C}$, en general es muy difícil saber si $P \in K[x]$ es irreducible. Un criterio que es de utilidad en algunos casos es el siguiente.

Proposición 2.8 (Criterio de Eisenstein): *Si $P = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ es un polinomio con coeficientes enteros y p es un primo tal que $p \nmid a_n$, $p | a_i$ si $0 \le i < n$ y $p^2 \nmid a_0$ entonces P es irreducible en $\mathbb{Q}[x]$.*

<u>Dem.</u>: Por el Lema de Gauss (véase más abajo), si P no es irreducible se puede escribir como $P = (b_lx^l + b_{l-1}x^{l-1} + \ldots + b_0)(c_mx^m + c_{m-1}x^{m-1} + \ldots + c_0)$ con $l + m = n$ y $b_i, c_i \in \mathbb{Z}$. Igualando los coeficientes de los términos del mismo grado, se tiene

$$a_0 = b_0c_0, \qquad a_1 = b_1c_0 + b_0c_1, \qquad a_2 = b_2c_0 + b_1c_1 + b_0c_2, \qquad \ldots$$

Por hipótesis $p|a_0$ pero $p^2\not| a_0$, así pues p divide a b_0 o a c_0 pero no a ambos simultáneamente. Supongamos por ejemplo que p divide a b_0, entonces por la segunda igualdad, $p|b_1$ y por la tercera $p|b_2$ y en general $p|b_i$ $0 \le i \le l$, lo que implica que p divide a todos los a_i lo que contradice nuestra hipótesis $p\not| a_n$. ■

Damos también otro criterio de irreducibilidad que es muy simple pero efectivo (la demostración se deja como ejercicio).

Proposición 2.9 : *Sea $P \in \mathbb{Z}[x]$ mónico y sea $\overline{P} \in \mathbb{F}_p[x]$ el polinomio que resulta al reducir los coeficientes módulo p. Si $\partial P = \partial \overline{P}$ y $\overline{P}$ es irreducible en $\mathbb{F}_p[x]$ entonces P es irreducible en $\mathbb{Q}[x]$.*

<u>OBSERVACIÓN</u>: El recíproco, en general, no se cumple. Por ejemplo, $P = x^2 + x + 1$ es irreducible en $\mathbb{Q}[x]$ pero no lo es en $\mathbb{F}_3$.

<u>Ejemplo 1</u>. El polinomio $x^3 - 17x^2 + 105$ es irreducible en $\mathbb{Q}[x]$, porque al tomar módulo 2 obtenemos $x^3 + x^2 + 1$ y si este polinomio se pudiera descomponer en $\mathbb{F}_2$ se podría escribir como $(x^2+ax+b)(x-c)$ pero esto es imposible porque ni x ni $x-1$ dividen a $x^3 + x^2 + 1$.

<u>Ejemplo 2</u>. (Polinomio Ciclotómico) Gauss demostró que si p es primo el polinomio (ciclotómico) $P = x^{p-1} + x^{p-2} + \ldots + x + 1$ es irreducible en $\mathbb{Q}[x]$. A pesar de que no es posible aplicar directamente el criterio anterior, si P es irreducible $Q = (x+1)^{p-1} + (x+1)^{p-2} + \ldots + (x+1) + 1$ también lo es (ejercicio) y como

$$Q = \frac{(x+1)^p - 1}{x+1-1} = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \ldots + \binom{p}{p-2} x + \binom{p}{p-1},$$

el criterio de Eisenstein es aplicable sobre Q (ejercicio).

<u>Ejemplo 3</u>. Como consecuencia del ejemplo anterior deducimos que $\mathbb{Q}[x]/(P)$, donde $P = x^{p-1} + x^{p-2} + \ldots + x + 1$, es un cuerpo. Para ello basta comprobar que todo elemento no nulo tiene inverso multiplicativo. Si $Q \notin (P)$, como P es irreducible en $\mathbb{Q}[x]$, el máximo común divisor de P y Q es 1 y existen $A, B \in \mathbb{Q}[x]$ tales que $1 = AP + BQ$. Así pues, $\overline{B}$ es el inverso de $\overline{Q}$ y existe siempre que que $\overline{Q} \ne \overline{0}$. En general, si P es irreducible en $K[x]$, $K[x]/(P)$ es un cuerpo.

Hay cierta falta de simetría en los criterio anteriores, porque partimos de un polinomio en $\mathbb{Z}[x]$ y concluimos que es irreducible en $\mathbb{Q}[x]$. Gauss demostró que en ambos anillos el concepto de irreducibilidad es el mismo.

Lema 2.10 (de Gauss): *Si $P \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}[x]$ también lo es en $\mathbb{Q}[x]$.*

<u>DEM.</u>: Si $P = P_1P_2$ con $P_1, P_2 \in \mathbb{Q}[x]$ multiplicando por cierto número natural, n,

que cancele todos los denominadores tenemos que

(2.1) $nP = (b_l x^l + b_{l-1}x^{l-1} + \ldots + b_0)(c_m x^m + c_{m-1}x^{m-1} + \ldots + c_0)$ con $b_i, c_i \in \mathbb{Z}$.

Supongamos que n es el menor número tal que nP se descompone en $\mathbb{Z}[x]$. si $n = 1$ el lema está probado. Supongamos que $n > 1$, sea p un divisor primo de n, entonces no todos los b_i ni todos los c_i pueden ser divisibles por p (ya que en ese caso podríamos simplificar por p en (2.1) reduciendo n a n/p). Sean b_i y c_j tales que $p\not| b_i$, $p\not| c_j$ pero $p|b_r$, $p|c_s$ si $r < i$, $s < j$ (podría ocurrir que $i, j = 0$), entonces igualando en (2.1) los coeficientes de grado $i + j$ se tiene

$$na_{i+j} = b_{i+j}c_0 + b_{i+j-1}c_1 + \ldots + b_i c_j + \ldots + b_0 c_{i+j}$$

y de aquí se deduce que $p|b_i c_j$ en contra de nuestra hipótesis $p\not| b_i$, $p\not| c_j$. ■

Un polinomio de $A[x]$ se puede considerar también como una función $A \to A$ sin más que sustituir la variable indeterminada por elementos del anillo.

Definición: *Se dice que $\alpha \in A$ es un cero o una raíz de $P \in A[x]$ si $P(\alpha) = 0$.*

Proposición 2.11 (Regla de Ruffini): *α es un cero de un polinomio de $K[x]$ si y sólo si $x - \alpha$ divide a ese polinomio.*

Definición: *Sea α un cero de $P \in K[x]$. Se dice que α tiene multiplicidad n si $(x - \alpha)^n | P$ y $(x - \alpha)^{n+1} \not| P$.*

Nota: A un cero de multiplicidad uno se le suele llamar cero simple.

Corolario 2.12: *El número de raíces de $P \in K[x]$ contadas con su multiplicidad es menor o igual que ∂P.*

Definición: *Se dice que un polinomio de $K[x]$ es mónico si su coeficiente de mayor grado es 1.*

Supongamos que un polinomio mónico P tiene ∂P raíces, entonces por la Regla de Ruffini se descompone en factores lineales

$$P = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

y operando en el segundo miembro e igualando coeficientes, se tiene que los coeficientes se pueden expresar en términos de las raíces con la fórmula $a_{n-k} = (-1)^k \sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ donde σ_k es un polinomio en $\alpha_1, \alpha_2, \ldots, \alpha_n$ igual a la suma de todos los posibles productos de k de estas variables. Por ejemplo

$$\sigma_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n, \quad \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n, \quad \ldots \quad \sigma_n = \alpha_1\alpha_2\ldots\alpha_n$$

Notación: A $\sigma_k(x_1, x_2, \ldots, x_n)$ se le suele llamar polinomio simétrico elemental de grado k y n variables.

En general se dice que un polinomio en varias variables es simétrico si queda invariante bajo cualquier permutación de sus variables.

El siguiente resultado justifica por qué a los σ_k se les llama elementales

Teorema 2.13 : *Cualquier polinomio simétrico sobre un dominio de integridad se puede expresar como un polinomio sobre dicho dominio cuyas variables son los polinomios simétricos elementales.*

<u>NOTA</u>: Aunque no lo haremos aquí, es posible probar la unicidad de esta expresión.

<u>DEM.</u>: Sea $P \in \mathcal{D}[x_1, x_2, \dots, x_n]$ simétrico. Apliquemos el siguiente algoritmo:

1) Seleccionar el monomio $kx_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ (algunos α_i pueden ser nulos) que tiene mayor grado en x_1, si todavía hubiera varios escójase entre ellos el de mayor grado en x_2 y si hubiera varios el de mayor grado en x_3, etc. Por la simetría de P se tiene $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$ (ejercicio).

2) Sea $Q = P - k\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\dots\sigma_n^{\alpha_n}$. Entonces $P = k\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\dots\sigma_n^{\alpha_n} + Q$ y ahora se repite todo el proceso con Q hasta llegar a $Q = 0$.

Obsérvese que el monomio selecionado en 1) no aparece en Q y que el algoritmo siempre termina porque al aplicarlo sucesivas veces o bien el grado en x_1 se ha reducido o ha quedado igual, y en este último caso el grado en x_2 se habrá reducido o habrá quedado igual, etc. (Ejercicio: dar una demostración detallada de esto). ■

<u>Ejemplo</u> Escribir el polinomio $P \in \mathbb{Q}[x_1, x_2, x_3]$ dado por

$$P = x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 + 2x_1 + 2x_2 + 2x_3$$

en términos de los polinomios simétricos elementales.

Según el proceso descrito en 1) debemos escoger el monomio $x_1^2x_2$, por tanto $\alpha_1 = 2$, $\alpha_2 = 1$, $\alpha_3 = 0$ y se tiene

$$P = \sigma_1\sigma_2 + Q \qquad \text{con} \qquad Q = -3x_1x_2x_3 + 2x_1 + 2x_2 + 2x_3. \tag{2.2}$$

(Recuérdese que $\sigma_1 = x_1 + x_2 + x_3$ y $\sigma_3 = x_1x_2x_3$).

Ahora repetimos el proceso con Q escogiendo el monomio $-3x_1x_2x_3$ lo que implica $\alpha_1 = \alpha_2 = \alpha_3 = 1$ y por tanto

$$Q = -3\sigma_3 + \widetilde{Q} \qquad \text{con} \qquad \widetilde{Q} = 2x_1 + 2x_2 + 2x_3. \tag{2.3}$$

Obsérvese que $\widetilde{Q} = 2\sigma_1$, así pues de (2.2) y (2.3) obtenemos finalmente

$$P = \sigma_1\sigma_2 - 3\sigma_3 + 2\sigma_1.$$

El teorema anterior tiene gran importancia histórica en el desarrollo de la teoría de Galois y la teoría de grupos en general. Para ilustrar su interés demostraremos el siguiente resultado

Corolario 2.14: *Si $P \in \mathbb{Q}[x]$ es un polinomio mónico que se descompone en $\mathbb{C}[x]$ como*

$$P = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n),$$

entonces para cualquier $Q \in \mathbb{Q}[x]$ el polinomio

$$P_Q = (x - Q(\alpha_1))(x - Q(\alpha_2)) \dots (x - Q(\alpha_n))$$

pertenece a $\mathbb{Q}[x]$.

<u>DEM.</u>: Los coeficientes de P_Q son $a_{n-k} = (-1)^k \sigma_k\big(Q(\alpha_1), Q(\alpha_2), \dots, Q(\alpha_n)\big)$, lo que considerando los α_i como variables define un polinomio simétrico de $\mathbb{Q}[\alpha_1, \alpha_2, \dots, \alpha_n]$. Por el teorema anterior, a_{n-k} se puede escribir como un polinomio con coeficientes racionales evaluados en $\sigma_1(\alpha_1, \alpha_2, \dots, \alpha_n)$, $\sigma_2(\alpha_1, \alpha_2, \dots, \alpha_n)$,...etc, y estas últimas cantidades son racionales porque coinciden, salvo un signo, con los coeficientes de P.

<u>Ejemplo</u>. Las raíces de $P = x^3 - 2$ son $\sqrt[3]{2}$, $\sqrt[3]{2}\,(-1 + i\sqrt{3})/2$ y $\sqrt[3]{2}\,(-1 - i\sqrt{3})/2$. Tomando $Q = x^2 + x$ se tiene que

$$\begin{aligned}\big(x - \sqrt[3]{4} - \sqrt[3]{2}\big)\big((x - \sqrt[3]{4}\,(-1 - i\sqrt{3})/2 - \sqrt[3]{2}\,(-1 + i\sqrt{3})/2\big)\cdot \\ \cdot\big(x - \sqrt[3]{4}\,(-1 + i\sqrt{3})/2 - \sqrt[3]{2}\,(-1 - i\sqrt{3})/2\big)\end{aligned}$$

es un polinomio de $\mathbb{Q}[x]$. En particular se deduce que $\sqrt[3]{4} + \sqrt[3]{2}$ es raíz de un polinomio con coeficientes racionales.

§3. EXTENSIONES DE CUERPOS.

Una de las ideas básicas que aparece en el trabajo de Gauss en ciclotomía es que resolver una ecuación algebraica requiere a veces pasar por las soluciones de otras ecuaciones auxiliares, y una vez que hemos "extendido" suficientemente el número de cantidades conocidas podremos factorizar la ecuación original. Más adelante, Galois demostraría que la naturaleza de estas extensiones queda fielmente reflejada en la estructura de cierto grupo.

DEFINICIÓN: *Decimos que el cuerpo L es una <u>extensión</u> de K, si K es un subcuerpo de L, es decir, $K \subset L$ y las operaciones $+$ y $\times$ en K coinciden con las de L.*

La notación que se usa habitualmente para designar una extensión es L/K o también se usa $L : K$.

Aunque la definición anterior es satisfactoria en casi todos los casos que aparecerán en el curso conviene al menos mencionar otra definición un poco más general y más conveniente desde el punto de vista abstracto.

DEFINICIÓN: *(generalizada) Decimos que el cuerpo L es una <u>extensión</u> de K, si existe un monomorfismo $f : K \longrightarrow L$.*

<u>OBSERVACIÓN</u>: Un monomorfismo es una función inyectiva que preserva las operaciones del cuerpo. Esto podría dar la idea de que ambas definiciones son idénticas, pero no es exactamente así. Por ejemplo, es obvio que $\mathbb{C}$ es una extensión de $\mathbb{R}$ con la primera y la

segunda definición, pero si escribimos los elementos de $\mathbb{R}$ usando un sistema de numeración que utilice letras en vez de números y llamamos $\mathbb{R}'$ al conjunto formado por esas nuevas sucesiones de símbolos, en rigor no podemos afirmar que $\mathbb{R}' \subset \mathbb{C}$ porque $\mathbb{C}$ es un conjunto de números y $\mathbb{R}'$ lo es de letras. El lector podría argüir que $\mathbb{R}$ y $\mathbb{R}'$ son esencialmente lo mismo (isomorfos), y que $\mathbb{R}'$ está incluido en $\mathbb{C}$ en el sentido de que existe una función inyectiva de $\mathbb{R}'$ en $\mathbb{C}$; con lo cual estaría usndo la segunda definición. Aunque estas distinciones no tendrán relevancia en general, aparecerán de forma natural al estudiar cuerpos de descomposición.

Si tanto L como K pertenecen a un cuerpo mayor, muchas veces lo más cómodo para definir L es decir qué cantidades nuevas añadimos a K, esto motiva la definición siguiente.

DEFINICIÓN: *Sea M/K y C un subconjunto de M, se llama* <u>subcuerpo generado por C</u>*, y se escribe $K(C)$, al menor subcuerpo de M que contiene a $K \cup C$.*

<u>Ejemplo 1</u>. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,/\, a, b \in \mathbb{Q}\}$.

<u>Ejemplo 2</u>. $\mathbb{R}(i) = \mathbb{C}$.

<u>Ejemplo 3</u>. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \,/\, a, b, c, d \in \mathbb{Q}\}$. De hecho, en breve veremos que ambos conjuntos son iguales.

Destacamos varios tipos de extensiones de cuerpos:

DEFINICIÓN: *Se dice que una extensión, L/K, es*

1) <u>simple</u>*, si $L = K(\alpha)$ con $\alpha \in L$.*

2) <u>algebraica</u>*, si todo $\alpha \in L$ es* <u>algebraico</u> *sobre K, es decir, existe un polinomio $P \in K[x]$ tal que $P(\alpha) = 0$.*

3) <u>trascendente</u>*, si no es algebraica.*

<u>Ejemplo 1</u>. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ y $\mathbb{Q}(x)/\mathbb{Q}(x^2)$ son simples y algebraicas.

Nótese en el segundo caso que $\mathbb{Q}(x) = \mathbb{Q}(x^2, x) = \big(\mathbb{Q}(x^2)\big)(x)$.

<u>Ejemplo 2</u>. $\mathbb{Q}(x)/\mathbb{Q}$ y $\mathbb{R}(x, y)/\mathbb{R}(x)$ son simples y trascendentes.

<u>Ejemplo 3</u>. (Lindemann 1882) $\mathbb{Q}(\pi)/\mathbb{Q}$ es trascendente. En el próximo capítulo veremos una demostración de este hecho.

<u>OBSERVACIÓN</u>: Una extensión puede ser simple aunque aparentemente esté generada por un conjunto de varios elementos. Así por ejemplo, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es simple porque como veremos en un próximo ejemplo, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

El siguiente teorema es casi trivial, pero ocupa un papel destacado en la teoría.

Teorema 3.1 : *Si L/K es una extensión de K, entonces L es un espacio vectorial sobre K.*

Este resultado no sería tan importante si no tuvieramos maneras de calcular dimensiones y bases. De ello tratan las proposiciones siguientes, pero antes de enunciarlas es conveniente introducir algunas definiciones.

DEFINICIÓN: *A la dimensión de L como espacio vectorial sobre K se le llama* grado *de L/K y se escribe $[L:K]$. Si el grado es finito se dice que la extensión es* finita*, en caso contrario se dice que es* infinita.

DEFINICIÓN: *Si α es algebraico sobre K, se dice que $P \in K[x]$ es el* polinomio mínimo *de α si P es mónico, α es un cero de P y no hay otro polinomio de grado menor con estas características.*

No es difícil demostrar que el polinomio mínimo, P, de α está únicamente determinado, y además cumple (ejercicio)

$$1)\ P \text{ es irreducible} \qquad 2)\ Q \in K[x],\ Q(\alpha) = 0 \ \Rightarrow\ P|Q.$$

Ejemplo . El polinomio mínimo de $\sqrt[4]{3}$ sobre $\mathbb{Q}$ es $x^4 - 3$ y sobre $\mathbb{Q}(\sqrt{3})$ es $x^2 - \sqrt{3}$.

Proposición 3.2 : *Si $K \subset L \subset M$ entonces*

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

De hecho, si L/K y M/L son finitas y $\{x_1, x_2, \ldots, x_r\}$, $\{y_1, y_2, \ldots, y_s\}$ son sus bases, entonces $\{x_1y_1, x_1y_2, \ldots, x_ry_s\}$ es una base de M/K.

Proposición 3.3 : *Toda extensión finita es algebraica.*

Proposición 3.4 : *$K(\alpha)/K$ es finita si y sólo si α es algebraico sobre K. Además en ese caso $[K(\alpha):K] = n$ donde n es el grado del polinomio mínimo de α, de hecho*

$$K(\alpha) = \{\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \ldots + \lambda_{n-1}\alpha^{n-1} \ \text{ con } \lambda_i \in K\}.$$

Antes de dar la demostración de estas proposiciones veamos algunas consecuencias. En primer lugar deduciremos el teorema que anunciamos en la primera sección:

Teorema 3.5 : *Si $K \subset \mathbb{C}$, los números algebraicos sobre K forman un cuerpo.*

NOTA: La hipótesis $K \subset \mathbb{C}$ no es realmente necesaria. Lo único importante es que K se pueda incluir dentro de un cuerpo en el que todo polinomio factoriza y esto es siempre posible aunque la demostración se sale fuera del contenido de este curso.

DEM.: Tenemos que demostrar que si α y $\beta \neq 0$ son algebraicos, $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ y α/β también lo son. Por la Proposición 3.3 basta demostrar que $K(\alpha, \beta)/K$ es finita. Pero por la Propoposición 3.2

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

y los dos términos del segundo miembro son finitos por la Proposición 3.4 ■

Ejemplo 1. La Proposición 3.4 asegura que $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$ y además

$$\mathbb{Q}(\sqrt[4]{3}) = \{a + b\sqrt[4]{3} + c\sqrt[4]{9} + d\sqrt[4]{27} \,/\, a, b, c, d \in \mathbb{Q}\}.$$

Nótese que no es en absoluto trivial probar que el segundo miembro es un cuerpo sin usar esta igualdad. El mismo resultado se podría haber deducido de la Proposición 3.2 considerando las extensiones $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.

Ejemplo 2. El propósito de este ejemplo es comparar los cuerpos $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}$. En este y en otros casos es conveniente representar las extensiones con un diagrama como el que aquí se adjunta. Las letras cursivas indican los correspondientes grados.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[d, dash, "a"] \arrow[ddl, dash, "e"'] \arrow[ddr, dash, "c"] & \\
 & \mathbb{Q}(\sqrt{2}+\sqrt{3}) \arrow[dd, dash, "b"] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "f"'] & & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash, "d"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Los polinomios mínimos sobre $\mathbb{Q}$ de $\sqrt{2}$ y $\sqrt{3}$ son $x^2 - 2$ y $x^2 - 3$ respectivamente. $x^2 - 2$ es también el polinomio mínimo de $\sqrt{2}$ en la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{3})$, ya que si factorizase en $\mathbb{Q}(\sqrt{3})$ se tendría $\sqrt{2} = r + s\sqrt{3}$ con $r, s \in \mathbb{Q}$ y esto no es posible (basta elevar al cuadrado). Estas consideraciones permiten concluir que $d = f = e = 2$. La Proposición 3.2 asegura $ab = cd = ef = 4$, por tanto $c = 2$ y las únicas posibilidades para a y b son $b = 4/a$ con $a = 1, 2, 4$. Nótese que $a = 4$ es imposible porque $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$ (de nuevo basta elevar al cuadrado).

Veamos que $a = 1$ y $b = 4$, para ello considérense los polinomios $\big(x - (\sqrt{2}+\sqrt{3})\big)^2 - 3$ y $x^2 - 2$. Ambos están en $\mathbb{Q}(\sqrt{2}+\sqrt{3})[x]$ y ambos son distintos y tienen a $x = \sqrt{2}$ como raíz, por tanto su máximo común divisor en $\mathbb{Q}(\sqrt{2}+\sqrt{3})[x]$ es $x - \sqrt{2}$, así que $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ y $\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Esto permite concluir $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \supset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y como $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ es trivial, se tiene que ambos cuerpos son iguales o equivalentemente, $a = 1$ y por tanto $b = 4$.

Ejemplo 3. Calcular el polinomio mínimo de $\sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$.

Por el ejemplo anterior $[\mathbb{Q}\big(\sqrt{2} + \sqrt{3}\big) : \mathbb{Q}] = 4$, así que el polinomio mínimo, P, debe tener grado 4. Digamos que es $P = x^4 + ax^3 + bx^2 + cx + d$, entonces

$$(\sqrt{2} + \sqrt{3})^4 + a(\sqrt{2} + \sqrt{3})^3 + b(\sqrt{2} + \sqrt{3})^2 + c(\sqrt{2} + \sqrt{3}) + d = 0.$$

Operando obtenemos una expresión de la forma $A + B\sqrt{2} + C\sqrt{3} + D\sqrt{6} = 0$. Como $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ son una base de $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big) = \mathbb{Q}\big(\sqrt{2} + \sqrt{3}\big)$ (ver Proposición 3.2), entonces los coeficientes A, B, C y D (que dependen de a, b, c y d) deben ser nulos. Esto nos lleva al sistema de ecuaciones

$$\begin{matrix} A = 49 + 5b + d = 0 & \qquad & C = 9a + c = 0 \\ B = 11a + c = 0 & \qquad & D = 20 + 2b = 0, \end{matrix}$$

cuya solución es $a = c = 0$, $b = -10$, $d = 1$; por tanto $P = x^4 - 10x^2 + 1$.

Otra manera más sencilla de proceder en este caso es considerar el polinomio $Q = (x - \sqrt{2})^2 - 3$. Obviamente $\sqrt{2} + \sqrt{3}$ es una raíz de Q, pero $Q = x^2 - 2\sqrt{2}\,x - 1 \notin \mathbb{Q}[x]$. Para eliminar los radicales podemos "multiplicar por el conjugado", así $P = (x^2 - 2\sqrt{2}\,x - 1)(x^2 + 2\sqrt{2}\,x - 1)$ es un polinomio en $\mathbb{Q}[x]$ que tiene a $\sqrt{2} + \sqrt{3}$ como raíz, además $\partial P = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$ implica que es el polinomio mínimo.

<u>Ejemplo 4</u>. Consideremos el polinomio $P = x^3 + 3x + 3 \in \mathbb{Q}[x]$, y sea α una de sus raíces. Como P es mónico e irreducible (por Eisenstein), es el polinomio mínimo de α y según la Proposición 3.4 todo elemento de $\mathbb{Q}(\alpha)$ es una combinación lineal racional de 1, α y α^2. El propósito de este ejemplo es escribir $1/(\alpha + 1)$ de esta forma, es decir, hallar $a, b, c, d \in \mathbb{Q}$ tales que

$$\frac{1}{\alpha + 1} = a + b\alpha + c\alpha^2.$$

Sea $Q = x + 1$, como P es irreducible el máximo común divisor de P y Q es 1 y por la Proposición 2.4 existen $A, B \in \mathbb{Q}[x]$ tales que

$$1 = AP + BQ.$$

En nuestro caso es fácil ver que puede tomarse $A = -1$ y $B = x^2 - x + 4$. Dividiendo por Q y sustituyendo α, se tiene finalmente

$$\frac{1}{\alpha + 1} = 4 - \alpha + \alpha^2.$$

<u>Ejemplo 5</u>. Calcular el grado del polinomio mínimo de $\sqrt[3]{7}$ en $\mathbb{Q}(\sqrt[5]{2})$.

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2}) & \\
\mathbb{Q}(\sqrt[3]{7}) \arrow[ur, dash, "b"] & & \mathbb{Q}(\sqrt[5]{2}) \arrow[ul, dash, "a"'] \\
& \mathbb{Q} \arrow[ul, dash, "3"] \arrow[ur, dash, "5"'] &
\end{tikzcd}$$

Por la Proposición 3.4, el problema se reduce a calcular $a = [\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2}) : \mathbb{Q}(\sqrt[5]{2})]$. Designemos por n el grado de $\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2})/\mathbb{Q}$, entonces por la Proposición 3.2 se cumple $n = 5a$ y $n = 3b$ donde b es, como indica el esquema, el grado de $\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2})/\mathbb{Q}(\sqrt[3]{7})$. Esto implica que 3 divide a a y 5 divide a b. Por otra parte, $P = x^3 - 7$ es un polinomio de $\mathbb{Q}(\sqrt[5]{2})[x]$ (y también de $\mathbb{Q}[x]$) tal que $\sqrt[3]{7}$ es uno de sus ceros, así pues el grado del polinomio mínimo es menor o igual que 3, es decir, $a \leq 3$. Como ya hemos probado que 3 divide a a, se tiene que $a = 3$. De hecho, este mismo argumento ha probado que $b = 5$ y que $n = 15$.

A continuación daremos la demostración de las tres proposiciones anteriores. Obsérvese que en todas ellas el punto crucial está en la estructura de espacio vectorial.

<u>Dem.(de la Proposición 3.2)</u>: Nos restringiremos al caso en que las extensiones son finitas (el otro queda como ejercicio). Toda la proposición se reduce a probar que $B = \{x_1y_1, x_1y_2, \dots, x_ry_s\}$ es una base de M/K.

1) *B es un sistema de generadores*: Si $z \in M$ entonces como M es un espacio vectorial sobre L con base $\{y_1, y_2, \dots, y_s\}$

$$z = \lambda_1 y_1 + \lambda_2 y_2 + \ldots + \lambda_s y_s \qquad \text{con } \lambda_i \in L. \tag{3.1}$$

Pero, de la misma forma, como $\lambda_i \in L$

$$\lambda_i = \mu_{i1} x_1 + \mu_{i2} x_2 + \ldots + \mu_{ir} x_r \qquad \text{con } \mu_{ir} \in K. \tag{3.2}$$

Sustituyendo (3.2) en (3.1) se obtiene que z es una combinación lineal de elementos de B con coeficientes en K.

2) *Los elementos de B son linealmente independientes*:. Supongamos que tenemos una combinación lineal nula

$$\sum_{i=1}^{r}\sum_{j=1}^{s} \lambda_{ij} x_i y_j = 0 \qquad \text{con } \lambda_{ij} \in K,$$

entonces podemos reescribirla como

$$\sum_{j=1}^{s}\Big(\sum_{i=1}^{r} \lambda_{ij} x_i\Big) y_j = 0.$$

Los términos entre paréntesis pertenecen a L y los y_j son una base de M/L, por tanto

$$\sum_{i=1}^{r} \lambda_{ij} x_i = 0 \qquad 1 \le j \le s.$$

Como los x_i son una base de L/K, se concluye finalmente $\lambda_{ij} = 0$. ■

<u>Dem.(de la Proposición 3.3)</u>: Sean L/K y $\alpha \in L$, entonces como L/K es finita hay alguna combinación lineal no trivial nula entre los elementos 1, α, α^2, α^3, $\ldots$; esto es, existen $\lambda_i \in K$ no todos nulos y $n \in \mathbb{N}$ tales que $\lambda_n\alpha^n + \lambda_{n-1}\alpha^{n-1} + \ldots + \lambda_1\alpha + \lambda_0 = 0$, por tanto α es algebraico. ■

<u>Dem.(de la Proposición 3.4)</u>: Considérese el conjunto

$$\mathcal{A} = \big\{\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \ldots + \lambda_{n-1}\alpha^{n-1} \;\text{ con } \lambda_i \in K\big\}.$$

Obviamente $\alpha \in \mathcal{A}$ y $\mathcal{A} \subset K(\alpha)$, si demostramos que $\mathcal{A}$ es un cuerpo se tiene $K(\alpha) = \mathcal{A}$ (porque $K(\alpha)$ es el menor cuerpo que contiene a α). Está claro que $\mathcal{A}$ es cerrado por sumas y restas, basta ver que también es cerrado por divisiones (la multiplicación se reduce a dos divisiones: $a \cdot b = a\big/1/b$). Si $a, b \in \mathcal{A}$ entonces $a/b = Q_1(\alpha)/Q_2(\alpha)$ donde Q_1 y $Q_2 \neq 0$ son polinomios de grado menor que n. Sea P el polinomio mínimo de α, como $\partial Q_2 < \partial P = n$, Q_2 y P son primos entre sí y por la Proposición 2.4 existen $A, B \in K[x]$ tales que

$$1 = AP + BQ_2.$$

Multiplicando por Q_1, dividiendo por Q_2 y susituyendo α, se tiene

$$\frac{Q_1(\alpha)}{Q_2(\alpha)} = Q_1(\alpha)B(\alpha), \tag{3.3}$$

y por la Proposición 2.2 $Q_1B = PC + R$ con $\partial R < \partial P = n$, lo que sustituyendo en (3.3) prueba el resultado.

Finalmente, para comprobar que $[K(\alpha) : K] = n$, basta ver que no existe ninguna combinación lineal no trivial nula. Si $\mu_0 + \mu_1\alpha + \ldots + \mu_k\alpha^k$ con $k < n$, entonces α sería raíz de un polinomio de grado menor que n, lo cual es una contradicción. ■

Quiza el lector esté un poco asombrado por el ejemplo 2 en el que demostramos que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es simple. Terminamos este capítulo mencionando un sorprendente teorema del que se deduce que éste no es un caso aislado, sino que casi todas las extensiones en las que uno piensa normalmente son simples.

Teorema 3.6 (del elemento primitivo): *Si K tiene característica cero y L/K es finita, entonces es simple.*

NOTA: En realidad se puede extender el teorema a cuerpos de característica positiva siempre que se cumpla cierta condición, que definiremos más adelante, llamada "separabilidad". Hay una versión más fuerte (y aparentemente muy distinta) de este teorema en el libro de Stewart, p.210.

1) Demostrar que $\mathbb{Z}/6\mathbb{Z}$ no es un cuerpo. Hallar las unidades.

2) Hallar el inverso multiplicativo de 5 en $\mathbb{Z}/21\mathbb{Z}$ usando el algoritmo de Euclides

3) Demostrar que

i) $\{n + m\sqrt{3} \,/\, n, m \in \mathbb{Z}\}$ es un anillo.

ii) $\{a + b\sqrt{3} \,/\, a, b \in \mathbb{Q}\}$ es un cuerpo.

iii) $\{a + b\sqrt[4]{3} \,/\, a, b \in \mathbb{Q}\}$ no es un anillo.

*iv) $\{a + b\sqrt[3]{3} + c\sqrt[3]{9} \,/\, a, b, c \in \mathbb{Q}\}$ es un cuerpo.

4) Hallar el máximo común divisor de $P = x^4 + 6x^3 + 13x^2 + 12x + 3$ y $Q = x^4 + 5x^3 + 9x^2 + 8x + 2$, y escribirlo en la forma $AP + BQ$.

5) Hallar el generador mónico del ideal $I = (x^3 + 1, x^2 + 1)$ en $\mathbb{F}_2[x]$.

6) Demostrar que si la característica de un cuerpo no es cero, entonces es un número primo.

7) Demostrar que $\mathbb{Q}[x]/(x^2 - 5x + 6)$ no es un dominio de integridad.

8) El polinomio $f = x^3 - 3x + 1$ es irreducible en $\mathbb{Q}[x]$. Sea $\beta = \overline{x^4 - 3x^2 + 2x + 3} \in \mathbb{Q}[x]/(f)$. Hallar β^{-1} y β^2 expresándolos como combinación lineal de $\{1, \overline{x}, \overline{x}^2\}$.

9) Demostrar que en $\mathbb{Z}$ y en $k[x]$ (k un cuerpo) hay infinitos irreducibles no asociados.

<u>Observación</u>: Sea k un cuerpo, todo polinomio de grado 1 es irreducible y un polinomio de grado 2 ó 3 es irreducible si y sólo si no tiene una raíz (un cero) en k. Se dice que k es algebraicamente cerrado cuando todo polinomio irreducible en $k[x]$ es de grado 1. (i.e. cuando todo polinomio de grado≥ 1 tiene una raíz).

10) Si k es un cuerpo finito no es algebraicamente cerrado.

11) Estudiar la irreducibilidad de $P = x^2 + 1$ en $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, $\mathbb{F}_7[x]$, $\mathbb{F}_{11}[x]$, $\mathbb{F}_{13}[x]$ y $\mathbb{F}_{17}[x]$. Intentar inducir (sin demostración) una regla general que permita decidir la irreducibilidad de P sin calcular sus raíces.

12) Hallar todos los polinomios irreducibles de grado≤ 4 en $\mathbb{F}_2[x]$. ¿Cuántos irreducibles hay de grado 2, 3 y 4?

13) Demostrar que $\mathbb{F}_2[x] \Big/ (x^2 + x + 1)$ es un cuerpo con cuatro elementos. Dar sus tablas de suma y producto. (Nótese que esto prueba que existen cuerpo finitos distintos de $\mathbb{F}_p$).

Hoja 2

1) Decir si son irreducibles en $\mathbb{Q}[x]$ los polinomios

$$3x^2 - 7x - 5, \qquad 6x^3 - 3x - 18; \qquad x^3 - 7x + 1.$$

2) Demostrar que $x^3 - x + 1$ es irreducible en $\mathbb{F}_3[x]$.

3) Demostrar que $x^5 - x^2 + 1$ es irreducible en $\mathbb{F}_2[x]$.

4) Los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$

$$x^5 - 3x + 3, \qquad x^{p-1} + x^{p-2} + \ldots + x + 1 \text{ (con } p \text{ primo)}, \qquad x^6 - 6x + 2$$

$$x^2 + 1, \qquad x^4 + 1, \qquad x^6 + x^3 + 1$$

5) Hallar en $\mathbb{Q}[x]$ el polinomio mónico de grado mínimo (polinomio mínimo) que tenga a $e^{i\theta}$, $\theta = 2\pi/7$, como raíz.

6) Demostrar que $x^m - p$ (p primo) es irreducible en $\mathbb{Q}[x]$.

7) Decidir si los siguientes polinomios son reducibles en $\mathbb{R}$, $\mathbb{Q}$ y $\mathbb{C}$.

$$i)\ x^4 + 3x + 6 \qquad ii)\ x^4 + 1$$

$$iii)\ x^3 + 11^{11}x + 13^{13} \qquad iv)\ x^4 - x^3 - x - 1$$

8) Demostrar que $x^5 - 9x^2 + 1$ es irreducible en $\mathbb{Q}[x]$ (*Sugerencia*: ver problema 3).

9) Sea $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ en $K[x]$ con $a_0, a_n \neq 0$. f es irreducible si y sólo si $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$ es irreducible.

10) Demostrar que $2x^4 + 4x^2 + 1$ es irreducible en $\mathbb{Q}[x]$.

11) Demostrar que un polinomio de la forma $f = x^n + px + p^2$ es irreducible en $\mathbb{Z}[x]$. *Indicación*: Pruébese primero que no admite una raíz en $\mathbb{Z}$, y que, por tanto, si f no es irreducible $f = gh$ con $grad\, g \geq 2$ $grad\, h \geq 2$. Demuéstrese finalmente que si $g = \sum g_ix^i$ y $h = \sum h_jx^j$, se tiene que $g_i \equiv 0\,(p)$ $\forall i < grad\, g$, $h_j \equiv 0\,(p)$ $\forall j < grad\, h$; de donde se deduce en particular que $p^2 | p = g_0h_1 + g_1h_0$ (absurdo).

12) Escribir $x_1^2 + x_2^2 + x_3^2$ y $x_1^3 + x_2^3 + x_3^3$ en términos de los polinomios simétricos elementales.

13) Sea $s_k = x_1^k + x_2^k + \ldots + x_n^k$ para $0 < k$ y $s_0 = k$. Demostrar las "identidades de Newton"

$$(-1)^{k+1}s_k = \sum_{i=0}^{k-1}(-1)^i s_i \sigma_{k-i} \qquad \text{para } 0 < k \leq n$$

$$(-1)^{k+1}s_k = \sum_{i=k-n}^{k-1}(-1)^i s_i \sigma_{k-i} \qquad \text{para } k > n$$

donde σ_i son los polinomios simétricos elementales. *Indicación:* Defínase $\sigma_i = 0$ para $i > n$ y aplíquese inducción para demostrar simultáneamente ambas identidades.

1) Hallar el grado de las siguientes extensiones y decir de qué tipo son:

$i)$ $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$	$ii)$ $\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}$
$iii)$ $\mathbb{R}(\sqrt{3})/\mathbb{R}$	$iv)$ $\mathbb{R}(\sqrt[4]{-3})/\mathbb{R}$
$v)$ $\mathbb{F}_7(t)/\mathbb{F}_7(t^2)$	$vi)$ $\mathbb{F}_7(t)/\mathbb{F}_7$
$vii)$ $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})/\mathbb{Q}$	$viii)$ $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})/\mathbb{Q}$

$ix)$ $A/\mathbb{Q}$ donde A son los números algebraicos sobre $\mathbb{Q}$.

2) Demostrar que una extensión de grado primo es simple.

3) Sea $K(\alpha, \beta)$ una extensión algebraica de K, $n_\alpha = [K(\alpha) : K]$, $n_\beta = [K(\beta) : K]$ y $n = [K(\alpha, \beta) : K]$

i) Demostrar que $\text{mcm}(n_\alpha, n_\beta) | n$ y $n \leq n_\alpha \cdot n_\beta$. ¿Qué se puede decir si n_α y n_β son coprimos?

ii) Mostrar un ejemplo con $n_\alpha \neq n_\beta$ en el que se cumpla $n < n_\alpha \cdot n_\beta$.

4) Hallar $[\mathbb{Q}(\sqrt[7]{2}, \sqrt[5]{3}) : \mathbb{Q}]$.

5) Sean α y β en L/K tales que $[K(\alpha) : K] = m$ y $[K(\beta) : K] = n$. Demostrar que el grado del polinomio mínimo de β en $K(\alpha)$ es n si y sólo si el grado del polinomio mínimo de α en $K(\beta)$ es m.

6) Calcular el polinomio mínimo de $\sqrt{3} + \sqrt{5}$ en $\mathbb{Q}(\sqrt{15})$.

7) Sea α una raíz de $P = x^3 - x - 2 \in \mathbb{Q}[x]$. Escribir $(\alpha + 1)/(\alpha - 1)$ como una combinación lineal de 1, α y α^2.

8) Si $K(\alpha)/K$ es una extensión de grado tres, calcular $[K(\alpha^2) : K]$. Suponiendo que el polinomio mínimo de α es $x^3 + x - 1$, hallar el polinomio mínimo de α^2.

9) Calcular el polinomio mínimo de $\sqrt[3]{9} + \sqrt[3]{3} - 1$

10) Calcular el grado del polinomio mínimo de $\cos(2\pi/p)$ sobre $\mathbb{Q}$ donde p es un primo. *Indicación*: Hállese primero el polinomio mínimo de $\zeta = e^{2\pi i/p}$.

11) Si n y m son enteros positivos y no son cuadrados perfectos, comparar los cuerpos $\mathbb{Q}(\sqrt{n}, \sqrt{m})$, $\mathbb{Q}(\sqrt{n} + \sqrt{m})$ y $\mathbb{Q}(\sqrt{nm})$.

12) Demostrar que $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7})/\mathbb{Q}$ es simple sin usar el teorema del elemento primitivo.

13) Hallar el grado de la extensión $\mathbb{Q}\left(\sqrt{1 + \sqrt{3}}\right)/\mathbb{Q}$.

2. Tres problemas clásicos

En este capítulo estudiaremos tres problemas que los antiguos geómetras griegos no supieron abordar. El principal interés de tratarlos aquí es comprobar la profundidad del lenguaje introducido en el capítulo anterior. Concretamente veremos que dos de estos problemas clásicos ("La duplicación del cubo" y "La trisección del ángulo") se vuelven muy sencillos tras algunas consideraciones acerca del grado de ciertas extensiones; mientras que un tercer problema ("La cuadratura del círculo") requiere una demostración complicada pero que, de nuevo, sólo tiene sentido dentro del marco de la teoría de cuerpos.

§1. Construcciones con regla y compás.

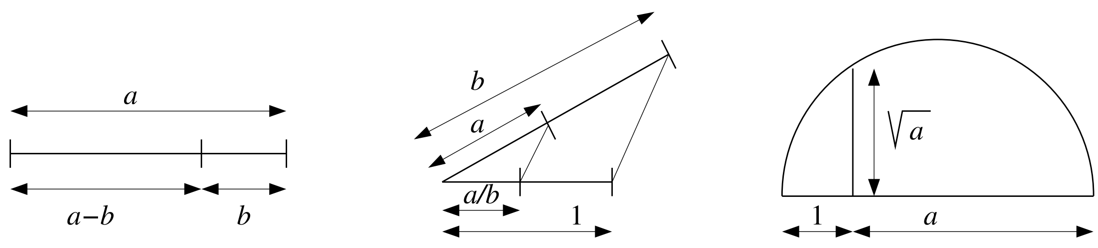
Los problemas que consideraremos tratan acerca de construcciones con regla y compás. La utilidad de estos instrumentos en las construcciones geométricas clásicas queda limitada de manera que la regla solo se puede usar para trazar una recta que pasa por dos puntos conocidos, y el compás sólo se puede usar para trazar una circunferencia de la que se conocen centro y radio.

Una vez fijada una unidad de medida, digamos determinada por $(0,0)$ y $(1,0)$, como las rectas tienen ecuaciones de primer grado y las circunferencias de segundo grado, todos los puntos que se pueden construir como intersecciones sucesivas de ellas tienen coordenadas que están en sucesivas extensiones cuadráticas. Por tanto, si $(x,y) \in \mathbb{R}^2$ es un punto construible con regla y compás entonces existe una cadena de cuerpos

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n = L \tag{1.1}$$

con $[L_{k+1} : L_k] = 2$ y $x, y \in L \subset \mathbb{R}$.

Con la ayuda de algunas construcciones geométricas sencillas conocidas desde la antigüedad es posible comprobar que la suma, resta, multiplicación, división y raíz cuadrada de longitudes construibles con regla y compás, también es construible con regla y compás. Todo lo necesario está contenido en los siguientes diagramas:



1. Construcción de $a-b$ 2. Construcción de a/b 3. Construcción de $\sqrt{a}$.

De todo esto se deduce que cualquier elemento de un cuerpo real, L, para el que exista una cadena de subcuerpos como (1.1) puede ser obtenido como coordenada de un punto construible con regla y compás, es decir, se tiene la siguiente caracterización que tomaremos como definición:

> *Un punto $(x, y) \in \mathbb{R}^2$ es* construible *con regla y compás si y sólo si x e y pertenecen a un cuerpo $L \subset \mathbb{R}$ tal que existe una cadena de subcuerpos*
>
> $$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n = L$$
>
> *donde todas las extensiones son de grado dos.*

También usaremos el término "longitud construible" para referirnos a aquellas longitudes que pueden aparecer como coordenadas de puntos construibles.

Un sencillo resultado que será crucial en el resto del capítulo es el siguiente

Lema 1.1 : *Si x es una longitud construible con regla y compás, entonces $[\mathbb{Q}(x) : \mathbb{Q}]$ es una potencia de dos.*

DEM.: Con la notación introducida anteriormente se tiene $x \in L$ y

$$[L : \mathbb{Q}] = \prod_{k=1}^{n} [L_k : L_{k-1}] = 2^n.$$

Además $x \in L \supset \mathbb{Q}$ implica que $[\mathbb{Q}(x) : \mathbb{Q}]$ divide a $[L : \mathbb{Q}]$ y esto prueba el resultado. ■

Es importante notar que el recíproco no es cierto en general. Es decir, que existen extensiones reales $\mathbb{Q}(x)/\mathbb{Q}$ tales que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^k$ con x no construible. No conocemos ningún contraejemplo sencillo, lo cual parece natural porque la constructibilidad de x involucra la estructura de los subcuerpos de $\mathbb{Q}(x)$, que puede ser muy complicada. De todas maneras, intentaremos ilustrar brevemente la situación:

Si α es el único cero real y positivo de $P = x^4 - 10x^3 + 26x^2 + 16x - 14$, se puede demostrar (usando teoría de Galois) que $\mathbb{Q}(\alpha)$ no tiene subcuerpos propios, es decir, que si $\mathbb{Q} \subset M \subset \mathbb{Q}(\alpha)$, entonces $M = \mathbb{Q}$ ó $M = \mathbb{Q}(\alpha)$. En particular, α no es construible. Por otra parte, como P es irreducible (por el criterio de Eisenstein), se tiene $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Como fenómeno curioso, obsérvese que en el contraejemplo anterior podemos expresar α en términos de radicales cuadráticos y cúbicos resolviendo la ecuación $P = 0$ (lo cual es bastante complicado) y la no constructibilidad de α implica que no es posible suprimir los radicales cúbicos a pesar de que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

§2. La duplicación del cubo y la trisección del ángulo.

Los dos problemas recogidos en el título se pueden formular de la manera siguiente:

P 1: *Dada la arista de un cubo, construir con regla y compás la arista de un cubo de volumen doble.*

P 2: *Dado un ángulo, hallar un método para trisecarlo con regla y compás.*

Eratóstenes transmitió dos leyendas acerca del primer problema. Según dijo, en cierta obra trágica un personaje legendario proponía duplicar la tumba de su hijo que era cúbica y tenía 100 pies de lado. También refiere como origen del problema que en Delos el oráculo ordenó duplicar el volumen del altar de Apolo (¿para acabar con cierta plaga?), lo cual interesó a algunos miembros de la Academia de Platón quienes encontraron soluciones valiéndose de curvas auxiliares (distintas de la recta y la circunferencia). También hallaron soluciones por procedimientos mecánicos que involucraban la regla y el compás pero usándolos de manera no convencional. (Estos tipos de soluciones también eran conocidos para trisecar el ángulo).

El segundo problema es bastante natural desde el punto de vista geométrico, ya que así como la bisección del ángulo (que es fácilmente realizable con regla y compás) permite construir el octógono regular y el hexágono regular a partir del cuadrado y del triángulo equilátero; la trisección del ángulo permitiría, por ejemplo, construir el eneágono (polígono de 9 lados) regular. Como veremos en capítulos posteriores, la constructibilidad con regla y compás de los polígonos regulares está estrechamente relacionada con la teoría de Galois.

Las proposiciones siguientes demuestran que ninguno de estos problemas tiene solución.

Proposición 2.1 : *Si la arista de un cubo es constructible con regla y compás, la del cubo de volumen doble no lo es.*

Dem.: Si pudiéramos construir un segmento de longitud a (la arista del cubo) y otro de longitud $a\sqrt[3]{2}$ (la arista del cubo de volumen doble) entonces también podríamos construir un segmento de longitud $\sqrt[3]{2}$, pero como el polinomio mínimo de $\sqrt[3]{2}$ es $x^2 - 2$, se tiene $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ y esto contradice el Lema 1.1. ■

Proposición 2.2 : *El ángulo de 60^0 no puede trisecarse con regla y compás.*

Observación: En particular se deduce que tampoco se puede trisecar el ángulo de 120^0 y por tanto el eneágono regular no es construible con regla y compás.

Dem.: Sea el ángulo de 60^0 grados $\widehat{POQ}$ formado por los puntos construibles $P = (1, 0)$, $O = (0, 0)$, $Q = (1/2, \sqrt{3}/2)$.

Trisecar $\widehat{POQ}$ equivale a construir $(\cos 20^0, \operatorname{sen} 20^0)$. Por la fórmula del ángulo triple o utilizando dos veces la fórmula para $\cos(\alpha + \beta)$, se tiene

$$\frac{1}{2} = \cos 60^0 = 4\cos^3 20^0 - 3\cos 20^0.$$

Así pues, $\cos 20^0$ es una raíz del polinomio $P = x^3 - 3x/4 - 1/8$. Aplicando el criterio de Eisenstein a $8P\big((x+1)/2\big)$ se deduce que P es irreducible, por tanto es el polinomio mínimo de $\cos 20^0$ y se tiene $[\mathbb{Q}(\cos 20^0) : \mathbb{Q}] = 3$, lo que contradice el Lema 1.1. ■

NOTA: Aunque la demostración de la imposibilidad de los dos problemas que nos ocupan se atribuye a P.-L. Wantzel en 1837 (al menos en el *Encylopedic Dictionary of Mathematics* de la *Mathematical Society of Japan*), es claro que los artículos finales en la obra de Gauss *Disquisitiones Arithmeticae* indican que él ya conocía en 1801 la imposibilidad de trisecar el ángulo (y posiblemente de duplicar el cubo). Por otra parte, también es claro que Abel (1802-1829) o Galois (1811-1832) podrían haber deducido ambas pruebas de imposibilidad a partir de los conceptos introducidos en sus trabajos.

§3. La cuadratura del círculo

El último problema del que nos ocuparemos se conoce con el nombre de "la cuadratura del círculo", y tiene el siguiente enunciado

P 3: *Dado un círculo, construir con regla y compás un cuadrado de igual área.*

Resolver este problema para el círculo unidad llevaría a construir un cuadrado de lado $\sqrt{\pi}$. Por el Lema 1.1, basta demostrar que $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ no es una potencia de dos para concluir que tampoco este problema tiene solución. Esto no es sencillo en absoluto y, de hecho, la cuadratura del círculo ha quedado como paradigma de dificultad e imposibilidad en el lenguaje usual.

En esta sección demostraremos que π es trascendente sobre $\mathbb{Q}$, es decir, no es raíz de ningún polinomio de $\mathbb{Q}[x]$ y por tanto $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$. La demostración de la trascendencia de π es bastante misteriosa y se sale un poco fuera del contenido del curso, no obstante es difícil resistir la tentación de incluirla después de la relevancia histórica del problema.

Antes de entrar en las demostraciones de trascendencia veamos el siguiente lema que es una consecuencia sencilla del teorema de los polinomios simétricos.

Lema 3.1 : *Sea $P = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 \in \mathbb{Z}[x]$ y sean $\alpha_1, \alpha_2, \ldots, \alpha_n$ sus raíces en $\mathbb{C}$. Si $S(x_1, x_2, \ldots, x_n)$ es un polinomio simétrico con coeficientes enteros de grado k (esto es $\partial S(x, x, \ldots, x) = k$), entonces $c_n^k S(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$.*

---

* Para el lector interesado damos algunas ideas que subyacen a la mayoría de las demostraciones de irracionalidad y trascendencia: Si $\alpha \in \mathbb{R}$ y encontramos una sucesión de enteros distintos, n_k, con $|\alpha - n_k| < \epsilon(k)$ y $\epsilon(k) \to 0$, entonces obviamente α no es un entero. Si la sucesión es de números racionales distintos, n_k/m_k y $|\alpha - n_k/m_k| < \epsilon(k)/m_k$ con $\epsilon(k) \to 0$, entonces α no es racional (basta multiplicar por m_k y el posible denominador de α). En general no es muy difícil demostrar que si $|\alpha - n_k/m_k| < \epsilon(k)/m_k^r$ con $\epsilon(k) \to 0$, entonces α no satisface una ecuación de grado r (véase ej. 3 Cap. 20, 1ª edición, "Calculus" de Spivak). Así que, en cierta manera, la trascendencia de un número α se "reduce" a encontrar buenas aproximaciones por racionales (o enteros, si quitamos denominadores). Antes de la llegada de las computadoras este tipo de aproximaciones para valores especiales de funciones como $\operatorname{sen} x$, $\cos x$, e^x, etc. tenían gran importancia para hacer cálculos.

<u>DEM.</u>: Factorizando P/c_n se tiene que

$$\sigma_j(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^j c_{n-j}/c_n.$$

Por otra parte, el teorema de los polinomios simétricos (Teorema 2.13 Cap.1) afirma que $S(\alpha_1, \alpha_2, \ldots, \alpha_n)$ se puede escribir como un polinomio (con coeficientes enteros) en los $\sigma_j(\alpha_1, \alpha_2, \ldots, \alpha_n)$, como el grado de este polinomio no excede k, multiplicando por c_n se cancelan todos los denominadores. ■

Las ideas principales para abordar la trascendencia de π, de e y de algunas cantidades relacionadas, están contenidas en la demostración del siguiente resultado

Teorema 3.2: *Si $P \in \mathbb{Z}[x]$ con $\partial P = n$ y sus raíces en $\mathbb{C}$, α_1, α_2,...,α_n, son no nulas, entonces $E_P = e^{\alpha_1} + e^{\alpha_2} + \ldots + e^{\alpha_n} \notin \mathbb{Z} - \{0\}$.*

<u>DEM.</u>: Definamos

$$\mathcal{P} = \sum_{r=1}^{n} e^{\alpha_r} \int_{\alpha_r}^{\infty} \frac{x^{p-1}e^{-x}}{(p-1)!} \big(P(x)\big)^p dx \qquad \text{y} \qquad \mathcal{Q} = \int_0^{\infty} \frac{x^{p-1}e^{-x}}{(p-1)!} \big(P(x)\big)^p dx$$

donde p es un número primo que se escogerá más adelante. Nótese que las integrales tienen sentido aunque los α_r sean complejos, de todas formas es siempre posible pasar a integrales reales con el cambio $x' = x - \alpha_r$.

Gracias a la fórmula

$$\int_0^{\infty} \frac{x^{p-1}e^{-x}}{(p-1)!} x^k dx = \frac{(p+k-1)!}{(p-1)!}$$

se deduce que $\mathcal{Q} \in \mathbb{Z}$ y tomando $p \nmid P(0)$ se tiene $p \nmid \mathcal{Q}$. Un argumento similar con $\mathcal{P}$, tras el cambio $x' = x - \alpha_r$, permite deducir que cada uno de sus sumandos es un polinomio en α_r con coeficientes enteros múltiplos de p (nótese que $P(x' + \alpha_r)$ no tiene término independiente). Así pues, $\mathcal{P}$ puede considerarse como un polinomio simétrico en $\alpha_1, \alpha_2, \ldots, \alpha_n$ multiplicado por p y el lema anterior asegura que $c_n^{np}\mathcal{P} \in \mathbb{Z}$ (donde c_n es el coeficiente de mayor grado de P), y además $p | c_n^{np}\mathcal{P}$.

La clave de la demostración (véase la anterior nota a pie de página) es que si p es grande el número racional $\mathcal{P}/\mathcal{Q}$ aproxima muy bien a E_P y ambas cantidades no son iguales, lo que llevará a una contradicción si E_P es entero.

Si $E_P \in \mathbb{Z} - \{0\}$, tomando $p > c_n E_P$ se tiene $p \nmid c_n^{np} E_P \mathcal{Q} - c_n^{np}\mathcal{P}$ y por tanto

$$1 \le |c_n|^{np} |E_P \mathcal{Q} - \mathcal{P}| = |c_n|^{np} \Big| \sum_{r=1}^{n} e^{\alpha_r} \int_0^{\alpha_r} \frac{x^{p-1}e^{-x}}{(p-1)!} \big(P(x)\big)^p dx \Big| < \frac{K_2 \cdot K_1^p}{(p-1)!}$$

donde, una vez fijado P, K_1 y K_2 son constantes. Nótese que tomando p suficientemente grande se llega a contradicción. ■

Pequeñas variaciones en la demostración permiten probar un resultado más general.

Teorema 3.3 : *Sean $P_1, P_2, \dots, P_m \in \mathbb{Z}[x]$ tales que $P = P_1 \cdot P_2 \cdot \dots \cdot P_m$ cumple $P(0) \neq 0$, entonces dados $k_1, k_2, \dots, k_m \in \mathbb{Z}$ no simultáneamente nulos, $k_1 E_{P_1} + k_2 E_{P_2} + \dots + k_m E_{P_m} \notin \mathbb{Z} - \{0\}$.*

<u>DEM.</u>: Basta proceder como en el teorema anterior pero tomando

$$\mathcal{P} = \sum_{i=1}^{m} \mathcal{P}_i \quad \text{con} \quad \mathcal{P}_i = k_i \sum_{r=1}^{n_i} e^{\alpha_{i,r}} \int_{\alpha_{i,r}}^{\infty} \frac{x^{p-1} e^{-x}}{(p-1)!} \big(P(x)\big)^p dx$$

donde $\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,n_i}$ son las raíces de P_i. ■

Corolario 3.4 (Hermite, 1873)**:** *e es trascendente sobre $\mathbb{Q}$.*

<u>DEM.</u>: Tómese $P_1 = x-1$, $P_2 = x-2$,..., $P_m = x-m$ en el teorema anterior. ■

Corolario 3.5 (Lindemann, 1882)**:** *π es trascendente sobre $\mathbb{Q}$.*

<u>DEM.</u>: Si π fuera algebraico, $i\pi$ también lo sería (donde $i = \sqrt{-1}$). En ese caso, sea $Q \in \mathbb{Z}[x]$ un polinomio con coeficiente de mayor grado c_n y cuyas raíces son $\alpha_1 = i\pi$, α_2, ..., α_n. La fórmula de Euler implica $e^{\alpha_1} = -1$ con lo cual

$$\prod_{k=1}^{n} \left(1 + e^{\alpha_k}\right) = 0.$$

Operando en esta igualdad se obtiene

$$1 + \sum_{j_1} e^{\alpha_{j_1}} + \sum_{j_1 < j_2} e^{\alpha_{j_1} + \alpha_{j_2}} + \sum_{j_1 < j_2 < j_3} e^{\alpha_{j_1} + \alpha_{j_2} + \alpha_{j_3}} + \dots = 0$$

Si consideramos $c_n^K \prod_k^K (x - e_k)$ donde e_k denota todos los exponentes no nulos que aparecen en al fórmula anterior, entonces $P \in \mathbb{Z}[x]$ (basta aplicar el Lema 3.1 a sus coeficientes). La igualdad anterior se podría escribir entonces como

$$1 + r + E_P = 0$$

donde r es el número de posibles exponentes nulos, y esto contradice el Teorema 3.3. ■

Decidir la trascendencia sobre $\mathbb{Q}$ de un número dado es, en general, muy difícil. Entre los resultados más espectaculares obtenidos desde la demostración de Hermite, se encuentran el teorema de Lindemann y el teorema de Gelfond-Schneider que afirman, respectivamente, que e^α y α^β son trascendentes sobre $\mathbb{Q}$ cuando $\alpha, \beta \neq 0, 1$ son algebraicos con β irracional. Sus demostraciones utilizan en gran medida las ideas originales de Hermite. De estos teoremas se deduce, por ejemplo, que $e^{\sqrt{3}}$, $2^{\sqrt{2}}$ y e^π son trascendentes (nótese que $e^\pi = i^{-2i}$). Por otra parte, la trascendencia de números tales como $e+\pi$, πe ó π^e, se desconoce.

1) Decir cuáles de las siguientes longitudes son construibles con regla y compás

$$\sqrt{\sqrt{2}+\sqrt{3}}, \qquad \sqrt[3]{7+5\sqrt{2}}, \qquad \sqrt{1+\sqrt{\sqrt{2}+\sqrt[3]{3}}}, \qquad e^{i\pi/8}+e^{-i\pi/8}.$$

2) Diseñar un método sencillo para construir con regla y compás la longitud

$$\frac{\sqrt{1+\sqrt{3}}}{\sqrt{2}}.$$

3) Demostrar que los polígonos regulares inscritos en el círculo unidad de 7, 11, 13 y 19 lados no son construibles con regla y compás. *Indicación*: Considérense las raíces del polinomio irreducible $x^{p-1}+x^{p-2}+\ldots+x+1=(x^p-1)/(x-1)$ con p primo.

4) ¿Es el pentágono regular construible con regla y compás? *Indicación:* Hallar $\cos(2\pi/5)+\cos(4\pi/5)$ y $\cos(2\pi/5)\cdot\cos(4\pi/5)$.

5) Decir si las siguientes extensiones son algebraicas o trascendentes.

$$\mathbb{Q}(\pi,\sqrt{3})/\mathbb{Q}(\sqrt{3}), \qquad \mathbb{Q}(\sqrt{\pi})/\mathbb{Q}(\pi), \qquad \mathbb{Q}(e)/\mathbb{Q}(e^5-e^3+7e^2+100e-1).$$

6) Demostrar que si α y β son trascendentes sobre $\mathbb{Q}$, entonces $\alpha+\beta$ o $\alpha\cdot\beta$ son trascendentes sobre $\mathbb{Q}$. Dar un contraejemplo a la implicación: α,β trascendentes $\Rightarrow$ $\alpha+\beta$ trascendente.

7) Usando los principios de lo que más tarde sería la teoría de Galois, Gauss demostró (a los 19 años) que

$$\cos\frac{2\pi}{17}=-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

Deducir que el polígono regular de 17 lados se puede construir con regla y compás.

<u>Nota</u>: Esta construcción geométrica es una de las pocas que había escapado al ingenio de los antiguos geómetras griegos. Según se dice, Gauss mandó que fuera inscrita en su tumba.

8) Demostra que si los polígonos regulares de n y m lados son construibles con regla y compás, también lo es el de $\mathrm{mcm}(n,m)$ lados. Concluir del ejercicio anterior que el polígono regular de 204 lados es construible con regla y compás.

9) ¿Se puede triplicar el cubo?

10) ¿Se puede trisecar el ángulo de $\pi/2^n$ radianes?

11) Supongamos que disponemos de una regla curva cuyo borde tiene la forma de la gráfica de $y=x^3$ para $x\geq 0$. Esta regla está sin graduar (aunque tiene marcado el cero) y sólo puede ser usada para trazar la curva que une dos puntos construibles, uno de ellos situado en el origen de la regla. Demostrar que con regla, compás y regla curva se puede duplicar el cubo. ¿Se puede cuadrar el círculo? ¿Y trisecar el ángulo?

3. Grupo de Galois.
Extensiones Normales y Separables.

La dimensión es suficiente en álgebra lineal para clasificar (salvo isomorfismos) los espacios vectoriales sobre $\mathbb{R}$, pero la situación es bien distinta en lo que respecta a extensiones de cuerpos (que son espacios vectoriales con más estructura). Así por ejemplo

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$$

y sin embargo, al menos en apariencia, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$ son bien distintas.

Ya antes de Galois se conocían diferentes versiones del teorema de los polinomios simétricos (Teorema 2.13 del Capítulo 1) y por tanto que todas las raíces del polinomio mínimo juegan un papel "simétrico" cuando las consideramos sobre $\mathbb{Q}$. Por eso no parece descabellado decir que si $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$ fueran "isomorfas" también lo serían $L_1/\mathbb{Q}$ y $L_2/\mathbb{Q}$ con

$$L_1 = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}, \sqrt[4]{2}) \qquad \big(=\mathbb{Q}(\sqrt[4]{2}, i)\big)$$

$$L_2 = \mathbb{Q}(\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}+\sqrt{3}, -\sqrt{2}-\sqrt{3}) \qquad \big(=\mathbb{Q}(\sqrt{2}, \sqrt{3})\big)$$

porque L_1 está generado por las raíces del polinomio mínimo de $\sqrt[4]{2}$ y L_2 por las raíces del polinomio mínimo de $\sqrt{2}+\sqrt{3}$. Pero es evidente que L_1 y L_2 son "esencialmente" distintos porque tienen diferente grado sobre $\mathbb{Q}$.

Con esto hemos querido mostrar que podemos restringirnos a comparar cuerpos "simétricos", en el sentido de que contengan todas las raíces del polinomio mínimo de sus generadores. Supongamos ahora que L_1 es como antes pero $L_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ que tiene el mismo grado que L_1 sobre $\mathbb{Q}$. También podríamos comprobar que L_1 y L_2 son bien distintos viendo que la "simetría", σ, que pasa $\sqrt[4]{2}$ a $i\sqrt[4]{2}$ y deja i fijo tiene orden 4, concretamente

$$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}, \quad \sigma(i\sqrt[4]{2}) = -\sqrt[4]{2}, \quad \sigma(-\sqrt[4]{2}) = -i\sqrt[4]{2}, \quad \sigma(-i\sqrt[4]{2}) = \sqrt[4]{2},$$

mientras que todas las "simetrías" de $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ son de orden 2 porque corresponden a cambios de signo de $\sqrt{2}$, $\sqrt{3}$ y $\sqrt{5}$.

En este capítulo definiremos rigurosamente estas "simetrías" (*automorfismos*) de una extensión y probaremos que forman un grupo (*el grupo de Galois*). Siempre que la extensión contenga a cada elemento y su "simétrico" (que sea *normal*) y satisfaga una condición técnica (que sea *separable*), demostraremos que el grupo de "simetrías" refleja fielmente toda la estructura de la extensión. Éste constituye el teorema fundamental de la teoría de Galois.

§1. Automorfismos y grupo de Galois.

Aunque nuestro principal interés son los cuerpos, será útil tener las siguientes definiciones en el marco general de los anillos

Definición: *Sean A y B anillos (conmutativos y unitarios) un* homomorfismo *de anillos es una función $\phi : A \longrightarrow B$ que respeta la suma, la multiplicación y el elemento unidad, esto es*

$$i)\ \phi(a_1+a_2)=\phi(a_1)+\phi(a_2) \qquad ii)\ \phi(a_1a_2)=\phi(a_1)\phi(a_2) \qquad iii)\ \phi(1_A)=1_B.$$

Definición: *i) Si ϕ es inyectiva se dice que es un* monomorfismo*.*

ii) Si ϕ es sobreyectiva se dice que es un epimorfismo*.*

iii) Si ϕ es biyectiva se dice que es un isomorfismo*.*

iv) Si ϕ es biyectiva y $A=B$ se dice que es un automorfismo*.*

Los dos últimos apartados de la definición anterior sólo los usaremos para cuerpos.

Definición: *Los automorfismos (o isomorfismos) que dejan fijos los elementos de cierto subcuerpo K, se llaman* K-automorfismos *(o* K-isomorfismos*).*

Definición: *Dada L/K, al conjunto de K-automorfismos de L se le llama* grupo de Galois *de L/K y se escribe $\mathcal{G}(L/K)$.*

Nota: Otras notaciones que se utilizan (por ejemplo en el libro de Stewart) en lugar de $\mathcal{G}(L/K)$ son $\Gamma(L:K)$ y en cierto contexto K^*.

Lema 1.1: *$\mathcal{G}(L/K)$ es un grupo (con la composición).*

Dem.: La composición es cerrada porque si σ y τ son K-automorfismos, es decir, dejan fijo K, entonces $\sigma\circ\tau$ (que abreviaremos con $\sigma\tau$) también deja fijo K. El resto de las propiedades de grupo se siguen fácilmente de las propiedas de la composición de funciones. ■

Ejemplo 1. $\mathcal{G}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})\cong\mathbb{Z}/2\mathbb{Z}$.

Un elemento, σ, de $\mathcal{G}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ queda caracterizado por la imagen, a, de $\sqrt{2}$, y se tiene

$$a=\sigma(\sqrt{2}) \ \Rightarrow\ a^2=\sigma(\sqrt{2})\sigma(\sqrt{2})=\sigma(2)=2.$$

Por tanto σ puede dejar fijo a $\sqrt{2}$ o puede mandarlo a $-\sqrt{2}$. en el primer caso σ es la identidad y en el segundo caso es la conjugación, $\text{conj.}(a+b\sqrt{2})=a-b\sqrt{2}$ que obviamente es un $\mathbb{Q}$-automorfismo (porque $\text{conj.}((a+b\sqrt{2})+(c+d\sqrt{2}))=\text{conj.}(a+b\sqrt{2})+\text{conj.}(c+d\sqrt{2})$, etc) y tiene orden 2. Con ello hemos demostrado

$$\mathcal{G}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})=\{\text{Id},\text{conj.}\}\cong\mathbb{Z}/2\mathbb{Z}.$$

Ejemplo 2. $\mathcal{G}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}\}$.

Como antes, un elemento, $\sigma \in \mathcal{G}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ queda caracterizado por la imagen, a, de $\sqrt[3]{2}$, y se tiene

$$a = \sigma(\sqrt[3]{2}) \;\Rightarrow\; a^3 = \sigma(\sqrt[3]{2})\sigma(\sqrt[3]{2})\sigma(\sqrt[3]{2}) = \sigma(2) = 2.$$

Pero el único $a \in \mathbb{Q}(\sqrt[3]{2})$ que cumple $a^3 = 2$ es $\sqrt[3]{2}$, así que σ deja fijo a $\sqrt[3]{2}$ y por tanto es la identidad.

Con este ejemplo vemos que, en principio, el grupo de Galois no "distingue" entre $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ y la extensión trivial $\mathbb{Q}/\mathbb{Q}$. Más adelante veremos que esto ha ocurrido porque $\mathbb{Q}(\sqrt[3]{2})$ no contiene a las otras raíces del polinomio mínimo de $\sqrt[3]{2}$ (diremos que la extensión no es normal).

El intento de recuperar la estructura de una extensión a partir de $\mathcal{G}$ sugiere la siguiente definición

DEFINICIÓN: *Sea H un subgrupo de $\mathcal{G}(L/K)$, se dice que*

$$\{x \in L \,/\, \sigma(x) = x \text{ para todo } \sigma \in H\}$$

es el <u>*subcuerpo fijo por H*</u> *y a veces se denota con H' o $H^\dagger$.*

La definición anterior tiene sentido gracias al siguiente resultado

Lema 1.2: *Si H es un subgrupo de $\mathcal{G}(L/K)$ entonces H' es un subcuerpo de L*

DEM.: Si $x, y \in H'$ entonces para todo $\sigma \in \mathcal{G}(L/K)$ se tiene $\sigma(x) = x$ y $\sigma(y) = y$, pero entonces $\sigma(x+y) = x+y$ y por tanto $x + y \in H'$. Lo mismo se haría con el resto de las operaciones. ■

OBSERVACIÓN: Nótese que $\big(\mathcal{G}(L/K)\big)' = K$ no es cierto en general, por ejemplo

$$\mathcal{G}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}\} \;\Rightarrow\; \big(\mathcal{G}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})\big)' = \mathbb{Q}(\sqrt[3]{2}).$$

El teorema fundamental de la teoría de Galois afirmará que esta igualdad (y de hecho una más general) se cumple bajo ciertas condiciones.

La próxima proposición asegura que hay restricciones para definir los automorfismos de $\mathcal{G}(L/K)$, y la siguiente asegura que $\mathcal{G}(L/K)$ determina el grado de ciertas subextensiones de L/K.

Proposición 1.3: *Sea L/K y $P \in K[x]$. Si $\alpha \in L$ es un cero de P, entonces $\sigma(\alpha)$ con $\sigma \in \mathcal{G}(L/K)$ también lo es.*

OBSERVACIÓN: Esto implica que cada $\sigma \in \mathcal{G}(L/K)$ induce una permutación actuando sobre el conjunto $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ de raíces distintas de P en L. (Nótese que $\sigma(\alpha_i) = \sigma(\alpha_j) \Rightarrow \sigma(\alpha_i - \alpha_j) = 0 \Rightarrow \alpha_i = \alpha_j$).

Proposición 1.4: *Sea H un subgrupo finito de $\mathcal{G}(L/K)$. Si H' es el subcuerpo fijo por los automorfismos de H, entonces*

$$[L : H'] = |H|.$$

De esta proposición se deduce inmediatamente

Corolario 1.5: *Sea L/K una extensión finita y sea H un subgrupo de $\mathcal{G}(L/K)$, entonces*

$$[H' : K] = \frac{[L : K]}{|H|}.$$

<u>OBSERVACIÓN</u>: Nótese que de estos resultados se deduce que a cada subgrupo de $\mathcal{G}(L/K)$ se le puede asociar de forma unívoca un subcuerpo de L conteniendo a K.

<u>Ejemplo</u> . Más adelante demostraremos que

$$\mathcal{G}(\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6, \sigma^7\} \cong \mathbb{Z}/8\mathbb{Z}$$

donde $\sigma\big(\cos\frac{2\pi}{17}\big) = \cos\frac{6\pi}{17}$. En este ejemplo veremos cómo se deduce la estructura de $\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}$ a partir de la información contenida en $\mathbb{Z}/8\mathbb{Z}$.

Sea $\zeta = e^{2\pi i/17}$, como ζ es raíz del polinomio (ciclotómico) irreducible $x^{16} + x^{15} + \ldots + x + 1$, se tiene

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 16.$$

Obviamente $\mathbb{Q}(\zeta) \neq \mathbb{Q}(\cos\frac{2\pi}{17})$ y $\mathbb{Q}(\zeta) \supset \mathbb{Q}(\cos\frac{2\pi}{17})$, porque $\cos\frac{2\pi}{17} = (\zeta + \zeta^{-1})/2$, así pues

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 16, \quad [\mathbb{Q}(\zeta) : \mathbb{Q}(\cos\frac{2\pi}{17})] > 1 \;\Rightarrow\; [\mathbb{Q}(\cos\frac{2\pi}{17}) : \mathbb{Q}] \leq 8.$$

Pero por la Proposición 1.4 el grado de $\mathbb{Q}(\cos\frac{2\pi}{17})$ sobre el subcuerpo fijo por el grupo de Galois es 8 y como este subcuerpo incluye a $\mathbb{Q}$ concluimos

$$[\mathbb{Q}(\cos\frac{2\pi}{17}) : \mathbb{Q}] = 8.$$

Por otra parte, $\mathbb{Z}/8\mathbb{Z}$ tiene subgrupos de orden 1,2, 4 y 8 que corresponden a

$$H_1 = \{\mathrm{Id}\}, \quad H_2 = \{\mathrm{Id}, \sigma^4\}, \quad H_4 = \{\mathrm{Id}, \sigma^2, \sigma^4, \sigma^6\}, \quad H_8 = \mathcal{G}(\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}).$$

Según el Corolario 1.5 se tiene

$$[H'_n : \mathbb{Q}] = \frac{[\mathbb{Q}(\cos\frac{2\pi}{17}) : \mathbb{Q}]}{n} = \frac{8}{n} \qquad n = 1, 2, 4, 8.$$

Por tanto

$$\mathbb{Q} = H'_8 \subset H'_4 \subset H'_2 \subset H'_1 = \mathbb{Q}(\cos\frac{2\pi}{17})$$

es una cadena de subcuerpos tal que todas las extensiones son de grado dos, en particular $\cos\frac{2\pi}{17}$ es una longitud construible con regla y compás y, por tanto, el polígono de 17 lados es construible con regla y compás. De hecho, hallando explícitamente los H'_n uno podría obtener un método para construirlo.

<u>Nota histórica</u>: Los razonamientos con los subcuerpos fijos guardan una analogía esencial con la demostración original de Gauss de que el polígono de 17 lados es construible con regla y compás. Partiendo de ζ, Gauss construía polinomios en ζ que eran invariantes al cambiar ζ por algunas de sus potencias. Por ejemplo $\zeta + \zeta^{16}$ es invariante al cambiar ζ por ζ^{16} y $\zeta+\zeta^4+\zeta^{13}+\zeta^{16}$ es invariante al cambiar ζ por ζ^{13} o por ζ^{16}. Considerando sumas y productos de estos polinomios, lograba una mayor invariancia (por ejemplo, $\zeta + \zeta^{16}$ y $\zeta^4+\zeta^{13}$ son invariantes por $\zeta \mapsto \zeta^{16}$ mientras que $(\zeta+\zeta^{16})+(\zeta^4+\zeta^{13})$ y $(\zeta+\zeta^{16})(\zeta^4+\zeta^{13})$ también lo son por $\zeta \mapsto \zeta^{13}$) hasta llegar a cantidades que eran racionales (simétricas en todos los ζ^j). Partiendo de ellas pudo recuperar las expresiones polinómicas en ζ resolviendo sucesivas ecuaciones de segundo grado, ya que sabiendo la suma y el producto de dos números se pueden calcular con una ecuación de este tipo. Con ello, expresó $\cos\frac{2\pi}{17}$ en términos de números racionales y sucesivas raíces cuadradas.

Gauss dio condiciones necesarias y suficientes para la constructibilidad del polígono de n lados, para ello, esencialmente, tuvo que calcular $\mathcal{G}(\mathbb{Q}(\cos\frac{2\pi}{p})/\mathbb{Q})$ (años antes de que Galois naciera) lo que conllevaba utilizar algunas ideas fundamentales de la teoría de Galois (incluso la resolubilidad de ecuaciones por radicales se menciona en el Art. 359 de las "Disquisitiones Arithmeticae" de Gauss).

Hablando en rigor, hay una parte de este cálculo que Gauss no publicó (o al menos no ha llegado hasta nosotros), además no está clara la influencia de Gauss sobre Galois ni de Lagrange sobre Gauss (véase §27 en "Galois Theory" de Edwards) y lo cierto es que el trabajo posterior de Galois es más general porque se aplica a otras extensiones y permite una solución definitiva del problema de resolubilidad por radicales.

<u>Dem.(de la Proposición 1.3)</u>: Sea $P = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Si α es un

cero de P

$$\begin{aligned} 0 =& \sigma\big(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0\big) \\ =& a_n\big(\sigma(\alpha)\big)^n + a_{n-1}\big(\sigma(\alpha)\big)^{n-1} + \ldots + a_1\sigma(\alpha) + a_0 \quad \text{ porque } a_i \in K. \end{aligned}$$

Por tanto $\sigma(\alpha)$ también es una raíz de P.

Para demostrar la Proposición 1.4 necesitaremos el siguiente lema

Lema 1.6 : *Sean $\sigma_1, \sigma_2, \ldots, \sigma_n \in \mathcal{G}(L/K)$ distintos, entonces el conjunto $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ es linealmente independiente sobre L. Es decir, si $\lambda_1, \lambda_2, \ldots, \lambda_n \in L$ no son simultáneamente nulos entonces $\lambda_1\sigma_1 + \lambda_2\sigma_2 + \ldots + \lambda_n\sigma_n$ no es la función idénticamente nula en L.*

DEM.: Procedemos por reducción al absurdo.

Sea $\lambda_1\sigma_1 + \lambda_2\sigma_2 + \ldots + \lambda_n\sigma_n$ con $\lambda_1 \neq 0$, la combinación lineal más corta (con n más pequeño) que produce la función nula en L, esto es,

$$\lambda_1\sigma_1(\alpha) + \lambda_2\sigma_2(\alpha) + \ldots + \lambda_n\sigma_n(\alpha) = 0 \quad \forall\alpha \in L. \tag{1.1}$$

Como α es arbitrario lo podemos sustituir por $\alpha\beta$ donde $\beta \in L$ se escogerá a continuación, por tanto

$$\lambda_1\sigma_1(\alpha)\sigma_1(\beta) + \lambda_2\sigma_2(\alpha)\sigma_2(\beta) + \ldots + \lambda_n\sigma_n(\alpha)\sigma_n(\beta) = 0 \quad \forall\alpha \in L. \tag{1.2}$$

Elijamos β tal que $\sigma_1(\beta) \neq \sigma_n(\beta)$, esto es posible por que σ_1 y σ_n son distintos. Multiplicando (1.1) por $\sigma_n(\beta)$ y restándole (1.2) se tiene

$$\lambda_1'\sigma_1(\alpha) + \lambda_2'\sigma_2(\alpha) + \ldots + \lambda_{n-1}'\sigma_{n-1}(\alpha) = 0 \quad \forall\alpha \in L$$

con $\lambda_1' \neq 0$, pero esto contradice que hubiéramos tomado la combinación lineal más corta. ∎

DEM.(de la Proposición 1.4):

a) $[L : H'] \geq |H|$.

Sean $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ una base de L/H' y sea $H = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ (por tanto $r = [L : H']$ y $n = |H|$). Consideremos el sistema de ecuaciones

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_2(\alpha_1)x_2 + \ldots + \sigma_n(\alpha_1)x_n &= 0 \\ \sigma_1(\alpha_2)x_1 + \sigma_2(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_2)x_n &= 0 \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad &\ldots \\ \sigma_1(\alpha_r)x_1 + \sigma_2(\alpha_r)x_2 + \ldots + \sigma_n(\alpha_r)x_n &= 0. \end{aligned}$$

Si $r < n$ (es decir, si $[L : H'] < |H|$) tiene una solución trivial $x_1 = \lambda_1, x_2 = \lambda_2, \ldots, x_n = \lambda_n$ de modo que

$$\lambda_1\sigma_1(\alpha_i) + \lambda_2\sigma_2(\alpha_i) + \ldots + \lambda_n\sigma_n(\alpha_i) = 0 \qquad 1 \leq i \leq r,$$

pero como $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ es una base esto implica

$$\lambda_1\sigma_1(\alpha) + \lambda_2\sigma_2(\alpha) + \ldots + \lambda_n\sigma_n(\alpha) = 0 \qquad \forall\alpha \in L.$$

Lo cual contradice el lema anterior.

b) $[L : H'] \leq |H|$

Sean $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$, r y n como en a). Tenemos que demostrar $r \leq n$. Supongamos $r > n$, entonces el sistema

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \ldots + \sigma_1(\alpha_r)x_r &= 0 \\ \sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \ldots + \sigma_2(\alpha_r)x_r &= 0 \\ \ldots \qquad \ldots \quad \ldots \qquad \ldots \quad & \ldots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_r)x_r &= 0 \end{aligned} \tag{1.3}$$

es compatible indeterminado. Además por el teorema de Rouché-Frobenius existen soluciones no triviales, digamos $x_1 = \lambda_1, x_2 = \lambda_2, \ldots, x_n = \lambda_n$, y hay $r - n$ de las variables que se pueden elegir arbitrariamente (las soluciones dependen de $r - n$ parámetros). Quizá reordenando las variables, podemos suponer que éstas son las $r - n$ primeras. Definamos

$$\Lambda_i = \sigma_1(\lambda_i) + \sigma_2(\lambda_i) + \ldots \sigma_n(\lambda_i)$$

para $1 \leq i \leq r$. Como $\lambda_1, \lambda_2, \ldots, \lambda_{r-n}$ son arbitrarios, pueden escogerse de manera que Λ_i sea no nulo cuando $1 \leq i \leq r - n$ (recuérdese que los σ_j son independientes).

Como H es un grupo $\sigma(\Lambda_i) = \Lambda_i$ para todo $\sigma \in H$ (ya que $\sigma\sigma_r = \sigma\sigma_s \Rightarrow \sigma_r = \sigma_s$) y por tanto $\Lambda_i \in H'$. Por otra parte

$$\sum_{i=1}^{r} \Lambda_i\alpha_i = \sum_{j=1}^{n} \sigma_j \left(\sum_{i=1}^{r} \sigma_j^{-1}(\alpha_i)\lambda_i \right) = 0,$$

donde la última igualdad está justificada porque el término entre paréntesis es una de la ecuaciones de (1.3) (nótese que $\sigma_j^{-1} \in H$). Pero esto implica que $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ es un conjunto linealmente dependiente sobre H' y por tanto no es una base, lo que contradice nuestras hipótesis. ■

§2. Extensiones normales.

Para que $\mathcal{G}(L/K)$ tenga información significativa acerca de L/K, los polinomios de $K[x]$ deben factorizar completamente en $L[x]$. Intuitivamente, se puede afirmar que como las raíces de un polinomio juegan un papel simétrico las necesitamos a todas para obtener todas las “simetrías” que caracterizan a la extensión.

Un primer problema técnico es saber si un polinomio se factoriza en alguna extensión.

Lema 2.1 : *Dado $P \in K[x]$ no constante, existe una extensión finita, L/K, tal que P tiene una raíz en L.*

<u>Observación</u>: Este teorema es trivial si $K \subset \mathbb{C}$, porque en ese caso podemos aplicar el teorema fundamental del Álgebra, pero por ejemplo, si $K = \mathbb{F}_2$ y $P = x^2 + x + 1$, el lema asegura que existe una extensión de $\mathbb{F}_2$ que contiene a las raíces de P lo cual no es en absoluto evidente.

<u>Dem.</u>: Podemos suponer que P es irreducible (en otro caso tómese uno de sus factores irreducibles) y que $\partial P > 1$ (Si $\partial P = 1$, $L = K$). Consideremos el anillo

$$L = K[x]\big/(P).$$

Obviamente K está “incluido” en L, o más concretamente, existe un monomorfismo $\phi : K \longrightarrow L$. Además L es de hecho un cuerpo, lo cual se puede deducir sabiendo que (P) es maximal (usando teoremas del curso anterior) o directamente observando que la Proposición 2.4 del primer capítulo implica que $\forall Q \notin (P)\ \exists A, B \in K[x] \big/ AP + BQ = 1$ y por tanto el inverso de la clase $\overline{Q} = Q + (P)$ es $\overline{B} = B + (P)$. Por último, nótese que L/K es finita y que $\overline{x} = x + (P)$ es una raíz de P (hablando en rigor, de su imagen en $L[X]$ inducida por ϕ), ya que $P(\overline{x}) = \overline{P(x)}$ coincide con la clase de cero en L. ■

<u>Ejemplo</u> . Sea $K = \mathbb{F}_2$. Según la demostración del lema anterior, se tiene que $P = x^2 + x + 1$ factoriza en $L = \mathbb{F}_2[x]/(P)$ (considerando L como extensión de $\mathbb{F}_2$). En un ejercicio (véase la Hoja 1) habíamos visto que $L = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$ (nótese que $\overline{x}^2 = \overline{-x-1} = \overline{x+1}$, etc.). En dicho ejercicio también habíamos calculado las tablas de suma y multiplicación de este cuerpo de cuatro elementos. Llamando α a $\overline{x}$ y β a $\overline{x+1}$ y abreviando $\overline{0}$, $\overline{1}$ con 0 y 1, dichas tablas son

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Obsérvese que usando estas tablas se tiene que α y β son raíces de P porque

$$\begin{aligned} \alpha^2 + \alpha + 1 = \beta + \alpha + 1 = 1 + 1 = 0 \\ \beta^2 + \beta + 1 = \alpha + \beta + 1 = 1 + 1 = 0 \end{aligned}.$$

Así que podríamos escribir $P = (x - \alpha)(x - \beta)$ en $L[x]$. Más adelante llamaremos $\mathbb{F}_4$ a este cuerpo, L, que extiende a $\mathbb{F}_2$ de manera que P factoriza.

En las demostraciones de esta sección apelaremos al siguiente lema que concreta más la idea de la demostración del resultado anterior.

Lema 2.2 : *Sea L/K y sea P el polinomio mínimo de $\alpha \in L$ sobre K, entonces*

$$\psi : K(\alpha) \longrightarrow K[x]/(P)$$

con $\psi(\alpha) = \overline{x} = x + (P)$, define un K-isomorfismo. En particular, si $\beta \in L$ es otra raíz de P, existe un K-isomorfismo $i : K(\alpha) \longrightarrow K(\beta)$ con $i(\alpha) = \beta$.

<u>DEM.</u>: Por la Proposición 3.4 del Capítulo 1 se tiene que $\alpha_1, \alpha_2 \in K(\alpha) \Rightarrow \alpha_1 = Q_1(\alpha)$, $\alpha_2 = Q_2(\alpha)$, $\alpha_1\alpha_2 = Q_3(\alpha)$ con $\partial Q_i < \partial P$.

Es obvio que ψ deja fijo K (lo definimos así) y que

$$\psi(\alpha_1 + \alpha_2) = \psi\big(Q_1(\alpha) + Q_2(\alpha)\big) = \overline{Q_1(x)} + \overline{Q_2(x)} = \psi(\alpha_1) + \psi(\alpha_2).$$

Nótese que $Q_1Q_2 - Q_3$ se anula en α, por tanto es divisible por P y su clase en $K[x]/(P)$ es la clase de cero. Por tanto

$$\psi(\alpha_1)\psi(\alpha_2) - \psi(\alpha_1\alpha_2) = \overline{Q_1(x)Q_2(x)} - \overline{Q_3(x)} = \overline{0}.$$

Como ψ aplica el generador de $K(\alpha)$ en el generador de $K[x]/(P)$ (siempre sobre K), es un epimorfismo. Además $\psi(\alpha_1) - \psi(\alpha_2) = 0 \Rightarrow Q_1 - Q_2 \in (P) \Rightarrow P | Q_1 - Q_2$ y como $\partial Q_i < \partial P$, $Q_1 = Q_2$ y ψ también es un monomorfismo. ■

DEFINICIÓN: *Sea $P \in K[x]$ y L/K una extensión. Se dice que L es un <u>cuerpo de descomposición de P</u>, $\partial P > 1$, si se verifican las condiciones:*

a) P se descompone en factores lineales en $L[x]$, esto es,

$$P = k(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n) \quad \text{en } L[x].$$

b) L/K es la menor extensión de K tal que se cumple a).

<u>NOTA</u>: Con la notación de la definición anterior, se tiene que el cuerpo de descomposición de P es $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Proposición 2.3 : *Para cada $P \in K[x]$ existe un cuerpo de descomposición de P y además es único salvo K-isomorfismos.*

<u>DEM.</u>: Para la existencia basta aplicar repetidas veces el Lema 2.1 hasta obtener un L en el que P se descomponga en factores lineales $x - \alpha_1$, $x - \alpha_2$,…,$x - \alpha_n$, entonces $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ es el cuerpo de descomposición de K.

$$\begin{tikzcd}
L_1 \arrow[d, dash] & & L_2 \arrow[d, dash] \\
K(\alpha_1) \arrow[dr, "i"'] & & K(\beta_1) \arrow[dl, "\widetilde{i}"] \\
& K[x]/(P) &
\end{tikzcd}$$

Para demostrar la unicidad salvo K-isomorfismos supongamos que L_1 y L_2 son cuerpos de descomposición de P. Procedemos por inducción en ∂P. Si $\partial P = 1$ es trivial. Si $\partial P > 1$, sea Q un factor mónico irreducible de P, entonces

$$Q = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n) \quad \text{en } L_1[x]$$

y

$$Q = (x - \beta_1)(x - \beta_2)\dots(x - \beta_n) \quad \text{en } L_2[x].$$

Por el Lema 2.2 se tienen K-isomorfismos

$$i : K(\alpha_1) \longrightarrow K[x]/(P) \qquad \widetilde{i} : K(\beta_1) \longrightarrow K[x]/(P),$$

por tanto $K(\alpha_1)$ y $K(\beta_1)$ son K-isomorfos por $\widetilde{i}^{-1} \circ i$.

L_1 es una extensión de $K(\alpha_1)$ y también L_2 puede considerarse que extiende a $K(\alpha_1)$ por medio del K-monorfismo $j \circ \widetilde{i}^{-1} \circ i : K(\alpha_1) \hookrightarrow L_2$ donde $j : K(\beta_1) \hookrightarrow L_2$ es la inclusión. Nótese que L_1 y L_2 son obviamente cuerpos de descomposición de P sobre $K(\alpha_1)$ y como $\alpha_1 \in K(\alpha_1)$ también lo son de $\widetilde{P} = P/(x - \alpha_1)$. La demostración se concluye por la hipótesis de inducción (ya que $\partial\widetilde{P} < \partial P$). ■

<u>Ejemplo</u> . El cuerpo de descomposición de $P = x^2 - 2 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\sqrt{2})$.

<u>Ejemplo</u> . El cuerpo de descomposición de $P = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (nótese que $P = (x^2 - 2)(x^2 - 3)$).

El concepto fundamental de esta sección se recoge en la definición siguiente

Definición: *Se dice que una extensión, L/K es <u>normal</u> si todo polinomio irreducible $P \in K[x]$ que tiene una raíz en L se descompone en factores lineal en $L[x]$.*

La definición de extensión normal parece ser mucho más restrictiva que la de cuerpo de descomposición en el sentido de que, en principio, una extensión normal debe contener los cuerpos de descomposición de "muchos" polinomios. Sin embargo se tiene el siguiente resultado

Proposición 2.4: *L/K es normal y finita $\Leftrightarrow$ L es el cuerpo de descomposición de un polinomio de $K[x]$.*

<u>Dem.</u>:

$\Rightarrow$) Sea $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Sean P_1, P_2,…,P_n, sus polinomios mínimos sobre K y sea $P = P_1 \cdot P_2 \cdot \ldots \cdot P_n$. Como L/K es normal, cada P_i se descompone en factores lineales y lo mismo ocurre con P; por tanto L contiene al cuerpo de descomposición de P y como L está generado por la raíces de P, coincide con él.

$\Leftarrow$) Sea L el cuerpo de descomposición de $Q \in K[x]$. Basta demostrar que si α y β son raíces de un polinomio mónico irreducible, $\in K[x]$, entonces $\alpha \in L \Rightarrow \beta \in L$.

Por el Lema 2.2 existe un K-isomorfismo $i : K(\alpha) \longrightarrow K(\beta)$. Por otra parte, $L(\alpha)$ es un cuerpo de descomposición de $Q \in K(\alpha)[x]$ y también $L(\beta)$ puede considerarse como otro cuerpo de descomposición teniendo en cuenta la "K-inclusión" $K(\alpha) \xrightarrow{i} K(\beta) \hookrightarrow L(\beta)$. La Proposición 2.3 implica que $L(\alpha)$ y $L(\beta)$ son isomorfos como extensiones de $K(\alpha)$, por tanto $[L(\alpha) : K] = [L(\beta) : K]$. Si $\alpha \in L$, se tiene

$$1 = [L(\alpha) : L] = \frac{[L(\alpha) : K]}{[L : K]} = \frac{[L(\beta) : K]}{[L : K]} = [L(\beta) : L] = 1,$$

es decir, $\beta \in L$. ■

Terminamos esta sección con una proposición que se será fundamental en el cálculo explícito de grupos de Galois

Proposición 2.5 : *Sea L/K normal y finita y sean M_1 y M_2 dos subcuerpos de L conteniendo a K. Si $i : M_1 \longrightarrow M_2$ es un K-isomorfismo, entonces existe $\sigma \in \mathcal{G}(L/K)$ tal que restringido a M_1 coincide con i.*

De aquí se deduce un resultado más fuerte que la Proposición 1.3

Corolario 2.6: *Sea L/K normal. Si P es un polinomio irreducible y $\alpha, \beta \in L$ son raíces de P, entonces existe $\sigma \in \mathcal{G}(L/K)$ con $\sigma(\alpha) = \beta$.*

<u>DEM.</u>: Basta aplicar la proposición tomando $M_1 = K(\alpha)$, $M_2 = K(\beta)$ y el isomorfismo $i : M_1 \longrightarrow M_2$ del Lema 2.2. ■

<u>DEM.(de la Proposición 2.5)</u>: Como $[L : M_1] < \infty$, basta aplicar repetidas veces que si $\alpha \in L$ entonces se puede extender a un K-isomorfismo $\widetilde{i} : M_1(\alpha) \longrightarrow M_2(\beta)$ con cierto $\beta \in L$. El resto de la demostración se dedica a construir $\widetilde{i}$.

Sea P el polinomio mínimo de α sobre K y sea P_1 el polinomio mínimo sobre M_1, obviamente $P_1 | P$. Podemos suponer que $\partial P_1 > 1$ (en otro caso tomaríamos $\widetilde{i} = i$). Sea $P_2 = i(P_1)$ (i actúa sobre los coeficientes). P_2 es mónico e irreducible y divide a P, porque $P = P_1 \cdot Q_1 \Rightarrow P = i(P) = i(P_1) \cdot i(Q_1)$. como L/K es normal, todas las raíces de P, y por tanto también las de P_2, están en L. Sea $\beta \in L$ con $P_2(\beta) = 0$, por el Lema 2.2 se tiene un M_1-isomorfismo, i_1, y un M_2-isomorfismo, i_2,

$$i_1 : M_1(\alpha) \longrightarrow M_1[x]/(P_1), \qquad i_2 : M_2(\beta) \longrightarrow M_2[x]/(P_2).$$

Por otra parte, i induce un K-isomorfismo, i_3,

$$i_3 : M_1[x]/(P_1) \longrightarrow M_2[x]/(P_2),$$

así pues basta tomar $\widetilde{i} = i_2^{-1} \circ i_3 \circ i_1$. ■

Aunque dedicaremos casi toda la sección 4 a dar ejemplos explícitos del cálculo del grupo de Galois, vemos cómo se aplican estos resultados en un caso sencillo:

Ejemplo . Hallar $\mathcal{G}\big(\mathbb{Q}(\zeta)/Q\big)$ donde $\zeta = e^{2\pi i/5}$.

Como la extensión es simple y generada por ζ, cada $\sigma \in \mathcal{G}\big(\mathbb{Q}(\zeta)/Q\big)$ está determinado por su valor en ζ. Las raíces del polinomio ciclotómico $x^4+x^3+x^2+x+1$ son ζ, ζ^2, ζ^3 y ζ^4; así pues, el Corolario 2.6 implica que existen $\mathbb{Q}$-automorfismos σ_1, σ_2, σ_3 y σ_4 tales que

$$\sigma_1(\zeta)=\zeta, \qquad \sigma_2(\zeta)=\zeta^2, \qquad \sigma_3(\zeta)=\zeta^3, \qquad \sigma_4(\zeta)=\zeta^4.$$

Con lo cual se tiene $\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\} \subset \mathcal{G}\big(\mathbb{Q}(\zeta)/Q\big)$. Por otra parte, la Proposición 1.4 con $H=\mathcal{G}\big(\mathbb{Q}(\zeta)/Q\big)$ implica $|\mathcal{G}\big(\mathbb{Q}(\zeta)/Q\big)| \le 4$, ya que $[\mathbb{Q}(\zeta):H'] \le [\mathbb{Q}(\zeta):\mathbb{Q}]=4$. Por tanto la única posibilidad es

$$\mathcal{G}\big(\mathbb{Q}(\zeta)/Q\big)=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}.$$

Nótese que $\sigma_1 =$Id y que σ_2 genera al resto de los automorfismos, ya que

$$\begin{aligned}\sigma_2^2(\zeta) =& \sigma_2(\sigma_2(\zeta)) = \sigma_2(\zeta^2) = \zeta^4 = \sigma_4(\zeta)\\ \sigma_2^3(\zeta) =& \sigma_2(\sigma_2^2(\zeta)) = \sigma_2(\zeta^4) = \zeta^8 = \zeta^3 = \sigma_4(\zeta).\end{aligned}$$

Por consiguiente $\mathcal{G}\big(\mathbb{Q}(\zeta)/Q\big) \cong \mathbb{Z}/4\mathbb{Z}$.

§3. Extensiones separables.

Una condición técnica que necesitaremos más adelante es que las raíces de un polinomio irreducible sean distintas, ya que en otro caso la información contenida en el grupo de Galois puede ser muy pobre (véase la observación que sigue a la Proposición 1.3). A pesar de que esta condición técnica se cumple en todas las extensiones algebraicas relevantes en este curso, tiene interés considerarla desde una perspectiva general.

Definición: *Se dice que un polinomio irreducible $P \in K[x]$ es* <u>separable</u> *sobre K si cuando lo descomponemos en su cuerpo de descomposición como $P = k(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ todos los α_i son distintos. En caso contrario se dice que es* <u>inseparable</u>.

Definición: *Dado $\alpha \in L$ algebraico sobre K, se dice que α es* <u>separable</u> *sobre K si su polinomio mínimo lo es, y se dice que L/K es una extensión* <u>separable</u> *si todo elemento de L es separable sobre K.*

Hay una condición muy sencilla para saber si un polinomio es irreducible es separable sobre K y esta condición se satisface trivialmente cuando $K \subset \mathbb{C}$. Antes de enunciarla necesitaremos una definición.

Definición: *Dado $P = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in K[x]$, al polinomio*

$$P' = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2x + a_1,$$

se le llama <u>derivada formal</u> *de P.*

Proposición 3.1: *Un polinomio irreducible $P \in K[x]$ es inseparable si y sólo si $P' = 0$.*

De aquí se deduce inmediatamente

Corolario 3.2: *Si K es un cuerpo de característica cero, todo polinomio irreducible es separable.*

Corolario 3.3: *Si K es un cuerpo de característica $p > 0$ entonces los únicos polinomios inseparables son de la forma*

$$P = a_n x^{np} + a_{n-1}x^{(n-1)p} + \ldots + a_1 x^p + a_0$$

con $a_i \in K$, $0 < i \leq n$.

<u>DEM.(de la Proposición 3.1)</u>:

$\Rightarrow$) Como P es inseparable, existe α en el cuerpo de descomposición tal que $(x-\alpha)^2|P$ y se tiene

$$P = (x-\alpha)^2 R \;\Rightarrow\; P' = 2(x-\alpha)R + (x-\alpha)^2 R' \;\Rightarrow\; x-\alpha|P' \text{ y } x-\alpha|\text{mcd}\,(P,P').$$

Si $P' \neq 0$ entonces $1 \leq \partial\text{mcd}\,(P,P') < \partial P$ y por tanto $\text{mcd}\,(P,P')$ es un factor no trivial de P, lo que contradice que sea irreducible.

$\Leftarrow$) Si P fuera separable

$$P = k(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$$

con $\alpha_i \neq \alpha_j$ perteneciendo al cuerpo de descomposición de P sobre K. Entonces

$$P' = \sum_{i=1}^{n} P_i \qquad \text{donde} \qquad P_i(x) = \frac{P(x)}{x-\alpha_i}.$$

Como $x-\alpha_1|P_i$ para $2 \leq i \leq n$ y $x-\alpha_1 \not| P_1$ (porque α_1 no coincide con ninguna otra raíz) se tiene que $x-\alpha_1 \not| P'$ y por tanto $P' = 0$ es imposible. ■

Por el pequeño teorema de Fermat, $a^p = a$ para todo $a \in \mathbb{F}_p$, así que todos los polinomios de los que habla el Corolario 3.3 se pueden escribir como (nótese que en $\mathbb{F}_p$, $(a+b)^p = a^p + b^p$)

$$\begin{aligned} a_n x^{np} + a_{n-1}x^{(n-1)p} + \ldots + a_1 x^p + a_0 =& a_n^p x^{np} + a_{n-1}^p x^{(n-1)p} + \ldots + a_1^p x^p + a_0^p \\ =& (a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0)^p, \end{aligned}$$

* Quizá al lector le sorprenda que no llamemos a P' simplemente *derivada de P*. La razón para ello es que en muchos cuerpos, por ejemplo en $\mathbb{F}_p$, no tiene sentido el concepto de límite y con este nombre queremos hacer hincapié en que la definición es puramente formal y no tiene nada que ver con la definición habitual a pesar de comparte las mismas propiedades.

y por tanto no son irreducibles, de donde se deduce que no hay polinomios irreducibles inseparables sobre $\mathbb{F}_p$. La situación se puede generalizar un poco más definiendo el morfismo dado por "elevar a p".

DEFINICIÓN: *Sea K un cuerpo de característica $p > 0$, se llama* morfismo de Frobenius *a la función $\phi : K \longrightarrow K$ dada por $\phi(x) = x^p$.*

DEFINICIÓN: *Se dice que un cuerpo K es* un cuerpo perfecto, *o bien si tiene característica cero, o bien si tiene característica $p > 0$ y el morfismo de Frobenius es un isomorfismo.*

Ejemplo . Los cuerpos $\mathbb{F}_p$ son perfectos, ya que el automorfismo de Frobenius es $\phi = \mathrm{Id}$ (por el pequeño teorema de Fermat) y por tanto es un isomorfismo.

La misma demostración que hemos hecho para demostrar que en $\mathbb{F}_p$ no hay polinomios irreducibles inseparables, combinada con el Corolario 3.2, sirve para demostrar

Teorema 3.4 : *Si K es un cuerpo perfecto, entonces todo polinomio irreducible es separable.*

Ejemplo 1. En cualquier cuerpo $K \subset \mathbb{C}$ o en $\mathbb{F}_p$ todo polinomio irreducible es separable.

Ejemplo 2. Cualquier extensión algebraica de $\mathbb{F}_p$ es separable.

El teorema anterior combinado con la siguiente proposición (que no demostraremos) asegura que casi todas las extensiones que podamos imaginar son separables.

Proposición 3.5 : *Sean $K \subset L \subset M$ cuerpos y α algebraico sobre K, entonces*

a) Si α es separable sobre K, $K(\alpha)/K$ es separable.

b) Si M/L y L/K son separables, M/K es separable.

Como hemos comentado al principio de esta sección, la no separabilidad de una extensión constituye una dificultad para que la teoría de Galois sea útil en dicha extensión. Afortunadamente, todos los resultados anteriores sugieren que los ejemplos de extensiones no separables son un poco artificiales. Veamos uno.

Ejemplo . Consideremos la extensión $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$. El polinomio mínimo de t sobre $\mathbb{F}_2(t^2)$ es

$$P = x^2 - t^2 \qquad P \in \mathbb{F}_2(t^2)[x].$$

Se puede comprobar que este polinomio es inseparable con la Proposición 3.1 o bien notando que sus raíces, t y $-t$, coinciden en $\mathbb{F}_2(t)$ (ya que $-1 = 1$ en $\mathbb{F}_2$). Por tanto $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$ no es una extensión separable.

Nótese que la extensión $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$ es normal porque es finita y coincide con el cuerpo de descomposición de P (utilícese la Proposición 2.4). Sin embargo $\mathcal{G}\big(\mathbb{F}_2(t)/\mathbb{F}_2(t^2)\big)$

es trivial porque la Proposición 1.3 implica que $\sigma(t) = t$ para todo $\sigma \in \mathcal{G}\big(\mathbb{F}_2(t)/\mathbb{F}_2(t^2)\big)$. De alguna manera, no tenemos suficientes raíces distintas para que sus "simetrías" representen la estructura de la extensión.

§4. Teorema fundamental de la teoría de Galois y ejemplos.

Recuérdese que los ejemplos al comienzo del capítulo hacían pensar que algunas propiedades de las extensiones de cuerpos quedaban representadas por sus "simetrías". El teorema fundamental de la teoría de Galois afirma que esta representación es "exacta" cuando la extensión es normal finita y separable, en el sentido de que *existe una correspondencia uno a uno entre subcuerpos y subgrupos del grupo de Galois, y entre subextensiones normales y subgrupos normales.*

Es muy conveniente recordar la formulación intuitiva del teorema fundamental de la teoría Galois dada en el párrafo anterior para entender el enunciado concreto, que es el siguiente

Teorema 4.1 (Teorema fundamental de la teoría de Galois): *Si L/K es normal, finita y separable y M es un subcuerpo $K \subset M \subset L$, entonces $\mathcal{G}(L/M)$ es un subgrupo de $\mathcal{G}(L/K)$ y $M = \big(\mathcal{G}(L/M)\big)'$. Además M/K es normal si y sólo si $\mathcal{G}(L/M)$ es un subgrupo normal de $\mathcal{G}(L/K)$, en ese caso $\mathcal{G}(M/K)$ es isomorfo a $\mathcal{G}(L/K)/\mathcal{G}(L/M)$.*

<u>Observación</u>: Nótese que tras los resultados de la primera sección (Proposición 1.4) el teorema implica $[L : M] = \mathcal{G}(L/M)$. En particular el grado de la extensión es el orden del grupo de Galois.

La demostración no es muy complicada, una vez que se conoce todo el lenguaje y resultados de las dos secciones anteriores.

<u>Dem.</u>: Por definición $\mathcal{G}(L/M)$ es un subgrupo de $\mathcal{G}(L/K)$. Obviamente $\big(\mathcal{G}(L/M)\big)' \supset M$. Procedemos por contradicción suponiendo que existe $x \in \big(\mathcal{G}(L/M)\big)' - M$. Sea P su polinomio mínimo sobre M, P se descompone totalmente en L y sus raíces son distintas porque L/K es separable, por tanto el Corolario 2.6 con $K = M$ nos asegura que existe $\sigma \in \mathcal{G}(L/M)$ tal que $\sigma(x) \neq x$, lo que contradice $x \in \big(\mathcal{G}(L/M)\big)'$.

Veamos ahora que M/K es normal si y sólo si $\mathcal{G}(L/M)$ es un subgrupo normal.

$\Rightarrow$) Por la Proposición 2.4, $M = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ donde α_i son las raíces de un polinomio $P \in K[x]$. Dado $\sigma \in \mathcal{G}(L/K)$, por la Proposición 1.3 se tiene $\sigma(M) = M$ y por tanto $\sigma|_M \in \mathcal{G}(M/K)$, donde $\sigma|_M$ es la restricción de σ a M. Esto define un homomorfismo de grupos

$$\begin{aligned} \phi : \mathcal{G}(L/K) &\longrightarrow \mathcal{G}(M/K) \\ \sigma &\longrightarrow \sigma|_M \end{aligned}$$

que es sobreyectivo (por la Proposición 2.5 con $M_1 = M_2 = M$) y cuyo núcleo es $\mathcal{G}(L/M)$, por tanto el teorema del isomorfismo (véase el repaso de teoría de grupos del próximo capítulo) implica que $\mathcal{G}(L/M)$ es un grupo normal de $\mathcal{G}(L/K)$ y que $\mathcal{G}(M/K)$ es isomorfo a $\mathcal{G}(L/K)/\mathcal{G}(L/M)$.

$\Leftarrow$) Si M/K no fuera normal, entonces existe un polinomio, P, con dos raíces $\alpha, \beta \in L$ tales que $\alpha \in M$ y $\beta \notin M$. Por el Corolario 2.5 existe $\tau \in \mathcal{G}(L/K)$ tal que $\tau(\alpha) = \beta$. Como $\beta \notin M$ y L/M es separable (por que L/K lo es), el Corolario 2.6 asegura que también existe $\sigma \in \mathcal{G}(L/M)$ tal que $\sigma(\beta) \neq \beta$, entonces $\tau^{-1}\sigma\tau(\alpha) \neq \alpha$ y por tanto $\tau^{-1}\mathcal{G}(L/M)\tau \neq \mathcal{G}(L/M)$, pero esto contradice que $\mathcal{G}(L/M)$ sea un subgrupo normal de $\mathcal{G}(L/K)$. ■

Según lo visto en las dos secciones anteriores, si K tiene característica cero o $K = \mathbb{F}_p$ (o incluso si K es una extensión finita de $\mathbb{F}_p$), entonces decir que L/K es normal, finita y separable es lo mismo que decir que L es el cuerpo de descomposición de un polinomio sobre K con raíces distintas. Esto sugiere la siguiente definición

DEFINICIÓN: *Se llama* grupo de Galois de $P \in K[x]$ *al grupo de Galois de su cuerpo de descomposición sobre K.*

Dado un polinomio arbitrario es realmente difícil, en general, calcular su grupo de Galois incluso usando computadoras. Dedicaremos el resto de la sección a calcular el grupo de Galois de algunas extensiones normales, finitas y separables de las que tenemos una descripción bastante explícita (fundamentalmente, los cuerpos estarán generados por combinaciones sencillas de radicales), lo que permite que los cálculos se puedan llevar a cabo.

Ejemplo 1. Calcular el grupo de Galois del (cuerpo de descomposición del) polinomio $x^4+x^3+x^2+x+1$ sobre $\mathbb{Q}$, describiendo explícitamente todos los subcuerpos intermedios.

Como $x^4 + x^3 + x^2 + x + 1 = (x^5 - 1)/(x - 1)$ (polinomio ciclotómico), sus raíces son ζ, ζ^2, ζ^3, ζ^4 con $\zeta = e^{2\pi i/5}$; así pues tenemos que calcular $G = \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Cada automorfismo en G está determinado por su acción sobre ζ y según el Corolario 2.6 existen automorfismos σ_1, σ_2, σ_3, $\sigma_4 \in G$ tales que

$$\sigma_1(\zeta) = \zeta \quad \sigma_2(\zeta) = \zeta^2 \quad \sigma_3(\zeta) = \zeta^3 \quad \sigma_4(\zeta) = \zeta^4.$$

Como $|G| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ ya no hay más automorfismos, es decir,

$$G = \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}.$$

* En principio hay un algoritmo (basado en la definición de grupo de Galois del propio Galois) pero requiere tantos cálculos que es casi inviable en la práctica, incluso para grados pequeños. El lector interesado lo puede encontrar en el apéndice a la segunda edición de "Galois Theory" de I. Stewart.

Veamos qué estructura tiene G. Obviamente $\sigma_1 = \mathrm{Id}$, $\sigma_2^2(\zeta) = \sigma_2(\zeta^2) = \big(\sigma_2(\zeta)\big)^2 = \zeta^4 \Rightarrow \sigma_4 = \sigma_2^2$. También $\sigma_2^3(\zeta) = \sigma_2(\zeta^4) = \zeta^8 \Rightarrow \sigma_3 = \sigma_2^3$. Así pues G es cíclico generado por σ_2

$$G = \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \langle \sigma_2 \rangle = \{\mathrm{Id}, \sigma_2, \sigma_2^2, \sigma_2^3\} \cong \mathbb{Z}/4\mathbb{Z}.$$

(Recuérdese que, en general, la notación $\langle g_1, g_2, \dots \rangle$ indica el subgrupo generado por $g_1, g_2 \dots$). Los únicos subgrupos de G son $\{\mathrm{Id}, \sigma_2^2\}$ y el grupo trivial $\{\mathrm{Id}\}$. Según el teorema fundamental de la teoría de Galois se tiene

$$\begin{array}{ccccc}
G = \{\mathrm{Id}, \sigma_2, \sigma_2^2, \sigma_2^3\} & = & \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) & & (\cong \mathbb{Z}/4\mathbb{Z}) \\
| & & & & \\
H = \{\mathrm{Id}, \sigma_2^2\} & = & \mathcal{G}(\mathbb{Q}(\zeta)/M) & & (\cong \mathbb{Z}/2\mathbb{Z}) \\
| & & & & \\
H = \{\mathrm{Id}\} & = & \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)) & & (\cong \{e\})
\end{array}$$

donde M es un cuerpo intermedio con $[M : \mathbb{Q}] = |G|/|H| = 2$. Como hay una correspondencia uno a uno entre subgrupos y subcuerpos, el único subcuerpo entre $\mathbb{Q}$ y $\mathbb{Q}(\zeta)$ es $M = H'$. Este cuerpo se puede calcular explícitamente usando la definición

$$M = H' = \{x \in \mathbb{Q}(\zeta) \,/\, \sigma(x) = x \ \forall \sigma \in H\}.$$

Como $H = \{\mathrm{Id}, \sigma_2^2\}$, y $\{1, \zeta, \zeta^2, \zeta^3\}$ es una base de $\mathbb{Q}(\zeta)$, se tiene

$$M = \big\{a + b\zeta + c\zeta^2 + d\zeta^3 \,/\, \sigma_2^2(a + b\zeta + c\zeta^2 + d\zeta^3) = a + b\zeta + c\zeta^2 + d\zeta^3,\ a, b, c, d \in \mathbb{Q}\big\}.$$

Un cálculo prueba

$$\begin{aligned}
\sigma_2^2(a + b\zeta + c\zeta^2 + d\zeta^3) &= a + b\zeta^4 + c\zeta^3 + d\zeta^2 \\
&= (a-b)\zeta - b\zeta + (d-b)\zeta^2 + (c-b)\zeta^3
\end{aligned}$$

donde en la segunda igualdad hemos usado $\zeta^4 = -1 - \zeta - \zeta^2 - \zeta^3$. Como $\{1, \zeta, \zeta^2, \zeta^3\}$ es una base de $\mathbb{Q}(\zeta)$,

$$\sigma_2^2(a + b\zeta + c\zeta^2 + d\zeta^3) = a + b\zeta^4 + c\zeta^3 + d\zeta^2 \ \Leftrightarrow \ \begin{array}{ll} a - b = a & -b = b \\ d - b = c & c - b = d. \end{array}$$

Resolviendo este sistema se tiene finalmente

$$M = \big\{a + c(\zeta^2 + \zeta^3) \,/\, a, c \in \mathbb{Q}\big\}.$$

Como $\zeta^2 + \zeta^3 = e^{4\pi i/5} + e^{6\pi i/5} = 2\cos(4\pi/5)$, se puede escribir más explícitamente $M = \mathbb{Q}(\cos(4\pi/5))$. Como H es un subgrupo normal de G (porque $G \cong \mathbb{Z}/4\mathbb{Z}$ que es abeliano), entonces $M/\mathbb{Q}$ es una extensión normal.

<u>Observación</u>: Quizá al lector le parezca que $\mathbb{Q}(\cos(2\pi/5))$ es "otro" cuerpo intermedio, contradiciendo al teorema fundamental. en realidad, usando las fórmulas de adición

de las funciones trigonométricas no es difícil probar que $\mathbb{Q}(\cos(2\pi/5)) = \mathbb{Q}(\cos(4\pi/5))$.

Veamos ahora uno de los ejemplos más completos que se pueden poner a este nivel. Nótese cómo entra en juego de forma fundamental la Proposición 2.5 que dice intuitivamente que podemos obtener automorfismos en una extensión grande ampliando otros de una extensión menor más sencilla. Esta situación se repetirá en ejemplos posteriores.

Ejemplo 2. Calcular el grupo de Galois (del cuerpo de descomposición) del polinomio x^4-2 sobre $\mathbb{Q}$ y calcular el número de subcuerpos intermedios, describiendo explícitmente uno de ellos y diciendo si da lugar a una extensión normal.

Las raíces de x^4-2 son $i^k\sqrt[4]{2}$ con $k=0,1,2,3$, por tanto su cuerpo de descomposición es $\mathbb{Q}(i,\sqrt[4]{2})$. *En este, como en otros ejemplos, es conveniente "descomponer" la extensión en subextensiones normales que sean más sencillas,* consiguiendo que se repita de alguna manera la situación del ejemplo anterior. Por ello consideramos

$$\begin{array}{c} L=\mathbb{Q}(i,\sqrt[4]{2}) \\ | \\ M=\mathbb{Q}(i) \\ | \\ K=\mathbb{Q} \end{array}$$

Nótese que L/M es normal (porque L/K lo es) y M/K también es normal porque M es el cuerpo de descomposición de x^2+1. Antes de nada, calculemos $[L:K]$ para saber el orden del grupo de Galois

$$[L:\mathbb{Q}(\sqrt[4]{2})]=2\ \big(\text{porque } i\notin\mathbb{Q}(\sqrt[4]{2})\big)\ \Rightarrow\ [L:K]=[L:\mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=8.$$

El cálculo de $\mathcal{G}(L/K)$ se basa en calcular los grupos más sencillos $\mathcal{G}(L/M)$ y $\mathcal{G}(M/K)$, intentando más tarde unir ambas informaciones "pegando" ambos grupos.

Comencemos con $\mathcal{G}(L/M)$. Como $[L:M]=[L:K]/[M:K]=4$, el polinomio mínimo de $\sqrt[4]{2}$ sobre M es x^4-2. Cada automorfismo de $\mathcal{G}(L/M)$ está determinado por su valor en $\sqrt[4]{2}$, lo que combinado con el Corolario 2.6 implica que $\mathcal{G}(L/M)=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$ con

$$\sigma_1(\sqrt[4]{2})=\sqrt[4]{2}\qquad \sigma_2(\sqrt[4]{2})=i\sqrt[4]{2}\qquad \sigma_3(\sqrt[4]{2})=-\sqrt[4]{2}\qquad \sigma_2(\sqrt[4]{2})=-i\sqrt[4]{2}.$$

Como estos automorfismos dejan fijos M se cumple $\sigma_n(i)=i$, $n=1,2,3,4$. Obviamente $\sigma_1=\mathrm{Id}$ y algunos cálculos demuestran que $\sigma_3=\sigma_2^2$ y $\sigma_4=\sigma_2^3$. Simplemente para abreviar, escribamos σ en lugar de σ_2. Hemos demostrado

$$\mathcal{G}(L/M)=\langle\sigma\rangle=\{\mathrm{Id},\sigma,\sigma^2,\sigma^3\}\cong\mathbb{Z}/4\mathbb{Z}.$$

Todos estos elementos están en $\mathcal{G}(L/K)$, ya que $\mathcal{G}(L/M)$ es un subgrupo de $\mathcal{G}(L/K)$, como $[L:K]=8$ nos faltan otros cuatro automorfismos, que vamos a conseguir "extendiendo" un automorfismo de $\mathcal{G}(M/K)$.

La extensión M/K es normal, y por el Corolario 2.6 se tiene que $\mathcal{G}(M/K) = \{\mathrm{Id}, \mathrm{conj.}\}$ donde conj. es el automorfismo dado por la conjugación. La Proposición 2.5 asegura que podemos extender cada automorfismo de $\mathcal{G}(M/K)$ a $\mathcal{G}(L/K)$. Concretamente, existe $\tau \in \mathcal{G}(L/K)$ tal que $\tau|_M = \mathrm{conj.}$, esto es, $\tau(i) = -i$. La proposición no nos dice cuál es el valor de $\tau(\sqrt[4]{2})$ pero como sabemos que tiene que ser una raíz de $x^4 - 2$ (por el Corolario 2.6). Quizá componiendo con σ_2, σ_3 ó σ_4, podemos suponer que $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$ (por ejemplo, si $\tau(\sqrt[4]{2}) = -\sqrt[4]{2}$ tomaríamos $\widetilde{\tau} = \tau\sigma_3$ en lugar de τ). Con esto no sólo hemos conseguido un nuevo elemento de $\mathcal{G}(L/K)$ sino que también todos los productos de τ con los elementos ya calculados también estarán en $\mathcal{G}(L/K)$, concretamente

$$\langle \sigma, \tau \rangle \subset \mathcal{G}(L/K).$$

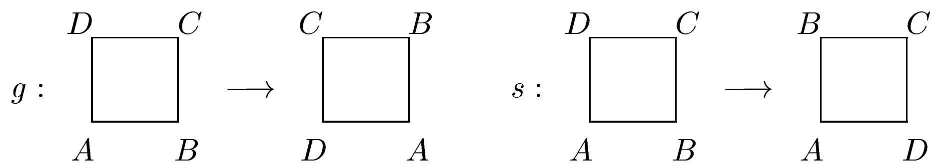
En particular se tiene que

$$\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \subset \mathcal{G}(L/K)$$

y como todos estos automorfismos son distintos y $[L : K] = 8$ se tiene que éste es el grupo de Galois

$$\mathcal{G}(L/K) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \cong D_8.$$

El último isomorfismo requiere alguna explicación. Recuérdese que D_8 es el grupo de movimientos del plano (giros y simetrías) que dejan fijo un cuadrado $ABCD$. El grupo D_8 está generado por el giro, g, de 90^o y la simetría, s, por una de las diagonales



Los grupos $\mathcal{G}(L/K)$ y D_8 son isomorfos porque σ puede identificarse con g y τ con s, ya que ambos son generadores de los grupos correspondientes con el mismo orden (cuatro y dos, respectivamente) y satisfacen la relación que caracteriza a D_8, que es $\tau\sigma = \sigma^3\tau$.

Para verificar las afirmaciones del párrafo anterior, es conveniente tener una tabla con la acción de todos los automorfismos de $\mathcal{G}(L/K)$ y sus órdenes. También será útil disponer de ella en el cálculo de los subgrupos de $\mathcal{G}(L/K)$, por ello la damos a continuación

$$\begin{array}{rccl@{\qquad\qquad}rccl}
 & i & \sqrt[4]{2} & & & i & \sqrt[4]{2} & \\
 & \downarrow & \downarrow & & & \downarrow & \downarrow & \\
\mathrm{Id}: & i & \sqrt[4]{2} & (\text{orden } 1) & \tau: & -i & \sqrt[4]{2} & (\text{orden } 2) \\
\sigma: & i & i\sqrt[4]{2} & (\text{orden } 4) & \sigma\tau: & -i & i\sqrt[4]{2} & (\text{orden } 2) \\
\sigma^2: & i & -\sqrt[4]{2} & (\text{orden } 2) & \sigma^2\tau: & -i & -\sqrt[4]{2} & (\text{orden } 2) \\
\sigma^3: & i & -i\sqrt[4]{2} & (\text{orden } 4) & \sigma^3\tau: & -i & -i\sqrt[4]{2} & (\text{orden } 2).
\end{array}$$

Para hallar los subcuerpos de L tenemos que calcular los subgrupos $\mathcal{G}(L/K)$. Los subgrupos de orden 2 de $\mathcal{G}(L/K)$ contienen un elemento de orden 2 y la identidad, y los subgrupos de orden 4 están generados por un elemento de orden 4 (si es que son $\cong \mathbb{Z}/4\mathbb{Z}$) o por dos de orden 2 que conmutan (si es que son $\cong \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$). Con estas observaciones y la tabla anterior, no es difícil comprobar que el retículo de subgrupos (diagrama de subgrupos indicando inclusiones) queda representado con el siguiente esquema

$$\begin{array}{ccccccccl}
 & & & \mathcal{G}(L/K) = \langle\sigma,\tau\rangle & & & & & \longrightarrow \text{ orden } 8\\
 & & / & | & \backslash & & & & \\
 & \langle\sigma^2,\tau\rangle & & \langle\sigma\rangle & & \langle\sigma^2,\sigma\tau\rangle & & & \longrightarrow \text{ orden } 4\\
/ & | & & \backslash|/ & & | & \backslash & & \\
\langle\sigma^2\tau\rangle & \langle\tau\rangle & & \langle\sigma^2\rangle & & \langle\sigma\tau\rangle & \langle\sigma^3\tau\rangle & & \longrightarrow \text{ orden } 2
\end{array}$$

Para mayor simplicidad hemos omitido el grupo trivial $\{\mathrm{Id}\}$ que está contenido en todos ellos.

Del esquema anterior deducimos que hay 8 subcuerpos, M, tales que $K \subsetneq M \subsetneq L$. Algunos de ellos dan lugar a extensiones normales de K y otros no. Por ejemplo, $\langle\sigma\rangle$ es un subgrupo normal de $\mathcal{G}(L/K)$ (un subgrupo de índice dos es siempre normal) y por tanto $\langle\sigma\rangle'$ es una extensión normal de $\mathbb{Q}$. Sin embargo, $\langle\tau\rangle$ no es un subgrupo normal de $\mathcal{G}(L/K)$ ya que $\sigma^{-1}\{\mathrm{Id},\tau\}\sigma \neq \{\mathrm{Id},\tau\}$, por tanto $\langle\tau\rangle'$ no es una extensión normal de $\mathbb{Q}$.

No es difícil comprobar que $\langle\sigma\rangle' = \mathbb{Q}(i)$ y $\langle\tau\rangle' = \mathbb{Q}(\sqrt[4]{2})$. Veamos, por ejemplo, la segunda igualdad

$$\langle\tau\rangle' = \{x \in L \,/\, \tau(x) = x\}.$$

Como $\{1, i\}$ y $\{1, \sqrt[4]{2}, \sqrt[4]{2^2}, \sqrt[4]{2^3}\}$ son bases de M/K y L/M, por los resultados del primer capítulo se obtiene una base de L/K multiplicando los elementos de estos dos conjuntos, así pues

$$x \in L \;\Rightarrow\; a + bi + c\sqrt[4]{2} + di\sqrt[4]{2} + e\sqrt[4]{2^2} + fi\sqrt[4]{2^2} + g\sqrt[4]{2^3} + hi\sqrt[4]{2^3}$$

con $a, b, c, d, e, f, g, h \in K$. como τ es la conjugación

$$\tau(x) = x \;\Leftrightarrow\; b = d = f = h = 0,$$

y se tiene

$$\langle\tau\rangle' = a + c\sqrt[4]{2} + e\sqrt[4]{2^2} + g\sqrt[4]{2^3} \,/\, a, c, e, g \in \mathbb{Q}\} = \mathbb{Q}(\sqrt[4]{2})$$

como habíamos afirmado.

<u>Ejemplo 3</u>. Calcular el grupo de Galois de $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

La extensión es normal. Consideramos

$$\begin{array}{c} L=\mathbb{Q}(\sqrt{2},\sqrt{3}) \\ | \\ M=\mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

Las extensiones $L/M = M(\sqrt{3})/M$ y $M/K = K(\sqrt{2})/K$ son normales de grado dos, de lo cual se deduce (ver Corolario 2.6)

$$\mathcal{G}(L/M) = \{\mathrm{Id}, \sigma\} \qquad \mathcal{G}(M/K) = \{\mathrm{Id}, \sigma'\}$$

donde σ y σ' son los automorfismos

$$\sigma : \sqrt{3} \longrightarrow \sqrt{3} \qquad \sigma' : \sqrt{2} \longrightarrow \sqrt{2}.$$

$\sigma \in \mathcal{G}(L/K)$, pero tenemos que extender σ' con la Proposición 2.5 para obtener un automorfismo de $\mathcal{G}(L/K)$. Sea $\tau \in \mathcal{G}(L/K)$ tal que $\tau|_M = \sigma'$. en principio τ podría enviar $\sqrt{3}$ a $\sqrt{3}$ ó $-\sqrt{3}$ (las raíces del polinomio mínimo de $\sqrt{3}$ sobre K), pero podemos suponer $\tau(\sqrt{3}) = \sqrt{3}$ porque si éste no fuera el caso consideraríamos $\sigma\tau$ en lugar de τ. Con ello tenemos que $\sigma, \tau \in \mathcal{G}(L/K)$ y

$$\sigma(\sqrt{3}) = -\sqrt{3}, \quad \sigma(\sqrt{2}) = \sqrt{2}, \qquad \tau(\sqrt{3}) = \sqrt{3}, \quad \tau(\sqrt{2}) = -\sqrt{2}.$$

Ahora podemos combinar estos automorfismos de todas las formas posibles , obteniéndose $\{\mathrm{Id}, \tau, \sigma, \tau\sigma\}$. Como $[L : K] = 4$ estos son todos los elementos de $\mathcal{G}(L/K)$. Es muy sencillo comprobar

$$\mathcal{G}(L/K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Como $\mathbb{Z}_2$ sólo tiene tres subgrupos propios, $\langle(\overline{0}, \overline{1})\rangle$, $\langle(\overline{1}, \overline{0})\rangle$, $\langle(\overline{1}, \overline{1})\rangle$, L/K sólo tienen tres subcuerpos propios que son $M_1 = \langle\tau\rangle'$, $M_2 = \langle\sigma\rangle'$, $M_3 = \langle\tau\sigma\rangle'$. Los dos primeros subcuerpos son $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt{2})$, respectivamente (ejercicio). Hallemos M_3

$$M_3 = \{x \in L \,/\, \tau\sigma(x) = x\}.$$

$\{1, \sqrt{2}\}$, $\{1, \sqrt{3}\}$ son bases de L/M y $M/K \Rightarrow \{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ es base de L/K, así pues

$$M_3 = \{x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \,/\, \tau\sigma(x) = x, \ a, b, c, d \in \mathbb{Q}\},$$

pero

$$\tau\sigma(x) = x \ \Leftrightarrow \ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{2}\sqrt{3}$$

lo que implica $b = c = 0$ y por tanto $M_3 = \mathbb{Q}(\sqrt{6})$.

<u>Ejemplo 4</u>. Hallar el grupo de Galois del cuerpo de descomposición de $P = x^3 - 2$ sobre $\mathbb{Q}$.

Las raíces de P son $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, donde $\omega = (-1+i\sqrt{3})/2$, así que el cuerpo de descomposición es $\mathbb{Q}(\omega, \sqrt[3]{2})$. Consideramos

$$\begin{array}{c} L = \mathbb{Q}(\omega, \sqrt[3]{2}) \\ | \\ M = \mathbb{Q}(\omega) \\ | \\ K = \mathbb{Q} \end{array}$$

entonces L/M y M/K son extensiones simples normales de grados 3 y 2 respectivamente. De nuevo, por el Corolario 2.6, se tiene

$$\mathcal{G}(L/M) = \{\mathrm{Id}, \sigma, \sigma^2\} \qquad \mathcal{G}(M/K) = \{\mathrm{Id}, \mathrm{conj.}\},$$

donde $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. Sea $\tau \in \mathcal{G}(L/K)$ tal que $\tau|M =$conj., entonces $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ ó $\omega\sqrt[3]{2}$ ó $\omega^2\sqrt[3]{2}$, pero siempre podemos suponer, quizá componiendo con σ ó σ^2, que ocurre el primer caso. Es decir,

$$\begin{array}{ll} \sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2} \qquad & \tau(\sqrt[3]{2}) = \sqrt[3]{2} \\ \sigma(\omega) = \omega & \tau(\omega) = \overline{\omega} = \omega^2. \end{array}$$

σ tiene orden 3 y τ tiene orden 2, multiplicando potencias de ambos obtenemos 6 automorfismos distintos que forman el grupo de Galois porque $[L:K] = 6$

$$\mathcal{G}(L/K) = \{\mathrm{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Es fácil comprobar que el grupo no es abeliano y que actúa sobre ω y $\sqrt[3]{2}$ como en la siguiente tabla

$$\begin{array}{rccl} & \omega & \sqrt[3]{2} & \\ & \downarrow & \downarrow & \\ \mathrm{Id}: & \omega & \sqrt[3]{2} & (\text{orden } 1) \\ \sigma: & \omega & \omega\sqrt[3]{2} & (\text{orden } 3) \\ \sigma^2: & \omega & \omega^2\sqrt[3]{2} & (\text{orden } 3) \end{array} \qquad \begin{array}{rccl} & \omega & \sqrt[3]{2} & \\ & \downarrow & \downarrow & \\ \tau: & \omega^2 & \sqrt[3]{2} & (\text{orden } 2) \\ \sigma\tau: & \omega^2 & \omega\sqrt[3]{2} & (\text{orden } 2) \\ \sigma^2\tau: & \omega^2 & \omega^2\sqrt[3]{2} & (\text{orden } 2) \end{array}$$

$\mathcal{G}(L/K)$ es isomorfo a D_6 (compruébese la relación $\tau\sigma = \sigma^2\tau$) que a su vez es isomorfo a S_3. Los subcuerpos propios son $M_1 = \langle\sigma\rangle'$, $M_2 = \langle\tau\rangle'$, $M_3 = \langle\sigma\tau\rangle'$ y $M_4 = \langle\sigma^2\tau\rangle'$. Se puede comprobar (ejercicio) que

$$M_1 = \mathbb{Q}(\omega), \qquad M_2 = \mathbb{Q}(\sqrt[3]{2}), \qquad M_3 = \mathbb{Q}(\omega\sqrt[3]{4}), \qquad M_4 = \mathbb{Q}(\omega\sqrt[3]{2}),$$

y que como $\langle\sigma\rangle$ es el único subgrupo normal, la única subextensión normal sobre K es M/K.

Sólo a modo ilustrativo, veamos un ejemplo en el que extender los automorfismos requiere alguna consideración más precisa.

Ejemplo 5. Hallar el grupo de Galois del cuerpo de descomposición de $P = x^4 - 2x^2 - 1$ sobre $\mathbb{Q}$.

Resolviendo la ecuación bicuadrada $P = 0$, se tiene que sus raíces son $\pm\sqrt{1+\sqrt{2}}$, $\pm\sqrt{1-\sqrt{2}}$, así que el cuerpo de descomposición es

$$L = \mathbb{Q}\big(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}\big).$$

Antes de nada, intetemos simplificar los generadores, para ello nótese que

$$\sqrt{1+\sqrt{2}} \cdot \sqrt{1-\sqrt{2}} = \sqrt{-1} = i,$$

por tanto, definiendo $\alpha = \sqrt{1+\sqrt{2}}$ se tiene que las raíces de P son $\alpha, -\alpha, i/\alpha, -i/\alpha$, y $L = \mathbb{Q}(\alpha, i)$. Obsérvese que α está en una extensión de grado 4 que contiene a $\sqrt{2}$, eso nos lleva a considerar

$$\begin{array}{c} L = \mathbb{Q}(i,\alpha) \\ | \\ M = \mathbb{Q}(i,\sqrt{2}) \\ | \\ \mathbb{Q}(i) \\ | \\ K = \mathbb{Q} \end{array}$$

donde todas las extensiones son de grado 2.

El polinomio mínimo de α en $\mathbb{Q}(\sqrt{2})$ es $x^2 - (1+\sqrt{2})$, así pues

$$\mathcal{G}(L/M) = \{\mathrm{Id}, \sigma\} \qquad \sigma(\alpha) = -\alpha.$$

Por otra parte, $\mathcal{G}(M/K)$ se puede calcular como en el ejemplo 3

$$\mathcal{G}(M/K) = \{\mathrm{Id}, \beta_1, \beta_2, \beta_1\beta_2\} \text{ con } \begin{array}{l} \beta_1(i) = -i \quad \beta_1(\sqrt{2}) = \sqrt{2} \\ \\ \beta_2(i) = i \quad \beta_2(\sqrt{2}) = -\sqrt{2}. \end{array}$$

Sean τ_1 y $\tau_2 \in \mathcal{G}(L/K)$ tales que $\tau_1|_M = \beta_1$ y $\tau_2|_M = \beta_2$. Como α está en una extensión de grado 4, su polinomio mínimo sobre $\mathbb{Q}$ es P, así pues se tiene que $\tau_i(\alpha) \in \{\alpha, -\alpha, i/\alpha, -i/\alpha\}$, $i = 1, 2$; es decir, que en principio τ_1 y τ_2 podrían tomar cuatro valores

* Es posible considerar otras extensiones, pero hemos elegido ésta porque en ella aparece de manera natural el problema de la extensión de automorfismos.

distintos, y componer con σ sólo permite pasar de uno de los valores a otro. Cuando sucede esto es que hay algunas extensiones de β_1 y β_2 que no son posibles, por ejemplo

$$\tau_2(\alpha) = \alpha \Rightarrow \tau_2(\alpha^2) = \alpha^2 \Rightarrow \tau_2(\sqrt{2}) = \sqrt{2}$$

lo que contradice $\tau_2|_M = \beta_2$. De la misma forma, $\tau_2(\alpha) = -\alpha$, $\tau_1(\alpha) = i/\alpha$, $\tau_1(\alpha) = -i/\alpha$, son imposibles, así pues $\tau_1(\alpha) \in \{\alpha, -\alpha\}$, $\tau_2(\alpha) \in \{i/\alpha, -i/\alpha\}$, y, quizá componiendo con σ, siempre podemos suponer $\tau_1(\alpha) = \alpha$ y $\tau_2(\alpha) = i/\alpha$. El grupo de Galois viene entonces dado por

$$\mathcal{G}(L/K) = \{\mathrm{Id}, \tau_1, \tau_2, \tau_1\tau_2, \sigma, \sigma\tau_1, \sigma\tau_2, \sigma\tau_1\tau_2\}.$$

Nótese que no es abeliano

$$\tau_1\tau_2(\alpha) = \tau_1(i/\alpha) = -i/\alpha \qquad \tau_2\tau_1(\alpha) = \tau_2(\alpha) = i/\alpha.$$

Aunque no lo haremos aquí, con un poco de trabajo se puede comprobar que $\mathcal{G}(L/K) \cong D_8$.

Concluimos esta sección calculando el grupo de Galois de la extensión ciclotómica $\mathbb{Q}(\zeta)/\mathbb{Q}$ donde $\zeta = e^{2\pi i/n}$.

El caso $n = p$ primo, es bastante sencillo.

Proposición 4.2 : *Si n es primo, $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}$ donde $\sigma_j : \zeta \longrightarrow \zeta^j$.*

<u>DEM.</u>: Claramente $\mathbb{Q}(\zeta)$ es el cuerpo de descomposición del polinomio ciclotómico $P = x^{n-1} + x^{n-2} + \ldots + 1$. Como P es irreducible y tiene a ζ como raíz, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = n - 1$, por tanto $|\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})| = n - 1$. Por otra parte es claro que $\sigma_j \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$, porque su efecto es enviar ζ a otra raíz, ζ^j, de P. ■

Extender el resultado anterior al caso general (n no necesariamente primo) no es en absoluto sencillo. Aquí sólo daremos una demostración suponiendo conocido el siguiente lema (su prueba puede encontrarse en "Elementos de álgebra abstracta" de A. Clark.

Lema 4.3 : *Si $n > 2$ entonces $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ donde ϕ es la función de Euler, $\phi(n) = n \prod_{p|n}(1 - p^{-1})$.*

Recuérdese que $\phi(n)$ da el número de enteros positivos menores que un número n y primos con él.

Proposición 4.4 : *Si $n > 2$, $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ está formado por los automorfismos $\sigma_j : \zeta \longrightarrow \zeta^j$ donde $1 \le j < n$ con j y n primos entre sí.*

Por ejemplo, como consecuencia se tendría

$$\mathcal{G}(\mathbb{Q}(e^{2\pi i/12})/\mathbb{Q}) = \{\sigma_1, \sigma_5, \sigma_7, \sigma_{11}\}.$$

Mediante la correspondencia $\sigma_j \mapsto \overline{j}$ podemos asignar de forma única a cada elemento del grupo de Galois de la proposición anterior un elemento invertible de $\mathbb{Z}/n\mathbb{Z}$. Además, como $\sigma_j\sigma_k \mapsto \overline{jk}$, se puede reformular el resultado como

Corolario 4.5: *Si $n > 2$, $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}_n^*$ donde $\mathbb{Z}_n^*$ es el grupo de unidades (elementos con inverso multiplicativo) del anillo $\mathbb{Z}/n\mathbb{Z}$.*

<u>DEM.(de la Proposición 4.4)</u>: En este caso, no podemos asegurar que el polinomio $P = x^{n-1} + x^{n-2} + \ldots + 1$ sea irreducible (de hecho no lo es si n no es primo). Como las raíces de P son $\zeta, \zeta^2, \ldots, \zeta^{n-1}$, lo único que podemos asegurar es

$$\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) \subset \{\sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}.$$

Si $\mathrm{mcd}(j,n) = d > 1$, entonces $\sigma_j \notin \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ ya que en ese caso $\sigma_j(\zeta^{n/d}) = e^{2\pi i j/d} = 1$, lo que es imposible porque $\zeta^{n/d} \neq 1$. Así pues

$$\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) \subset \{\sigma_j \,/\, \mathrm{mcd}(j,n) = 1\}.$$

Como $|\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})| = \phi(n)$ (por el lema) y el cardinal del segundo conjunto es también $\phi(n)$, entonces la inclusión debe ser una igualdad. ■

<u>Ejemplo 6</u>. Calcular $\mathcal{G}\big(\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}\big)$.

La relación $\cos\frac{2\pi}{17} = (\zeta + \zeta^{-1})/2$ con $\zeta = e^{2\pi i/17}$, sugiere calcular primero $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$, que según los resultados anteriores es

$$\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\mathrm{Id} = \sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_{16}\}.$$

Se reduce a unos cuantos cálculos comprobar que σ_3 genera todo el grupo, por ejemplo, $\sigma_8 = \sigma_3^{10}$ porque

$$\begin{aligned}\sigma_3(\zeta) = \zeta^3 \Rightarrow \sigma_3^2(\zeta) = \zeta^9 \Rightarrow \sigma_3^4(\zeta) &= \zeta^{81} = \zeta^{13}\\ \Rightarrow \sigma_3^{10}(\zeta) &= \sigma_3^4\big(\sigma_3^4(\sigma_3^2(\zeta))\big) = \zeta^{9\cdot 13\cdot 13} = \zeta^8.\end{aligned}$$

Así pues

$$\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \langle \sigma_3 \rangle \cong \mathbb{Z}_{16}.$$

Obsérvese que $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos\frac{2\pi}{17})] = 2$, así que $\mathbb{Q}(\cos\frac{2\pi}{17}) = H'$ donde H es un subgrupo de orden dos. Nótese que este subgrupo es normal porque $\mathbb{Z}_{16}$ es abeliano, por tanto (usando el teorema fundamental de la teoría de Galois) se tiene que la extensión $\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}$ es normal y que

$$\mathcal{G}\big(\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}\big) \cong \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})/H \cong \mathbb{Z}_8$$

De hecho, como podemos obtener automorfismos de $\mathcal{G}\big(\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}\big)$ restringiendo al subcuerpo $\mathbb{Q}(\cos\frac{2\pi}{17})$ los de $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$, (por ejemplo $\sigma_3 : \zeta \longrightarrow \zeta^3$ actúa sobre $\cos\frac{2\pi}{17} = (\zeta + \zeta^{-1})/2$ como $\sigma_3\big(\cos\frac{2\pi}{17}\big) = (\zeta^3 + \zeta^{-3})/2 = \cos\frac{6\pi}{17}$) se tiene

$$\mathcal{G}\big(\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}\big) \cong \langle \sigma \rangle \qquad \text{con } \sigma\big(\cos\frac{2\pi}{17}\big) = \cos\frac{6\pi}{17}.$$

1) ¿Cuáles son los automorfismos de $\mathbb{Q}$? ¿y los $\mathbb{R}$-homomorfismos (homomorfismos que dejan fijo $\mathbb{R}$) de $\mathbb{C}$ en $\mathbb{C}$?

2) Calcular $\mathcal{G}(\mathbb{Q}(x,y)/\mathbb{Q}(x+y,xy))$ y $\mathcal{G}(\mathbb{Q}(x,y,z)/\mathbb{Q}(x+y+z,xy+xz+yz,xyz))$ ($\mathbb{Q}(x,y)$ y $\mathbb{Q}(x,y,z)$ denotan los cuerpos de funciones racionales en dos y tres variables respectivamente).

***3)** Calcular $\mathcal{G}(\mathbb{Q}(x)/\mathbb{Q})$.

4) Recuérdese que el cuerpo de descomposición, L, de $P = x^2+x+1 \in \mathbb{F}_2[x]$ es un cuerpo de cuatro elementos. Hallar sus automorfismos y sus $\mathbb{F}_2$-automorfismos, es decir, $\mathcal{G}(L/\mathbb{F}_2)$.

5) Hallar el cuerpo de descomposición de $x^3-5 \in \mathbb{Q}[x]$.

6) Sea $P \in K[x]$ irreducible de grado tres, y sea L su cuerpo de descomposición. Demostrar que o bien $[L:K]=3$ o bien $[L:K]=6$.

7) Sea L el cuerpo de descomposición de $x^2+x-1 \in \mathbb{Q}[x]$. Hallar $\mathcal{G}(L/\mathbb{Q})$.

8) Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})\big)$, $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}(\sqrt{3})\big)$, $\mathcal{G}\big(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}\big)$.

9) Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt{5}+\sqrt{7})/\mathbb{Q}\big)$ poniendo especial cuidado en demostrar que realmente cada "posible" $\mathbb{Q}$-automorfismo en realidad lo es.

10) Sabiendo que $\mathcal{G}(\mathbb{Q}(\cos\frac{2\pi}{17})/\mathbb{Q}) = \{\mathrm{Id},\sigma,\sigma^2,\sigma^3,\sigma^4,\sigma^5,\sigma^6,\sigma^7\} \cong \mathbb{Z}/8\mathbb{Z}$ donde $\sigma\big(\cos\dfrac{2\pi}{17}\big) = \sigma\big(\dfrac{\zeta+\zeta^{-1}}{2}\big) = \dfrac{\zeta^3+\zeta^{-3}}{2}$ con $\zeta = e^{2\pi i/17}$, demostrar que $\cos\dfrac{2\pi k}{17} \in \mathbb{Q}(\cos\dfrac{2\pi}{17})$ y que $\sigma(\cos\dfrac{2\pi k}{17}) = \cos\dfrac{6\pi k}{17}$. Si $H = \{\mathrm{Id},\sigma^4\}$, comprobar que $H' \supset \mathbb{Q}(x_1,x_2)$ donde $x_1 = \cos\frac{2\pi}{17} + \cos\frac{26\pi}{17}$ y $x_2 = \cos\frac{2\pi}{17}\cdot\cos\frac{26\pi}{17}$. Demostrar que, de hecho, $H' = \mathbb{Q}(x_1,x_2)$.

11) Si L es el cuerpo de descomposición de $x^3+x^2+1 \in \mathbb{F}_2[x]$, demostrar que $L/\mathbb{F}_2$ es simple. (*Sugerencia*: Si α es un cero de este polinomio entonces α^2 también lo es).

12) Sabiendo que $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ con $\zeta = e^{2\pi i/7}$ está generado por el automorfismo $\sigma : \zeta \longrightarrow \zeta^3$, demostrar que $|\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})| = 6$ y encontrar los elementos de $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ que dejan fijo a $\zeta+\zeta^2+3\zeta^3+\zeta^4+3\zeta^5+3\zeta^6$.

13) Demostrar que $Y^n - x^n$ es irreducible en $K(x^n)[Y]$. Si además K es un subcuerpo de $\mathbb{C}$, demostrar que las funciones $\sigma_k : K(x) \longrightarrow \mathbb{C}(x)$ definidas por $\sigma_k\big(f(x)/g(x)\big) = f(e^{2k\pi i/n}x)/g(e^{2k\pi i/n}x)$, con $1 \le k \le n$, son homomorfismos y son los únicos que fijan $K(x^n)$.

14) Hallar $\mathcal{G}(\mathbb{Q}(x)/\mathbb{Q}(x^n))$, $\mathcal{G}(\mathbb{C}(x)/\mathbb{C}(x^n))$ y $\mathcal{G}(K(x)/K(x^{15}))$ con $K = \mathbb{Q}(e^{2\pi i/3})$, calculando en cada caso los cuerpos que quedan fijos por todos los automorfismos.

15) Demostrar que $K_1 = \mathbb{F}_2[x]/(x^3+x+1)$ y $K_2 = \mathbb{F}_2[x]/(x^3+x^2+1)$ son cuerpos de descomposición de $x^8-x \in \mathbb{F}_2[x]$. Concluir que K_1 y K_2 son isomorfos.

1) Si $K \subset M \subset L$ y $[L:K] < \infty$, demostrar

i) L/K normal $\Rightarrow$ L/M normal.

ii) L/K normal $\not\Rightarrow$ M/K normal.

iii) M/K, L/M normales $\not\Rightarrow$ L/K normal.

iv) L/K separable $\Rightarrow$ L/M separable.

v) M/K separable $\not\Rightarrow$ L/K separable.

2) Demostrar que dada una extensión finita M/K siempre existe un L, $L \supset M \supset K$ tal que L/K es normal. Al menor cuerpo con estas características se le llama <u>clausura normal</u> (o cierre normal) de M/K. Hallar la clausura normal de $\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}$.

3) Demostrar que toda extensión de grado dos es normal.

4) Estudiar si $\mathbb{Q}(x)/\mathbb{Q}(x^3)$ es normal.

5) Si L es el cuerpo de descomposición de $P \in K[x]$, demostrar que $[L:K] \big| (\partial P)!$.

6) Sea $L = \mathbb{F}_3(\sqrt[3]{x}, \sqrt[3]{y})$ y $K = \mathbb{F}_3(x,y)$. Demostrar que L/K es normal y $[L:K] = 9 < \infty$, pero existen infinitos subcuerpos intermedios $K \subset M \subset L$. ¿Por qué esto no contradice el teorema fundamental de la teoría de Galois?

7) Hallar una extensión separable y normal que no sea finita.

8) Probar que $P = x^6 + x^3 + 1$ es irreducible en $\mathbb{Q}[x]$ y utilizarlo para demostrar que la extensión $\mathbb{Q}(e^{2\pi i/9})/\mathbb{Q}$, es normal y de grado 6.

9) Si H y N son subgrupos de $\mathcal{G}(L/K)$ cuyos cuerpos fijos son $H' = L_1$ y $N' = L_2$, calcular $\langle \sigma, \tau \,\big/\, \sigma \in H,\ \tau \in N \rangle'$.

10) Recuérdese (Ej.5-2) que si $L = \mathbb{Q}(x,y,z)$ y $K = \mathbb{Q}(x+y+z, xy+xz+yz, xyz)$ entonces $\mathcal{G}(L/K) = S_3$. Demostrar que $\langle (1,2,3) \rangle' = K\big((x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\big)$.

1) Demostrar que si L es un cuerpo de descomposición de un polinomio sobre $\mathbb{Q}$ y $\mathcal{G}(L/\mathbb{Q})$ es abeliano, entonces $M/\mathbb{Q}$ es normal para todo subcuerpo M, $\mathbb{Q} \subset M \subset L$.

2) Hallar el grupo de Galois del cuerpo de descomposición de $P = (x^2-3)(x^2+3)$ sobre $\mathbb{Q}$, calculando los subcuerpos intermedios.

3) Lo mismo para $P = x^5 + 3x^3 - 3x^2 - 9$.

4) Lo mismo para $P = x^4 + 1$.

5) Lo mismo para $P = x^7 + 4x^5 - x^2 - 4$.

6) Calcular $\mathcal{G}(\mathbb{Q}(\sqrt{3+\sqrt{8}})/\mathbb{Q})$ y $\mathcal{G}(\mathbb{Q}(\sqrt{3+\sqrt{10}})/\mathbb{Q})$, hallando todas las subextensiones normales, $M/\mathbb{Q}$, de estas extensiones.

7) Sabiendo que $L/\mathbb{Q}$ es normal y $[L:\mathbb{Q}] = p$, hallar un grupo isomorfo a $\mathcal{G}(L/\mathbb{Q})$.

8) Si $\mathcal{G}(L/\mathbb{Q}) \approx \mathbb{Z}/pq\mathbb{Z}$ (donde p y q son primos distintos) con L/K normal, finita y separable, ¿cuántos subcuerpos, M, hay con $K \subset M \subset L$?

9) Demostrar que si $\mathbb{Q} \subset M \subset \mathbb{Q}(e^{2\pi i/k})$ $\mathcal{G}(M/\mathbb{Q})$ es abeliano.

10) Si n no es divisible por un cuadrado se cumple que $n \big| [\mathbb{Q}(e^{2\pi i/n^2}) : \mathbb{Q}]$. Demostrar que existe $\mathbb{Q} \subset M \subset \mathbb{Q}(e^{2\pi i/n^2})$ tal que $[\mathbb{Q}(e^{2\pi i/n^2}) : M] = n$.

11) Sabiendo que $\mathcal{G}(\mathbb{Q}(e^{2\pi i/257})/\mathbb{Q}) \approx \mathbb{Z}/256\mathbb{Z}$, demostrar que el polígono de 257 lados es construible con regla y compás.

4. Grupos finitos y cuerpos finitos

§1. Repaso de teoría de grupos.

La primera idea al incluir esta sección era recordar algunos de los conceptos y resultados más avanzados que se vieron el curso pasado, en particular los resultados de isomorfía que damos a continuación. A pesar de que sólo tendrán un papel auxiliar en algunas demostraciones del resto del curso, el lector debe saber y entender el primero de ellos y al menos recordar los dos siguientes. El último es de menor importancia.

Teorema del isomorfismo Si $\phi : G \longrightarrow G'$ es un homomorfismo de grupos, entonces $\operatorname{Nuc}\phi$ es un subgrupo normal de G y

$$G/\operatorname{Nuc}\phi \cong \operatorname{Im}\phi.$$

$1^{\underline{\text{er}}}$ **Teorema de isomorfía** Si $H \lhd G$, $N \lhd G$ y $N \subset H$, entonces

$$G/N\big/_{H/N} \cong G/H.$$

$2^{\underline{\text{o}}}$ **Teorema de isomorfía** Si $H \subset G$ y $N \lhd G$, entonces

$$HN/N \cong H/(H \cap N).$$

$3^{\underline{\text{er}}}$ **Teorema de isomorfía** Si $N_1 \lhd H_1 \lhd G$, $N_2 \lhd H_2 \lhd G$, entonces

$$N_1(H_1 \cap H_2)\big/_{N_1(H_1 \cap N_2)} \cong H_1 \cap H_2\big/_{(H_1 \cap N_2)(H_2 \cap N_1)}.$$

§2. Series de composición y grupos solubles.

El teorema fundamental de la teoría de Galois es un arma muy poderosa que permite traducir teoremas de teoría de grupos en teoremas de teoría de cuerpos. La principal motivación de Galois fue el estudio de la resolubilidad por radicales de ecuaciones algebraicas. En este estudio Galois encontró natural ir ampliando el cuerpo de partida con diferentes radicales hasta llegar al cuerpo de descomposición en el que la ecuación se resolvía. De alguna manera, él "factorizaba" el cuerpo de descomposición en ciertos subcuerpos que diferían uno de otro en un radical. Gracias al teorema fundamental de la teoría de Galois esto nos lleva al problema de "factorizar", en algún sentido, el grupo de Galois en ciertos subgrupos. En esta sección introduciremos notación y daremos ciertos resultados que ponen en rigor esta idea. Aunque se tratarán varios temas, lo único esencial para el estudio de la resolubilidad por radicales son las definiciones de grupo simple y soluble, las Proposiciones 2.4 y 2.5, y el Corolario 2.8.

Definición: *Sea G un grupo finito, se dice que una cadena de subgrupos de G*

$$\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_n = G$$

es una <u>serie normal</u> *si $G_{i-1} \lhd G_i$ para $i = 1, 2, \ldots, n$.*

OBSERVACIÓN: Recuérdese que $A \lhd B \lhd C \not\Rightarrow A \lhd C$, así que G_i no tiene por qué ser en general un subgrupo normal de G.

Ejemplo . $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

$$\{\overline{0}\} \subset \{\overline{0}, \overline{2}\} \subset \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

es una serie normal de G. También serie serie normal

$$\{\overline{0}\} \subset \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}.$$

Ejemplo . Para $D_8 = \langle \sigma, \tau \,/\, \sigma^4 = e,\ \tau^2 = e,\ \tau\sigma = \sigma^3\tau \rangle$, dos series normales serían

$$\{e\} \subset \langle \sigma \rangle \subset D_8 \qquad \{e\} \subset \langle \sigma^2 \rangle \subset \langle \sigma \rangle \subset D_8.$$

Los ejemplos anteriores sugieren que debiéramos definir algo así como la serie normal mayor, ese es el contenido de la siguiente definición

DEFINICIÓN: *Se dice que una serie normal de un grupo G*

$$\{e\} = G_0 \underset{\neq}{\subset} G_1 \underset{\neq}{\subset} G_2 \ldots \underset{\neq}{\subset} G_n = G,$$

es una serie de composición de G si no puede ampliarse, es decir, si para ningún $1 \le i \le n$ existe H tal que $G_{i-1} \lhd H \lhd G_i$.

Ejemplo . $\{\overline{0}\} \subset \mathbb{Z}_4$ no es una serie de composición de $\mathbb{Z}_4$ porque $H = \{\overline{0}, \overline{2}\}$ amplia esta serie normal.

Ejemplo . $\{\overline{0}\} \subset \mathbb{Z}_n$ es una serie de composición de $\mathbb{Z}_n \Leftrightarrow n = p$ primo. Porque si n no es primo existe un elemento distinto de $\overline{0}$ de orden menor que n y por tanto genera un subgrupo, H, $\{\overline{0}\} \underset{\neq}{\subset} H \underset{\neq}{\subset} \mathbb{Z}_n$. H es normal en $\mathbb{Z}_n$ porque $\mathbb{Z}_n$ es abeliano.

De alguna manera, hallar la serie de composición de un grupo es descomponerlo lo más posible. Guardando esta analogía, es natural pensar que existe algún resultado que afirme que la descomposición es única en algún sentido, ese es el contenido del teorema de Jordan-Hölder que damos a continuación

Teorema 2.1 (Jordan-Hölder): *Si tenemos dos series de composición para G*

$$\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_n = G$$
$$\{e\} = H_0 \subset H_1 \subset H_2 \ldots \subset H_m = G$$

entonces $n = m$ y los cocientes G_i/G_{i-1} H_i/H_{i-1} son isomorfos pero quizá apareciendo en distinto orden.

DEM.: Definiendo los grupos

$$\widetilde{G}_{qm+r} = G_q(G_{q+1} \cap H_r) \qquad \widetilde{H}_{qm+r} = H_q(H_{q+1} \cap G_r)$$

se tienen las siguientes series normales

$$\begin{array}{ccccccccccc} \{e\} = & \widetilde{G}_0 & \subset \widetilde{G}_1 \ldots \subset & \widetilde{G}_m & \subset \ldots \subset & \widetilde{G}_{2m} & \subset \ldots \subset & \widetilde{G}_{nm} & = G \\ & \| & & \| & & \| & & \| & \\ & G_0 & & G_1 & & G_2 & & G_m & \end{array}$$

y

$$\begin{array}{ccccccccccc} \{e\} = & \widetilde{H}_0 & \subset \widetilde{H}_1 \ldots \subset & \widetilde{H}_n & \subset \ldots \subset & \widetilde{H}_{2n} & \subset \ldots \subset & \widetilde{H}_{nm} & = G. \\ & \| & & \| & & \| & & \| & \\ & H_0 & & H_1 & & H_2 & & H_n & \end{array}$$

Usando el tercer teorema de isomorfía se puede demostrar (ejercicio) que los cocientes de la forma $\widetilde{G}_{um+v}/\widetilde{G}_{um+v-1}$ y $\widetilde{H}_{vn+u}/\widetilde{H}_{vn+u-1}$ son isomorfos, por tanto, las dos series normales anteriores tienen cocientes isomorfos (quizá en diferente orden). Por la definición de serie de composición en estas series todos los grupos están repetidos excepto $G_1, G_2, \ldots, G_m$ (en el primer caso) y $H_1, H_2, \ldots, H_m$ (en el segundo). Esto, y lo dicho anteriormente acerca de los cocientes, prueba el teorema. ■

Insistiendo en la analogía entre factorización y series de composición, los "grupos primos" serían los que responden a la siguiente definición

DEFINICIÓN: *Se dice que un grupo G es* simple *si no tiene subgrupos normales propios (distintos del trivial y de él mismo).*

NOTA: G simple $\Leftrightarrow$ $\{e\} \subset G$ es serie de composición.

En este contexto el siguiente resultado parece bastante natural

Proposición 2.2: *Una serie normal $\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_n = G$ es de composición $\Leftrightarrow$ G_i/G_{i-1} es simple, $i = 1, 2, \ldots, n$.*

DEM.: $\Rightarrow$) Si G_i/G_{i-1} no es simple $\Rightarrow \exists \widetilde{G}/G_{i-1} \lhd G_i/G_{i-1} \Rightarrow G_{i-1} \lhd \widetilde{G} \lhd G_i \Rightarrow$ no es serie de composición.

$\Leftarrow$) Si no es una serie de composición $\Rightarrow \exists \widetilde{G}\ G_{i-1} \lhd \widetilde{G} \lhd G_i \Rightarrow \widetilde{G}/G_{i-1} \lhd G_i/G_{i-1} \Rightarrow$ G_i/G_{i-1} no es simple. ■

Ahora daremos la definición central de este capítulo que es la de grupos solubles, intuitivamente son grupos que se pueden descomponer del todo

DEFINICIÓN: *Se dice que un grupo (finito), G, es* soluble *si tiene una serie de composición*

$$\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_n = G$$

de modo que $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$, *con* p_i *primo,* $i = 1, 2, \ldots, n$.

De la Proposición 2.2 se deducen condiciones menos restrictivas que aseguran que un grupo sea soluble, un ejemplo de ello es el siguiente resultado que algunos autores usan como definición de grupo soluble

Corolario 2.3: *G es soluble si y sólo si existe una serie de normal*

$$\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_n = G$$

de modo que G_i/G_{i-1} *es abeliano. En particular, todo grupo abeliano es soluble.*

A continuación damos los resultados que utilizaremos en el problema de la solubilidad por radicales

Proposición 2.4 : *Si G es soluble, $H \subset G$ también lo es.*

Proposición 2.5 : *Sea $N \triangleleft G$, entonces*

$$G \text{ soluble} \Leftrightarrow G/N \text{ y } N \text{ son solubles.}$$

Una definición que tiene bastante interés en teoría de grupos (gracias a los llamados “teoremas de Sylow”) es la siguiente

DEFINICIÓN: *Se dice que un grupo finito, G, es un $p-$grupo (con p primo) si su orden es una potencia de p.*

Ejemplo . D_8 y $\mathbb{Z}_9$ son $p-$grupos con $p = 2$ y $p = 3$ respectivamente.

Un importante (y nada fácil) resultado de teoría de grupos afirma: *Todo $p-$grupo de orden mayor que p tiene un subgrupo normal propio.* Conociendo este resultado, de la proposición anterior se puede deducir por inducción

Corolario 2.6: *Todo $p-$grupo es soluble.*

El otro resultado que utilizaremos el próximo capítulo es

Teorema 2.7 : *Una serie de composición para S_n viene dada por*

a) Si $n = 2 \quad \{e\} \subset S_2$.

b) Si $n = 3 \quad \{e\} \subset A_3 \subset S_3$.

c) Si $n = 4 \quad \{e\} \subset \langle(1,2)(3,4)\rangle \subset \langle(1,2)(3,4),(1,3)(2,4)\rangle \subset S_4$.

d) Si $n \geq 5 \quad \{e\} \subset A_n \subset S_n$.

Una formulación casi equivalente de este resultado es

Corolario 2.8: *A_n es simple para $n \geq 5$, y S_n es soluble $\Leftrightarrow n < 5$.*

Concluimos esta sección con las demostraciones de la proposiciones 2.4 y 2.5

Dem.(de la Proposición 2.4): G soluble implica que

$$\{e\} = G_0 \underset{\neq}{\subset} G_1 \underset{\neq}{\subset} G_2 \ldots \underset{\neq}{\subset} G_n = G,$$

es serie de composición con $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$.

Sea

$$\{e\} = G_0 \cap H \underset{\neq}{\subset} G_1 \cap H \underset{\neq}{\subset} G_2 \cap H \ldots \underset{\neq}{\subset} G_n \cap H = H,$$

entonces definiendo $H_i = G_i \cap H$, se tiene (utilícese el segundo teorema de isomorfía)

$$\frac{H_i}{H_{i-1}} \cong \frac{G_i \cap H}{G_{i-1} \cap H} \cong \frac{G_i \cap H}{G_{i-1} \cap (G_i \cap H)} \cong \frac{G_{i-1} \cdot (G_i \cap H)}{G_{i-1}}$$

y

$$\frac{G_{i-1} \cdot (G_i \cap H)}{G_{i-1}} \subset G_i/G_{i-1} \cong \mathbb{Z}_{p_i} \;\Rightarrow\; \frac{H_i}{H_{i-1}} \cong \mathbb{Z}_{p_i} \text{ ó } H_i = H_{i-1},$$

por tanto H es soluble. ■

Dem.(de la Proposición 2.5):

$\Rightarrow$) Por la Proposición 2.4 N es soluble. Si

$$\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_n = G,$$

es serie de composición con $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$. Del primer y segundo teorema de isomorfía se deduce (ejercicio) que

$$\{e\} = G_0N/N \subset G_1N/N \subset G_2N/N \ldots \subset G_nN/N = G/N,$$

es una serie normal para G/N en la que todos los factores de grupos sucesivos son cierto cociente de G_i/G_{i-1} y por tanto, cada factor es trivial o isomorfo a $\mathbb{Z}_{p_i}$.

$\Leftarrow$) De nuevo es un ejercicio con el primer teorema de isomorfía comprobar que si

$$\{e\} = N_0 \subset N_1 \subset N_2 \ldots \subset N_n = N \quad \{e\} = G_0/N \subset G_1/N \subset G_2/N \ldots \subset G_m/N = G/N$$

son series de composición con $N_i/N_{i-1} \cong \mathbb{Z}_{p_i}$ $(G_i/N)/(G_{i-1}/N) \cong \mathbb{Z}_{p_i'}$, entonces la serie

$$\{e\} = N_0 \subset N_1 \subset N_2 \ldots \subset N_n = N = G_0 \subset G_1 \subset G_2 \ldots \subset G_m = G$$

también tiene esa propiedad y por tanto G es soluble. ■

§3. Cuerpos finitos.

A pesar de que la teoría de Galois clásica se centra sobre extensiones finitas de $\mathbb{Q}$, no queremos terminar estas notas sin hacer una breve mención a la teoría en cuerpos finitos. Su estudio no es una abstracción innecesaria, ya que los cuerpos finitos aparecen de manera natural en geometría algebraica, teoría de códigos y teoría de números. En algún sentido, $\mathbb{Z}$ se puede considerar a veces como un "límite" de $\mathbb{F}_p$ y por ello no es del todo sorprendente su conexión con la aritmética.

Nótese que si L es un cuerpo finito, entonces su característica es positiva (porque $(L,+)$ es un grupo finito), y como ya mencionamos en su día, la característica (si no es nula) es siempre un número primo. El siguiente resultado limita el orden que puede tener un cuerpo finito

Proposición 3.1 : *Sea L un cuerpo finito de característica p, entonces $|L| = p^n$ para algún $n > 0$.*

<u>DEM.</u>: Si la característica es p, entonces la función

$$\begin{aligned} f : \mathbb{F}_p &\hookrightarrow L \\ \overline{x} &\hookrightarrow 1 + 1 + \overset{x \text{ veces}}{\cdots\cdots} + 1 \end{aligned}$$

es un monomorfismo, y por tanto L se puede considerar como una extensión de $\mathbb{F}_p$. Sea $b_1, b_2, \ldots, b_n$ con $n = [L : \mathbb{F}_p]$, una base de L sobre $\mathbb{F}_p$ (o si uno quiere ser muy riguroso, una base sobre $f(\mathbb{F}_p)$), entonces

$$L = \{\lambda_1 b_1 + \lambda_2 b_2 + \ldots \lambda_n b_n \,/\, \lambda_i \in \mathbb{F}_p\}$$

y L tiene tantos elementos como posibles valores de $\lambda_1, \lambda_2, \ldots, \lambda_n$, es decir, $|L| = p^n$. ■

El siguiente resultado nos da también una limitación sobre la estructura de un cuerpo finito

Proposición 3.2 : *Si L es un cuerpo finito con $|L| = q$, entonces el grupo multiplicativo, $L^* = L - \{0\}$ es cíclico e isomorfo a $\mathbb{Z}_{q-1}$.*

<u>DEM.</u>: $x \in L^* \to x^{q-1} = 1$ porque $|L^*| = |L - \{0\}| = q - 1$. Sea x_0 un elemento de orden máximo, n_0, en L^*. Entonces, como L^* es abeliano, el orden de cualquier elemento de L^* divide a n_0 (utilícese, por ejemplo, el teorema de estructura de grupos abelianos). Por tanto, para todo $x \in L^*$ se tiene $x^{n_0} = 1$, pero esto implica que el polinomio $x^{n_0+1} - x$ tiene $|L| = q$ soluciones, lo que implica que $n_0 + 1 \geq q$. Como L^* sólo tiene $q - 1$ elementos el orden de x_0 debe ser $n_0 = q - 1$, lo que prueba el resultado. ■

Con la siguiente definición vamos a introducir una generalización de los $\mathbb{F}_p$

DEFINICIÓN: *Se llama $\mathbb{F}_q$ con $q = p^n$ al cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$.*

El objetivo de esta sección es el siguiente resultado, que afirma que los $\mathbb{F}_q$ son los únicos cuerpos finitos y calcula el grupo de Galois de sus extensiones.

Teorema 3.3 : *Si L es un cuerpo finito de caracterísitca p, entonces L es isomorfo a $\mathbb{F}_q$ con $q = p^n = |L|$, además $\mathcal{G}(\mathbb{F}_q/\mathbb{F}_p)$ es un grupo cíclico de orden n generado por el automorfismo de Frobenius, $\phi : x \longrightarrow x^p$.*

<u>DEM.</u>: Como L^* es cíclico, todo elemento de x es raíz de $P = x^q - x \in \mathbb{F}_p[x]$ (aquí consideramos la "inclusión" $\mathbb{F}_p \hookrightarrow L$ de la primera demostración). como L tiene exactamente $q = \partial P$ elementos, L es (isomorfo) al cuerpo de descomposición de P sobre $\mathbb{F}_p$, esto es, a $\mathbb{F}_q$. Obsérvese que $L/\mathbb{F}_p \cong \mathbb{F}_q/\mathbb{F}_p$ es normal, finita y separable, por ser cuerpo de descomposición sobre $\mathbb{F}_p$, así pues

$$|\mathcal{G}(\mathbb{F}_q/\mathbb{F}_p)| = [L : \mathbb{F}_p] = n \qquad (\text{ porque } L = \{\lambda_1 b_1 + \lambda_2 b_2 + \dots \lambda_n b_n \,/\, \lambda_i \in \mathbb{F}_p\}),$$

por tanto basta probar que el automorfismo de Frobenius tiene orden mayor o igual que n. Obsérvese en primer lugar que realmente ϕ es un automorfismo, ya que es monomorfismo

$$\phi(x) = \phi(y) \Rightarrow x^p = y^p \Rightarrow (x-y)^p = 0 \Rightarrow x - y = 0$$

y como $\phi : L \longrightarrow L$ con L finito, monomorfismo $\Rightarrow$ epimorfismo. Además ϕ deja fijo $\mathbb{F}_p$ por el pequeño teorema de Fermat.

Para ver que ϕ tiene orden$\geq n$, sea x_0 generador de $\mathbb{F}_q^*$, entonces x_0 tiene orden $q-1$ y si el orden de ϕ es m, se tiene

$$x = \phi^m(x) = x^{p^m} \Rightarrow x^{p^m} = 1 \Rightarrow p^m - 1 \geq q - 1 = p^n - 1 \Rightarrow m \geq n$$

lo que concluye la demostración. ■

<u>Ejemplo 1</u>. $\mathcal{G}(\mathbb{F}_8/\mathbb{F}_2) = \{\mathrm{Id}, \phi, \phi^2\}$.

<u>Ejemplo 2</u>. Para calcular $\mathcal{G}(\mathbb{F}_{81}/\mathbb{F}_9)$, obsérvese que según el teorema $\mathcal{G}(\mathbb{F}_{81}/\mathbb{F}_3) = \{\mathrm{Id}, \phi, \phi^2, \phi^3\}$ y viendo la definición de $\mathbb{F}_9$ se observa que sólo ϕ^2 (y la identidad) dejan fijo a $\mathbb{F}_9$, por tanto $\mathcal{G}(\mathbb{F}_{81}/\mathbb{F}_9) = \{\mathrm{Id}, \phi^2\}$. En general $\mathcal{G}(\mathbb{F}_{p^{nk}}/\mathbb{F}_{p^k}) = \langle \phi^k \rangle$.

Hoja 8

1) Demostrar que no existe un epimorfismo $\phi : S_4 \longrightarrow \mathbb{Z}_7$ ni $\phi : S_4 \longrightarrow \mathbb{Z}_7^*$.

2) Calcular el orden de un grupo sabiendo que cuenta con menos de 100 elementos y contiene a un elemento de orden 10 y a otro de orden 14.

3) Hallar todos los subgrupos de D_6 (el grupo de movimientos del plano que dejan invariante el triángulo equilátero).

4) Demostrar que S_4 no tiene ningún subgrupo normal de orden 3.

5) Hallar un grupo, G, y dos subgrupos suyos, $H_1 \subset H_2 \subset G$ de manera que H_1 sea normal en H_2 y H_2 sea normal en G pero H_1 no sea normal en G.

6) Demostrar que $\mathbb{Z}_8^*$ no es cíclico.

7) Estudiar si las dos funciones siguientes son homomorfismos y en caso afirmativo decir de qué tipo

$$\phi_1 : S_4 \longrightarrow S_4 \quad \phi_1(\sigma) = \sigma^3 \qquad \phi_2 : \mathbb{Z}_7^* \longrightarrow \mathbb{Z}_7^* \quad \phi_2(\overline{x}) = \overline{x}^3.$$

8) Demostrar que un subgrupo de índice dos es siempre normal.

9) Demostrar que en S_n todo elemento de orden tres es producto de $3-$ciclos disjuntos.

10) El grupo de cuaterniones, Q, es un grupo de orden 8 no abeliano dado por

$$Q = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

donde a y b tienen orden 4 y se cumple $b^2 = a^2$ y $aba = b$. Demostrar que es soluble escribiendo explícitamente una cadena de subgrupos $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = Q$ con $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$.

11) Se puede demostrar que D_8 y Q son los únicos grupos no abelianos de orden 8. Ya sabemos que D_8 es isomorfo al grupo de Galois del cuerpo de descomposición de $x^4 - 2$ sobre $\mathbb{Q}$. Demostrar que Q no es el grupo de Galois cuerpo de descomposición de ningún polinomio de cuarto grado. *Sugerencia*: Demostrar que Q no es isomorfo a ningún subgrupo de S_4.

12) Sea un grupo de orden n, $G = \{g_1, g_2, \ldots, g_n\}$.

i) Dado $g \in G$, demostrar que $\alpha_g(g_i) = gg_i$ define una biyección en el conjunto G.

ii) Demostrar que $\phi : G \longrightarrow$ Biyecciones de G definido por $\phi(g) = \alpha_g$, es un homomorfismo de grupos.

iii) Concluir que G es isomorfo a un subgrupo de S_n (Teorema de Cayley).

13) Sean $\sigma_1, \sigma_2 \ldots, \sigma_n$ los polinomios simétricos elementales en las variables indeterminadas $x_1, x_2, \ldots, x_n$. Sabiendo que $\mathbb{Q}(x_1, x_2, \ldots, x_n)/\mathbb{Q}(\sigma_1, \sigma_2, \ldots, \sigma_n)$ es una extensión normal finita y separable con grupo de Galois isomorfo a S_n, demostrar, aplicando iii) del ejercicio anterior, que todo grupo finito es el grupo de Galois de alguna extensión.

<u>Nota</u>: Este resultado es todavía una conjetura si se pide que la extensión sea sobre $\mathbb{Q}$.

5. Resolubilidad por radicales

§1. El teorema de Galois

A lo largo de todo este capítulo supondremos que todos los cuerpos que aparecen son de característica cero. Esta hipótesis no es sólo una cuestión técnica para asegurar la separabilidad, se puede comprobar que el teorema de Galois no es cierto para algunas extensiones de $\mathbb{F}_p$.

Definición: *Se dice que una extensión finita, L/K es* radical *si los elementos de L se pueden expresar en términos de radicales, es decir, si existe una cadena de subcuerpos*

$$K = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n$$

tales que $L_n \supset L$ y $L_i = L_{i-1}\big(\sqrt[m_i]{\alpha_i}\big)$ con $\alpha_i \in L_{i-1}$, $i = 1, 2, \ldots, n$, donde $x = \sqrt[m_i]{\alpha_i}$ indica un elemento tal que $x^{m_i} = \alpha_i$.

Definición: *Se dice que un polinomio $P \in K[x]$ es* soluble por radicales *si su cuerpo de descomposición es una extensión radical de K.*

Obviamente en la definición de extensión radical siempre podemos suponer $L_i \neq L_{i-1}$. También, quizá introduciendo algunos cuerpos intermedios, podemos suponer que los m_i son primos ya que $\sqrt[pq]{z} = \sqrt[q]{\sqrt[p]{z}}$, es decir, $L_i = L_{i-1}\big(\sqrt[p_i]{\alpha_i}\big)$ con $L_i \neq L_{i-1}$. Nótese además que las raíces de $x^{p_1} - \alpha_1$ en su cuerpo de descomposición son de la forma $\zeta^\nu \sqrt[p_1]{\alpha_1}$ donde $\zeta = \sqrt[p_1]{1}$ es una raíz p_1-ésima de la unidad (i.e. una raíz $\zeta \neq 1$ de $x^{p_1} - 1$). Por tanto, quizá añadiendo un subcuerpo intermedio que contenga a ζ, se puede extender L_1 a L_1' con L_1'/K normal. De la misma manera, tomando raíces p_2-ésimas de los generadores de L_1' y de la unidad, L_2 se extiende, añadiendo radicales, a L_2' con L_2'/K normal, y así sucesivamente. En conclusión, se puede suponer que L_n/K es normal y contiene a las raíces p_i-ésimas de la unidad, $1 \le i \le n$.

Las raíces de la unidad tienen ciertas propiedades un tanto distintas de los otros radicales, por ello conviene considerarlas aparte. Nótese que todo lo dicho en el párrafo anterior se resume en el siguiente lema

Lema 1.1 : *Si L/K es finita y radical, entonces se tiene una sucesión de subcuerpos*

$$\widetilde{K} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n$$

donde $L_n \supset L$, L_n/K es normal, $L_i = L_{i-1}\big(\sqrt[p_i]{\alpha_i}\big)$ con $\alpha_i \in L_{i-1}$, p_i primo, $i = 1, 2, \ldots, n$, y $\widetilde{K}$ es el cuerpo generado por las raíces de la unidad (elementos del cuerpo de descomposición de $x^n - 1$) en L, en particular, $\widetilde{K}$ contiene todas las raíces p_i-ésimas de la unidad.

Gracias a los dos resultados siguientes, casi recíprocos, el teorema de Galois será una consecuencia del teorema fundamental de la teoría de Galois combinado con alguno de los resultado de teoría de grupos del capítulo anterior.

Lema 1.2 : *Con la notación e hipótesis del Lema 1.1, se tiene que L_i/L_{i-1} es normal y $\mathcal{G}(L_i/L_{i-1}) \cong \mathbb{Z}_{p_i}$.*

Lema 1.3 : *Si M_2/M_1 es normal y finita con $\mathcal{G}(M_2/M_1) \cong \mathbb{Z}_p$ entonces es radical.*

Veamos ahora el teorema central de este capítulo

Teorema 1.4 (de Galois): *Sea L/K normal y finita, entonces L/K es una extensión radical $\Leftrightarrow$ $\mathcal{G}(L/K)$ es un grupo soluble.*

Una formulación equivalente del teorema es

Corolario 1.5: *Un polinomio $P \in K[x]$ es soluble por radicales $\Leftrightarrow$ Su grupo de Galois sobre K es soluble.*

<u>Observación</u>: Recuérdese que siempre estamos bajo la hipótesis $\operatorname{char} K = 0$, en otro caso estos resultados no son ciertos.

<u>Nota</u>: Recuérdese también que, con cierto abuso de notación, se llama grupo de Galois de un polinomio al grupo de Galois de su cuerpo de descomposición.

<u>Dem.(del Teorema de Galois)</u>: Las dos implicaciones se reducen a usar el teorema fundamental de la teoría de Galois para pasar la información acerca de los subcuerpos a los subgrupos y viceversa.

$\Leftarrow$) Si $\mathcal{G}(L/K)$ es soluble, entonces se tiene

$$\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_n = \mathcal{G}(L/K)$$

con $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$, $i = 1, 2, \ldots, n$. Por el teorema fundamental de la teoría de Galois

$$L = G_0' \supset G_1' \supset G_2' \ldots \supset G_n' = K$$

con $\mathcal{G}(G_{i-1}'/G_i') \cong \mathbb{Z}_{p_i}$ (porque $\left|\mathcal{G}(G_{i-1}'/G_i')\right| = [G_i : G_{i-1}] = p_i$), y el Lema 1.3 implica que G_{i-1}'/G_i' es radical y, por tanto, L/K también.

$\Rightarrow$) Por el Lema 1.1 se tiene

$$\widetilde{K} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n.$$

Por el teorema fundamental de la teoría de Galois esto se traduce en la sucesión de subgrupos

$$\{e\} = \mathcal{G}(L_n/L_n) \subset \mathcal{G}(L_n/L_{n-1}) \subset \mathcal{G}(L_n/L_0) = \mathcal{G}(L_n/\widetilde{K}).$$

Aplicando la segunda parte del teorema fundamental y el Lema 1.2, se tiene

$$\mathcal{G}(L_n/L_{i-1})/\mathcal{G}(L_n/L_i) \cong \mathcal{G}(L_i/L_{i-1}) \cong \mathbb{Z}_{p_i},$$

por tanto $\mathcal{G}(L_n/\widetilde{K})$ es soluble.

L/K y $\widetilde{K}/K$ son normales ($\widetilde{K}/K$ es el cuerpo de descomposición de varios polinomios de la forma $x^n - 1$), por tanto,

$$\mathcal{G}(L/K) \cong \mathcal{G}(L_n/K)/\mathcal{G}(L_n/L) \quad \text{y} \quad \mathcal{G}(L_n/K)/\mathcal{G}(L_n/\widetilde{K}) \cong \mathcal{G}(\widetilde{K}/K),$$

y gracias a las Proposición 2.4 y 2.5 del capítulo anterior sólo resta demostrar que $\mathcal{G}(\widetilde{K}/K)$ es soluble para concluir que $\mathcal{G}(L_n/K)$ y $\mathcal{G}(L_n/L)$, y por tanto $\mathcal{G}(L/K)$, lo son. Pero nótese que $\widetilde{K}$ es el cuerpo generado por las raíces de la unidad y por tanto $\mathcal{G}(\widetilde{K}/K)$ es abeliano (porque $\sigma,\tau \in \mathcal{G}(\widetilde{K}/K)$, $\zeta \in \widetilde{K}$ raíz de la unidad $\Rightarrow \sigma(\zeta)=\zeta^r$, $\tau(\zeta)=\zeta^s \Rightarrow \sigma\tau(\zeta)=\tau\sigma(\zeta)=\zeta^{rs}$) y en particular es soluble. ■

Terminamos dando las demostraciones de los dos lemas que hemos utilizado

<u>Dem.(del Lema 1.2)</u>: L_i/L_{i-1} es simple, así que todo automorfismo está determinado por su acción sobre $x = \sqrt[p_i]{\alpha_i}$. Las otras raíces del polinomio mínimo de x sobre L_{i-1} serán de la forma ζx donde $\zeta \neq 1$ es una raíz de $x^{p_i}-1$; $\zeta \in \widetilde{K} \subset L_{i-1} \Rightarrow \zeta x \in L_i$ y por tanto L_i/L_{i-1} es normal. Además todo automorfismo $\phi(x)=\zeta x$ tiene orden p_i y es obvio que $[L_i : L_{i-1}] \le p_i$, por tanto $\mathcal{G}(L_i/L_{i-1}) = \langle\phi\rangle \cong \mathbb{Z}_{p_i}$. ■

<u>Dem.(del Lema 1.3)</u>: Como $[M_2 : M_1] = p$, debe cumplirse $M_2 = M_1(x)$ para cualquier $x \in M_2 - M_1$. Supongamos primero que existe $\zeta \in M_1$ tal que $\zeta^p = 1$, $\zeta \neq 1$. Consideremos

$$x_1 = x + \zeta\phi(x) + \zeta^2\phi^2(x) + \ldots + \zeta^{p-1}\phi^{p-1}(x)$$

donde ϕ es el generador de $\mathcal{G}(M_2/M_1)$, entonces

$$\begin{aligned} \phi(x_1) = \zeta^{p-1}x_1 \;\Rightarrow\; x_1 \notin M_1 \;\Rightarrow\; M_2 = M_1(x_1) \\ \phi(x_1^p) = \big(\phi(x_1)\big)^p = x_1^p \;\Rightarrow\; x_1^p \in M_1, \end{aligned}$$

por tanto $x_1 = \sqrt[p]{\alpha}$ con $\alpha \in M_1$ y $M_2 = M_1(\sqrt[p]{\alpha})$.

Si $\zeta \notin M_1$ y $\zeta \in M_2$ entonces $M_2 = M_1(\zeta) = M_1(\sqrt[p]{1})$. Finalmente, si $\zeta \notin M_1, M_2$, $\mathcal{G}\big(M_2(\zeta)/M_1(\zeta)\big) \cong \mathcal{G}(M_2/M_1)$ por restricción de los automorfismos a M_2 y se aplicaría la primera parte de la demostración para concluir $M_2(\zeta) = M_1(\zeta)(\sqrt[p]{\alpha})$, y $M_2(\zeta)/M_1(\zeta)$, $M_1(\zeta)/M_1$ radicales implica M_2/M_1 radical. ■

§2. Algunas aplicaciones

En esta sección veremos algunas aplicaciones a problemas clásicos de las ideas que rodean al teorema de Galois. La primera es la más conocida y afirma que no existe una fórmula general con radicales para resolver todas las ecuaciones de un grado dado, $n \ge 5$. Esto cierra el problema de la solubilidad por radicales de las ecuaciones algebraicas, ya que desde el siglo XVI se conocen fórmulas para tratar los casos $n \le 4$.

Teorema 2.1 (Abel): *No existe ninguna extensión radical del cuerpo generado por los coeficientes de la ecuación general de grado $n \ge 5$ que contenga a sus raíces.*

<u>Dem.</u>: Sea la ecuación

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 = 0$$

con coeficientes variables indeterminadas $a_0, a_1, a_2, \ldots, a_{n-1}$. Si las raíces de este polinomio son $x_1, x_2, \ldots, x_n$, queremos demostrar que $K(x_1, x_2, \ldots, x_n)/K(a_{n-1}, a_{n-2}, \ldots, a_0)$ no es radical. Pero se tiene

$$\mathcal{G}\big(K(x_1, x_2, \ldots, x_n)/K(a_{n-1}, a_{n-2}, \ldots, a_0)\big)=\mathcal{G}\big(K(x_1, x_2, \ldots, x_n)/K(\sigma_1, \sigma_2, \ldots, \sigma_n)\big)\cong S_n$$

porque $a_{n-i} = (-1)^i\sigma_i(x_1, x_2, \ldots, x_n)$, donde σ_i son los polinomios simétricos elementales, y es evidente que $K(\sigma_1, \sigma_2, \ldots, \sigma_n)$ es invariante sólo por las permutaciones de las n variables $x_1, x_2, \ldots, x_n$. Por el Corolario 2.8 del capítulo anterior se tiene que S_n no es soluble si $n \geq 5$ y el resultado se deduce del teorema de Galois. ∎

Nótese que el resultado anterior afirma que no existe una fórmula con radicales que sirva para resolver todas las ecuaciones de grado n cuando $n \geq 5$, pero es obvio que hay algunas que se pueden resolver con radicales (por ejemplo $x^5 - a = 0$). Galois no dio ningún ejemplo de una ecuación que no fuera soluble por radicales. Esto no debiera extrañarnos, porque calcular el grupo de Galois del cuerpo de descomposición de un polinomio es en general muy difícil. Sin embargo, en el siguiente resultado emplearemos algunos artificios de teoría de grupos para simplificar este cálculo en un ejemplo explícito.

Proposición 2.2: *Sea L el cuerpo de descomposición de $P = x^5 - 6x + 3 \in \mathbb{Q}[x]$, entonces $L/\mathbb{Q}$ no es una extensión radical, es decir, las soluciones de $P = 0$ no pueden expresarse mediante radicales.*

DEM.: P es irreducible por el criterio de Eisenstein y tiene tres raíces reales y dos complejas conjugadas (dibújese la gráfica del polinomio), así pues $\tau = \text{conj.} \in \mathcal{G}(L/\mathbb{Q})$. Como los elementos de $\mathcal{G}(L/\mathbb{Q})$ permutan las cinco raíces se tiene que $\mathcal{G}(L/\mathbb{Q}) \hookrightarrow S_5$ (monomorfismo) y τ (que intercambia dos raíces) corresponde a una trasposición. Si α es raíz de P, $5 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \Rightarrow 5\big||\mathcal{G}(L/\mathbb{Q})|$, y un teorema de teoría de grupos (Teorema de Cauchy) implica que si p divide al orden de un subgrupo, H, de S_p entonces H contiene un $p-$ciclo. Finalmente, un $5-$ciclo y una trasposición cualesquiera generan todo S_5 (ejercicio), así pues $\mathcal{G}(L/\mathbb{Q}) \cong S_5$ que no es un grupo soluble. ∎

De la teoría del segundo capítulo se deduce que si L es una extensión real y finita de $\mathbb{Q}$ que sólo contine elementos construibles), entonces $[L : \mathbb{Q}] = 2^k$. Si $L/\mathbb{Q}$ es normal, usando las ideas de la prueba del teorema de Galois se puede demostrar el recíproco, concretamente

Proposición 2.3: *Si $\mathbb{Q} \subset L \subset \mathbb{R}$ y $L/\mathbb{Q}$ es normal, entonces $[L : \mathbb{Q}] = 2^k \Leftrightarrow$ Los elementos de L son construibles con regla y compás.*

DEM.: Como $[L : \mathbb{Q}] = 2^k$, $\mathcal{G}(L/\mathbb{Q})$ es un $2-$ grupo. Por el Corolario 2.6 del capítulo anterior

$$\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_k = \mathcal{G}(L/\mathbb{Q})$$

con $G_i/G_{i-1} \cong \mathbb{Z}_2$. Por el teorema fundamental de la teoría de Galois

$$L = G_0' \supset G_1' \supset G_2' \ldots \supset G_k' = \mathbb{Q}$$

con $[G'_{i-1} : G_i] = 2$, lo que prueba el resultado. ■

<u>OBSERVACIÓN</u>: Si $L/\mathbb{Q}$ no es normal el resultado puede no ser cierto. Por ejemplo, si α es la raíz real y positiva de $P = x^4 - 10x^3 + 26x^2 + 16x - 14$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = 2^2$, y sin embargo α no es construible con regla y compás, ya que se puede probar que el grupo de Galois de P es A_4 que no tiene subgrupos de orden 6 y por tanto $\mathbb{Q}(\alpha)/\mathbb{Q}$ no tiene subcuerpos intermedios propios.

En el tercer capítulo enunciamos que $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \phi(n)$ donde ϕ es la función de Euler (recuérdese que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ con p_i primos distintos, entonces $\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_n^{\alpha_n - 1}(p_n - 1)$, en particular $\phi(p) = p - 1$). De este resultado y de la Proposición 2.3 se deduce el siguiente bellísimo teorema de Gauss, quien lo enunció en el último artículo de su obra maestra "*Disquisitiones Arithmeticae*" 30 años antes de que Galois diera sus teoremas. Aunque Gauss afirmó tener una prueba completa y rigurosa de su resultado, sólo ha llegado hasta nosotros la demostración que dio de una de las implicaciones (la difícil desde el punto de vista actual). Para el autor de estas notas éste es el teorema más bello que ha visto nunca en Matemáticas

Corolario 2.4 (GAUSS): *El polígono regular de n lados es construible con regla y compás si y sólo si $n = 2^k p_1 p_2 \dots p_n$ con p_i primos de Fermat distintos.*

<u>NOTA</u>: Para el que desconozca su definición, se llama <u>primos de Fermat</u> a aquellos de la forma $2^{2^m} + 1$, en honor a Fermat, quien pensó erróneamente que $2^{2^m} + 1$ era primo para todo $m \in \mathbb{N}$. El primer contraejemplo ocurre para $m = 5$.

<u>Ejemplo 1</u>. El polígono de 15 lados es construible porque

$$15 = 3 \cdot 5 = (2^{2^0} + 1)(2^{2^1} + 1).$$

<u>Ejemplo 2</u>. El polígono de 380 lados no es construible porque

$$15 = 2^2 \cdot 5 \cdot 19 \qquad \text{y } 5 = 2^{2^1} + 1, \text{ pero } 19 \neq 2^{2^m} + 1.$$

<u>Ejemplo 3</u>. El polígono de 289 lados no es construible porque

$$289 = 17 \cdot 17 \qquad 17 = 2^{2^2} + 1.$$

pero no son primos de Fermat distintos.

Hoja 9

1) Sea G soluble de orden $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, si $\{e\} = G_0 \subset G_1 \subset \dots \subset G_N = G$ con G_i subgrupo normal de G_{i+1} (i.e. es una serie normal) y G_{i+1}/G_i abeliano no trivial, demostrar que $N \leq \alpha_1 + \alpha_2 + \dots + \alpha_n$.

2) Demostrar que $\mathbb{Z}_2 \times S_3$ es soluble. (Recuérdese que $\mathbb{Z}_2 \times S_3 = \{(\overline{x}, \sigma) \,/\, \overline{x} \in \mathbb{Z}_2,\ \sigma \in S_3\}$ con la operación $(\overline{x_1}, \sigma_1) \cdot (\overline{x_2}, \sigma_2) = (\overline{x_1 + x_2}, \sigma_1\sigma_2)$)

3) Un teorema demostrado por Sylow implica que si $p \big| |G|$, p =primo, entonces existe un monomorfismo $\phi : G_p \longrightarrow G$ donde G_p es un $p-$grupo (grupo de orden p^n, $n \geq 1$). Sabiendo este resultado y que todo $p-$grupo es soluble, demostrar el Teorema de Cauchy: "Si p primo divide al orden de un grupo, entonces existe un elemento de orden p".

4) Demostrar que el grupo aditivo de $\mathbb{F}_{p^n}$ es $\mathbb{Z}_p \times \overset{n \text{ veces}}{\dots} \times \mathbb{Z}_p$.

5) Si L es el cuerpo de descomposición de $x^3 + x^2 - 2 \in \mathbb{F}_3[x]$, hallar $\mathcal{G}(L/\mathbb{F}_3)$.

6) Estudiar si el polinomio $x^2 + x + 1$ es irreducible en $\mathbb{F}_2[x]$ y en $\mathbb{F}_8[x]$.

7) Halar todos los generadores del grupo $\mathcal{G}(\mathbb{F}_{256}/\mathbb{F}_4)$.

8) ¿Cuántos subcuerpos hay entre $\mathbb{F}_4$ y $\mathbb{F}_{256}$?

9) ¿Cuál es el cuerpo de descomposición de $(x^9 - x)(x^{27} - x) \in \mathbb{F}_3[x]$?