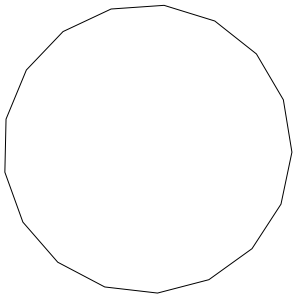
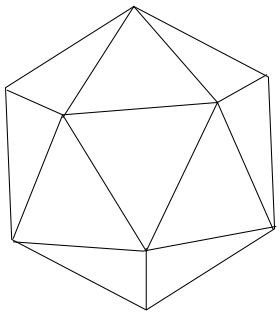
¡Qué bonita es la teoría de Galois!

Álgebra II. Tercero de Matemáticas.



Gauss



Abel

Galois

Lorente Fernando
2004/2005
Cozimah

Álgebra II reloaded

Esto será en el futuro un prefacio. Por ahora, hasta que no finalice el curso, no puedo decir más que generalidades. Entre ellas, la más relevante es que estas notas están basadas en otras que escribí de la asignatura homónima los cursos 1995/96 y 1996/97, disponibles en la página `http://www.uam.es/fernando.chamizo` (en mi "segunda vivienda").

Evidentemente, el cambio de título indica que ha habido modificaciones sustanciales desde entonces. La más notable se debe a que la parte de teoría de anillos que ha perdido Álgebra I, ahora pertenece a la asignatura que nos ocupará, por ello hay un primer capítulo totalmente nuevo. También se han añadido gran cantidad de ejercicios, algunos ejemplos, observaciones, apéndices y tonterías. En fin, nada que me haya servido para nada más que fabricarme un trocito de pasado.

Acabo estas breves líneas agradeciendo a Carlos Vinuesa (estudiante y cinéfilo) la revisión profunda que hizo de muchas secciones de la antigua versión de las notas. En reconocimiento he puesto a este prefacio provisional el título de uno de sus mensajes. Dicho sea de paso, el capítulo de agradecimientos está abierto, y ruego a los que tengan ánimo y ganas de investigar erratas, fallitos y errores vergonzantes, que me los comuniquen para incorporar los cambios pertinentes a estos apuntes.

Madrid, febrero de 2004

Prefacio

Estos apuntes reflejan los contenidos de un curso típico de teoría de Galois con un capítulo inicial de teoría de anillos. Hay muchos y buenos libros sobre el tema, especialmente el de I. Stewart *Galois Theory*. La única débil publicidad que puedo hacer a mis apuntes es su precio (igual en pesetas que en euros) y que se ajustan bien al temario real de la asignatura. Respecto a su estructura, hay cuatro capítulos, cada uno complementado con una colección de ejercicios y con un apéndice de curiosidades, consejos y tonterías. Los pocos ejercicios señalados por la leyenda correspondiente como "muy difíciles", realmente lo son, posiblemente incluso para los alumnos más aventajados. Los identificados como "opcionales" no son necesariamente complicados pero no están relacionados con el centro del curso. A veces lo están con material complementario escrito en letra pequeña.

Avanzo que no habrá grandes cambios con respecto a la versión de estos apuntes escrita el curso pasado. Si alguien dispone de una copia de ellos, puede aprovecharla por el bien de nuestros bosques. En ese caso, consúltese en la página de la asignatura `http://www.uam.es/fernando.chamizo` la lista de erratas detectadas. Allí también se pueden obtener los presentes apuntes corregidos, capítulo a capítulo.

Tras la experiencia del curso pasado, lo más posible es que la materia tal como se presenta en clase, sufra algunas reducciones con respecto a lo aquí escrito. La última sección se puede suprimir totalmente, y las otras dos secciones del cuarto capítulo presentarse con reducciones en los detalles técnicos. Especialmente la primera, ya que la teoría de grupos es un medio pero no un fin por sí mismo en este curso.

Madrid, febrero de 2005

Contenidos

La teoría de Galois en menos de cincuenta minutos

La idea genial bajo la teoría de Galois es que se pueden representar ciertos conjuntos asociados a la solución de ecuaciones algebraicas mediante grupos de simetrías. Esta frase es tan lapidaria como incomprensible. Afortunadamente todavía podemos utilizar los 49 minutos 50 segundos restantes para tratar de clarificarla un poco.

Comencemos resolviendo la ecuación general de segundo grado $x^2 + bx + c = 0$. Considerando sus raíces r_1 y r_2 como variables arbitrarias, los coeficientes b y c vienen dados por funciones polinómicas simétricas de ellas:

$$x^2 + bx + c = (x - r_1)(x - r_2) \;\Rightarrow\; b = b(r_1, r_2) = -r_1 - r_2, \quad c = c(r_1, r_2) = r_1 r_2.$$

La fórmula para resolver la ecuación (hallar r_1 y r_2 a partir de b y c) es $(-b+\sqrt{b^2-4c})/2$ donde el radical no es una verdadera función univaluada, sino que hay que asignarle dos valores, uno con más y otro con menos. Este radical obra el milagro de pasar de una función simétrica en r_1 y r_2, concretamente $b^2 - 4c = (r_1 + r_2)^2 - 4r_1 r_2$, a dos funciones no simétricas, $\sqrt{b^2 - 4c} = \pm(r_1 - r_2)$.

En la ecuación de tercer grado $x^3 + bx^2 + cx + d = 0$, de nuevo b, c y d se pueden considerar como funciones simétricas en las variables r_1, r_2 y r_3 que representan las raíces:

$$b = -r_1 - r_2 - r_3, \qquad c = r_1 r_2 + r_1 r_3 + r_2 r_3 \quad \text{y} \quad d = -r_1 r_2 r_3.$$

La fórmula para resolver la ecuación es en este caso bastante más complicada y se puede escribir como:

$$-\frac{b}{3} + \frac{t}{3} + \frac{b^2 - 3c}{3t} \qquad \text{con} \quad t = \sqrt[3]{E}$$

donde

$$E = \frac{9bc - 2b^3 - 27d + \sqrt{D}}{2} \qquad \text{y} \qquad D = (9bc - 2b^3 - 27d)^2 + 4(3c - b^2)^3.$$

En resumidas cuentas, la resolución de la ecuación pasa por hallar primero una raíz cuadrada de D y después otra cúbica (trivaluada) de E. Si tuviéramos tiempo y paciencia para sustituir b, c y d en términos de las raíces veríamos que

$$D = -27(r_1 - r_2)^2 (r_1 - r_3)^2 (r_2 - r_3)^2 \qquad \text{y} \qquad E = (r_1 + \zeta r_2 + \zeta^2 r_3)^3,$$

donde ζ es una raíz cúbica no trivial de la unidad, esto es, $\zeta = (-1 \pm i\sqrt{3})/2$.

De nuevo observamos la pérdida de simetrías por medio de los radicales: D es una función simétrica en r_1, r_2 y r_3, mientras que $\sqrt{D}$ no lo es, aunque perduran algunas simetrías, por ejemplo, $\sqrt{D}$ es invariante al cambiar $(r_1, r_2, r_3) \mapsto (r_2, r_3, r_1)$. También E goza de estas simetrías de $\sqrt{D}$ pero al extraer la raíz cúbica se pierden todas ellas.

Para resolver la ecuación de cuarto grado la fórmula es muchísimo más compleja. En una de las maneras de escribirla, primero hay que hacer una raíz cuadrada $\sqrt{F}$, después una raíz cúbica $\sqrt[3]{G}$, y luego dos raíces cuadradas más $\sqrt{H}$ y $\sqrt{I}$. Al expresar todo en

términos de las variables r_1, r_2, r_3 y r_4 que representan las raíces, el fenómeno de pérdida de simetrías se repite, desde F que las tiene todas, hasta $\sqrt{I}$ que no tiene ninguna.

Volvamos al caso de segundo grado. Consideremos el conjunto K_0 de todas las expresiones (fórmulas) que se pueden obtener a partir de b y c haciendo sumas, restas, multiplicaciones y divisiones, por ejemplo $b/(c^2-b)+b^2 \in K_0$, y $K_0\big(\sqrt{b^2-4c}\big)$ definido de igual manera pero permitiendo también operar con $\sqrt{b^2-4c}$. Se tiene $b, c \in K_0$ y $r_1, r_2 \in K_1 = K_0\big(\sqrt{b^2-4c}\big)$, de forma que el paso de K_0 a K_1 representa resolver la ecuación. Como las funciones de K_0 son invariantes al permutar sus dos variables (r_1 y r_2), diremos que su grupo de simetrías es S_2, mientras que las funciones de K_1 no son en general simétricas de ningún modo y por tanto le asignaremos el grupo trivial de simetrías $\{\mathrm{Id}\}$. En un esquema:

$$\begin{array}{lcl} K_0 & \longrightarrow & K_1 = K_0\big(\sqrt{b^2-4c}\big) \\ G_0 = S_2 & \longrightarrow & G_1 = \{\mathrm{Id}\} \end{array}$$

Con la misma notación, en el caso de tercer grado el esquema sería:

$$\begin{array}{lcccl} K_0 & \longrightarrow & K_1 = K_0\big(\sqrt{D}\big) & \longrightarrow & K_2 = K_1\big(\sqrt[3]{E}\big) \\ G_0 = S_2 & \longrightarrow & G_1 = A_3 & \longrightarrow & G_2 = \{\mathrm{Id}\} \end{array}$$

donde A_3 son las permutaciones pares, las generadas por $(r_1, r_2, r_3) \mapsto (r_2, r_3, r_1)$.

Sin entrar en detalles, en el caso de grado cuatro se tiene:

$$\begin{array}{lcccccccl} K_0 & \longrightarrow & K_1 & \longrightarrow & K_2 & \longrightarrow & K_3 & \longrightarrow & K_4 \\ G_0 = S_4 & \longrightarrow & G_1 = A_4 & \longrightarrow & G_2 & \longrightarrow & G_3 & \longrightarrow & G_4 = \{\mathrm{Id}\} \end{array}$$

con $K_1 = K_0\big(\sqrt{F}\big)$, $K_2 = K_1\big(\sqrt[3]{G}\big)$, $K_3 = K_2\big(\sqrt{H}\big)$ y $K_4 = K_3\big(\sqrt{I}\big)$, y G_2 y G_3 ciertos subgrupos de S_4 de órdenes 4 y 2 respectivamente.

De esta forma reflejamos el método para resolver las ecuaciones de grado $n = 2, 3, 4$ en una "tira" de subgrupos que empieza en S_n y acaba en $\{\mathrm{Id}\}$. Además, y aquí está la clave del teorema de Galois, siempre que empleemos radicales para romper simetrías cada subgrupo debe ser normal en el anterior, $G_i \triangleright G_{i+1}$. Para probar esto debemos tener a mano nuestros apuntes de Álgebra I y, si $K_{i+1} = K_i(R)$ con $R^p \in K_i$ (digamos con p primo y $R \notin K_i$), considerar el homomorfismo:

$$\begin{array}{rcl} \phi : G_i & \longrightarrow & \big(\mathbb{C} - \{0\}, \cdot\big) \\ \sigma & \longmapsto & \dfrac{R(r_{\sigma(1)}, r_{\sigma(2)}, \ldots, r_{\sigma(n)})}{R(r_1, r_2, \ldots, r_n)} \end{array}$$

Ahora leamos muy despacito, siempre con el Álgebra I presente: La imagen de este homomorfismo son las raíces p-ésimas de la unidad porque R^p es invariante por G_i y por consiguiente $R^p(r_{\sigma(1)}, r_{\sigma(2)}, \ldots, r_{\sigma(n)}) = R^p(r_1, r_2, \ldots, r_n)$; de donde $\mathrm{Im}\ \phi \cong \mathbb{Z}_p$. Además $\mathrm{Ker}\ \phi = G_{i+1}$ y el primer teorema de isomorfía implica $\mathrm{Ker}\ \phi = G_{i+1} \triangleleft G_i$ y $G_i/G_{i+1} \cong \mathrm{Im}\ \phi \cong \mathbb{Z}_p$.

En definitiva, la única forma de romper simetrías usando radicales es con subgrupos normales cuyo cociente sea isomorfo a un $\mathbb{Z}_p$.

Ahora podemos recoger los frutos de esta representación por medio de simetrías: Un teorema de teoría de grupos asegura que no existe ninguna cadena de grupos desde S_5 a $\{\mathrm{Id}\}$ siendo cada uno subgrupo normal del anterior y con cociente cíclico, por tanto *no existe una fórmula para resolver la ecuación de quinto grado usando sólo sumas, restas, multiplicaciones, divisiones y radicales* (Teorema de Abel). Lo mismo se aplica a la ecuación general de grado $n > 5$.

Evidentemente, hay casos particulares, como por ejemplo $x^6 - 7 = 0$, que sí pueden resolverse con radicales. El *Teorema de Galois* afirma que una ecuación se puede resolver con radicales si y sólo si existe una tira de subgrupos desde el llamado *grupo de Galois* a $\{\mathrm{Id}\}$ con las propiedades antes indicadas. El grupo de Galois es esencialmente el formado por las permutaciones de las raíces que son compatibles con las operaciones elementales (suma, resta, multiplicación y división) y que por tanto respeten las igualdades creadas con ellas. Por ejemplo, $x^4 - 2 = 0$ tiene como raíces $r_1 = \sqrt[4]{2}$, $r_2 = -\sqrt[4]{2}$, $r_3 = i\sqrt[4]{2}$, $r_4 = -i\sqrt[4]{2}$, y la permutación que intercambia r_2 y r_3 (dejando fijas las otras raíces) debe ser excluida del grupo de Galois porque, por ejemplo, $r_1^2 - r_2^2 = r_4^2 - r_3^2$ pero $r_1^2 - r_3^2 \neq r_4^2 - r_2^2$. A lo largo del curso veremos cómo hallar el grupo de Galois en casos suficientemente sencillos sin tener que pensar en todas las posibles igualdades. Si las raíces se consideran variables arbitrarias, como hemos hecho antes, no hay relaciones entre ellas, y el grupo de Galois es S_n.

El interés de este grupo no se limita a su relación con la resolubilidad por radicales, aunque sea su origen histórico. El *teorema fundamental de la Teoría de Galois* implica que para cualquier ecuación algebraica particular, la estructura interna de K_0 está fielmente reflejada en la estructura del grupo de Galois, lo cual es realmente destacable porque permite pasar de estudiar un conjunto infinito y de alguna forma continuo, a otro finito discreto.

Capítulo 1

Teoría de anillos

1.1. Definición de anillo

Un anillo intuitivamente no es más que un conjunto en el que podemos sumar, restar y multiplicar con las propiedades habituales excepto que la multiplicación no tiene por qué ser conmutativa, aunque esta salvedad no se considerará en este curso.

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 $c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$.

Si además $\otimes$ es una operación conmutativa se dice que A es un *anillo conmutativo*, y si $\otimes$ tiene elemento neutro, se dice que A es un *anillo con unidad*.

Observación: Que las operaciones sean *cerradas* simplemente quiere decir que al efectuarlas siempre el resultado estará en A. Con la notación habitual, que seguiremos en lo posible aquí, se escribe 0 para indicar el elemento neutro de $\oplus$ y 1 para indicar el de $\otimes$. Además se suelen utilizar las notaciones de la suma y producto habituales: $+$ y $\cdot$ (muchas veces omitida). Se dice que 1 es la *unidad* del anillo, y en general con la terminología al uso se llama *unidades* (o *elementos invertibles*) a todos los los elementos con inverso respecto de $\otimes$.

Como se ve, incluso para leer la primera definición es necesario saber qué es un grupo. Y, en general, es un requisito indispensable para este curso cierto conocimiento de la teoría de grupos. Como una concesión de primera página, recordaremos al menos la definición.

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: $\forall g \in G \ \exists h \in G \ : \ h * g = g * h = e$.

Ya hemos insinuado que en este curso sólo aparecerán anillos conmutativos. Ésta es una excusa como cualquier otra para introducir una nueva definición que especifica más el concepto de anillo.

Definición: Se dice que un anillo conmutativo con unidad es un *dominio de integridad* si $a \cdot b = 0 \Rightarrow a = 0$ ó $b = 0$ para cualquier par de elementos a, b.

Observación: Cuando un anillo no es un dominio de integridad, a los elementos no nulos a y b con $a \cdot b = 0$, se les llama *divisores de cero*. Éstos constituyen el obstáculo para poder simplificar en una igualdad (propiedad de cancelación). Concretamente, sólo podemos deducir $x = y$ a partir de $ax = ay$ si a no es un divisor de cero.

Siempre que se estudian estructuras algebraicas abstractas surge en nuestra mente el lejano soniquete de nuestra infancia: "¿y por qué?", "¿y para qué?". Una posible primera respuesta es la economía de medios. Por ejemplo, la teoría de grupos da un marco general que permite hallar los grupos cristalográficos, resolver el cubo de Rubik, dar una demostración rápida del pequeño teorema de Fermat, clasificar partículas en física cuántica o adivinar la última carta de nuestro adversario jugando a la escoba. El concepto de grupo abstrae cierta noción genérica de simetría que podemos aplicar en diferentes problemas. Aunque la unificación de la esencia de varios ejemplos importantes es históricamente responsable de la creación de la mayoría de las estructuras algebraicas, no se agotan ahí las razones para su estudio. La mayoría de los matemáticos situarían a la estética como guía directora. A pesar de que no tenga una "utilidad" clara disponer de una lista de todos los grupos simples, es algo natural, como en otro ámbito lo es colocar los libros en una estantería.

Después de esta inyección de fe ciega, veamos unos cuantos ejemplos.

Ejemplo. $\mathbb{Z}$ es un anillo conmutativo con unidad, de hecho un dominio de integridad.

Ejemplo. $\{a + b\sqrt{2} \ : \ a, b \in \mathbb{Z}\}$ es un dominio de integridad.

Ejemplo. Los enteros pares (divisibles por dos, negativos incluidos) conforman un anillo conmutativo pero no un anillo con unidad.

Ejemplo. $\{z \in \mathbb{C} \ : \ \frac{1}{2}\Re z, \frac{1}{2}\Im z \in \mathbb{Z}\}$ es un anillo conmutativo pero no un anillo con unidad. (Aquí y en lo sucesivo los símbolos $\Im$ y $\Re$ se emplearán para indicar las partes imaginaria y real, respectivamente).

Ejemplo. $\mathbb{Z}_6$, esto es, las clases de restos módulo 6 es un anillo conmutativo con unidad pero no un dominio de integridad porque $\overline{2} \cdot \overline{3} = \overline{0}$.

Ejemplo. Los matrices reales 2×2 forman un anillo, pero no un anillo conmutativo.

En estos ejemplos lo más que hay que comprobar es que las operaciones son cerradas, ya que las tres propiedades de la definición de anillo vienen heredadas por las correspondientes en $\mathbb{C}$, que se dan por supuestas.

Los ejemplo más importantes de anillo en este curso son los anillos de polinomios.

Dado un anillo conmutativo A, se denota con $A[x]$ al *anillo de polinomios sobre* A con la indeterminada x. Es decir al conjunto de expresiones formales del tipo $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ con $a_j \in A$ y las operaciones suma y producto habituales. 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.

Ciertamente se podría dar una definición más rigurosa de polinomio (véase [Cl] p. 203) pero el concepto es tan bien conocido de cursos pasados que sólo lograría darnos dolor de cabeza.

Puestos en faena, veamos la definición de grado y una proposición tonta para romper el hielo.

Definición: Si $P \in A[x]$ es de la forma $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ con $a_n \neq 0$ diremos que P tiene *grado* n y escribiremos $\partial P = n$ o también $\operatorname{gr} P = n$. Si $P = 0$ escribiremos formalmente $\partial P = -\infty$ o $\operatorname{gr} P = -\infty$.

Proposición 1.1.1 *Sea A un dominio de integridad. Entonces $A[x]$ también lo es y además para $P, Q \in A[x]$ se cumple:*

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

Demostración: Las propiedades 1) y 2) se siguen fácilmente de la definición de grado. 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). □

Recuérdese que se dice que un polinomio de grado $n \geq 1$, $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$, es *mónico* si $a_n = 1$. Esta definición tiene sentido para cualquier anillo con unidad.

Los polinomios mónicos más sencillos son de la forma $x+\alpha$. Si multiplicamos n de ellos obtendremos un polinomio de grado n:

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

y se tiene la fórmula $a_{n-k} = \sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ 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

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

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

Nota: Aunque no lo haremos aquí, es posible probar la unicidad de esta expresión.

Demostración: Sea $P \in A[x_1, x_2, \ldots, x_n]$ simétrico. Apliquemos el siguiente algoritmo:
1) Seleccionar el monomio $kx_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ (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 $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$.
2) Sea $Q = P - k\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_n^{\alpha_n}$. Entonces $P = k\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_n^{\alpha_n} + Q$ 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. □

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 1.1.3 *Sean $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$. Si $P = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ pertenece a $\mathbb{Q}[x]$, entonces para cualquier $Q \in \mathbb{Q}[x]$ el polinomio $P_Q = (x-Q(\alpha_1))(x-Q(\alpha_2))\ldots(x-Q(\alpha_n))$ también pertenece a $\mathbb{Q}[x]$.*

Demostración: Los coeficientes de P_Q son $a_{n-k} = (-1)^k\sigma_k\big(Q(\alpha_1), Q(\alpha_2), \ldots, Q(\alpha_n)\big)$. Considerando los α_i como variables, a_{n-k} define un polinomio simétrico de $\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_n]$, que por el teorema anterior se puede escribir como un polinomio con coeficientes racionales evaluado en $\sigma_1(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\sigma_2(\alpha_1, \alpha_2, \ldots, \alpha_n)$,... etc, y estas últimas cantidades son racionales porque coinciden, salvo un signo, con los coeficientes de P. □

Por ejemplo, de este resultado se deduce que como $\sqrt[3]{2}$ es raíz de $P = x^3 - 2$, entonces para cada $a, b, c \in \mathbb{Z}$, $a\sqrt[3]{2^2} + b\sqrt[3]{2} + c$ también es raíz de un polinomio de grado 3 en $\mathbb{Z}[x]$. Una demostración directa (hallando el polinomio), sería muy farragosa.

Una vez que tenemos anillos podemos considerar aplicaciones entre ellos que respeten las operaciones. La notación rococó es la misma que en teoría de grupos, y ya debería ser conocida.

Definición: Sean A y B anillos con unidad. Un *homomorfismo* de anillos es una función $\phi : A \longrightarrow B$ que respeta la suma, la multiplicación y el elemento unidad, esto es,

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

Nota: Para anillos sin unidad, y a veces en general, la condición *iii)* se suprime.

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.*

Si $f : A \longrightarrow B$ es un homomorfismo de anillos, su núcleo y su imagen se definen como en teoría de grupos o álgebra lineal:

$$\text{Ker } f = \{a \in A \ :\ f(a) = 0\}, \qquad \text{Im } f = \{b \in B \ :\ f^{-1}(b) \neq \emptyset\},$$

y es muy fácil comprobar que ambos son anillos (con las operaciones heredadas de A y B respectivamente).

Ejemplo. $f : \mathbb{Z} \longrightarrow \mathbb{C}$, con f la inclusión, es un monomorfismo.

Ejemplo. Sea M el subconjunto de $\mathcal{M}_{2\times 2}(\mathbb{R})$ (el anillo de matrices reales 2×2) definido como $M = \{(a_{ij})_{i,j=1}^{2} \ : \ a_{11} = a_{22},\ a_{12} = -a_{21}\}$. Entonces la aplicación $f : \mathbb{C} \longrightarrow M$ dada por

$$f(z) = \begin{pmatrix} \Re z & \Im z \\ -\Im z & \Re z \end{pmatrix}$$

es un isomorfismo.

La biyectividad es obvia, y las propiedades de homomorfismo sencillas de comprobar. Nótese que está garantizado que M es un anillo por ser la imagen de la aplicación f extendida a $\mathbb{C} \longrightarrow \mathcal{M}_{2\times 2}(\mathbb{R})$.

Ejemplo. $f : \mathbb{Z} \longrightarrow \mathbb{Z}_6$ con $f(x) = \overline{x}$, la clase de x módulo 6, es un epimorfismo.

Ejemplo. La conjugación $\mathbb{C} \longrightarrow \mathbb{C}$ es un automorfismo.

Ejemplo. Si $A \subset B$ con A y B anillos conmutativos con unidad. Para cada $b \in B$ la función $f_b : A[x] \longrightarrow B$ dada por $f_b(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0$ es un homomorfismo.

A la imagen de este homomorfismo de evaluación se le denota escribiendo $A[b]$. (Nótese el leve abuso de notación debido a que $A[b]$ no es un anillo de polinomios). Y copiando la notación del análisis se escribe $P(b)$ en lugar de $f_b(P)$. Este tipo de anillos con $A = \mathbb{Z}$ o $\mathbb{Q}$ y b ciertos números complejos, tienen gran importancia en problemas aritméticos e históricamente están en el origen del propio concepto de anillo.

Ejemplo. $\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\}$.

Ejemplo. $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Q}\}$.

Es cierto que todos los ejemplos de anillos y aplicaciones entre ellos incluidos en esta sección, se reducen a una comprobación directa de la definición. Son todos demasiado sencillos. En unos momentos complicaremos las cosas introduciendo anillos cociente. Mientras tanto, el que quiera quejarse por el tiempo perdido, que se dirija a R. Descartes que consideró como una de sus *reglas para la dirección de la mente*: "Hay que dirigir toda la penetración de nuestro espíritu o mente a lo que es menos importante y más fácil. Y es conveniente que nos detengamos en ello durante bastante tiempo, hasta que hayamos adquirido el hábito de ver la verdad por intuición de una manera distinta y clara".

1.2. Ideales y cocientes

Un ideal es un subanillo que es absorbente con respecto al producto. Esto puede que sea verdad, pero como no hay quien lo entienda, demos una definición menos sintética y más comprensible.

Definición: Sea A un anillo. Se dice que $I \subset A$ es un ideal si:

$$i) \quad (I,+) \text{ es un subgrupo}, \qquad ii) \quad a \in A,\ b \in I \ \Rightarrow\ ab, ba \in I.$$

Nótese que estas propiedades aseguran que $+$ y $\cdot$ son cerradas en I, y por tanto I hereda la estructura de anillo de A. Además $ii)$ indica que I es invariante por multiplicaciones. Éste es el significado de la definición sintética.

Notación: Dados $a_1, a_2, \ldots, a_n \in A$, se suele denotar mediante $\langle a_1, a_2, \ldots, a_n \rangle$ o $(a_1, a_2, \ldots, a_n)$ (preferimos la segunda notación por razones tipográficas) al menor ideal, en el sentido de la inclusión, que contiene a $\{a_1, a_2, \ldots, a_n\}$. Se dice que los a_j son *generadores* del ideal. Es fácil ver que la intersección de ideales es un ideal, lo que asegura la existencia del susodicho "menor ideal", basta hacer la intersección de todos los que contienen a $\{a_1, a_2, \ldots, a_n\}$. Si A es un anillo conmutativo con unidad, es un sencillo ejercicio comprobar que

$$\langle a_1, a_2, \ldots, a_n \rangle = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \ :\ \lambda_j \in A\}.$$

Ejemplo. $I = \{\text{números pares}\}$ es un ideal de $\mathbb{Z}$.

Ejemplo. $I = \langle d \rangle = \{\text{múltiplos de } d\}$ es un ideal de $\mathbb{Z}$.

Ejemplo. En $\mathbb{R}[x, y]$, el ideal $\langle x, y \rangle$ es el formado por los polinomios de dos variables cuyo término independiente se anula.

Ejemplo. Los ideales de $\mathbb{Z}_4$ son $I_1 = \{\overline{0}\}$, $I_2 = \{\overline{0}, \overline{2}\}$, $I_3 = \mathbb{Z}_4$.

Ejemplo. En $\mathbb{Z}$, $\langle 2, 5 \rangle = \langle 1 \rangle = \mathbb{Z}$, ya que $3 \cdot 2 + (-1) \cdot 5 = 1$.

Distinguiremos dos tipos de ideales que aparecerán en la próxima sección.

Definición: Se dice que un ideal $I \subset A$ es *principal* si puede generarse con un único elemento. Esto es, si $I = \langle a \rangle$ para cierto $a \in A$.

Definición: Se dice que un ideal $I \subset A$ es *maximal* si es propio ($I \neq \{0\}, A$) y no existe otro ideal J tal que $I \subsetneqq J \subsetneqq A$.

Ejemplo. El ideal $I = \langle 6, 10 \rangle \subset \mathbb{Z}$ es principal, ya que no es difícil probar que $I = \langle 2 \rangle$.

Ejemplo. El ideal del ejemplo anterior es maximal porque si intentamos "añadir" un número impar, $2n + 1$, a I entonces también debería estar $(2n + 1) + (-n) \cdot 2 = 1$ y por tanto todo $\mathbb{Z}$.

Ejemplo. El ideal $I = \langle 9 \rangle \subset \mathbb{Z}$ no es maximal porque $\langle 9 \rangle \subsetneqq \langle 3 \rangle \subsetneqq \mathbb{Z}$

Ejemplo. Por la regla de Ruffini, en $\mathbb{R}[x]$ el ideal $I = \{P \in \mathbb{R}[x] \ :\ P(-1) = 0\}$ es $I = \langle x + 1 \rangle$ y por tanto principal.

Ejemplo. En $\mathbb{R}[x,y]$ el ideal $I=\langle x,y\rangle$ no es principal, ya que $I=\langle P\rangle$ implicaría $P|x$ y $P|y$. Por otra parte, I sí es maximal porque $I\subsetneq J$ sólo es posible si existe $Q\in J$ con término independiente $a_0\neq 0$, y $a_0-Q\in I$ implica $a_0\in J$, y por tanto $1=a_0^{-1}a_0\in J$.

En $\mathbb{Z}$, en realidad los ideales "tienen truco". Como veremos, y no es difícil adivinar, todos los ideales de $\mathbb{Z}$ son principales y los maximales son (p) con p primo. Además se cumple el siguiente resultado que permite simplificar generadores.

Proposición 1.2.1 *En $\mathbb{Z}$, si a y b no son simultáneamente nulos se cumple la igualdad entre ideales*

$$\langle a,b\rangle=\langle \mathrm{mcd}(a,b)\rangle$$

donde $\mathrm{mcd}(a,b)$ *es el máximo común divisor de a y b.*

Demostración: Sean $I=\langle a,b\rangle$ y $J=\langle \mathrm{mcd}(a,b)\rangle$. Evidentemente $I\subset J$ (porque $a,b\in J$). Por otra parte, por la identidad de Bezout existen λ_1,λ_2 tales que $\mathrm{mcd}(a,b)=\lambda_1 a+\lambda_2 b\in I$, y se sigue que $J\subset I$. □

Vayamos ahora a unos cuantos ejemplos más difíciles.

Ejemplo. El ideal $I=\langle 2,1+\sqrt{-5}\rangle$ es maximal en $A=\mathbb{Z}[\sqrt{-5}]$.

Sea $\alpha=a+b\sqrt{-5}\notin I$. Necesariamente $a-b$ es impar porque en otro caso $\alpha=2(a-b)/2+b(1+\sqrt{-5})\in I$. Pero si $a-b$ es impar, $1=2(a-b+1)/2+b(1+\sqrt{-5})+(-1)\alpha$. Por tanto $\langle 2,1+\sqrt{-5},\alpha\rangle=\langle 1\rangle=A$. Es decir, el ideal I no se puede ampliar con ningún elemento.

Ejemplo. El ideal $I=\langle 2,1+\sqrt{-5}\rangle$ no es principal en $A=\mathbb{Z}[\sqrt{-5}]$.

Si $I=\langle\alpha\rangle$ con $\alpha=a+b\sqrt{-5}$, entonces $2=\alpha\beta$ y $1+\sqrt{-5}=\alpha\gamma$ para ciertos $\beta,\gamma\in A$. Multiplicando estas igualdades por sus conjugadas se tiene que a^2+5b^2 debe dividir a 4 y a 6. Esto sólo deja las posibilidades $a=\pm 2,\ b=0$ y $a=\pm 1,\ b=0$. El primer caso es imposible porque $1+\sqrt{-5}$ no es un múltiplo de 2. El segundo caso sólo se daría si $I=A$, y esto no es cierto porque no es difícil ver que si $x+y\sqrt{-5}\in A$ es múltiplo de 2 o de $1+\sqrt{-5}$ entonces x e y tienen la misma paridad.

Ejemplo. El ideal $I=\langle 11+7\sqrt{2},8+11\sqrt{2}\rangle$ es principal en $A=\mathbb{Z}[\sqrt{2}]$.

Tratamos de pasar a números enteros multiplicando por el conjugado, concretamente $23=(11+7\sqrt{2})(11-7\sqrt{2})$ y $-178=(8+11\sqrt{2})(8-11\sqrt{2})$ están en I. Utilizando el algoritmo de Euclides se obtiene $1=31\cdot 23+4\cdot(-178)$. Por tanto,

$$1=\big[31(11-7\sqrt{2})\big](11+7\sqrt{2})+\big[4(8-11\sqrt{2})\big](8+11\sqrt{2}),$$

y el ideal no sólo es principal sino que $I=\langle 1\rangle=A$.

Ejemplo. Estudiar si el ideal $I=\langle 1+4\sqrt{-2},-9+6\sqrt{-2}\rangle$ es principal en $A=\mathbb{Z}[\sqrt{-2}]$.

Como antes, $33=(1+4\sqrt{-2})(1-4\sqrt{-2})\in I$ y $153=(-9+6\sqrt{-2})(-9-6\sqrt{-2})\in I$. El máximo común divisor en $\mathbb{Z}$ de estos números es 3, de forma que si $I=\langle\alpha\rangle$ con $\alpha=a+b\sqrt{-2}$, entonces $3=(a+b\sqrt{-2})\beta$ con $\beta\in A$. Al multiplicar por el conjugado

las posibilidades son $\alpha = \pm 1, \pm 1 \pm \sqrt{-2}, \pm 1 \pm 2\sqrt{-2}$. De estos valores, $1+\sqrt{-2}$ divide a los generadores de I, concretamente $I = \langle (1+\sqrt{-2})(3+\sqrt{-2}), (1+\sqrt{-2})(1+5\sqrt{-2})\rangle$. Ahora con $3+\sqrt{-2}$ y $1+5\sqrt{-2}$ podemos dar lugar a enteros coprimos. Por ejemplo, $5(3+\sqrt{-2}) - (1+5\sqrt{-2}) = 14$ y $\sqrt{-2}(3+\sqrt{-2}) - 3(3+\sqrt{-2}) = -11$. Como $14x + (-11)y = 1$ tiene solución, existen $\gamma, \delta \in A$ tales que $(3+\sqrt{-2})\gamma + (1+5\sqrt{-2})\delta = 1$ y se concluye $I = \langle 1+\sqrt{-2}\rangle$.

Seguramente muchos de los lectores ya habrán perdido la paciencia. Como sucede a menudo en matemáticas, y en particular en álgebra abstracta, las definiciones parecen gratuitas, desmotivadas, y la teoría aislada e inasequible. Podemos tener fe en que hay muchos anillos interesantes y que conviene estudiarlos en general, pero ¿y los ideales? ¿cómo a alguien en su sano juicio se le pudo ocurrir introducirlos? ¿para qué los ideales principales y maximales? Si estos conceptos son triviales en $\mathbb{Z}$, ¿en qué anillos resultó interesante crear esta parte de la teoría? Puede que el lector se sienta engañado al saber que respetando el orden histórico las secciones de este capítulo debieran estar escritas en orden inverso: los problemas de factorización llevaron al concepto de ideal y después se desarrolló la teoría de anillos. Sin embargo desde el punto de vista actual y con la preponderancia de lo deductivo frente a lo inductivo en las matemáticas modernas, es más natural no comenzar la casa por el tejado. De todas maneras, al margen de las buenas palabras, disculpas y excusas, ¿es posible explicar las razones que llevaron a la teoría de ideales? Lo que sigue es un intento un poco burdo desde el punto de vista histórico (para una descripción fiel véase [Ri] y [Sm]) pero que puede arrojar alguna luz.

Los ideales los introdujo E. Kummer tratando de probar el último teorema de Fermat y se revelarían como un instrumento muy adecuado permitiendo demostrarlo para muchos exponentes especiales. La ecuación de Fermat $x^n + y^n = z^n$ se puede factorizar como

$$(x-\zeta y)(x-\zeta^2 y)\cdots(x-\zeta^n y) = z \cdot z^{\overset{n \text{ veces}}{\cdots\cdots}} z \tag{1.1}$$

con $\zeta = e^{\pi i/n}$. Esto conduce a estudiar cuándo dos productos coinciden en el anillo $\mathbb{Z}[\zeta]$. En $\mathbb{Z}$ es evidente que si tenemos unos cuantos números que son coprimos dos a dos con otros, el producto de los primeros no puede coincidir con el de los segundos. Esto es, productos iguales implica divisores comunes de los factores. Sin embargo en otros anillos no ocurre así. Por ejemplo, en $\mathbb{Z}[\sqrt{-5}]$ se cumple

$$3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$$

y sin embargo 3 y $1 \pm 2\sqrt{-5}$ no tienen divisores comunes no triviales en $\mathbb{Z}[\sqrt{-5}]$, ni 7 y $1 \pm 2\sqrt{-5}$. Si no ocurrieran casos patológicos como éste en $\mathbb{Z}[\zeta]$, Kummer disponía de técnicas para probar que (1.1) es imposible con n =primo y $x, y \in \mathbb{Z}^+$ coprimos, de donde se deduciría el último teorema de Fermat. Desafortunadamente estos casos patológicos son habituales en $\mathbb{Z}[\zeta]$, pero la buena noticia es que la teoría de ideales permite tratarlos creando un sustituto de los divisores comunes ausentes. Por ejemplo, partiendo de $3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$, nos gustaría que existiesen los divisores comunes antes indicados, digamos $\alpha_\pm = \mathrm{mcd}(3, 1 \pm 2\sqrt{-5})$, $\beta_\pm = \mathrm{mcd}(7, 1 \pm 2\sqrt{-5})$, de forma que

$$3 = \alpha_+ \cdot \alpha_-, \qquad 7 = \beta_+ \cdot \beta_-, \qquad 1+2\sqrt{-5} = \alpha_+ \cdot \beta_+, \qquad 1-2\sqrt{-5} = \alpha_- \cdot \beta_-. \tag{1.2}$$

Como hemos mencionado, tales $\alpha_\pm, \beta_\pm$ no existen. Pero según la Proposición 1.2.1, al menos en $\mathbb{Z}$, un ideal con dos generadores es un sustituto para el máximo común divisor. Y así resulta que (1.2) pasa a ser cierto reemplazando 3, 7 y $1 \pm 2\sqrt{-5}$ por los ideales que generan, $\alpha_\pm$ por $\langle 3, 1 \pm 2\sqrt{-5}\rangle$ y $\beta_\pm$ por $\langle 7, 1 \pm 2\sqrt{-5}\rangle$ (el producto de ideales se define como el menor ideal que contiene a los productos de sus elementos).

Las cantidades $\alpha_\pm$, $\beta_\pm$ son literalmente "ideales" en (1.2), no existen, y en general sólo corresponderían a cantidades "reales" cuando los ideales fueran principales (esta cantidad real sería el generador). Además, la maximalidad de los ideales indicaría que es imposible seguir descomponiendo en más factores. El obstáculo para probar el último teorema de Fermat con este método, por lo que Kummer sólo tuvo éxito parcial, es que es difícil saber en general si los ideales que aparecen en ciertas factorizaciones son principales, y por tanto si posibles soluciones "ideales" de la ecuación de Fermat son "irreales".

Un ideal I en un anillo A permite establecer una relación de equivalencia dada por

$$a \sim b \;\Leftrightarrow\; a - b \in I.$$

Cuando hay una relación de equivalencia, hay un conjunto cociente A/I (el conjunto de las clases de equivalencia) y es fácil ver, si uno entiende los conceptos básicos, que hereda la estructura de anillo.

Proposición 1.2.2 *Si $I \subset A$ es un ideal, entonces A/I es un anillo con las operaciones heredadas de A (es decir, se definen $\overline{a} + \overline{b} := \overline{a+b}$ y $\overline{a} \cdot \overline{b} := \overline{ab}$).*

Demostración: Las propiedades de las operaciones se siguen de las de A. Sólo hay que comprobar que están bien definidas, no dependiendo del representante elegido. Esto es, si $\overline{a_1} = \overline{b_1}$ y $\overline{a_2} = \overline{b_2}$ donde $\overline{a_j}$ y $\overline{b_j}$ son las clases de equivalencia de a_j y b_j, hay que probar $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ y $\overline{a_1 a_2} = \overline{b_1 b_2}$. Para el producto:

$$x - a_1 a_2 \in I \Leftrightarrow x - a_1 a_2 + a_1(a_2 - b_2) + (a_1 - b_1)b_2 \in I \Leftrightarrow x - b_1 b_2 \in I.$$

Donde se ha usado que $a_2 - b_2, a_1 - b_1 \in I$. Para la suma es aún más sencillo. □

Si pidiéramos a I sólo que fuera un subanillo pero no un ideal, entonces A/I no heredaría la estructura de anillo. Por ejemplo, en $\mathbb{Z} \times \mathbb{Z}$, $I = \{(a, b) \;:\; 2|a - b\}$ es un subanillo pero la operación producto no pasa bien al cociente, por ejemplo $\overline{(0,1)} = \overline{(1,0)}$ pero $\overline{(1,0)} \cdot \overline{(1,0)} = \overline{(1,0)} \neq \overline{(0,1)} \cdot \overline{(1,0)}$.

Es muy fácil comprobar que el núcleo de un homomorfismo es un ideal. El primer teorema de isomorfía para grupos se extiende a este contexto afirmando que para cualquier homomorfismo de anillos $f : A \longrightarrow B$, se tiene que $A/\mathrm{Ker}\, f$ es isomorfo a $\mathrm{Im} f$.

Los cocientes por ideales maximales tienen una insospechada e importante particularidad.

Proposición 1.2.3 *Sea A un anillo conmutativo con unidad. Un ideal $I \subset A$ es maximal si y sólo si todos los elementos de A/I diferentes de $\overline{0}$ son unidades.*

Demostración: Cualquier ideal que contenga a I y a algún $a \in A - I$, obviamente debe contener al ideal $J = \{x \in A \;:\; x - \lambda a \in I \text{ con } \lambda \in A\}$. Evidentemente $J = A$ si y sólo si $1 \in J$, esto es, si y sólo si $1 - \lambda_0 a \in I$ para algún λ_0, o equivalentemente $\overline{1} = \overline{\lambda_0}\overline{a}$. □

Observación: Nótese que A/I no sería un dominio de integridad si algún elemento $x \in I$ se pudiera factorizar como $x = ab$ con $a, b \notin I$. Por ello se llaman *ideales primos* a los que cumplen que A/I es un dominio de integridad. En particular, según el resultado anterior, todo ideal maximal es primo. Surge la pregunta natural de si ambos conceptos son equivalentes. Como el estudio de los ideales primos excede los contenidos de este curso, aquí solamente avanzaremos que en los anillos de polinomios estudiados en Álgebra III los ideales primos y maximales son bien distintos (por ejemplo $\langle x + y^2 \rangle$ es primo no maximal en $\mathbb{R}[x, y]$), mientras que en los anillos de números complejos que se manipulan en Teoría de Números (por ejemplo en todos los $\mathbb{Z}[\sqrt{d}]$) no hay diferencia entre primos y maximales.

En esta sección hemos dado por supuesto que el lector domina perfectamente el concepto de conjunto cociente, y más adelante haremos lo propio con el de grupo cociente. Si esta suposición fuera gratuita, es el momento de repasar cursos anteriores. De todos modos se añaden a continuación unas pocas líneas de nivel ínfimo, para desperezarse.

Cuando tenemos una forma de relacionar los elementos de un conjunto, el conjunto cociente no es más que el conjunto de las colecciones de elementos del mismo tipo. Esta clasificación en diferentes clases no es totalmente ajena al significado del cociente usual de números naturales. Por ejemplo $40 \div 4 = 10$ significa que si repartimos 40 caramelos entre 4 niños, tocan a 10 cada uno. Supongamos que los caramelos estuvieran numerados del 1 al 40 y que cada niño pusiera su nombre a los que recibiera. Si los repartimos de uno en uno ordenadamente, los caramelos 1, 5, 9, 13,... 37 tendrían el nombre del primer niño, los caramelos 2, 6, 10,... 38, el del segundo, etc. Con la relación $a \sim b \Leftrightarrow 4|a - b$, los caramelos relacionados entre sí son los que pertenecen al mismo niño. El conjunto cociente sería $\{N_1, N_2, N_3, N_4\}$ donde N_j es el conjunto de caramelos del niño j-ésimo (la clase de equivalencia de j), como las cuatro clases tienen el mismo tamaño, cada una tiene $40/4 = 10$ elementos. Al principio es un poco lioso que el conjunto cociente sea un conjunto de conjuntos, pero no lo es tanto pensando que por ejemplo un conjunto de libros es un conjunto de conjuntos de páginas.

En grupos (o anillos) hay relaciones de equivalencia (formas de repartir caramelos) naturales asociadas a ciertos subgrupos (o subanillos). Por ejemplo si H es un subgrupo de G uno puede inventarse $g_1 \sim g_2 \Leftrightarrow g_1 \cdot g_2^{-1} \in H$ que expresa algo así como que al repartir los caramelos de G "coherentemente" entre los elementos de H, g_1 y g_2 corresponden al mismo niño (elemento) de H. El conjunto cociente correspondiente se suele denotar como G/H. Una cuestión técnica muy importante es que la operación de grupo de G puede no estar bien definida en G/H. Sólo lo está cuando H es un subgrupo normal. De forma que si queremos descomponer un grupo en grupitos, clasificando sus elementos, no podemos tomar cociente entre un subgrupo cualquiera. Con los anillos ocurre algo similar y debemos limitarnos a las relaciones de equivalencia que vengan de ideales, no de subanillos cualesquiera.

1.3. Factorización

Como ya hemos mencionado, la teoría de ideales surgió en relación con ciertos problemas de factorización en anillos. A título meramente ilustrativo, nótese que por ejemplo hallar las soluciones enteras de $xy = 10^{20}$ requiere factorizar 10^{20} en $\mathbb{Z}$, y hallar las de $x^2 + y^2 = 10^{20}$, debido a la fórmula $x^2 + y^2 = (x - iy)(x + iy)$, requeriría factorizar 10^{20} en $\mathbb{Z}[i]$.

Sabemos que en $\mathbb{N}$ todo número mayor que uno se escribe como producto de primos de forma única salvo el orden de los factores. Éste es el llamado *teorema fundamental de la aritmética*. En $\mathbb{Z}$ la unicidad se complica por culpa de los signos. Por ejemplo

$$30 = 2 \cdot 3 \cdot 5 = (-2) \cdot 3 \cdot (-5) = 2 \cdot (-3) \cdot (-5) = (-2) \cdot (-3) \cdot 5.$$

La culpa la tiene el elemento -1, que al poseer inverso multiplicativo (él mismo), puede introducirse y compensarse a voluntad. En otros anillos puede haber más elementos invertibles que causen problemas similares. La definición de unicidad de la factorización en un anillo tendrá esta particularidad en cuenta. Antes introduciremos una notación *chic* que llama irreducibles a los primos en un anillo (algunos autores los siguen llamando primos).

Definición: Sea A un anillo. Se dice que dos elementos $a, b \in A$ están *asociados* si $a = ub$ con u una unidad.

Definición: Sea A un dominio de integridad. Se dice que un elemento $p \in A - \{0\}$ es *irreducible* si no es una unidad y $p = ab$ implica que p está asociado con a o con b.

Definición: Se dice que un dominio de integridad A es un *dominio de factorización única* si todo elemento de $A - \{0\}$ que no sea una unidad se puede expresar como un producto de factores irreducibles de forma única salvo el orden de los factores y el empleo de irreducibles asociados.

Ejemplo. $\mathbb{Z}$ es un dominio de factorización única.

Ejemplo. $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única, ya que por ejemplo $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Comprobar que los factores de esta doble factorización son realmente irreducibles conlleva algunos cálculos. Si fuera $2 = (x + y\sqrt{-5})(u + v\sqrt{-5})$, multiplicando por el conjugado se tendría $4 = (x^2 + 5y^2)(u^2 + 5v^2)$, y evidentemente esto sólo es posible si $y = v = 0$, y se tiene $x + y\sqrt{-5} = \pm 1$ o $u + v\sqrt{-5} = \pm 1$. La misma demostración sirve para 3. Análogamente $1 \pm \sqrt{-5} = (x + y\sqrt{-5})(u + v\sqrt{-5})$ implica $6 = (x^2 + 5y^2)(u^2 + 5v^2)$, y la única posibilidad, salvo intercambiar x e y por u y v, es $x = \pm 1$, $y = \pm 1$, $u = \pm 1$, $v = 0$.

Los dominios de factorización única se muestran más sencillos en algunos problemas que los anillos que no lo son, y nos gustaría saber detectarlos.

Una vez que sabemos qué queremos hacer, vamos a abstraer las propiedades necesarias para llevarlo a cabo. Si repasamos el teorema fundamental de la aritmética, veremos que la prueba se basa en la existencia del máximo común divisor. A su vez, ésta dependía de la existencia del algoritmo de Euclides. Uniendo estos cabos buscamos un teorema que diga algo así como que los dominios de integridad en los que existe un algoritmo de Euclides son los de factorización única. Pero ¿qué es un algoritmo de Euclides en general? En $\mathbb{N}$ era un procedimiento que simplemente requería la existencia de una división inexacta: dados a y b se calculaba un cociente c y un resto $r < b$ tales que $a = bc + r$. Todo esto lo podemos copiar en anillos arbitrarios salvo el signo "$<$" ya que en general no hay relaciones de orden en un anillo. Por tanto para salvar la idea del algoritmo de Euclides requerimos que exista una función que permita medir lo grandes que son sus elementos traspasando el problema a $\mathbb{N}$. Habida cuenta de todo esto, la siguiente definición concretará la idea buscada de dominio con algoritmo de Euclides.

Definición: Se dice que un dominio de integridad A es un *dominio euclídeo* si existe una función $N : A - \{0\} \longrightarrow \mathbb{N}$ tal que:
i) $\forall a, b \in A - \{0\}$ se cumple $N(a) \leq N(ab)$.
ii) $\forall a, b \in A - \{0\}$ existen $c, r \in A$ tales que $a = bc + r$ con $r = 0$ o $N(r) < N(b)$.

Observación: Algunos autores piden que N sea una función multiplicativa, esto es, $N(ab) = N(a)N(b)$, lo cual es más fuerte que $i)$.

Ejemplo. $\mathbb{Z}$ es un dominio euclídeo con $N(a) = |a|$.

Ejemplo. $\mathbb{Q}[x]$ es un dominio euclídeo con $N(P) = \partial P$.

Veamos qué consecuencias tiene la existencia del máximo común divisor en relación con los ideales. Es interesante comparar el siguiente resultado con la Proposición 1.2.1.

Teorema 1.3.1 *Si A es un dominio euclídeo entonces todos los ideales de A son principales.*

Notación: Para abreviar se suele hablar de *dominio de ideales principales* para indicar un dominio de integridad con todos sus ideales principales.

Demostración: Sea $I \neq \langle 0 \rangle$ un ideal de A y sea b el elemento de I para el que $N(b)$ es mínimo. Dado $a \in I$, por ser A dominio euclídeo $a = bc + r$ con $r = 0$ (ya que $N(r) < N(b)$ es imposible porque $r = a - bc \in I$). Por tanto $a = bc \in \langle b \rangle$ y como esto se cumple para todo $a \in I$, se deduce $I = \langle b \rangle$. □

El próximo resultado simplemente ilustra que en algunas situaciones los ideales maximales son más tangibles que lo que su definición indica.

Proposición 1.3.2 *Sea A un dominio de ideales principales. Un ideal $I \subsetneqq A$ es maximal si y sólo si $I = \langle p \rangle$ con p irreducible.*

Demostración: $\Rightarrow$) Si $I = \langle a \rangle$ con $a = bc$, b y c no invertibles, se tendría $I \subsetneqq \langle b \rangle \subsetneqq A$.
$\Leftarrow$) Si $I = \langle p \rangle \subset J = \langle b \rangle \subset A$ entonces $p \in \langle b \rangle$ implica $p = bc$. Por la irreducibilidad, b o c son invertibles y por consiguiente o bien $J = A$ o bien $J = I$. □

Aparentemente nos hemos desviado en nuestro estudio de la factorización. El siguiente resultado mostrará que estábamos a mitad de camino.

Teorema 1.3.3 *Si A es un dominio de ideales principales entonces A es un dominio de factorización única.*

Demostración: Sea $a \in A - \{0\}$ no invertible. Veamos primero que a se puede escribir como producto de un número finito de irreducibles. Si no fuera así, tendríamos una sucesión infinita de igualdades

$$a = p_1 a_1 = p_1 p_2 a_2 = p_1 p_2 p_3 a_3 = p_1 p_2 p_3 p_4 a_4 = \dots$$

con p_j irreducibles y $a_j = p_{j+1}a_{j+1}$. Sea el ideal $I = \bigcup_{j=1}^{\infty}\langle a_j\rangle$. Por estar en un dominio de ideales principales $I = \langle b\rangle$, con $b \in \langle a_k\rangle$ para cierto k, y esto implica $I = \langle a_k\rangle$ porque $b \in \langle a_k\rangle \supset I = \langle b\rangle$. Lo cual lleva a la contradicción $\langle a_{k+1}\rangle = \langle a_k/p_{k+1}\rangle \notin I$.

Una vez que hemos visto que hay una factorización, debemos probar que es única. Supongamos que hubiera dos factorizaciones en irreducibles que coinciden

$$p_1 \cdot p_2 \cdots p_l = q_1 \cdot q_2 \cdots q_m. \tag{1.3}$$

Queremos probar que ambas son iguales salvo en el orden de los factores y multiplicación por elementos invertibles.

Procedemos por inducción en $n = \min(l, m)$. Evidentemente $l = 1 \Leftrightarrow m = 1$ (por la irreducibilidad) y el caso $n = 1$ es trivial. Sea por tanto $n > 1$. El ideal $I = \langle p_l, q_m\rangle$ debe ser principal, digamos $I = \langle b\rangle$. Por tanto $p_l = rb$, $q_m = sb$, y como p_l y q_m son irreducibles, o bien r y s son invertibles o bien b es invertible. En el primer caso p_l y q_m son asociados porque $p_l = r^{-1}sq_m$, y simplicando en (1.3), el resultado se sigue por la hipótesis de inducción. Si b es invertible $I = A$, en particular

$$1 \in \langle p_l, q_m\rangle \;\Rightarrow\; \lambda p_l + \mu q_m = 1 \;\Rightarrow\; \lambda p_l q_1 q_2 \ldots q_{m-1} + \mu p_1 p_2 \ldots p_l = q_1 q_2 \ldots q_{m-1}.$$

De forma que $cp_l = q_1 q_2 \ldots q_{m-1}$ para cierto $c \in A$ y por la hipótesis de inducción se sigue que p_l es asociado de alguno de los q_j. Simplificando como antes p_l y q_j en (1.3) se concluye la prueba empleando la hipótesis de inducción. □

En resumen, lo que hemos demostrado es:

Dom. euclídeo ⇒ Dom. de ideales principales ⇒ Dom. de factorización única.

Es posible dar contraejemplos a los recíprocos. Por ejemplo, se puede probar (pero no es nada fácil) que $\mathbb{Z}[(1+\sqrt{-19})/2]$ es un dominio de ideales principales pero no un dominio euclídeo (véase en [Cam] una demostración abreviada). También se puede probar que $\mathbb{Z}[x]$ es un dominio de factorización única (se sigue de que $\mathbb{Q}[x]$ lo es) pero no un dominio de ideales principales, ya que $I = \langle 3, x^2\rangle$ no es principal.

A continuación mostramos algunos ejemplos desarrollados que no debieran hacernos demasiado optimistas, porque incluso en anillos sencillos hay todavía problemas abiertos respecto a la factorización única.

Ejemplo. El anillo $\mathbb{Z}[i] = \{a + bi \;:\; a, b \in \mathbb{Z}\}$ es un dominio de factorización única. De hecho es un dominio euclídeo con $N(z) = |z|^2$ donde $|\cdot|$ indica la norma usual en $\mathbb{C}$.

Como $N(z_1z_2) = N(z_1)N(z_2)$, la primera propiedad de los dominios euclídeos está asegurada. Los círculos unitarios $\{z \in \mathbb{C} \;:\; N(z-w) < 1\}$ recubren todo $\mathbb{C}$ cuando w recorre $\mathbb{Z}[i]$; por tanto dados $z_1, z_2 \in \mathbb{Z}[i] - \{0\}$ siempre existe $w \in \mathbb{Z}[i]$ tal que $N(z_1/z_2 - w) < 1$, o lo que es lo mismo $N(z_1 - z_2w) < N(z_2)$. Esto prueba la segunda propiedad con $r = z_1 - z_2w$. Como $N(0) = 0$, el caso $r = 0$ está incluido en $N(r) < N(z_2)$.

Ejemplo. El anillo $\mathbb{Z}[\sqrt{-3}]$ no es de factorización única y por tanto no es de ideales principales ni euclídeo.

Un ejemplo de factorización no única es $2\cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. Para comprobar que cada factor es irreducible se puede usar el mismo argumento empleado para $\mathbb{Z}[\sqrt{-5}]$. De esta doble factorización se deduce que el ideal $I = \langle 2, 1+\sqrt{-3}\rangle$ no es principal. No es muy difícil comprobar que I es maximal.

Ejemplo. El anillo $\mathbb{Z}[(1+\sqrt{-3})/2]$ es de factorización única. De hecho es un dominio euclídeo con $N(z) = |z|^2$.

Observando que $((1+\sqrt{-3})/2)^2 = (-1+\sqrt{-3})/2$, se deduce que

$$\mathbb{Z}[(1+\sqrt{-3})/2] = \{a + b(1+\sqrt{-3})/2 \ : \ a, b \in \mathbb{Z}\}.$$

Como en el caso de $\mathbb{Z}[i]$, los círculos de radio 1 centrados en los puntos de $\mathbb{Z}[(1+\sqrt{-3})/2]$ cubren todo $\mathbb{C}$ y la demostración es similar.

Nota: Los anillos de la forma $\mathbb{Z}[\sqrt{d}]$ son más difíciles de estudiar en el caso $d > 0$. Si queremos probar que son de factorización única, la función N "natural" a considerar es $N(z) = |z \cdot \overline{z}|$ donde $\overline{z}$ es el conjugado real (esto es, $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$) y $|\cdot|$ es el valor absoluto. Parte de la complicación proviene de que ahora hay que considerar recubrimientos por regiones hiperbólicas no acotadas, en vez de por círculos.

Para cerrar el bucle, volvamos al problema del principio de la sección: supongamos que queremos hallar las soluciones de

$$x^2 + y^2 = 10^{20}.$$

En $\mathbb{Z}[i]$ se tiene la factorización $2 = (1+i)(1-i)$ con $1+i$ y $1-i$ irreducibles asociados porque $1+i = i(1-i)$; y $5 = (2+i)(2-i)$. De modo que la ecuación anterior se puede escribir como

$$(x+iy)(x-iy) = (1-i)^{40}(2+i)^{20}(2-i)^{20},$$

lo que implica que existen enteros $0 \le \alpha \le 40$ y $0 \le \beta, \gamma \le 20$ tales que

$$x + iy = u(1-i)^{\alpha}(2+i)^{\beta}(2-i)^{\gamma} \quad \text{y} \quad x - iy = u^{-1}(1-i)^{40-\alpha}(2+i)^{20-\beta}(2-i)^{20-\gamma}$$

con u algún elemento invertible. Conjugando la segunda ecuación y usando que que la factorización es única (recuérdese que $1+i$ y $1-i$ están asociados) se sigue $\alpha = 40-\alpha$, $\beta = 20-\gamma$ y $\gamma = 20-\beta$. Por tanto las soluciones enteras x, y de la ecuación original vienen dadas por

$$x + iy = u(1-i)^{20}(2+i)^{\beta}(2-i)^{20-\beta}.$$

Como hay 21 posibles valores de $0 \le \beta \le 20$ y 4 posibles valores de u (en $\mathbb{Z}[i]$ los elementos invertibles son $1, -1, i, -i$), tenemos 84 soluciones.

Para terminar descansadamente, recordemos los buenos y tiernos tiempos de Conjuntos y Números a través de los inofensivos anillos de polinomios $\mathbb{C}[x]$, $\mathbb{R}[x]$ y $\mathbb{Q}[x]$. Todos ellos son dominios de factorización única por ser dominios euclídeos (basta elegir como función N el grado).

Nos han dicho muchas veces que todo polinomio no constante tiene una raíz compleja, lo que por el teorema del resto se traduce en:

Teorema 1.3.4 (Teorema fundamental del Álgebra) *Sea $P \in \mathbb{C}[x]$ no constante, P es irreducible en $\mathbb{C}[x]$ si y sólo si* $\operatorname{gr} P = 1$.

Seguramente el lector ya habrá visto dos demostraciones de este teorema, una en Topología y otra en Variable Compleja I. No es posible dar una prueba totalmente algebraica porque la propia definición de $\mathbb{C}$ depende de la de $\mathbb{R}$, que está en la base del análisis. De todas formas, si alguien quiere opinar lo contrario puede, cuando termine el curso, leer [St] §18 y hacer caso omiso de las excusas.

En $\mathbb{R}[x]$ las cosas no son muy diferentes:

Teorema 1.3.5 *Si $P \in \mathbb{R}[x]$ es irreducible en $\mathbb{R}[x]$ entonces* $\operatorname{gr} P \leq 2$.

Demostración: Por el teorema anterior, si $\partial P > 1$, existe $z \in \mathbb{C}$ y $Q \in \mathbb{C}[x]$ tal que $P = (x - z)Q$. Si $z \in \mathbb{R}$, entonces $x - z$ es un factor de grado 1 de P en $\mathbb{R}[x]$. En otro caso, conjugando $P = (x - \overline{z})\overline{Q}$. Como $x - z$ y $x - \overline{z}$ son irreducibles no asociados en $\mathbb{C}[x]$, se deduce $R|P$ con $R = (x - z)(x - \overline{z})$, y es evidente que $R \in \mathbb{R}[x]$ con $\partial R = 2$. □

En $\mathbb{Q}[x]$ las cosas son más complicadas. Parece muy fácil probar que quitando denominadores podemos pasar el problema a $\mathbb{Z}[x]$, pero la demostración tiene intríngulis suficiente como para que invoquemos el nombre del *princeps mathematicorum*.

Lema 1.3.6 (Lema de Gauss) *Si $P \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}[x]$ también lo es en $\mathbb{Q}[x]$.*

Demostración: 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

$$nP = (b_l x^l + b_{l-1}x^{l-1} + \cdots + b_0)(c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0) \qquad \text{con } b_i, c_i \in \mathbb{Z}. \tag{1.4}$$

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 (1.4) 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 (1.4) los coeficientes de grado $i + j$ se tiene

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

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

Decidir si un polinomio es irreducible en $\mathbb{Z}[x]$ o $\mathbb{Q}[x]$ puede ser muy laborioso. Un criterio que es de utilidad en algunos casos es el siguiente.

Proposición 1.3.7 (Criterio de Eisenstein) *Si $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ es un polinomio con coeficientes enteros y p es un primo tal que $p \not| a_n$, $p|a_i$ si $0 \leq i < n$ y $p^2 \not| a_0$ entonces P es irreducible en $\mathbb{Q}[x]$.*

Demostración: Por el Lema de Gauss, si P no es irreducible se puede escribir como $P = (b_l x^l + b_{l-1}x^{l-1} + \cdots + b_0)(c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0)$ con $l + m = n$ y $b_i, c_i \in \mathbb{Z}$. Igualando los coeficientes de los términos del mismo grado, se tiene

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

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 $p|b_i$ $0 \leq i \leq l$, lo que implica que p divide a todos los a_i lo que contradice nuestra hipótesis $p \not| a_n$. □

Ejemplo. Los polinomios $P = x^5 - 2x + 6$ y $Q = x^7 - 12$ son irreducibles en $\mathbb{Q}[x]$. (Tómese $p = 2$ y $p = 3$ en el criterio de Eisenstein).

Una aplicación indirecta de este criterio prueba que el polinomio llamado *ciclotómico*

$$P = x^{p-1} + x^{p-2} + \cdots + x + 1$$

es irreducible en $\mathbb{Q}[x]$ si p es primo. Para ello nótese que P es irreducible si y sólo si $Q = (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1$ también lo es (ejercicio) y como

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

el criterio de Eisenstein es aplicable a Q (ejercicio). Además se puede probar que P no es irreducible si p no es primo, aunque no lo haremos aquí.

Recordemos también otro criterio sencillo de Conjuntos y Números. La demostración es muy sencilla y se deja al lector.

Proposición 1.3.8 *Dado $P \in \mathbb{Z}[x]$ sea $\overline{P} \in \mathbb{Z}_p[x]$ el polinomio que resulta al reducir los coeficientes módulo p (primo). Suponiendo que $\partial P = \partial \overline{P}$, si $\overline{P}$ es irreducible en $\mathbb{Z}_p[x]$ entonces P es irreducible en $\mathbb{Q}[x]$.*

Ejemplo. El polinomio $x^3 - 17x^2 + 10x + 105$ 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 $\mathbb{Z}_2[x]$ se podría escribir como $(x^2 + ax + b)(x - c)$, lo cual es imposible porque ni x ni $x - 1$ dividen a $x^3 + x^2 + 1$.

Ejercicios del Capítulo 1

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 1.1

1. 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 anillo tal que todos sus elementos no nulos son unidades.
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 anillo tal que todos sus elementos no nulos son unidades.

♡**2.** Sean $R_1, \ldots, R_n$ anillos. Demostrar que $R_1 \oplus \ldots \oplus R_n$ es un anillo con las operaciones de suma y producto obvias (las dadas por las de cada R_i coordenada a coordenada).

♡**3.** Escribir la tabla de multiplicación del anillo $\mathbb{Z}_3[i] = \{a + bi : a, b \in \mathbb{Z}_3\}$.

4. El conjunto $\{0, 2, 4, 6, 8\}$ es un anillo conmutativo con unidad, con la suma y el producto módulo 10. ¿Cuál es la unidad multiplicativa? ¿Y los elementos invertibles?

5. Probar que los elementos neutros de las operaciones de un anillo con unidad son únicos.

6. Comprobar que las unidades de $\mathbb{Z}_{17}$ forman un grupo cíclico.

7. ¿Cuántas unidades hay en $\mathbb{Z}_{10^6}$?

8. Hallar todas las unidades en $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[(1 + \sqrt{-3})/2]$ y en el anillo de matrices enteras 2×2.

9. Probar que $2x + 1$ tiene inverso multiplicativo en $\mathbb{Z}_4[x]$.

10. Hallar las unidades del anillo de matrices 2×2 con elementos en $\mathbb{Z}_4$.

11. Hallar el inverso multiplicativo de 5 en $\mathbb{Z}_{21}$ usando el algoritmo de Euclides.

12. Probar que en el anillo de matrices reales $n \times n$, para todo elemento, m, que no es una unidad, existe $m' \neq 0$ tal que $m'm = 0$.

13. Encontrar un anillo R en el que no se verifiquen ninguna de las siguientes propiedades:
i) Si $a^2 = a$, entonces $a = 1$ ó $a = 0$.
ii) Si $ab = ac$ para $a \neq 0$ entonces $b = c$.

14. Si R no es un dominio de integridad la intuición que tenemos sobre ecuaciones algebraicas puede ser completamente errónea. Meditemos sobre este hecho:
i) Buscar un anillo R en el que la ecuación $ax = b$ con $a, b \in R$ tenga más de una solución.

ii) Encontrar todas las soluciones de la ecuación $x^2 - 5x + 6 = 0$ en $\mathbb{Z}_{12}$.

♡**15.** Sea $f : R \to S$ un homomorfismo de anillos. Demostrar que:
i) Para todo $r \in R$, y para todo entero positivo n, se tiene que $f(r^n) = f(r)^n$.
ii) La imagen de R por f, $\{s \in S : s = f(r), \text{ para algún } r \in R\}$, es un subanillo de S.

♡**16.** Sea $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ dada por $\phi(P) = 2^{\partial P}$. Estudiar si es un homomorfismo.

17. Probar que el anillo $\mathbb{Z}_6$ es isomorfo al anillo $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

18. Demostrar que los anillos $\mathbb{Z}[\sqrt{7}] = \{a + b\sqrt{7} : a, b \in \mathbb{Z}\}$ y

$$R = \left\{ \begin{pmatrix} c & 7d \\ d & c \end{pmatrix} : c, d \in \mathbb{Z} \right\}$$

son isomorfos.

19. Demostrar que la aplicación $f : \mathbb{Z}_n \to \mathbb{Z}_n$ dada por $f(x) = x^n$ es un homomorfismo de anillos si n es primo. ¿Es el resultado cierto si n no es primo?

∘**20.** 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.

∘**21.** Sea $s_k = x_1^k + x_2^k + \cdots + x_n^k$ para $0 < k$ y $s_0 = k$. Demostrar las "identidades de Newton"

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

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

Sección 1.2

♡**22.** Probar que a y b están asociados si y sólo si $\langle a \rangle = \langle b \rangle$.

23. ¿Cuándo tiene sentido $n\mathbb{Z}/m\mathbb{Z}$?

24. Hallar el generador mónico del ideal $I = \langle x^3 + 1, x^2 + 1 \rangle$ en $\mathbb{Z}_2[x]$.

♡**25.** Demostrar que $\mathbb{Q}[x]/\langle x^2 - 5x + 6 \rangle$ no es un dominio de integridad.

26. En $\mathbb{Z}[x]$ sea I el subconjunto formado por los polinomios tales que la suma de sus coeficientes es cero. Probar que I es un ideal y que $\mathbb{Z}[x]/I$ es isomorfo a $\mathbb{Z}$.

27. Hallar un subanillo de $A = \mathbb{Z}[\sqrt{2}]$ que no sea ideal.

28. Probar que todos los subanillos de $\mathbb{Z}$ son ideales. Dar un contraejemplo si $\mathbb{Z}$ se reemplaza por $\mathbb{Z} \oplus \mathbb{Z}$.

29. Demostrar que el grupo multiplicativo de $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ es cíclico y dar un generador.

30. Hallar los ideales de $\mathbb{Z}_{24}$.

31. Sea $f : R \to S$ un homomorfismo de anillos. Demostrar que:
i) Si $J \subset S$ es un ideal, entonces $f^{-1}(J) = \{r \in R : f(r) \in J\}$ es un ideal en R.
ii) El núcleo de f es un ideal.
iii) Un homomorfismo de anillos es inyectivo si y sólo si su núcleo es $\{0\}$.

32. Dado un anillo R y un ideal $I \subset R$, demostrar que hay una correspondencia biyectiva entre los ideales de R/I y los ideales de R que contienen a I. *Indicación*: usar el homomorfismo natural $\pi : R \to R/I$, que a cada elemento $a \in R$ le asocia su clase módulo I, y observar que la imagen inversa de un ideal por un homomorfismo de anillos es también un ideal.

33. Sea $A = \mathbb{Z}[\sqrt{2}]$. Hallar todos los ideales del anillo $A/2A$.

34. Hallar los ideales de $\mathbb{Q}[x]/\langle x^3-1\rangle$.

35. Decidir si el ideal $\langle 29, 13+\sqrt{-5}\rangle$ es principal en $\mathbb{Z}[\sqrt{-5}]$

36. Probar que el anillo de matrices cuadradas reales $n \times n$ no tiene ideales no triviales.

37. Encontrar todos los ideales maximales de los anillos $\mathbb{Z}_8$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$ y $\mathbb{Z}_n$.

38. Probar que $I = \{(3n, m) : n, m \in \mathbb{Z}\}$ es un ideal maximal en $\mathbb{Z} \oplus \mathbb{Z}$.

39. Sea $I \subset \mathbb{Z}[\sqrt{-5}]$ dado por $I = \{a + b\sqrt{-5} \ : \ a + b \text{ es par}\}$. Demostrar que es un ideal maximal de $\mathbb{Z}[\sqrt{-5}]$.

♢**40.** Sean I y J, con $J \subset I$, ideales de un anillos A. Probar que A/I es isomorfo a $(A/J)/(I/J)$. (Esto requiere en particular probar que este último cociente tiene sentido).

♢**41.** Sea p primo y sea $A \subset \mathbb{Q}$ el anillo formado por todas las fracciones cuya forma irreducible tiene denominador no divisible por p. Hallar un anillo sencillo que sea isomorfo a $A/\langle p\rangle$.

Sección 1.3

42. Sea el conjunto $H = \{1, 5, 9, 13, 17, 21, 25 \dots\}$. Decimos que $p \in H$ es un H-primo si $p \neq 1$ y no es divisible por ningún elemento de H salvo por sí mismo y por uno. Por ejemplo, 5 y 9 son H-primos, pero $25 = 5 \cdot 5$ no. Comprobar que 693 tiene varias posibles descomposiciones en factores H-primos. (Nota: Hilbert (1862-1943) propuso H como un conjunto sencillo en el que no se cumple el análogo del teorema fundamental de la aritmética).

43. Hallar todos los polinomios irreducibles en $\mathbb{Z}_2[x]$ de grados 2, 3 y 4.

44. Decir si son irreducibles en $\mathbb{Q}[x]$ los polinomios $3x^2-7x-5$, $6x^3-3x-18$ y x^3-7x+1.

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

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

47. Probar la irreducibilidad en $\mathbb{Q}[x]$ de los polinomios: x^5-3x+3, x^6-6x+2, x^2+1, x^4+1 y x^6+x^3+1.

48. Probar que $P\in\mathbb{Q}[x]$ es irreducible si y sólo si Q dado por $Q(x)=P(x+1)$, lo es.

49. Probar que el criterio de Eisenstein es aplicable al polinomio

$$x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\cdots+\binom{p}{p-2}x+\binom{p}{p-1}.$$

50. Decidir si los siguientes polinomios son irreducible en $\mathbb{Q}[x]$: x^4+3x+6, $x^3+11^{11}x+13^{13}$, $\frac{1}{3}x^5+\frac{5}{2}x^4+\frac{3}{2}x^3+\frac{1}{2}$, x^5-9x^2+1 y x^4-x^3-x-1.

51. Probar que x^2+bx+c es irreducible en $\mathbb{Z}_7[x]$ si y sólo si $b^2-4c=3,5,6$.

52. Estudiar la irreducibilidad de $P=x^2+1$ en $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_7[x]$, $\mathbb{Z}_{11}[x]$, $\mathbb{Z}_{13}[x]$ y $\mathbb{Z}_{17}[x]$.

∘**53.** Intentar inducir (sin demostración) una regla general sencilla que permita decidir la irreducibilidad de $P=x^2+1$ en $\mathbb{Z}_p[x]$ sin calcular sus raíces.

54. Hallar un contraejemplo a la Proposición 1.3.8 si se omite la condición $\partial P=\partial\overline{P}$.

55. Estudiar si $\mathbb{Z}[\sqrt{-2}]$ es un dominio de factorización única.

56. Demostrar que $\mathbb{Z}[\sqrt{2}]$ es un dominio de factorización única y encontrar la factorización de 20. *Indicación*: La ecuación en enteros $a^2-2b^2=5$ no tiene solución (lleva a contradicción módulo 5).

57. Estudiar si $\mathbb{Z}[\sqrt{-6}]$ es un dominio de factorización única.

♢**58.** Estudiar si $\mathbb{Z}[\sqrt{6}]$ es un dominio de factorización única.

♢**59.** Demostrar que un polinomio de la forma $P=x^n+px+p^2$ es irreducible en $\mathbb{Z}[x]$.

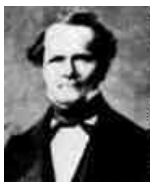
♢**60.** Sea $p>2$ primo. Demostrar que existen $n,m\in\mathbb{Z}$ tales que $p=n^2+mn+m^2$ si y sólo si $P=x^2+x+1$ factoriza en $\mathbb{Z}_p[x]$.

Apéndice del Capítulo 1

Conoce a tus héroes

(Más información en: `http://turnbull.mcs.st-and.ac.uk/history/`)

E. Kummer no sólo fue un gran matemático sino también un magnífico profesor con gran predicamento entre los alumnos. Su trabajo relativo al último teorema de Fermat fue verdaderamente revolucionario, tanto es así, que la Academia de Ciencias de París le concedió en 1857 el premio destinado al que probase este resultado, a pesar de que los razonamientos de Kummer no se podían aplicar a todos los exponentes, constituyendo una solución parcial.



Apellido: Kummer
Nombre: (Ernst) Eduard
Nacimiento: 1810 Sorau
Defunción: 1893 Berlín

Bla, bla, bla

- *La introducción de tales números complejos ideales tiene el mismo motivo simple y básico que lleva a introducir fórmulas imaginarias en álgebra y análisis; concretamente, la descomposición de funciones racionales en sus factores más simples, los lineales.* E. Kummer 1847.

- *. . . la fuente de todas las Matemáticas grandiosas es el caso particular, el ejemplo concreto. Es frecuente en Matemáticas que toda aparición de un concepto de aparente gran generalidad sea en esencia la misma que la de un concreto y pequeño caso particular.* P. Halmos.

- [Acerca del título del libro de Al-Khwārizmī, *Hisab al-jabr w'al-muqābala*, que dio origen a la palabra "álgebra"] Jabr *es la colocación de un hueso, de aquí reducción o restauración;* muqābala *es confrotación, oposición, enfrentamiento.* Citado en [Ca], p. 203.

- *En esto fueron razonando los dos, hasta que llegaron a un pueblo donde fue ventura hallar un algebrista, con quien se curó el Sansón desgraciado.* "El ingenioso hidalgo don Quijote de la Mancha"(2ª parte). Capítulo XV.

¿Qué hay que saberse?

Todo lo que no esté en letra pequeña. En particular, hay que saber: manejar el concepto de anillo (y aplicaciones entre ellos) y de ideal (principal, maximal); manipular

cocientes con soltura; comprender el problema de factorización y su relación con los ideales, siendo capaz de estudiar si hay factorización única en ejemplos fáciles; saber decidir la irreducibilidad en $\mathbb{Q}[x]$ y $\mathbb{Z}[x]$ de polinomios sencillos.

(PQR) Preguntón, quejoso y respondón

P- ¿Hay un algoritmo para factorizar en $\mathbb{Q}[x]$?

R- Por el lema de Gauss, basta considerar el problema en $\mathbb{Z}[x]$. Si $R = PQ$ entonces los términos independientes de P y Q son divisores del de R, lo cual da un número finito de posibilidades para ellos, lo mismo se puede hacer inductivamente para el resto de los coeficientes. El problema es que este algoritmo es tan poco eficiente que muy pocas veces lo podríamos llevar a cabo "a mano", de ahí el interés de los trucos como el criterio de Eisenstein.

Q- Si no hay métodos sistemáticos para humanos sin ordenador, ¿cómo quieren que factoricemos en $\mathbb{Q}[x]$ en este curso?

R- Evidentemente los ejemplos están preparados y se trata de atajar los cálculos con ingenio.

Q- Eso de los ideales es una cosa muy rara.

R- Sí que lo es, pero se muestra fundamental al estudiar la factorización.

P- No entiendo por qué para factorizar en $\mathbb{Z}[\sqrt{-5}]$ hay que introducir esos extraños números ideales. Por ejemplo, para hacer un polinomio de $\mathbb{R}[x]$ factorice del todo sólo hay que permitir usar números complejos, que pueden ser raros, pero son números al fin y al cabo.

R- Sí, en principio se podría resolver el problema de factorización en subanillos de $\mathbb{C}$ ampliándolos con nuevos números complejos. Lo malo es que los nuevos números añadidos pueden tener a su vez problemas de factorización entre ellos y necesitar de otra ampliación. La llamada teoría de cuerpos de clases nos dice que el proceso podría no terminar nunca.

P- Entonces los ideales sólo sirven para factorizar.

R- Se inventaron para ello, pero los ideales tienen un alcance mucho más amplio porque son lo único con lo que se pueden hacer cocientes de anillos, es decir, reducirlos. Si tomamos cociente entre los ideales más grandes, los maximales, nos quedaremos con los trozos de anillo más pequeños. Por ejemplo, en geometría algebraica se arreglan las cosas para que una curva algebraica sea un anillo, y en esta correspondencia los puntos son los ideales maximales. En general se puede asignar un anillo a una variedad algebraica (curvas, superficies, etc. definidas por polinomios) y sus ideales primos corresponden a las subvariedades algebraicas.

Q- Eso parece más raro todavía.

P- ¿Dónde se pueden aprender esas cosas?

R- En Álgebra III.

Capítulo 2

Cuerpos y sus extensiones

2.1. Definición de cuerpo

A lo largo de todo el curso trabajaremos primordialmente con raíces de polinomios, y en la próxima sección probaremos que las operaciones elementales (suma, resta, multiplicación y división) preservan el conjunto formado por ellas. Por ejemplo, podremos deducir que $(1+\sqrt{7})/(1-\sqrt[3]{5})$ es raíz de cierto polinomio en $\mathbb{Q}[x]$ porque 1, $\sqrt{7}$ y $\sqrt[3]{5}$ son raíces de polinomios en $\mathbb{Q}[x]$. Con esto en mente, procedemos como es habitual en Matemáticas, creando una estructura algebraica general que permita abstraer las propiedades esenciales.

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

En pocas palabras, un cuerpo es un conjunto donde podemos sumar, restar, multiplicar y dividir con las propieddes habituales. La exclusión del cero en la definición se debe simplemente a que como todo el mundo sabe, no se puede dividir por cero (bueno, todos menos K. Marx que en "El capital" I §9, después de enunciar una ley económica paradójica, escribe: "Para resolver esta contradicción aparente se requieren aún muchos eslabones intermedios, tal como en el plano del álgebra elemental se necesitan muchos términos medios para comprender que 0/0 puede representar una magnitud real").

Ejemplo. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.

Ejemplo. $K=\{a+b\sqrt{2}\ :\ a,b\in\mathbb{Q}\}$ es un cuerpo.
Lo único que no es del todo evidente es la existencia del inverso multiplicativo. Sólo hay que racionalizar:

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in K.$$

Ejemplo. 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 $r/s\sim t/u\Leftrightarrow ru=ts$. Con las operaciones naturales, el cuerpo de fracciones hace honor a su nombre y realmente tiene estructura de cuerpo.

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 $\mathbb{Q}$.

Si $\mathcal{D}$ no fuera dominio de integridad, por mucho que nos empeñásemos en dividir, no podríamos llegar a nada con sentido. Por ejemplo, si queremos inventar un "algo" en un cuerpo que extienda a $\mathbb{Z}_6$, tal que $2/3 = algo$, multiplicando por 9 tenemos $0 = 3{\cdot}$algo, con lo que "algo" no tendría inverso (en ese caso $0 = 3$). Las dificultades las dan los divisiores de cero, si no fuera por ellos, como en el cuento de Aladino, tendríamos un flamante cuerpo a partir de un anillo .

Si K es un cuerpo, $K[x]$ es un dominio de integridad y se puede definir su cuerpo de fracciones que se denota con $K(x)$.

$$K(x) = \Big\{ \frac{P}{Q} \ : \ P, Q \in K[x], \ Q \neq 0 \Big\}.$$

Como en el caso de $K[x]$, se suele abusar ligeramente de la notación permitiendo escribir $K(\alpha)$ con α en algún cuerpo que contiene a K, para representar

$$K(\alpha) = \Big\{ \frac{P(\alpha)}{Q(\alpha)} \ : \ P, Q \in K[x], \ Q(\alpha) \neq 0 \Big\}.$$

Desde otro punto de vista, $K(\alpha)$ es el resultado de añadir α a K y hacer todas las posibles sumas, restas, multiplicaciones y divisiones. Con este lenguaje el cuerpo del penúltimo ejemplo es $\mathbb{Q}(\sqrt{2})$. En general, razonando de la misma forma:

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Q}\}.$$

La notación admite una generalización obvia. Se indica con $K(x_1, x_2, \dots \ x_n)$ el cuerpo de fracciones de $K[x_1, x_2, \dots \ x_n]$, y si $\alpha_1, \alpha_2, \dots \ \alpha_n$ están en un cuerpo que contiene a K entonces se escribe $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ para representar:

$$\Big\{ \frac{P(\alpha_1, \alpha_2, \dots, \alpha_n)}{Q(\alpha_1, \alpha_2, \dots, \alpha_n)} \ : \ P, Q \in K[x_1, x_2, \dots, x_n], \ Q(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0 \Big\}.$$

Es fácil ver que $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ es el cuerpo "más pequeño" que contiene a K y a $\alpha_1, \alpha_2, \dots \ \alpha_n$. También es posible razonar definiendo inductivamente este cuerpo como $K(\alpha_1, \alpha_2, \dots, \alpha_n) = \big(K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})\big)(\alpha_n)$.

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

Esto no es más que un caso particular de la Proposición 1.2.3 porque $\mathbb{Z}_p$ es por definición $\mathbb{Z}/p\mathbb{Z}$.

Observación: Cuando consideramos $\mathbb{Z}_p$ como cuerpo en vez de como anillo, la notación habitual, que utilizaremos a partir de ahora, es $\mathbb{F}_p$.

Estirando este ejemplo, podemos transformar la Proposición 1.2.3 en conjunción con la 1.3.2 en una fábrica de cuerpos muy retorcidos. Antes de ello, una observación.

Teorema 2.1.1 *Si K es un cuerpo, $K[x]$ es un dominio euclídeo.*

Demostración: La misma que en $\mathbb{Q}$. Basta tomar $N(P) = \partial P$. $\square$

Ejemplo. Dado un cuerpo K y $P \in K[x] - \{0\}$ irreducible, $K[x]/(P)$ es un cuerpo.

Por la Proposición 1.3.2, (P) es maximal y basta aplicar la Proposición 1.2.3. De hecho la irreducibilidad de P es condición necesaria y suficiente para que el cociente sea cuerpo.

Los cocientes de anillos de polinomios serán especialmente importantes este curso, pero nada impediría crear cuerpos tomando cociente en otros anillos. Sólo para practicar veamos un ejemplo desarrollado en este sentido.

Ejemplo. Si $A \subset \mathbb{C}$ es el anillo $A = \left\{n+m\sqrt{-2} \ : \ n, m \in \mathbb{Z}\right\}$, entonces $A/\langle 1+\sqrt{-2}\rangle$ 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 $A/\langle 1+\sqrt{-2}\rangle = \left\{\overline{0}, \overline{1}, \overline{2}\right\}$ (es fácil comprobar que estas tres clases son distintas). Con ello demostramos que $A/\langle 1 + \sqrt{-2}\rangle$ es idéntico a $\mathbb{F}_3$ salvo cambiar nombres (isomorfo). 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 $A/\langle n+m\sqrt{-2}\rangle$ es isomorfo a $\mathbb{F}_p$.

Nota: Las defininiciones de epimorfismo, monomorfismo e isomorfismo se pueden aplicar igualmente a cuerpos, porque un cuerpo es en particular un anillo con unidad.

Aunque la Proposiciones 1.2.3 y 1.3.2 nos juren por los axiomas de las Matemáticas que si P es irreducible $K[x]/\langle P\rangle$ es un cuerpo, no parece nada claro cómo hacer divisiones allí, concretamente cómo hallar el inverso. Para solucionar este problema basta recordar cómo se procede en $\mathbb{F}_p$. Si queremos hallar el inverso de $\overline{a}$, resolvemos la ecuación en enteros $1 = ax + py$, lo cual se podía hacer empleando el algoritmo de Euclides, y reduciendo módulo p se sigue $\overline{1} = \overline{a} \cdot \overline{x}$, esto es, $\overline{a}^{-1} = \overline{x}$. En $K[x]/\langle P\rangle$ todo funciona exactamente igual cambiando el primo p por el polinomio irreducible P.

Como eso del algoritmo de Euclides y la identidad de Bezout se pierde en los añejos abismos de Conjuntos y Números, no está de más ver un par de ejemplos que clarifiquen la situación.

Ejemplo. Hallar el inverso de $\overline{8}$ en $\mathbb{F}_{29}$.

Según lo indicado antes, debemos hallar una solución $n, m \in \mathbb{Z}$ de $1 = 29n + 8m$ y, al reducir módulo 29, se tiene que $\overline{m}$ es la clase que buscamos. Para hallar una solución $n, m \in \mathbb{Z}$ se aplica primero el algoritmo de Euclides a 29 y 8. Como son coprimos (condición necesaria y suficiente para que exista el inverso), al final se obtendrá un uno, que podemos despejar de abajo a arriba hasta conseguir la solución deseada:

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

Así pues podemos tomar $n = -3$ y $m = 11$ y se concluye que $\overline{11}$ es el inverso de $\overline{8}$. Para los incrédulos: $11 \cdot 8 = 88 = 1 + 3 \cdot 29$.

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

Obsérvese que P es irreducible por ser el polinomio ciclotómico para $p = 5$. Buscamos una solución de $1 = AP + BQ$ para ciertos $A, B \in \mathbb{Q}[x]$, de donde $\overline{1} = \overline{BQ}$, y $\overline{B}$ será el inverso de $\overline{Q}$. Calculamos A y B procediendo como en el ejemplo anterior:

$$\begin{array}{l} P = Q \cdot x^2 + (x+1) \\ Q = (x+1) \cdot x + 1 \end{array} \Rightarrow \begin{array}{l} (2^{\text{a}} \text{ ecuación}) \ 1 = Q - x(x+1) \\ (1^{\text{a}} \text{ ecuación}) \ 1 = Q - x(P - x^2 Q) = -xP + (x^3+1)Q. \end{array}$$

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

Los $\mathbb{F}_p$ no son los únicos cuerpos finitos.

Ejemplo. $K = \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$ es un cuerpo de cuatro elementos y el inverso de $\overline{x}$ es $\overline{x + a}$.

Como $x^2 + x + 1$ es irreducible en $\mathbb{F}_2[x]$ (es de segundo grado y no tiene raíces en $\mathbb{F}_2$), K es un cuerpo. Ahora, hallando el resto al dividir por $x^2 + x + 1$, cualquier polinomio $P \in \mathbb{F}_2[x]$ es equivalente a otro de la forma $ax + b$ con $a, b \in \mathbb{F}_2$. Esto da cuatro posibilidades (no equivalentes), obteniéndose $K = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$. En $\mathbb{F}_2[x]$ se cumple $x(x+1) = 1 + (x^2 + x + 1)$, por tanto $\overline{x}$ y $\overline{x+1}$ son inversos uno del otro.

Nota: Tras este ejemplo cabría preguntarse qué cardinal puede tener un cuerpo finito. Resolveremos este problema más adelante en el curso cuando clasifiquemos todos los cuerpos finitos. Por ahora, como intriga de serial, avanzaremos que la lista de posibles cardinales comienza con 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17,.... La solución, en el tercer capítulo.

Ligado a los cuerpos finitos, pero no específico de ellos, está el concepto de característica, que desempeña un curioso papel en algunas propiedades de los cuerpos necesarias para poder aplicar la teoría de Galois.

Definición: Diremos que un cuerpo K (o un anillo) tiene *característica* n si n es el menor número natural tal que $1 + 1 + \overset{n \text{ veces}}{\ldots} + 1 = 0$. Si esta suma fuera siempre distinta de cero se dice que el cuerpo tiene *característica cero*. La notación habitual es $\text{char}(K) = n$.

Ejemplo. $\mathbb{C}$, $\mathbb{R}$ y $\mathbb{Q}$ tienen característica cero.

Ejemplo. $\mathbb{F}_5$ y $\mathbb{F}_5(x)$ tienen característica 5. (El primer cuerpo es finito y el segundo no lo es).

Ejemplo. Si K es un subcuerpo de $\mathbb{C}$, $\text{char}(K) = n$.

2.2. Extensiones de cuerpos

Habitualmente, para resolver una ecuación algebraica no basta con hacer sumas, restas, multiplicaciones y divisiones de los coeficientes, sino que tenemos que añadir algo que extienda el cuerpo generado por los coeficientes (por ejemplo $\sqrt{b^2-4ac}$ en el caso de la ecuación de segundo grado). Así como en Álgebra I estuvimos todo el rato mirando dentro de los grupos estudiando subgrupos y más subgrupos, en Álgebra II seremos más místicos y universalistas buscando experiencias fuera de los cuerpos.

Definición (provisional): Decimos que el cuerpo L es una *extensión* 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.

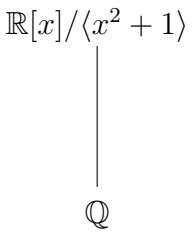
La notación que se usa habitualmente para designar una extensión es L/K o también $L : K$ (aquí preferiremos la primera).

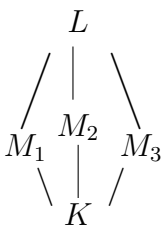
Aunque la definición anterior es satisfactoria en casi todos los casos que aparecerán en el curso, conviene al menos mencionar otra definición un poco más general y más conveniente desde el punto de vista abstracto.

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

Observación: Como recordamos en el primer capítulo, un monomorfismo es una función inyectiva compatible con las operaciones. Para comparar ambas definiciones consideremos $\mathbb{C}$ y $\mathbb{R}/\langle x^2+1\rangle$, que más adelante veremos que son cuerpos isomorfos, es decir, son el mismo cuerpo cambiando los nombres de los elementos. Con la primera definición $\mathbb{C}$ es una extensión de $\mathbb{Q}$, pero en rigor $\mathbb{Q}$ no está incluido en $\mathbb{R}[x]/\langle x^2+1\rangle$ porque este segundo cuerpo es un conjunto de clases de polinomios. Todo vuelve a funcionar si consideramos la composición $\mathbb{Q} \hookrightarrow \mathbb{C} \longleftrightarrow \mathbb{R}[x]/\langle x^2+1\rangle$ que es inyectiva y se ajusta a la segunda definición. A primera vista estas sutilezas y excesos de rigor parecen pamplinas matemáticas, sin embargo aparecerán de forma natural al estudiar cuerpos de descomposición.

Las extensiones de cuerpos muchas veces se indican con diagramas similares a los empleados por ejemplo en los retículos de subgrupos, situándose a mayor altura los cuerpos que "extienden" y conectándolos con líneas a los que son "extendidos". Por ejemplo, la extensión que acabamos de mencionar está representada en el diagrama de la izquierda, mientras que el de la derecha significa que L/M_1, L/M_2, L/M_3, M_1/K, M_2/K y M_3/K son extensiones de cuerpos. En particular, L/K también lo será.





Señalaremos tres tipos destacados de extensiones de cuerpos. En este curso trataremos fundamentalmente las del segundo con $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ y α_i raíces de polinomios en $K[x]$. Un sorprendente resultado del próximo capítulo (el teorema del elemento primitivo) asegurará que casi todas las extensiones de esta forma que podemos imaginar a este nivel, son también del primer tipo.

Definición: Se dice que una extensión, L/K, es:

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

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

3) *trascendente*, si no es algebraica. En particular existirá algún $\alpha \in L$ que es *trascendente*, es decir, que no es no algebraico.

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

La segunda es simple porque $\mathbb{Q}(x) = \mathbb{Q}(x^2, x) = \big(\mathbb{Q}(x^2)\big)(x)$. Los elementos $\mathbb{Q}\big(\sqrt{2}\big)$ son de la forma $a+b\sqrt{2}$ con $a, b \in \mathbb{Q}$ y satisfacen la ecuación algebraica $(x-a)^2-2b^2 = 0$, por tanto la primera extensión es algebraica. Para la segunda el argumento es similar si tomamos la precaución de no confundir x con la variable del polinomio que elijamos. Los elementos de $\mathbb{Q}(x)/\mathbb{Q}(x^2)$ son de la forma $f + xg$ con $f, g \in \mathbb{Q}(x^2)$ y por tanto resuelven la ecuación $(X - f)^2 - x^2g^2 = 0$. Nótese que $(X - f)^2 - x^2g^2 \in \mathbb{Q}(x^2)[X]$.

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

Ejemplo. $\mathbb{C}(x, y)/\mathbb{Q}$ no es simple y es trascendente.

Ejemplo. (Lindemann 1882) $\mathbb{Q}(\pi)/\mathbb{Q}$ es trascendente.

Éste es un resultado muy difícil que probaremos en la última sección del presente capítulo, junto con que $\mathbb{Q}(e)/\mathbb{Q}$ es trascendente.

Observación: 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 resultado es prácticamente trivial, pero ocupa un papel destacado porque permite ligar la teoría de cuerpos, que todavía no nos sabemos, con el álgebra lineal de la que conocemos todo.

Proposición 2.2.1 *Si L/K es una extensión de K, entonces L es un espacio vectorial sobre K.*

Este resultado no sería tan relevante y pasaría de proposición a observación pedante, si no tuvieramos maneras de hacer cálculos con dimensiones y bases, y de usar verdaderamente el álgebra lineal. De ello trata una ristra de proposiciones que se enunciarán enseguida. Antes, un par de sencillas pero cruciales definiciones para poder hablar más con menos palabras.

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.

Nota: Recuérdese que un polinomio es *mónico* si su coeficiente de mayor grado es 1.

Observación: No es difícil demostrar que el polinomio mínimo, P, de α es único y además cumple (ejercicio)

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

Evidentemente, el polinomio mínimo depende del cuerpo sobre el que trabajemos. Muchas veces, si no se indica otra cosa, se sobreentiende que $K = \mathbb{Q}$.

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

Ahora ya pasamos a la prometida ristra de proposiciones:

Proposición 2.2.2 *Si L/K y M/L son extensiones de cuerpos*

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

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.

Demostración: Nos restringiremos al caso en que las extensiones son finitas (el otro queda como ejercicio). La proposición se reduce a probar que $B = \{x_1y_1, x_1y_2, \ldots, x_ry_s\}$ 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 $\{y_1, y_2, \ldots, y_s\}$

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

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

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

Sustituyendo estas igualdades en las anteriores se obtiene que z es una combinación lineal de elementos de B con coeficientes en K.

2) *B es linealmente independiente*: 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

$$\sum_{j=1}^{s}\left(\sum_{i=1}^{r}\lambda_{ij}x_i\right)y_j=0 \;\Rightarrow\; \sum_{i=1}^{r}\lambda_{ij}x_i=0 \qquad 1\le j\le s,$$

porque los términos entre paréntesis pertenecen a L y los y_j son una base de M/L. Como, por otra parte, los x_i son una base de L/K, de la última igualdad se concluye finalmente $\lambda_{ij}=0$. □

Proposición 2.2.3 *Toda extensión finita es algebraica.*

Demostración: 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, ...; esto es, existen $\lambda_i\in K$, $0\le i\le n$, no todos nulos tales que $\lambda_n\alpha^n+\lambda_{n-1}\alpha^{n-1}+\cdots+\lambda_1\alpha+\lambda_0=0$, por tanto α es algebraico. □

Proposición 2.2.4 *$K(\alpha)/K$ 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*

$$K(\alpha)=\left\{\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+\cdots+\lambda_{n-1}\alpha^{n-1} \;\; \textit{con } \lambda_i\in K\right\}.$$

Demostración: Sea $\mathcal{A}$ el conjunto que aparece al final del enunciado, esto es,

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

Suponiendo conocido que $K(\alpha)=\mathcal{A}$, para comprobar que $[K(\alpha):K]=n$, basta ver que no existe ninguna combinación lineal no trivial nula en $\mathcal{A}$. Si $\lambda_0+\lambda_1\alpha+\cdots+\lambda_k\alpha^k$ con $k\le n$, entonces α sería raíz de un polinomio de grado menor que n, lo cual es una contradicción.

Falta por tanto comprobar $K(\alpha)=\mathcal{A}$. 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, aplicando el algoritmo de Euclides podemos encontrar $A,B\in K[x]$ tales que

$$1=AP+BQ_2.$$

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

$$\frac{Q_1(\alpha)}{Q_2(\alpha)}=Q_1(\alpha)B(\alpha).$$

Por otra parte, al dividir Q_1B entre P se consigue $Q_1B=PC+R$ con $\partial R<\partial P=n$, lo que empleado en la igualdad anterior prueba el resultado. □

Las extensiones algebraicas simples, también se pueden ver como cocientes por ideales, y esto no es rizar el rizo, sino que tendrá gran utilidad en el próximo capítulo para probar elegante y simplemente algunos resultados básicos de la teoría de Galois.

Proposición 2.2.5 *Sea L/K y sea P el polinomio mínimo de $\alpha \in L$ sobre K, entonces*

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

con $\psi(\alpha) = \overline{x} = x + \langle P\rangle$, define un isomorfismo de cuerpos.

Demostración: Por la proposición anterior se tiene que $\alpha_1, \alpha_2 \in K(\alpha) \Rightarrow \alpha_1 = Q_1(\alpha)$, $\alpha_2 = Q_2(\alpha)$ y $\alpha_1\alpha_2 = Q_3(\alpha)$ con $\partial Q_i < \partial P$.

Es obvio 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 $K[x]/\langle P\rangle$ 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 α en $\overline{x}$, que genera $K[x]/\langle P\rangle$, 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. □

Ejemplo. $\mathbb{C}$ es isomorfo a $\mathbb{R}[x]/\langle x^2 + 1\rangle$.

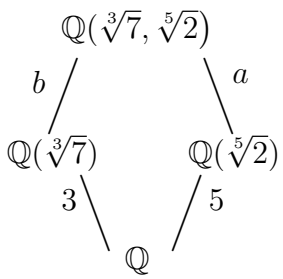
Esta aplicación directa de la Proposición 2.2.5 permite pensar en los números complejos sin introducir cosas tan poco justificables como la raíz cuadrada de -1. A cambio hay que dar un gran salto en la abstracción.

Ejemplo. La Proposición 2.2.4 asegura que $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$ y además

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

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 2.2.2 considerando las extensiones $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.

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



Por la Proposición 2.2.4, 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 2.2.2 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 en $\mathbb{Q}(\sqrt[5]{2})[x]$ (y también en $\mathbb{Q}[x]$) 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 concluye que $b = 5$ y que $n = 15$.

Ejemplo. Si $\alpha \in \mathbb{C}$ es una raíz del polinomio irreducible $P = x^3 + 3x + 3$, expresar $1/(\alpha+1)$ como una combinación lineal racional de 1, α y α^2; es decir, hallar $a, b, c \in \mathbb{Q}$ tales que $1/(\alpha+1) = a + b\alpha + c\alpha^2$.

Nótese que la Proposición 2.2.4 asegura que esto es posible. Tomemos $Q = x + 1$, como P es irreducible el máximo común divisor de P y Q es 1, existen $A, B \in \mathbb{Q}[x]$ tales que

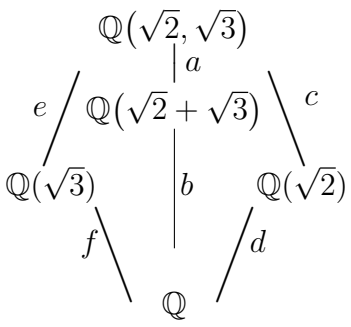
$$1 = AP + BQ.$$

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

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

Ejemplo. Comparar los cuerpos $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}$.

Se tiene un esquema como el adjunto, donde las letras cursivas representan los grados, que hallaremos a continuación.



Los polinomios mínimos sobre $\mathbb{Q}$ de $\sqrt{2}$ y $\sqrt{3}$ son $x^2 - 2$ y $x^2 - 3$ respectivamente, y $x^2 - 2$ 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 2.2.2 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). Para ver que $a = 1$ y $b = 4$, considérense los polinomios $\left(x - (\sqrt{2}+\sqrt{3})\right)^2 - 3$ 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 $x - \sqrt{2}$, por tanto $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ 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 $b = 4$.

Parece una casualidad o un milagro forzado que en el ejemplo anterior se hayan podido reducir dos generadores a uno, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, pero como antes hemos insinuado, hay un sorprendente resultado del próximo capítulo que afirma que esto es moneda común. En particular se deducirá que es imposible encontrar extensiones finitas de cuerpos normales y corrientes ($\mathbb{Q}$, $\mathbb{F}_p$, subcuerpos de $\mathbb{C}\ldots$) que no sean simples.

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

Por el ejemplo anterior $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$, 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 $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ es una base de $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big) = \mathbb{Q}\big(\sqrt{2}+\sqrt{3}\big)$ (por la Proposición 2.2.2), 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

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

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 $\partial P = [\mathbb{Q}\big(\sqrt{2}+\sqrt{3}\big) : \mathbb{Q}] = 4$ implica que es el polinomio mínimo.

Ejemplo. Dada la extensión $L/\mathbb{F}_2$ con $L = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$, calcular su grado y el polinomio mínimo de $\alpha = \overline{x^4 + x^2 + 1}$.

En $\mathbb{F}_2[x]$, $x^4+x^2+1 = x+1+(x^3+x+1)x$, por tanto $\alpha = \overline{x+1}$. En general, dividiendo por x^3+x+1, todos los elementos de L se escriben de manera única como combinaciones lineales de $\{\overline{1}, \overline{x}, \overline{x^2}\}$, por consiguiente $[L : \mathbb{F}_2] = 3$. El grado del polinomio mínimo de α debe ser 3 ya que α no está en $\mathbb{F}_2$ (o en su imagen por el monomorfismo $\mathbb{F}_2 \longrightarrow L$, si uno es un purista), y basta entonces hallar un polinomio mónico cúbico que tenga a α como raíz. Sabemos que $\overline{x^3 + x + 1} = 0$. De aquí $(\alpha - 1)^3 + (\alpha - 1) + 1 = 0$ y operando el primer miembro es $\alpha^3 + \alpha^2 + 1$. Así pues, el polinomio mínimo es $P = X^3 + X^2 + 1$.

2.3. Tres problemas clásicos

Esta sección es una de las más bellas del curso. Veremos que el mundo artificial que hemos poblado en las secciones anteriores con estructuras algebraicas tales como cuerpos, espacios vectoriales, anillos y cocientes, no pertenece a la estratosfera de la abstracción matemática, sino que desciende suavemente hasta la base de nuestra historia para dar respuesta a tres cuestiones geométricas con enunciado elemental que no supieron resolver los antiguos griegos.

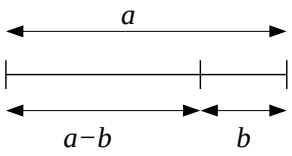
Las cuestiones a las que nos referimos tratan acerca de construcciones con regla y compás, donde la utilidad de estos instrumentos queda limitada de manera que la regla solamente se puede usar para trazar una recta que pasa por dos puntos conocidos, y el compás sólo se puede emplear para trazar una circunferencia 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 (esto es, de segundo grado). Por tanto, si $(x, y) \in \mathbb{R}^2$ es un punto construible con regla y compás entonces existe una cadena de cuerpos

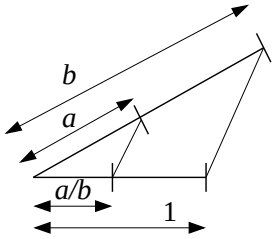
$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$$

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

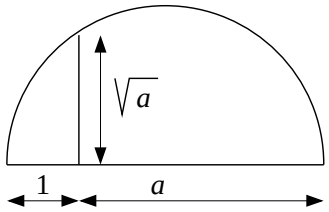
Con la ayuda de algunas construcciones geométricas sencillas conocidas desde la antigüedad es posible comprobar que la suma, resta, multiplicación, división y raíz cuadrada de longitudes construibles con regla y compás, también es construible con regla y compás. Todo lo necesario está contenido en los 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 la anterior, puede ser obtenido como coordenada de un punto construible con regla y compás, es decir, se tiene la siguiente caracterización que tomaremos como definición:

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

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$$

donde todas las extensiones son de grado dos. En breve, diremos que un número real es construible si aparece como coordenada de un punto contruible.

Una consecuencia inmediata de la definición en virtud de la Proposición 2.2.2, es:

Lema 2.3.1 *Si $u \in \mathbb{R}$ es construible, $[\mathbb{Q}(u) : \mathbb{Q}]$ es una potencia de dos.*

Observación: El recíproco de este lema no es cierto sin hipótesis adicionales. Para probar la existencia de contraejemplos se debe utilizar la teoría de Galois en toda su fuerza, así que pospondremos esta cuestión.

Ahora pasaremos a enunciar las tres cuestiones clásicas que se plantearon los antiguos griegos.

⁎1 Dada la arista de un cubo, construir con regla y compás la arista de un cubo de volumen doble.
⁎2 Dado un ángulo, hallar un método para trisecarlo con regla y compás.
⁎3 Dado un círculo, construir con regla y compás un cuadrado de igual área.

Si existiera una construcción que resolviera el primer problema para el cubo de arista 1, entonces se podría construir $\sqrt[3]{2}$. El segundo problema se debe entender como que dado un punto podemos construir otro que subtiende un ángulo (con el eje OX) que

sea la tercera parte. En particular, como $(\cos 60°, \operatorname{sen} 60°) = (1/2, \sqrt{3}/2)$ es construible, el método permitiría construir $(\cos 20°, \operatorname{sen} 20°)$. Por último, una construcción que resolviera el tercer problema para el caso del círculo de radio 1, permitiría construir $\sqrt{\pi}$.

Tras estas observaciones, las dos proposiciones siguientes muestran que no hay ninguna construcción con regla y compás en los términos requeridos que permita resolver estos problemas. La sencillez de la primera proposición contrasta con los siglos que transcurrieron hasta probar la imposibilidad de ⋇1 y ⋇2, lo que debe hacernos meditar sobre la importancia de crear el lenguaje adecuado para resolver un problema matemático. La segunda proposición es bastante más compleja y su prueba opcional en este curso.

Proposición 2.3.2 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$*, por tanto* ⋇1 *y* ⋇2 *no tienen solución con regla y compás.*

Demostración: La igualdad $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ es trivial porque $x^3 - 2$ es el polinomio mínimo de $\sqrt[3]{2}$. Lás fórmulas de adición de la fórmulas trigonométricas implican:

$$\begin{aligned} \cos(3\alpha) = \cos(2\alpha + \alpha) &= \cos(2\alpha)\cos\alpha - \operatorname{sen}(2\alpha)\operatorname{sen}\alpha \\ &= (\cos^2\alpha - \operatorname{sen}^2\alpha)\cos\alpha - (2\operatorname{sen}\alpha\cos\alpha)\operatorname{sen}\alpha \\ &= 4\cos^3\alpha - 3\cos\alpha \end{aligned}$$

Sustituyendo $\alpha = 20°$, se tiene que $\cos 20°$ 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 $\cos 20°$ y $[\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$. □

Proposición 2.3.3 (Lindemann) π *es trascendente sobre* $\mathbb{Q}$*, en particular* ⋇3 *no tiene solución con regla y compás.*

Para los que quieran leer la letra pequeña, o para los que no quieran leerla pero tengan interés en saber la idea bajo la demostración, una pequeña explicación previa en miniatura:

El resultado de Lindemann se basa en un trabajo anterior de Hermite en el que probaba que e es un número trascendente. Ambas demostraciones son parecidas gracias a la misteriosa relación $e^{i\pi} = -1$. Lo que hizo Hermite es encontrar fracciones m_j/N que aproximan excepcionalmente bien a e^j, de forma que cuando $N \to \infty$ (con N en cierta subsucesiónde $\mathbb{N}$) el error tiende a cero más rápido que $1/N$. Con ello, fijados $a_n, a_{n-1}, \ldots, a_1 \in \mathbb{Z}$ y definiendo

$$A_N = a_n e^n + a_{n-1}e^{n-1} + \cdots + a_2 e^2 + a_1 e^1 - a_n\frac{A_n}{N} - a_{n-1}\frac{A_{n-1}}{N} - \cdots - a_2\frac{A_2}{N} - a_1\frac{A_1}{N},$$

se tiene $\lim_{N\to\infty} NA_N = 0$. Si e fuera un cero del polinomio $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Entonces NA_N conformaría una sucesión de enteros que tiende a cero, y las únicas sucesiones con estas características son las que a partir de un término son idénticamente nulas. Recapitulando, la estrategia para demostrar la trascendencia de e consiste en encontrar una aproximación racional muy buena de sus potencias, y probar

que no ocurre el milagro de que el error es idénticamente nulo para una combinación lineal de ellas.

Para la demostración "de verdad", si $P \in \mathbb{Z}[x]$ con $\partial P \geq 1$, fatoriza en $\mathbb{C}[x]$ como $P = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$, definimos

$$E_P = e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_k}.$$

El resultado fundamental será el que enunciamos a continuación:

Teorema 2.3.4 *Sean $P_1, P_2, \ldots, P_n \in \mathbb{Z}[x]$ tales que $P_j(0) \neq 0$, $1 \leq j \leq n$. Dados $a_n, a_{n-1}, \ldots, a_1 \in \mathbb{Z}$ no simultáneamente nulos, se tiene $a_n E_{P_n} + a_{n-1} E_{P_{n-1}} + \cdots + a_1 E_{P_1} \notin \mathbb{Z} - \{0\}$.*

Demostración: Digamos que P_j factoriza en $\mathbb{C}[x]$ como $P_j = c_j(x-\alpha_{j1})(x-\alpha_{j2})\cdots(x-\alpha_{jk_j})$. Sea $P = \prod_j \prod_l (c_j(x-\alpha_{jl})) \in \mathbb{Z}[x]$ y consideremos las cantidades mágicas (esencialmente introducidas por Hermite)

$$A = \sum_j a_j \sum_l e^{\alpha_{jl}} \int_{\alpha_{jl}}^{\infty} \frac{x^{p-1}e^{-x}}{(p-1)!}\big(P(x)\big)^p dx \qquad \text{y} \qquad B = \int_0^{\infty} \frac{x^{p-1}e^{-x}}{(p-1)!}\big(P(x)\big)^p dx$$

con p un número primo que elegiremos más adelante. Aunque parezca increíble, A y B son enteros y A/B aproxima excepcionalmente bien a la expresión del enunciado.

La igualdad

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

prueba inmediatamente que $B \in \mathbb{Z}$, y si elegimos $p \not| P_j(0)$, se tiene $p \not| B$ porque P tiene un término independiente no nulo. Un argumento similar en A, tras el cambio de variable $u = x - \alpha_{jl}$ en la integral, permite deducir que la suma en l es un polinomio simétrico de coeficientes enteros en $c_j\alpha_{j1}, c_j\alpha_{j2}, \ldots$, esto es, en las raíces del polinomio mónico $c_j^{k_j-1}P_j(x/c_j) \in \mathbb{Z}[x]$. Según el Teorema 1.1.2 se tiene que la suma en l es un polinomio entero evaluado en los coeficientes de este polinomio, y por tanto $A \in \mathbb{Z}$. Además como $P(u+\alpha_{jl})$ no tiene término independiente, $p|A$.

Por otra parte, si llamamos E a la expresión del enunciado, se tiene para ciertas constantes K_1 y K_2

$$|BE - A| = \Big|\sum_j a_j \sum_l e^{\alpha_{jl}} \int_0^{\alpha_{jl}} \frac{x^{p-1}e^{-x}}{(p-1)!}\big(P(x)\big)^p dx\Big| \leq \frac{K_1 \cdot K_2^p}{(p-1)!},$$

donde se ha usado que un polinomio en un intervalo finito está acotado. Tomando p suficientemente grande se consigue que el segundo miembro sea menor que 1. Si E fuera un entero no nulo, podríamos suponer también $p \not| E$ y esto lleva a una contradicción, porque $BE - A$ sería un entero no divisible por p y de valor absoluto menor que 1. □

Corolario 2.3.5 (Hermite 1873) *e es trascendente sobre $\mathbb{Q}$.*

Demostración: Tómese $P_1 = x - 1$, $P_2 = x - 2$,..., $P_m = x - m$ en el teorema anterior. □

Demostración de la Proposición 2.2.3: Si π fuera algebraico, $i\pi$ también lo sería (donde $i = \sqrt{-1}$). En ese caso existe un polinomio irreducible en $\mathbb{Z}[x]$ cuyas raíces son $\alpha_1 = i\pi$, α_2, ... Digamos que c es su coeficiente de mayor grado. La fórmula de Euler implica $e^{\alpha_1} = -1$ con lo cual $\prod_k \left(1 + e^{\alpha_k}\right) = 0$. Y operando en esta igualdad se obtiene

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

Si consideramos $\prod_m (c(x - e_m))$ donde e_m denota cada exponente no nulo que aparece en la fórmula anterior, entonces $P \in \mathbb{Z}[x]$ (basta aplicar el Teorema 1.1.2 como en el teorema). La igualdad se podría escribir entonces como $1 + r + E_P = 0$ donde r es el número de posibles exponentes nulos, y esto implica $E_P \in \mathbb{Z}^-$ en contradicción con el Teorema 2.3.4. □

Ejercicios del Capítulo 2

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 2.1

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

2. 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 $AP + BQ$.

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

4. Demostrar que un dominio de integridad finito es un cuerpo.

5. Sea F un cuerpo y $f(x) \in F[x]$ un polinomio. Se dice que $a \in F$ es un cero de $f(x)$ si $f(a) = 0$. Demostrar que a es un cero de $f(x)$ si y sólo si $x - a$ divide a $f(x)$. *Indicación*: Estudiar el resto al dividir $f(x)$ por $x - a$.

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

7. Probar que si P es un polinomio no nulo sobre un cuerpo, su número de raíces es menor que el grado. Dar un contraejemplo si el cuerpo se reemplaza por un anillo.

8. Si K es un cuerpo y R es un anillo, probar que cualquier homomorfismo no nulo $f : K \longrightarrow R$ es necesariamente un monomorfismo.

9. Dado un cuerpo L, sea K la intersección de todos sus subcuerpos (K recibe el nombre de *subcuerpo primo* de L). Demostrar que la característica de L es positiva si y sólo si K es isomorfo a $\mathbb{F}_p$, y es cero si y sólo si K es isomorfo a $\mathbb{Q}$.

10. Sea $f : L \to M$ un homomorfismo no trivial de cuerpos. Probar que la característica de L es igual a la de M, y que si K es el subcuerpo primo de L entonces $f(s) = s$ para todo $s \in K$.

11. Encontrar todos los automorfismos de $\mathbb{Q}(\sqrt[3]{5})$. *Indicación*: Hallar la imagen de 5 y emplear $(\sqrt[3]{5})^3 = 5$ para determinar la de $\sqrt[3]{5}$.

12. Calcular todos los automorfismos de $\mathbb{Q}(\sqrt{7})$.

13. Demostrar que $\mathbb{Q}(\sqrt{2})$ no es isomorfo a $\mathbb{Q}(\sqrt{5})$.

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

15. Se dice que un cuerpo K es algebraicamente cerrado si todo polinomio $P \in K[x]$ con $\partial P \geq 2$ se descompone en factores lineales. Probar que ningún cuerpo finito es algebraicamente cerrado

16. Establecer las relaciones de inclusión que hay entre los cuerpos $\mathbb{Q}(i, \sqrt{3})$, $\mathbb{Q}(\sqrt{-3})$ y $\mathbb{Q}(i + \sqrt{3})$.

17. Demostrar que $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ es un cuerpo y calcular su cardinal. Dar la tabla de su producto.

18. Construir un cuerpo con 25 elementos y otro con 27. *Indicación*: No es necesario escribir la tabla de las operaciones en estos cuerpos.

19. Probar que sólo hay un cuerpo de cuatro elementos salvo isomorfismos.

20. Probar que no hay dominios de integridad de seis elementos (por lo tanto no hay cuerpos de seis elementos).

21. Probar que para todo primo p, en $\mathbb{F}_p[x]$ se cumple

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p - 1)).$$

22. Si K tiene característica p, probar que $\phi : K \longrightarrow K$ dado por $\phi(k) = k^p$ es un homomorfismo.

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

♢**24.** Sea A un dominio de integridad y supongamos que existe un cuerpo $K \subset A$ tal que A es un espacio vectorial de dimensión finita sobre K. Demostrar que A es también un cuerpo.

♢**25.** Demostrar que si un primo p es de la forma $p = n^2 + 2m^2$ con $n, m \in \mathbb{Z}$, entonces $\mathbb{Z}[\sqrt{-2}]/(n + m\sqrt{-2})$ es isomorfo a $\mathbb{F}_p$.

Sección 2.2

26. 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) $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})/\mathbb{Q}$ viii) $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})/\mathbb{Q}(\sqrt{5})$

27. Probar que $\mathbb{Q}(\sqrt{7}, \sqrt[3]{7}, \ldots, \sqrt[n]{7}, \ldots)$ no es una extensión finita de $\mathbb{Q}$.

♡**28.** Probar que $A/\mathbb{Q}$ es una extensión infinita, donde $A \subset \mathbb{C}$ son los números algebraicos sobre $\mathbb{Q}$.

29. Demostrar que una extensión de grado primo es simple.

30. Si L/K es finita y P es un polinomio irreducible en $K[x]$, demostrar que si P tiene alguna raíz en L, entonces ∂P divide a $[L : K]$.

31. Si L/K es finita y $K \subset M \subset L$, probar que para cualquier $\alpha \in L$ se cumple $[M(\alpha) : M] \leq [K(\alpha) : K]$.

32. 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 $n < n_\alpha \cdot n_\beta$.

33. Probar que L/K y M/L algebraicas, implica M/K algebraica.

34. Sea $a < 0$ un número real algebraico sobre $\mathbb{Q}$, y sea $p(x) \in \mathbb{Q}[x]$ el polinomio mínimo de a sobre $\mathbb{Q}$. Demostrar que $\sqrt{a}$ es también algebraico sobre $\mathbb{Q}$, y determinar su polinomio mínimo sobre $\mathbb{Q}$.

♡**35.** Sea F un cuerpo y sea $f(x) \in F[x]$ un polinomio no nulo. Probar que si a está en alguna extensión de F, y $f(a)$ es algebraico sobre F, entonces a es algebraico sobre F.

♡**36.** Sea β un cero de $f(x) = x^5 + 2x + 6$. Probar que ninguno de los números $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}$ pertenece a $\mathbb{Q}(\beta)$.

♡**37.** Si α es trascendente sobre K, ¿cuál es el grado de $K(\alpha)/K$?

38. Probar que un polinomio mónico P (no constante) es el polinomio mínimo de α sobre $K[x]$ si y sólo si es irreducible y cualquier $Q \in K[x]$ con $Q(\alpha) = 0$ es divisible por P.

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

40. Si $[K(\alpha):K] = n$ y $P \in K[x]$ es el polinomio mínimo de α, indicar alguna base de $K[x]/\langle P\rangle$ sobre K.

41. 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.

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

43. 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.

44. 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.

♢**45.** Calcular el polinomio mínimo de $\sqrt[3]{9} + \sqrt[3]{3} - 1$.

46. Probar que $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

47. Calcular el grado del polinomio mínimo de $\cos(2\pi/p)$ sobre $\mathbb{Q}$ donde p es un primo. *Indicación*: Compárese la extensión correspondiente con $\mathbb{Q}\big(e^{2\pi i/p}\big)/\mathbb{Q}$.

48. Si n y m son enteros positivos libres de cuadrados (no divisibles por cuadrados distintos de 1^2), comparar los cuerpos $\mathbb{Q}(\sqrt{n}, \sqrt{m})$, $\mathbb{Q}(\sqrt{n} + \sqrt{m})$ y $\mathbb{Q}(\sqrt{nm})$.

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

50. Probar que $\mathbb{Q}(\alpha)/\mathbb{Q}$ es trascendente si y sólo si $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ lo es.

51. Sea $A \subset \mathbb{C}$ el cuerpo formado por todos los números algebraicos sobre $\mathbb{Q}$. Demostrar que todo polinomio no constante de $A[x]$ se descompone en factores lineales en este anillo.

52. Si α es trascendente sobre K, hallar $[K(\alpha) : K\big(\alpha^3/(\alpha+1)\big)]$.

♢**53.** Probar que $\mathbb{R}$ no es una extensión simple de $\mathbb{Q}$.

♢**54.** Sea α raíz de un polinomio irreducible $P = x^n - a_{n-1}x^{n-1} + \cdots + (-1)^{n-1}a_1x + (-1)^n a_0$ de grado n primo. Probar que si $\beta = Q(\alpha) \notin \mathbb{Q}$, entonces el polinomio mínimo sobre $\mathbb{Q}$ de β viene dado por el determinante

$$\det(xI - Q(A)) \qquad \text{donde} \qquad A = \begin{pmatrix} 0 & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & 0 & -1 & \dots & 0 \\ \dots & & \dots & & \dots & \\ 0 & 0 & 0 & 0 & \dots & -1 \\ a_0 & a_1 & a_2 & a_3 & \dots & a_{n-1} \end{pmatrix}$$

Sección 2.3

55. Decir cuáles de las siguientes longitudes son construibles con regla y compás

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

56. Diseñar un método sencillo para construir la longitud $\sqrt{1+\sqrt{3}}/\sqrt{2}$ con regla y compás.

57. Probar que la distancia al origen de un punto construible, es construible.

58. 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*: Considérese la extensión $\mathbb{Q}\big(e^{2\pi i/p}\big)/\mathbb{Q}$ con p primo.

59. ¿Algún cubo es duplicable? ¿Algún ángulo es trisecable?

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

♢**61.** Crear un método para construir el pentágono regular.

62. Usando los principios de lo que más tarde sería la teoría de Galois, Gauss demostró (a los 19 años) que el valor de $\cos(2\pi/17)$ es

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

Explicar por qué de esta fórmula se deduce que el polígono regular de 17 lados se puede construir con regla y compás. (Nota: 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).

63. Demostrar 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.

64. Sea α la única raíz real positiva de $P = x^4 - 10x^3 + 26x^2 + 16x - 14$. Sabiendo que no existe $\mathbb{Q} \subsetneqq M \subsetneqq \mathbb{Q}(\alpha)$ tal que $M/\mathbb{Q}$ sea de grado 2, probar que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ pero α no es construible.

65. ¿Se puede triplicar el cubo?

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

67. Decir si las siguientes extensiones son algebraicas o trascendentes.

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

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

69. Responder a la siguiente crítica: El argumento para probar que el ángulo de $60°$ no se puede trisecar no es concluyente, porque sólo se demuestra que $(\cos 20°, \operatorname{sen} 20°)$ no es construible, y quizá haya algún otro punto distinto del origen) en la recta $u = x \tan 20°$ que sí sea construible, lo que permitiría la trisección.

70. 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?

$\diamondsuit$**71.** Sea $P(x) = x^n(1-x)^n/n!$. Probar que si π^2 fuera una fracción con numerador a, entonces $E_n = a^n\pi \int_0^1 P(x) \operatorname{sen}(\pi x)\, dx$ sería un entero no nulo para todo n. Demostrar que $\lim E_n = 0$, llegando a una contradicción con que $\pi^2 \in \mathbb{Q}$.

Apéndice del Capítulo 2

Conoce a tus héroes

(Más información en: `http://turnbull.mcs.st-and.ac.uk/history/`)

Apellido: Gauss
Nombre: (Johann) Carl Friedrich
Nacimiento: 1777 Brunswick
Defunción: 1855 Göttigen

Casi siempre se incluye a C.F. Gauss en la subjetiva e hipotética tríada de los mejores matemáticos de todos los tiempos. No mostró interés en publicar rápidamente sus resultados, prefiriendo pulirlos al máximo de acuerdo con su lema *Pauca sed matura* (pocos pero maduros). En relación con el contenido de este curso, probó el teorema fundamental del álgebra, dio un criterio para la constructibilidad del polígono de n lados (para lo que tuvo que crear la teoría de Galois en un caso particular antes de que naciera Galois), se adelantó a la teoría de ideales de Kummer estudiando la teoría de formas cuadráticas (lo que le llevó a la clasificación de los grupos abelianos finitos antes de que fueran siquiera definidos). En el lado negativo, el trabajo sobre la imposibilidad de resolver la quíntica con radicales que le envió Abel en situación desesperada, apareció sin abrir siquiera a la muerte de Gauss.

Bla, bla, bla

- *Que este tema [los números complejos] haya estado rodeado hasta ahora de una misteriosa oscuridad debe ser atribuido en gran medida a una notación mal adaptada. Si por ejemplo, $+1$ y -1 y la raíz cuadrada de -1 hubieran sido llamadas unidades directa, inversa y lateral, en vez de positiva, negativa e imaginaria (o imposible), tal oscuridad podría haber desaparecido.* C.F. Gauss.

- *Cuéntase que uno de los antiguos poetas trágicos hacía aparecer en escena a Minos en el momento en que construía la tumba de Glauco, y al observar que sólo medía cien pies por cada lado, dijo: "Es un espacio muy pequeño para sepulcro de un rey. Duplicadla conservando su forma cúbica, duplicando el lado." Es evidente que se equivocaba, porque duplicando los lados de una figura plana se cuadruplica, mientras que una sólida se octuplica. Entonces se propuso a los geómetras la cuestión de duplicar una figura sólida dada conservando su forma, y este problema se llamó duplicación del cubo. [...] Se cuenta también que, más tarde, los de Delos; obligados por el oráculo a duplicar el altar, tropezaron con la misma dificultad, y entonces se enviaron embajadores a los geómetras que, con Platón, frecuentaban la Academia para que resolvieran la cuestión.* Eratóstenes, 276 a.C. - 194 a.C. (Véase [Ve]).

- *Ningún hombre de ciencia está obligado a resolver toda clase de dificultades que le planteen, sino sólo aquellas que son deducidas falsamente de los principios de la ciencia: no es de nuestra incumbencia refutar aquellas que no surgen de esa forma: así como el deber del geómetra es refutar la cuadratura del círculo por medio de segmentos, pero no es su trabajo refutar la prueba de Antifonte.* Aristóteles, "Física", Libro I.

¿Qué hay que saberse?

Todo lo que no esté en letra pequeña. Especialmente hay que saber calcular polinomios mínimos y grados de extensiones en casos como los descritos en este capítulo.

(PQR) Preguntón, quejoso y respondón

Q- El cálculo del grado en extensiones con radicales parece innecesariamente complicado. Está claro que si añadimos a $\mathbb{Q}$ una raíz cuadrada, la extensión será de grado 2; si añadimos otra distinta será de grado 4; con otra cúbica se tendría grado 12; etc.

R- Sin embargo $\left[\mathbb{Q}\left(\sqrt{2},(\sqrt{8}+1)^{-1}\right):\mathbb{Q}\right]=2$.

Q- Evidentemente porque $\sqrt{8}=2\sqrt{2}$ y entonces es la misma raíz.

R- Entonces, por ejemplo $\left[\mathbb{Q}\left(\sqrt{17+12\sqrt{2}}\right):\mathbb{Q}\right]=4$ y $\left[\mathbb{Q}\left(\sqrt{11+6\sqrt{2}}+\sqrt{11-6\sqrt{2}}\right):\mathbb{Q}\right]=16$, deben ser ciertas.

Q- Creo que sí. Bueno, en el segundo caso no lo veo bien porque quizá $11+6\sqrt{2}$ y $11-6\sqrt{2}$ tengan algo que ver por ser conjugados.

R- Pues los grados son 2 y 1 porque $17+12\sqrt{2}=(3+2\sqrt{2})^2$ y $\sqrt{11+6\sqrt{2}}+\sqrt{11-6\sqrt{2}}=6$.

Q- Pero eso es trampa, porque se puede simplificar.

R- En realidad, el cálculo de polinomios mínimos es una manera de comprobar si se puede simplificar y por tanto detecta las trampas. Los grados suelen coincidir con el productos de los índices de los radicales, pero no siempre, no podemos hacer un teorema de ello.

P- El cálculo de polinomios mínimos lleva al estudio de la irreducibilidad en ciertas extensiones, ¿cómo podemos llevarla a cabo? Parece muy difícil.

R- Y lo es. Ni siquiera en $\mathbb{Q}[x]$ hay un criterio sencillo e infalible.

Q- No me creo que las demostraciones de imposibilidad de los tres problemas clásicos, lo sean realmente. En realidad lo que hemos hecho es dar una definición de construible en términos de la teoría de cuerpos que ningún antiguo griego entendería ni podría considerar nunca como la auténtica definición.

R- Podríamos dar una definición inductiva como en [St] que no apela a la teoría de cuerpos y después deducir la nuestra. Lo fundamental es fijar en términos precisos qué es construir con regla y compás, porque en otro caso podríamos encontrar soluciones que ya los antiguos griegos consideraban ilícitas.

P- ¿Qué tipo de construcciones?

R- Por ejemplo algunas en las que se permite que la regla rote por un punto al tiempo que mide. Por dar una idea, el haz de rectas $y=-mx+1$ corta a la circunferencia unidad en un punto con $x=2m/(m^2+1)$ y al eje OX en $x=1/m$. Que la diferencia entre estas longitudes sea constante da lugar a una ecuación cúbica. Los antiguos griegos crearon algunas curvas mecánicas a través de estas construcciones ilícitas.

Capítulo 3

Teoría de Galois

3.1. Extensiones normales y separables

La teoría de Galois trata de representar la estructura de la extensión generada por todas las raíces de un polinomio, por medio de sus simetrías. Para que este proyecto funcione en un contexto general son necesarias dos condiciones. La primera es que realmente podamos inventarnos un sitio donde vivan las raíces de un polinomio (¿dónde están las raíces de $x^2 + 1 \in \mathbb{F}_3[x]$?). La segunda está en los márgenes de los contraejemplos del curso por su naturaleza mucho más técnica, y es que ningún elemento sea raíz múltiple de todos los polinomios que anula. Esto provocaría que algunas simetrías colapsasen y que no representaran fielmente la extensión. Como veremos más adelante, no hay que preocuparse mucho por esta condición, porque la cumplen prácticamente todas las extensiones que podemos imaginar este curso.

La primera condición, a la que dedicaremos casi todos nuestros esfuerzos en esta sección, tiene que ver con los conceptos de cuerpo de descomposición y de extensión normal. En breve probaremos que ambos están estrechamente relacionados y que son en cierto modo equivalentes para extensiones finitas, pero ahora limitémonos a sus definiciones. En ellas y en el resto del capítulo utilizaremos el abuso de notación consistente en hablar de la descomposición de $P \in K[x]$ en $L[x]$ cuando L/K es una extensión. En rigor el polinomio P sólo está en $L[x]$ después de aplicar el monomorfismo de la extensión $j : K \longrightarrow L$ a sus coeficientes. (Quien no entienda este comentario no debe preocuparse porque tampoco detectará el abuso de notación).

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

Definición: Sea L/K una extensión. Se dice que L es un *cuerpo de descomposición* (o *cuerpo raíz*) de $P \in K[x]$, $\partial P > 1$, si P se descompone en factores lineales en $L[x]$, esto es, $P = k(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$, y no existe ningún subcuerpo propio de L (conteniendo la imagen de K en L) con esta propiedad.

Observación: Con la notación de la definición anterior, imponiendo $L \supset K$, se tiene que el cuerpo de descomposición de P es $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, el cuerpo más pequeño

que contiene a las raíces. Sin embargo no hay que olvidar que fuera de $\mathbb{C}$, donde el teorema fundamental del álgebra acude en nuestro auxilio, no está en absoluto claro que las raíces existan en algún sitio (esto es, que siempre haya un cuerpo de descomposición) ni tampoco que no podamos crear muchos cuerpos de descomposición distintos. En seguida resolveremos estas cuestiones de existencia y unicidad.

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

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

Ejemplo. El cuerpo de descomposición de $P = x^n - 1 \in \mathbb{Q}(\sqrt{2})[x]$ es $\mathbb{Q}(\sqrt{2}, \zeta)$ con $\zeta = e^{2\pi i/n}$.

Como acabamos de señalar, la existencia del cuerpo de descomposición no es evidente porque en sitios suficientemente raros no sabemos hallar las raíces de un polinomio, por ejemplo en el caso antes citado $x^2 + 1 \in \mathbb{F}_3[x]$. Para resolver este problema nos inventaremos un sitio más raro todavía, un anillo cociente, donde vive algo que se comporta como una raíz. Después bastará darle a la manivela de la inducción para que el resto de las raíces se unan a la fiesta. Realmente todo el artificio fue ya introducido en el primer capítulo.

Lema 3.1.1 *Dado un polinomio no constante $P \in K[x]$, existe una extensión finita, L/K, tal que P tiene una raíz en L.*

Demostración: Podemos suponer que P es irreducible (en otro caso elegiríamos uno de sus factores irreducibles) y que $\partial P > 1$ (si $\partial P = 1$, $L = K$). Sea el anillo $L = K[x]/\langle P \rangle$. Obviamente K está "incluido" en L, o más exactamente, existe un monomorfismo $\phi : K \longrightarrow L$. Además L es de hecho un cuerpo, por la Proposición 1.2.3 en combinación con la 1.3.2. Por último, la finitud de L/K se sigue de la Proposición 2.2.4, porque $L = K(\overline{x})$ con $\overline{x} = x + \langle P \rangle$, y $\overline{x}$ es algebraico al ser $P(\overline{x}) = \overline{P(x)}$ la clase de cero en L. □

Ejemplo. Según el resultado anterior, $P = x^2 + x + 1 \in \mathbb{F}_2[x]$ factoriza en $L = \mathbb{F}_2[x]/\langle P \rangle = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$.

Para que los más escépticos se sientan a gusto, demos a estos cuatro elementos nombre más vulgares, digamos $L = \{0, 1, \alpha, \beta\}$. Entonces las tablas de suma y multiplicación en L 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

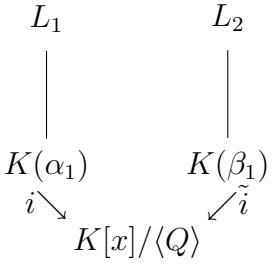
$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Si lo preferimos, podemos empezar desde aquí y definir L como un cuerpo cuyas operaciones tienen las tablas anteriores. Como $\alpha+\beta = \alpha\beta = 1$, se concluye $P = (x-\alpha)(x-\beta)$ en $L[x]$. De hecho L es el cuerpo de descomposición de P, ya que $[L : \mathbb{F}_2] = 2$ (ejercicio) y por tanto no hay subextensiones propias de $L/\mathbb{F}_2$. También podemos comprobar directamente con estas tablas que α y β son raíces de P. Por ejemplo $\alpha^2+\alpha+1 = \beta+\alpha+1 = 1+1 = 0$.

Si hubiéramos partido de un polinomio de tercer grado, el lema anterior nos habría llevado a un lugar donde hay una descomposición del tipo $k(x-\gamma)(x^2+\delta x+\epsilon)$. Para conseguir la factorización total en factores lineales, sólo hay que iterar. Si además recordamos la Proposición 2.2.5, veremos que las raíces están exactamente representadas por los anillos cociente, y que el procedimiento lleva a un único resultado salvo los nombres con los que nos apetezca bautizar a las raíces invitadas. En breve:

Proposición 3.1.2 *Para cada $P \in K[x]$ existe un cuerpo de descomposición L de P y además es único salvo isomorfismos que dejan fijo K (en rigor la imagen de K en L).*

Demostración: Para la existencia basta aplicar repetidas veces el Lema 3.1.1 hasta obtener un L en el que P se descomponga en factores lineales: $P = k(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$, entonces $K(\alpha_1,\alpha_2,\dots,\alpha_n)$ será el cuerpo de descomposición de P (para ser totalmente rigurosos deberíamos escribir en lugar de K su imagen en L). Para demostrar la unicidad salvo isomorfismos que dejan fijo K, supongamos que L_1 y L_2 son cuerpos de descomposición de P. Procedemos por inducción en el grado de P. Si gr $P = 1$ es trivial. Si gr $P > 1$, sea Q un factor mónico irreducible de P, entonces $Q = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ en $L_1[x]$ y $Q = (x-\beta_1)(x-\beta_2)\dots(x-\beta_n)$ en $L_2[x]$. Por la Proposición 2.2.5 se tienen isomorfismos $i : K(\alpha_1) \longrightarrow K[x]/\langle Q\rangle$, $\widetilde{i} : K(\beta_1) \longrightarrow K[x]/\langle Q\rangle$, por tanto $\widetilde{i}^{-1} \circ i : K(\alpha_1) \longrightarrow K(\beta_1)$ es un isomorfismo, que por la construcción de i e $\widetilde{i}$, deja fijo K.



Por definición, L_1 es una extensión de $K(\alpha_1)$ y también L_2 puede considerarse que extiende a $K(\alpha_1)$ por medio del 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 también lo son de $\widetilde{P} = P/(x-\alpha_1)$ porque $\alpha_1 \in K(\alpha_1)$. La demostración se concluye por la hipótesis de inducción (ya que gr $\widetilde{P} <$ gr P). □

Ejemplo. El cuerpo $\mathbb{F}_3[i]$ donde $i \notin \mathbb{F}_3$ es un símbolo que operamos formalmente como $i^2 = -1$, es el cuerpo de descomposición de x^2+1 sobre $\mathbb{F}_3$.

Si nos creemos que $\mathbb{F}_3[i]$ es un cuerpo bien definido (en principio sólo tiene estructura de anillo), entonces $\mathbb{F}_3[i] = \mathbb{F}_3(i) = \mathbb{F}_3(i,-i)$. Como $x^2+1 = (x-i)(x+i)$ en $(\mathbb{F}_3[i])[x]$, se tiene que es el cuerpo de descomposición (el cuerpo generado por las raíces). La forma de probar que $\mathbb{F}_3[i]$ es un cuerpo es considerar el isomorfismo $\mathbb{F}_3[i] \longrightarrow \mathbb{F}_3[x]/\langle x^2+1\rangle$ donde $i \mapsto \overline{x}$. Como el segundo anillo es un cuerpo (por la Proposición 1.2.3), el primero también lo es. Ambos son cuerpos de descomposición de x^2+1 porque los dos conforman extensiones de grado 2 que contienen a las raíces. En concordancia con la última proposición la única diferencia entre ambos se reduce a un cambio de nombre en las raíces, $\pm i$ por $\pm\overline{x}$.

Nota: Siempre podemos dar a las raíces los nombres que nos apetezca, pero el ejemplo anterior no debe hacernos pensar que podemos imponer junto con esos nombres una estructura algebraica a nuestro arbitrio. Por ejemplo, el cuerpo de descomposición de x^2+1 sobre $\mathbb{F}_2$ no es $\mathbb{F}_2[i]$ con i definido como antes, porque $x^2+1 = (x+1)^2$ en $\mathbb{F}_2[x]$

y por tanto el cuerpo de descomposición es el propio $\mathbb{F}_2$. De hecho $\mathbb{F}_2[i]$ no es un cuerpo si nos empeñamos en que i sea algo distinto de 1 que tenga la propiedad $i^2 = -1$, ya que $(i-1)(i-1) = 0$ implicaría $i = 1$ en un dominio de integridad.

Aparentemente, lo que pedimos a una extensión para que sea normal es mucho más restrictivo que lo que exigimos en la definición de cuerpo de descomposición, ya que una extensión normal debe contener los cuerpos de descomposición de "muchos" polinomios. Pero el siguiente resultado nos da en el caso finito (el único de interés en este curso) las dos definiciones al precio de una:

Proposición 3.1.3 *Una extensión L/K es normal y finita si y sólo si L es el cuerpo de descomposición de un polinomio de $K[x]$.*

Demostración: Distingamos cada una de las implicaciones. Como siempre, comenzamos con lo más fácil:

$\Rightarrow$) Sea $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ y sea $P = P_1 \cdot P_2 \cdot \cdots \cdot P_n$ donde P_j es el polinomio mínimo de α_j sobre K. Como L/K es normal, cada P_i se descompone en factores lineales en $L[x]$ 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 en $K[x]$, entonces $\alpha \in L \Rightarrow \beta \in L$.

Por la Proposición 2.2.5 (empleada como en la demostración de la proposición anterior) 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 el monomorfismo $K(\alpha) \longrightarrow K(\beta) \hookrightarrow L(\beta)$. Así pues, por la proposición anterior, los cuerpos $L(\alpha)$ y $L(\beta)$ son isomorfos como extensiones de $K(\alpha)$. En definitiva, si $\alpha \in L$, se tiene

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

es decir, $\beta \in L$. Por tanto L/K es normal (la finitud es inmediata porque cada raíz de Q está en una extensión de grado menor o igual que ∂Q). $\square$

Ejemplo. La extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ es normal porque $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el cuerpo de descomposición de $P = (x^2 - 2)(x^2 - 3)$ sobre $\mathbb{Q}$.

Ejemplo. La extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal porque sólo una de las raíces de $x^3 - 2$ está en $\mathbb{Q}(\sqrt[3]{2})$, las otras son números complejos. Sin embargo la extensión $\mathbb{Q}(\sqrt[3]{2}, \sqrt{7})/\mathbb{Q}(\sqrt[3]{2})$ sí es normal porque $\mathbb{Q}(\sqrt[3]{2}, \sqrt{7})$ es el cuerpo de descomposición de $x^2 - 7$ sobre $\mathbb{Q}(\sqrt[3]{2})$.

Ejemplo. La extensión $\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}$ es normal porque $\mathbb{Q}(e^{2\pi i/n})$ es el cuerpo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$.

Entre los cuerpos de descomposición vamos a señalar un caso especial que seguidamente veremos que es general en el universo de los cuerpos finitos. Históricamente aparecieron por vez primera en uno de los trabajos del propio Galois bajo el epígrafe *Sur la théorie des nombres* [Gal].

Definición: Si $q = p^n$ donde p es primo y $n \in \mathbb{Z}^+$, se denota con $\mathbb{F}_q$ (o con GF_q) y se llama a veces *cuerpo de Galois*, al cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$.

Ejemplo. $\mathbb{F}_4$ es, salvo isomorfismos, el cuerpo $L = \{0, 1, \alpha, \beta\}$ descrito anteriormente porque $x^4 - x = x(x+1)(x^2+x+1)$.

Ejemplo. $\mathbb{F}_9$ es, salvo isomorfismos, el cuerpo $L = \mathbb{F}_3[i]$, también considerado anteriormente, porque tras la factorización:

$$x^9 - x = x(x-1)(x-2)(x^2+1)\big((x+1)^2+1\big)\big((x-1)^2+1\big)$$

se sigue que todas las raíces están en L.

Parece una gran casualidad estas coincidencias de cuerpos, pero ya deberíamos estar acostumbrados a que en Matemáticas las grandes casualidades suelen ser en realidad teoremas, pequeñas verdades universales veladas a nuestros ojos. La sorpresa es que los cuerpos de descomposición sobre $\mathbb{F}_p$, y de hecho todos los cuerpos finitos, son lo mismo que (isomorfos a) algún $\mathbb{F}_q$. Con este resultado que probaremos a continuación, los $\mathbb{F}_q$ que se ocultaban humildemente bajo su apariencia de caso particular, adquieren un puesto de palco en la teoría de cuerpos. Todavía suben más alto teniendo en cuenta su importancia en las aplicaciones. Por ejemplo parte de la teoría de códigos (sí, la que hace funcionar los discos compactos) vive de los cuerpos finitos y hasta la prueba del último teorema de Fermat requiere entenderlos bien. En este curso, sin embargo, no les daremos una importancia especial prefiriendo centrarnos en ejemplos más familiares y completos que viven dentro del reino de los números complejos (la teoría de Galois es muy fácil en cuerpos finitos). Tal felonía, requiere al menos unas líneas en letra pequeña.

Un *byte* es una lista ordenada de 8 *bits*, es decir, de ocho ceros y unos. Al transmitir un conjunto de *bytes*, un fichero, para tener alguna certeza de que no ha habido errores podemos añadir un *byte de paridad* que no contiene información adicional pero fuerza a que en nuestro conjunto de *bytes* haya un número par de unos en el primer *bit*, y en el segundo, ... y así hasta el octavo.

byte 1	1	0	0	0	1	0	0	1
byte 2	1	1	1	1	1	1	0	0
byte 3	1	0	1	0	1	0	0	1

byte de paridad	1	1	0	1	1	1	0	0
nº total de unos	4	2	2	2	4	2	0	2

Podemos identificar los ceros y unos de los *bits* con los elementos de $\mathbb{F}_2$. En seguida veremos que $\mathbb{F}_{256}/\mathbb{F}_2$ es una extensión de grado 8, por tanto $\mathbb{F}_{256}$ es un espacio vectorial de dimensión 8 sobre $\mathbb{F}_2$ y cada uno de sus elementos corresponde a un vector $(b_1, b_2, \ldots, b_8)$ con $b_i \in \mathbb{F}_2$, esto es, a un *byte*, y la suma en $\mathbb{F}_{256}$ corresponde a la suma coordenada a coordenada módulo 2. Así pues, si el fichero (con su *byte* de paridad) está representado en $\mathbb{F}_{256}$ por $\alpha_1, \alpha_2, \ldots, \alpha_N$, se debe cumplir $\sum \alpha_i = 0$ si no hay errores. Hasta aquí toda esta terminología son ganas de complicar las cosas. Idealmente, si hubiera algún error de transmisión nos gustaría que se reparase automática e inmediatamente, sin tener que transmitir de nuevo el fichero. Con este fin, fijamos de antemano N elementos distintos no nulos, $\beta_1, \ldots, \beta_N \in \mathbb{F}_{256}$ (suponemos $N < 256$) y ponemos ahora dos *bytes* de paridad α_{N-1} y α_N elegidos

de manera que se cumpla $\sum \alpha_i = 0$ y $\sum \beta_i \alpha_i = 0$. Si un solo *byte* α_j se hubiera modificado durante la transmisión pasando a $\alpha_j + \gamma$ entonces lo notaríamos porque el valor de $\sum \alpha_i$ sería $\gamma \neq 0$, mientras que el de $\sum \beta_i \alpha_i$ sería $\beta_j \gamma$. Por tanto $\beta_j = \sum \beta_i \alpha_i / \sum \alpha_i$. Como los β_i son distintos, β_j corresponde a un solo *byte*, al j-ésimo, y podríamos detectar el error y corregirlo (simplemente restando a este *byte* $\gamma = \sum \alpha_i$).

Complicando las cosas se pueden detectar y corregir más posibles errores siempre a costa de añadir algunos *bytes* de sobra. Más información sobre el tema (o, más bien, alguna información sobre el tema) se puede encontrar por ejemplo en [Ak] y [Ga] y por supuesto en el curso de Teoría de Códigos y Criptografía. Como curiosidad, un CD recién sacado de su envoltorio de regalo puede tener medio millón de errores. Tan asombroso o más que la existencia de algoritmos eficientes para eliminarlos es que la tecnología haya sido capaz de hacer que operen en tiempo real, manejando cantidades ingentes de información por segundo.

Teorema 3.1.4 *Sea L un cuerpo finito, entonces es isomorfo a $\mathbb{F}_q$, $q = p^n$, donde p es la característica de L, $n = [L : \mathbb{F}_p]$ y q es el cardinal de L. Además $L/\mathbb{F}_p$ es normal.*

Demostración: Notemos antes de comenzar que la característica de un cuerpo, si no es nula, es un primo, ya que $\mathrm{char}(L) = n_1 n_2 \Rightarrow (1+1+\overset{n_1 \text{ veces}}{\ldots}+1)(1+1+\overset{n_2 \text{ veces}}{\ldots}+1) = 0 \Rightarrow 1+1+\overset{n_1 \text{ veces}}{\ldots}+1 = 0$ ó $1+1+\overset{n_2 \text{ veces}}{\ldots}+1 = 0$, lo que contradice la minimalidad pedida en la definición de característica.

Por ser L finito, su característica es positiva (el grupo aditivo es de orden finito). Digamos $\mathrm{char}(L) = p$. La función $\overline{n} \mapsto 1+1+\overset{n \text{ veces}}{\ldots}+1$ induce un monomorfismo de $\mathbb{F}_p$ en L y por tanto $L/\mathbb{F}_p$ es una extensión. Sea $n = [L : \mathbb{F}_p]$. Una vez fijada una base $\{\alpha_1, \ldots, \alpha_n\}$, todo elemento de L se escribe de forma única como $\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n$ con $\lambda_j \in \mathbb{F}_p$, por tanto $|L| = p^n = q$. El orden del grupo multiplicativo $L - \{0\}$ es $q-1$ y consecuentemente, por el teorema de Lagrange, $x^{q-1} - 1 = 0$ para todo $x \in L - \{0\}$. Así pues todos los elementos de L son raíces de $P = x^q - x$. Por otra parte, el número de raíces de un polinomio no puede superar a su grado. Como $\partial P = q = |L|$, se sigue necesariamente que P se descompone en factores lineales en L y que L es su cuerpo de descomposición (en particular normal sobre $\mathbb{F}_p$), por tanto es isomorfo a $\mathbb{F}_q$. □

Observación: Del teorema se sigue que $\mathbb{F}_q$ y todos los cuerpos finitos isomorfos a él tienen $q = p^n$ elementos. Así hay cuerpos con 16, 17 y 19 elementos pero no con 18 o 20.

Ejemplo. El cuerpo de descomposición de $x^3 + 2x + 1 \in \mathbb{F}_5[x]$ es isomorfo a $\mathbb{F}_{125}$.

El polinomio $x^3 + 2x + 1 \in \mathbb{F}_5[x]$ es irreducible (no tiene raíces en $\mathbb{F}_5$). Sea α una raíz en el cuerpo de descomposición, entonces $\mathbb{F}_5(\alpha)$ es un cuerpo finito (ya que $\mathbb{F}_5(\alpha)/\mathbb{F}_5$ es una extensión finita). Por el teorema anterior $\mathbb{F}_5(\alpha)/\mathbb{F}_5$ es normal y por tanto x^3+2x+1 se descompone en factores lineales en $\mathbb{F}_5(\alpha)$, que es su cuerpo de descomposición. Como $\mathbb{F}_5(\alpha)$ tiene característica 5 y $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 3$, según el teorema es isomorfo a $\mathbb{F}_{5^3}$.

Ejemplo. Estudiar si el polinomio $P = x^4 + x + 1$ es irreducible en $\mathbb{F}_4[x]$ y hallar el grado de su cuerpo de descomposición sobre $\mathbb{F}_4$.

El polinomio P no tiene raíces en $\mathbb{F}_2$ ni tampoco es divisible por $x^2 + x + 1$, que es el único polinomio en $\mathbb{F}_2[x]$ de grado dos irreducible, por tanto P es irreducible en $\mathbb{F}_2[x]$ y procediendo como en el ejemplo anterior su cuerpo de descomposición sobre $\mathbb{F}_2$ es isomorfo a $\mathbb{F}_{2^4}$. Como $[\mathbb{F}_{2^4} : \mathbb{F}_{2^2}] = [\mathbb{F}_{2^4} : \mathbb{F}_2]/[\mathbb{F}_{2^2} : \mathbb{F}_2] = 4/2$, el grado buscado es 2. Si P fuera irreducible en $\mathbb{F}_4$ entonces el cuerpo de descomposición de P tendría al menos grado 4 sobre $\mathbb{F}_4$ y por tanto 8 sobre $\mathbb{F}_2$, lo que contradice que sea isomorfo a $\mathbb{F}_{2^4}$.

Pasemos ahora a estudiar la segunda condición técnica a la que nos referimos al comienzo de la sección, relacionada con la existencia de raíces múltiples de polinomios irreducibles. Para ahorrar en papel, tinta y analgésicos, prácticamente aquí nos limitaremos a probar que en casi todas las extensiones que podemos imaginar la condición que solicitamos se cumple. (Para un análisis breve más profundo, véase [Ka] p. 55-59).

El concepto básico está recogido en la siguiente definición. Para no sobrecargar demasiado la terminología nos limitaremos a polinomios irreducibles.

Definición: Se dice que un polinomio irreducible $P \in K[x]$ es *separable* sobre K si no tiene raíces múltiples (en su cuerpo de descomposición). Si L/K es una extensión algebraica, se dice que $\alpha \in L$ es *separable* sobre K si su polinomio mínimo lo es. Finalmente, se dice que la propia extensión L/K es *separable* si todo $\alpha \in L$ lo es sobre K. En caso de que un polinomio, elemento o extensión no sea separable, se dice que es *inseparable*.

Antes de nada, veamos un resultado auxiliar que a primera vista parece implicar que no existen polinomios inseparables.

Lema 3.1.5 *Dado $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ irreducible, entonces P es inseparable si y sólo si el polinomio $P' = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$, llamado* derivada formal *de P, es el polinomio nulo.*

Nota: La denominación tiquismiquis de P' como *derivada formal* en vez de simplemente *derivada* es inofensiva y sólo intenta recordarnos que en muchos cuerpos, por ejemplo en $\mathbb{F}_p$, no tiene sentido el concepto usual de límite ni por tanto la definición usual de derivada. La definición de P' es simplemente formal, aunque comparta las propiedades algebraicas (por ejemplo la fórmula para derivar un producto) con la de toda la vida de Cálculo I.

Demostración: Distinguimos las dos implicaciones:

$\Rightarrow$) Si P es inseparable, existe α en el cuerpo de descomposición tal que $(x-\alpha)^2 | P$ y se tiene $P = (x-\alpha)^2 Q$, y de aquí $P' = 2(x-\alpha)Q + (x-\alpha)^2 Q'$. Por tanto $x - \alpha$ divide a $R = \mathrm{mcd}(P, P') \in K[x]$. Si $P' \neq 0$ entonces R es un polinomio no constante con $\partial R < \partial P$ que divide a P, lo que contradice la irreducibilidad.

$\Leftarrow$) 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 $P' = \sum_{i=1}^{n} P_i$ donde $P_i(x) = P(x)/(x-\alpha_i)$. 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 $x - \alpha_1 \not| P'$ lo cual contradice $P' = 0$. $\square$

Una consecuencia inmediata es la imposibilidad de encontrar ejemplos de extensiones inseparables con números normales y corrientes.

Proposición 3.1.6 *Si K es un cuerpo de característica cero, todo polinomio irreducible en $K[x]$ es separable. En particular cualquier extensión algebraica L/K con $K \subset \mathbb{C}$ es separable.*

Demostración: Por el lema anterior, para que $P = a_n x^n + \dots a_1 x + a_0 \in K[x]$ sea inseparable, $ja_j = 0$, $1 \leq j \leq n$. Por estar en un cuerpo de característica cero, $j = 1 + 1 + \overset{j \text{ veces}}{\dots} + 1 \neq 0$, así pues $a_j = 0$ para todo $1 \leq j \leq n$. □

Nuestras sospechas se centran ahora sobre $\mathbb{F}_p$, pero tampoco allí es posible encontrar ejemplos inseparables.

Proposición 3.1.7 *Si K es un cuerpo finito, todo polinomio irreducible en $K[x]$ es separable. En particular cualquier extensión algebraica $L/\mathbb{F}_q$ es separable.*

Demostración: Es fácil ver que si L/M y M/K son extensiones algebraicas, L/K separable implica L/M separable (ejercicio). Así que, después del teorema de clasificación de cuerpos finitos (Teorema 3.1.4), basta considerar el caso $K = \mathbb{F}_p$.

Según el lema, los únicos polinomios inseparables deberán ser de la forma $P = a_{np}x^{np} + \dots + a_{2p}x^{2p} + a_p x^p + a_0$. Por el pequeño teorema de Fermat, $a^p = a$ para todo $a \in \mathbb{F}_p$. Además $(A+B)^p = A^p + B^p$ para $A, B \in \mathbb{F}_p[x]$, ya que los coeficientes binómicos $\binom{p}{k}$ son divisibles por p para $0 < k < p$ (ejercicio). Por tanto

$$P = (a_{np}x^n)^p + \dots + (a_{2p}x^2)^p + (a_p x)^p + a_0^p = \left(a_{np}x^n + \dots + a_{2p}x^2 + a_p x + a_0\right)^p,$$

y se concluye que P no es irreducible. □

La pregunta natural es qué diantres puede ser una extensión no separable, no vaya a ser que estemos introduciendo un nuevo nombre para el conjunto vacío.

Ejemplo. La extensión $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$ (donde t es una variable) es inseparable, porque el polinomio mínimo de t sobre $\mathbb{F}_2(t^2)$ es $x^2 - t^2 \in \mathbb{F}_2(t^2)[x]$ que se descompone en $\mathbb{F}_2(t)[x]$ como $(x-t)^2$.

Para terminar esta ya larga sección, estableceremos que las extensiones separables, esto es, todas las que aparecerán en este curso excluyendo el ejemplo anterior, tienen una insospechada propiedad que ya anunciamos en el segundo capítulo.

Teorema 3.1.8 (Teorema del elemento primitivo) *Toda extensión separable finita es simple.*

Demostración: Separamos primero el caso en que los cuerpos de la extensión son finitos. Por el Teorema 3.1.4 nos podemos restringir a la extensión $\mathbb{F}_q/\mathbb{F}_p$ (ejercicio). Si $q = p^n$, escojamos un polinomio mónico irreducible $P \in \mathbb{F}_p[x]$ de grado n, tal polinomio existe porque en otro caso cada elemento de $\mathbb{F}_q$ estaría en algún $\mathbb{F}_{p^m}$ con $m|n$ (ejercicio), lo cual es imposible porque $p + p^2 + \dots + p^{n-1} < p^n$. Si α es una raíz de P, $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$ y según el Teorema 3.1.4 (véase también el ejemplo posterior) se tiene que $\mathbb{F}_p(\alpha)$ es igual (isomorfo) a $\mathbb{F}_q$.

Supongamos ahora que los cuerpos que participan en la extensión tienen infinitos elementos. Todo lo que hay que probar es que toda extensión $K(\alpha, \beta)/K$ con α y β algebraicos sobre K es simple, porque de ahí, iterando, se deduce que cualquier extensión finita $K(\alpha_1, \alpha_2, \dots, \alpha_n)/K$ es simple.

Sean Q y P los polinomios mínimos de α y β respectivamente. Digamos que sus raíces en el cuerpo de descomposición de QP son $\alpha = s_1, s_2 \dots, s_m$ y $\beta = r_1, r_2, \dots, r_l$. Sea $\gamma = k\beta - \alpha$ donde $k \in K$ es no nulo y distinto de todos los elementos de la forma $(s_i - \alpha)/(r_j - \beta)$, $1 < i \leq m$, $1 < j \leq l$, como K es infinito es posible esta elección. Consideremos el polinomio $R \in K[\gamma][x]$ con $R(x) = Q(kx - \gamma)$. Nótese que β es raíz de P y R, y además ninguna de las otras raíces de P lo es de R (porque la elección de k implica $kr_j - \gamma \neq s_i$). Así pues $\mathrm{mcd}(P, R) \in K(\gamma)[x]$ tiene como única raíz a β y por la separabilidad esta raíz es simple en P. Por tanto este máximo común divisor es $x - \beta$. De la pertenencia a $K(\gamma)[x]$ se deduce $\beta \in K(\gamma)$ y de aquí $\alpha = k\beta - \gamma \in K(\gamma)$ concluyéndose $K(\alpha, \beta) = K(\gamma)$. □

3.2. El grupo de Galois

La estética que anima el edificio de las Matemáticas muchas veces no es otra cosa que una arquitectura de las simetrías, y dentro de las estructuras algebraicas, la de grupo es la que más comúnmente se asocia con la idea de simetría. El propio concepto de grupo nació (al tiempo que la teoría de Galois) a partir del estudio de las simetrías de las funciones al intercambiar sus variables.

En muchos contextos la representación a través de un grupo es una manera útil de distinguir o incluso caracterizar objetos matemáticos. Una de las manifestaciones más conocidas de este hecho es el llamado *Erlanger Programm* (véase [Kl]), basado en una conferencia que dio F. Klein en la Universidad de Erlangen en 1872, que postula que las diferentes geometrías se deben definir y clasificar por medio de los grupos de transformaciones que admiten. Como ya hemos anunciado, el objetivo de la teoría de Galois (materializado en la próxima sección) se encuadra también dentro de esquemas similares, siendo caracterizar la estructura de ciertas extensiones por medio de un grupo de simetrías. Antes de entrar en las puras definiciones, dejémonos cautivar por unos ejemplos bobos que pueden arrojar alguna luz y darnos no sólo coraje sino también ganas de continuar.

Pensemos en cualquier identidad involucrando las operaciones elementales (suma, resta, multiplicación y división) dentro del cuerpo de los números complejos. Por ejemplo:

$$-2 = \frac{2+3i}{1+i} \cdot (3-i) - (10+i).$$

Si en todos los sitios cambiamos i por $-i$, la igualdad sigue siendo válida. Más adelante expresaremos esto diciendo que la conjugación está en el grupo de Galois de $\mathbb{C}/\mathbb{R}$, un grupo que engloba todas las posibles simetrías. Podemos representar que el primer miembro es un número real, porque queda invariante por la conjugación.

Si escribimos ahora una identidad en $\mathbb{Q}(\sqrt{2},\sqrt{3})$, por ejemplo:

$$(1+\sqrt{2}+\sqrt{3})^2 - 2\sqrt{3} - (\sqrt{2}+\sqrt{3})^2 = 1+2\sqrt{2},$$

esta vez tenemos dos conjugaciones reales. Todas las formas de elegir los signos en $\sqrt{2} \mapsto \pm\sqrt{2}$ y $\sqrt{3} \mapsto \pm\sqrt{3}$, dan lugar a simetrías (invariancias) de esta identidad o de cualquier otra en $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Podríamos decir que el segundo miembro está en $\mathbb{Q}(\sqrt{2})$ porque es invariante por las simetrías que cambian de signo $\sqrt{3}$.

Por último, analicemos la situación con una identidad en $\mathbb{Q}(\sqrt[3]{2})$. Por ejemplo:

$$\frac{1}{1+\sqrt[3]{2}+(\sqrt[3]{2})^2} - \sqrt[3]{2} = -1.$$

No está claro cuál es la conjugación en $\mathbb{Q}(\sqrt[3]{2})$. De hecho probaremos que no hay simetrías dentro de $\mathbb{Q}(\sqrt[3]{2})$ y diremos que el grupo de Galois de $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ es trivial. La razón de este fracaso (una extensión no trivial tienen grupo trivial) es que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal, y lo podemos transformar en un éxito sin más que ampliarla a una extensión normal que la contenga, como $\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})/\mathbb{Q}$, donde vive la simetría $\sqrt[3]{2} \mapsto (-1+\sqrt{-3})\sqrt[3]{2}/2$.

Vayamos a las definiciones que sintetizan estas ideas. Los automorfismos serán los objetos matemáticos que representen las simetrías.

Definición: Dada una extensión L/K, se dice que $\sigma : L \longrightarrow L$ es un *K-automorfismo* si es un automorfismo que deja fijos los elementos de K (en rigor, sus imágenes en L). Al conjunto formado por todos los K-automorfismos se le llama *grupo de Galois* de la extensión y lo representaremos con $\mathcal{G}(L/K)$.

Definición: Dado un subgrupo H de $\mathcal{G}(L/K)$, se dice que $\{x \in L \ : \ \sigma(x) = x, \ \forall \sigma \in H\}$ es el *subcuerpo fijo por H* y lo denotaremos con H'.

Con estas definiciones nos hemos adelantado a la estructura algebraica que tienen estos objetos. Para que sean definiciones coherentes necesitamos el siguiente resultado básico y sencillo que probaremos sólo por romper el hielo.

Proposición 3.2.1 *$\mathcal{G}(L/K)$ es un grupo con la composición de automorfismos, y si H es un subgrupo de $\mathcal{G}(L/K)$, entonces H' es un subcuerpo de L que contiene a K (en rigor a su imagen en L).*

Demostración: 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 son consecuencia de las propiedades de la composición de funciones.

Si $x, y \in H'$, para todo $\sigma \in H'$ se tiene $\sigma(x) = x$ y $\sigma(y) = y$, entonces $\sigma(x+y) = x+y$ y por tanto $x + y \in H'$. Lo mismo se haría con el resto de las operaciones. □

La acción del grupo de Galois preserva el conjunto de raíces de polinomios en el siguiente sentido:

Proposición 3.2.2 *Sea L/K y $P \in K[x]$. Si $\alpha \in L$ es una raíz 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 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de raíces distintas de P en L. (Nótese que $\sigma(\alpha_i) = \sigma(\alpha_j) \ \Rightarrow \ \sigma(\alpha_i - \alpha_j) = 0 \ \Rightarrow \ \alpha_i = \alpha_j$). Lo cual está relacionado con la forma en que apareció el grupo de Galois históricamente como subgrupo de permutaciones [Gal], [Ed], porque en tiempos de Galois no existían los K-automorfismos. También sugiere la naturalidad de las condiciones de normalidad y separabilidad que exigiremos más adelante para que el grupo de Galois represente bien la extensión. Si la extensión no es normal, faltarán raíces de algunos polinomios y nos perderemos algunos automorfismos, y si no es separable la coincidencia entre raíces provocará que los automorfismos se repitan.

Demostración: $P(\alpha) = 0 \Rightarrow \sigma\big(P(\alpha)\big) = 0 \Rightarrow P\big(\sigma(\alpha)\big) = 0$. □

Antes de ahogarnos en un mar de ideas intuitivas sostenidas por un par de definiciones y proposiciones, agarrémonos a la tabla salvadora de algunos ejemplos que concreten lo dicho al comienzo de la sección.

Ejemplo. $\mathcal{G}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \mathrm{conj}\} \cong \mathbb{Z}_2$, donde $\mathrm{conj}(z) = \overline{z}$ es la conjugación compleja.

Se tiene $\mathbb{C} = \mathbb{R}(i)$ y como i y $-i$ son las raíces de $x^2 + 1 \in \mathbb{R}[x]$, los únicos posibles automorfismos son $a + ib \mapsto a + ib$ y $a + ib \mapsto a - ib$. El primero es la identidad y el segundo la conjugación. Este último es un $\mathbb{R}$-automorfismo porque deja fijos a los reales, es biyectivo (es su propia inverso) y satisface las propiedades de homomorfismo ($\overline{z+w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z}\,\overline{w}$ y $\overline{1} = 1$). Si $H = \mathcal{G}(\mathbb{C}/\mathbb{R})$ se tiene $H' = \mathbb{R}$.

Ejemplo. $\mathcal{G}\big(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\big) = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_1\sigma_2\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ donde σ_1 y σ_2 son los $\mathbb{Q}$-automorfismos verificando $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_1(\sqrt{3}) = \sqrt{3}$, $\sigma_2(\sqrt{2}) = \sqrt{2}$, $\sigma_2(\sqrt{3}) = -\sqrt{3}$.

Cada elemento de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ se puede escribir de forma única como $x + y\sqrt{2}$ con $x, y \in \mathbb{Q}(\sqrt{3})$. La aplicación $\sigma_1(x+y\sqrt{2}) = x - y\sqrt{2}$ es un $\mathbb{Q}$-automorfismo por la misma razón que lo es la conjugación compleja (es biyectiva, fija $\mathbb{Q}$ y respeta las operaciones). Análogamente, también se puede escribir cada elemento de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ de forma única como $x + y\sqrt{3}$ con $x, y \in \mathbb{Q}(\sqrt{2})$, y se deduce que $\sigma_2(x + y\sqrt{3}) = x - y\sqrt{3}$ es un $\mathbb{Q}$-automorfismo. Esto prueba que $\{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_1\sigma_2\} \subset \mathcal{G}\big(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\big)$. No puede haber más $\mathbb{Q}$-automorfismos en $\mathcal{G}\big(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\big)$ porque según la última proposición aplicada a los polinomios $x^2 - 2$ y $x^2 - 3$, cualquier elemento del grupo de Galois sólo puede modificar el signo de $\sqrt{2}$ y $\sqrt{3}$, que generan la extensión y las cuatro combinaciones de signos quedan cubiertas por los automorfismos ya enumerados.

Al ser $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ una base de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$,

$$L = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \ : \ a, b, c, d \in \mathbb{Q}\}$$

y para $H = \{\mathrm{Id}, \sigma_1\sigma_2\}$ se tiene $H' = \{a + d\sqrt{2}\sqrt{3} \ : \ a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$. De la misma forma, $\{\mathrm{Id}, \sigma_1\}' = \mathbb{Q}(\sqrt{3})$, $\{\mathrm{Id}, \sigma_2\}' = \mathbb{Q}(\sqrt{2})$ y $\big(\mathcal{G}\big(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\big)\big)' = \mathbb{Q}$.

Ejemplo. $\mathcal{G}\big(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\big) = \{\mathrm{Id}\}$ porque un $\mathbb{Q}$-automorfismo no trivial debería aplicar $\sqrt[3]{2}$ (que genera la extensión) en alguna de las otras dos raíces de $x^3 - 2$, y ninguna de ellas está en $\mathbb{Q}(\sqrt[3]{2})$. Obviamente $\big(\mathcal{G}\big(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\big)\big)' = \{\mathrm{Id}\}' = \mathbb{Q}(\sqrt[3]{2})$.

Hay una sencilla relación entre el grado de los subcuerpos fijos y el orden de los subgrupos que los fijan. Su prueba pasa por un curioso lema auxiliar que trata los automorfismos como si fueran vectores.

Lema 3.2.3 *Sean $\sigma_1, \sigma_2, \ldots, \sigma_r \in \mathcal{G}(L/K)$ automorfismos distintos, entonces el conjunto $\{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ es linealmente independiente sobre L. Es decir, si $\lambda_1, \lambda_2, \ldots, \lambda_r \in L$ no son simultáneamente nulos entonces $\lambda_1\sigma_1 + \lambda_2\sigma_2 + \cdots + \lambda_r\sigma_r$ no es la función idénticamente nula en L.*

Demostración: Procedemos por reducción al absurdo. Sea n el menor número de coeficientes λ_j no nulos que participan en una combinación lineal que produce la función nula. Renombrando los automorfismos podemos suponer que son $\lambda_1, \lambda_2, \ldots, \lambda_n$. Esto es,

$$\lambda_1\sigma_1(\alpha) + \lambda_2\sigma_2(\alpha) + \cdots + \lambda_n\sigma_n(\alpha) = 0 \quad \forall \alpha \in L \tag{3.1}$$

para ciertos $\lambda_j \neq 0$. Como α es arbitrario lo podemos sustituir por $\alpha\beta$ donde $\beta \in L$ se escogerá a continuación, por tanto

$$\lambda_1\sigma_1(\alpha)\sigma_1(\beta) + \lambda_2\sigma_2(\alpha)\sigma_2(\beta) + \cdots + \lambda_n\sigma_n(\alpha)\sigma_n(\beta) = 0 \quad \forall \alpha \in L.$$

Elijamos β tal que $\sigma_1(\beta) \neq \sigma_n(\beta)$, esto es posible porque σ_1 y σ_n son distintos. Multiplicando (3.1) por $\sigma_n(\beta)$ y restándole la igualdad anterior, se tiene

$$\lambda'_1\sigma_1(\alpha) + \lambda'_2\sigma_2(\alpha) + \cdots + \lambda'_{n-1}\sigma_{n-1}(\alpha) = 0 \quad \forall \alpha \in L$$

con $\lambda'_1 \neq 0$, pero esto contradice que hubiéramos tomado la combinación lineal más corta. □

Proposición 3.2.4 *Sea H un subgrupo finito de $\mathcal{G}(L/K)$. Si H' es el subcuerpo fijo por los automorfismos de H, entonces*

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

Demostración: Obviamente la segunda igualdad se sigue de la primera por la Proposición 2.2.2. Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ una base de L/H', sea $H = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ (por tanto $r = [L : H']$ y $n = |H|$) y sea la matriz $A \in \mathcal{M}_{r\times n}(L)$ cuyas columnas son $\sigma_j(\vec{\alpha})$ donde $\vec{\alpha} \in L^r$ es el vector cuya i-ésima coordenada es α_i y los automorfismos σ_j actúan de la manera obvia coordenada a coordenada. Estas columnas son linealmente independientes por el lema anterior (ya que $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ es una base y $\sum \lambda_j\sigma_j(\vec{\alpha}) = \vec{0}$ implicaría $\sum \lambda_j\sigma_j(x) = 0$ para todo $x \in L$). Queremos demostrar demostrar $r = n$, es decir, que la matriz A es cuadrada. Procedemos por reducción al absurdo.

Si $r < n$ entonces $\mathrm{rg}(A) \leq r$, lo que contradice que las n columnas de A sean linealmente independientes.

Si $r > n$ entonces $\mathrm{rg}(A) = n$ y las r filas de A deben ser linealmente dependientes. Por tanto existe $\vec{x} \in L^r - \{0\}$ con $\sigma_j(\vec{\alpha})\cdot\vec{x} = 0$ para todo j. Si x_r es una coordenada no nula de $\vec{x}$, por el lema anterior se puede elegir t tal que $\sigma_1+\sigma_2+\cdots+\sigma_n$ aplicado a tx_r sea no nulo (ya que no es la aplicación nula). En particular, el vector $\vec{v} = \sigma_1(t\vec{x})+\sigma_2(t\vec{x})+\cdots+\sigma_n(t\vec{x})$ es no nulo. Además $\vec{v} \in (H')^r$ porque $\sigma(\vec{v}) = \vec{v}$ para $\sigma \in H$ (ya que la suma es en todos los elementos de H). Aplicando σ_j^{-1} a $\sigma_j(\vec{\alpha}) \cdot t\vec{x} = 0$, debe cumplirse $\vec{\alpha} \cdot \sigma_j^{-1}(t\vec{x}) = 0$, $1 \leq j \leq n$, esto es, $\vec{\alpha} \cdot \sigma(t\vec{x}) = 0$ para todo $\sigma \in H$. En particular $\vec{\alpha} \cdot \vec{v} = 0$, lo que contradice que las coordenadas de $\vec{\alpha}$ conformen una base de L sobre H'. □

Sólo por el placer de ver funcionar los engranajes de los teoremas, comprobemos la primera igualdad de la proposición anterior en nuestra exigua colección de grupos de Galois.

Ejemplo. Si $H = \mathcal{G}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \mathrm{conj}\}$, se tiene $[\mathbb{C} : H'] = [\mathbb{C} : \mathbb{R}] = 2 = |H|$.

Ejemplo. Si $H = \{\mathrm{Id}, \sigma_1\sigma_2\} \subset \mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big)$, donde se ha usado la notación de un ejemplo anterior, se tiene $H' = \mathbb{Q}(\sqrt{6})$ y $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : H'] = 2 = |H|$.

Ejemplo. Si $H = \mathcal{G}\big(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\big) = \{\mathrm{Id}\}$, se tiene $[\mathbb{Q}(\sqrt[3]{2}) : H'] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 1 = |H|$.

Los pocos ejemplos que hemos visto de grupos de Galois, se resisten a grandes generalizaciones. Vaya por delante que incluso cuando se utilizan ordenadores para calcular grupos de Galois, los grados y las formas de presentar las extensiones están seriamente limitados. Una ambición razonable es no tener que comprobar con todo cuidado que los presumibles K-automorfismos lo son realmente, y disponer de alguna fórmula con la que sepamos cuántos K-automorfismos tenemos que buscar. Todas estas aspiraciones se consiguen bajo hipótesis de finitud, normalidad y separabilidad, gracias a una propiedad de extensión de isomorfismos. Más importante que el resultado en sí son las consecuencias, que prácticamente constituyen la primera mitad del teorema fundamental de la teoría de Galois que enunciaremos en la próxima sección.

Proposición 3.2.5 *Sea L/K normal y finita y sean M_1 y M_2 dos subcuerpos de L conformando extensiones de K. Si $i : M_1 \longrightarrow M_2$ es un isomorfismo que deja fijos los elementos de K (en rigor de su imagen en L), entonces existe $\sigma \in \mathcal{G}(L/K)$ tal que restringido a M_1 coincide con i.*

Demostración: 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 la Proposición 2.2.5 se tienen isomorfismos

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

Por otra parte, i induce un isomorfismo $i_3 : M_1[x]/\langle P_1\rangle \longrightarrow M_2[x]/\langle P_2\rangle$, así pues basta tomar $\widetilde{i} = i_2^{-1} \circ i_3 \circ i_1$. Por construcción los elementos de K quedan fijos por $\widetilde{i}$. □

Corolario 3.2.6 *Sea L/K normal y finita. Si P es un polinomio irreducible y $\alpha, \beta \in L$ son raíces de P, entonces existe $\sigma \in \mathcal{G}(L/K)$ con $\sigma(\alpha) = \beta$.*

Demostración: Basta aplicar la proposición tomando $M_1 = K(\alpha)$, $M_2 = K(\beta)$ y el isomorfismo $i : M_1 \longrightarrow M_2$ de la Proposición 2.2.5. □

Corolario 3.2.7 *Si L/K es normal, finita y separable, $|\mathcal{G}(L/K)| = [L : K]$.*

Demostración: Tomando $H = \mathcal{G}(L/K)$ en la Proposición 3.2.4 se sigue $[L : K] \geq [L : H'] = |\mathcal{G}(L/K)|$. Si fuera $[L : K] > |\mathcal{G}(L/K)|$, necesariamente existiría $\alpha \in \big(\mathcal{G}(L/K)\big)' - K$. Al ser la extensión normal y separable, el polinomio mínimo de α sobre K factoriza totalmente en $L[x]$ y tiene raíces distintas en L. Por el corolario anterior existe un elemento de $\mathcal{G}(L/K)$ que no fija a α, que lo envía a otra de las raíces, lo que contradice $\alpha \in \big(\mathcal{G}(L/K)\big)'$. □

Ahora veamos ejemplos y más ejemplos, en multitud tan abigarrada que invadirán la siguiente sección.

Nota: Al hallar grupos de Galois, para asegurar la normalidad, muchas veces se presentan los cuerpos como cuerpos de descomposición de un polinomio. De hecho es común usar la expresión *grupo de Galois de* $P \in K[x]$ para referirse a $\mathcal{G}(L/K)$ con L el cuerpo de descomposición de P sobre K, aunque aquí preferimos evitar esta notación.

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

Como la extensión es simple y generada por ζ, cada $\sigma \in \mathcal{G}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big)$ está determinado por el valor en el que aplica 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, $\mathbb{Q}(\zeta)$ es su cuerpo de descomposición y el Corolario 3.2.6 implica que existen $\mathbb{Q}$-automorfismos σ_1, σ_2, σ_3 y σ_4 tales que $\sigma_1(\zeta)=\zeta$, $\sigma_2(\zeta)=\zeta^2$, $\sigma_3(\zeta)=\zeta^3$, $\sigma_4(\zeta)=\zeta^4$. Con lo cual se tiene $\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\} \subset \mathcal{G}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big)$. Y la igualdad se da por el Corolario 3.2.7 (porque $[\mathbb{Q}(\zeta):\mathbb{Q}]=4$). Nótese que $\sigma_1 =$Id y que σ_2 genera al resto de los automorfismos, ya que

$$\sigma_2^2(\zeta)=\sigma_2(\sigma_2(\zeta))=(\zeta^2)^2=\sigma_4(\zeta) \quad \text{y} \quad \sigma_2^3(\zeta)=\sigma_2(\sigma_2^2(\zeta))=(\zeta^4)^2=\zeta^3=\sigma_3(\zeta).$$

Por consiguiente $\mathcal{G}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big) \cong \mathbb{Z}_4$.

No es difícil generalizar este ejemplo reemplazando 5 por cualquier primo.

Ejemplo. Si $\zeta = e^{2\pi i/p}$ con p primo, entonces $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \big\{\sigma_1,\sigma_2,\ldots,\sigma_{p-1}\big\}$ donde $\sigma_j : \zeta \mapsto \zeta^j$. Además $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ es isomorfo al grupo (multiplicativo) de unidades de $\mathbb{Z}_p$. (aunque no lo haremos aquí, se puede probar que este grupo es siempre isomorfo a $\mathbb{Z}_{p-1}$).

Como antes, $\mathbb{Q}(\zeta)$ es el cuerpo de descomposición del polinomio ciclotómico $P = x^{p-1}+x^{p-2}+\cdots+1 = (x^p-1)/(x-1)$. Como P es irreducible y tiene a ζ como raíz, $[\mathbb{Q}(\zeta):\mathbb{Q}] = p-1$, por tanto $|\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})| = p-1$. Por otra parte $\sigma_j \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$, gracias al Corolario 3.2.6 y se tiene $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \big\{\sigma_1,\sigma_2,\ldots,\sigma_{p-1}\big\}$.

El isomorfismo $\phi : \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^*$ donde $\mathbb{Z}_p^*$ son las unidades de $\mathbb{Z}_p$, viene dado simplemente por $\phi(\sigma_j) = \overline{j}$. Se reduce a un cálculo comprobar que $\phi(\sigma_i\sigma_j) = \phi(\sigma_i)\phi(\sigma_j)$, y su inversa es simplemente $\overline{j} \mapsto \sigma_j$ para $0 < j < p$.

Ejemplo. En $\mathbb{Q}(\zeta)/\mathbb{Q}$ con $\zeta = e^{2\pi i/7}$ hallar el cuerpo fijo $H' =< \sigma_2 >'$ y su grado sobre $\mathbb{Q}$. (Empleamos la notación anterior, esto es, $\sigma_2 : \zeta \mapsto \zeta^2$).

Al ser $B = \{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$ una base de la extensión (Proposición 2.2.4) todo $x \in \mathbb{Q}(\zeta)$ se puede expresar como $x = \sum_{j=0}^{5} \lambda_j\zeta^j$ con $\lambda_j \in \mathbb{Q}$. Entonces la condición $x = \sigma_2(x)$ necesaria y suficiente para que $x \in H'$, es

$$\begin{aligned} x &= \lambda_0+\lambda_1\zeta^2+\lambda_2\zeta^4+\lambda_3\zeta^6+\lambda_4\zeta^8+\lambda_5\zeta^{10} \\ &= \lambda_0+\lambda_4\zeta+\lambda_1\zeta^2+\lambda_5\zeta^3+\lambda_2\zeta^4+\lambda_3\zeta^6 \\ &= (\lambda_0-\lambda_3)+(\lambda_4-\lambda_3)\zeta+(\lambda_1-\lambda_3)\zeta^2+(\lambda_5-\lambda_3)\zeta^3+(\lambda_2-\lambda_3)\zeta^4-\lambda_3\zeta^5 \end{aligned}$$

donde se ha empleado $\zeta^8=\zeta$, $\zeta^{10}=\zeta^3$ y $\zeta^6 = -1-\zeta-\zeta^2-\zeta^3-\zeta^4-\zeta^5$ (recuérdese el polinomio ciclotómico). Igualando coordenadas con respecto a la base B, se tiene:

$$\lambda_0=\lambda_0-\lambda_3, \quad \lambda_1=\lambda_4-\lambda_3, \quad \lambda_2=\lambda_1-\lambda_3, \quad \lambda_3=\lambda_5-\lambda_3, \quad \lambda_4=\lambda_2-\lambda_3, \quad \lambda_5=-\lambda_3.$$

En definitiva, $\lambda_3 = \lambda_5 = 0$, $\lambda_1 = \lambda_4 = \lambda_2$, o escrito de otra forma, $x = a + b(\zeta + \zeta^2 + \zeta^4)$. Esto prueba $H' = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. El orden de σ_2 es 3, y según la Proposición 3.2.4, el grado de la extensión es $[H' : \mathbb{Q}] = 6/|H| = 2$.

Observación: Una forma más breve de calcular H' en el problema anterior pasa por notar que para cualquier $x \in \mathbb{Q}(\zeta)$ se cumple $u = x + \sigma_2(x) + \sigma_2^2(x) \in H'$ porque $\sigma_2(u) = u$ (utilizamos que σ_2 tiene orden 3). Tomando $x = \zeta$ se obtiene $\zeta + \zeta^2 + \zeta^4 \in H'$. Además $\zeta + \zeta^2 + \zeta^4 \notin \mathbb{Q}$ porque σ_3 no lo deja invariante, y $[H' : \mathbb{Q}] = 2$ implica $H' = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. Este truco de forzar las simetrías haciendo actuar todos los elementos de un grupo ya apareció en la demostración de la Proposición 3.2.4 y se muestra también en diferentes versiones en áreas alejadas del tema que nos ocupa, por ejemplo es análogo al *método de las imágenes* introducido por Lord Kelvin para resolver algunas ecuaciones en derivadas parciales provinientes de problemas físicos. Históricamente fue Gauss el primero en calcular subcuerpos fijos en $\mathbb{Q}(e^{2\pi i/p})$ de esta forma, antes de que existiera la teoría de Galois y el propio Galois (un lector avezado podría tratar de interpretar en nuestro lenguaje los ejemplos de [Gau] Art. 353, 354). A pesar de que nos permitiría reducir algunos cálculos, no sistematizaremos el método en este curso.

La sencillez del cálculo del grupo de Galois en los tres ejemplos anteriores se debe a que el cuerpo de descomposición del polinomio ciclotómico está generado por una de sus raíces. Todavía podemos encontrar ejemplos sencillos saliéndonos de esta situación.

Ejemplo. 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 $\omega = (-1 + i\sqrt{3})/2$, por tanto el cuerpo de descomposición es $\mathbb{Q}(\omega, \sqrt[3]{2})$. La conjugación compleja es claramente en $\mathbb{Q}$-automorfismo en $\mathbb{C}$, en particular lo es en $\mathbb{Q}(\omega, \sqrt[3]{2})$. Llamémosla τ cuando la consideramos como elemento de $\mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$. Su efecto sobre los generadores de la extensión es $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau(\omega) = \overline{\omega} = \omega^2$. Por otra parte, el Corolario 3.2.6 asegura que existe $\sigma \in \mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ con $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. Además $\sigma(\omega)$ debe ser ω ó $\overline{\omega} = \omega^2$ porque ambas cantidades son raíces de $x^2 + x + 1$. Quizá sustituyendo σ por $\sigma\tau$ siempre podemos suponer por ejemplo $\sigma(\omega) = \omega$. El automorfismo σ tiene orden tres porque

$$\sigma^3(\omega) = \omega \quad \text{y} \quad \sigma^3(\sqrt[3]{2}) = \sigma^2(\omega\sqrt[3]{2}) = \omega\,\sigma^2(\sqrt[3]{2}) = \omega\,\sigma(\omega\sqrt[3]{2}) = \omega^3\sqrt[3]{2} = \sqrt[3]{2}.$$

Los $\mathbb{Q}$-automorfismos Id, σ, σ^2, τ, $\sigma\tau$ y $\sigma^2\tau$ son distintos. Su acción sobre ω y $\sqrt[3]{2}$ se recoge en las siguientes tablas:

	ω	$\sqrt[3]{2}$
Id	ω	$\sqrt[3]{2}$
σ	ω	$\omega\sqrt[3]{2}$
σ^2	ω	$\omega^2\sqrt[3]{2}$

	ω	$\sqrt[3]{2}$
τ	ω^2	$\sqrt[3]{2}$
$\sigma\tau$	ω^2	$\omega\sqrt[3]{2}$
$\sigma^2\tau$	ω^2	$\omega^2\sqrt[3]{2}$

El grupo de Galois tiene orden 6 (Corolario 3.2.7), así pues se debe tener

$$\mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Este grupo no es abeliano, porque por ejemplo $\sigma\tau(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ y $\tau\sigma(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$.

Si recordamos los tiempos de Álgebra I, tendremos que el único grupo no abeliano de orden 6 es S_3 (el de permutaciones de tres elementos), por tanto $\mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) \cong S_3$. Una forma de realizar este isomorfismo es asignar a cada elemento del grupo de Galois la permutación que efectúa sobre las raíces $r_1 = \sqrt[3]{2}$, $r_2 = \omega\sqrt[3]{2}$, $r_3 = \omega^2\sqrt[3]{2}$, del polinomio P. Por ejemplo, la acción de σ es $r_1 \mapsto r_2$, $r_2 \mapsto r_3$, $r_3 \mapsto r_1$, lo que corresponde a la permutación $(1, 2, 3)$, mientras que la conjugación τ corresponde a la transposición $(2, 3)$. (Como ya hemos comentado, en su infancia histórica el grupo de Galois era un subgrupo de permutaciones que hoy en día se muestra ataviado con las galas del álgebra como grupo de K-automorfismos).

Veamos un breve ejemplo en el que el cuerpo base no es $\mathbb{Q}$, y otro más completo con un grupo que tenemos que recordar de Álgebra I.

Ejemplo. Hallar el grupo de Galois de $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega)$ donde, como antes, ω es la raíz cúbica de la unidad $(-1 + i\sqrt{3})/2$.

La extensión es normal de grado 3. Cada automorfismo del grupo de Galois queda evidentemente caracterizado por la imagen de $\sqrt[3]{2}$. Por el Corolario 3.2.6 aplicado a x^3-2, existen, aparte de la identidad, $\mathbb{Q}(\omega)$-automorfismos $\sigma_1 : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ y $\sigma_2 : \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$. Así pues $\mathcal{G}\big(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega)\big) = \{\mathrm{Id}, \sigma_1, \sigma_2\}$ que es claramente isomorfo a $\mathbb{Z}_3$.

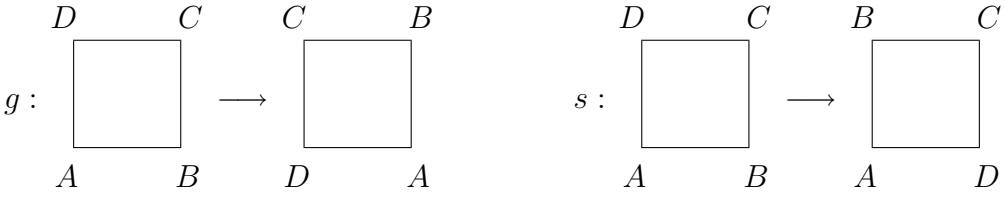
Ejemplo. Hallar el grupo de Galois del cuerpo de descomposición del polinomio $P = x^4 - 2$ sobre $\mathbb{Q}$.

Las raíces de P son $i^k\sqrt[4]{2}$ con $k = 0, 1, 2, 3$, por tanto su cuerpo de descomposición es $L = \mathbb{Q}(\sqrt[4]{2}, i)$. Como antes, tenemos que la conjugación compleja, digamos τ, pertenece al grupo de Galois de $L/\mathbb{Q}$ porque incluso pertenece al de $\mathbb{C}/\mathbb{Q}$. El grado de la extensión es sencillo de calcular porque

$$[L : \mathbb{Q}(\sqrt[4]{2})] = 2 \;\Rightarrow\; [L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8.$$

Por el Corolario 3.2.6 existe un $\mathbb{Q}$-automorfismo con $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ y, quizá cambiando σ por $\sigma\tau$, podemos suponer que $\sigma(i) = i$. Este automorfismo tiene orden 4 (ejercicio). De aquí se deduce que $\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ es un subconjunto de ocho automorfismos distintos y por tanto debe coincidir con $\mathcal{G}(L/\mathbb{Q})$.

Este grupo de Galois no es abeliano. Por ejemplo, $\sigma\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$ mientras que $\tau\sigma(\sqrt[4]{2}) = -i\sqrt[4]{2}$. Podemos identificarlo como un grupo conocido en Álgebra I notando que $\tau\sigma = \sigma^3\tau$ (ejercicio), de donde $\mathcal{G}(L/\mathbb{Q}) = \langle \sigma, \tau \;:\; \sigma^4 = \tau^2 = \mathrm{Id},\ \tau\sigma = \sigma^3\tau \rangle$, lo cual era la presentación de D_8, el grupo diédrico de ocho elementos (también denotado a veces como D_4, lo que causa desafortunadas confusiones). Recuérdese que por definición, D_8 es el grupo de movimientos del plano que dejan fijos un cuadrado, y que está generado por el giro, g, de 90° y la simetría, s, por una de las diagonales



El isomorfismo $\mathcal{G}(L/\mathbb{Q}) \cong D_8$ consiste simplemente en asociar $\sigma \mapsto g$ y $\tau \mapsto s$.

Ejemplo. Hallar el subcuerpo fijo por $H = \langle \sigma^2, \tau \rangle$ en el ejemplo anterior.

Como $\{1, i\}$ y $\{1, \sqrt[4]{2}, \sqrt[4]{2^2}, \sqrt[4]{2^3}\}$ son bases de $L/\mathbb{Q}(\sqrt[4]{2})$ y de $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, por la Proposición 2.2.2 cada $x \in L$ se escribe de forma única como

$$x = \lambda_0 + \lambda_1 i + \lambda_2 \sqrt[4]{2} + \lambda_3 i \sqrt[4]{2} + \lambda_4 \sqrt[4]{2^2} + \lambda_5 i \sqrt[4]{2^2} + \lambda_6 \sqrt[4]{2^3} + \lambda_7 i \sqrt[4]{2^3}$$

con $\lambda_j \in \mathbb{Q}$. Por una parte, $\tau(x) = x$ implica $\lambda_1 = \lambda_3 = \lambda_5 = \lambda_7 = 0$, y por otra, para x con estos coeficientes, $\sigma^2(x) = x$ implica $\lambda_2 = \lambda_6 = 0$. En definitiva, $H' = \{\lambda_0 + \lambda_4 \sqrt[4]{2^2} \ : \lambda_2, \lambda_4 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$. Nótese que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [L : \mathbb{Q}]/|H| = 8/4$.

Hasta ahora no ha sido necesaria una extensión efectiva de los automorfismos, porque teníamos la conjugación que de hecho se aplica en algo tan grande como $\mathbb{C}/\mathbb{Q}$. Veamos un ejemplo un poco artificial que incide en que la extensión de automorfismos no es arbitraria.

Ejemplo. 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 seguir, intentemos 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 genera una extensión de grado 4 sobre $\mathbb{Q}$ que contiene a $\sqrt{2}$ (porque $\sqrt{2} = \alpha^2 - 1$ y $\alpha \neq a + b\sqrt{2}$). Por tanto $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)]\ [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$.

Sea $M = \mathbb{Q}(\sqrt{2}, i)$, como $[L : M] = 2$, el polinomio mínimo de α en M es $x^2 - (1+\sqrt{2})$, lo que asegura que hay un elemento $\sigma \in \mathcal{G}(L/M)$ tal que $\sigma(\alpha) = -\alpha$. Evidentemente también $\sigma \in \mathcal{G}(L/\mathbb{Q})$ y se cumple $\sigma(i) = i$ y $\sigma(\sqrt{2}) = \sqrt{2}$. Lo que no esta claro es cómo deben comportarse los automorfismos que sí actúan sobre M, para ello bajamos un nivel y estudiamos primero los elementos de $\mathcal{G}(M/\mathbb{Q})$. Los cuatro automorfismos que debe haber en $\mathcal{G}(M/\mathbb{Q})$ se extenderán a $\mathcal{G}(L/\mathbb{Q})$ y después de componerlos con $\mathrm{Id}, \sigma \in \mathcal{G}(L/M)$ darán lugar a los ocho automorfismos de $\mathcal{G}(L/\mathbb{Q})$. Nótese que este proceso lo podemos llevar a cabo en general siempre que podamos "descomponer" una extensión (finita y separable) en subextensiones normales.

En $\mathbb{Q}(\sqrt{2})$ se tiene la conjugación real $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ que se extiende a un elemento de $\mathcal{G}(M/\mathbb{Q})$. También está la conjugación compleja. Combinándolas de todas las formas posibles se tienen los cuatro $\mathbb{Q}$-automorfismos de $\mathcal{G}(M/\mathbb{Q})$. Escribamos $\mathcal{G}(M/\mathbb{Q}) = \langle \beta_1, \beta_2 \rangle = \{\mathrm{Id}, \beta_1, \beta_2, \beta_1\beta_2\}$ donde $\beta_1(i) = -i$, $\beta_1(\sqrt{2}) = \sqrt{2}$, $\beta_2(i) = i$, $\beta_2(\sqrt{2}) = -\sqrt{2}$,

Por la Proposición 3.2.5, existen $\tau_1, \tau_2 \in \mathcal{G}(L/\mathbb{Q})$ 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 $\tau_j(\alpha) \in \{\alpha, -\alpha, i/\alpha, -i/\alpha\}$, $j = 1, 2$; es decir, que en principio τ_1 y τ_2 podrían tomar cuatro valores 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

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

Nótese que no es abeliano: $\tau_1\tau_2(\alpha) = \tau_1(i/\alpha) = -i/\alpha$ y $\tau_2\tau_1(\alpha) = \tau_2(\alpha) = i/\alpha$. Aunque no lo haremos aquí, como antes, se puede comprobar que $\mathcal{G}(L/\mathbb{Q}) \cong D_8$.

Una extensión finita que no sea normal siempre podemos considerarla dentro de una extensión mayor que sí lo sea. Gracias a la Proposición 3.2.5 todos los elementos del grupo de Galois de la primera extensión serán restricciones de los de la segunda. Pero muchas veces no hace falta ir tan lejos.

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

Por el Lema 3.2.2, cualquier elemento de $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}\big)$ debe dejar fijo $\sqrt[3]{3}$ porque el resto de las raíces de $x^3 - 2$ son complejas y no pertenecen a $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. Como $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}(\sqrt[3]{3})$ es normal, por el Corolario 3.2.6 existe un automorfismo σ que pasa $\sqrt{2}$ a $-\sqrt{2}$ y deja fijo $\mathbb{Q}(\sqrt[3]{3})$, y de hecho éste y la identidad son los únicos $\mathbb{Q}(\sqrt[3]{2})$-automorfismos, ya que el grado de la extensión anterior es 2. Por tanto el grupo de Galois buscado es $\{\mathrm{Id}, \sigma\}$.

Para terminar, vamos a estudiar el grupos de Galois de las extensiones más raras con las que hemos trabajado: las de cuerpos finitos. Resulta que la teoría en ellos es ridículamente sencilla. Esencialmente sólo hay un automorfismo y sus potencias.

Definición: Se llama *automorfismo de Frobenius* en $\mathbb{F}_q$ con $q = p^n$ a la aplicación $\phi : \mathbb{F}_q :\longrightarrow \mathbb{F}_q$ definida como $\phi(x) = x^p$.

Proposición 3.2.8 *El automorfismo de Frobenius es realmente un automorfismo y ϕ^n (esto es, ϕ compuesto consigo mismo n veces) deja invariantes a los elementos de $\mathbb{F}_q$ con $q = p^n$ y tiene orden d en $\mathbb{F}_{q'}$ con $q' = p^{nd}$.*

Demostración: Es evidente que $\phi(x)\phi(y) = \phi(xy)$ y $\phi(1) = 1$, mientras que la igualdad $\phi(x + y) = \phi(x) + \phi(y)$ se sigue del binomio de Newton empleando que el número combinatorio $\binom{p}{k}$ es divisible por p, $0 < k < p$. Es un monomorfismo porque $x^p = 0 \Rightarrow x = 0$ (estamos en un dominio de integridad), por tanto $|\mathrm{Im}\ \phi| = |\mathbb{F}_q|$ y se tiene que también es biyectiva.

Por definición los elementos de $\mathbb{F}_q$ satisfacen $x^{p^n} = x$, esto es, $\phi^n(x) = x$. Por otro lado, si ϕ^{nk} fuera la identidad en $\mathbb{F}_{q'}$ para algún $0 < k < d$, entonces todos los elementos de $\mathbb{F}_{q'}$ satisfarían $x^{p^{nk}} = x$ y de aquí se deduciría $\mathbb{F}_{p^{nk}} \supset \mathbb{F}_{q'}$, lo cual contradice $|\mathbb{F}_{p^{nk}}| = p^{nk} < |\mathbb{F}_{q'}| = p^{nd}$. □

Corolario 3.2.9 *Si $q = p^n$ y $q' = p^{nd}$ entonces $\mathcal{G}(\mathbb{F}_{q'}/\mathbb{F}_q) = \langle\phi^n\rangle \cong \mathbb{Z}_d$.*

Demostración: Según la proposición, $\mathbb{Z}_d \cong \langle \phi^n \rangle \subset \mathcal{G}(\mathbb{F}_{q'}/\mathbb{F}_q)$ y la igualdad se sigue, a través del Corolario 3.2.7, de $[\mathbb{F}_{q'} : \mathbb{F}_q] = [\mathbb{F}_{q'} : \mathbb{F}_p]/[\mathbb{F}_q : \mathbb{F}_p] = nd/n = d$. □

Ejemplo. Hallar $\mathcal{G}(L/\mathbb{F}_2)$ y $\mathcal{G}(L/\mathbb{F}_4)$ donde L es el cuerpo de descomposición de $P = x^4 + x + 1$.

Ya habíamos visto anteriormente que P es irreducible en $\mathbb{F}_2[x]$ y que L es (isomorfo a) $\mathbb{F}_{2^4}$. Según el corolario anterior $\mathcal{G}(L/\mathbb{F}_2) = \langle \phi \rangle \cong \mathbb{Z}_4$ y $\mathcal{G}(L/\mathbb{F}_4) = \langle \phi^2 \rangle \cong \mathbb{Z}_2$ con $\phi(x) = x^2$.

Como comprobación, nótese que es fácil verificar que ϕ^4 deja fija a cada raíz α de P en L porque $\phi^4(\alpha) = \alpha^{16} = (\alpha^4)^4 = (-\alpha - 1)^4 = \alpha^4 + 1 = -\alpha - 1 + 1 = \alpha$.

3.3. El teorema fundamental de la teoría de Galois

A continuación vamos a enunciar un teorema de tal calado que justifica su aparición en solitario dentro de esta sección sin más compañía que un leve acuerdo de notación y la ineludible corte de ejemplos que den boato a su majestad. Este teorema establecerá un diccionario que permite traducir problemas de extensiones finitas en otros de grupos finitos. Todavía más, dentro del reino de las extensiones finitas normales y separables, el diccionario será perfecto, sin ambigüedades ni sinónimos. En particular todo funcionará a las mil maravillas en los cuerpos de descomposición de polinomios sobre un subcuerpo de $\mathbb{C}$. Éste es el caso sobre el que trabajaba Galois para atacar el problema de la resolubilidad por radicales. Aunque en su tiempo no existiera ni siquiera la definición de cuerpo, no está de más hacer de la notación un monumento a su nombre.

Definición: Se dice que L/K es una *extensión de Galois* si es normal, finita y separable.

Teorema 3.3.1 (Teorema fundamental de la teoría de Galois) *Sea L/K una extensión de Galois. La aplicación $H \mapsto H'$ define una biyección entre los subgrupos de $\mathcal{G}(L/K)$ y los subcuerpos $M \subset L$ que conforman extensiones de K, cuya inversa es $M \mapsto \mathcal{G}(L/M)$. Además M/K es una extensión normal si y sólo si $\mathcal{G}(L/M) \triangleleft \mathcal{G}(L/K)$. En este caso $\mathcal{G}(M/K) \cong \mathcal{G}(L/K)/\mathcal{G}(L/M)$.*

Nota: Recuérdese que la notación $H \triangleleft G$ significa que H es un subgrupo normal de G, esto es, que para todo $\tau \in G$ se cumple $\tau^{-1} H \tau = H$.

Demostración: Para probar la biyectividad de la aplicación indicada basta *precomponerla* y *poscomponerla* con su posible inversa y verificar que se obtiene la identidad, esto es, hay que verificar las igualdades $\big(\mathcal{G}(L/M)\big)' = M$ y $\mathcal{G}(L/H') = H$.

Por la Proposición 3.2.4 y el Corolario 3.2.7, $[L : \big(\mathcal{G}(L/M)\big)'] = |\mathcal{G}(L/M)| = [L : M]$ y como $\big(\mathcal{G}(L/M)\big)' \supset M$, se deduce la primera igualdad (de hecho ya fue implícitamente probada en la demostración del Corolario 3.2.7). Para la segunda, nótese que por la Proposición 3.2.4 y la primera igualdad, $|\mathcal{G}(L/H')| = [L : \big(\mathcal{G}(L/H')\big)'] = [L : H'] = |H|$, de donde $\mathcal{G}(L/H') = H$, ya que la inclusión $\mathcal{G}(L/H') \supset H$ es trivial.

Supongamos que M/K es normal. Dado $\sigma \in \mathcal{G}(L/K)$, como M es un cuerpo de descomposición (Proposición 3.1.3), la Proposición 3.2.2 implica que σ aplica M en 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

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

que es sobreyectivo (por la Proposición 3.2.5 con $M_1 = M_2 = M$) y cuyo núcleo es $\mathcal{G}(L/M)$, por tanto el teorema del homomorfismo (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 $\mathcal{G}(L/K)/\mathcal{G}(L/M)$.

Por otra parte, si M/K no es normal, existen $\alpha \in M$ y $\beta \notin M$ raíces de un mismo polinomio irreducible en $K[x]$. Sea $\gamma \neq \beta$ una raíz del polinomio mínimo de β sobre M (existe por la separabilidad). Por el Corolario 3.2.6, existen automorfismos $\tau \in \mathcal{G}(L/K)$ y $\sigma \in \mathcal{G}(L/M)$ tales que $\tau(\alpha) = \beta$ y $\sigma(\beta) = \gamma$. Si fuera $\mathcal{G}(L/M) \lhd \mathcal{G}(L/K)$ entonces $\tau^{-1}\sigma\tau \in \mathcal{G}(L/M)$ y en particular debería dejar invariante a $\alpha \in M$, pero esto contradice $\tau^{-1}\sigma\tau(\alpha) = \tau^{-1}(\gamma) \neq \tau^{-1}(\beta) = \alpha$. □

Un resultado como el anterior raramente nos podrá dejar impávidos una vez que lo comprendemos. Resulta que la estructura fina de los conjuntos de números que podemos construir con sumas, restas, multiplicaciones y divisiones, operaciones ancestrales y naturales, adquiere fiel reflejo en la artificial definición de un grupo, al tiempo que el concepto de subgrupo normal que permanecía agazapado en nuestros apuntes de un curso pasado se revela ahora como representante de todos los números que podemos obtener a partir de las soluciones de ecuaciones algebraicas (cuerpos de descomposición). Es cautivador soñar que los grupos y subgrupos normales ya preexistían en algún mundo de las ideas matemáticas y que fueron descubiertos, como pieza que completa un rompecabezas, más que inventados. Esta tendencia al platonismo es lugar de recreo eventual entre los matemáticos, a pesar de los jarros de agua fría descargados por la realidad, la historia de la Ciencia y los filósofos empiristas seguidores de D. Hume, quien ya recogió la situación en su *Tratado de la Naturaleza Humana*, escribiendo: "A los matemáticos les es habitual pretender que las ideas de que se ocupan son de naturaleza tan refinada y espiritual que no son del dominio de la fantasía, sino que deben ser comprendidas por una visión pura e intelectual de la que sólo las facultades del alma son capaces".

Como hemos anunciado, el resto de la sección estará compuesta de ejemplos. Para abreviar y no alargar más este capítulo, ya desproporcionado, aprovecharemos parte de los ejemplos desarrollados en la sección anterior. Para comenzar, un ejemplo conspicuo en la historia de nuestra ciencia ya que constituye un descubrimiento del joven Gauss a los 19 años que favoreció su decisión de dedicarse a las Matemáticas. En el último capítulo volveremos sobre la teoría general al respecto que plasmó en la última sección de su obra maestra [Gau].

Ejemplo. Existen cuerpos $\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset L_3 = \mathbb{Q}(\cos(2\pi/17))$ satisfaciendo $[L_j : L_{j-1}] = 2$, $j = 1, 2, 3$. Por tanto el polígono regular de 17 lados inscrito en la circunferencia unidad es construible con regla y compás. (Nótese que a partir de $\cos(2\pi/17)$ se puede construir el ángulo de $2\pi/17$ radianes).

Sabemos que $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{16}\}$ con $\zeta = e^{2\pi i/17}$ y $\sigma_j(\zeta) = \zeta^j$. Tras algunos cálculos, se tiene que este grupo de orden 16 es cíclico generado por ejemplo por $\sigma = \sigma_3$. Los únicos subcuerpos serán $\mathbb{Q} = \langle\sigma\rangle'$, $L_1 = \langle\sigma^2\rangle'$, $L_2 = \langle\sigma^4\rangle'$, $L_3 = \langle\sigma^8\rangle'$ y $\mathbb{Q}(\zeta) = \langle\{\mathrm{Id}\}\rangle'$. Por la Proposición 3.2.4, $[L_j : \mathbb{Q}] = 2^j$. De la relación $x + 1/x = 2\cos(2\pi/17)$ válida para $x = \zeta$ se sigue que $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos(2\pi/17))] \leq 2$, además $\mathbb{Q}(\zeta) \neq \mathbb{Q}(\cos(2\pi/17))$ porque el segundo cuerpo no contiene números complejos. Así que la única posibilidad es $\mathbb{Q}(\cos(2\pi/17)) = L_3$.

Ejemplo. Hallar todos los subcuerpos de $L = \mathbb{Q}(\zeta)/\mathbb{Q}$ con $\zeta = e^{2\pi i/7}$.

La extensión $L/\mathbb{Q}$ es de Galois (L es el cuerpo de descomposición de $x^7 - 1$ sobre $\mathbb{Q}$) y todo subcuerpo $M \subset L$ conforma una extensión de $\mathbb{Q}$ ($1 \in M \Rightarrow \mathbb{Z} \subset M \Rightarrow \mathbb{Q} \subset M$).

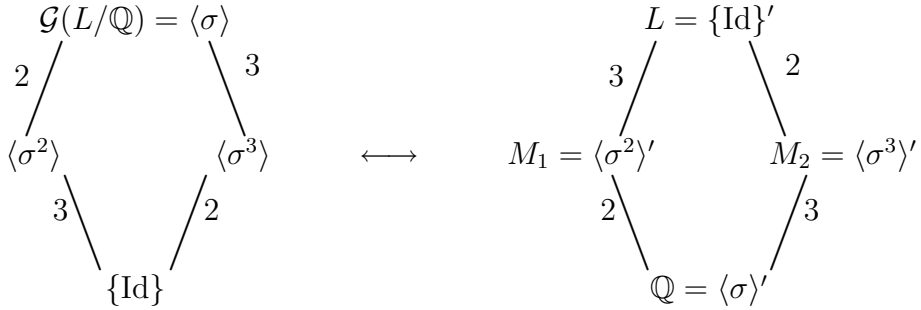
Sabíamos que $\mathcal{G}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_6\}$ con $\sigma_j(\zeta) = \zeta^j$. Es fácil ver con algunos cálculos que $\sigma = \sigma_3$ es generador de este grupo ya que $\sigma^2, \sigma^3 \neq \mathrm{Id}$. Así pues $\mathcal{G}(L/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}_6$. Los subgrupos propios son por tanto $\langle\sigma^2\rangle$ y $\langle\sigma^3\rangle$, de órdenes 3 y 2 respectivamente. Los subcuerpos fijos son $M_1 = \langle\sigma^2\rangle'$ y $M_2 = \langle\sigma^3\rangle'$ con $[M_1 : \mathbb{Q}] = 6/3 = 2$ y $[M_2 : \mathbb{Q}] = 6/2 = 3$. En un ejemplo anterior ya habíamos probado que el subcuerpo fijo por σ_2, que coincide con σ^2, es $M_1 = \mathbb{Q}(\zeta+\zeta^2+\zeta^4)$. Podemos proceder de la misma forma para hallar M_2. Nótese que $\sigma^3(\zeta) = \zeta^6 = -1-\zeta-\zeta^2-\zeta^3-\zeta^4-\zeta^5$ y por tanto para $x = \sum_{j=0}^{6} \lambda_j\zeta^j \in L$, $\sigma^3(x) = x$ equivale a

$$\begin{aligned} x &= \lambda_0 + \lambda_1\zeta^6 + \lambda_2\zeta^{12} + \lambda_3\zeta^{18} + \lambda_4\zeta^{24} + \lambda_5\zeta^{30} \\ &= \lambda_0 + \lambda_5\zeta^2 + \lambda_4\zeta^3 + \lambda_3\zeta^4 + \lambda_2\zeta^5 + \lambda_1\zeta^6 \\ &= (\lambda_0 - \lambda_1) - \lambda_1\zeta + (\lambda_5 - \lambda_1)\zeta^2 + (\lambda_4 - \lambda_1)\zeta^3 + (\lambda_3 - \lambda_1)\zeta^4 + (\lambda_2 - \lambda_1)\zeta^5 \end{aligned}$$

y de aquí $\lambda_1 = 0$, $\lambda_3 = \lambda_4$, $\lambda_2 = \lambda_5$. Lo cual prueba $M_2 = \mathbb{Q}(\zeta^3 + \zeta^4, \zeta^2 + \zeta^5)$.

Nótese que $2\cos(2\pi/7) = \zeta + \zeta^6 = -1 - (\zeta^3 + \zeta^4) - (\zeta^2 + \zeta^5) \in M_2$ y como $[\mathbb{Q}(\cos(2\pi/7)) : \mathbb{Q}] = 3$ se cumple $M_2 = \mathbb{Q}(\cos(2\pi/7))$. También M_1 se puede simplificar, ya que $[M_1 : \mathbb{Q}] = 2$ implica $M_1 = \mathbb{Q}(\sqrt{q})$ con $q \in \mathbb{Q}$. Con algo de trabajo se puede demostrar que $M_1 = \mathbb{Q}(\sqrt{7})$, aunque no lo haremos aquí.

El teorema fundamental de la teoría de Galois asegura que M_1 y M_2 son los únicos subcuerpos propios (distintos de L y $\mathbb{Q}$) de L. En un esquema se puede visualizar la relación entre el retículo de subgrupos y el de subcuerpos. A través de la aplicación $H \mapsto H'$ el segundo se obtiene a partir del primero de forma invertida. Los números indican índices (cocientes de órdenes de grupos) y grados.



Todos los subgrupos de $\mathcal{G}(L/\mathbb{Q})$ son normales porque es abeliano, por tanto $M_1/\mathbb{Q}$ y $M_2/\mathbb{Q}$ son normales.

Observación: La correspondencia entre índices y grados es consecuencia de la Proposición 3.2.4. Si $N \subset M \subset L$ con $M = H'$ y $N = G'$, entonces el índice de H en G, habitualmente denotado con $[G : H]$, es $|G|/|H| = [L : N]/[L : M] = [M : N]$.

Ejemplo. Hallar todos los subcuerpos de L, el cuerpo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$ e indicar si dan lugar a extensiones normales sobre $\mathbb{Q}$.

Sabíamos que $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\} \cong S_3$ donde τ es la conjugación (de orden 2) y $\sigma(\omega) = \omega$, $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ (de orden 3), $\omega = (-1+i\sqrt{3})/2$. Como $|S_3| = 6$, los órdenes de sus subgrupos propios sólo puede ser dos o tres. Los de orden 2 están generados por un elemento del mismo orden y hay tres de ellos, correspondiendo a cada una de las trasposiciones: $(1, 2)$, $(1, 3)$ y $(2, 3)$. Hay un solo subgrupo de orden tres, $A_3 = \langle(1, 2, 3)\rangle$, generado por un elemento de orden tres. En $\mathcal{G}(L/\mathbb{Q})$ tenemos los elementos de orden dos τ, $\sigma\tau$ y $\sigma^2\tau$, y el de orden tres σ. Por el teorema fundamental de la teoría de Galois los subcuerpos propios son, por consiguiente, $M_1 = \langle\sigma\rangle'$, $M_2 = \langle\tau\rangle'$, $M_3 = \langle\tau\sigma\rangle'$, y $M_4 = \langle\tau\sigma^2\rangle'$. Como $A_3 \lhd S_3$, pero una transposición no genera un subgrupo normal (ejercicio), se tiene que $M_1/\mathbb{Q}$ es una extensión normal mientras que $M_2/\mathbb{Q}$, $M_3/\mathbb{Q}$ y $M_4/\mathbb{Q}$ no lo son. Para calcularlos, escribamos cada $x \in L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ en función de una base de $L/\mathbb{Q}$, $x = \lambda_0 + \lambda_1\omega + \lambda_2\sqrt[3]{2} + \lambda_3\omega\sqrt[3]{2} + \lambda_4\sqrt[3]{2^2} + \lambda_5\omega\sqrt[3]{2^2}$. Por definición, $x \in M_1$ si y sólo si $x = \sigma(x)$, que empleando $\omega^2 = -\omega - 1$ se puede escribir como

$$x = \lambda_0 + \lambda_1\omega - \lambda_3\sqrt[3]{2} + (\lambda_2 - \lambda_3)\omega\sqrt[3]{2} + (\lambda_5 - \lambda_4)\sqrt[3]{2^2} - \lambda_4\omega\sqrt[3]{2^2}.$$

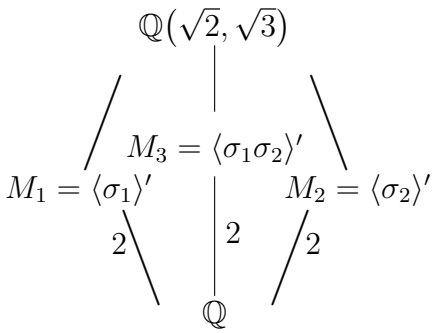
Al igualar coeficientes se obtiene $\lambda_2 = \lambda_3 = \lambda_4 = \lambda_5 = 0$, lo que implica $M_1 = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. Los otros cuerpos fijos se hallan de igual manera. Por ejemplo, al imponer $x = \tau(x)$ se tiene

$$x = (\lambda_0 - \lambda_1) - \lambda_1\omega + (\lambda_2 - \lambda_3)\sqrt[3]{2} - \lambda_3\omega\sqrt[3]{2} + (\lambda_4 - \lambda_5)\sqrt[3]{2^2} - \lambda_5\omega\sqrt[3]{2^2}.$$

Así que $\lambda_1 = \lambda_3 = \lambda_5 = 0$ y $M_2 = \mathbb{Q}(\sqrt[3]{2})$. Igualmente, $M_3 = \mathbb{Q}(\omega\sqrt[3]{2})$ y $M_4 = \mathbb{Q}(\omega^2\sqrt[3]{2})$.

Ejemplo. Hallar los subcuerpos de L, el cuerpo de descomposición de $P = x^4 - 5x^2 + 6$ sobre $\mathbb{Q}$.

Gracias a la factorización $P = (x^2 - 2)(x^2 - 3)$, se sigue $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Ya habíamos calculado su grupo de Galois, $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_1\sigma_2\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ donde $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_1(\sqrt{3}) = \sqrt{3}$, $\sigma_2(\sqrt{2}) = \sqrt{2}$, $\sigma_2(\sqrt{3}) = -\sqrt{3}$. Como $\mathbb{Z}_2 \times \mathbb{Z}_2$ sólo tiene tres subgrupos propios, $\langle(\overline{0}, \overline{1})\rangle$, $\langle(\overline{1}, \overline{0})\rangle$, $\langle(\overline{1}, \overline{1})\rangle$, el teorema fundamental de la teoría de Galois asegura que L sólo tiene tres subcuerpos propios que vienen dados por $M_1 = \langle\sigma_1\rangle'$, $M_2 = \langle\sigma_2\rangle'$, $M_3 = \langle\sigma_1\sigma_2\rangle'$. Ya habíamos comprobado que estos subcuerpos fijos son $M_1 = \mathbb{Q}(\sqrt{3})$, $M_2 = \mathbb{Q}(\sqrt{2})$ y $M_3 = \mathbb{Q}(\sqrt{6})$. De nuevo, como $\mathbb{Z}_2 \times \mathbb{Z}_2$ es un grupo abeliano todos sus subgrupos son normales y de antemano podríamos saber que las extensiones correspondientes son normales.



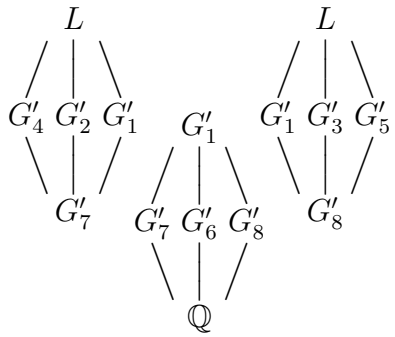
Ejemplo. Calcular cuántos subcuerpos tiene $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

La extensión $L/\mathbb{Q}$ es de Galois porque L es el cuerpo de descomposición de $x^4 - 2$ sobre $\mathbb{Q}$. Según un ejemplo de la sección anterior, $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ con τ la conjugación compleja y $\sigma(i) = i$, $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$. Por el teorema fundamental de la teoría de Galois el número de subcuerpos coincide con el de subgrupos de $\mathcal{G}(L/\mathbb{Q})$. Aparte de los subgrupos triviales $\{\mathrm{Id}\}$ y $\mathcal{G}(L/\mathbb{Q})$, el resto sólo puede tener orden dos o cuatro. Los subgrupos de orden dos son los generados por un elemento de orden dos, y los subgrupos de orden cuatro o bien están generados por un elemento de orden cuatro (si es que son isomorfos a $\mathbb{Z}_4$) o por dos de orden dos que conmutan (si es que son isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$). Podemos revisar todas las posibilidades empleando la siguiente tabla que expresa la accción de los elementos de $\mathcal{G}(L/\mathbb{Q})$ sobre i y $\sqrt[4]{2}$, los generadores de la extensión.

	i	$\sqrt[4]{2}$	orden
Id	i	$\sqrt[4]{2}$	1
σ	i	$i\sqrt[4]{2}$	4
σ^2	i	$-\sqrt[4]{2}$	2
σ^3	i	$-i\sqrt[4]{2}$	4

	i	$\sqrt[4]{2}$	orden
τ	$-i$	$\sqrt[4]{2}$	2
$\sigma\tau$	$-i$	$i\sqrt[4]{2}$	2
$\sigma^2\tau$	$-i$	$-\sqrt[4]{2}$	2
$\sigma^3\tau$	$-i$	$-i\sqrt[4]{2}$	2

De aquí se deduce que los subgrupos de orden dos son $G_1 = \langle\sigma^2\rangle$, $G_2 = \langle\tau\rangle$, $G_3 = \langle\sigma\tau\rangle$, $G_4 = \langle\sigma^2\tau\rangle$, $G_5 = \langle\sigma^3\tau\rangle$, y los de orden cuatro son $G_6 = \langle\sigma\rangle$, $G_7 = \langle\sigma^2, \tau\rangle$, $G_8 = \langle\sigma^2, \sigma\tau\rangle$.



En total hay, por tanto, diez subcuerpos de L: todos los G'_j y los subgrupos triviales L y $\mathbb{Q}$.

Hemos representado el retículo de subcuerpos en tres esquemas por razonas tipográficas (debemos unir el de en medio a los de los lados pegando los cuerpos idénticos). Los subcuerpos a la altura inmediatamente posterior a $\mathbb{Q}$ dan lugar a extensiones de grado dos, y los siguientes, a extensiones de grado cuatro. No todas las extensiones son normales, de hecho, aunque no lo comprobaremos aquí, exactamente $G'_2/\mathbb{Q}$, $G'_3/\mathbb{Q}$, $G'_4/\mathbb{Q}$ y $G'_5/\mathbb{Q}$ no son normales y el resto de los subcuerpos fijos dan lugar a extensiones normales sobre $\mathbb{Q}$.

Ejemplo. Hallar todos los subcuerpos $\mathbb{Q}(\sqrt{2}) \subsetneq M \subsetneq \mathbb{Q}(\sqrt[4]{2}, i)$.

Con la notación del ejemplo previo, ya habíamos visto en la sección anterior que $\mathbb{Q}(\sqrt{2}) = G'_7$. Por tanto debe ser $M = H'$ con H un subgrupo propio de G_7. Las únicas posibilidades son $M = G'_1$, $M = G'_2$ y $M = G'_4$. Escribamos cada $x \in M$ como

$$x = \lambda_0 + \lambda_1 i + \lambda_2\sqrt[4]{2} + \lambda_3 i\sqrt[4]{2} + \lambda_4\sqrt[4]{2^2} + \lambda_5 i\sqrt[4]{2^2} + \lambda_6\sqrt[4]{2^3} + \lambda_7 i\sqrt[4]{2^3} \qquad \text{con } \lambda_j \in \mathbb{Q}.$$

En el primer caso $\sigma^2(x) = x$ lleva a $\lambda_2 = \lambda_3 = \lambda_6 = \lambda_7 = 0$, de donde $M = \mathbb{Q}(\sqrt{2}, i)$. En el segundo caso $\tau(x) = x$ conduce claramente a $M = \mathbb{Q}(\sqrt[4]{2})$. Finalmente, $\sigma^2\tau(x) = x$ implica $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_6 = 0$ y $M = \mathbb{Q}(i\sqrt[4]{2})$.

Podemos trabajar con extensiones que no sean de Galois si es posible extenderlas a otras que lo sean.

Ejemplo. Hallar todos los subcuerpos de $\mathbb{Q}(\sqrt[4]{2})$.

Como $\mathbb{Q}(\sqrt[4]{2}) \subset L = \mathbb{Q}(\sqrt[4]{2}, i)$, los subcuerpos de $\mathbb{Q}(\sqrt[4]{2})$ lo serán también de L. Además $\mathbb{Q}(\sqrt[4]{2}) = G_2'$ implica que corresponderán a subgrupos de $\mathcal{G}(L/\mathbb{Q})$ que contengan a G_2. Según nuestro estudio, las únicas posibilidades son G_7, $\mathcal{G}(L/\mathbb{Q})$ y el propio G_2. En definitiva, los únicos subcuerpos son $G_7' = \mathbb{Q}(\sqrt{2})$, $\big(\mathcal{G}(L/\mathbb{Q})\big)' = \mathbb{Q}$ y $\mathbb{Q}(\sqrt[4]{2})$.

Demos paso ahora a un ejemplo bastante más complicado en el que calcular el grupo de Galois, e incluso el grado de la extensión, lleva a aplicar el teorema fundamental de la teoría de Galois.

Ejemplo. Hallar $\mathcal{G}(\mathbb{Q}(\zeta, \sqrt[3]{3})/\mathbb{Q})$ con $\zeta = e^{2\pi i/13}$.

No está claro si la extensión es normal. Tenemos la inclusión $\mathbb{Q}(\zeta, \sqrt[3]{3}) \subset L = \mathbb{Q}(\zeta, \sqrt[3]{3}, \omega)$ con $L/\mathbb{Q}$ normal, $\omega = (-1 + i\sqrt{3})/2$. En $\mathcal{G}(L/\mathbb{Q})$, de acuerdo con el Corolario 3.2.6, cualquier $\mathbb{Q}$-automorfismo aplica $\sqrt[3]{3}$ en $\sqrt[3]{3}$, $\omega\sqrt[3]{3}$ o $\omega^2\sqrt[3]{3}$. A continuación probaremos que $\omega\sqrt[3]{3}, \omega^2\sqrt[3]{3} \notin \mathbb{Q}(\zeta, \sqrt[3]{3})$, de donde se concluye que todos los automorfismos de $\mathcal{G}(\mathbb{Q}(\zeta, \sqrt[3]{3})/\mathbb{Q})$ fijan $\sqrt[3]{3}$. Por tanto sus automorfismos serán los extendidos desde $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$, es decir, $\mathcal{G}(\mathbb{Q}(\zeta, \sqrt[3]{3})/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{12}\}$ con $\sigma_j(\zeta) = \zeta^j$ y $\sigma_j(\sqrt[3]{3}) = \sqrt[3]{3}$.

Resta por tanto demostrar que $\omega\sqrt[3]{3}, \omega^2\sqrt[3]{3} \notin \mathbb{Q}(\zeta, \sqrt[3]{3})$, lo cual equivale a $\omega \notin \mathbb{Q}(\zeta, \sqrt[3]{3})$. No puede ser $\sqrt[3]{3} \in \mathbb{Q}(\zeta)$ porque al ser $\mathbb{Q}(\zeta)/\mathbb{Q}$ normal se tendría la inclusión $\mathbb{Q}(\sqrt[3]{3}, \omega\sqrt[3]{3}, \omega^2\sqrt[3]{3}) \subset \mathbb{Q}(\zeta)$ lo que lleva a una contradicción porque el grupo de Galois (sobre $\mathbb{Q}$) del primer cuerpo no es abeliano y el segundo sí. Por consiguiente $[\mathbb{Q}(\zeta, \sqrt[3]{3}) : \mathbb{Q}(\zeta)] = 3$ lo que implica que $\omega \notin \mathbb{Q}(\zeta, \sqrt[3]{3}) - \mathbb{Q}(\zeta)$ ya que ω está en una extensión de grado a lo más dos sobre $\mathbb{Q}(\zeta)$. Con algunos cálculos (ejercicio) se prueba que el único subcuerpo de $\mathbb{Q}(\zeta)$ de grado dos sobre $\mathbb{Q}$ es $\mathbb{Q}(\zeta + \zeta^3 + \zeta^4 + \zeta^9 + \zeta^{10} + \zeta^{12})$. Este subcuerpo es de números reales ya que $\zeta^k + \zeta^{13-k} = 2\cos(2\pi k/13)$, por tanto no puede coincidir con $\mathbb{Q}(\omega)$.

En extensiones de cuerpos finitos todo es muy fácil, porque el grupo de Galois es siempre cíclico y hay un subgrupo de cada orden que divida al del grupo. Cada uno de ellos corresponderá a un subcuerpo isomorfo a algún $\mathbb{F}_q$. Sin embargo siempre podemos complicar un poco las cosas pidiendo una representación particular de los subcuerpos.

Ejemplo. Sea α una raíz de $x^4 + x + 1 \in \mathbb{F}_2[x]$ en su cuerpo de descomposición. Describir los subcuerpos $\mathbb{F}_2 \subsetneq M \subsetneq \mathbb{F}_2(\alpha)$ como $M = \mathbb{F}_2(\beta)$ para algún $\beta \in \mathbb{F}_2(\alpha)$

Como x^4+x+1 es irreducible, $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$, $\mathbb{F}_2(\alpha)$ es isomorfo a $\mathbb{F}_{2^4}$ y el grupo de Galois es $\mathcal{G}(\mathbb{F}_2(\alpha)/\mathbb{F}_2) = \langle\phi\rangle \cong \mathbb{Z}_4$ donde ϕ es el automorfismo de Frobenius $\phi(x) = x^2$. El único subgrupo propio es $\langle\phi^2\rangle$ y por tanto $M = \langle\phi^2\rangle'$. Cualquier $x \in \mathbb{F}_2(\alpha)$ se escribe como $x = \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3$ con $\lambda_j \in \mathbb{F}_2$. En $\mathbb{F}_2(\alpha)$, $(a+b)^4 = a^4 + b^4$ (porque tiene característica dos, ejercicio) y empleando $\alpha^4 + \alpha + 1 = 0$ se tiene que $x = \phi^2(x)$ equivale a

$$\begin{aligned} x &= \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3 = \lambda_0 + \lambda_1(\alpha+1) + \lambda_2(\alpha+1)^2 + \lambda_3(\alpha+1)^3 \\ &= (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3) + (\lambda_1 + \lambda_3)\alpha + (\lambda_2 + \lambda_3)\alpha^2 + \lambda_3\alpha^3 \end{aligned}$$

de donde $\lambda_3 = 0$ y $\lambda_1 = \lambda_2$. Por tanto $M = \mathbb{F}_2(\alpha + \alpha^2)$.

Ejercicios del Capítulo 3

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 3.1

1. Hallar el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $x^6 - 8$, y calcular el grado de la extensión correspondiente.

2. Hallar el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $x^4 + 5x^2 + 5$ y calcular su grado.

3. Probar que $P = x^4 - 2x^3 - x^2 - 2x - 2$ y $Q = x^5 - 3x^3 + x^2 - 3$ tienen el mismo cuerpo de descomposición sobre $\mathbb{Q}$. *Indicación*: Nótese que i es raíz del primero y que $\sqrt{3}$ es raíz del segundo.

4. Sean cuerpos $K \subset M \subset L$ y sea $P \in K[x]$ no constante. Si L es cuerpo de descomposición de P sobre K, probar que L es cuerpo de descomposición de P sobre M.

5. Si L es el cuerpo de descomposición de $P \in K[x]$, demostrar que $[L : K] \big| (\partial P)!$. *Indicación*: Procédase por inducción en el grado del polinomio, distinguiendo dos casos al aplicar la hipótesis de inducción dependiendo de la irreducibilidad de P. Recuérdese que $r!s!$ divide a $(r + s)!$ por la fórmula para los números combinatorios.

6. Sea L/K una extensión de grado 4. Demostrar que si L es el cuerpo de descomposición de un polinomio irreducible de la forma $x^4 + ax^2 + b \in K[x]$, existe un cuerpo intermedio $K \subset E \subset L$ tal que $[E : K] = 2$.

7. Si $K \subset M \subset L$, demostrar que L/K normal $\Rightarrow$ L/M normal, pero L/K normal $\not\Rightarrow$ M/K normal, y L/M, M/K normales $\not\Rightarrow$ L/K normal.

8. Estudiar si las extensiones $\mathbb{Q}(\sqrt[3]{-2}, \sqrt{-2})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[3]{-3}, \sqrt{-3})/\mathbb{Q}$, son normales.

9. 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.

10. Demostrar que toda extensión de grado dos es normal.

11. Dar un ejemplo de una extensión normal que no sea finita.

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

13. Dar un ejemplo de una extensión normal de grado 3.

♢**14.** Dar un ejemplo de extensión normal de grado 3 sobre $\mathbb{Q}$. *Indicación*: Buscar un polinomio cuyas raíces sean $\cos(2\pi/7)$, $\cos(4\pi/7)$ y $\cos(6\pi/7)$.

15. Demostrar que dada una extensión finita M/K siempre existe un L, $L \supset M \supset K$ tal que L/K es normal y finita. A un cuerpo con estas características y $[L : K]$ mínimo

se le llama *clausura normal* (o cierre normal) de M/K. Probar que sólo hay una clausura normal salvo isomorfismos y hallar la de $\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}$.

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

17. Probar que $\mathbb{F}_8$ es el cuerpo de descomposición de $x^3+x^2+1 \in \mathbb{F}_2[x]$ y que $\mathbb{F}_8/\mathbb{F}_2$ es simple.

18. ¿Cuál es el grupo aditivo de $\mathbb{F}_8$?

19. Si $P \in \mathbb{F}_p[x]$ es irreducible y gr $P = n$, ¿es su cuerpo de descomposición isomorfo a $\mathbb{F}_{p^n}$?

20. Estudiar si $\mathbb{F}_{64}$ es una extensión de $\mathbb{F}_{16}$ y de $\mathbb{F}_8$ y en su caso hallar el grado.

21. Sea $P = x^q - x$ con $q = p^n$. Demostrar que cualquier polinomio irreducible en $\mathbb{F}_p[x]$ de grado n divide a P.

22. Probar que todos los factores irreducibles de $x^q - x \in \mathbb{F}_p[x]$ con $q = p^n$, son de grado menor o igual que n.

23. Demostrar que si α es una raíz de $x^3 - 2$ en $\mathbb{F}_{7^3}$, entonces -1, α y $-1+\alpha$ tienen orden (multiplicativo) 2, 9 y 19 respectivamente en el grupo multiplicativo de $\mathbb{F}_{7^3}$. Galois utilizó este hecho para deducir que una raíz de $x^3 - x + 1 \in \mathbb{F}_7[x]$ genera este grupo multiplicativo. Tratar de reconstruir su argumento. *Indicación*: $7^3 - 1 = 2 \cdot 9 \cdot 19$ y en un grupo abeliano $|\langle g\rangle| = n$, $|\langle h\rangle| = m \Rightarrow |\langle gh\rangle| = \text{mcm}(n, m)$.

♢**24.** Probar que el grupo multiplicativo de un cuerpo finito es cíclico. *Indicación*: Estudiar el número de raíces de $x^n - 1$.

∘**25.** Se dice que un cuerpo de característica p es un *cuerpo perfecto* si el morfismo de Frobenius $x \mapsto x^p$ es un isomorfismo. Probar que si K es perfecto todo polinomio irreducible en $K[x]$ es separable. *Indicación*: Tratar de ajustar la prueba vista en el caso $K = \mathbb{F}_p$.

26. ¿Cuántas raíces distintas tiene $x^{12} + 2x^6 + 1 \in \mathbb{F}_3[x]$ en su cuerpo de descomposición?

♢**27.** Sea K un cuerpo de característica $p > 0$ y supongamos que $P = x^p - x - a$ es irreducible en $K[x]$. Probar que si $\alpha \in L \supset K$ es raíz de P entonces $K(\alpha)/K$ es normal.

28. Sea K un cuerpo de característica $p \neq 0$, y sea $f(x) = x^p - a \in K[x]$. Demostrar que $f(x)$ es irreducible sobre K, o que descompone como producto de factores de grado 1 sobre K.

29. Si $K \subset M \subset L$ con L/K finita, demostrar que L/K separable$\Rightarrow$ L/M separable, pero M/K separable $\not\Rightarrow$ L/K separable.

30. Hallar una extensión separable y normal que no sea finita.

31. Dar un ejemplo de una extensión de grado 3 no separable.

32. Sea K un cuerpo de característica $p \neq 0$. Probar que $x^{p^n} - x$ no tiene raíces repetidas.

33. Sea L/K una extensión algebraica con K un cuerpo de característica $p > 0$. Demostrar que si $\alpha \in L$ es separable sobre K y $\alpha^n \in K$ con n una potencia de la característica, entonces $\alpha \in K$.

34. Sea L/K una extensión algebraica con K un cuerpo de característica $p > 0$. Probar que $\alpha \in L$ es separable sobre K si y sólo si $K(\alpha) = K(\alpha^p)$.

35. Sabiendo que el cuerpo de descomposición de un polinomio sin raíces múltiples da lugar siempre a una extensión separable (lo cual es el contenido de un ejercicio de la próxima sección), probar que los elementos separables sobre un cuerpo siempre forman un cuerpo.

♢♢**36.** Sea L/K finita, a partir de la conclusión del ejercicio anterior, probar que si L/M y M/K son separables, L/K también lo es. *Indicación*: Comenzar probando que para todo $\alpha \in L$ existe n igual a una potencia de $\mathrm{char}(K)$ tal que α^n es separable.

37. ¿Es cierto el recíproco del teorema del elemento primitivo?

♢♢**38.** Demostrar que si $K \subset L$ y $[L : K] < \infty$, la extensión L/K no es simple si y sólo si existen infinitos cuerpos intermedios $K \subset M \subset L$. *Indicación*: Si $L = K(\alpha)$, probar que M debe estar generado sobre K por los coeficientes de algún factor del polinomio mínimo de α.

Sección 3.2

♡**39.** Si $L = K(a_1, \ldots, a_n)$ y σ es un K-automorfismo de L tal que $\sigma(a_i) = a_i$ para todo i, probar que σ es la identidad.

40. Sea L un cuerpo. Demostrar que cualquier automorfismo es un K-automorfismo donde K es la intersección de todos los subcuerpos de L (el llamado *subcuerpo primo*).

41. Demostrar que los conjuntos:

$$A = \{\lambda_1 + \lambda_2\sqrt{7} \ : \ \lambda_1, \lambda_2 \in \mathbb{Q}\} \quad \text{y} \quad B = \left\{\lambda_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ : \ \lambda_1, \lambda_2 \in \mathbb{Q}\right\}$$

son espacios vectoriales sobre $\mathbb{Q}$ isomorfos, pero no son cuerpos isomorfos. *Indicación*: Sólo en uno de ellos la ecuación $x^2 + 1 = 0$ tiene solución.

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

43. Este ejercicio determina $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.

i) Probar que cada $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ lleva cuadrados a cuadrados y reales positivos a reales positivos. Concluir que $a < b \Rightarrow \sigma(a) < \sigma(b)$.

ii) Probar que $|a - b| < 1/m \ \Rightarrow \ |\sigma(a) - \sigma(b)| < 1/m$. Concluir que σ es una aplicación continua de $\mathbb{R}$.

iii) Comprobar que una aplicación continua de $\mathbb{R}$ que es la identidad sobre $\mathbb{Q}$ debe ser la identidad en todo $\mathbb{R}$, y por tanto $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{Id}\}$.

44. Probar con todo rigor que en $\mathbb{Q}(\sqrt{2},\sqrt{3})$ la aplicación $\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$ con $a,b,c,d\in\mathbb{Q}$ es un $\mathbb{Q}$-automorfismo.

45. Hallar el grupo de Galois del cuerpo de descomposición de x^4+x^2-6 sobre $\mathbb{Q}$.

46. Encontrar el grupo de Galois de una extensión normal de $\mathbb{Q}$ de grado mínimo conteniendo a $\sqrt{2}+\sqrt[3]{2}$.

47. Calcular el grupo de Galois de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q}$.

48. Hallar el grupo de Galois del polinomio x^4-9 sobre $\mathbb{Q}$.

49. Hallar el grupo de Galois del polinomio x^4+9 sobre $\mathbb{Q}$.

50. Calcular $\mathcal{G}(L/K)$ donde $K=\mathbb{Q}(e^{2\pi i/5})$ y L es el cuerpo de descomposición de $P=x^5-7$ sobre K.

51. Sea $K\subset\mathbb{C}$ el cuerpo de descomposición de $x^2-x+1\in\mathbb{Q}[x]$ y L el de x^3-2. Hallar $\mathcal{G}(L/K)$.

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

53. 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.

54. Sea $P\in K[x]$ irreducible de grado tres con $\mathrm{char}(K)=0$, y sea L su cuerpo de descomposición. Demostrar que o bien $[L:K]=3$ o bien $[L:K]=6$.

55. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})\big)$, $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}(\sqrt{6})\big)$, $\mathcal{G}\big(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}\big)$.

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

57. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt{5}+\sqrt{7})/\mathbb{Q}\big)$.

58. Sea $P=x^4-3x^2+4\in\mathbb{Q}[x]$. Calcular el grupo de Galois de su cuerpo de descomposición sobre $\mathbb{Q}$.

59. Sea $\alpha=\sqrt{2}+i$ y sea P el polinomio mínimo de α sobre $\mathbb{Q}$. Hallar el grupo de Galois del cuerpo de descomposición de P sobre $\mathbb{Q}$.

60. Calcular $\mathcal{G}(\mathbb{Q}(x,y)/\mathbb{Q}(x+y,xy))$ y $\mathcal{G}(\mathbb{Q}(x,y,z)/\mathbb{Q}(x+y+z,xy+xz+yz,xyz))$ donde $\mathbb{Q}(x,y)$ y $\mathbb{Q}(x,y,z)$ denotan los cuerpos de funciones racionales en dos y tres variables respectivamente. *Indicación*: En el primer caso, x e y son raíces del polinomio $X^2-(x+y)X+xy\in\mathbb{Q}(x+y,xy)[X]$.

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

62. Hallar un grupo sencillo que sea isomorfo a $\mathcal{G}\big(\mathbb{Q}(e^{2\pi i/13})/\mathbb{Q}\big)$.

♡**63.** ¿Por qué $\mathcal{G}(L/H')\supset H$ es trivial?

64. Probar que si $L = \mathbb{Q}(\cos\frac{2\pi}{17})$, $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6, \sigma^7\} \cong \mathbb{Z}_8$ donde $\sigma\big(2\cos(2\pi/17)\big) = \sigma\big(\zeta + \zeta^{-1}\big) = \zeta^3 + \zeta^{-3}$ con $\zeta = e^{2\pi i/17}$. Demostrar que $\cos(2\pi k/17) \in L$ y que $\sigma(\cos(2\pi k/17)) = \cos(6\pi k/17)$. Si $H = \{\mathrm{Id}, \sigma^4\}$, probar que $H' = \mathbb{Q}(x_1, x_2)$ donde $x_1 = \cos\frac{2\pi}{17} + \cos\frac{26\pi}{17}$ y $x_2 = \cos\frac{2\pi}{17} \cdot \cos\frac{26\pi}{17}$.

65. Encontrar todos los elementos de $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ con $\zeta = e^{2\pi i/7}$ que dejan fijo a $\zeta + \zeta^2 + 3\zeta^3 + \zeta^4 + 3\zeta^5 + 3\zeta^6$.

66. Hallar $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^3 + \zeta^9))$ con $\zeta = e^{2\pi i/13}$.

67. Sean L_1 y L_2 los cuerpos de descomposición de dos polinomios P_1 y P_2 sobre $\mathbb{Q}$. Demostrar que si $L_1 \cap L_2 = \mathbb{Q}$, entonces $\mathcal{G}(L_1/\mathbb{Q}) \times \mathcal{G}(L_2/\mathbb{Q}) \cong \mathcal{G}(L/\mathbb{Q})$ donde L es el cuerpo de descomposición de P_1P_2.

68. Hallar una extensión cuyo grupo de Galois sea isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

69. Si H y N son subgrupos de $\mathcal{G}(L/K)$ cuyos subcuerpos fijos son $H' = L_1$ y $N' = L_2$, indicar qué subcuerpo es $\langle \sigma, \tau \,:\, \sigma \in H,\ \tau \in N\rangle'$.

70. Si $L = \mathbb{Q}(x, y, z)$ y $K = \mathbb{Q}(x + y + z, xy + xz + yz, xyz)$, probar que $\mathbb{Q}\big((x - y)(x - z)(y - z)\big) = \langle\sigma\rangle'$ con σ un elemento de orden 3 de $\mathcal{G}(L/K)$.

♢**71.** Sea L el cuerpo de descomposición de un polinomio sin raíces múltiples. Digamos $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ con $P = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in K[x]$, $\alpha_i \neq \alpha_j$. Sea $L_j = K(\alpha_1, \alpha_2, \ldots, \alpha_j)$ y $L_0 = K$. Probar que cada monomorfismo $L_j \longrightarrow L$ se extiende a $[L_{j+1} : L_j]$ monomorfismos $L_{j+1} \longrightarrow L$. Deducir de ello que $|\mathcal{G}(L/K)| = [L : K]$. Concluir finalmente que todos los elementos de L son separables sobre K.

72. 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.

73. Hallar $\mathcal{G}(\mathbb{F}_2(x)/\mathbb{F}_2(x^2))$.

74. Consideremos $\zeta = e^{2\pi i/5}$ y sea σ el $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\zeta)$ dado por $\sigma(\zeta) = \zeta^4$. Demostrar que el cuerpo fijo de σ es $\mathbb{Q}(\sqrt{5})$. *Indicación*: Elevar al cuadrado $\frac{1}{2} + \zeta^2 + \zeta^3$.

75. Sea $L = \mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle$ y $K = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$. Hallar $\mathcal{G}(L/K)$ y comprobar que el orden del morfismo de Frobenius en L es 4.

♡**76.** Si σ tiene orden 4 y $\tau \neq \sigma^2$ tiene orden 2, ¿por qué sabemos que los automorfismos en $\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ son distintos?

77. Sea L el cuerpo de descomposición en $\mathbb{C}$ del polinomio $x^4 + 1$ sobre $\mathbb{Q}$. Encontrar los automorfismos de L con cuerpos fijos $\mathbb{Q}(\sqrt{-2})$ y $\mathbb{Q}(\sqrt{2})$.

78. Sea σ un elemento de $\mathcal{G}(L/K)$ de orden $2n$. Demostrar que para cualquier $\alpha \in L$, $\alpha + \sigma^2(\alpha) + \sigma^4(\alpha) + \cdots + \sigma^{2n-2}(\alpha) \in \langle\sigma^2\rangle'$.

Sección 3.3

79. Sea $L = \mathbb{Q}(\zeta)$ donde $\zeta = e^{2\pi i/11}$. Demostrar que L es una extensión normal de $\mathbb{Q}$ y determinar su grupo de Galois. Encontrar todos los cuerpos intermedios de la

extensión $L/\mathbb{Q}$ y los subgrupos de $\mathcal{G}(L/\mathbb{Q})$ que les corresponden indicando cuáles dan lugar a extensiones normales de $\mathbb{Q}$.

80. Si L/K es una extensión de Galois con grupo de Galois cíclico, probar que dos cuerpos intermedios M_1, M_2 (conteniendo a K) satisfacen $M_1 \subset M_2$ si y sólo si $[L : M_1]$ es un múltiplo de $[L : M_2]$.

81. Sean $K \subset M \subset L$ con L/K de Galois. Probar que $M = K(a)$ con $a \in M$ si y sólo si los únicos elementos de $\mathcal{G}(L/K)$ que fijan a están en $\mathcal{G}(L/M)$. Emplear este resultado para dar una nueva prueba de $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Demostrar de igual manera que $\mathbb{Q}(\sqrt[3]{17}, \sqrt{17}) = \mathbb{Q}(\sqrt[3]{17} + \sqrt{17})$.

♡**82.** Si $K \subset M \subset L$ y L/K es de Galois, ¿deben ser necesariamente L/M y M/K de Galois?

83. Si en una extensión de Galois L/K, con $\mathrm{char}(K) \neq 2$, el grupo de Galois es $\mathbb{Z}_2 \times \mathbb{Z}_2$, demostrar que $L = K(\alpha, \beta)$ con $\alpha^2, \beta^2 \in K$.

84. Sea $\alpha = \sqrt{2} + i$ y sea P el polinomio mínimo de α sobre $\mathbb{Q}$. Hallar todos los subcuerpos de su cuerpo de descomposición sobre $\mathbb{Q}$.

♡**85.** 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, $\mathbb{Q} \subset M \subset L$.

86. Supongamos que $f(x) \in \mathbb{Q}[x]$ es irreducible con $\partial f = 4$ y su cuerpo de descomposición sobre $\mathbb{Q}$ tiene grupo de Galois A_4. Sea θ una raíz de $f(x)$ y sea $L = \mathbb{Q}(\theta)$. Probar que L es una extensión de grado 4 de $\mathbb{Q}$ que no tiene subcuerpos propios. ¿Hay alguna extensión de Galois de $\mathbb{Q}$ de grado cuatro sin subcuerpos propios?

87. Probar que si el grupo de Galois del cuerpo de descomposición de una cúbica sobre $\mathbb{Q}$ es $\mathbb{Z}_3$, entonces todas las raíces de la cúbica son reales.

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

89. Calcular cuántos subcuerpos tiene el cuerpo de descomposición de $P = x^5 + 3x^3 - 3x^2 - 9$ sobre $\mathbb{Q}$.

90. Calcular cuántos subcuerpos tiene el cuerpo de descomposición de $P = x^7 + 4x^5 - x^2 - 4$ sobre $\mathbb{Q}$.

91. Hallar todos los subcuerpos del cuerpo de descomposición sobre $\mathbb{Q}$ de $P = x^4 + 1$.

92. Hallar todos los subcuerpos propios del cuerpo de descomposición de $P = x^4 - 2$ sobre $\mathbb{Q}$.

93. Calcular cuántos subcuerpos tiene $\mathbb{Q}\big(\cos(2\pi/13)\big)$.

94. Estudiar qué automorfismos de $\mathcal{G}\big(\mathbb{Q}(e^{2\pi i/7})/\mathbb{Q}\big)$ dejan invariante $i\,\mathrm{sen}(2\pi/7)$ y utilizar el resultado para hallar $[\mathbb{Q}\big(i\,\mathrm{sen}(2\pi/7)\big) : \mathbb{Q}]$ y $[\mathbb{Q}(e^{2\pi i/7}) : \mathbb{Q}\big(i\,\mathrm{sen}(2\pi/7)\big)]$.

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

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

97. Si $\mathcal{G}(L/\mathbb{Q}) \cong \mathbb{Z}_{p^2q}$ (donde p y q son primos distintos) con $L/\mathbb{Q}$ de Galois, probar que L tiene subcuerpos L_1, L_2, L_3 tales que $[L_1 : \mathbb{Q}] = p$, $[L_2 : \mathbb{Q}] = p^2$ y $[L_3 : \mathbb{Q}] = q$.

98. Sea K un cuerpo de característica cero, y sea E el cuerpo de descomposición de algún polinomio sobre K. Si $\mathcal{G}(E/K)$ es isomorfo a A_4, probar que E no tiene ningún subcuerpo L tal que $[E : L] = 2$.

99. Sea α una raíz de $x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. Hallar β en función de α de tal forma que $\mathbb{F}_2 \subsetneq \mathbb{F}(\beta) \subsetneq \mathbb{F}_2(\alpha)$ y dar un polinomio en $\mathbb{F}_2[x]$ cuyo cuerpo de descomposición sea $\mathbb{F}_2(\beta)$.

100. Demostrar que si $\mathbb{Q} \subset M \subset \mathbb{Q}(e^{2\pi i/k})$, entonces $\mathcal{G}(M/\mathbb{Q})$ es abeliano. (Nota: El recíproco, para $M/\mathbb{Q}$ de Galois, es un profundo resultado llamado *teorema de Kronecker-Weber*).

101. Para cada n par hallar un polinomio $P \in \mathbb{Q}[x]$ con $\partial P = n$ y raíces distintas no racionales, tal que el grupo de Galois de su cuerpo de descomposición sea isomorfo a $\mathbb{Z}_2$.

102. Hallar una extensión normal de $\mathbb{Q}$ cuyo grupo de Galois sea $\mathbb{Z}_9$. *Indicación*: $9 = (19 - 1)/2$.

103. Sea L/K una extensión de Galois y sean M_1/K y M_2/K subextensiones de Galois. Demostrar que si M_3 es el menor subcuerpo de L que contiene a M_1 y M_2, entonces $\mathcal{G}(M_3/M_1)$ es isomorfo a $\mathcal{G}(M_2/(M_1 \cap M_2))$.

104. Sea $p = 2q + 1$ con p y q primos, hallar cuántos subcuerpos tiene $\mathbb{Q}(e^{2\pi i/p})$.

105. Sea L un cuerpo y sea G un subgrupo finito del grupo de automorfismos $\phi : L \longrightarrow L$. Sea $K = \{a \in L \ : \ \phi(a) = a, \ \forall \ \phi \in G\}$. *i*) Probar que K es un subcuerpo de L con $[L : K] = |G|$. *ii*) Probar que si L/K es simple, es de Galois. $\diamondsuit$*iii*) Probar incondicionalmente que L/K es de Galois.

106. Demostrar que $\sqrt[3]{n} \in \mathbb{Q}(e^{2\pi i/p})$ con $n \in \mathbb{Z}$ y p primo si y sólo si n es un cubo perfecto.

$\diamondsuit\diamondsuit$**107.** Sea p un primo con $p - 1$ divisible por 4. Demostrar que $\sqrt{n} \in \mathbb{Q}(e^{2\pi i/p})$ con $n \in \mathbb{Z}$ si y sólo si n o n/p son cuadrados perfectos. *Indicación*: Probar que $\sum_{n=1}^{p} e^{2\pi i n^2/p}$ genera la única subextensión de grado 2 de $\mathbb{Q}(e^{2\pi i/p})$.

108. 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 finita, pero existen infinitos subcuerpos intermedios $K \subset M \subset L$. ¿Por qué esto no contradice el teorema fundamental de la teoría de Galois?

$\circ$**109.** Galois enunció el siguiente lema sin demostración *"Sea una ecuación cualquiera sin raíces iguales, digamos $a, b, c, \ldots$ Siempre se puede formar una función V de las raíces tal que los valores que se obtienen permutando dichas raíces de todas las formas posibles son todos desiguales. Por ejemplo se puede tomar $V = Aa + Bb + Cc + \ldots$,*

siendo $A, B, C, \ldots$ *números enteros* [no nulos] *convenientemente elegidos"*. Y después dedujo otro lema: *"La función tomada anteriormente tienen la propiedad de que todas las raíces de la ecuación propuesta se expresan racionalmente en función de* V*"*. En notación moderna esto es $a, b, c, \cdots \in K(V)$ donde K es el cuerpo generado por los coeficientes de la ecuación. Probar estos resultados (para $K \subset \mathbb{C}$). *Indicación*: El primero se cumple para números complejos arbitrarios. Para el segundo, Galois aplicó el teorema de los polinomios simétricos al producto de factores $(Ax + Bb + Cc + \cdots - V)$ permutando de todas las formas posibles $b, c, \ldots$ pero sin cambiar V.

Apéndice del Capítulo 3

Conoce a tus héroes

(Más información en: `http://turnbull.mcs.st-and.ac.uk/history/`)

Apellido: Galois
Nombre: Evariste
Nacimiento: 1811 Bourg La Reine
Defunción: 1832 París

E. Galois vivió durante los tumultuosos años de la restauración monárquica en Francia después de Napoleón. A pesar de su brevísima vida, el importante estudio que realizó sobre la resolución de ecuaciones algebraicas por medio de grupos de permutaciones ha brindado a las Matemáticas una de sus partes más bellas, conocida hoy de forma genérica en su honor como *teoría de Galois*. Sus trabajos no recibieron la merecida atención en su tiempo, y no alcanzaron difusión entre la comunidad matemática hasta más de una década tras su muerte. Esto, combinado con la juventud de Galois, su intensa actividad revolucionaria y su fallecimiento en un duelo, ha transformado a veces su biografía en una leyenda no siempre fiel a la realidad [Rot].

Bla, bla, bla

- *Sea una ecuación tal con congruencias, $F(x) = 0$, y p el módulo. Supongamos, para simplificar, que la congruencia no admite ningún factor conmensurable, esto es, que no existen funciones $\phi(x)$, $\psi(x)$, $\chi(x)$ tales que $\phi(x)\psi(x) = F(x) + p\chi(x)$. En ese caso, la congruencia no admitirá ninguna raíz entera, ni ninguna raíz inconmensurable de grado inferior. Consideremos las raíces de esta congruencia como una especie de símbolos imaginarios, ya que no se ajustan a discusiones con números enteros, símbolos cuyo empleo en los cálculos será tan útil como el del imaginario $\sqrt{-1}$ en el análisis ordinario.* E. Galois 1830.

- Teorema: *Sea una ecuación dada y a, b, c, ... sus m raíces. Hay un grupo de permutaciones de las letras a, b, c, ... que goza de las propiedades siguientes:* i) *Toda función de las raíces invariante por las sustituciones del grupo es racionalmente conocida;* ii) *Recíprocamente, toda función de las raíces determinable racionalmente es invariante por las sustituciones.* E. Galois 1831.

- *Hemos hecho grandes esfuerzos para comprender las pruebas de Galois. Su razonamiento no está ni suficientemente claro ni desarrollado para permitirnos juzgar su corrección, y no podemos hacernos una idea de él. El autor anuncia que la proposición que constituye el objetivo de esta memoria forma parte de una teoría general susceptible de muchas aplicaciones.* S.D. Poisson 1831.

- *Pide a Jacobi o a Gauss públicamente que den su opinión, no acerca de la certeza, sino de la importancia de estos teoremas. Más adelante habrá gente, espero, que encontrará provechoso descifrar todo este lío.* E. Galois 1832 (de su carta a A. Chevalier, el día antes del duelo que causó su muerte).

¿Qué hay que saberse?

Esencialmente, manejar extensiones normales, conocer el concepto de separabilidad, calcular grupos de Galois de extensiones suficientemente sencillas y, por supuesto, hay que saberse perfectamente el teorema fundamental de la teoría de Galois y cómo se aplica en diferentes ejemplos.

(PQR) Preguntón, quejoso y respondón

P- La teoría de Galois, ¿es realmente de Galois?

R- En tiempos de Galois no habían sido definidos los automorfismos, ni las extensiones de cuerpos, ni sus grados, y los grupos eran sólo de permutaciones; de modo que no podemos esperar encontrar en los trabajos de Galois algo similar a lo que contienen los libros de hoy en día titulados "Teoría de Galois".

Q- Entonces el nombre es inadecuado.

R- No, porque la idea de que la estructura del cuerpo de descomposición queda fielmente reflejado en un grupo y la utilización de ello para dar una solución final al problema de resolubilidad por radicales, son suyas.

P- El cálculo del grupo de Galois parece algo combinatorio que se reduce a comprobar unas cuantas posibilidades, ¿no es así?

R- Sólo cuando tenemos extensiones de Galois presentadas de forma muy simple. Si nos enfrentásemos al cuerpo de descomposición de $x^5 - 6x + 3$ no sabríamos cómo empezar.

P- Tendríamos que hallar explícitamente las raíces.

R- Una consecuencia de la teoría de Galois es que tal cosa es imposible con las operaciones algebraicas habituales.

Q- Entonces no hay ningún método general para hallar $\mathcal{G}(L/\mathbb{Q})$ con $L/\mathbb{Q}$ de Galois.

R- En realidad sí, pero requeriría tantas operaciones que es impracticable.

Q- Pero si en general no podemos hallar el grupo de Galois, la teoría de Galois no sirve para nada.

R- Nos dice que es lo mismo estudiar subcuerpos que subgrupos, lo cual es un descubrimiento matemático de primer orden, independientemente de lo difíciles que sean los cálculos.

P- ¿Y es posible obtener cualquier grupo finito como grupo de Galois del cuerpo de descomposición de un polinomio en $\mathbb{Q}[x]$?

R- Se cree que sí, pero nadie ha conseguido demostrarlo hasta ahora.

Capítulo 4

Resolubilidad por radicales

4.1. Grupos solubles

El capítulo anterior se puede esquematizar diciendo que en las extensiones de Galois podemos transformar problemas de teoría de cuerpos en otros de teoría de grupos. Por ello no es de extrañar que resultados profundos acerca de grupos permitan deducir algunas propiedades finas de las extensiones de cuerpos.

Nuestro objetivo principal en este capítulo es el estudio de la resolubilidad por radicales de ecuaciones algebraicas, para lo cual sólo emplearemos como temas ajenos a los capítulos previos la definición de grupo soluble y un resultado acerca de este tipo de grupos, el Teorema 4.1.1. Por ello esta sección admite dos lecturas: una concisa que termina con los ejemplos tras dicho resultado, y otra más extensa que traspasa la frontera de los ejemplos incluyendo su prueba y la teoría que la rodea. Ya optemos por la versión económica o por la lujosa, nada nos evitará tener que escudriñar en el arcón de los recuerdos para airear el importantísimo concepto de subgrupo normal, introducido en Álgebra I y que ya reapareció en el capítulo previo.

De alguna forma, los subgrupos normales son los únicos con los que es posible "descomponer" un grupo sin perder su estructura. Explícitamente, si H es un subgrupo de G, el conjunto cociente G/H hereda la estructura de grupo si y sólo si H es un subgrupo normal de G. El cardinal de G/H es $|H|$ veces menor que el de G, y G/H se obtiene agrupando de cierta forma los elementos de G de $|H|$ en $|H|$. Con esta idea de descomposición, los "grupos primos" serían los siguientes:

Definición: Se dice que un grupo G es *simple* si no tiene subgrupos normales propios (distintos del trivial y de él mismo).

Y la división sucesiva de un número con cocientes primos, responde a:

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

$$\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 \cdots \subsetneqq G_n = G$$

es una *serie de composición* si $G_{i-1} \triangleleft G_i$ y G_i/G_{i-1} es un grupo simple para $0 < i \leq n$.

Al igual que todo número factoriza en primos, cualquier grupo finito tiene una serie de composición, aunque ello no esté claro en absoluto sin recordar vívidamente el

curso de Álgebra I. Aún más, el llamado teorema de Jordan-Hölder mimetiza el teorema fundamental de la aritmética afirmando que la serie de composición es única en cierto sentido salvo reordenaciones de los factores simples G_{i+1}/G_i. Continuando con esta analogía, entre los grupos simples finitos hay una especie de "superprimos" que ni siquiera admiten subgrupos propios. No es difícil probar que los grupos aditivos $\mathbb{Z}_p$ son los únicos con esta propiedad. La definición que perseguimos es la de grupo que factoriza en "superprimos".

Definición: Se dice que un grupo finito, G, es *soluble* si tiene una serie de composición

$$\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 \cdots \subsetneqq G_n = G$$

tal que $G_{i+1}/G_i \cong \mathbb{Z}_{p_i}$, con p_i primo, $0 \leq i < n$.

Finalmente, llegamos al resultado que necesitaremos en la próxima sección.

Teorema 4.1.1 *Sea G un grupo finito y $H \triangleleft G$, entonces G es soluble si y sólo si G/H y H lo son. Además todo subgrupo de un grupo soluble es soluble.*

Nuestra experiencia nos dice que es singular que un subgrupo sea normal y que los $\mathbb{Z}_p$ son ejemplos muy particulares de grupos, lo cual sugiere que hay pocos grupos solubles, sin embargo hay que esperar nada menos que hasta orden sesenta para poder encontrar un grupo no soluble. De hecho hay varios resultados que permiten obtener muchos grupos solubles. El más sorprendente de ellos es el teorema de Feit-Thompson que afirma que todo grupo de orden impar es soluble. La longitud de su demostración (más de doscientas páginas) puso en cuestión qué debía considerarse una prueba matemática, y todavía estaba por llegar la clasificación de los grupos simples finitos (véanse los comentarios en [Ga] §25), cuya prueba en conjunto ocuparía muchos miles de páginas. (De nuevo el escepticismo de Hume planea desasosegante sobre nuestras cabezas: "No existe algebrista ni matemático tan experto en su ciencia que llegue a otorgar plena confianza a una verdad nada más descubrirla, y que no la considere sino como mera probabilidad. Cada vez que revisa sus pruebas, aumenta su confianza; la aprobación de sus amigos la aumenta aún más, pero es la aprobación universal y los aplausos del mundo ilustrado lo que la lleva a su más alto grado").

Sirvan las razones aducidas para excusar que en los siguientes ejemplos sólo aparezcan grupos solubles, reservando la aparición de nuestro flamante grupo no soluble de 60 elementos para una ocasión en que sea más espectacular, en relación con la solubilidad por radicales.

Ejemplo. Una serie de composición para $\mathbb{Z}_{12}$ es:

$$\{0\} \subset \{0, 6\} \subset \{0, 3, 6, 9\} \subset \mathbb{Z}_{12}.$$

Ejemplo. La cadena de subgrupos

$$\{0\} \subset \{0, 4, 8\} \subset \{0, 2, 4, 6, 8, 10\} \subset \mathbb{Z}_{12}$$

es otra serie de composición para $\mathbb{Z}_{12}$.

Ejemplo. El grupo S_3 es soluble porque se tiene la serie de composición:

$$\{\mathrm{Id}\} \subset A_3 = \langle (1,2,3) \rangle \subset S_3,$$

con cocientes isomorfos a $\mathbb{Z}_3$ y $\mathbb{Z}_2$.

Ejemplo. El grupo de movimientos del plano que dejan invariante un cuadrado, $D_8 = \langle \sigma, \tau \rangle$ con τ la simetría por una diagonal y σ un giro de 90^o alrededor del centro, es soluble porque se tiene la serie de composición:

$$\{\mathrm{Id}\} \subset \langle \sigma^2 \rangle \subset \langle \sigma \rangle \subset D_8,$$

con cocientes isomorfos a $\mathbb{Z}_2$.

Ejemplo. Si Q es el grupo de cuaterniones $\{\pm 1, \pm i, \pm j, \pm k\}$ con $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$; entonces $G = \mathbb{Z}_6 \times Q$ es soluble porque

$$\{0\} \times \{1\} \subset \{0,2\} \times \{1\} \subset \mathbb{Z}_6 \times \{1\} \subset \mathbb{Z}_6 \times \{\pm 1\} \subset \mathbb{Z}_6 \times \{\pm 1, \pm i\} \subset \mathbb{Z}_6 \times Q$$

es una serie de composición con cocientes isomorfos a $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2$, $\mathbb{Z}_2$ y $\mathbb{Z}_2$.

Ejemplo. El grupo $\mathbb{Z}_3 \times Q$ es soluble, porque con el monomorfismo $\mathbb{Z}_3 \longrightarrow \mathbb{Z}_6$, $n \mapsto 2n$, se puede considerar un subgrupo del grupo del ejemplo anterior.

Ejemplo. Todo grupo abeliano finito es soluble.

Aunque no sea la manera más elemental de probar esta afirmación, se deduce por inducción del Teorema 4.1.1 tomando como H el grupo generado por cualquier elemento de orden primo.

Ejemplo. Si G es un grupo de orden 210 con un subgrupo normal soluble H de orden 30, necesariamente G es soluble por el Teorema 4.1.1, ya que G/H tiene orden 7 y por tanto es isomorfo a $\mathbb{Z}_7$.

Aquí concluye la versión utilitaria de esta sección y comienza la cultural, que consistirá en una demostración del Teorema 4.1.1, que con la excusa de ser autocontenida, propiciará algunas paradas en la teoría de grupos para contemplar las vistas.

Lo primero que necesitamos es cierta maestría manipulando subgrupos normales. Una fábrica de subgrupos normales que además permite interpretar los cocientes es el siguiente resultado, llamado a veces teorema del homomorfismo, del isomorfismo o primer teorema de isomorfía.

Teorema 4.1.2 *Si $f : G \longrightarrow G'$ es un homomorfismo de grupos, entonces* Ker f *es un subgrupo normal de G y $G/\mathrm{Ker}\ f \cong \mathrm{Im}\ f$.*

Sea cual sea el alias por el que lo conozcamos, fue parte fundamental del curso de Álgebra I, y quien no sea capaz de recuperar su prueba debe ser castigado a forzar la vista.

Demostración: Si $g \in G$ y $x \in \text{Ker } f$, se tiene $f(g^{-1}xg) = f(g^{-1})$ e $f(g) = e$ por tanto $g^{-1}xg \in \text{Ker } f$ y $\text{Ker } f \triangleleft G$.

La aplicación $\phi : G/\text{Ker } f \longrightarrow \text{Im } f$ dada por $\phi(g\text{Ker } f) = f(g)$ está bien definida ($g\text{Ker } f$ representa la clase de g) porque si $g_1\text{Ker } f = g_2\text{Ker } f$ entonces $g_1 = g_2x$ con $x \in \text{Ker } f$ y $f(g_1) = f(g_2)$. Es obviamente sobreyectiva, y es inyectiva porque $f(g) = e \Leftrightarrow g \in \text{Ker } f \Leftrightarrow g\text{Ker } f = \text{Ker } f$. Además es homomorfismo ya que $g_1\text{Ker } f \cdot g_2\text{Ker } f = g_1g_2\text{Ker } f$ (lo que se sigue de $\text{Ker } f \triangleleft G$). Por consiguiente ϕ es un isomorfismo. □

Había también en Álgebra I algunas consecuencias que permitían establecer algunos otros isomorfismos, y junto con el resultado anterior recibían el nombre genérico de *teoremas de isomorfía*, aunque los resultados concretos que se recogen bajo esta denominación cambian en función de los autores (compárese [Cl], [Do-He] y [Rotm]).

Corolario 4.1.3 (Teoremas de isomorfía) *Sea G un grupo y H un subgrupo normal.*

a) Si N es subgrupo de H y $N \triangleleft G$, entonces $H/N \triangleleft G/N$ y

$$(G/N)/(H/N) \cong G/H.$$

b) Si N es un subgrupo de G entonces $NH = \{nh \ : \ n \in N, \ h \in H\}$ es un grupo, $H \triangleleft NH$, $NH = HN$ y

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

Demostración: Consideramos las funciones:

$$f_1 : \begin{array}{ccc} G/N & \longrightarrow & G/H \\ gN & \longmapsto & gH \end{array} \quad \text{y} \quad f_2 : \begin{array}{ccc} N & \longrightarrow & NH/H \\ g & \longmapsto & gH \end{array}$$

Como $N \subset H$, f_1 está bien definida. Es un homomorfismo porque $g_1H \cdot g_2H = g_1g_2H$, al ser $H \triangleleft G$. Su núcleo es $\text{Ker } f = \{gN \ : \ g \in H\} = H/N$ y evidentemente $\text{Im } f_1 = G/H$. Por tanto *a)* es una consecuencia del teorema anterior.

Para *b)*, nótese primero que $H \triangleleft G$ implica que para cada $n \in N$ y $h \in H$ existe $h' \in H$ tal que $nh = h'n$. Por tanto $(nh)^{-1} = (h'n)^{-1} = n^{-1}(h')^{-1} \in NH$, y se sigue que NH es un grupo y que coincide con HN ($nh \in NH \Rightarrow (nh)^{-1} \in HN$). Además es subgrupo de G y de aquí $H \triangleleft NH$. La prueba de que f_2 es epimorfismo es similar a la de f_1, y *b)* se deduce del teorema anterior notando que $\text{Ker } f_2 = \{g \in N \ : \ gH = H\} = \{g \in N \ : \ g \in H\}$. □

Vayamos ahora a la demostración del resultado principal de esta sección.

Demostración del Teorema 4.1.1: En primer lugar veamos que un subgrupo H de un grupo soluble G es también soluble. Para ello transformemos la serie de composición de G

$$\{e\} = G_0 \subset G_1 \subset G_2 \cdots \subset G_n = G \qquad \text{con} \qquad G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$$

en una cadena de subgrupos normales que acaba en H:

$$\{e\} = G_0 \cap H \subset G_1 \cap H \subset G_2 \cap H \cdots \subset G_n \cap H = H.$$

Por el Corolario 4.1.3 *b)*, se cumple:

$$(G_i \cap H) \cdot G_{i-1}/G_{i-1} \cong (G_i \cap H)/(G_{i-1} \cap H).$$

Como $(G_i \cap H) \cdot G_{i-1}$ es un subgrupo de G_i, el primer cociente es un subgrupo de $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$, y por tanto isomorfo al grupo trivial $\{e\}$ o a $\mathbb{Z}_{p_i}$. De este modo (4.1) se transforma en una serie de composición de un grupo soluble sin más que eliminar los subgrupos repetidos en la cadena.

Una vez hecho esto, veamos que G es soluble si y sólo si G/H y H son solubles.

$\Rightarrow$) Acabamos de probar que H es soluble. La prueba de que G/H es soluble sigue líneas parecidas. A partir de la serie de composición de G creamos la cadena de subgrupos:

$$\{e\} = G_0H/H \subset G_1H/H \subset G_2H/H \cdots \subset G_nH/H = G/H,$$

lo cual tiene sentido por la primera parte del Corolario 4.1.3 *b*). Además por el apartado *a*) y después por el *b*) con $N = G_i$,

$$(G_iH/H)\big/(G_{i-1}H/H) \cong G_iH/G_{i-1}H \cong G_i/\big(G_i \cap (G_{i-1}H)\big).$$

Como $G_{i-1} \lhd G_i \cap (G_{i-1}H)$, por el Corolario 4.1.3 *a*) el último cociente es isomorfo al cociente de $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$ por $\big(G_i \cap (G_{i-1}H)\big)/G_{i-1}$. De nuevo las posibilidades son el grupo trivial y $\mathbb{Z}_{p_i}$ y la cadena de subgrupos se transforma en la serie de composición de un grupo soluble sin más que tachar los eslabones repetidos.

$\Leftarrow$) De alguna forma lo que hay que hacer es "pegar" las series de composición de H y G/H. Digamos que éstas son:

$$\{e\} = H_0 \subset H_1 \cdots \subset H_n = H, \quad \{e\} = G_0/H \subset G_1/H \cdots \subset G_m/H = G/H,$$

(nótese que cualquier subgrupo de G/H es de la forma N/H con $N \subset G$) donde $H_i/H_{i-1} \cong \mathbb{Z}_{p_i}$ y $(G_i/H)\big/(G_{i-1}/H) \cong \mathbb{Z}_{p_i'}$. Consideremos ahora

$$\{e\} = H_0 \subset H_1 \subset H_2 \cdots \subset H_n = G_0 \subset G_1 \subset G_2 \cdots \subset G_m = G.$$

Ésta es la serie de composición de un grupo soluble, ya que aplicando el Corolario 4.1.3, $G_i/G_{i-1} \cong (G_i/H)\big/(G_{i-1}/H) \cong \mathbb{Z}_{p_i'}$. □

Para terminar esta sección daremos oportunidad de conocer el teorema de Jordan-Hölder a los lectores más interesados. Como ya hemos sugerido, en un paralelismo con el teorema fundamental de la aritmética, los cocientes G_i/G_{i-1} en una serie de composición corresponderían a los primos, mientras que los subgrupos G_i serían productos parciales. Si la analogía es adecuada, los G_i no están unívocamente determinados y por ello la serie de composición de un grupo no es única en general (como quedó reflejado en los ejemplos), sin embargo los cocientes G_i/G_{i-1} deberían ser los mismos (isomorfos) salvo reordenaciones en las diferentes series de composición.

Teorema 4.1.4 (Jordan-Hölder) *Si tenemos dos series de composición para G*

$$\{e\} = G_0 \subset G_1 \subset G_2 \cdots \subset G_n = G, \qquad \{e\} = H_0 \subset H_1 \subset H_2 \cdots \subset H_m = G$$

entonces $n = m$ y los cocientes G_i/G_{i-1} y H_j/H_{j-1} son isomorfos pero quizá apareciendo en distinto orden.

Demostración: Para $0 \leq j < n$ y $0 \leq k < m$, sea $\widetilde{G}_{jm+k} = G_j(G_{j+1} \cap H_k)$. Este conjunto es un grupo por el Corolario 4.1.3 *b*) con $H = G_j$, $N = G_{j+1} \cap H_k$ y $G = G_{j+1}$. Además $G_j(G_{j+1} \cap H_k) \triangleleft G_j(G_{j+1} \cap H_{k+1})$ porque $x \in G_j$, $y \in G_{j+1} \cap H_{k+1}$ implica

$$(xy)^{-1}G_j(G_{j+1} \cap H_k)xy = (y^{-1}x^{-1}G_jy)(y^{-1}(G_{j+1} \cap H_k)y)(y^{-1}xy) \in G_j(G_{j+1} \cap H_k)G_j$$

y $G_j(G_{j+1} \cap H_k)G_j = G_j(G_{j+1} \cap H_k)$ (por el Corolario 4.1.3, $HN = NH$). La igualdad $\widetilde{G}_{jm+k+1} = G_j(G_{j+1} \cap H_{k+1})$ se da incluso si $k+1 = m$, definiendo $\widetilde{G}_{nm} = G$, con lo cual hemos probado que se tiene la cadena de subgrupos normales

$$\{e\} = \widetilde{G}_0 \triangleleft \widetilde{G}_1 \triangleleft \widetilde{G}_2 \triangleleft \ldots \widetilde{G}_{nm-1} \triangleleft \widetilde{G}_{nm} = G. \tag{4.1}$$

De la misma forma, definiendo $\widetilde{H}_{km+j} = H_k(H_{k+1} \cap G_j)$ para $0 \leq j < n$, $0 \leq k < m$, y $\widetilde{H}_{mn} = G$, se tiene

$$\{e\} = \widetilde{H}_0 \triangleleft \widetilde{H}_1 \triangleleft \widetilde{H}_2 \triangleleft \ldots \widetilde{H}_{mn-1} \triangleleft \widetilde{H}_{mn} = G. \tag{4.2}$$

Es evidente que $\widetilde{G}_{jm} = G_j$. De hecho todos los $\widetilde{G}_r$ con $jm < r < (j+1)m$ son iguales a G_j o a G_{j+1}, ya que tomando r el máximo valor en este rango con $\widetilde{G}_r \subsetneqq \widetilde{G}_{(j+1)m} = G_{j+1}$ se tiene por el Corolario 4.1.3 *a*) que $G_{j+1}/\widetilde{G}_r$ es un subgrupo normal de $\widetilde{G}_{(j+1)m}/\widetilde{G}_{jm} = G_{j+1}/G_j$, que es simple, por lo que necesariamente $\widetilde{G}_r = G_j$.

Lo mismo puede aplicarse a los $\widetilde{H}_s$ y H_k.

En definitiva, (4.1) y(4.2) coinciden con las series de composición del enunciado salvo que algunos grupos están repetidos. Así pues, para cada $0 \leq j < n$ existe un único r con $G_j = \widetilde{G}_r$, $G_{j+1} = \widetilde{G}_{r+1}$, y recíprocamente si $\widetilde{H}_s \neq \widetilde{H}_{s+1}$, se tiene $\widetilde{H}_s = H_k$, $\widetilde{H}_{s+1} = H_{k+1}$, para cierto k. Por tanto el resultado del teorema se deduce si existe una biyección B en $\{0, 1, 2, \ldots, nm-1\}$ tal que $\widetilde{G}_{r+1}/\widetilde{G}_r \cong \widetilde{H}_{B(r)+1}/\widetilde{H}_{B(r)}$. Es fácil comprobar que, fijados m y n, $B(jm+k) = kn+j$, $0 \leq j < n$, $0 \leq k < m$, define una biyección en el conjunto indicado y por tanto es suficiente probar:

$$\widetilde{G}_{jm+k+1}/\widetilde{G}_{jm+k} \cong \widetilde{H}_{kn+j+1}/\widetilde{H}_{kn+j} \qquad \text{para} \quad 0 \leq j < n,\ 0 \leq k < m. \tag{4.3}$$

El primer miembro de (4.3) es HN/H con $H = G_j(G_{j+1} \cap H_k)$ y $N = G_{j+1} \cap H_{k+1}$, y por el Corolario 4.1.3 *b*) se tiene (nótese que $H = \widetilde{G}_{jm+k} \triangleleft \widetilde{G}_{jm+k+1}$)

$$\widetilde{G}_{jm+k+1}/\widetilde{G}_{jm+k} \cong N/(N \cap H) = \frac{G_{j+1} \cap H_{k+1}}{(G_{j+1} \cap H_{k+1}) \cap (G_j(G_{j+1} \cap H_k))}.$$

Es fácil ver que $(G_{j+1} \cap H_{k+1}) \cap (G_j(G_{j+1} \cap H_k)) \supset (G_j \cap H_{k+1}) \cdot (G_{j+1} \cap H_k)$. También la inclusión contraria es cierta, porque si $xy \in G_{j+1} \cap H_{k+1}$ con $x \in G_j$, $y \in G_{j+1} \cap H_k$, entonces $x = (xy)y^{-1} \in H_{k+1}$. En suma, el primer miembro de (4.3) es:

$$\widetilde{G}_{jm+k+1}/\widetilde{G}_{jm+k} \cong \frac{G_{j+1} \cap H_{k+1}}{(G_j \cap H_{k+1}) \cdot (G_{j+1} \cap H_k)}.$$

Y de la misma forma, se tiene que el segundo miembro de (4.3) es

$$\widetilde{H}_{kn+j+1}/\widetilde{G}_{kn+j} \cong \frac{H_{k+1} \cap G_{j+1}}{(H_k \cap G_{j+1}) \cdot (H_{k+1} \cap G_j)}.$$

Al ser $H_k \cap G_{j+1} \triangleleft H_{k+1} \cap G_{j+1}$, se sigue que los dos factores en el último "denominador" se pueden intercambiar, concluyéndose la prueba de (4.3). □

4.2. El teorema de Galois

Los polinomios $P \in \mathbb{Q}[x]$ que aparecían en los ejemplos del capítulo anterior para generar cuerpos de descomposición siempre tenían raíces que se escribían en términos

de radicales sencillos, lo que es natural porque en otro caso no habríamos podido aplicar nuestra algoritmia para calcular grupos de Galois. Por otro lado, a primera vista es razonable tratar de invertir cualquier función polinómica con operaciones elementales y radicales ya que tales funciones se construyen operando los coeficientes con potencias de la variable. Sin embargo, más de doscientos años después de que G. Cardano publicase (en su *Ars Magna* de 1545) las soluciones con radicales de las ecuaciones generales de tercer y cuarto grado, había cierta opinión entre la comunidad matemática de que tales soluciones no existían para grados superiores. Finalmente, N.H. Abel demostró en 1824 su famoso teorema afirmando la imposibilidad de resolver la ecuación general de quinto grado con radicales (años antes P. Ruffini había obtenido una prueba poco rigurosa y con lagunas, que alcanzó escasa difusión).

Aquí invertiremos el orden histórico deduciendo el teorema de Abel (cuya versión clásica pospondremos hasta la sección siguiente) a partir del bien conocido teorema de Galois, la estrella de esta sección, que da una condición necesaria y suficiente (de poca utilidad práctica pero de gran atractivo teórico) para la solubilidad por radicales.

Antes de nada veamos un par de definiciones. La primera concreta el significado de que los elementos de una extensión se puedan expresar con radicales, mientras que la segunda es puramente notacional.

Definición: Se dice que una extensión finita L/K es *radical* si existe una cadena de subcuerpos:

$$K = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n$$

con $L_n \supset L$, tales que para cada $0 < j \leq n$, $L_j = L_{j-1}(\alpha_j)$ donde $\alpha_j^{m_j} \in L_{j-1}$ y $m_j \in \mathbb{Z}^+$.

Nota: Esto es, cada subcuerpo se obtiene a partir del anterior añadiendo la raíz m_j-ésima de algún elemento. Algunos autores [St] piden que L_n coincida exactamente con L, pero ello no está inmediatamente de acuerdo con nuestra intuición. Por ejemplo, no sería evidente que $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})/\mathbb{Q}$ es radical.

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.

Ejemplo. La extensión $\mathbb{Q}(\sqrt{3}, \sqrt{\sqrt[3]{5}+\sqrt[3]{2}})/\mathbb{Q}$ es radical, como muestra la cadena de subcuerpos:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{5}, \sqrt[3]{2}) \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{5}, \sqrt[3]{2}, \sqrt{\sqrt[3]{5}+\sqrt[3]{2}}).$$

Ejemplo. El polinomio $P = x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 3 \in \mathbb{Q}[x]$ es soluble por radicales porque podemos escribir $P = (x-1)^5 - 2$, por tanto todas las raíces son $1+\zeta^k\sqrt[5]{2}$ con $\zeta = e^{2\pi i/5}$, $0 \leq k < 5$. El cuerpo de descomposición es $L = \mathbb{Q}(\zeta, \sqrt[5]{2})$ y $L/\mathbb{Q}$ es evidentemente radical porque ζ es una raíz quinta de la unidad. Más explícitamente $\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta, \sqrt[5]{2}) = L$ con $\zeta^5 = 1 \in \mathbb{Q}$ y $(\sqrt[5]{2})^5 = 5 \in \mathbb{Q}(\zeta)$.

Una simplificación que será útil más adelante es que en la definición de extensión radical siempre se puede suponer que L_n/K es normal. La idea es sencillamente añadir todas las raíces de los polinomios mínimos de los generadores de la extensión.

Lema 4.2.1 *Sea L/K radical. Siempre se puede modificar la cadena de subcuerpos de la definición a*

$$K = M_0 \subset M_1 \subset \cdots \subset M_N$$

con propiedades análogas de forma que $M_N \supset L_n$ y M_N/K sea normal.

Demostración: Procedemos por inducción en n, la longitud de la cadena inicial. Si $n = 1$ basta añadir sucesivamente las raíces de $x^{m_1} - \alpha_1^{m_1}$ para obtener su cuerpo de descomposición sobre K y por tanto una extensión normal.

Si se cumple para $n-1$, entonces $K = M_0 \subset M_1 \subset \cdots \subset M_N$ con $M_N \supset L_{n-1}$ donde M_N/K es normal, digamos que M_N es el cuerpo de descomposición de $P \in K[x]$. Sea Q el polinomio mínimo de α_n sobre K, sean $\beta_1 = \alpha_n$, β_2,... β_k sus raíces y sea M el cuerpo de descomposición de $PQ \in K[x]$. Por el Corolario 3.2.6, para cada $1 \leq i \leq k$ existe $\sigma_i \in \mathcal{G}(M/K)$ tal que $\sigma_i(\alpha_n) = \beta_i$. Como $\alpha_n^{m_n} \in L_{n-1} \subset M_N$ y M_N es normal, $\sigma_i(\alpha_n^{m_n}) = \beta_i^{m_n} \in M_N$. Por tanto definiendo $M_{N+i} = M_{N+i-1}(\beta_i)$ para $1 \leq i \leq k$, se tiene la extensión buscada de subcuerpos, $L_{n-1} \subset M_N \subset M_{N+1} \subset \cdots \subset M_{N+k}$ con $M = M_{N+k} \supset L_n = L_{n-1}(\alpha_n)$. □

En la apasionante historia (véase [Kl]) que va desde la solución de las ecuaciones de tercer y cuarto grado al teorema de Galois, hay un punto medio crucial que fue la introducción de las llamadas *resolventes de Lagrange*. Para ilustrar su significado, nótese por ejemplo que la función $F(x, y, z) = (x + \omega y + \omega^2 z)^3$, $\omega = e^{2\pi i/3}$, es invariante por las permutaciones circulares de x, y, z; mientras que su raíz cúbica $x + \omega y + \omega^2 z$ no queda invariante por ninguna permutación de las variables. Este truco, convenientemente generalizado, permitió en 1770 a J.L. Lagrange (y poco antes a A.T. Vandermonde, véase [Ed]) unificar las complicadas soluciones de las ecuaciones de tercer y cuarto grado, a la vez que atisbar que las de quinto grado dan lugar a un obstáculo insalvable. Con el lenguaje actual, permite asociar un radical a cada cociente cíclico del grupo de Galois.

En el próximo resultado aplicaremos el truco de Lagrange para probar que cada extensión de Galois cuyo grupo de galois sea isomorfo a $\mathbb{Z}_p$ se obtiene añadiendo un radical de índice p. De ello a probar que grupo de Galois soluble implica polinomio soluble por radicales, sólo hay un paso, aunque entorpecido por ciertas incomodidades técnicas relacionadas con las raíces de la unidad.

Proposición 4.2.2 *Sea L/K una extensión de Galois con $\mathcal{G}(L/K) \cong \mathbb{Z}_p$ con p primo. Supongamos que K contiene a las raíces p-ésimas de la unidad (el cuerpo de descomposición de $x^p - 1$) y $p \neq char(K)$, entonces $L = K(\alpha)$ con $\alpha^p \in K$.*

Demostración: Dada una ráiz ζ de $x^p - 1$ y $\phi \in \mathcal{G}(L/K)$, definimos la *resolvente de Lagrange* como la aplicación $L \longrightarrow L$ dada por

$$\mathcal{L}(\zeta, \phi) = \mathrm{Id} + \zeta\phi + \zeta^2\phi^2 + \cdots + \zeta^{p-1}\phi^{p-1}$$

donde ϕ^k indica la composición del automorfismo ϕ consigo mismo k veces. Elijamos $\zeta \neq 1$ (siempre existe porque $\mathrm{char}(K) \neq p$ implica que no todas las raíces son iguales) y ϕ generando $\mathcal{G}(L/K)$. Sea β tal que $L = K(\beta)$ (basta tomar $\beta \in L - K$, porque el grado

$[L : K]$ es primo) y $\alpha = \mathcal{L}(\zeta, \phi)(\beta)$. Por la independencia lineal de los automorfismos (Lema 3.2.3) $\alpha \neq 0$, y $\phi(\alpha) = \zeta^{p-1}\alpha = \zeta^{-1}\alpha$ que es distinto de α (porque $\zeta \neq 1$). Así pues $K \subsetneqq K(\alpha) \subset L$ lo que implica $L = K(\alpha)$, (como antes, porque $[L : K]$ es primo). Además $\phi(\alpha^p) = (\phi(\alpha))^p = (\zeta^{-1}\alpha)^p = \alpha^p$ implica $\alpha^p \in K$. □

Vayamos ahora sin más dilación al resultado principal de este capítulo y de alguna forma la culminación del curso. Para evitar hipótesis tan enrevesadas como las de la proposición anterior es obligado restringirse al caso de característica cero, y poner unos cuantos parches en los sótanos de la demostración para contemplar el caso en que no queramos añadir de antemano las raíces de la unidad. Esos parches se pueden obviar en una primera lectura.

Teorema 4.2.3 (Teorema de Galois) *Sea $P \in K[x]$ con $char(K) = 0$ y sea L su cuerpo de descomposición, entonces P es soluble por radicales si y sólo si $\mathcal{G}(L/K)$ es un grupo soluble.*

Demostración:

$\Rightarrow$) Añadiendo subcuerpos intermedios siempre se pueden escoger los m_j primos en la definición de extensión radical (ya que $\sqrt[p]{\sqrt[q]{\ }} = \sqrt[pq]{\ }$), y así lo haremos en esta demostración. Momentáneamente supondremos también que K contiene todas las raíces m_j-ésimas de la unidad, esto es, que $(x^{m_1} - 1)(x^{m_2} - 1) \cdots (x^{m_n} - 1)$ se descompone en factores lineales en $K[x]$. Más adelante veremos cómo eliminar esta hipótesis.

De acuerdo con el Lema 4.2.1, en la definición de extensión radical se puede suponer que L_n/K es normal. Como también es finita y separable ($\mathrm{char}(K) = 0$), el teorema fundamental de la teoría de Galois permite asociar unívocamente a la cadena se subcuerpos una cadena de subgrupos:

$$\{\mathrm{Id}\} = \mathcal{G}(L_n/L_n) \subset \mathcal{G}(L_n/L_{n-1}) \subset \cdots \subset \mathcal{G}(L_n/L_0) = \mathcal{G}(L_n/K). \tag{4.4}$$

Para cada $1 \leq j \leq n$ la extensión L_j/L_{j-1} es normal ya que L_j es el cuerpo de descomposición de $Q_j = x^{m_j} - \alpha^{m_j} \in L_{j-1}[x]$ porque $L_j = L_{j-1}(\alpha_j)$ y cualquier raíz de Q_j es α_j por una raíz m_j-ésima de la unidad. Por ello, si $\alpha_j \notin L_{j-1}$, o equivalentemente si $L_{j-1} \neq L_j$, lo cual siempre podemos dar por hecho, el polinomio Q_j es irreducible. El teorema fundamental de la teoría de Galois asegura que $\mathcal{G}(L_n/L_j) \triangleleft \mathcal{G}(L_n/L_{j-1})$ y $\mathcal{G}(L_n/L_{j-1})/\mathcal{G}(L_n/L_j) \cong \mathcal{G}(L_j/L_{j-1})$ que tiene orden $[L_j : L_{j-1}] = \partial Q_j = m_j$, que es primo, y por tanto isomorfo a $\mathbb{Z}_{m_j}$, en definitiva, (4.4) es la serie de composición de un grupo soluble. Por el Teorema 4.1.1, como $\mathcal{G}(L_n/L)$ es un subgrupo de $\mathcal{G}(L_n/K)$, es soluble, y $\mathcal{G}(L/K) \cong \mathcal{G}(L_n/K)/\mathcal{G}(L_n/L)$ también lo es.

Veamos ahora el caso el caso en que K no contiene a todas las raíces m_j-ésimas de la unidad. Si $\zeta_j \neq 1$ es raíz de $x^{m_j} - 1$, todas las raíces son $1, \zeta_j, \zeta_j^2, \ldots, \zeta_j^{m_j-1}$ (son distintas porque $\zeta_j^a = 1$, $0 < a < m$ implicaría $\zeta_j = 1$ elevando al inverso de a módulo p). Entonces el cuerpo de descomposición de $(x^{m_1} - 1)(x^{m_2} - 1) \cdots (x^{m_n} - 1) \in K[x]$ es $\widetilde{K} = K(\zeta_1, \zeta_2, \ldots, \zeta_n)$ y cada $\sigma \in \mathcal{G}(\widetilde{K}/K)$ actúa como $\sigma(\zeta_j) = \zeta_j^{r_j}$, por lo que $\mathcal{G}(\widetilde{K}/K)$ es abeliano, en particular soluble. Si $\widetilde{L} \supset L$ es el cuerpo de descomposición de P sobre $\widetilde{K}$, por la demostración anterior $\mathcal{G}(\widetilde{L}/\widetilde{K})$ es soluble. Por el Teorema 4.1.1 con $G = \mathcal{G}(\widetilde{L}/K)$,

$H = \mathcal{G}(\widetilde{L}/\widetilde{K})$ y $G/H \cong \mathcal{G}(\widetilde{K}/K)$, se tiene que G es soluble. Y como $\mathcal{G}(\widetilde{L}/L)$ es un subgrupo normal de G, $\mathcal{G}(L/K) \cong G/\mathcal{G}(\widetilde{L}/L)$ también es soluble.

$\Leftarrow$) Si $\mathcal{G}(L/K)$ es soluble, por la correspondencia entre subgrupos y subcuerpos podemos pasar de la serie de composición a una cadena de subcuerpos:

$$K = G'_n \subset G'_{n-1} \subset \cdots \subset G'_1 \subset G'_0 = L,$$

y por el teorema fundamental de la teoría de Galois, G'_{i-1}/G'_i es una extensión de Galois porque $\mathcal{G}(L/G'_{i-1}) = G_{i-1} \triangleleft G_i = \mathcal{G}(L/G'_i)$ y su grado es primo, p_i. En analogía con lo hecho anteriormente, supongamos primero que disponemos de todas las raíces p_i-ésimas de la unidad en G'_i, entonces $G'_{i-1} = G_i(\alpha)$ con $\alpha^p \in G'_i$ por la Proposición 4.2.2 y L/K sería una extensión radical.

Si no se cumpliera nuestra suposición, digamos que $\zeta \neq 1$ con $\zeta^{p_i} = 1$ no está en G_i, consideramos la extensión $G'_{i-1}(\zeta)/G'_i(\zeta)$ que es normal (si G'_{i-1} es el cuerpo de descomposición de $Q \in G'_i[x]$, entonces $G'_{i-1}(\zeta)$ lo es de $(x^{p_i}-1)Q$). Sea el homomorfismo

$$\begin{array}{rccc} \phi : \mathcal{G}\big(G'_{i-1}(\zeta)/G'_i(\zeta)\big) & \longrightarrow & \mathcal{G}(G'_{i-1}/G'_i) \\ \sigma & \longmapsto & \sigma|_{G'_{i-1}} \end{array}$$

Se cumple $\operatorname{Ker}\phi = \{e\}$ porque si σ fija los elementos de G'_{i-1} y los de $G'_i(\zeta)$, es la identidad en $G'_{i-1}(\zeta)$. Por consiguiente ϕ es un isomorfismo y se cumple $\mathcal{G}\big(G'_{i-1}(\zeta)/G'_i(\zeta)\big) \cong \mathbb{Z}_{p_i}$ y podemos aplicar la Proposición 4.2.2 para concluir que $G'_{i-1}(\zeta)/G'_i(\zeta)$ es radical y por tanto G'_{i-1}/G'_i también lo es. □

Con el teorema de Galois a nuestra disposición podemos deducir que es posible resolver con radicales todas las ecuaciones hasta grado cuatro. De hecho, como la demostración es constructiva, en principio podríamos elaborar fórmulas explícitas para resolverlas. Volveremos sobre este punto en la próxima sección.

Corolario 4.2.4 *Sea $P \in K[x]$ con $char(K) = 0$. Si $\partial P \leq 4$ entonces P es soluble por radicales.*

Demostración: Sabemos que el grupo de Galois permuta las raíces, con lo cual es isomorfo a un subgrupo de $S_m \subset S_4$ donde m es el número de raíces distintas. Por tanto, gracias a la segunda parte del Teorema 4.1.1, basta probar que S_4 es soluble. Para ello consideramos la serie de composición:

$$\{\mathrm{Id}\} \subset \langle\sigma\rangle \subset \langle\sigma,\tau\rangle \subset A_4 \subset S_4$$

con $\sigma = (1,2)(3,4)$, $\tau = (1,3)(2,4)$. Nótese que A_4 está generado por σ, τ y $\lambda = (1,2,3)$ (no es necesario embarcarse en muchos cálculos, ya que los cuatro elementos de $\langle\sigma,\tau\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ multiplicados por Id, λ y λ^2 dan lugar a 12 elementos distintos y por tanto necesariamente a todo A_4) y $\lambda^{-1}\sigma\lambda = \tau$, $\lambda^{-1}\tau\lambda = \sigma\tau$ implican $\langle\sigma,\tau\rangle \triangleleft A_4$. Es mucho más sencillo comprobar que el resto de los subgrupos son normales, por ejemplo viendo que son de índice 2. Los cocientes respectivos son de órdenes primos 2, 2, 3 y 2, con lo cual S_4 es soluble. □

En el otro sentido, para demostrar que no hay resolubilidad por radicales en general para grados superiores, "sólo" hay que encontrar un cuerpo de descomposición de un polinomio de quinto grado cuyo grupo de Galois no sea soluble. A nuestro nivel esto no parece en absoluto sencillo porque no conocemos todavía ningún grupo no soluble y no está claro cómo hallar siquiera el cuerpo de descomposición si no podemos emplear radicales. El primer problema lo resolveremos con un lema de teoría de grupos que nos hemos estado reservando, mientras que para el segundo podremos evitar describir explícitamente el cuerpo de descomposición empleando un ingenioso regate teórico.

Lema 4.2.5 *El grupo A_5 de permutaciones pares de cinco elementos es simple, esto es, no tiene subgrupos normales propios.*

Observación: Evidentemente de este lema se deduce que A_5 no es soluble. El orden de A_5 es $|S_5|/2 = 5!/2 = 60$ y con técnicas de teoría de grupos se puede probar (véanse los ejercicios de [Cl] §59) que todo grupo de orden menor es soluble. En este sentido, A_5 es el primer grupo no soluble.

La demostración del lema es puramente combinatoria y con modificaciones (véase [Cl]) serviría para obtener que A_n es simple para $n \geq 5$.

Demostración: Sea $\{\mathrm{Id}\} \neq H \lhd A_5$. Todo lo que hay que demostrar es que se debe cumplir $H = A_5$. Si $\mathrm{Id} \neq \alpha \in H$, al descomponer α en ciclos disjuntos se tiene que α es un 3-ciclo, un 5-ciclo o un producto de dos trasposiciones disjuntas. En estos dos últimos casos podemos suponer, quizá renumerando los objetos que se permutan, que α es $\alpha_1 = (1,2,3,4,5)$ o $\alpha_2 = (1,2)(3,4)$. Un cálculo prueba que en ambos casos $(3,4,5)^{-1}\alpha_i^{-1}(3,4,5)\alpha_i$ es un 3-ciclo, que debe pertenecer a H porque $H \lhd A_5$. Con ello hemos probado que siempre hay un 3-ciclo en H, digamos $\alpha = (1,2,3)$. Si $\{a_1, a_2, \ldots, a_5\}$ es una reordenación de $\{1,2,\ldots,5\}$, quizá intercambiando a_4 y a_5 se tiene que la permutación definida por $\gamma(a_i) = i$ es par, entonces $\gamma^{-1}\alpha\gamma = (a_1, a_2, a_3) \in H$. En definitiva, H debe contener todos los 3-ciclos, y como éstos generan A_5, necesariamente se verifica $H = A_5$. □

Y ahora el ingenioso juego de manos para calcular un grupo de Galois sin hacer cálculos. Abel trató la ecuación de quinto grado con coeficientes generales, lo que no le permitió dar ejemplos explícitos, por lo que reservaremos su nombre para un resultado de este tipo de la próxima sección, a pesar de que podríamos ponerlo sin rubor en éste.

Proposición 4.2.6 *Sea $P \in \mathbb{Q}[x]$ irreducible con $\partial P = 5$ y exactamente tres raíces reales, entonces el grupo de Galois de su cuerpo de descomposición es isomorfo a S_5 y P no es soluble por radicales.*

Nota: La prueba podría acortarse utilizando un resultado de teoría de grupos del final del curso de Álgebra I (véase [St]) pero aquí preferimos el camino pedestre.

Demostración: La segunda parte es consecuencia de la primera, porque si P fuera soluble por radicales, S_5 sería un grupo soluble, y $A_5 \subset S_5$ también lo sería por el Teorema 4.1.1, lo que contradice el lema.

Como ya hemos empleado antes, el grupo de Galois permuta las raíces y puede identificarse con un subgrupo H de S_5. Según el Corolario 3.2.6 para cualquier $i, j \in A = \{1, 2, 3, 4, 5\}$ existe $\sigma \in H$ con $\sigma(i) = j$, esta propiedad se suele llamar *transitividad* (se dice que el subgrupo $H \subset S_5$ es transitivo). Además la conjugación compleja intercambia exactamente dos raíces, es decir, corresponde a una trasposición, digamos $(1, 2)$. Lo que vamos a probar es que el único subgrupo transitivo de S_5 conteniendo a $(1, 2)$ es el propio S_5. Para ello definimos en A la relación $i\mathcal{R}j$ si $i = j$ ó $(i, j) \in H$. Esta relación es de equivalencia, la propiedad transitiva se sigue de $(i, k) = (j, k)(i, j)(j, k)$, y todas sus clases tienen el mismo número de elementos, porque si $\sigma \in H$ cumple $\sigma(i) = j$, la igualdad $\sigma^{-1}(j, \sigma(k))\sigma = (i, k)$ implica $k \in \overline{i} \Leftrightarrow \sigma(k) \in \overline{j}$. Supongamos que hay c clases de equivalencia distintas, como éstas conforman una partición de A, $5 = c \cdot |\overline{1}|$. La única posibilidad es $c = 1$, porque $1, 2 \in \overline{1}$, por consiguiente $i\mathcal{R}j$ para todo $i, j \in A$, o lo que es lo mismo, H contiene a todas las trasposiciones y por tanto $H = S_5$. □

Ejemplo. El polinomio $P = x^5 - 6x + 3 \in \mathbb{Q}[x]$ no es soluble por radicales.

Considerando la función $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = P(x)$, se tiene que $f'(x) = 5x^4 - 6$, de donde f alcanza un máximo en $x_0 = -\sqrt[4]{6/5}$ y un mínimo en $x_1 = \sqrt[4]{6/5}$. La función f es creciente en $(-\infty, x_0)$ y en (x_1, ∞) y decreciente en (x_0, x_1). Como $f(x_0) > 0$ y $f(x_1) < 0$, necesariamente hay exactamente un cero real en cada uno de los tres intervalos indicados.

Se puede probar que A_5 es isomorfo al grupo de movimientos en el espacio que dejan fijo el icosaedro. En este sentido la insolubilidad de la quíntica tiene que ver con que los radicales sólo otorgan simetrías que vienen de "pegar" unos cuantos $\mathbb{Z}_p$, mientras que las simetrías del icosaedro son más ricas. En general, los grupos de movimientos son una fértil fuente de grupos simples, especialmente en espacios vectoriales sobre $\mathbb{F}_p$. Hay ciertas funciones (llamadas genéricamente funciones elípticas) que permiten generar todas las simetrías del icosaedro, y admitiendo su uso en lugar de los radicales, resolver la quíntica. Estas ideas fueron desarrolladas por Klein en 1877.

4.3. Algunas aplicaciones

En esta sección nos ocuparemos de algunas extensiones y aplicaciones de los resultados de resolubilidad por radicales. Los temas seleccionados son clásicos, precediendo cronológicamente a la teoría de Galois y motivándola. Sirva su abolengo como colofón histórico del curso.

El primer tema que vamos a tratar versa sobre ecuaciones algebraicas generales.

En la sección anterior hemos concluido que no se pueden resolver las quínticas con radicales porque existe una que no es soluble por radicales. En principio, bien podría ser un ejemplo aislado que no impidiera la existencia de una solución general que "colapsase" cuando los coeficientes guardan ciertas relaciones algebraicas, de la misma forma que, por poner un ejemplo burdo, la solución de la ecuación general de segundo grado colapsa si tratamos de aplicarla con $a = 0$. Además, considerar los coeficientes como variables

independientes es inherente al origen histórico del problema de la resolubilidad por radicales. Esto conduce a la definición de ecuación general.

Definición: Se llama *ecuación general de grado n* al polinomio $x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in K[x]$ donde $K = \mathbb{Q}[c_0, c_1, \ldots, c_{n-1}]$ con c_j variables indeterminadas distintas.

Esta ecuación general, tendrá n raíces, digamos $r_1, r_2, \ldots, r_n$ en su cuerpo de descomposición. La relación entre ellas y los coeficientes viene dada por las llamadas funciones simétricas elementales (conocidas para los que hayan leído la letra pequeña del primer capítulo), $\sigma_j = \sigma_j(r_1, r_2, \ldots, r_n)$, definidas como la suma de todos los productos de j raíces, sin importar el orden:

$$\sigma_1 = r_1 + r_2 + \cdots + r_n, \quad \sigma_2 = r_1r_2 + r_1r_3 + \cdots + r_{n-1}r_n, \quad \ldots \quad \sigma_n = r_1r_2 \ldots r_n.$$

Igualando $(x - r_1)(x - r_2)\cdots(x - r_n)$ y $x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ se tiene que $c_{n-k} = (-1)^k\sigma_k(r_1, r_2, \ldots, r_n)$. Si considerásemos las raíces r_j como variables, entonces para cada permutación $\pi \in S_n$, la aplicación $r_j \mapsto r_{\pi(j)}$ definiría un automorfismo perteneciente a $\mathcal{G}\big(\mathbb{Q}(r_1, r_2, \ldots, r_n)/\mathbb{Q}(\sigma_1, \ldots, \sigma_n)\big)$ y de hecho todos serían de esta forma porque los elementos del grupo de Galois quedan determinados por la permutación que inducen sobre las raíces. Esto prueba que el grupo de Galois anterior es isomorfo a S_n. Pero, la definición de ecuación general nos habla de coeficientes variables y no de raíces variables con lo cual el susodicho grupo de Galois no es exactamente el que corresponde al cuerpo de descomposición. Eso nos lleva a dar un rodeo. El concepto que escondemos bajo la alfombra sin mencionarlo es el de *grado de trascendencia* [Gar], [St], que es una generalización del grado para extensiones trascendentes (y por tanto infinitas) representando el número de variables independientes que necesitamos para generar la extensión. Intuitivamente, la conclusión será que el grupo de Galois es isomorfo a S_n siempre que los coeficientes no tengan nada que ver entre sí.

Proposición 4.3.1 *Si L es el cuerpo de descomposición de la ecuación general de grado n, entonces $\mathcal{G}(L/K) \cong S_n$.*

Demostración: Sean, como antes, $r_1, r_2, \ldots, r_n \in L$ las raíces. Veamos primero que cada $\alpha \in L$ se escribe de forma única como $\alpha = f(r_1, r_2, \ldots, r_n)$ donde $f \in \mathbb{Q}(x_1, x_2, \ldots, x_n)$, esto es, f es un cociente de polinomios de n variables y coeficientes racionales. Si tal representación no fuera única, restando dos de ellas tendríamos $g \in \mathbb{Q}(x_1, x_2, \ldots, x_n) - \{0\}$ tal que $g(r_1, r_2, \ldots r_n) = 0$. La función

$$F(x_1, x_2, \ldots, x_n) = \prod_{\pi \in S_n} g(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$$

no es idénticamente nula (porque g no lo es) y es simétrica en todas sus variables. Por el Teorema 1.1.2, o usando que $\mathcal{G}\big(\mathbb{Q}(x_1, x_2, \ldots, x_n)/\mathbb{Q}(\sigma_1, \ldots, \sigma_n)\big) \cong S_n$ como se explicó antes de la demostración, se tiene que $F = h(\sigma_1, \sigma_2, \ldots, \sigma_n)$, evidentemente con h no nula. Sustituyendo las variables en ambas funciones por las raíces $r_1, r_2, \ldots, r_n$, se llega a que $h((-1)^n c_0, (-1)^{n-1}c_1, \ldots, (-1)^1 c_{n-1}) = 0$ lo cual contradice que $c_0, c_1, \ldots, c_{n-1}$ sean variables y h no idénticamente nula.

Una vez que representamos cada α como $f(r_1, r_2, \ldots, r_n)$, la prueba es como en los comentarios previos a la demostración. A cada $\pi \in S_n$ le podemos asociar un K-automorfismo:

$$\begin{array}{rcl} L & \longrightarrow & L \\ f(r_1, r_2, \ldots, r_n) & \longmapsto & f(r_{\pi(1)}, r_{\pi(2)}, \ldots, r_{\pi(n)}) \end{array}$$

lo que implica que $\mathcal{G}(L/K)$ tiene un subgrupo isomorfo a S_n. Como además cada elemento del grupo de Galois está determinado por la permutación que efectúa sobre las raíces $r_1, r_2, \ldots, r_n$ (porque generan L), se deduce $\mathcal{G}(L/K) \cong S_n$. □

Con esto llegamos al famoso resultado de Abel de 1824. Entonces faltaban unos años para que Galois escribiera su famosa memoria, con lo cual no es de extrañar que la prueba original tenga poco que ver, al menos en apariencia, con la nuestra.

Corolario 4.3.2 (Teorema de Abel) *La ecuación general de grado n no es soluble por radicales para $n \geq 5$.*

Demostración: Se puede considerar que A_5 es un subgrupo de S_n, $n \geq 5$, haciendo actuar sus permutaciones sobre los cinco primeros elementos y fijando el resto. El resultado se deduce del Teorema de Galois y del Lema 4.2.5. □

Hasta ahora hemos escrito teoremas profundos acerca de la solubilidad por radicales y paradójicamente todavía no hemos sido capaces de dar la fórmula general para resolver la ecuación de tercer grado que es conocida desde hace casi quinientos años. Es hora de remediarlo. En vez de buscar una fórmula final compacta, que es muy poco atractiva, trataremos de dar un método que tenga ciertos visos de generalidad y que ilustre dónde entra la solubilidad del grupo. Sería estupendo que tras esta explicación algún lector comprendiera repentinamente cómo se las apañaban nuestros tatarabuelos matemáticos para hacer teoría de Galois sin toda la maquinaria del álgebra abstracta. Y sería excelso que también se percatase de que toda esta maquinaria no es superflua habida cuenta del pingüe negocio matemático que hacemos pagando abstracción por generalidad, rigor y elegancia. Con tan buenos propósitos damos paso al segundo tema, consistente en la solución explícita de la cúbica y su relación con la solubilidad de S_3.

Sean r_1, r_2, r_3 las raíces de la ecuación general de tercer grado $x^3 + c_2x^2 + c_1x + c_0$. Ya habíamos visto que $\mathcal{G}(K(r_1, r_2, r_3)/K) \cong S_3$ donde $K = \mathbb{Q}(c_0, c_1, c_2)$. El grupo S_3 es soluble porque se tiene la serie de composición

$$\{\mathrm{Id}\} \subset A_3 \subset S_3$$

con cocientes $A_3/\{\mathrm{Id}\} = \langle\sigma\rangle \cong \mathbb{Z}_3$ y $S_3/A_3 = \langle\tau A_3\rangle \cong \mathbb{Z}_2$, por ejemplo con $\sigma = (1, 2, 3)$ y $\tau = (2, 3)$.

Lo que hacía Lagrange con sus resolventes (definidas en la demostración de la Proposición 4.2.2) es conseguir aplicaciones invertibles con radicales que fuerzan a que el grupo de simetrías de una expresión sea $\mathbb{Z}_p$. Dando primero las simetrías de $A_3/\{\mathrm{Id}\} \cong \mathbb{Z}_3$ y después las de $S_3/A_3 \cong \mathbb{Z}_2$ podremos pasar, escalando por la serie de composición, de

la raíces (que no tienen simetrías) a los coeficientes (que las tienen todas). Invirtiendo estas aplicaciones se obtiene la solución deseada.

Para completar este esquema partamos de una de las raíces, digamos r_1. Como hay tres raíces cúbicas de la unidad, 1, ω y $\overline{\omega}$, tenemos tres resolventes de Lagrange asociadas al elemento σ de orden 3:

$$\begin{aligned} L_0 &= \mathcal{L}(1,\sigma)(r_1) = r_1 + r_2 + r_3 \\ L_1 &= \mathcal{L}(\omega,\sigma)(r_1) = r_1 + \omega r_2 + \overline{\omega} r_3 \\ L_2 &= \mathcal{L}(\overline{\omega},\sigma)(r_1) = r_1 + \overline{\omega} r_2 + \omega r_3 \end{aligned}$$

Conociendo estas tres cantidades podemos hallar fácilmente la raíz de partida mediante $r_1 = (L_0 + L_1 + L_2)/3$. Por inspección directa, o apelando a la prueba de la Proposición 4.2.2, se tiene que L_0^3, L_1^3 y L_2^3 son invariantes por σ y por tanto están en A_3', de hecho $L_0 = -c_2$ (esto se debe a que 1 es una raíz de la unidad muy especial). Ahora lo que hacemos es provocar nuevas simetrías en L_1^3 y L_2^3 para que también sean invariantes por τ. Se cumple $\tau(L_1^3) = L_2^3$, con lo cual basta provocar dichas simetrías en L_1. Esto no es ningún milagro, sino el reflejo de que como $A_3 \triangleleft S_3$ los cogrupos $\{A_3, \tau A_3\}$ conforman una partición de S_3 (y además heredan la estructura de grupo). Empleando las dos raíces cuadradas de la unidad, 1 y -1, se tienen las resolventes de Lagrange:

$$\begin{aligned} M_0 &= \mathcal{L}(1,\tau)(L_1) = L_1^3 + L_2^3 \\ M_1 &= \mathcal{L}(-1,\tau)(L_1) = L_1^3 - L_2^3 \end{aligned}$$

Podemos recuperar fácilmente L_1^3 a partir de M_0 y M_1 con $L_1^3 = (M_0 + M_1)/2$ y lo mismo con L_2^3. Finalmente, como M_0^2 y M_1^2 son invariantes por σ y τ (de nuevo, por inspección directa o la Proposición 4.2.2), lo son por todo elemento de S_3 y esto implica, lo creamos o no, que al hacer los cálculos deben pertenecer a K. Haciendo unas cuentas indeseables (pero sistemáticas si se procede como se indica en la prueba del Teorema 1.1.2), se tiene:

$$M_0 = -27c_0 + 9c_1c_2 - 2c_2^3, \qquad M_1^2 = -27(c_2^2c_1^2 + 18c_2c_1c_0 - 4c_1^3 - 4c_2^3c_0 - 27c_0^2).$$

Entonces una receta para obtener la solución general de la cúbica es:

1. Calcular M_0 y M_1^2 con las fórmulas anteriores.
2. Hallar $L_1^3 = (M_0 + M_1)/2$, $L_2^3 = (M_0 - M_1)/2$.
3. Finalmente, obtener $r_1 = (-c_2 + L_1 + L_2)/3$.

El nombre r_1 es evidentemente convencional, y de esta forma obtenemos las tres raíces. Hay dos signos posibles para $\sqrt{M_1^2}$ pero no tiene influencia en el resultado porque su eleccción sólo intercambia los valores de L_1^3 y L_2^3. En principio hay nueve posibles formas de combinar los argumentos de $\sqrt{L_1^3}$ y $\sqrt{L_2^3}$, pero de todas ellas sólo hay tres admisibles, correspondientes a las raíces. De hecho ambos argumentos deben ser opuestos para que den lugar a verdaderas raíces porque L_1L_2 es invariante por todo elemento de S_3.

Veamos un ejemplo particular, sólo para comprobar que no estamos mintiendo con toda esta abrumadora nube de fórmulas.

Ejemplo. Hallar las raíces de $x^3-3x^2+3x-3\in\mathbb{Q}[x]$ con el método antes indicado.

Aquí $c_0=c_2=-3$, $c_1=3$. Empleando las fórmulas, $M_0=54$, $M_1^2=54^2$. De donde $L_1^3=54$, $L_2^3=0$ (o en orden inverso si se escoge $M_1=-54$). Por tanto $L_1=3\sqrt[3]{2},3\omega\sqrt[3]{2},3\overline{\omega}\sqrt[3]{2}$. Finalmente, $r=1+\sqrt[3]{2},1+\omega\sqrt[3]{2},1+\overline{\omega}\sqrt[3]{2}$.

La ecuación general de cuarto grado se puede resolver de la misma forma escalando por la serie de composición, lo que ocurre es que ésta es el doble de larga, con lo cual los cálculos se duplican. El enfoque clásico es organizar las cuentas de manera que las raíces de la ecuación de cuarto grado se relacionen mediante radicales con las de una ecuación de tercer grado asociada, llamada comúnmente *cúbica resolvente* [Cl], [Rotm]. Desde el punto de vista de la teoría de Galois esto corresponde a que los cocientes $\mathbb{Z}_3$ y $\mathbb{Z}_2$ que aparecen en la serie de composición de S_3 son los mismos que aparecen al final de la serie de composición de S_4.

El tercer tema que trataremos es el del cálculo explícito del grupo de Galois del cuerpo de descomposición de un polinomio en $\mathbb{Q}[x]$, y para darle un toque clásico analizaremos un ejemplo que se puede relacionar con la constructibilidad con regla y compás.

Después de los resultados negativos que hemos visto, notamos que los ejemplos del capítulo anterior de grupos de Galois de cuerpos de descomposición de polinomios estaban ciertamente preparados. Dado un polinomio $P\in\mathbb{Q}[x]$, lo más posible es que no podamos dar siquiera generadores explícitos con radicales para su cuerpo de descomposición. Incluso en el caso $\partial P=3$, aunque tengamos fórmulas explícitas para las raíces, son tan complejas que en general no ayudan nada a la hora de calcular el grupo de Galois. Veamos que al menos en este caso hay un método sencillo para saber a qué grupo es isomorfo el grupo de Galois. Nos restringiremos al caso irreducible porque el otro es casi trivial. (Un análogo para $\partial P=4$ puede encontrarse en [Ka] Th. 43).

Teorema 4.3.3 *Sea $P=x^3+c_2x^2+c_1x+c_0\in\mathbb{Q}[x]$ irreducible, L su cuerpo de descomposición y*

$$\Delta=c_2^2c_1^2+18c_2c_1c_0-4c_1^3-4c_2^3c_0-27c_0^2.$$

Entonces $\mathcal{G}(L/\mathbb{Q})\cong A_3(\cong\mathbb{Z}_3)$ si y sólo si Δ es un cuadrado perfecto en $\mathbb{Q}$, esto es, $\sqrt{\Delta}\in\mathbb{Q}$. En otro caso $\mathcal{G}(L/\mathbb{Q})\cong S_3$.

Observación: A Δ se le suele llamar *discriminante* y generaliza al concepto homónimo en las ecuaciones de segundo grado en un sentido que se explicará más adelante. La proporcionalidad entre Δ y M_1^2 en la solución general de la cúbica no es casual y está relacionada con el hecho de que M_1 se construía de forma que tuviera las simetrías de A_3 pero no el resto de las de S_3.

Demostración: En primer lugar comprobemos la identidad algebraica:

$$3\sqrt{-3}(x-y)(x-z)(y-z)=(x+\omega y+\overline{\omega}z)^3-(x+\overline{\omega}y+\omega z)^3$$

con $\omega=(-1+\sqrt{-3})/2$. Ambos miembros se pueden considerar como polinomios de segundo grado en x que tienen el mismo coeficiente principal porque $3\sqrt{-3}(y-z)=3(\omega y+\overline{\omega}z)-3(\overline{\omega}y+\omega z)$. Además tienen las mismas raíces porque el segundo miembro

se anula para $x = y$ y $x = z$ (nótese que $1 + \omega = -\overline{\omega}$ y $\omega^3 = \overline{\omega}^3 = 1$). Sustituyendo en esta identidad las variables por las raíces r_1, r_2 y r_3 de P, elevando al cuadrado y empleando la fórmula para M_1^2, se obtiene

$$\Delta = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2.$$

Como $[\mathbb{Q}(r_1) : \mathbb{Q}] = 3$ divide a $|\mathcal{G}(L/\mathbb{Q})|$ y los elementos de $\mathcal{G}(L/\mathbb{Q})$ permutan las raíces, sólo puede ser $\mathcal{G}(L/\mathbb{Q}) \cong A_3$ o $\mathcal{G}(L/\mathbb{Q}) \cong S_3$. Todas las permutaciones de A_3 dejan fijo $(r_1 - r_2)(r_1 - r_3)(r_2 - r_3)$ y ninguna de las de $S_3 - A_3$ lo hace (en el primer caso basta comprobarlo para un 3-ciclo, y en el segundo para una trasposición). Así pues $\mathcal{G}(L/\mathbb{Q}) \cong A_3$ si y sólo si esta cantidad pertenece al cuerpo fijo $\big(\mathcal{G}(L/\mathbb{Q})\big)' = \mathbb{Q}$. Esto es, si y sólo si $\sqrt{\Delta} \in \mathbb{Q}$. □

El concepto de discriminante se puede generalizar si partimos de la igualdad para Δ probada en la demostración anterior.

Definición: Si $P \in K[x]$, $\partial P = n \geq 1$, y $r_1, r_2, \ldots, r_n$ son sus raíces (repetidas según sus multiplicidades) entonces se define el *discriminante* de P como

$$\Delta_n(P) = \prod_{1 \leq i < j \leq n} (r_i - r_j)^2.$$

Observación: Si L es el cuerpo de descomposición de P y L/K es separable (lo que está asegurado si se exige $\mathrm{char}(K) = 0$) entonces L/K es una extensión de Galois. Como $\Delta_n(P)$ es invariante por todos los elementos del grupo de Galois (porque es invariante por cualquier permutación de las raíces), necesariamente en el caso separable $\Delta_n(P) \in K$ y habrá una fórmula kilométrica que relacione el determinante con los coeficientes del polinomio. Según la demostración anterior $\Delta = \Delta_3(P)$ y un cálculo prueba que en $\mathbb{Q}[x]$, $\Delta_2(x^2 + bx + c) = b^2 - 4c$ lo que explica la notación.

En principio uno podría aventurarse en la búsqueda de un algoritmo para decidir el grupo de Galois de cualquier polinomio. Tal algoritmo existe (véase [St], [Gar]) pero es demasido complicado y computacionalmente costoso. Dicho esto, nos desquitaremos hallando el grupo de Galois del cuerpo de descomposición de un polinomio particular de cuarto grado, y elevaremos los cálculos al rango de lema porque nos servirán para tratar un problema de constructibilidad.

Lema 4.3.4 *Sea L el cuerpo de descomposición de $P = x^4 - 10x^2 - 4x + 6 \in \mathbb{Q}[x]$. Entonces $\mathcal{G}(L/\mathbb{Q}) \cong A_4$.*

Demostración: Sean r_1, r_2, r_3, r_4 las raíces de P y consideremos las cantidades:

$$s_1 = (r_1 + r_2)(r_3 + r_4), \qquad s_2 = (r_1 + r_3)(r_2 + r_4), \qquad s_3 = (r_1 + r_4)(r_2 + r_3).$$

El polinomio $Q = (x - s_1)(x - s_2)(x - s_3)$ es invariante por todas las permutaciones de las raíces (basta comprobar que el efecto de las trasposiciones $(1, 2)$, $(1, 3)$ es intercambiar los s_j) por tanto $Q \in \mathbb{Q}[x]$. Con las funciones simétricas elementales y suficiente paciencia uno tendría que poder expresar los coeficientes de Q en función de los de P.

Aquí llevaremos a cabo los cálculos en nuestro caso particular sin seguir un procedimiento sistemático (en [Rotm] p.61 se puede encontrar una fórmula general). Concretamente lo que haremos es hallar un polinomio mónico cúbico irreducible que tiene como raíz a s_1, lo que implica que necesariamente coincide con Q. Con este propósito definimos $A = r_1r_2$ y $B = r_3r_4$. Como el último coeficiente de P es el producto de raíces, $AB = 6$. El coeficiente de x^2 es $-10 = r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4 = A + B + s_1$, y el coeficiente de x se puede escribir como $-4 = -r_3r_4(r_1 + r_2) - r_1r_2(r_3 + r_4)$. Empleando que $r_1 + r_2 + r_3 + r_4 = 0$ (del coeficiente de x^3), la última igualdad equivale a $-4 = -B\sqrt{-s_1} + A\sqrt{-s_1}$. En resumen, tenemos las ecuaciones:

$$AB = 6, \qquad A + B = -10 - s_1, \qquad (A - B)^2 = -16/s_1.$$

Si multiplicamos por -4 la primera, le sumamos el cuadrado de la segunda y restamos la tercera, se obtiene que s_1 es raíz de

$$Q = x^3 + 20x^2 + 76x + 16.$$

Este polinomio es irreducible sobre $\mathbb{Q}$ (por ejemplo reduciendo módulo 3) y el resultado anterior implica, tras unos cálculos, que el grupo de Galois de su cuerpo de descomposición es isomorfo a $A_3 \cong \mathbb{Z}_3$. Por tanto los automorfismos de $\mathcal{G}(L/\mathbb{Q})$ deben permutar cíclicamente los s_j. Como ninguna trasposición de las raíces r_j tiene esta propiedad, y sí la tiene cualquier 3-ciclo, se deduce que $\mathcal{G}(L/\mathbb{Q})$ es isomorfo a un subgrupo de A_4 (que está generado por los 3-ciclos). Por otra parte, sabemos que $[\mathbb{Q}(r_1) : \mathbb{Q}] = 4$ y $[\mathbb{Q}(s_1) : \mathbb{Q}] = 3$ (P y Q son irreducibles) dividen al orden de $\mathcal{G}(L/\mathbb{Q})$. En definitiva, la única posibilidad es $\mathcal{G}(L/\mathbb{Q}) \cong A_4$. □

Esto conduce a un contraejemplo al recíproco del Lema 2.3.1 que se puede generalizar con la ayuda del teorema del elemento primitivo.

Proposición 4.3.5 *Para cada $n \geq 2$ existe un número real α no construible con regla y compás tal que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$.*

Demostración: Para el caso $n = 2$, sea α una raíz real de $P = x^4 - 10x^2 - 4x + 6$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Si α fuera construible entonces existiría $\mathbb{Q} \subset M \subset \mathbb{Q}(\alpha)$ con $[M : \mathbb{Q}] = 2$ y por tanto, por el teorema fundamental de la teoría de Galois, $\mathcal{G}(L/M)$, con L el cuerpo de descomposición de P, sería un subgrupo de índice dos (de orden 6) de $\mathcal{G}(L/\mathbb{Q}) \cong A_4$, pero A_4 no tiene tales subgrupos.

Ahora generalizamos el contraejemplo por inducción. Supongamos dado $\beta \in \mathbb{R}$ no construible con regla y compás tal que $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2^n$. Siempre podemos hallar $\sqrt{m} \notin \mathbb{Q}(\beta)$, $m \in \mathbb{Z}^+$, porque el cuerpo de descomposición de β, que incluye a $\mathbb{Q}(\beta)$, tiene un número finito de subcuerpos por el teorema fundamental del teorema de Galois. El teorema del elemento primitivo (Teorema 3.1.8) asegura que existe γ tal que $\mathbb{Q}(\gamma) = \mathbb{Q}(\beta, \sqrt{m})$. Además

$$[\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(\beta)(\sqrt{m}) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = 2^{n+1},$$

y γ no es construible con regla y compás, porque si lo fuera, como los elementos construibles forman un cuerpo, también lo sería β. Por inducción se deduce que hay elementos no construibles para cualquier grado $2^N \geq 4$. □

Observación: El recíproco del Lema 2.3.1 sin embargo sí es cierto con la hipótesis adicional de que $\mathbb{Q}(\alpha)/\mathbb{Q}$ sea normal, y por tanto de Galois. Un teorema de teoría de grupos asegura que los grupos de orden 2^n son solubles (véase [Cl], [Ga]), en particular lo es el grupo de Galois de $\mathbb{Q}(\alpha)/\mathbb{Q}$ y, aplicando la correspondencia entre subgrupos y subcuerpos, la serie de composición se transforma en la cadena de subcuerpos requerida para la constructibilidad.

Como tema final, estudiaremos las extensiones ciclotómicas y su relación con la constructibilidad de polígonos regulares.

Teorema 4.3.6 *El grupo de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}$ con $\zeta = e^{2\pi i/n}$, es isomorfo al grupo (multiplicativo) de unidades de $\mathbb{Z}_n$.*

Demostración: Sea $P \in \mathbb{Q}[x]$ el polinomio mínimo de ζ. Como $P|x^n - 1$, se tiene de hecho $P \in \mathbb{Z}[x]$ (por el lema de Gauss, ejercicio). Basta demostrar que las raíces de P son exactamente ζ^k, $1 \leq k < n$, con k y n coprimos, ya que en ese caso los $\mathbb{Q}$-automorfismos serían los σ_k determinados por $\sigma_k(\zeta) = \zeta^k$ (Corolario 3.2.6) y la aplicación del grupo de Galois en el grupo de Galois en el grupo de unidades dada por $\Phi(\sigma_k) = \overline{k}$ sería claramente un isomorfismo: es biyectiva y $\Phi(\sigma_k\sigma_l) = \Phi(\sigma_{kl}) = \Phi(\sigma_k) \cdot \Phi(\sigma_l)$.

Para probar que los ζ^k son las raíces de P, definimos Q_m como el polinomio resultante al sustituir en P la variable x por x^m. En particular $P(\zeta^k) = 0 \Leftrightarrow Q_k(\zeta) = 0$. Sea R_m el resto al dividir Q_m entre P. La sucesión de restos $R_1, R_2, R_3, \ldots$ es periódica de periodo n porque $Q_{m+n}(\zeta) - Q_m(\zeta) = 0$ y, como P es el polinomio mínimo de ζ, P debe dividir a $Q_{m+n} - Q_m$.

Por otra parte, desarrollando $(a_n x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1 x^p + a_0) - (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p$ se obtiene

$$\sum_{j=0}^{n}(a_j - a_j^p)x^{jp} - \sum_{r_0+r_1+\cdots+r_n=p} \frac{p!}{r_0!r_1!\cdots r_n!} a_0^{r_0}(a_1x)^{r_1}\cdots(a_nx^n)^{r_n}$$

con $0 \leq r_j < p$. Los coeficientes del segundo sumatorio son obviamente divisibles por p, y los del primero también lo son por el pequeño teorema de Fermat. En particular, los coeficientes de $Q_p - P^p$ son divisibles por p para todo primo. Digamos que $Q_p - P^p = pC = p(A_pP + B_p)$ con $\partial B_p < P$, entonces necesariamente $R_p = pB_p$ (Q_p es un múltiplo de P más pB_p) y se deduce que los coeficientes de R_p son todos múltiplos de p. Sea N mayor que el máximo valor absoluto de los coeficientes de los R_j (está bien definido porque los restos son periódicos). Evidentemente, si $p > N$ se tiene $R_p = 0$.

Si $k = p_1p_2\cdots p_r$ con p_j primos mayores que N, entonces $R_{p_j} = 0 \Rightarrow P|Q_{p_j}$ y de aquí $P(\zeta^{p_1}) = Q_{p_1}(\zeta) = 0$, $P(\zeta^{p_1p_2}) = Q_{p_2}(\zeta^{p_1}) = 0$ (porque $P(\zeta^{p_1}) = 0$), e iterando $P(\zeta^k) = 0$.

Como $\zeta^k = \zeta^{k+an}$, lo único que falta por demostrar es que a cualquier $1 \leq k < n$ le podemos sumar un múltiplo de n de forma que todos los factores primos del resultado sean mayores que N. Esto es inmediato sumando $n\mathcal{P}$ con $\mathcal{P}$ el producto de los primos menores que N que no dividen a k. Nótese que $\mathcal{P}$ está bien definido, por la infinitud de los primos, eligiendo N suficientemente grande, lo cual es siempre posible. □

Si uno recuerda el curso de Conjuntos y Números el siguiente corolario es una consecuencia directa, en otro caso, hay que husmear en la demostración.

Corolario 4.3.7 *Si n factoriza como $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ con p_j primos distintos y $\alpha_j \in \mathbb{Z}^+$, el grado de $\mathbb{Q}(\zeta)/\mathbb{Q}$ viene dado por la función de Euler $\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$*

Demostración: Por definición, la función ϕ de Euler cuenta los $1 \leq k < n$ coprimos con n, así que lo único que hay que recordar es la fórmula para $\phi(n)$. Veamos una de las pruebas que se pudo incluir en el curso de Conjuntos y Números:

Si p es primo, se cumple $\phi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha - p^{\alpha-1}$ porque entre 1 y p^α hay exactamente $p^{\alpha-1}$ múltiplos de p. Con ello sólo resta probar que $\phi(ab) = \phi(a)\phi(b)$ si a y b son coprimos. Si $1 \leq r < ab$ es coprimo con ab, al reducirlo módulo a y b se obtienen restos r_a y r_b coprimos con a y b respectivamente. Recíprocamente el teorema chino del resto asegura que, dados estos r_a y r_b, existe un único r módulo ab tal que $r \equiv r_a \pmod{a}$ y $r \equiv r_b \pmod{b}$. Así que los cardinales contados con $\phi(ab)$ y $\phi(a)\phi(b)$ coinciden. □

Antes de seguir fijemos una notación que previsiblemente también se mencionó en Conjuntos y Números.

Definición: Los primos p para los que $p - 1$ es potencia de dos se llaman *primos de Fermat*.

Si excluimos $p = 2$ como caso especial, todos los primos de Fermat son de la forma $2^{2^n} + 1$ porque $2^{ab} + 1$ con $b > 1$ impar es compuesto: $2^{ab} + 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \cdots - 2^a + 1)$. La terminología viene porque Fermat creyó erróneamente que todos los números de la forma $2^{2^n} + 1$ eran primos. El primer contrajemplo lo encontró Euler: $2^{2^5} + 1 = 641 \cdot 6700417$. De hecho a partir de $n = 5$ no se ha encontrado todavía ningún primo.

Con esto ya estamos preparados para extasiarnos con el resultado de Gauss sobre constructibilidad de polígonos regulares, uno de los más bellos de las Matemáticas.

Teorema 4.3.8 *El polígono regular de n lados es construible con regla y compás si y sólo si $n = 2^r p_1 p_2 \cdots p_k$ con p_i primos de Fermat distintos.*

Demostración: Distingamos ambas implicaciones. Escribamos $\zeta = e^{2\pi i/n}$.

⇒) Según el Teorema 4.3.6 y su corolario, $\mathbb{Q}(\zeta)/\mathbb{Q}$ tiene grupo de Galois abeliano de orden una potencia de dos. Como $\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}$ es una subextensión de $\mathbb{Q}(\zeta)/\mathbb{Q}$, debe ser de Galois (en un grupo abeliano todo subgrupo es normal) y tener también estas propiedades. Digamos $G = \mathcal{G}\big(\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}\big)$ con $|G| = 2^m$. Al ser G abeliano, es soluble y existe una serie de composición:

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$$

Con $|G_i|/|G_{i-1}| = 2$. Por la correspondencia de Galois esto da lugar a una cadena de subgrupos:

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_m = \mathbb{Q}(\cos\frac{2\pi}{n})$$

donde $L_j = G'_{m-j}$ tal que $[L_{j+1} : L_j] = 2$.

$\Leftarrow$) Si n no es de la forma indicada, entonces $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ no es una potencia de dos, y como $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos(2\pi/n))] \leq 2$, porque $\zeta + \zeta^{-1} = 2\cos(2\pi/n)$, $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$ tampoco lo es. El Lema 2.3.1 implica entonces que $\cos(2\pi/n)$ no es construible. $\square$

Ejercicios del Capítulo 4

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 4.1

♡**1.** Probar que si un grupo finito no trivial G no tiene subgrupos propios, $G \cong \mathbb{Z}_p$.

2. Si un grupo soluble tiene como cocientes $\mathbb{Z}_2$ y $\mathbb{Z}_3$, apareciendo en ese orden, ¿puede encontrarse siempre otra serie de composición de manera que aparezcan en orden inverso?

♡**3.** Dar una serie de composición para $\mathbb{Z}_{p^k}$.

4. Deducir del ejercicio anterior y del teorema de clasificación de grupos abelianos finitos que todo grupo abeliano finito es soluble.

5. Hallar tres series de composición distintas para $\mathbb{Z}_{15} \times S_3$.

6. Hallar una serie de composición para D_{10}.

♡**7.** Hallar $H_1 \subset H_2 \subset G$ tales que $H_1 \lhd H_2$, $H_2 \lhd G$ pero de modo que H_1 no sea normal en G.

♡**8.** Demostrar que todo subgrupo de índice dos es normal.

9. Sean $K \subset M \subset L$ con M/K y L/K extensiones de Galois, demostrar que si $\mathcal{G}(L/K)$ es soluble, entonces $\mathcal{G}(M/K)$ también lo es.

10. Demostrar que si G y H son solubles entonces su producto directo $G \times H$ también lo es.

11. Demostrar que S_4 es soluble.

12. Dar dos series de composición para S_4.

13. Dado un grupo finito G se define su *conmutador* como $C(G) = \langle g^{-1}h^{-1}gh \ : g, h \in G \rangle$. Demostrar que $C(G)$ es un subgrupo normal y $G/C(G)$ es abeliano. Deducir que si $C(G)$ es soluble, G también lo es.

14. Demostrar que una cadena de subgrupos normales $\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 \cdots \subsetneqq G_n = G$, $G_i \lhd G_{i+1}$, $0 \leq i < n$, no es serie de composición si y sólo si para algún i existe un subgrupo H tal que $G_i \lhd H \lhd G_{i+1}$ con $H \neq G_i, G_{i+1}$.

15. Demostrar con detalle que todo grupo finito tiene al menos una serie de composición.

16. Demostrar que un grupo G es soluble si y sólo si existe una cadena de subgrupos $\{e\} = G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_n = G$, tal que G_{i+1}/G_i es abeliano, $0 \leq i < n$.

17. Dado un grupo G sea $l(G)$ la longitud de su serie de composición (el teorema de Jordan-Hölder asegura que está bien definida). Demostrar que si $H \subsetneqq G$ y G es soluble, entonces $l(H) < l(G)$. Nota: Si G no es soluble, hay contraejemplos.

18. Hallar todas las series de composición de $\mathbb{Z}_4 \times S_3$.

$\circ$**19.** Proceder como en la prueba del teorema de Jordan-Hölder para deducir que si $N_1 \triangleleft H_1 \triangleleft G$, $N_2 \triangleleft H_2 \triangleleft G$, entonces $N_1(H_1 \cap H_2)/N_1(H_1 \cap N_2) \cong H_1 \cap H_2/(H_1 \cap N_2)(H_2 \cap N_1)$.

$\diamondsuit$**20.** Se llaman *clases de conjugación* en un grupo G, a las clases de equivalencia de la relación $g_1 \mathcal{R} g_2 \Leftrightarrow g_1 = h^{-1} g_2 h$. Demostrar que el cardinal de cada clase de conjugación divide a $|G|$. *Indicación*: Definir $H_g = \{h \in G \ : \ h^{-1}gh = g\}$ y probar que hay una biyección entre los elementos de la clase de conjugación que contiene a g y los cogrupos de G/H_g.

$\diamondsuit$**21.** Demostrar que en un grupo de orden p^n, con p primo, las clases de conjugación con un solo elemento conforman un subgrupo normal no trivial. Deducir de ello que todo grupo de orden p^n es soluble.

$\diamondsuit\diamondsuit$**22.** Demostrar que cualquier grupo de orden 100 es soluble. *Indicación*: La dificultad radica en gran medida en recordar los teoremas de Sylow.

Sección 4.2

$\heartsuit$**23.** Demostrar que todo $P \in \mathbb{R}[x]$ es soluble por radicales.

24. Demostrar que M/K radical y L/M radical $\Rightarrow$ L/K radical.

25. Si $\alpha, \beta \in \mathbb{C}$ están en sendas extensiones radicales de $\mathbb{Q}$, probar que $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ es radical.

26. Sea α en una extensión radical de K. Probar que $L(\alpha)/K(\alpha)$ radical $\Rightarrow$ L/K radical.

$\heartsuit$**27.** Probar que si una raíz de un polinomio irreducible en $\mathbb{Q}[x]$ está en una extensión radical, entonces lo están todas.

28. Dar tres ejemplos de quínticas no solubles por radicales.

29. Probar que si las raíces de $P \in \mathbb{Q}[x]$ son iguales salvo multiplicar por elementos de K, entonces P es soluble por radicales. *Indicación*: La terminología "abeliano" viene del estudio que hizo Abel de este tipo de polinomios.

30. Sea $P \in \mathbb{Q}[x]$ un polinomio irreducible de grado primo $\partial P = p > 3$. Usando un resultado de teoría de grupos se puede probar que el grupo de Galois G de su cuerpo de descomposición tiene un elemento de orden p. Dando esto por supuesto, demostrar que si P tiene exactamente dos raíces complejas entonces $G \cong S_p$ y P no es soluble por radicales.

31. Demostrar que existe $P \in \mathbb{Q}[x]$ con $\partial P = 5$ y $\mathcal{G}(L/\mathbb{Q}) \cong \mathbb{Z}_5$, donde L es el cuerpo de descomposición de L.

32. Probar detalladamente que $\{\mathrm{Id}\} \subset \langle\sigma\rangle \subset \langle\sigma, \tau\rangle \subset A_4 \subset S_4$ con $\sigma = (1,2)(3,4)$ y $\tau = (1,3)(2,4)$, es realmente una serie de composición de S_4.

33. Demostrar que para resolver una ecuación de cuarto grado, se necesitan a lo más raíces cuadradas y cúbicas.

34. Verificar que si $\alpha = (1,2,3,4,5)$ ó $\alpha = (1,2)(3,4)$ entonces $(3,4,5)^{-1}\alpha^{-1}(3,4,5)\alpha$ es un 3-ciclo.

35. Explicar por qué los 3-ciclos en S_n generan todas las permutaciones pares.

36. Refinar el problema anterior, probando que los 3-ciclos de la forma $(1,a,b) \in S_n$ generan A_n.

♡**37.** Dar un ejemplo de un polinomio de sexto grado no soluble por radicales.

38. Sea P un polinomio irreducible de $\mathbb{Q}[x]$ con $\partial P = 4$ y cuerpo de descomposición L. Demostrar que si P tiene dos raíces reales, entonces $\mathcal{G}(L/Q)$ es isomorfo a S_4 o a D_8.

♢**39.** Sea un subgrupo $H \subset G$ tal que H no contiene a ningún subgrupo normal no trivial de G. Probar que G es isomorfo a un subgrupo de S_m con $m = |G|/|H|$. Deducir de ello que al permutar las variables de una función $f \in K[x_1, x_2, \ldots, x_n]$ de todas las formas posibles, si se obtienen más de dos funciones distintas, entonces se obtienen al menos n. *Indicación*: Comenzar probando que cada $g \in G$ está totalmente determinado por su acción sobre los cogrupos de G/H.

♢♢**40.** Sea $L/\mathbb{Q}$ una extensión de Galois tal que para cualquier par de subcuerpos M_1, M_2, hay una relación de inclusión (esto es, $M_1 \subset M_2$ o $M_2 \subset M_1$). Demostrar que $L/\mathbb{Q}$ es radical. *Indicación*: Utilizar los teoremas de Sylow y que por un problema anterior los grupos de orden p^n son solubles.

41. Usando un resultado de teoría de grupos que implica que un grupo de orden múltiplo de orden 5 siempre tiene un elemento de orden 5, simplificar la prueba de que $P \in \mathbb{Q}[x]$, $\partial P = 5$, irreducible con exactamente tres raíces reales $\Rightarrow P$ no es soluble por radicales.

♢♢**42.** Sea $P \in \mathbb{Q}[x]$ irreducible de grado primo p y sea L su cuerpo de descomposición. Demostrar que si P es soluble por radicales entonces cualquier serie de composición de $\mathcal{G}(L/\mathbb{Q})$ debe tener primer grupo no trivial $G_1 \cong \mathbb{Z}_p$.

Sección 4.3

43. Hallar los posibles grupos de Galois de una cúbica no irreducible en $\mathbb{Q}[x]$.

44. Demostrar que si $\alpha_1, \alpha_2, \alpha_3$ y α_4 son raíces de $P \in \mathbb{Q}[x]$, $\partial P = 4$, entonces $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, $\alpha_1\alpha_4 + \alpha_2\alpha_3$ son raíces de cierto $Q \in \mathbb{Q}[x]$ con $\partial Q = 3$ y se cumple $\Delta_4(P) = \Delta_3(Q)$.

45. Sea L el cuerpo de descomposición de polinomio de cuarto grado irreducible sobre $\mathbb{Q}$. Demostrar que $\mathcal{G}(L/\mathbb{Q})$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$, D_8, A_4 o S_4.

46. Encontrar ejemplos explícitos de polinomios de cuarto grado irreducibles sobre $\mathbb{Q}$, tales que el grupo de Galois de su cuerpo de descomposición sea isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ y a $\mathbb{Z}_4$.

47. Resolver con radicales $x^3 + x + 3 = 0$.

48. Demostrar que si $P \in \mathbb{Q}[x]$ es un polinomio cúbico irreducible y α es una de sus raíces, su cuerpo de descomposición es $L = \mathbb{Q}(\sqrt{\Delta}, \alpha)$.

49. Sea $P \in \mathbb{Q}[x]$ irreducible de grado n. Demostrar que $\sqrt{\Delta_n(P)} \in \mathbb{Q}$ si y sólo si el grupo de Galois (identificado como grupo de permutaciones de las raíces) de su cuerpo de descomposición es un subgrupo de A_n.

50. Sea K un cuerpo de característica distinta de 2 y $x^4 + ax^2 + b \in K[x]$ irreducible. Probar que el grupo de Galois de su cuerpo de descomposición es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ si $\sqrt{b} \in K$; es isomorfo a $\mathbb{Z}_4$ si $\sqrt{b} \notin K$ y $\sqrt{b(a^2 - 4b)} \in K$; y es isomorfo a D_8 si $\sqrt{b} \notin K$ y $\sqrt{b(a^2 - 4b)} \notin K$;

51. Si $P \in \mathbb{Q}[x]$ es un polinomio irreducible de tercer grado con sus tres raíces reales, probar que no existe ninguna extensión radical real que contenga a las tres. Esto es, no se puede resolver la ecuación $P(x) = 0$ sólo con radicales reales.

52. Probar con detalle que el polinomio mínimo sobre $\mathbb{Q}$ de $e^{2\pi i/n}$ debe pertenecer a $\mathbb{Z}[x]$.

$\diamondsuit$**53.** Demostrar que el polinomio mínimo de $e^{2\pi i/n}$ sobre $\mathbb{Q}$ es $P = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$, donde $\mu(d)$ es la función de Möbius, que vale 1 si $d = 1$, $(-1)^r$ si d es producto de r primos distintos, y cero en otro caso. Utilizar este resultado para hallar el polinomio mínimo sobre $\mathbb{Q}$ de $e^{\pi i/10}$.

54. Demostrar que el polinomio mínimo de $e^{2\pi i/p^2}$ sobre $\mathbb{Q}$ es $x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1$.

55. Demostrar con detalle que si p es primo, todos los coeficientes del polinomio $(a_n x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1 x^p + a_0) - (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p$ son divisibles por p.

56. Hallar todos los n menores que 260 tales que el polígono regular de n lados sea construible con regla y compás.

Apéndice del Capítulo 4

Conoce a tus héroes

(Más información en: `http://turnbull.mcs.st-and.ac.uk/history/`)

Apellido: Abel
Nombre: Niels Henrik
Nacimiento: 1802 Frindoe
Defunción: 1829 Froland

La breve vida de Abel estuvo dominada por penalidades y su temprana muerte motivada por la penuria que le tocó sufrir. Su resultado más conocido es la prueba de la imposibilidad de resolver la ecuación general de quinto grado con radicales (cuya publicación en un artículo de seis páginas, sufragó él mismo), para lo cual empleó algunas herramientas de lo que hoy llamaríamos teoría de cuerpos y un teorema de Cauchy de la incipiente teoría de grupos. Sus avances en otras áreas de las Matemáticas son también de primer orden, a pesar de su corta vida. Así contribuyó a la teoría de series y a la teoría de funciones elípticas, y creó lo que hoy conocemos como integrales abelianas. Su nombre ha quedado inmortalizado en la notación matemática común asociado a la conmutatividad.

Bla, bla, bla

- *Todo el mundo sabe que los geómetras más eminentes no han tenido éxito en la búsqueda de una solución general de las ecuaciones de grado mayor que cuatro, o (para ser más preciso) en la REDUCCIÓN DE ECUACIONES MIXTAS A ECUACIONES PURAS. Y hay pocas dudas de que este problema no está simplemente más allá de la potencia del análisis contemporáneo, sino que se muestra imposible.* C.F. Gauss 1801.

- *Teorema: Si uno añade a una ecuación dada la raíz r de una ecuación auxiliar irreducible:* (1) *una de estas dos cosas ocurren: o el grupo de la ecuación no cambia, o se dividirá en p grupos, cada uno de los cuales pertenece a la ecuación dada cuando se añade una raíz de la ecuación auxiliar;* (2) *estos grupos tienen la notable propiedad de que se puede pasar de uno a otro aplicando la misma sustitución de letras a todas las permutaciones del primero.* E. Galois 1832.

- *Los matemáticos han tratado de encontrar con ahínco la solución general de las ecuaciones algebraicas, y algunos han intentado probar la imposibilidad de ello. Sin embargo, si no estoy equivocado, no han tenido éxito hasta ahora. Así pues, me atrevo a esperar que los matemáticos acogerán esta memoria de buen grado,*

ya que su propósito es llenar esta laguna en la teoría de ecuaciones algebraicas.
N.H. Abel 1824.

¿Qué hay que saberse?

Digamos que en una versión mínima, es necesario saber la definición de grupo soluble y la relación entre solubilidad de grupos y de ecuaciones, esto es, el teorema de Galois.

(PQR) Preguntón, quejoso y respondón

Q- ¿Realmente a alguien le importa si una ecuación es soluble por radicales o no? El teorema de Galois no parece interesante, porque con un ordenador podemos aproximar las raíces con precisión arbitraria.

R- En los libros de divulgación habitualmente se menciona el teorema de Galois, con lo cual seguramente sea atractivo incluso para los que no son matemáticos profesionales, a pesar de su escaso valor práctico.

P- ¿Hay algoritmos para calcular el grupo de Galois, salvo isomorfismos, del cuerpo de descomposición de un polinomio en $\mathbb{Q}[x]$ que sean suficientemente eficientes como para ser programados en un ordenador?

R- Sí, al menos para grados pequeños, porque hay paquetes matemáticos para ordenadores personales que incluyen esa función.

P- ¿Todavía se investiga en teoría de Galois?

R- Aunque la teoría de Galois clásica, que es la que hemos estudiado, tiene un aspecto maravillosamente cerrado y perfecto, su relación con diferentes temas abre nuevos horizontes y lleva la teoría de Galois, en un sentido amplio, a la vanguardia de la investigación.

Q- Según creo, la prueba de Abel de su teorema constaba de 6 páginas, la memoria de Galois de 17, y Gauss dedicó sólo la última sección de su obra maestra *Disquisitiones Arithmeticae* a la constructibilidad de polígonos regulares. No entiendo por qué a nosotros nos ha costado todo un largo curso obtener sus resultados.

R- En primer lugar, hemos elaborado una teoría general que era desconocida por ellos y que permite entender lo que hicieron dentro de un contexto más amplio. Además en el caso de los trabajos de Abel y Galois (no en el de Gauss) hay fallas de rigor que no serían aceptables con los niveles comúnmente exigidos actualmente.

Q- De todas formas parece más fácil entender las ideas fundamentales a través de unas pocas páginas no muy rigurosas que entresacarlas de las demostraciones de una maraña de teoremas generales.

R- Puede que sí, y muchos matemáticos eminentes han recomendado leer a los clásicos.

Bibliografía

[Ak] A.G. Akritas. *Elements of computer algebra, with applications*. Wiley, 1989.

[Ca] R. Calinger (Ed.). *Classics of Mathematics*. Prentice-Hall, 1995.

[Cam] O.A. Cámpoli. A Principal Ideal Domain That Is Not a Euclidean Domain. Amer. Math. Monthly 95 (1988), 868–871.

[Cl] A. Clark. *Elementos de álgebra abstracta*. Alhambra, 1987.

[De-Fu-Xa] F. Delgado, C. Fuertes, S. Xambó. *Introducción al álgebra (Anillos, factorización y teoría de cuerpos)*. Universidad de Valladolid, 1998.

[Do-He] J.R. Dorronsoro, E. Hernández. *Números, grupos y anillos*. Addison-Wesley Iberoamericana–UAM, 1996.

[Ed] H.M. Edwards. *Galois Theory*. Springer, 1998.

[Es] *J.-P. Escofier. *Galois Theory*. Graduate Texts in Mathematics 204, Springer-Verlag, 2001.

[Ga] J.A. Gallian. *Contemporary Abstract Algebra*. Houghton Mifflin Company, 2002.

[Gal] E. Galois. *Oeuvres Mathèmatiques publièes en 1846 dans le Journal de Liouville*. Jacques Gabay, 1989.

[Gar] D.J.H Garling. *A course in Galois Theory*. Cambridge University Press, 1986.

[Gau] C.F. Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, 1986.

[Ha] C.R. Hadlock. *Field Theory and its Classical Problems*. The Mathematical Association of America, 1978.

[Ja] N. Jacobson. *Lectures in Abstract Algebra*. Vol.3. Theory of fields and Galois theory. Van Nostrand, 1964.

[Ka] I. Kaplansky. *Fields and Rings*. University of Chicago Press, 1974.

[Kl] M. Kline. *Mathematical thought from ancient to modern times*. Oxford University Press, 1972.

[Mo] *P. Morandi. *Field and Galois Theory*. Graduate Texts in Mathematics 167. Springer-Verlag, 1995.

[Ri] P. Ribenboim. *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, 1979.

[Ro] *S. Roman. *Field Theory*. Graduate Texts in Mathematics 158. Springer-Verlag, 1998.

[Rot] T. Rothman. *Genius and biographers: the fictionalization of Evariste Galois*. Amer. Math. Monthly 89 (1982), 84–106.

[Rotm] J.J. Rotman. *Galois Theory*. Springer-Verlag, 1990.

[Sm] D.E. Smith. *A Source Book in Mathematics*. Dover Publications Inc., 1959.

[St] I. Stewart. *Galois Theory*. Chapman and Hall, 1973.

[Ve] F. Vera. *Científicos griegos* Vol I,II. Aguilar, 1970.

(Un asterisco indica una referencia de mayor nivel de dificultad).