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

$$(G/N)\big/(H/N) \cong G/H.$$

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:

$$(G_i \cap H) \cdot G_{i-1}\big/G_{i-1} \cong (G_i \cap H)\big/(G_{i-1} \cap H).$$

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 $A_3 \lhd S_3$ 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.