Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

Resolución por radicales de ecuaciones algebraicas

Autora: Carmen Gómez Cambronero
Tutor: Félix Delgado de la Mata
Curso 2024-2025

Índice general

1. El problema de la resolubilidad por radicales. **3**
1.1. La historia del problema y su interés. . . . 3
1.2. Fórmula de Cardano-Tartaglia para la cúbica. . . . 4
1.3. Algunos detalles importantes. . . . 6

2. Polinomios simétricos. Grupos resolubles. **9**
2.1. Revisión del grupo simétrico y del grupo alternado. . . . 9
2.1.1. Grupo simétrico. . . . 9
2.1.2. Grupo alternado. . . . 10
2.2. Polinomios simétricos. . . . 11
2.3. Grupos resolubles. . . . 16
2.3.1. Definición y propiedades. . . . 16
2.3.2. Grupos simples. El grupo S_n. . . . 20

3. Extensiones no resolubles. **23**
3.1. Revisión de Teoría de Galois. . . . 23
3.1.1. Grupo de Galois de un polinomio. . . . 25
3.2. Extensiones radicales y resolubles. . . . 27
3.3. La extensión $X^n - a$. . . . 29
3.4. Teorema de Galois: Extensión resoluble implica grupo resoluble. . . . 31
3.5. Polinomios no resolubles por radicales. El Teorema de Abel. . . . 34
3.5.1. La ecuación general de grado n. . . . 35
3.5.2. Teorema de Abel. . . . 36

4. Extensiones resolubles. El Teorema de Galois. **37**
4.1. Resolventes de Lagrange. . . . 37
4.2. Teorema de Galois: Grupo resoluble implica extensión resoluble. . . . 40
4.3. Regreso a la cúbica. . . . 41

5. Resolubilidad real. **45**
5.1. Radicales reales. . . . 45
5.2. Polinomios irreducibles con raíces radicales reales . . . 47

Resumen

En este trabajo se estudia el problema de resolución por radicales de ecuaciones algebraicas en base a la teoría de Galois. Se empieza describiendo la importancia histórica del problema, así como uno de los métodos clásicos más conocidos (la fórmula de Cardano-Tartaglia para la cúbica) y un estudio de las posibles soluciones según el discriminante. Se presenta también el concepto de grupo resoluble y se estudian sus propiedades, particularmente el ejemplo del grupo simétrico, y su aplicación a los polinomios simétricos. Se formaliza la expresión de ecuaciones resolubles por radicales al presentar los conceptos de extensión radical y extensión resoluble, y finalmente, se demuestran los teoremas de Abel y de Galois, presentando también la técnica de las resolventes de Lagrange para la resolución de la cúbica. Por último, se realiza un estudio de la resolubilidad en el cuerpo de los números reales.

Abstract

In this project we study the problem of solvability by radicals based on Galois theory. We begin by describing its historical importance, as well as one of the best known classical methods (Cardano-Tartaglia's formula for the cubic) and a discussion on the possible solutions according to the discriminant. We also present the concept of solvable group and study its properties, especially the example of the symmetric group, and its application to symmetric polynomials. The expression of equations tha are solvable by radicals is formalized by presenting the concepts of radical extension and solvable extension, and finally, we prove the theorems of Abel and Galois, presenting also the technique of Lagrange's resolvents for the resolution of the cubic. Lastly, we discuss solvability in the field of real numbers.

Introducción

La estudio y la resolución de las ecuaciones algebraicas, o equivalentemente, el cálculo de las raíces de un polinomio, es uno de los problemas más antiguos de la historia de las matemáticas. El estudio de la existencia de estas raíces, así como la búsqueda de métodos para el cálculo de las mismas, ha llevado a la creación de nuevos conceptos (como por ejemplo, los números complejos) y de nuevas ramas de estudio.

Conviene decir que, en el contexto clásico, cuando hablamos de calcular las raíces de un polinomio, nos referimos a la expresión de las raíces mediante fórmulas cerradas, definidas a partir de los coeficientes y que involucran operaciones algebraicas conocidas, incluyendo el cálculo de raíces de un número: pensamos, por ejemplo, en las raíces de la ecuación de segundo grado o en las raíces de $X^3 - 2$.

La comprensión de las raíces de un polinomio evoluciona en este sentido hasta el desarrollo de la Teoría de Galois, que es el contexto en el que enunciaremos este trabajo. Precisamente la no existencia de fórmulas cerradas para las raíces de un polinomio es también un factor importante para le evolución del cálculo aproximando por otros métodos y el desarrollo de los métodos numéricos.

La teoría de Galois, en esencia, pone en relación la teoría de cuerpos y la de grupos. Uno de sus resultados principales es el Teorema de Galois que afirma que una ecuación es resoluble por radicales si y solo si lo es su grupo de Galois. El objetivo de este trabajo es, primero explicar qué significa esta afirmación y segundo, demostrarla.

En el contexto de los estudios de Grado en Matemáticas de la Universidad de Valladolid, la teoría de Galois es el fin esencial de la asignatura de "Ecuaciones Algebraicas". Sin embargo, por razones de tiempo, el problema de la resolubilidad (tanto el Teorema de Galois como el de Abel) queda, lamentablemente, fuera de los contenidos del curso. Su importancia en las matemáticas, junto con la elegancia de los resultados, hace que, en nuestra opinión, sea un tema muy adecuado para un TFG.

La organización de la memoria sigue el esquema siguiente: en primer lugar, en el Capítulo 1, empezaremos situando el problema en su contexto histórico viendo alguno de los métodos clásicos más importantes: la fórmula de Cardano-Tartaglia para la resolución de la cúbica. Continuaremos presentando algunas ideas más modernas, que serán las herramientas necesarias para entender y probar el teorema de Galois. Puesto que el teorema relaciona la estructura de los grupos con la de las extensiones de cuerpos, necesitaremos hacer una revisión de la teoría básica de ambas partes, además de definir nuevos conceptos.

Así, el Capítulo 2 se dedica a revisar los conceptos de teoría de grupos necesarios y ya conocidos como preludio del estudio de los grupos resolubles. El papel central del grupo simétrico se pone también de manifiesto incluyendo el estudio de los polinomios simétricos.

El Capítulo 3, después de una revisión de la Teoría de Galois, se dedica al estudio de

las extensiones resolubles que son el punto fundamental de la memoria. En este capítulo se prueba la primera parte del Teorema de Galois: el grupo de Galois de una extensión resoluble es resoluble. Este resultado permite ya demostrar la imposibilidad de resolver por radicales polinomios de grado mayor o igual a 5. Más aún, el Teorema de Abel (que probamos al final del capítulo) muestra que la ecuación general de grado > 4 no se puede resolver por radicales.

El Capítulo 4 se dedica a completar la prueba del Teorema de Galois, es decir, que si el grupo de Galois de una extensión es resoluble, entonces la extensión es resoluble. Para ello necesitaremos estudiar primero las resolventes de Lagrange, que además serán de utilidad para expresar las raíces de la cúbica mediante radicales, usando un método diferente.

Para terminar, en el capítulo 5, estudiaremos qué ocurre si se restringe el problema al caso real, lo que proporciona resultados muy interesantes.

Capítulo 1

El problema de la resolubilidad por radicales.

En este capítulo haremos un repaso por la historia, viendo cómo se enfrentaron los matemáticos al problema de la obtención de raíces de ecuaciones algebraicas y cómo esto motivó la creación de nuevos resultados y conceptos matemáticos, entre ellos la teoría de Galois
Detallaremos también uno de los métodos clásicos más importantes para la resolución de la cúbica: la fórmula de Cardano-Tartaglia.

Para la introducción histórica seguiremos el libro de Stewart [7] y el artículo de Rzedowski [6]. Para el estudio de la fórmula se siguen los textos de Delgado-Fuertes-Xambó [3] e Ivorra [4].

1.1. La historia del problema y su interés.

La resolución de ecuaciones polinómicas es un problema que se remonta a las primeras civilizaciones. En el antiguo Egipto, ya se planteaban problemas que se resolvían mediante ecuaciones de primer grado, y existen tablillas babilónicas que datan de alrededor del año 1600 a.C. en las que se describen métodos para la resolución de la ecuación de segundo grado. Estos métodos, que en la actualidad equivalen al método de completación de cuadrados, proporcionan la conocida fórmula general de la ecuación $aX^2 + bX + c = 0$, con $a \neq 0$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

El problema de obtención de raíces aparece en diversas partes del mundo, como Grecia ($\sim$ 300 a.C.), China ($\sim$ 200 a.C.) o la India ($\sim$ 500 d.C.), aunque cabe destacar que en ninguno de estos casos el problema se planteaba desde un punto de vista algebraico (y de hecho, la notación necesaria no apareció hasta el siglo primero d.C.) si no mediante construcciones geométricas.

En el caso de la ecuación cúbica, en cambio, no se halló una fórmula general hasta el siglo XVI. Aunque había resoluciones para ejemplos particulares, que se conocían desde la antigua Grecia, la cúbica general fue resuelta por matemáticos italianos durante el Renacimiento: primero por del Ferro en 1515 y más tarde, en 1535, por Tartaglia, aunque no fue hasta 1545 que la fórmula fue publicada por Cardano, en su obra *Ars Magna*. Las

ecuaciones que resolvieron fueron

$$X^3 + pX = q, \qquad X^3 = pX + q \qquad \text{y} \qquad X^3 + q = pX,$$

que por aquel entonces eran consideradas distintas, ya que no se reconocía la existencia de los número negativos. La fórmula, que detallaremos en la sección 1.2, es similar a la de segundo grado, en el sentido de que solo involucraba los coeficientes del polinomio, las operaciones elementales (suma, resta, multiplicación y división) y la extracción de raíces. A este tipo de obtención de raíces la llamaremos de ahora en adelante, *resolución mediante radicales* y será el tema central de este trabajo.

La ecuación general de grado 4 la resolvió Ferrari, alumno de Cardano, al observar que el problema podía reducirse a la resolución de una ecuación cúbica (de forma similar a cómo la cúbica puede reducirse a una ecuación de grado 2). La solución, publicada también en el *Ars Magna*, podía obtenerse mediante radicales y parecía indicar que todas la ecuaciones se podrían resolver de tal manera.

Sin embargo, todos los posteriores intentos para resolver la quíntica fracasaron. Lagrange probó un nuevo método (utilizando las resolventes de Lagrange, como veremos en la sección 4.3) para la resolución de las ecuaciones cúbica y cuártica en términos de permutaciones de sus raíces, y observó que fallaba para la quíntica. También Gauss, al estudiar la construcción de polígonos regulares, observó que los polinomios de grado > 4 no se podían reducir a algún grado menor, lo cual llevó a pensar que la quíntica no se podía resolver por radicales. Fue Ruffini el primero en tratar de probar esto, usando grupos de permutaciones. Sin embargo, no lo logró. En 1824, Abel consiguió completar la demostración errónea de Ruffini y probó finalmente que la quíntica no es una ecuación resoluble por radicales.

Es importante destacar que esto no significa que ninguna ecuación de grado 5 pueda resolverse: el Teorema Fundamental del Álgebra prueba que si admitimos soluciones complejas, estas raíces existen siempre, y se pueden calcular aproximaciones suficientemente exactas de diversas maneras. Tampoco significa que es imposible hallar raíces de esta forma para ninguna quíntica (existen ecuaciones concretas que sí se pueden resolver mediante extracción de radicales, como por ejemplo $X^5 - 1 = 0$). Simplemente se refiere a que, en general, las raíces de las ecuaciones de grado > 4 no siempre podrán expresarse en función de radicales.

Solo faltaba generalizar el resultado. Aquí es donde entra la teoría de Galois, que surgió precisamente a raíz de este problema. Galois probó que una ecuación es resoluble por radicales si, y solamente si el grupo de permutaciones de sus raíces (conocido en la actualidad como grupo de Galois) es resoluble. Este resultado es conocido como el Teorema de Galois y es uno de los resultados esenciales de esta teoría, debido a su importancia histórica.

1.2. Fórmula de Cardano-Tartaglia para la cúbica.

A continuación detallaremos la resolución para la cúbica que halló Tartaglia (aunque la fórmula lleva también el nombre de Cardano por ser él quien la publicó). Notemos que la demostración no será idéntica a la clásica, principalmente por el uso que haremos de las raíces de la unidad y los números complejos, pues tradicionalmente no solían considerarse

a la hora de resolver ecuaciones, ya que estas soluciones "no existían".

Consideramos la ecuación general de tercer grado

$$a_0X^3 + a_1X^2 + a_2X + a_3 = 0,$$

con $a_0, a_1, a_2, a_3 \in \mathbb{Q}$, $a_0 \neq 0$. Para calcular sus raíces, empezamos por simplificar la ecuación dividiendo entre a_0. Así obtenemos la ecuación

$$X^3 + aX^2 + bX + c = 0,$$

y sustituyendo X por $Y - a/3$ (transformación de Tschirnhausen), llegamos a la ecuación

$$Y^3 + pY + q = 0, \tag{1.1}$$

donde, los coeficientes son

$$p = -\frac{a_1^2}{3a_0^2} + \frac{a_2}{a_0} \qquad \text{y} \qquad q = \frac{2a_1^3}{27a_0^3} - \frac{a_1a_2}{3a_0^2} + \frac{a_3}{a_0}.$$

Podemos suponer $p, q \neq 0$ ya que en el caso de que algún coeficiente fuese nulo, el problema se reduciría a uno ya conocido. En la ecuación obtenida, hacemos el cambio de variable $Y = u + v$, y observamos que

$$Y^3 = (u+v)^3 = u^3 + 3uv(u+v) + v^3 = u^3 + v^3 + 3uvY,$$

luego se tiene que

$$Y^3 - 3uvY - u^3 - v^3 = 0. \tag{1.2}$$

Igualando los coeficientes de las ecuaciones (1.1) y (1.2), se llega a $p = -3uv$, $q = -u^3 - v^3$. Por tanto, tenemos que

$$u^3 + v^3 = -q \qquad \text{y} \qquad u^3v^3 = -p^3/27$$

y como consecuencia, u^3 y v^3 serán las raíces del polinomio $Z^2 + qZ - p^3/27 = 0$ (fórmulas de Cardano-Vieta). Luego

$$u^3 = \frac{-q + \sqrt{q^2 + 4p^3/27}}{2}, \quad v^3 = \frac{-q - \sqrt{q^2 + 4p^3/27}}{2}.$$

Entonces, podemos tomar

$$u = \sqrt[3]{\frac{-q + \sqrt{q^2 + 4p^3/27}}{2}}, \quad v = \sqrt[3]{\frac{-q - \sqrt{q^2 + 4p^3/27}}{2}},$$

y se llega a que una solución de la ecuación 1.1 es

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

La expresión anterior no es más que la forma simbólica clásica para expresar las raíces de la ecuación. En efecto, sabemos que $\frac{-q+\sqrt{q^2+4p^3/27}}{2}$ tiene 3 raíces cúbicas complejas a las que llamaremos u_1, u_2, u_3. Fijando una de ellas como $u = u_1$, las dos restantes se obtienen como $u_2 = \xi u$ y $u_3 = \xi^2 u$, siendo $\xi = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$ una raíz cúbica primitiva

de la unidad. De la misma forma, llamamos v_1, v_2, v_3 a las raíces de $\frac{-q-\sqrt{q^2+4p^3/27}}{2}$. La relación $uv = -p/3$ indica cómo combinar las raíces u_1, u_2, u_3 con v_1, v_2, v_3 para obtener el resto e soluciones de la ecuación 1.1. Es decir, si $u = u_1$, entonces $v_1 = -p/3u = v$. Se obtiene fácilmente que $v_2 = -p/3u_2 = \xi^2 v$ y $v_3 = -p/3u_3 = \xi v$. Así pues, las 3 raíces de (1.1) son:

$$y_1 = u + v, \quad y_2 = \xi u + \xi^2 v \quad \text{y} \quad y_3 = \xi^2 u + \xi v.$$

Para hallar la soluciones de la ecuación original, bastaría con deshacer la transformación sustituyendo los coeficientes p y q por sus valores en función de a_0, a_1, a_2, a_3.

1.3. Algunos detalles importantes.

Vamos a estudiar cómo son las raíces de (1.1) en función del discriminante (ver 3.4). Sea $\mathcal{D} = q^2 + \frac{4p^3}{27}$ el discriminante de la ecuación

$$Z^2 + qZ - \frac{p^3}{27} = 0. \tag{1.3}$$

Dependiendo del valor de $\mathcal{D}$, podremos separar en distintos casos los tipos de soluciones de esta ecuación, que a su vez nos indicará cómo son las soluciones de (1.1).

- Si $\mathcal{D} = 0$, la ecuación (1.3) tiene una solución real doble, $z = -q/2$. Si $u = \sqrt[3]{-q/2}$ es la raíz cúbica real de $-q/2$, las raíces de (1.1) serán entonces

  $$y_1 = 2\sqrt[3]{-q/2}, \qquad y_2 = (\xi + \xi^2)\sqrt[3]{-q/2},$$

  donde esta última tiene multiplicidad 2. (Obsérvese que $y_2 = -\sqrt[3]{-q/2}$ puesto que $\xi + \xi^2 = \xi + \overline{\xi} = -1$). Luego en este caso, todas las raíces de $Y^3 + pY + q = 0$ son reales, y una de ellas es doble.

- Si $\mathcal{D} > 0$, la ecuación (1.3) tiene dos raíces reales $z_1 = \frac{-q+\sqrt{\mathcal{D}}}{2}$ y $z_2 = \frac{-q-\sqrt{\mathcal{D}}}{2}$. Si llamamos $u = \sqrt[3]{z_1}$ y $v = \sqrt[3]{z_2}$ a las raíces cúbicas reales, como antes, se tiene que las raíces de (1.1) son

  $$y_1 = u + v, \qquad y_2 = -\frac{u+v}{2} + i\frac{\sqrt{3}}{2}(u+v), \qquad y_3 = -\frac{u+v}{2} - i\frac{\sqrt{3}}{2}(u+v).$$

  Es decir, en este caso $Y^3 + pY + q = 0$ tiene una raíz real y_1 y dos raíces complejas conjugadas, y_2 e $y_3 = \overline{y_2}$.

- Si $\mathcal{D} < 0$, la ecuación (1.3) tiene dos raíces complejas conjugadas, $z_1 = \frac{-q+i\sqrt{|\mathcal{D}|}}{2}$ y $z_2 = \frac{-q-i\sqrt{|\mathcal{D}|}}{2} = \overline{z_1}$. Tomando como antes $u = \sqrt[3]{z_1}$ y $v = \sqrt[3]{z_2}$, se tiene que las raíces de (1.1) son

  $$y_1 = u + \overline{u}, \qquad y_2 = \xi u + \overline{\xi u}, \qquad y_3 = \xi^2 u + \overline{\xi^2 u},$$

  pues se tiene que $v = \overline{u}$ (y $\overline{\xi} = \xi^2$). Observamos que estas raíces son todas reales, por ser suma de un número complejo y su conjugado.
  Este caso, conocido como *casus irreducibilis* (o "caso irreducible"), es particularmente interesante pues se utilizan números complejos para la obtención de raíces reales. Como hemos mencionado antes, tradicionalmente las soluciones complejas no eran válidas (simplemente se consideraba que la ecuación no tenía solución), pero existen

múltiples ejemplos de ecuaciones que claramente tienen soluciones reales (como por ejemplo, $X^3 - 15X - 4 = 0$, que se anula en $X = 4$) y sin embargo, la fórmula proporciona una solución en función de números complejos:

$$X = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}.$$

Este hecho llevó a los matemáticos a plantearse que quizá era necesario ampliar al conjunto de posibles soluciones y a considerar el estudio de los números complejos.

El discriminante de la ecuación $Y^3 + pY + q$ es $D = -4p^3 - 27q^2 = -27\mathcal{D}$. Por lo tanto, los casos anteriores son:

Proposición 1.1. *Dado el polinomio $X^3 + pX + q$, sea $D = -4p^3 - 27q^2$ su discriminante. Entonces:*

- *Si $D \geq 0$, entonces todas las raíces de $X^3 + pX + q = 0$ son reales. En particular, si $D = 0$, una de las raíces será doble.*
- *Si $D < 0$, entonces $X^3 + pX + q = 0$ tendrá una raíz real y dos raíces complejas conjugadas.*

Capítulo 2

Polinomios simétricos. Grupos resolubles.

El objetivo de este capítulo es presentar y estudiar las propiedades básicas de los grupos resolubles. Dichos grupos son el reflejo (gracias a la teoría de Galois) en la teoría de grupos de la caracterización de los polinomios cuyas raíces de expresan con radicales. Puesto que el ejemplo fundamental de grupo no resoluble es el grupo simétrico, se comienza con una revisión sucinta del mismo. Posteriormente se aplica (sección 2.2) al estudio de los polinomios simétricos. La sección final se dedica al estudio propiamente dado de los grupos resolubles.

Este capítulo está basado principalmente en la sección 2.7 de [3] y la sección 3.13 de [2].

2.1. Revisión del grupo simétrico y del grupo alternado.

2.1.1. Grupo simétrico.

El conjunto de permutaciones de un conjunto X (es decir, de biyecciones de X en X), que denotaremos por S_X, es un grupo no conmutativo con la composición de aplicaciones. En el caso de $X = \{1, \dots, n\}$ lo llamaremos *grupo de permutaciones de n elementos*, o *grupo simétrico*, y lo denotaremos por S_n. Es evidente que $|S_n| = n!$.

Representaremos la permutación $\boldsymbol{i} \in S_n$ mediante la n-upla $[i_1, \dots, i_n]$, donde $i_j = \boldsymbol{i}(j)$ para cada $j = 1, \dots, n$.

Un tipo particular son las *permutaciones cíclicas*: si $k_1, \dots, k_r \in \{1, \dots, n\}$, representaremos por $(k_1, \dots, k_r)$ la permutación $\boldsymbol{i} \in S_n$ dada por

$$\boldsymbol{i}(k_l) = \begin{cases} k_l & \text{si } l \notin \{1, \dots, r\}, \\ k_{l+1} & \text{si } 1 \leq l < r, \\ k_1 & \text{si } l = r. \end{cases}$$

También se les llama *r-ciclos* o *ciclos de orden r*, pues $\boldsymbol{i}^r(k) = k$ para todo $k \in \{1, \dots, n\}$. A los ciclos de orden 2 se los llama *trasposiciones*.

Un resultado importante es que los ciclos disjuntos (es decir, aquellos cuyos conjuntos de índices son disjuntos) conmutan. Además, se tiene el siguiente resultado:

Proposición 2.1. *Sea $\boldsymbol{i} \in S_n$, $\boldsymbol{i} \neq 1$. Entonces $\boldsymbol{i}$ es composición de ciclos disjuntos dos a dos. En particular, $\boldsymbol{i}$ es producto de trasposiciones, pues cada r-ciclo lo podemos escribir*

de la siguiente manera:

$$(k_1, k_2, \ldots, k_r) = (k_1, k_2) \circ (k_2, k_3) \circ \cdots \circ (k_{r-1}, k_r).$$

Esto nos da un conjunto generador del grupo simétrico, aunque no el único.

Proposición 2.2. *El conjunto*

$$\{(1,2), (2,3), \ldots, (n-1, n)\},$$

es un conjunto de generadores del grupo simétrico S_n. También lo serán los conjuntos

$$\{(1,2), (1,3), \ldots, (1,n)\} \quad y \quad \{(1,2), (1,2,\ldots,n)\}.$$

Otro concepto importante es el de *signo* de una permutación $\boldsymbol{i}$, definido como la aplicación $\varepsilon : S_n \longrightarrow \{\pm 1\}$ dada por

$$\varepsilon(\boldsymbol{i}) = \begin{cases} +1 & \text{si } \boldsymbol{i} \text{ es par,} \\ -1 & \text{si } \boldsymbol{i} \text{ es impar,} \end{cases}$$

donde que $\boldsymbol{i}$ sea *par* significa que tiene una cantidad par de pares inversos (es decir, pares $\{i_k, i_h\}$ con $i_k > i_h$ cuando $k < h$), e *impar* el caso contrario.

Por ejemplo, las permutaciones $\boldsymbol{i} = [3,1,4,5,2]$, $\boldsymbol{j} = [4,3,2,5,1] \in S_5$ son respectivamente par e impar, pues los pares inversos de $\boldsymbol{i}$ son

$$\{3,1\},\ \{3,2\},\ \{4,2\}\ \text{ y }\ \{5,2\},$$

y los de $\boldsymbol{j}$ son

$$\{4,3\},\ \{4,2\},\ \{4,1\},\ \{3,2\},\ \{3,1\},\ \{2,1\}\ \text{ y }\ \{5,1\}.$$

En particular, la identidad es una permutación par, y las trasposiciones son siempre impares.

Se tiene el siguiente resultado:

Proposición 2.3. *Sean $\boldsymbol{i}, \boldsymbol{j} \in S_n$. Se tiene que $\varepsilon(\boldsymbol{j} \circ \boldsymbol{i}) = \varepsilon(\boldsymbol{j})\varepsilon(\boldsymbol{i})$.*
Por lo tanto, la aplicación $\varepsilon\colon S_n \longrightarrow \{\pm 1\}$ es un homomorfismo de grupos.

Como consecuencia, se tendrá que si $\boldsymbol{i} \in S_n$ es producto de exactamente r-trasposiciones, entonces $\varepsilon(\boldsymbol{i}) = (-1)^r$.

2.1.2. Grupo alternado.

Observamos que el núcleo de la aplicación signo está formado justamente por las permutaciones pares de S_n. A este conjunto lo llamaremos *grupo alternado* y lo denotaremos por $A_n = \ker(\varepsilon)$.
En particular, es un subgrupo normal de S_n y por tanto la aplicación ε induce un isomorfismo $S_n/A_n \simeq \{\pm 1\}$, luego $[S_n\colon A_n] = 2$.

Para $n \geq 3$ y para todos i, j, k, l índices distintos, se cumplen las siguientes igualdades:

1. $(i,j)(j,k) = (i,j,k)$,
2. $(i,j)(k,l) = (i,j,k)(j,k,l)$,
3. $(i,j,k) = (i,j,1)(1,j,k)$,
4. $(1,i,j) = (1,2,j)(1,2,i)^2$.

Estas igualdades prueban la siguiente proposición:

Proposición 2.4. *Si $n \geq 3$, el conjunto*

$$\{(1,2,3),(1,2,4),\ldots,(1,2,n)\},$$

es un conjunto de generadores del grupo alternado A_n.

2.2. Polinomios simétricos.

Vamos a considerar un dominio de integridad A y $X_1,\ldots,X_r$ indeterminadas, con $r \in \mathbb{Z},\ r \geq 1$. Dada $\tau \in S_r$ una permutación de $\{1,\ldots,r\}$, denotamos por $X_{\tau(1)},\ldots,X_{\tau(r)}$ las indeterminadas reordenadas según esta permutación. Definimos la aplicación

$$\begin{array}{rccc} \Phi_\tau\colon & A[X_1,\ldots,X_r] & \longrightarrow & A[X_1,\ldots,X_r] \\ & f & \longmapsto & f^\tau \end{array}$$

que permuta las indeterminadas del polinomio $f \in A[X_1,\ldots,X_r]$, es decir, tal que $f^\tau(X_1,\ldots,X_r) = f(X_{\tau(1)},\ldots,X_{\tau(r)})$. La aplicación Φ_τ es un automorfismo (su inversa se define tomando la permutación inversa de τ, $\Phi_\tau^{-1} = \Phi_{\tau^{-1}}$). Observamos que, además, la aplicación que asigna a cada permutación τ su correspondiente Φ_τ,

$$\begin{array}{ccc} S_r & \longrightarrow & Aut(A[X_1,\ldots,X_r]) \\ \tau & \longmapsto & \Phi_\tau \end{array}$$

es un homomorfismo.

Definición 2.5. Diremos que un polinomio $f \in A[X_1,\ldots,X_r]$ es *simétrico* si $f^\tau = f$ para cualquier permutación $\tau \in S_r$.
Denotaremos por $A[X_1,\ldots,X_r]^{S_r}$ el conjunto de polinomios simétricos de $A[X_1,\ldots,X_r]$. Es inmediato ver que $A[X_1,\ldots,X_r]^{S_r}$ es un subanillo de $A[X_1,\ldots,X_r]$.

Lema 2.6. *Sea $f \in A[X_1,\ldots,X_r]^{S_r}$. Si f es divisible por X_1, entonces es divisible por $X_1\cdots X_r$.*

Demostración. Sea $f \in A[X_1,\ldots,X_r]^{S_r}$ y supongamos que es divisible por X_1. Entonces, podemos escribirlo como

$$f(X_1,\ldots,X_r) = X_1 g(X_1,\ldots,X_r),$$

con $g \in A[X_1,\ldots,X_r]$. Nótese que por ser f simétrico, g también es simétrico. Además, se tiene que $f^\tau = f$ para todo $\tau \in S_r$. Es decir,

$$f(X_1,\ldots,X_r) = f(X_{\tau(1)},\ldots,X_{\tau(r)}) = X_{\tau(1)} g(X_{\tau(1)},\ldots,X_{\tau(r)}).$$

Luego f es divisible por $X_{\tau(1)}$ para cualquier permutación $\tau \in S_r$. Por tanto, f será divisible por cualquiera de las indeterminadas, y también lo será por el producto de todas ellas, $X_1\cdots X_r$. □

Ejemplo 2.7. Consideramos el polinomio $f = X^3 + aX^2 + bX + c \in A[X]$ cuyas raíces vamos a denotar por α_1, α_2 y α_3. Podemos escribir el polinomio de la forma siguiente

$$f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

Observamos que podemos permutar las raíces sin que cambie f, es decir, f es "simétrico respecto de $\alpha_1, \alpha_2, \alpha_3$". Desarrollando el término de la derecha llegamos a

$$f = X^3 - (\alpha_1 + \alpha_2 + \alpha_3)X^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)X - (\alpha_1\alpha_2\alpha_3),$$

y comparando los coeficientes se tiene que

$$\begin{aligned} a &= -(\alpha_1 + \alpha_2 + \alpha_3), \\ b &= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3), \\ c &= -(\alpha_1\alpha_2\alpha_3). \end{aligned}$$

Evidentemente, la expresión anterior nos dice que a, b, c son "simétricos" respecto a $\alpha_1, \alpha_2, \alpha_3$. Es decir, podemos escribir los coeficientes de un polinomio $f \in A[X]$ como polinomios simétricos en función de sus raíces. Estas fórmulas se generalizan fácilmente en las indeterminadas $X_1, \ldots, X_r$ (ver Fórmulas de Vieta).

Definición 2.8. Sea $k \in \mathbb{Z}$, $1 \leq k \leq r$. Definimos el *k-ésimo polinomio simétrico elemental* como

$$\sigma_k = \sum_{1 \leq i_1 < \ldots < i_k \leq r} X_{i_1} \cdots X_{i_k}.$$

Los denotaremos también por $\sigma_k = \sigma_k(X_1, \ldots, X_r)$.

Ejemplo 2.9. Los polinomio simétricos elementales para $r = 3$ son:

$$\sigma_1 = X_1 + X_2 + X_3, \quad \sigma_2 = X_1X_2 + X_1X_3 + X_2X_3 \quad \text{y} \quad \sigma_3 = X_1X_2X_3$$

Luego podemos escribir el polinomio f del ejemplo 2.7 como

$$X^3 - \sigma_1(\alpha_1, \alpha_2, \alpha_3)X^2 + \sigma_2(\alpha_1, \alpha_2, \alpha_3)X - \sigma_3(\alpha_1, \alpha_2, \alpha_3).$$

Para $r = 4$, los polinomios simétricos elementales son:

$$\begin{aligned} &\sigma_1 = X_1 + X_2 + X_3 + X_4, \quad \sigma_2 = X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4, \\ &\sigma_3 = X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4 \quad \text{y} \quad \sigma_4 = X_1X_2X_3X_4 \end{aligned}$$

Los hemos denotado igual que los polinomios para $r = 3$ para simplificar la escritura, pero claramente, no son iguales. De hecho observamos que los polinomios simétricos elementales para $r = 3$ se pueden obtener a partir de los de $r = 4$ sustituyendo X_4 por 0.

Observación 2.10. Sea $k \in \mathbb{Z}$, $1 \leq k \leq r$. Vamos a denotar por $(\sigma_k)_0$ al polinomio obtenido al sustituir $X_r = 0$ en el k-ésimo polinomio simétrico elemental. Es decir,

$$(\sigma_k)_0 = \sigma_k(X_1, \ldots, X_{r-1}, 0).$$

Se tiene que $(\sigma_1)_0, \ldots, (\sigma_{r-1})_0$ son los polinomios simétricos elementales en $X_1, \ldots, X_{r-1}$.

Proposición 2.11 (Fórmulas de Vieta)**.** *Sean A un dominio, $a_0 \in A$ y $X, X_1, \ldots, X_r$ indeterminadas sobre A. Consideramos $f = a_0(X - X_1)\cdots(X - X_r) \in A[X_1, \ldots, X_r][X]$, polinomio en X con coeficientes en $A[X_1, \ldots, X_r]$. Se puede escribir f de la forma*

$$f = a_0X^r + a_1X^{r-1} + \cdots + a_{r-1}X + a_r,$$

con $a_1, \ldots, a_r \in A[X_1, \ldots, X_r]$. Además, se tiene que $a_k = (-1)^k a_0\sigma_k$, $1 \leq k \leq r$. Es decir,

$$f = a_0X^r - a_0\sigma_1X^{r-1} + \cdots + (-1)^r a_0\sigma_r.$$

Demostración. Vamos a desarrollar la expresión $a_0(X - X_1)\cdots(X - X_r)$ y comprobar que se da la igualdad de coeficientes término a término, en función del grado del monomio, como una generalización del ejemplo 2.7.

- Para grado r, es claro que el coeficiente que acompaña a X^r es a_0.
- Para grado $r - 1$, obtendremos el coeficiente $a_0(-X_1 - \ldots - X_r) = -a_0\sigma_1$.
- Para grado $r - k$, habría que sumar todas las posibles combinaciones de productos con k factores $(-X_{i_1})\cdots(-X_{i_k})$. Es decir, el coeficiente correspondiente a X^{r-k} sería de la forma

  $$a_0 \sum_{1\leq i_1<\ldots<i_k\leq r} (-X_{i_1})\cdots(-X_{i_k}) = a_0(-1)^k \sum_{1\leq i_1<\ldots<i_k\leq r} X_{i_1}\cdots X_{i_k},$$

  y teniendo en cuenta que $\sigma_k = \sum_{1\leq i_1<\ldots<i_k\leq r} X_{i_1}\cdots X_{i_k}$ llegamos a que el coeficiente será $(-1)^k a_0\sigma_k$.
- Para grado 0, el coeficiente será $a_0(-X_1)\cdots(-X_r) = (-1)^r a_0(X_1\cdots X_r) = (-1)^r a_0\sigma_r$.

Por lo tanto, se tiene que

$$a_0(X - X_1)\cdots(X - X_r) = a_0X^r - a_0\sigma_1X^{r-1} + \cdots + (-1)^r a_0\sigma_r,$$

que es lo que queríamos obtener. □

Definición 2.12. Definimos el *peso* de un monomio $X_1^{n_1}\cdots X_r^{n_r}$ como

$$p(\mathbf{n}) = p(n_1, \ldots, n_r) = n_1 + 2n_2 + \cdots + rn_r,$$

donde $\mathbf{n} = (n_1, \ldots, n_r) \in \mathbb{N}^r$. El *peso* de un polinomio no nulo $f = \sum_{\mathbf{n}\in\mathbb{N}^r} a_{\mathbf{n}}X_1^{n_1}\cdots X_r^{n_r}$, será el máximo de los pesos de los monomios no nulos de f, es decir,

$$p(f) = \text{máx}\{p(\mathbf{n}) | a_{\mathbf{n}} \neq 0\}.$$

En el caso de $f = 0$, diremos que su peso es $p(f) = -\infty$.

Proposición 2.13. *Sea $f \in A[X_1, \ldots, X_r]^{S_r}$ un polinomio simétrico de grado d. Existe un polinomio $g \in A[Y_1, \ldots, Y_r]$ con peso d tal que*

$$f = g(\sigma_1, \ldots, \sigma_r).$$

Demostración. Razonamos por inducción sobre el número de indeterminadas.

- Si $r = 1$, se tiene que $S_1 = 1$ y $\sigma_1 = X_1$, luego dado un polinomio $f \in A[X_1]$ de grado d, basta tomar $g = f$.

- Ahora suponemos que el teorema es cierto para $r-1$ indeterminadas, con $r>1$. Comprobamos que también se cumple para r indeterminadas, razonando de nuevo por inducción, pero esta vez sobre el grado del polinomio.

  - Si suponemos $d=0$, f sería constante y nuevamente podemos tomar $g=f$.
  - Para terminar, supongamos que para cualquier polinomio en $A[X_1,\dots,X_r]^{S_r}$ de grado menor que $d>0$ el teorema se verifica. Consideramos $f\in A[X_1,\dots,X_r]^{S_r}$ de grado d. ¿Existirá $g\in A[Y_1,\dots,Y_r]$ de peso d tal que $f=g(\sigma_1,\dots,\sigma_r)$? Consideramos el polinomio que se obtiene al hacer $X_r=0$ en f y lo denotamos por f_0. Es decir, $f_0=f(X_1,\dots,X_{r-1},0)$ es un polinomio de $A[X_1,\dots,X_{r-1}]^{S_{r-1}}$ de grado $\leq d$, luego por hipótesis de inducción (sobre r), sabemos que existe $g_1\in A[Y_1,\dots,Y_{r-1}]$ de peso $\leq d$ tal que $f_0=g_1((\sigma_1)_0,\dots,(\sigma_{r-1})_0)$. Se considera el polinomio

$$f_1(X_1,\dots,X_r)=f(X_1,\dots,X_r)-g_1(\sigma_1,\dots,\sigma_{r-1}),$$

    cuyo grado será $\leq d$ puesto que $gr(f)=d$ y $gr(g_1)\leq d$ (pues g_1 tiene peso $\leq d$). También f_1 será un polinomio simétrico, por serlo f y g_1. Observamos, por otro lado, que

$$f_1(X_1,\dots,X_{r-1},0)=f_0-g_1((\sigma_1)_0,\dots,(\sigma_{r-1})_0)=0,$$

    y por tanto, f_1 es divisible por X_r, luego también lo será por $X_1\cdots X_r$ (según hemos visto en el lema 2.6). Es decir,

$$f_1=X_1\cdots X_r f_2(X_1,\dots,X_r)=\sigma_r f_2,$$

    para algún polinomio $f_2\in A[X_1,\dots,X_r]$. Tal polinomio será simétrico y su grado será $\leq d-r<d$. Entonces, por hipótesis de inducción (sobre d), se tiene que existe un cierto polinomio $g_2\in A[Y_1,\dots,Y_r]$ de peso $\leq d-r$ tal que $f_2=g_2(\sigma_1,\dots,\sigma_r)$. Por consiguiente,

$$\begin{aligned} f(X_1,\dots,X_r) &= g_1(\sigma_1,\dots,\sigma_{r-1})+f_1(X_1,\dots,X_r)= \\ &= g_1(\sigma_1,\dots,\sigma_{r-1})+\sigma_r g_2(\sigma_1,\dots,\sigma_r). \end{aligned}$$

    Visto como polinomio en $Y_1,\dots,Y_r$, lo expresaremos como $g_1+Y_r g_2$ y observamos que su peso es $\leq d$. Pero como $gr(f)=d$, necesariamente el peso de este nuevo polinomio debe ser exactamente d. Luego hemos construido un polinomio $g=g_1+Y_r g_2\in A[Y_1,\dots,Y_r]$ de peso d tal que $f=g(\sigma_1,\dots,\sigma_r)$, como queríamos probar.

□

Proposición 2.14. *Sean A un dominio, $X_1,\dots,X_r$ indeterminadas sobre A y $\sigma_1,\dots,\sigma_r$ los r primeros k-ésimos polinomios simétricos elementales. Entonces,*

$$A[\sigma_1,\dots,\sigma_r]=A[X_1,\dots,X_r]^{S_r}.$$

Demostración. Claramente $\sigma_k\in A[X_1,\dots,X_r]^{S_r}$ para todo $1\leq k\leq r$ (son polinomios simétricos de $A[X_1,\dots,X_r]$). Luego

$$A[\sigma_1,\dots,\sigma_r]\subseteq A[X_1,\dots,X_r]^{S_r}.$$

Veamos que también se verifica la contención opuesta. Dado $f \in A[X_1, \ldots, X_r]^{S_r}$, existirá $g \in A[X_1, \ldots, X_r]$ tal que $f = g(\sigma_1, \ldots, \sigma_r)$, por lo demostrado en la proposición 2.13. Es decir, $f \in A[\sigma_1, \ldots, \sigma_r]$. Luego

$$A[X_1, \ldots, X_r]^{S_r} \subseteq A[\sigma_1, \ldots, \sigma_r],$$

y por tanto, se llega a la igualdad que queríamos probar. □

Consideramos el homomorfismo

$$\begin{array}{rccc} \varphi: & A[Y_1, \ldots, Y_r] & \longrightarrow & A[X_1, \ldots, X_r] \\ & Y_k & \longmapsto & \sigma_k \end{array}$$

para $k = 1, \ldots, r$. Se tiene que $\varphi(g) = g(\sigma_1, \ldots, \sigma_r)$ para cada $g \in A[Y_1, \ldots, Y_r]$. Observamos que la imagen de φ es justamente $A[\sigma_1, \ldots, \sigma_r] = A[X_1, \ldots, X_r]^{S_r}$ (como acabamos de probar). Entonces, se cumple la siguiente proposición:

Proposición 2.15. *En los términos anteriores, la aplicación*

$$\begin{array}{rccc} \varphi: & A[Y_1, \ldots, Y_r] & \longrightarrow & A[X_1, \ldots, X_r]^{S_r} \\ & g & \longmapsto & g(\sigma_1, \ldots, \sigma_r) \end{array}$$

es un isomorfismo.

Demostración. Por la proposición 2.13, φ es un epimorfismo, luego basta probar que es una aplicación inyectiva. Sean $g_1, g_2 \in A[Y_1, \ldots, Y_r]^{S_r}$ tales que $g_1(\sigma_1, \ldots, \sigma_r) = g_2(\sigma_1, \ldots, \sigma_r)$. Consideramos $h = g_1 - g_2$. Entonces, φ será inyectiva si y solo si $h = 0$.
Razonamos mediante inducción sobre r. El caso $r = 1$ es trivial, luego suponemos $r > 1$ y que lo que queremos probar se cumple para $r-1$. Por definición, $\varphi(h) = h(\sigma_1, \ldots, \sigma_r) = 0$. Escribimos h como polinomio en Y_r, es decir,

$$h = h_0 + h_1 Y_r + \ldots + h_d Y_r^d \in A[Y_1, \ldots, Y_{r-1}][Y_r].$$

Puesto que $\varphi(h) = 0$, se obtiene la siguiente relación:

$$h_0(\sigma_1, \ldots, \sigma_{r-1}) + h_1(\sigma_1, \ldots, \sigma_{r-1})\sigma_r + \ldots + h_d(\sigma_1, \ldots, \sigma_{r-1})\sigma_r^d = 0.$$

Sustituyendo $X_r = 0$, se anulan los términos en los que aparece σ_r, luego se tiene que $h_0((\sigma_1)_0, \ldots, (\sigma_{r-1})_0) = 0$. Por hipótesis, $h_0 = 0$.
Luego podemos escribir h como $h = Y_r h'$, con $h' \in A[Y_1, \ldots, Y_r]$. Por lo tanto, como $\varphi(h) = \sigma_r h'(\sigma_1, \ldots, \sigma_r) = 0$, se tiene que $h'(\sigma_1, \ldots, \sigma_r) = 0$.
Para terminar, puesto que $gr(h') < gr(h)$, podemos razonar de forma inductiva reduciendo el grado de h' y llegar a la conclusión de que $h' = 0$. Por tanto, $h = 0$. □

Ejemplos 2.16. La demostración de la proposición 2.13 proporciona un método para expresar un polinomio simétrico $f \in A[X_1, \ldots, X_r]^{S_r}$ como polinomio en $\sigma_1, \ldots, \sigma_r$.

1. Tomemos $f \in A[X, Y, Z]^{S_3}$ dado por

$$f(X, Y, Z) = X^2(Y + Z) + Y^2(X + Z) + Z^2(X + Y).$$

Para empezar, vamos a considerar el polinomio $f_0(X, Y) = f(X, Y, 0) \in A[X, Y]^{S_2}$, que es simétrico. Se tiene que

$$f_0 = X^2 Y + XY^2 = XY(X + Y),$$

y teniendo en cuenta que $\sigma_1 = X + Y + Z$ y $\sigma_2 = XY + XZ + YZ$, obtenemos que

$$f_0 = (\sigma_2)_0(\sigma_1)_0.$$

Escogemos $g_1 \in A[X, Y]$ de tal forma que $g_1((\sigma_1)_0, (\sigma_2)_0) = f_0$. Es decir,

$$g_1(X, Y) = YX.$$

Así, construimos el polinomio $f_1(X, Y, Z) = f(X, Y, Z) - g_1(\sigma_1, \sigma_2)$ que será

$$f_1 = -3XYZ = -3\sigma_3,$$

donde $\sigma_3 = XYZ$. Entonces

$$f(X, Y, Z) = f_1(X, Y, Z) + g_1(\sigma_1, \sigma_2) = -3\sigma_3 + \sigma_1\sigma_2.$$

En conclusión, hemos construido un polinomio $g \in A[X, Y, Z]$ tal que $f = g(\sigma_1, \sigma_2, \sigma_3)$. Este polinomio es de hecho $g(X, Y, Z) = XY - 3Z$ y por lo tanto,

$$f = \sigma_1\sigma_2 - 3\sigma_3.$$

2. Sea $f \in A[X, Y, Z]^3$ el polinomio

$$f(X, Y, Z) = X^3(Y^2 + Z^2) + Y^3(X^2 + Z^2) + Z^3(X^2 + Y^2).$$

De forma análoga, se puede demostrar que

$$f = \sigma_1\sigma_2^2 - \sigma_3(2\sigma_1^2 + \sigma_2),$$

es decir, que $f = g(\sigma_1, \sigma_2, \sigma_3)$ siendo $g \in A[X, Y, Z]$ el polinomio dado por

$$g(X, Y, Z) = XY^2 - Z(2X^2 + Y).$$

2.3. Grupos resolubles.

2.3.1. Definición y propiedades.

Definición 2.17. Sea G un grupo. Llamaremos *torre* de subgrupos a una sucesión de subgrupos de G tales que

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G.$$

Si para cada $i = 0, \ldots, n-1$ se verifica que G_i es un subgrupo normal de G_{i+1}, diremos que es una *torre normal*, y si además el grupo cociente G_{i+1}/G_i es abeliano, diremos que es una *torre abeliana*.

Definición 2.18. Diremos que un grupo G es *resoluble* si tiene una torre abeliana.

Observación 2.19.

- En la definición 2.18, podemos sustituir las inclusiones $G_i \subseteq G_{i+1}$ por inclusiones estrictas $G_i \subset G_{i+1}$.
- Todo grupo abeliano es resoluble.

A continuación demostraremos las principales propiedades de los grupos resolubles, que nos serán de utilidad a lo largo del trabajo.

Proposición 2.20. *Sean G grupo resoluble y H subgrupo de G. Entonces, H es resoluble.*

Demostración. Por ser G resoluble, existirá una torre abeliana de subgrupos de G,

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G,$$

donde e denota el elemento neutro de G (y de H). Para cada $i = 0, \ldots, n$, consideramos $H_i = G_i \cap H$, que será un subgrupo de H (observamos que en particular, $H_0 = \{e\}$ y $H_n = H$). De esta forma construimos una nueva torre de subgrupos

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = H.$$

Para demostrar que H es resoluble, bastará comprobar que esta torre es de hecho abeliana, es decir, que H_i es normal en H_{i+1} y que H_{i+1}/H_i es abeliano, para $i = 0, \ldots, n-1$. Construimos el homomorfismo

$$\begin{array}{rccc} \pi\colon & H_{i+1} & \longrightarrow & G_{i+1}/G_i \\ & h & \longmapsto & hG_i \end{array}$$

que se obtiene al componer la aplicación de inclusión de H_{i+1} en G_{i+1} con la proyección canónica. Observamos que, dado $h \in H_{i+1}$,

$$h \in \ker(\pi) \quad \Leftrightarrow \quad \pi(h) = eG_i \quad \Leftrightarrow \quad hG_i = G_i \quad \Leftrightarrow \quad h \in G_i.$$

Luego h pertenecerá al núcleo de π si y solo si $h \in H_{i+1} \cap G_i = H \cap G_{i+1} \cap G_i = H \cap G_i = H_i$. Es decir $\ker(\pi) = H_i$ y por tanto, $H_i \lhd H_{i+1}$, $i = 0, \ldots, n-1$. Por último, aplicamos el primer teorema de isomorfía y se llega a que

$$H_{i+1}/H_i = H_{i+1}/\ker(\pi) \simeq \pi(H_{i+1}) \subseteq G_{i+1}/G_i,$$

luego para $i = 0, \ldots, n-1$, H_{i+1}/H_i será abeliano, al ser isomorfo a un subgrupo de un grupo abeliano. Así, queda probado que H contiene una torre abeliana y es por tanto resoluble. □

Proposición 2.21. *Sean G grupo resoluble y N subgrupo normal de G. Entonces G/N es resoluble.*

Demostración. Como G es resoluble, existe una torre abeliana de la forma

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G.$$

Llamemos $\overline{G}$ al cociente G/N y vamos a considerar la proyección canónica $\pi\colon G \longrightarrow \overline{G}$. Para cada $i = 1, \ldots, n$ definimos $\overline{G}_i = \pi(G_i)$ (en particular, $\overline{G}_0 = \pi(e) = \{eN\}$ es el neutro en el grupo cociente, y $\overline{G}_n = \pi(G) = \overline{G}$). Así, tenemos una torre de subgrupos

$$\{eN\} = \overline{G}_0 \subseteq \overline{G}_1 \subseteq \cdots \subseteq \overline{G}_n = \overline{G}.$$

Observamos que, para cada $i = 1, \ldots, n$, $\overline{G}_i \lhd \overline{G}_{i+1}$. Esto se puede comprobar viendo que, dados $x \in \overline{G}_i$, $y \in \overline{G}_{i+1}$, existen $g \in G_i$ y $h \in G_{i+1}$ tales que $x = \pi(g)$ e $y = \pi(h)$. Puesto que G_i subgrupo normal de G_{i+1}, se tiene que $hgh^{-1} \in G_i$, y entonces,

$$yxy^{-1} = \pi(h)\pi(g)\pi(h)^{-1} = \pi(hgh^{-1}) \in \overline{G}_i.$$

Ahora, consideramos el epimorfismo $\overline{G}_{i+1} \longrightarrow \overline{G}_{i+1}/\overline{G}_i$ y construimos la aplicación

$$\begin{array}{rccccc} \varphi\colon & G_{i+1} & \longrightarrow & \overline{G}_{i+1} & \longrightarrow & \overline{G}_{i+1}/\overline{G}_i \\ & g & \longmapsto & \pi(g) & \longmapsto & \pi(g)\overline{G}_i \end{array}$$

que también será un epimorfismo. Por lo tanto, sabemos que $G_{i+1}/\ker(\varphi) \simeq \overline{G}_{i+1}/\overline{G}_i$. Además, se tiene que $G_i \subseteq \ker(\varphi)$, luego como consecuencia del segundo teorema de isomorfía, obtenemos que $G_{i+1}/\ker(\varphi) \simeq (G_{i+1}/G_i)/(\ker(\varphi)/G_i)$, es decir,

$$\overline{G}_{i+1}/\overline{G}_i \simeq (G_{i+1}/G_i)/(\ker(\varphi)/G_i).$$

Puesto que G_{i+1}/G_i es abeliano, $\overline{G}_{i+1}/\overline{G}_i$ también lo será. Por lo tanto, la torre que hemos construido es abeliana y entonces, $\overline{G}$ es resoluble. □

Veamos que el recíproco también es cierto.

Proposición 2.22. *Sean G grupo y N subgrupo normal de G tales que N y G/N son resolubles. Entonces G también es resoluble.*

Demostración. Consideramos $\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = N$ una torre abeliana de N y $\{eN\} = \overline{G}_0 \subseteq \overline{G}_1 \subseteq \cdots \subseteq \overline{G}_n = \overline{G}$ una torre abeliana de $\overline{G} = G/N$. Sea $\pi\colon G \longrightarrow \overline{G}$ la proyección canónica. Definimos $G_i = \pi^{-1}(\overline{G}_i) \subseteq G$, para cada $i = 1, \ldots, n$. En particular, se tiene que $G_0 = \pi^{-1}(\{eN\}) = N$ y $G_n = \pi^{-1}(\overline{G}) = G$, luego hemos construido la torre

$$N = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G.$$

Si añadimos los términos $\{e\}, N_1, \ldots, N_{r-1}$, obtenemos una torre de G de la forma que queremos:

$$\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = N = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G.$$

Veamos que, de hecho, esta torre es abeliana. Es obvio que los primeros $r+1$ términos cumplen la propiedades necesarias, luego bastaría probar que G_i es normal en G_{i+1} y que G_{i+1}/G_i es abeliano, para $i = 1, \ldots, n$. De $\overline{G}_i \lhd \overline{G}_{i+1}$ se deduce que $G_i \lhd G_{i+1}$ (la demostración es análoga a la vista en la proposición anterior). Para ver que G_{i+1}/G_i es abeliano, basta aplicar el segundo teorema de isomorfía al epimorfismo $G_{i+1} \longrightarrow \overline{G}_{i+1}$ y se obtiene que

$$G_{i+1}/G_i \simeq \overline{G}_{i+1}/\overline{G}_i,$$

luego el cociente G_{i+1}/G_i será abeliano (por serlo $\overline{G}_{i+1}/\overline{G}_i$). Por lo tanto, podemos concluir que G es resoluble. □

Observación 2.23. En función de lo probado en las proposiciones anteriores (2.21 y 2.22), concluimos que un grupo G es resoluble si y solo si lo son N y G/N, siendo N subgrupo normal de G.

Ejemplos 2.24.

1. El grupo simétrico S_3 es resoluble.
   Sea $\{1\} \subseteq A_3 \subseteq S_3$ torre de S_3, donde $A_3 = \{1, (1,2,3), (1,3,2)\}$ denota el grupo alternado. Es obvio que $\{1\} \lhd A_3$, y observamos que A_3 es el núcleo de la aplicación signo $\varepsilon\colon S_3 \longrightarrow \pm 1$, luego la torre es normal. Además, $A_3/\{1\} \simeq A_3$ es isomorfo al grupo de rotaciones de un triángulo equilátero $\{1, \rho, \rho^2\}$, luego es abeliano. Por último, S_3/A_3 tiene orden 2, pues $[S_3\colon A_3] = 2$ y entonces será isomorfo al grupo cíclico $\mathbb{Z}_2$, que también es abeliano. Luego hemos hallado una torre abeliana, y por tanto, S_3 es resoluble.

2. El grupo simétrico S_4 es resoluble.
   Sea $\{1\} \subseteq V \subseteq A_4 \subseteq S_4$ torre de S_4, donde

$$V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

   es subgrupo de A_4. Se prueba fácilmente, de forma análoga al ejemplo anterior, que $\{1\} \lhd V$ y $A_4 \lhd S_4$. Veamos que V es subgrupo normal de A_4. Para ello, basta probar que V es invariante por conjugación por los 3-ciclos $\sigma = (1,2,3)$ y $\tau = (1,2,4)$, ya que estos generan A_4. Es decir, dado $v \in V$, queremos ver que $\sigma v \sigma^{-1}, \tau v \tau^{-1} \in V$:

$$\begin{array}{ll} \sigma(1,2)(3,4)\sigma^{-1} = (1,4)(2,3), & \tau(1,2)(3,4)\tau^{-1} = (1,3)(2,4), \\ \sigma(1,3)(2,4)\sigma^{-1} = (1,2)(3,4), & \tau(1,3)(2,4)\tau^{-1} = (1,4)(2,3), \\ \sigma(1,4)(2,3)\sigma^{-1} = (1,3)(2,4), & \tau(1,4)(2,3)\tau^{-1} = (1,2)(3,4). \end{array}$$

   Luego la torre definida es normal. Ahora, para probar que, de hecho, la torre es abeliana, debemos demostrar que $V \simeq V/\{1\}$ y A_4/V son abelianos (ya sabemos que S_4/A_4 lo es, por ser isomorfo a $\mathbb{Z}_2$). Observamos que $[A_4 \colon V] = |A_4|/|V| = \frac{4!/2}{4} = 3$ (tiene orden primo), luego es isomorfo al cíclico de orden 3 y por tanto, abeliano. Para terminar, se comprueba que los elementos de V conmutan:

$$\begin{array}{l} (1,2)(3,4)(1,3)(2,4) = (1,4)(2,3) = (1,3)(2,4)(1,2)(3,4), \\ (1,2)(3,4)(1,4)(2,3) = (1,3)(2,4) = (1,4)(2,3)(1,2)(3,4), \\ (1,3)(2,4)(1,4)(2,3) = (1,2)(3,4) = (1,4)(2,3)(1,3)(2,4). \end{array}$$

   Concluimos que $\{1\} \subseteq V \subseteq A_4 \subseteq S_4$ es una torre abeliana y S_4 resoluble.

3. Para $n \in \mathbb{N}$, el grupo diédrico D_n es resoluble.
   Sea $D_n = \{1, \rho, \ldots, \rho^{n-1}, \tau, \rho\tau, \ldots, \rho^{n-1}\tau\}$ el n-ésimo grupo diédrico, donde ρ representa el giro de amplitud $2\pi/n$ y τ una simetría. Sea $D_n^+ = \{1, \rho, \ldots \rho^{n-1}\}$ su subgrupo de rotaciones. Se cumple que $D_n^+ \simeq \mathbb{Z}_n$. Obviamente, $\{1\} \lhd D_n^+$ y es sencillo ver que D_n^+ es subgrupo normal de D_n (pues $[D_n : D_n^+] = 2$). Luego es una torre normal. Como D_n^+ es cíclico, $D_n^+/\{1\}$ es abeliano. También lo será $D_n/D_n^+ \simeq \mathbb{Z}_2$ y por tanto, la torre es abeliana. Luego se concluye que D_n es un grupo resoluble.

Definición 2.25. Dado G un grupo, decimos que una torre de subgrupos de G,

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G.$$

es *cíclica* si para cada $i = 0, \ldots, n-1$ se cumple que G_i es normal en G_{i+1} y G_{i+1}/G_i es cíclico.

Un grupo abeliano finito es siempre suma directa de grupos cíclicos (Teorema de estructura de los grupos abelianos finitos). Por lo tanto:

Proposición 2.26. *Un grupo G es resoluble si y solo si tiene una torre cíclica.*

Demostración. Es trivial ver que si G tiene una torre cíclica entonces es resoluble, pues todo grupo cíclico es abeliano. Probamos la implicación contraria.
Veamos primero que todo grupo G abeliano finito tiene una torre cíclica:
Por el teorema de estructura de los grupos abelianos finitos, sabemos que G se puede expresar como suma directa de subgrupos cíclicos (cuyos órdenes son potencias de primos). Pongamos $G = \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_r}$.
Consideramos la siguiente torre de subgrupos

$$\{1\} = \mathbb{Z}_{n_1} \subseteq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \subseteq \cdots \subseteq \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_r} = G.$$

Claramente, todos los subgrupos son normales, pues son abelianos. Además, observamos que $(\mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_{i+1}})/(\mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_i}) \simeq \mathbb{Z}_{n_{i+1}}$ es cíclico para todo $i = 0, \ldots, r-1$. Por tanto, es una torre cíclica, como queríamos ver.
Ahora, probemos que si G es resoluble, entonces tiene una torre cíclica.
Por definición, existe una torre abeliana de subgrupos de G, es decir,

$$\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G,$$

tal que para $i = 0, \ldots, n-1$, G_i es un subgrupo normal de G_{i+1} y G_{i+1}/G_i es abeliano. Fijamos i. Por lo que acabamos de probar, sabemos que G_{i+1}/G_i tiene una torre cíclica:

$$\{e\} = C_{i,0} \subseteq C_{i,1} \subseteq \ldots \subseteq C_{i,m} = G_{i+1}/G_i.$$

Los $C_{i,j}$, para $j = 0, \ldots, m$, son subgrupos de G_{i+1}/G_i, luego consideramos las contraimágenes $\pi^{-1}(C_{i,j}) \subseteq G_{i+1}$, donde $\pi : G_{i+1} \longrightarrow G_{i+1}/G_i$ es la proyección canónica. Observamos que π conserva el carácter cíclico y normal de los subgrupos. Así, tenemos la torre cíclica

$$G_i = \pi^{-1}(C_{i,0}) \subseteq \pi^{-1}(C_{i,1}) \subseteq \ldots \subseteq \pi^{-1}(C_{i,m}) = G_{i+1}.$$

Esto se obtiene para cada i, luego concatenando las torres obtenemos una nueva torre cíclica de subgrupos de G, como queríamos ver. □

2.3.2. Grupos simples. El grupo S_n.

En los ejemplos anteriores, hemos probado que el grupo simétrico S_n es resoluble para $n \leq 4$. En esta sección vamos a probar que de hecho, S_n no es resoluble para ningún $n \geq 5$. Este resultado será esencial para probar teoremas importantes en los próximos capítulos, como el Teorema de Abel. Para ello empezamos recordando la definición de grupo simple.

Definición 2.27. Un grupo G es *simple* si no tiene subgrupos normales propios no triviales. Es decir, si H es subgrupo normal de G, entonces o bien $H = \{e\}$, o bien $H = G$.

Ejemplos 2.28.

1. Los grupos cíclicos de orden primo son simples.
   Sea G un grupo cíclico y sea p primo el orden de G. Si H es un subgrupo de G de orden n, entonces n debería ser divisor de p (según el teorema de Lagrange), lo cual implica que n debe ser o bien 1 (y entonces $H = \{e\}$), o bien p (y entonces $H = G$). Es decir, G es simple.

2. A_4 no es un grupo simple.
   En el apartado 2 de los ejemplos 2.24 vemos que A_4 contiene un subgrupo normal propio y no trivial: $V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Luego no es un grupo simple.

Lema 2.29. *Sea G grupo no trivial, simple y resoluble. Entonces es cíclico y tiene orden primo.*

Demostración. Por definición de grupo resoluble, G contiene una torre abeliana, pero al ser simple, los únicos subgrupos normales de G son el trivial y el mismo G. Luego la torre será de la forma $\{e\} \subset G$. Además, se tiene que $G \simeq G/\{e\}$ debe ser abeliano, luego todos los subgrupos de G serán normales. Es decir, que los únicos posibles subgrupos de G son $\{e\}$ y G. Entonces, si tomamos $g \in G$, $g \neq e$, el subgrupo $\langle g \rangle$ debe ser exactamente G. Es decir $G = \langle g \rangle$ es cíclico. Además hemos visto que G no tiene subgrupos propios, lo que significa que si $|G| = p$ es el orden del grupo, entonces p no tiene divisores. Por tanto, es primo. □

Lema 2.30. *Sea N subgrupo normal de A_n, con $n \geq 3$. Si N contiene un 3-ciclo, entonces $N = A_n$.*

Demostración. Supongamos que N contiene el 3-ciclo $(1,2,3)$. Observamos que para $j \geq 3$,

$$(3,2,j)(1,2,3)^2(3,2,j)^{-1} = (3,2,j)(1,3,2)(3,j,2) = (1,2,j).$$

Luego $(1,2,j) \in N$, pues N es subgrupo normal, y entonces $\{(1,2,3),(1,2,4),\ldots,(1,2,n)\}$ está contenido en N. Sabemos que

$$A_n = \langle (1,2,3),(1,2,4),\ldots,(1,2,n)\rangle,$$

pues todo elemento de A_n se puede escribir como producto de 3-ciclos de la forma $(1,2,j)$ (proposición 2.4). Entonces, $A_n \subseteq N$, y como por hipótesis $N \subseteq A_n$, concluimos que $N = A_n$. □

Teorema 2.31. *El grupo alternado A_n es simple si y solo si $n \neq 4$.*

Demostración. A_1 y A_2 son ambos el grupo trivial, luego son simples. También sabemos que A_3 es simple, pues es cíclico de orden primo, pero que en cambio, A_4 no lo es (ver ejemplo 2.28). Bastará probar que A_n es simple para $n \geq 5$.
Sea $N \neq \{1\}$ un subgrupo normal de A_n. Entonces A_n es simple si y solo si $N = A_n$, o equivalentemente, si N contiene un 3-ciclo (por lo visto en el lema 2.30). Consideramos $x \in N,\ x \neq 1$. Entonces, por ser N normal, se tiene que para $y \in A_n$, $yxy^{-1} \in N$. Luego si definimos $z = yxy^{-1}x^{-1}$, también $z \in N$.
Vamos a considerar distintos casos respecto a la descomposición en ciclos disjuntos de x y ver que en cualquiera de ellos, se puede llegar a que N contiene algún 3-ciclo:

Caso 1: x está compuesto solo por trasposiciones.
De hecho, contendrá al menos 2 trasposiciones. Para simplificar la escritura, supondremos que $x = (1,2)(3,4)x'$, donde x' es producto de trasposiciones disjuntas de $(1,2)$ y $(3,4)$. (Se probaría de manera análoga en el caso general $x = (i_1,i_2)(i_3,i_4)x'$).
Suponemos $y = (2,3,4)$. Entonces,

$$\begin{aligned} z &= (2,3,4)(1,2)(3,4)x'(2,3,4)^{-1}((1,2)(3,4)x')^{-1} = \\ &= (2,3,4)(1,2)(3,4)x'(2,4,3)(x')^{-1}(3,4)(1,2) = (1,4)(2,3). \end{aligned}$$

Luego $(1,4)(2,3) \in N$. Si consideramos $t = (1,4,5) \in A_n$, también $tzt^{-1}z \in N$, donde

$$\begin{aligned} tzt^{-1}z &= (1,4,5)(1,4)(2,3)(1,4,5)^{-1}((1,4)(2,3))^{-1} = \\ &= (1,4,5)(1,4)(2,3)(1,5,4)(2,3)(1,4) = (1,5,4). \end{aligned}$$

Por tanto, N contiene al 3-ciclo $(1,5,4)$.

Caso 2: x está formado por trasposiciones y un único 3-ciclo.
Suponemos $x = (1,2,3)x' \in N$, siendo x' producto de trasposiciones disjuntas de $(1,2,3)$. Entonces, $x^2 \in N$, donde

$$x^2 = (1,2,3)^2(x')^2 = (1,3,2)(1) = (1,3,2),$$

luego N contiene al 3-ciclo $(1,3,2)$.

Caso 3: x es composición de al menos dos 3-ciclos disjuntos.

Sea $x = (1,2,3)(4,5,6)x'$, con x' que conmute con $(1,2,3)$ y $(4,5,6)$. Si consideramos $y = (2,3,4)$, entonces

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

Luego $z = (1,4,2,3,5) \in N$. Veamos que si N contiene un ciclo de orden ≥ 4, entonces también contiene un 3-ciclo. Sea $u = (1,2,\ldots,r)u' \in N$, con $r \geq 4$ y u' producto de ciclos disjuntos de $(1,2,\ldots,r)$, y sea $v = (1,2,3)$. Si ponemos $w = vuv^{-1}u^{-1}$, entonces

$$\begin{aligned} w &= (1,2,3)(1,2,\ldots,r)u'(1,2,3)^{-1}((1,2,\ldots,r)u')^{-1} = \\ &= (1,2,3)(1,2,\ldots,r)u'(1,3,2)(x')^{-1}(1,r,r-1,\ldots,2) = (1,2,4). \end{aligned}$$

Es decir, $w = (1,2,4) \in N$.

Por lo tanto, en cualquier caso $A_n = N$, luego es simple (siempre que $n \neq 4$). □

Por último, llegamos al resultado de interés en esta sección.

Corolario 2.32. *Para $n \geq 5$, S_n no es un grupo resoluble.*

Demostración. Razonamos por reducción al absurdo y suponemos que S_n es resoluble para $n \geq 5$. Entonces cualquiera de sus subgrupos, en particular, A_n, también lo serán. En virtud del teorema 2.31, A_n es un grupo simple cuando $n \geq 5$. Es decir, A_n es simple y resoluble. Por lo tanto, el lema 2.29 implica que A_n es un grupo cíclico de orden primo. Sin embargo, sabemos que el orden de A_n es $\frac{n!}{2}$ que claramente no es primo si $n > 3$. Hemos llegado a un absurdo, pues hemos tomado $n \geq 5$. Por lo tanto, concluimos que S_n no puede ser un grupo resoluble. □

Capítulo 3

Extensiones no resolubles.

El objetivo final de este capítulo es demostrar el Teorema de Abel, es decir, que las raíces de la ecuación general de grado n, para $n \geq 5$, no se puede expresar en radicales. Para ello, después de un resumen de los resultados esenciales de la Teoría de Galois, formalizaremos la expresión de ecuaciones resolubles por radicales mediante los conceptos de extensión resoluble y extensión radical. Posteriormente probamos que si una extensión es resoluble, entonces su grupo de Galois es resoluble (1ª parte del Teorema de Galois). Esta implicación es suficiente para mostrar ejemplos de extensiones no resolubles y para probar el Teorema de Abel.

Para este capítulo se han usado los libros de Delgado-Fuertes-Xambó (sección 6.4) [2], el de Cox (sección 8.2) [1] y el de Rotman [5].

3.1. Revisión de Teoría de Galois.

Dados dos cuerpos K, L, decimos que L es una *extensión* de K (o que K es un *subcuerpo* de L) si $K \subseteq L$ y las operaciones de K se obtienen restringiendo las de L. Lo denotamos por L/K.
Si vemos L como un K-espacio vectorial, podemos considerar la dimensión de L sobre K, a la que llamaremos *grado* de L/K y denotaremos por $[L : K]$. En particular, si $[L : K] < \infty$, se dice que L/K es una extensión *finita*.
Si E es un *cuerpo intermedio* de L/K (es decir, $K \subseteq E \subseteq L$), se cumple la *fórmula de los grados*:

$$[L : K] = [L : E][E : K]. \tag{3.1}$$

Por tanto, L/K es finita si y solo si lo son L/E y E/K.

Dadas dos extensiones L/K y L'/K' y un morfismo $\sigma : K \longrightarrow K'$, llamamos *morfismo de L/K en L'/K' sobre σ* a un homomorfismo $\tau : L \longrightarrow L'$ tal que $\tau|_K = \sigma$.
En particular, si $\sigma = Id$, (con $K = K'$) decimos que τ es un *morfismo de L en L' sobre K*, y a los isomorfismos de L/K en sí misma los llamamos *automorfismos de la extensión L/K*.
Al conjunto de estos automorfismos lo llamamos *grupo de Galois de L/K*, y lo denotamos por $G(L/K)$.
Observamos que, dado un polinomio f con coeficientes en K y $Z = \{\alpha \in L \mid f(\alpha) = 0\}$ el conjunto de sus raíces en L, el grupo de Galois de L/K se comporta como un subgrupo del grupo de permutaciones de Z. Esto es porque los elementos de $G(L/K)$, que dejan fijo

K por definición, transformarán cada una de las raíces de f en otra (pues si $f(\alpha) = 0$ y $\sigma \in G(L/K)$, entonces $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, es decir, $\sigma(\alpha)$ es raíz de f).

Sea L/K una extensión y sean $\alpha_1, \ldots, \alpha_r \in L$. La expresión $K[\alpha_1, \ldots, \alpha_r]$, representa al mínimo subanillo de L que contiene a K y a $\alpha_1, \ldots, \alpha_r$. Se puede describir como el anillo de expresiones polinómicas en $\alpha_1, \ldots, \alpha_r$ con coeficientes en K. Su cuerpo de fracciones se denota por $K(\alpha_1, \ldots, \alpha_r)$. Diremos que es la *extensión de K generada por $\alpha_1, \ldots, \alpha_r$*, y de hecho, coincide con el mínimo subcuerpo de L que contiene a K y a $\alpha_1, \ldots, \alpha_r$. En este caso, decimos que la extensión $K(\alpha_1, \ldots, \alpha_r)/K$ está *finitamente generada* y, en particular, si $r = 1$, que es *simple*.

Un elemento $\alpha \in L$ tal que existe algún polinomio $f \in K[X]$ no nulo que se anula en α es un elemento *algebraico sobre K*. Si esto ocurre para todo $\alpha \in L$, decimos que L/K es una *extensión algebraica*. En particular, se cumple que toda extensión finita es algebraica. Dado un elemento algebraico $\alpha \in L$, el *polinomio mínimo* de α sobre K es el polinomio mónico de menor grado con coeficientes en K que se anula en α. Lo denotaremos por $m_\alpha \in K[X]$.

Dados un polinomio $f \in K[X]$ de grado $r > 0$ y una extensión L/K, se dice que f *se descompone totalmente en L* si existen $\alpha_1, \ldots, \alpha_r \in L$ tales que

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

(siendo $a \in K$ el coeficiente dominante de f). Si además, $L = K(\alpha_1, \ldots, \alpha_r)$, diremos que L es un *cuerpo de descomposición de f sobre K*.

Una extensión L/K es *normal* si todo polinomio $f \in K[X]$, irreducible en $K[X]$, y tal que tenga una raíz $\alpha \in L$, se descompone totalmente en L.
Si L/K es una extensión, a la menor extensión normal N/K tal que L es un cuerpo intermedio de la misma la llamamos *clausura normal de L/K*.

Una extensión algebraica L/K es *separable* si para todo $\alpha \in L$, el polinomio mínimo $m_\alpha \in K[X]$ es separable sobre K (es decir, si todas sus raíces en un cuerpo de descomposición son distintas). Si K tiene característica 0, cualquier extensión algebraica es separable.

Las extensiones finitas que sean a su vez normales y separables, se dice que son *extensiones de Galois*. Por tanto, en característica 0, una extensión finita es de Galois si y solo si es normal.

Se tiene el siguiente resultado:

Teorema 3.1 (del elemento primitivo)**.** *Toda extensión L/K finita y separable es una extensión simple. Es decir, existe $\alpha \in L$ tal que $L = K(\alpha)$.*

Dados un cuerpo L, y un grupo G de automorfismos de L, el *cuerpo fijo de G* es el subcuerpo de L formado por los elementos que quedan fijos por todo automorfismo de G. Lo denotamos por L^G.

Teorema 3.2 (de Artin)**.** *Sean L un cuerpo y G un grupo finito de automorfismos de L. Consideramos $K = L^G$ el cuerpo fijo de G. Entonces, la extensión L/K es normal y separable, y se tiene que $[L : K] = |G|$.*

Existe una relación entre los cuerpos intermedios de una extensión L/K y los subgrupos de $G = G(L/K)$: Se tiene que si E es un cuerpo intermedio de L/K entonces $G(L/E)$ es un subgrupo de G. Análogamente, si H es un subgrupo de G, entonces el cuerpo fijo por H es un cuerpo intermedio de L/K. Las aplicaciones

$$\begin{array}{ccc} \{\text{Cuerpos intermedios de } L/K\} & \longleftrightarrow & \{\text{Subgrupos de } G\} \\ E & \longrightarrow & G(L/E) \\ L^H & \longleftarrow & H \end{array}$$

que ponen en relación los cuerpos intermedios con los subgrupos de G se llaman *correspondencias de Galois*.

Observemos que si E, F son cuerpos intermedios tales que $E \subset F$, entonces $G(L/F) \subset G(L/E)$. De la misma forma, si H, S son subgrupos de G, con $H \subset S$, entonces $L^S \subset L^H$. También notamos que si $H \subset G$ es un subgrupo, entonces L/L^H es una extensión de Galois de grado $|H|$ (por el teorema de Artin), pero en general, L^H/K no es de Galois.

Teorema 3.3 (Teorema fundamental de Galois)**.** *Sea L/K una extensión de Galois de grado n y sea E un cuerpo intermedio. Pongamos $G = G(L/K)$. Entonces:*

1. $|G| = n$.
2. *Las correspondencias de Galois son biyectivas, e inversas la una de la otra. Además, se verifica que*
$$[L : E] = |G(L/E)| \qquad y \qquad [E : K] = [G : G(L/E)].$$
3. *La extensión E/K es normal si y solo si el subgrupo E' es normal en G. En este caso,*
$$G(E/K) \simeq G/E'.$$

3.1.1. Grupo de Galois de un polinomio.

Dados un polinomio $f \in K[X]$, y L un cuerpo de descomposición de f sobre K, diremos que $G(L/K)$ es el *grupo de Galois de f* y lo denotaremos por $G(f)$.
Si Z es el conjunto de raíces de f en L, se tiene que $L = K(Z)$. Además, cada elemento de $G(f)$ quedará unívocamente determinado por las imágenes de los elementos de Z. Por tanto, puesto que $G(f)$ permuta las raíces de f, se puede identificar a un subgrupo del grupo S_Z de permutaciones de Z. Es decir, $G(f) \subseteq S_r$, siendo r es el grado del polinomio.

A continuación, se prueban un par de resultados que resultan útiles para el cálculo del grupo de Galois de un polinomio en casos particulares. Antes, definimos el discriminante de un polinomio.

Definición 3.4. Sea $f = a_0X^r + a_1X^{r-1} + \ldots + a_r \in K[X]$ un polinomio de grado $r \geq 2$ y sean $\alpha_1, \ldots, \alpha_r$ sus raíces. Sea L un cuerpo de descomposición de f en K y consideramos el elemento $\Delta \in L$ dado por

$$\Delta(f) = a_0^{n-1} \prod_{i<j} (\alpha_i - \alpha_j).$$

Definimos el *discriminante* de f como

$$D(f) = \Delta^2(f) = a_0^{2n-2} \prod_{1 \leq i < j \leq r} (\alpha_i - \alpha_j)^2.$$

Observación 3.5. Sea G el grupo de Galois del polinomio. Observamos dos cosas: la primera, que el discriminante se anula si y solo si f tiene alguna raíz múltiple. La segunda, que $\sigma(\Delta) = \varepsilon(\sigma)\Delta$ para cualquier $\sigma \in G$, siendo ε la aplicación signo. Por lo tanto, $\sigma(D) = \varepsilon(\sigma)^2 D = D$ para todo $\sigma \in G$, es decir, pertenece al cuerpo fijo por G. Luego $D \in K$.

Proposición 3.6. *Sea $f \in K[X]$ un polinomio mónico irreducible y separable de grado 3. Sea L el cuerpo de descomposición de f sobre K y $G = G(L/K)$, es decir el grupo de Galois del polinomio, $G(f)$. Denotemos por $D(f)$ el discriminante de f. Entonces:*

$$G \simeq \begin{cases} A_3 & \text{si } D(f) \text{ es un cuadrado en } K, \\ S_3 & \text{en otro caso.} \end{cases}$$

Demostración. Sabemos que $[L\colon K]$ es múltiplo de 3, luego $|G|$ también lo es. Como además $G \subseteq S_3$, y los únicos subgrupos de S_3 cuyo orden es divisible por 3 son A_3 y el mismo S_3 (de órdenes 3 y 6, respectivamente), entonces necesariamente, G debe ser isomorfo a uno de estos.
Hemos definido $D = \Delta^2$, siendo $\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$, donde $\alpha_1, \alpha_2, \alpha_3 \in L$ son las raíces de f. Observamos que, si $\sigma \in S_3$, entonces $\sigma(\Delta) = \varepsilon(\sigma)\Delta$. En particular, $\sigma(\Delta) = \Delta$ si y solo si $\sigma \in A_3$. Por tanto:

$$G \simeq A_3 \iff G \text{ no tiene permutaciones impares } \iff \sigma(\Delta) = \Delta \text{ para todo } \sigma \in G.$$

Esto último es equivalente a que $\Delta \in K$, y puesto que $D = \Delta^2$, se tiene que

$$G \simeq A_3 \iff D \text{ es un cuadrado en } K.$$

La única otra opción posible es S_3, luego en cualquier otro caso se tendrá que $G \simeq S_3$. □

Lema 3.7. *Sea p primo y $f \in \mathbb{Q}[X]$ un polinomio irreducible de grado p. Si f tiene exactamente $p-2$ raíces reales, y 2 raíces imaginarias conjugadas, entonces $G(f) = S_p$.*

Demostración. Sean $x_1, \ldots, x_{p-2} \in \mathbb{R}$ las raíces reales y $z, \overline{z} \in \mathbb{C}$ las raíces complejas conjugadas. Puesto que f es irreducible y $\mathbb{Q}$ tiene característica 0, f es un polinomio separable y por tanto, todas las raíces son distintas. Consideramos el cuerpo de descomposición de f sobre $\mathbb{Q}$,

$$L = \mathbb{Q}(x_1, \ldots, x_{p-2}, z, \overline{z}).$$

Sea $G = G(f)$ el grupo de Galois del polinomio, el cual podemos identificar con un subgrupo de S_p. Observamos que el automorfismo de conjugación en $\mathbb{C}$,

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ w & \longmapsto & \overline{w} \end{array}$$

induce un automorfismo en L que deja fijas las raíces reales $\{x_1, \ldots, x_{p-2}\}$ y permuta las complejas $\{z, \overline{z}\}$. Por lo tanto, G contiene la trasposición $(p-1, p)$.
Por otro lado, p divide a $[L : \mathbb{Q}]$ puesto que $[L : \mathbb{Q}] = [L : \mathbb{Q}(x_1)][\mathbb{Q}(x_1) : \mathbb{Q}]$ (3.1) y $[\mathbb{Q}(x_1) : \mathbb{Q}] = p$. Luego $|G|$ es divisible por p y por el teorema de Cauchy, existe un elemento de orden p en G, el cual es, necesariamente, un p-ciclo. Es decir, reordenando las raíces de f, si llamamos τ a la trasposición (i, j) y σ al p-ciclo $(1, 2, \ldots, p)$, entonces $\langle \tau, \sigma \rangle \subseteq G$.
Veamos que $S_p = \langle \tau, \sigma \rangle$. Para probar esta igualdad estudiamos dos casos:

- Si $\sigma(i) = j$ o $\sigma(j) = i$, tenemos uno de los conjuntos generadores de S_p conocidos (proposición 2.2), luego $S_p = \langle \tau, \sigma \rangle$.
- En caso contrario, existirá cierto $k < p$ tal que $\sigma^k(i) = j$, y así tendremos que $S_p = \langle \tau, \sigma^k \rangle$ y por tanto $S_p = \langle \tau, \sigma \rangle$.

En conclusión, $S_p = \langle \tau, \sigma \rangle$ es un subgrupo de G y como ya habíamos visto que G es un subgrupo de S_p, se tiene que $G = S_p$ como queríamos probar. □

3.2. Extensiones radicales y resolubles.

De ahora en adelante, supondremos que todos los cuerpos con los que trabajaremos en esta sección son de característica 0. Así, todas las extensiones serán separables.

Definición 3.8. Sea L/K una extensión de cuerpos, y sean $\alpha_1, \ldots, \alpha_r \in L$. Se dice que $\alpha_1, \ldots, \alpha_r$ es una *sucesión radical* de L/K si $L = K(\alpha_1, \ldots, \alpha_r)$ y existen $n_1, \ldots, n_r \in \mathbb{Z}$ positivos tales que,

$$\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1}), \qquad i = 1, \ldots, r.$$

Definición 3.9. Sea L/K una extensión. Diremos que es una *extensión radical* si posee una sucesión radical.

Observación 3.10. Equivalentemente, se puede decir que una extensión L/K es radical si existe una torre de subcuerpos de L,

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L,$$

donde $K_i = K_{i-1}(\alpha_i)$ y $\alpha_i^{n_i} \in K_{i-1}$ para algún n_i entero positivo, $i = 1, \ldots, r$. Luego la torre es de la forma

$$K = K_0 \subseteq K_0(\alpha_1) \subseteq \cdots \subseteq K_{r-1}(\alpha_r) = L,$$

o lo que es lo mismo,

$$K = K_0 \subseteq K_0(\alpha_1) \subseteq \cdots \subseteq K_0(\alpha_1, \ldots, \alpha_r) = K(\alpha_1, \ldots, \alpha_r) = L.$$

Aquí se observa que la construcción de extensiones radicales se basa en adjuntar sucesivamente raíces n_i-ésimas al subcuerpo K.

Ejemplo 3.11. La extensión $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ es radical.
Sean $K = \mathbb{Q}$ y $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. Veamos que L/K contiene una sucesión radical.
Consideramos $\alpha_1 = \sqrt{2}$ y $\alpha_2 = \sqrt{2+\sqrt{2}}$. Observamos que $\alpha_1^2 = (\sqrt{2})^2 = 2 \in K$ y que $\alpha_2^2 = (\sqrt{2+\sqrt{2}})^2 = 2+\sqrt{2} \in K(\alpha_1)$. Además, $L = K(\alpha_1, \alpha_2)$, pues $\alpha_1 = \alpha_2^2 - 2 \in K(\alpha_2)$. Luego α_1, α_2 es una sucesión radical y por tanto, L/K es una extensión radical. De hecho, la torre de subcuerpos correspondiente a la definición vista en la observación 3.10 es

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2+\sqrt{2}}).$$

Ejemplo 3.12. Ya hemos calculado las raíces de la ecuación cúbica $X^3 + pX + q = 0$ (ver sección 1.2). Sean

$$\alpha_1 = \sqrt{q^2 + 4p^3/27}, \quad \alpha_2 = \sqrt[3]{\frac{-q + \sqrt{q^2 + 4p^3/27}}{2}}, \quad \text{y} \quad \alpha_3 = \xi,$$

siendo ξ una raíz primitiva cúbica de la unidad. La torre de cuerpos

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha_1, \alpha_2) \subseteq \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3),$$

es radical (pues $\alpha_1^2 \in \mathbb{Q}$, $\alpha_2^3 \in \mathbb{Q}(\alpha_1)$ y $\alpha_3^3 \in \mathbb{Q} \subseteq \mathbb{Q}(\alpha_1, \alpha_2)$).
Luego si $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_1, \alpha_2)$, la extensión $L/\mathbb{Q}$ es radical. Además, observamos que el cuerpo de descomposición del polinomio sobre $\mathbb{Q}$ está contenido en L.

En general, el cuerpo de descomposición del polinomio no coincidirá con la extensión radical L que lo contiene. Vemos a continuación un ejemplo en el que, efectivamente, son distintos.

Ejemplo 3.13. Consideramos $f = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$ y sea L su cuerpo de descomposición sobre $\mathbb{Q}$. En el ejemplo 3.12 hemos visto que L está contenido en una extensión radical $L'/\mathbb{Q}$. Vamos a estudiar este caso particular.
Sea $\zeta = e^{2\pi i/7}$ una raíz séptima primitiva de la unidad. Consideramos

$$\alpha_j = \zeta^j + \zeta^{-j} = 2\cos(2\pi j/7), \qquad \text{para } j = 1, 2, 3.$$

Se puede comprobar que son las tres raíces de f. Sea $L' = \mathbb{Q}(\zeta)$. Observamos que contiene a todas las raíces de f y por tanto, $L \subseteq \mathbb{Q}(\zeta)$. En particular, $L'/\mathbb{Q}$ es radical pues $\zeta^7 \in \mathbb{Q}$.
Hemos hallado una extensión que contiene $L'/\mathbb{Q}$ tal que es radical, pero vamos a comprobar que $L/\mathbb{Q}$ no lo es.
Razonamos por reducción al absurdo y suponemos que $L/\mathbb{Q}$ es radical. Sabemos que f es irreducible sobre $\mathbb{Q}$ y que su discriminante es

$$\Delta(f) = 49,$$

(si $f = X^3 + bX^2 + cX + d$, entonces $\Delta(f) = -4b^3d + b^2c^2 + 18bcd - 4c^3 - 27d^2$). Puesto que $\Delta(f) > 0$, las raíces de f serán reales (proposición 1.1), luego $L \subseteq \mathbb{R}$. Además, como es un cuadrado perfecto, se tendrá que $G(L/\mathbb{Q}) \simeq A_3$ (según la proposición 3.6) y por tanto $[L : \mathbb{Q}] = 3$.
Puesto que hemos supuesto que $L/\mathbb{Q}$ es radical, existe $\gamma \in L$ tal que $L = \mathbb{Q}(\gamma)$, con $\gamma^m \in \mathbb{Q}$ para $m \geq 3$ (sabemos que es una extensión simple porque si existiese algún cuerpo intermedio M se tendría que $[L : \mathbb{Q}] = [L : M][M : \mathbb{Q}] = 3$ y por tanto, o bien $L = M$, o bien $M = \mathbb{Q}$). Sea g el polinomio mínimo de γ, sabemos que es de grado 3 y que divide a $x^m - \gamma^m$, luego las raíces de g serán de la forma $\xi^j\gamma$, con $j \in \{0, \ldots, m-1\}$, donde ξ es una raíz m-ésima de la unidad. Al ser $L/\mathbb{Q}$ de Galois, g se descompondrá completamente en $L = \mathbb{Q}(\gamma)$ y por lo tanto, existirán $j, k, l \in \{0, \ldots, m-1\}$ tales que $\xi^j\gamma, \xi^k\gamma, \xi^l\gamma \in L$. Pero $L \subseteq \mathbb{R}$ y como mucho, solo dos de esas tres raíces son reales (γ y $-\gamma$). Luego hemos llegado a un absurdo. Como consecuencia, $L/\mathbb{Q}$ no puede ser una extensión radical.

Esto nos lleva a definir un nuevo concepto más amplio, que nos será muy útil.

Definición 3.14. Una extensión L/K es *resoluble* si existe L' extensión radical sobre K tal que $K \subseteq L \subseteq L'$ (es decir, tal que L sea un cuerpo intermedio de L'/K).

Puesto que lo que nos interesa es encontrar una extensión en la cual las raíces de f se puedan expresar mediante radicales, esta es la definición adecuada. No necesitamos exigir tanto como que la extensión del cuerpo de descomposición del polinomio sobre K sea radical, si no que bastará con que esté contenido en una.

Observación 3.15. Evidentemente, toda extensión radical es resoluble, luego la extensión $L/\mathbb{Q}$ vista en el ejemplo 3.13 es resoluble.

Definición 3.16. Sea $f \in K[X]$ un polinomio y sea L un cuerpo de descomposición de f sobre K. Se dice que f es un *polinomio resoluble por radicales* (o que $f = 0$ es una *ecuación resoluble por radicales*) si L/K es una extensión resoluble.

Ejemplo 3.17. El polinomio $f = X^5 - 5X^4 + 10X^3 - 10X^2 + 5X - 3 \in \mathbb{Q}[X]$ es resoluble por radicales.
Observamos que podemos escribir

$$f = (X^5 - 5X^4 + 10X^3 - 10X^2 + 5X - 1) - 2 = (X-1)^5 - 2,$$

luego las raíces de f son:

$$1 + \xi^k \sqrt[5]{2}, \qquad k = 0, 1, 2, 3, 4,$$

donde ξ es una raíz quinta primitiva de la unidad y $\sqrt[5]{2}$ la raíz quinta real de 2. Si tomamos $\alpha_1 = \xi$, $\alpha_2 = \sqrt[5]{2}$ se tiene que $\alpha_1^5 \in \mathbb{Q}$ y que $\alpha_2^5 \in \mathbb{Q}(\alpha_1)$, luego hemos hallado una sucesión radical

$$\mathbb{Q} \subseteq \mathbb{Q}(\xi) \subseteq \mathbb{Q}(\xi, \sqrt[5]{5}).$$

Además $L = \mathbb{Q}(\xi, \sqrt[5]{2})$ es el cuerpo de descomposición de f sobre $\mathbb{Q}$. Por lo tanto la extensión $L/\mathbb{Q}$ es radical y resoluble, y f es entonces resoluble por radicales.

3.3. La extensión $X^n - a$.

Hemos visto que las extensiones radicales están formadas por una torre de extensiones en las que cada cuerpo intermedio se obtiene al adjuntar raíces n-ésimas al anterior. Así pues, estas extensiones intermedias son de la forma $K(\alpha)/K$, con $\alpha^n = a \in K$, y constituyen las 'piezas' básicas de las extensiones resolubles. Para estudiarlas, conviene verlas como una subextensión de K'/K, siendo K' el cuerpo de descomposición de $X^n - a$.

Consideremos el polinomio $f = X^n - a \in K[X]$. Sea K' un cuerpo de descomposición de dicho polinomio sobre K. La extensión de cuerpos K'/K será el prototipo de extensión resoluble (y de hecho, radical) y nos será de utilidad para la demostración del teorema de Galois.

Sea $\alpha \in K'$ una raíz de f, es decir, $\alpha^n = a$. El conjunto de raíces de f es

$$\{\xi^k \alpha \mid k = 0, 1, \ldots, n-1\},$$

donde $\xi \in K'$ es una raíz primitiva n-ésima de la unidad ($\xi^n = 1$). En particular, se tendrá que $K' = K(\alpha, \xi)$.

Proposición 3.18. *Sea n un número primo. Entonces $f = X^n - a \in K[X]$ es irreducible sobre K si y solo si no tiene raíces en K.*

Demostración. Una de las implicaciones es trivial, pues si f tiene una raíz $\alpha \in K$, entonces $X - \alpha \in K[X]$ en un factor de f y por tanto, es reducible.
Para probar la otra, supongamos que f no es irreducible y veamos que entonces, tiene una

raíz en K.
Sea L un cuerpo de descomposición de f sobre K. Entonces, podemos escribir

$$f = (X - \alpha_1) \cdots (X - \alpha_n) \in L[X],$$

siendo $\alpha_1, \ldots, \alpha_n \in L$ las raíces de f. Si $\alpha_1 = 0$, tendríamos una raíz en K y quedaría probado. Supongamos $\alpha_1 \neq 0$, y consideramos $\zeta_i = \alpha_i/\alpha_1$ para $i = 1, \ldots, n$. Como son raíces de f se tiene que $\alpha_i^n = a$ y entonces

$$\zeta_i^n = \frac{\alpha_i^n}{\alpha_1^n} = \frac{a}{a} = 1.$$

Es decir, son raíces n-ésimas de la unidad. Se tiene que $\alpha_i = \zeta_i \alpha_1$, luego

$$f = (X - \zeta_1\alpha_1) \cdots (X - \zeta_n\alpha_1).$$

Hemos supuesto que f es reducible, es decir, que existen $g, h \in K[X]$ tales que que $f = gh$ y con $gr(g) = r$, $gr(h) = s$ menores estrictamente que n. Se puede suponer que g y h son mónicos. Se sigue que g es producto de r de los factores $X - \zeta_i\alpha_1$ y, renombrando las raíces si fuese necesario, se llega a

$$g = (X - \zeta_1\alpha_1) \cdots (X - \zeta_r\alpha_1).$$

Puesto que $g \in K[X]$, el término independiente debe estar en K, es decir, $\zeta_1 \cdots \zeta_r \alpha_1^r \in K$. Denotemos $\zeta = \zeta_1 \cdots \zeta_r$ y notemos que ζ también es una raíz n-ésima de la unidad. Ahora, observamos que $mr + ln = 1$ para ciertos $m, l \in \mathbb{Z}$, pues $r < n$ y n es primo (Identidad de Bézout). Entonces,

$$\zeta^m \alpha_1 = \zeta^m \alpha_1^{mr+ln} = (\zeta\alpha_1^r)^m (\alpha_1^n)^l = a^l (\zeta\alpha_1^r)^m \in K,$$

pues $\zeta\alpha_1^r \in K$ y $\alpha_1^n = a \in K$. Es decir, $\zeta^m\alpha_1 \in K$. Además,

$$(\zeta^m\alpha_1)^n = (\zeta^n)^m \alpha_1^n = a,$$

lo cual prueba que $\zeta^m\alpha_1$ es una raíz de f en K. □

Obsérvese que el polinomio $X^n - a$ no es, en general, irreducible. No obstante se tiene el siguiente resultado.

Proposición 3.19. *Sea $f = X^n - a \in K[X]$ y sea K' el cuerpo de descomposición de f sobre K. Sea ξ una raíz primitiva n-ésima de la unidad. Consideramos $H = G(K'/K(\xi))$. Entonces, H se puede identificar a un subgrupo de $\mathbb{Z}_n$ y, en particular, H es cíclico.*

Demostración. Las raíces de f son $\{\alpha, \alpha\xi \ldots, \alpha\xi^{n-1}\}$, donde ξ es una raíz primitiva n-ésima de la unidad y $\alpha^n = a$. Sea $\sigma \in H$. Sabemos que los elementos del grupo de Galois transforman las raíces de f en otras raíces de f, y puesto que σ deja fijo ξ, quedará definida por su imagen en α. Pongamos $\sigma(\alpha) = \alpha\xi^k$ para cierto $k \in \mathbb{Z}_n$. Definimos la aplicación

$$\begin{array}{rccc} \mathcal{K}\colon & H & \longrightarrow & \mathbb{Z}_n \\ & \sigma & \longmapsto & k \end{array}$$

que asigna a cada elemento de H el exponente de ξ en la imagen de α por ese automorfismo de K'. Comprobamos que, de hecho, $\mathcal{K}$ es un monomorfismo.
Para ver que $\mathcal{K}$ es homomorfismo, queremos comprobar que, dados $\sigma, \tau \in H$, se tiene

que $\mathcal{K}(\sigma \circ \tau) = \mathcal{K}(\sigma) + \mathcal{K}(\tau)$. Sean $\sigma, \tau \in H$ dados por $\sigma(\alpha) = \alpha\xi^k$ y $\tau(\alpha) = \alpha\xi^l$, con $0 \leq k, l < n$. Vemos que

$$(\sigma \circ \tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha\xi^l) = \xi^l\sigma(\alpha) = \alpha\xi^l\xi^k = \alpha\xi^{k+l}.$$

Luego $\mathcal{K}(\sigma \circ \tau) = k + l = \mathcal{K}(\sigma) + \mathcal{K}(\tau)$ como queríamos ver. Entonces $\mathcal{K}$ es homomorfismo. Para ver que es inyectiva, basta observar que, si $\mathcal{K}(\sigma) = \mathcal{K}(\tau)$, entonces $k \equiv l \mod n$ y por tanto $\xi^k\alpha = \xi^l\alpha$. En consecuencia, $\sigma(\alpha) = \tau(\alpha)$ y $\sigma = \tau$.
Es decir, la aplicación que hemos construido es un homomorfismo inyectivo y por lo tanto, H será isomorfo a un subgrupo de $\mathbb{Z}_n$. En particular será cíclico.

□

A continuación, probamos un resultado que anticipa lo que será después el teorema de Galois.

Proposición 3.20. *En las condiciones anteriores, el grupo de Galois de la extensión K'/K es resoluble.*

Demostración. Sea $G = G(K'/K)$ el grupo de Galois de K'/K. Para probar la resolubilidad de G, buscamos una torre abeliana de subgrupos de G. Consideramos la torre de extensiones

$$K \subseteq K(\xi) \subseteq K' = K(\alpha, \xi),$$

que a través de las correspondencias de Galois nos da la torre de grupos

$$\{1\} = G(K'/K') \subseteq H = G(K'/K(\xi)) \subseteq G = G(K'/K).$$

Primero comprobamos que la torre que hemos construido es normal. Obviamente el grupo trivial es normal en H. Observamos que $K(\xi)/K$ es una extensión normal (pues es de Galois) y por el Teorema fundamental de Galois, H es un subgrupo normal de G. Luego la torre es normal.
Ahora, vemos que $H/\{1\} \simeq H = G(K'/K(\xi))$ es abeliano ya que es cíclico según lo probado en la proposición 3.19. Además, como H es normal en G, lo es la extensión $K(\xi)/K$, y

$$G/H = G(K'/K)/G(K'/K(\xi)) \simeq G(K(\xi)/K).$$

Veamos que $G(K(\xi)/K)$ (y por tanto, G/H) es abeliano. Dados $\sigma, \tau \in G(K(\xi)/K)$, están definidos por su acción sobre ξ: $\sigma(\xi) = \xi^i$, $\tau(\xi) = \xi^j$. Se tiene que $(\sigma \circ \tau)(\xi) = \xi^{ij} = (\tau \circ \sigma)(\xi)$. Luego $\sigma \circ \tau = \tau \circ \sigma$.
Por lo tanto, hemos probado que G posee una torre abeliana,

$$\{1\} \subseteq H \subseteq G,$$

y concluimos que es resoluble. □

3.4. Teorema de Galois: Extensión resoluble implica grupo resoluble.

El Teorema de Galois caracteriza las extensiones resolubles mediante la resolubilidad del grupo. Aunque en este capítulo solo probamos una implicación, escribimos el enunciado completo.

Teorema 3.21 (Galois)**.** *Una extensión es resoluble si y solo si lo es su grupo de Galois.*

Probamos a continuación que, si una extensión es resoluble, entonces su grupo de Galois es resoluble. El resultado recíproco se demostrará más adelante (ver sección 4.2).

Demostración. Sea E/K una extensión resoluble y sea $G = G(E/K)$ su grupo de Galois. Queremos probar que G es un grupo resoluble.

Paso 1 Para empezar, simplificaremos un poco el enunciado. Veamos que es equivalente probarlo para una extensión de Galois radical.

Paso 1.1 Puesto que la extensión E/K es resoluble, existe una extensión radical L/K tal que $K \subseteq E \subseteq L$.
Vamos a considerar $K_0 = E^G$ el cuerpo fijo por G. Por el teorema de Artin (3.2), sabemos que E/K_0 es una extensión de Galois, y además, $G(E/K_0) = G$.
Observamos que L/K_0 también es radical, pues lo es L/K, luego sustituyendo K por K_0, podemos suponer que E/K es una extensión de Galois.

Paso 1.2 A continuación consideramos L' la clausura normal de L/K. Veamos que L'/K es radical.
Puesto que L/K es radical, existen $\alpha_1, \dots, \alpha_r \in L$ y $n_1, \dots, n_r \in \mathbb{N}$ tales que $L = K(\alpha_1, \dots, \alpha_r)$ y $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$ para cada $i = 1, \dots, r$.
Probamos que L'/K es radical para el caso $r = 1$.
Se tiene la torre radical $K \subseteq K(\alpha) = L$, con $\alpha^n \in K$. Que L' se la clausura normal de $K(\alpha)$ significa que es un cuerpo de descomposición de m_α (el polinomio mínimo de α). Consideramos $\alpha_1, \dots, \alpha_s$ las raíces de m_α, tenemos que

$$K \subseteq K(\alpha) \subseteq K(\alpha_1, \dots, \alpha_s).$$

Los elementos de $G = G(K(\alpha_1, \dots, \alpha_s)/K)$ permutan las raíces de m_α, luego para todo $j = 1, \dots, s$ existe $\sigma \in G$ tal que $\sigma(\alpha) = \alpha_j$. Por lo tanto,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha_j^n \in K.$$

Es decir, $\alpha_1, \dots, \alpha_s$ es una sucesión radical y por tanto, $K(\alpha_1, \dots, \alpha_s)/K$ es una extensión radical.
Esto se puede generalizar fácilmente: puesto que acabamos de probar que al adjuntar las raíces del polinomio mínimo se obtiene una extensión radical, basta adjuntar las raíces de cada m_{α_i}, para $i = 1, \dots, r$. Así, llegamos a que L'/K es radical, como queríamos probar.
Por lo tanto, si sustituimos L por L', se puede suponer que la extensión L/K es normal.

Paso 1.3 Hemos supuesto que la extensión L/K es radical y normal, luego es una extensión de Galois (pues las extensiones radicales son separables). Podemos aplicar el Teorema fundamental de Galois, y se llega a que

$$G = G(E/K) \simeq G(L/K)/G(L/E).$$

Observamos que como E/K es de Galois, $G(L/E)$ será un subgrupo normal de $G(L/K)$. Por tanto, G será resoluble si lo es $G(L/K)$ (ver proposición 2.21). Luego podemos sustituir E por L y entonces L/K será una extensión de Galois radical.

Hemos probado que es equivalente probar el teorema si suponemos que L/K es una extensión de Galois radical (y por tanto, resoluble).

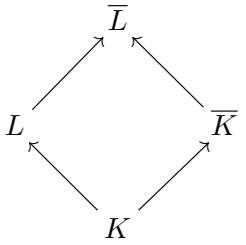
Paso 2 Sea L/K es una extensión de Galois radical. Existe una sucesión radical, $\alpha_1, \ldots, \alpha_r$ tal que $L = K(\alpha_1, \ldots, \alpha_r)$ y además, existen $n_1, \ldots, n_r \in \mathbb{N}$ tales que $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ para todo $i = 1, \ldots, r$.
Vamos a probar, mediante inducción sobre r, que $G(L/K)$ es un grupo resoluble.

- Suponemos $r = 1$. Entonces, $L = K(\alpha)$ y existe $n \in \mathbb{N}$ tal que $\alpha^n \in K$. Pongamos $a = \alpha^n$ y sea $f = X^n - a \in K[X]$. Consideramos L' un cuerpo de descomposición de f. Es decir, $L' = K(\alpha, \xi)$, donde ξ es una raíz primitiva n-ésima de la unidad. Por tanto, $G(L'/K)$ es resoluble (3.20). Se observa que

$$G(L/K) \simeq G(L'/K)/G(L'/L),$$

  y puesto que L/K es una extensión normal, el grupo $G(L'/L)$ también será normal. Por lo tanto, $G(L/K)$ es un grupo resoluble.

- Supongamos que se cumple para $r - 1$. Es decir, si una extensión de Galois contiene una cadena radical $\alpha_1, \ldots, \alpha_{r-1}$, entonces su grupo de Galois será resoluble. Vamos a probar que también se cumple par r.
  Razonamos de forma similar al caso anterior. Consideramos $X^{n_1} - 1 \in K[X]$ y $\overline{L}$ su cuerpo de descomposición sobre L, es decir, $\overline{L} = L(\xi) = K(\alpha_1, \ldots, \alpha_n, \xi)$, siendo ξ raíz primitiva n_1-ésima de la unidad. Consideramos también el cuerpo de descomposición de este polinomio sobre K y lo llamamos $\overline{K}$ (obtenido al adjuntar las raíces de $X^{n_1} - 1$ en $\overline{L}$ a K). Así se obtiene el diagrama siguiente:



  Se observa que todas las extensiones en el diagrama anterior son de Galois. Además,

$$G = G(L/K) \simeq G(\overline{L}/K)/G(\overline{L}/L).$$

  Luego para probar que $G(L/K)$ es resoluble, basta probar que lo es $G(\overline{L}/K)$. Vamos a denotar $\overline{G} = G(\overline{L}/K)$. Puesto que $K \subseteq \overline{K}$, se tiene que $G(\overline{L}/\overline{K}) \subseteq \overline{G}$. Denotamos este subgrupo por $N = G(\overline{L}/\overline{K})$ y observamos que es, de hecho, un subgrupo normal de $\overline{G}$ (pues $\overline{K}/K$ es una extensión normal). Además,

$$\overline{G}/N = G(\overline{L}/K)/G(\overline{L}/\overline{K}) \simeq G(\overline{K}/K).$$

  Como $\overline{K}/K$ es una extensión ciclotómica, $G' = G(\overline{K}/K)$ es un grupo abeliano y por tanto resoluble. Entonces, $\overline{G}$ será resoluble si lo es N (ver proposición 2.22).
  Luego solo falta probar que $N = G(\overline{L}/\overline{K})$ es resoluble. Se tiene la torre de extensiones de Galois

$$\overline{K} \subseteq \overline{K}(\alpha_1) \subseteq \overline{K}(\alpha_1, \ldots, \alpha_r) = \overline{L}.$$

  Luego

$$G(\overline{K}(\alpha_1)/\overline{K}) \simeq G(\overline{L}/\overline{K})/G(\overline{L}/\overline{K}(\alpha_1)) = N/G(\overline{L}/\overline{K}(\alpha_1)),$$

y por tanto, N será resoluble si y solo si lo son $G(\overline{K}(\alpha_1)/\overline{K})$ y $G(\overline{L}/\overline{K}(\alpha_1))$. Se ve fácilmente que $G(\overline{K}(\alpha_1)/\overline{K})$ es resoluble, pues es el caso $r = 1$, y hemos supuesto que $G(\overline{L}/\overline{K}(\alpha_1))$ también es resoluble (hipótesis de inducción). Por lo tanto, N es resoluble, y entonces lo es $G(L/K)$, como queríamos probar.

Hemos probado, por inducción, que $G(L/K)$ es resoluble, cuando L/K es una extensión de Galois radical. Luego, por lo probado en el **Paso 1**, también será resoluble en el caso general donde la extensión solamente es resoluble, y así queda probado el teorema. □

3.5. Polinomios no resolubles por radicales. El Teorema de Abel.

Una aplicación del teorema de Galois es que si tenemos un polinomio $f \in K[X]$ tal que su grupo de Galois $G(f)$ no es resoluble, entonces f tampoco será resoluble por radicales. Veamos un ejemplo.

Ejemplo 3.22. Sea $f = X^5 - 2aX + a \in \mathbb{Q}[X]$, con $a > 1$ un entero que no tenga factores que sean cuadrado de primos. Veamos que este polinomio no es resoluble por radicales. Observamos que f es irreducible (criterio de Eisenstein). Además,

$$f(0) = a > 0, \quad f(1/2) = 1/32 > 0, \quad f(1) = 1 - a < 0,$$

y sabemos que la función es negativa cuando x tiende a $-\infty$, y positiva cuando tiende a ∞. Entonces, f tendrá 3 raíces reales: $\alpha_1 \in (-\infty, 0)$, $\alpha_2 \in (\frac{1}{2}, 1)$ y $\alpha_3 \in (1, \infty)$.
De hecho, serán sus únicas raíces reales. Para comprobarlo, calculamos la derivada de f, $f' = 5X^4 - 2a$, y observamos que se anula en $\pm\sqrt[4]{\frac{2a}{5}}$. Puesto que f' tiene una raíz entre cada par de raíces reales de f (teorema de Rolle) y $-\sqrt[4]{2a/5} \in (\alpha_1, \alpha_2)$ y $\sqrt[4]{2a/5} \in (\alpha_2, \alpha_3)$, se tiene que f no puede tener más raíces reales.
Por lo tanto, f tendrá 3 raíces reales y 2 complejas conjugadas. Se ve en el lema 3.7 que el grupo de Galois de f es isomorfo a S_5, el cual sabemos que no es resoluble (2.32). Por lo tanto, f no es resoluble por radicales.

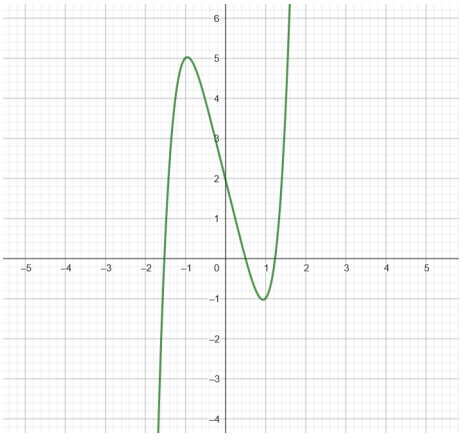


Figura 3.1: Quíntica no resoluble

3.5.1. La ecuación general de grado n.

Sea K un cuerpo y sean $X, X_1, \dots, X_n$ indeterminadas sobre dicho cuerpo. Consideramos $\sigma_1, \dots, \sigma_n$ los polinomios simétricos elementales en $X_1, \dots, X_n$. Sabemos que

$$(X - X_1) \cdots (X - X_n) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n,$$

según vimos en la proposición 2.11.

Definición 3.23. En las condiciones anteriores, diremos que $X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n$ es el *polinomio* (o *ecuación*) *general de grado n sobre K*.

La razón de estudiar la resolubilidad de este polinomio se entiende al observar que, si lo podemos resolver por radicales, entonces también podremos resolver cualquier otro polinomio de grado n, eligiendo los coeficientes σ_i según convenga. El recíproco no es cierto, pues puede que existan polinomios concretos que puedan ser resueltos por radicales, mientras que la ecuación general no lo es, como veremos que es el caso de la quíntica (y demás polinomios de grado $n > 4$).
También observamos que el grupo de Galois de la ecuación general es (relativamente) sencillo de calcular, como veremos a continuación.

Teorema 3.24. *La extensión $K(X_1, \dots, X_n)/K(\sigma_1, \dots, \sigma_n)$ es una extensión de Galois de grado $n!$. Además, su grupo de Galois es S_n.*

Demostración. Observamos que el grupo simétrico permuta las variables $X_1, \dots, X_n$ y por tanto, $S_n \subseteq G(K(X_1, \dots, X_n)/K)$. Luego para ver que el grupo de Galois de la extensión $K(X_1, \dots, X_n)/K(\sigma_1, \dots, \sigma_n)$ es S_n, basta probar que tienen el mismo cardinal. Veamos ahora que $[K(X_1, \dots, X_n) : K(\sigma_1, \dots, \sigma_n)] = n!$.
Consideramos F el cuerpo fijo de S_n y observamos que $K(\sigma_1, \dots, \sigma_n) \subseteq F$. Por el teorema de Artin (3.2) sabemos que $K(X_1, \dots, X_n)/F$ será una extensión normal y separable (y por tanto, de Galois) cuyo grado es $|S_n|$. Luego

$$[K(X_1, \dots, X_n) : F] = n!.$$

Por la fórmula de las dimensiones,

$$[K(X_1, \dots, X_n) : K(\sigma_1, \dots, \sigma_n)] = [K(X_1, \dots, X_n) : F][F : K(\sigma_1, \dots, \sigma_n)],$$

luego sabemos que $[K(X_1, \dots, X_n) : K(\sigma_1, \dots, \sigma_n)] \geq n!$. Por tanto, bastaría probar que

$$[K(X_1, \dots, X_n) : K(\sigma_1, \dots, \sigma_n)] \leq n!.$$

Razonamos por inducción sobre n.

- El caso $n = 1$ es trivial, pues $\sigma_1 = X_1$ y $[K(X_1) : K(\sigma_1)] = 1$.
- Para $n > 1$, supongamos que $[K(X_1, \dots, X_{n-1}) : K(\sigma_1, \dots, \sigma_{n-1})] \leq (n-1)!$.
  Sean $\sigma'_1, \dots, \sigma'_{n-1}$ los polinomios simétricos elementales en las variables $X_1, \dots, X_{n-1}$.
  Puesto que $\sigma'_j = \sigma_j - X_n \sigma_{j-1}$, se tiene que $K(\sigma_1, \dots, \sigma_n, X_n) = K(\sigma'_1, \dots, \sigma'_{n-1}, X_n)$.
  Entonces,

$$\begin{aligned}[K(X_1, \dots, X_n) : K(\sigma_1, \dots, \sigma_n, X_n)] &= [K(X_1, \dots, X_n) : K(\sigma'_1, \dots, \sigma'_{n-1}, X_n)] = \\ &= [K(X_n)(X_1, \dots, X_{n-1}) : K(X_n)(\sigma'_1, \dots, \sigma'_{n-1})] \leq (n-1)!\end{aligned}$$

donde esta última desigualdad se cumple por hipótesis de inducción. Además, como $X_1, \dots, X_n$ son las raíces del polinomio

$$X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n \in K(\sigma_1, \dots, \sigma_n)[X],$$

se tiene que

$$[K(\sigma_1, \dots, \sigma_n, X_n) : K(\sigma_1, \dots, \sigma_n)] \leq n.$$

Es decir, juntando ambas desigualdades se concluye que

$$\begin{aligned}[K(X_1, \dots, X_n) : K(\sigma_1, \dots, \sigma_n)] = \\ = [K(X_1, \dots, X_n) : K(\sigma_1, \dots, \sigma_n, X_n)][K(\sigma_1, \dots, \sigma_n, X_n) : K(\sigma_1, \dots, \sigma_n)] \leq \\ \leq (n-1)!\ n = n!,\end{aligned}$$

como queríamos probar.

□

3.5.2. Teorema de Abel.

Teorema 3.25 (de Abel)**.** *La ecuación general de grado $n > 4$ sobre K no es resoluble por radicales.*

Demostración. Sea $n > 4$ y sea

$$f = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n \in K(\sigma_1, \dots, \sigma_n)[X]$$

la ecuación general de grado n sobre K.
Buscamos un cuerpo de descomposición de f sobre $K(\sigma_1, \dots, \sigma_n)$: las Fórmulas de Vieta dicen que podemos escribir el polinomio como

$$f = (X - X_1) \cdots (X - X_n),$$

luego $X_1, \dots, X_n$ son las raíces de f y por tanto, $K(X_1, \dots, X_n)$ es un cuerpo de descomposición de f sobre $K(\sigma_1, \dots, \sigma_n)$.
Por último, probamos que $K(X_1, \dots, X_n)/K(\sigma_1, \dots, \sigma_n)$ es una extensión no resoluble. En el teorema 3.24 hemos visto que su grupo de Galois es de hecho S_n, que sabemos que no es resoluble para $n > 4$. En conclusión, la extensión tampoco será resoluble, y f no será resoluble por radicales. □

Como hemos mencionado antes, hemos probado que, en general, los polinomios de grado $n > 4$ no se pueden resolver mediante el uso de fórmulas que involucren solo los coeficientes de la ecuación, las operaciones básicas y la extracción de radicales, lo cual no implica que ningún polinomio concreto tenga soluciones de esta forma. De hecho vimos en el ejemplo 3.22 que el polinomio $X^5 - 5X^4 + 10X^3 - 10X^2 + 5X - 3$ se puede resolver por radicales.

Capítulo 4

Extensiones resolubles. El Teorema de Galois.

Este capítulo está dedicado a finalizar el teorema de Galois, es decir, a demostrar que si el grupo de Galois de una extensión de Galois es resoluble, entonces la extensión también lo es. Para ello se usa la idea de Lagrange (conocida como resolventes de Lagrange) que, de hecho, permite escribir las raíces en función de radicales.

Nos basaremos en las secciones 6.5 y 6.6 de [2] para el desarrollo de este capítulo.

4.1. Resolventes de Lagrange.

Sea L/K una extensión de Galois de grado $[L:K] = r$ y sea $G = G(L/K)$ su grupo de Galois. Supongamos que G es un grupo cíclico, con $G = \langle\sigma\rangle$ (luego $\sigma^r = 1$, pues $|G| = r$). Sea n múltiplo de r, se tendrá que $\sigma^n = 1$. Supongamos también que el cuerpo K contiene las raíces n-ésimas de la unidad, es decir, $\xi \in K$.

Definición 4.1. Definimos las *resolventes de Lagrange* de L/K correspondientes a ξ como los endomorfismos de L dados por

$$\rho_k = 1 + \xi^k\sigma + \xi^{2k}\sigma^2 + \ldots + \xi^{(n-1)k}\sigma^{n-1},$$

para cada $k = 0, 1, \ldots, n-1$.

Observamos que ρ_k es un endomorfismo, pues lo son los $\sigma^j \in G$ que aparecen como sumandos en la definición, para $j = 0, \ldots, n-1$ (donde $\sigma^0 = 1$ es la identidad sobre L). En particular, se tiene que para cada $\alpha \in L$,

$$\rho_k(\alpha) = \alpha + \xi^k\sigma(\alpha) + \xi^{2k}\sigma^2(\alpha) + \ldots + \xi^{(n-1)k}\sigma^{n-1}(\alpha).$$

Lema 4.2. *Se cumple que*

$$\rho_0 + \rho_1 + \ldots + \rho_{n-1} = n1.$$

Demostración. Por definición, sabemos que

$$\rho_k = 1 + \xi^k\sigma + \xi^{2k}\sigma^2 + \ldots + \xi^{(n-1)k}\sigma^{n-1}.$$

Entonces,

$$\begin{aligned}\rho_0+\rho_1+\ldots+\rho_{n-1} &= (1+\sigma+\ldots+\sigma^{n-1})\\ &\quad+(1+\xi\sigma+\ldots+\xi^{(n-1)}\sigma^{n-1})\\ &\quad\vdots\\ &\quad+(1+\xi^{n-1}\sigma+\ldots+\xi^{(n-1)^2}\sigma^{n-1})=(*),\end{aligned}$$

y reordenando los términos según el exponente de σ llegamos a

$$(*)=(\sum_{k=0}^{n-1}1)1+(\sum_{k=0}^{n-1}\xi^k)\sigma+\ldots+(\sum_{k=0}^{n-1}\xi^{(n-1)k})\sigma^{n-1},$$

luego basta calcular $\sum_{k=0}^{n-1}\xi^{jk}$ para $0\leq j\leq n-1$.
Si $j=0$, se tiene que

$$\sum_{k=0}^{n-1}1=n.$$

Para $j>0$ tenemos,

$$\sum_{k=0}^{n-1}(\xi^j)^k=\frac{\xi^{jn}-1}{\xi^j-1}=0,$$

pues $\xi^{jn}=1$ (nótese que $\xi^j-1\neq 1$). Luego se anularán todos los términos de la suma, excepto el primero. Por lo tanto,

$$\rho_0+\rho_1+\ldots+\rho_{n-1}=n1.$$

□

Lema 4.3. *Para $0\leq k\leq n-1$, se cumple que*

$$\sigma\circ\rho_k=\rho_k\circ\sigma=\xi^{-k}\rho_k.$$

Además, $(\rho_k(\alpha))^n\in K$ para todo $\alpha\in L$.

Demostración. Como $\rho_k=1+\xi^k\sigma+\xi^{2k}\sigma^2+\ldots+\xi^{(n-1)k}\sigma^{n-1}$, operando se tiene que

$$\begin{aligned}\sigma\circ\rho_k &= \sigma+\xi^k\sigma^2+\xi^{2k}\sigma^3+\ldots+\xi^{(n-1)k}\sigma^n=\\ &= \xi^{(n-1)k}+\sigma+\xi^k\sigma^2+\ldots+\xi^{(n-2)k}\sigma^{n-1}=\\ &= \xi^{-k}(1+\xi^k\sigma+\xi^{2k}\sigma^2+\ldots+\xi^{(n-1)k}\sigma^{n-1})=\xi^{-k}\rho_k.\end{aligned}$$

Análogamente, $\rho_k\circ\sigma=\xi^{-k}\rho_k$.
Por último, para probar que para todo $\alpha\in L$, $(\rho_k(\alpha))^n\in K$ basta ver que queda fijo para σ, pues K es el cuerpo fijo L^G.

$$\sigma((\rho_k(\alpha))^n)=\sigma(\rho_k(\alpha))^n=(\xi^{-1}\rho_k(\alpha))^n=\xi^{-nk}(\rho_k(\alpha))^n=(\rho_k(\alpha))^n.$$

□

Proposición 4.4. *Sea L/K una extensión de Galois de grado r y sea G su grupo de Galois. Supongamos que $G=\langle\sigma\rangle$ es cíclico. Entonces, L/K es una extensión resoluble.*

Demostración. El orden de σ es r, pues $|G| = r$, luego las resolventes de Lagrange serán de la forma

$$\rho_k = 1 + \xi^k \sigma + \ldots + \xi^{k(r-1)} \sigma^{r-1},$$

para $0 \leq k \leq r-1$, donde $1, \xi, \ldots, \xi^{r-1}$ son las raíces primitivas r-ésimas de la unidad. Separamos la demostración en dos posibles casos:

Caso 1: Las raíces $1, \xi, \ldots, \xi^{r-1}$ pertenecen a K.

Queremos probar que existe una extensión radical que contenga a L.
Según el teorema del elemento primitivo (3.1), existe $\alpha \in L$ tal que $L = K(\alpha)$. Por lo probado en el lema 4.3, sabemos que $(\rho_k(\alpha))^r \in K$ para $k = 0, \ldots, r-1$. Denotamos este elemento por $\alpha_k = \rho_k(\alpha)$. Vamos a construir una torre de cuerpos,

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r,$$

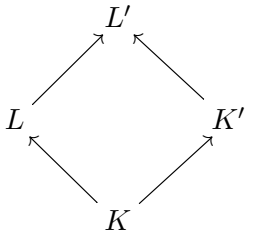
de forma que $K_0 = K$ y K_i sea el cuerpo de descomposición del polinomio $X^r - \alpha_i^r$ sobre K_{i-1}, para $i = 1, \ldots, r$. De esta forma, aseguramos que K_r/K es una extensión radical (pues $\alpha_1, \ldots, \alpha_r$ es una sucesión radical) y por tanto, solo falta comprobar que L es un cuerpo intermedio. Para ello, basta observar que podemos escribir α de la forma siguiente:

$$\alpha = \frac{1}{r} \sum_{k=0}^{r-1} \alpha_k = \frac{1}{r} \sum_{k=0}^{r-1} \rho_k(\alpha),$$

pues se tiene que $\rho_0 + \rho_r + \ldots + \rho_{r-1} = r1$ (por lo probado en el lema 4.2), y entonces $\rho_0(\alpha) + \rho_r(\alpha) + \ldots + \rho_{r-1}(\alpha) = r\alpha$. Luego se tiene que $\alpha \in K_r$ y por lo tanto, $L = K(\alpha) \subseteq K_r$. Es decir, L/K es una extensión resoluble.

Caso 2: Las raíces $1, \xi, \ldots, \xi^{r-1}$ no pertenecen a K.

Vamos a considerar el cuerpo de descomposición de $X^r - 1$ sobre L, y lo llamamos L'. Ahora sí, tenemos $1, \xi, \ldots, \xi^{r-1} \in L'$. Consideramos también el cuerpo $K' = K(\xi)$, y obtenemos el siguiente diagrama (similar al visto en la demostración de 3.21) en el cual, todas las extensiones representadas son de Galois:



Consideramos el grupo $G' = G(L'/K')$. Este grupo es isomorfo a un subgrupo de $G = G(L/K)$, luego G' es cíclico y su orden divide a r. Pongamos $|G'| = d$, con r múltiplo de d. Si η es una raíz primitiva d-ésima de la unidad, también es una raíz r-ésima de 1, luego $\eta \in K'$. Es decir, tenemos un grupo cíclico $G' = G(L'/K')$ de orden d, tal que las raíces $1, \eta, \ldots, \eta^{d-1}$ pertenecen a K': estamos en el **Caso 1**. Entonces, L'/K' es una extensión resoluble.
Como K'/K es radical y acabamos de probar que L'/K' es resoluble, la extensión L'/K también será resoluble y por consiguiente, L/K es resoluble.

□

4.2. Teorema de Galois: Grupo resoluble implica extensión resoluble.

Demostramos en esta sección, la implicación que faltaba del teorema 3.21: si L/K es una extensión de Galois tal que su grupo de Galois $G = G(L/K)$ es resoluble, entonces L/K es resoluble.

Demostración. Puesto que G es resoluble, contendrá una torre cíclica

$$\{1\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G,$$

donde $G_i \lhd G_{i+1}$ y G_{i+1}/G_i es cíclico, para todo $i = 0, \ldots, n-1$.
Vamos a construir una torre de cuerpos $K_0 \subseteq \ldots \subseteq K_n$ de forma que cada $G(K_{i+1}/K_i)$ sea cíclico. Así, aplicando la proposición 4.4, se tendrá que cada K_{i+1}/K_i es resoluble.
Para cada i, consideramos el cuerpo fijo de G_{n-i}, $K_i = L^{G_{n-i}}$. Las contenciones de la torre anterior se invierten, luego se tiene la torre de cuerpos siguiente:

$$L^{G_n} \subseteq L^{G_{n-1}} \subseteq \ldots \subseteq L^{G_0},$$

es decir,

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L.$$

El grupo de Galois de la extensión L/K_i es $G(L/K_i) = G_{n-i}$, para $i = 0, \ldots, n$. Luego como $G_{n-i-1} = G(L/K_{i+1})$ es normal en $G_{n-i} = G(L/K_i)$, se tendrá que la extensión K_{i+1}/K_i es normal. De hecho, K_{i+1}/K_i también es una extensión separable y finita (pues lo es L/K), por tanto para cada $i = 0, 1, \ldots, n$, la extensión K_{i+1}/K_i es de Galois. Por el Teorema fundamental de Galois, se tiene que

$$G(K_{i+1}/K_i) \simeq G(L/K_i)/G(L/K_{i+1}) = G_{n-i}/G_{n-i-1}.$$

Por tanto, $G(K_{i+1}/K_i)$ es cíclico y entonces K_{i+1}/K_i es una extensión resoluble para cada $i = 0, \ldots, n-1$. Veamos que entonces, también lo es L/K.
Razonamos por inducción sobre n. Se cumple trivialmente para $n = 1$. Supongamos que se cumple para $n-1$ y probémoslo para n. Por hipótesis, K_{n-1}/K_0 y K_n/K_{n-1} son ambas extensiones resolubles, luego existen extensiones radicales K'/K_0 y K''/K_{n-1} tales que

$$K_0 \subseteq K_{n-1} \subseteq K' \qquad \text{y} \qquad K_{n-1} \subseteq K_n \subseteq K''.$$

Luego tenemos una torre de la forma siguiente:

$$K_{n-1} \subseteq K_{n-1}(\alpha_1) \subseteq \ldots \subseteq K_{n-1}(\alpha_1, \ldots, \alpha_r) = K'',$$

con $\alpha_1, \ldots, \alpha_r \in K''$ tales que $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ para todo $i = 1, \ldots, r$.
Sea L' el mínimo cuerpo que contiene a K' y K''. Adjuntando los α_i a K' construimos una nueva torre de subcuerpos,

$$K' \subseteq K'(\alpha_1) \subseteq \ldots \subseteq K'(\alpha_1, \ldots, \alpha_r) = L',$$

donde la última igualdad se verifica pues $K_{n-1} \subseteq K'$ y entonces $K'' = K_{n-1}(\alpha_1, \ldots, \alpha_r) \subseteq K'(\alpha_1, \ldots, \alpha_r)$. Se observa que para cada $i = 1, \ldots, r$, $\alpha_i^{n_i} \in K'(\alpha_1, \ldots, \alpha_{i-1})$, y por tanto L'/K' es una extensión radical. A su vez, K'/K_0 es también radical, luego L'/K_0 es una extensión radical. Es decir, hemos hallado una extensión radical L'/K_0 tal que $K_0 \subseteq K_n \subseteq L'$ (pues $K_n \subseteq K'' \subseteq L'$). Por lo tanto, $K_n/K_0 = L/K$ es resoluble. □

4.3. Regreso a la cúbica.

Consideramos el polinomio $f = X^3 - a_1X^2 + a_2X - a_3 \in K[X]$, y mediante la transformación de Tschirnhausen ($X \mapsto X + a_1/3$), obtenemos el polinomio

$$X^3 + pX + q. \tag{4.1}$$

Puesto que obtener las raíces del polinomio original es equivalente a obtener las de este último polinomio, supongamos $a_1 = 0$, $a_2 = p$ y $a_3 = -q$, y trabajemos con la ecuación $X^3+pX+q = 0$. Podremos suponer también que $1, \xi, \xi^2 \in K$ siendo ξ raíz cúbica primitiva de la unidad (si no, sustituimos K por $K(\xi)$) y que f es irreducible.

Observación 4.5. Notemos que a_1, a_2, a_3 son los polinomios simétricos en las raíces $\alpha_1, \alpha_2, \alpha_3$ de f, puesto que $f = 0$ es la ecuación general. Luego

$$\begin{aligned} a_1 &= \alpha_1 + \alpha_2 + \alpha_3 = 0, \\ a_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p, \\ a_3 &= \alpha_1\alpha_2\alpha_3 = -q. \end{aligned}$$

Sea $\sigma \in A_3$ de forma que $A_3 = \langle\sigma\rangle$. Puesto que σ permuta cíclicamente las raíces de f, podemos suponer que

$$\sigma(\alpha_1) = \alpha_2, \quad \sigma(\alpha_2) = \alpha_3, \quad \sigma(\alpha_3) = \alpha_1,$$

y se tiene que $G(K(\alpha_1, \alpha_2, \alpha_3)/K(\Delta)) = A_3$.

Las resolventes de Lagrange vienen dadas por

$$\rho_k = 1 + \xi^k\sigma + \xi^{2k}\sigma^2,$$

para $0 \leq k \leq 2$. Evaluando en α_1, se tiene que

$$\begin{aligned} \rho_0(\alpha_1) &= \alpha_1 + \alpha_2 + \alpha_3, \\ \rho_1(\alpha_1) &= \alpha_1 + \xi\alpha_2 + \xi^2\alpha_3, \\ \rho_2(\alpha_1) &= \alpha_1 + \xi^2\alpha_2 + \xi\alpha_3. \end{aligned}$$

Observamos que $\rho_0(\alpha_1) = 0$. Vamos a hacer unos cálculos previos para luego poder hallar las raíces fácilmente.

- Veamos que $\rho_1(\alpha_1)\rho_2(\alpha_1) = -3p$.
  Tenemos que

  $$\begin{aligned} \rho_1(\alpha_1)\rho_2(\alpha_1) &= (\alpha_1 + \xi\alpha_2 + \xi^2\alpha_3)(\alpha_1 + \xi^2\alpha_2 + \xi\alpha_3) = \\ &= (\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + \xi(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) + \xi^2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = (*) \end{aligned}$$

  y como $\xi + \xi^2 = -1$, obtenemos

  $$\begin{aligned} (*) &= (\alpha_1^2 + \alpha_2^2 + \alpha_3^2) - (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = \\ &= -2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = \\ &= -3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -3p, \end{aligned}$$

  pues $(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) = -2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$ y $p = (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$.

- Calculemos $(\rho_1(\alpha_1))^3 + (\rho_2(\alpha_1))^3$.
  Observamos que $(\rho_i(\alpha_1))^3 \in K(\Delta)$ para $i = 0, 1, 2$, por lo probado en el lema 4.3. Se tiene que

$$(\rho_1(\alpha_1))^3 = (\alpha_1 + \xi\alpha_2 + \xi^2\alpha_3)^3 = \\ = (\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 3\xi(\alpha_1^2\alpha_2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3) + 3\xi^2(\alpha_1^2\alpha_3 + \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2) + 6(\alpha_1\alpha_2\alpha_3).$$

  Si consideramos $A = (\alpha_1^2\alpha_2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3)$ y $B = (\alpha_1^2\alpha_3 + \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2)$, tendremos

$$(\rho_1(\alpha_1))^3 = (\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 3A\xi + 3B\xi^2 + 6(\alpha_1\alpha_2\alpha_3),$$

  y observando que $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = 3\alpha_1\alpha_2\alpha_3$ y que $q = -\alpha_1\alpha_2\alpha_3$, se llega a que

$$(\rho_1(\alpha_1))^3 = 3A\xi + 3B\xi^2 - 9q.$$

  De forma análoga obtenemos que

$$(\rho_2(\alpha_1))^3 = 3A\xi^2 + 3B\xi - 9q.$$

  Por lo tanto,

$$(\rho_1(\alpha_1))^3 + (\rho_2(\alpha_1))^3 = 3A(\xi + \xi^2) + 3B(\xi^2 + \xi) - 18q = -3A - 3B - 18q.$$

  Concluimos observando que $(\rho_0(\alpha_1))^3 = 3A + 3B - 9q = 0$ y por lo tanto,

$$(\rho_1(\alpha_1))^3 + (\rho_2(\alpha_1))^3 = -27q.$$

Hemos probado que $\rho_1(\alpha_1)\rho_2(\alpha_1) = -3p$ y $(\rho_1(\alpha_1))^3 + (\rho_2(\alpha_1))^3 = -27q$. Consideramos el polinomio

$$Y^2 - ((\rho_1(\alpha_1))^3 + (\rho_2(\alpha_1))^3)Y + (\rho_1(\alpha_1))^3(\rho_2(\alpha_1))^3 = Y^2 + 27qY - 27p^3.$$

Entonces, $(\rho_1(\alpha_1))^3$ y $(\rho_2(\alpha_1))^3$ son sus raíces. Las raíces de $Y^2 + 27qY - 27p^3 = 0$ son

$$y = \frac{-27q \pm \sqrt{27^2q^2 + 108p^3}}{2} = -\frac{27}{2}q \pm \frac{3}{2}\sqrt{-3D} = -\frac{27}{2}q \pm \frac{3}{2}\sqrt{-3}\Delta,$$

donde $D = -4p^3 - 27q^2$ denota el discriminante de (4.1) y $\Delta = \sqrt{D}$. Luego

$$(\rho_1(\alpha_1))^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\Delta, \tag{4.2}$$

$$(\rho_2(\alpha_1))^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\Delta, \tag{4.3}$$

Consideramos entonces

$$\rho = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\Delta},$$

una raíz cúbica de (4.2).
Observamos que $\rho_1(\alpha_2) = \xi^2\rho_1(\alpha_1)$ y $\rho_1(\alpha_3) = \xi\rho_1(\alpha_1)$ (proposición 4.3), luego $\rho_1(\alpha_1), \rho_1(\alpha_2), \rho_1(\alpha_3)$ son las raíces cúbicas de (4.2). Pongamos $\rho = \rho_1(\alpha_1)$.

Ahora sea

$$\rho' = -3p/\rho = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\Delta} = \rho_2(\alpha_1)$$

Se tiene, como antes, que $\rho_2(\alpha_2) = \xi\rho_2(\alpha_1)$ y $\rho_2(\alpha_3) = \xi^2\rho_2(\alpha_1)$.

Por lo tanto, tenemos el siguiente sistema de ecuaciones,

$$\begin{cases} \rho_0(\alpha_1) + \rho_1(\alpha_1) + \rho_2(\alpha_1) = 3\alpha_1 = \rho + \rho' \\ \rho_0(\alpha_2) + \rho_1(\alpha_2) + \rho_2(\alpha_2) = 3\alpha_2 = \xi^2\rho + \xi\rho' \\ \rho_0(\alpha_3) + \rho_1(\alpha_3) + \rho_2(\alpha_3) = 3\alpha_3 = \xi\rho + \xi^2\rho' \end{cases}$$

el cual nos permite determinar las raíces de f,

$$\alpha_1 = \frac{\rho + \rho'}{3}, \quad \alpha_2 = \frac{\xi^2\rho + \xi\rho'}{3}, \quad \alpha_3 = \frac{\xi\rho + \xi^2\rho'}{3}.$$

Observación 4.6. Observamos que las raíces que hemos obtenido son justamente las que obtuvimos en la sección 1.2.

$$\frac{\rho + \rho'}{3} = \frac{1}{3}\sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3\Delta}} + \frac{1}{3}\sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3\Delta}} =$$

$$= \sqrt[3]{-\frac{1}{2}q + \frac{1}{2}\sqrt{-D/27}} + \sqrt[3]{-\frac{1}{2}q - \frac{1}{2}\sqrt{-D/27}} =$$

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

Capítulo 5

Resolubilidad real.

En la sección 1.3, vimos que, cuando el discriminante de la cúbica es positivo, las raíces son todas reales. Pero la fórmula de Cardano-Tartaglia expresa estas raíces en términos de números complejos. Este es el llamado "caso irreducible".

En este capítulo veremos si es posible expresar estas raíces utilizando exclusivamente radicales reales, y de ser así, en qué casos podrá hacerse: veremos que en algunos casos, como el de $f = X^3 + X^2 - 5X - 5 = (X + 1)(X^2 - 5)$, sí es posible (sus raíces son -1 y $\pm\sqrt{5}$), pero en general no será así (cuando f es irreducible).

Este capítulo está basado en la sección 8.6 de Cox [1].

5.1. Radicales reales.

Definición 5.1. Sea K un subcuerpo de $\mathbb{R}$.
Diremos que L/K es una *extensión radical real* si L/K es radical y además, $L \subseteq \mathbb{R}$.
Dado $\alpha \in \mathbb{R}$, diremos que *se puede expresar por radicales reales sobre* K si existe una extensión radical real L/K tal que $\alpha \in L$.

Antes de probar el teorema principal, demostramos unos resultado previos. Podemos limitarnos a radicales primos:

Lema 5.2. *Sea L/K una extensión radical. Existe una torre de subcuerpos de L,*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{n-1} \subseteq K_n = L,$$

donde $K_i = K_{i-1}(\gamma_i)$ y $\gamma_i^{m_i} \in K_{i-1}$ para algún m_i primo, $i = 1, \ldots, n$.

Demostración. Razonamos por inducción sobre n.

- Sea $n = 1$. Por definición de extensión radical, sabemos que existe $\gamma \in L$ tal que $L = K(\gamma)$ y $\gamma^m \in K$ para algún m entero positivo.
  Si m es un número primo, ya está.
  Si no, sea p uno de sus factores primos. Tomemos $\delta = \gamma^p$. Así, se tiene la torre de cuerpos siguiente:
  $$K \subseteq K(\delta) \subseteq K(\delta)(\gamma) = K(\gamma).$$
  Observamos que $\gamma^p = \delta \in K(\delta)$ y $\delta^{m/p} = \gamma^m \in K$.
  En el caso de que m/p fuese primo, quedaría probado.
  En caso contrario, volvemos a elegir un factor primo de m/p y razonamos de la misma manera.

- Supongamos que se cumple para $n-1$, es decir, que existen $\gamma_1, \dots, \gamma_{n-1} \in L$ tales que $K_i = K_{i-1}(\gamma_i)$ y $\gamma_i^{m_i} \in K_{i-1}$, con m_i primo, para $i = 1, \dots, n-1$.
  Falta probar que existe $\gamma_n \in L$ tal que $L = K_{n-1}(\gamma_n)$ y $\gamma_n^{m_n} \in K_{n-1}$ para m_n primo.
  Esto es justamente el caso anterior. Luego el lema queda probado.

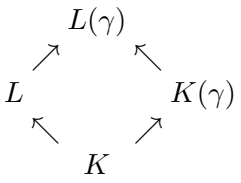
□

Lema 5.3. *Sea $E \subseteq R$ y sea $\gamma \in \mathbb{R}$ tal que $\gamma \notin E$ y $\gamma^m \in E$ para cierto m primo. Entonces $g = X^m - \gamma^m$ es un polinomio irreducible sobre E y $[E(\gamma) : E] = m$.*

Demostración. Puesto que m es primo, basta probar que $g \in E[X]$ no tiene raíces en E (proposición 3.18).
Razonamos por reducción al absurdo y suponemos que existe $\beta \in E$ que sea una raíz de g. Entonces, $\beta^m = \gamma^m$ y por tanto, $\beta = \xi\gamma$, siendo ξ una raíz m-ésima de la unidad. Puesto que $\beta \in E \subseteq \mathbb{R}$ y las únicas raíces reales de la unidad son ± 1, se tiene que $\beta = \pm\gamma$. Luego $\gamma = \pm\beta \in E$, lo que lleva a un absurdo.
Por lo tanto, g es irreducible en E y entonces $[E(\gamma) : E] = gr(g) = m$. □

Proposición 5.4. *Sea L/K una extensión de Galois con $L \subseteq \mathbb{R}$ y $[L : K] = p$, siendo p un primo impar. Entonces, L no está contenido en una extensión radical real de K.*

Demostración. Supongamos que existe $\gamma \in \mathbb{R}$ tal que $\gamma \notin K$, y $\gamma^m \in K$ para cierto m primo. Tenemos la extensión $K \subseteq K(\gamma)$, y por el lema 5.3, se tiene que $[K(\gamma) : K] = m$. Consideramos el siguiente diagrama:



Razonamos por reducción al absurdo y suponemos que $\gamma \in L$.
Puesto que $[L : K] = [L : K(\gamma)][K(\gamma) : K] = m$ es primo y $\gamma \notin K$, se tiene que $L = K(\gamma)$. Entones, de nuevo por el lema 5.3, se tiene que

$$[L : K] = [K(\gamma) : K] \quad \Longrightarrow \quad p = m,$$

luego m es impar. Además, $g = X^m - \gamma^m$ es el polinomio mínimo de γ sobre K, y como la extensión L/K es de Galois, en particular es normal, y por tanto, g se descompone completamente sobre L.
Sus raíces son $\zeta^l\gamma$, con $l = 0, \dots, m-1$, siendo $\zeta = e^{2\pi i/m}$. Como $\gamma \neq 0$, se tiene que $\zeta \in L$. Esto lleva a un absurdo, pues $L \subseteq \mathbb{R}$ y, ya que $m \neq 2$, $\zeta \notin \mathbb{R}$.
Por lo tanto, $\gamma \notin L$. Luego $[L(\gamma) : L] = m$. Observamos que, por la fórmula de los grados,

$$[L(\gamma) : K] = [L(\gamma) : L][L : K] = mp.$$

Además,

$$[L(\gamma) : K] = [L(\gamma) : K(\gamma)][K(\gamma) : K] = [L(\gamma) : K(\gamma)]m,$$

luego $[L(\gamma) : K(\gamma)] = p$. Es decir, al adjuntar γ, un radical primo real, no cambia el grado de la extensión.
Ahora bien, sabemos que una extensión radical real E/K se obtiene al adjuntar radicales primos reales (como vimos en el lema 5.2). Consideramos M el mínimo subcuerpo que

contiene a L y a E. Puesto que acabamos de probar que el grado de la extensión no varía al adjuntar este tipo de radicales, se tiene que

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

Entonces, $M \neq E$ y por lo tanto, $L \subsetneq E$. Es decir, L no puede estar contenido en una extensión radical real de K. □

5.2. Polinomios irreducibles con raíces radicales reales

El siguiente teorema caracteriza cuándo las raíces de un polinomio podrán ser expresadas por radicales reales.

Teorema 5.5. *Sean $K \subseteq \mathbb{R}$ y $f \in K[X]$ un polinomio irreducible. Sea L un cuerpo de descomposición de f sobre K, con $K \subseteq L \subseteq \mathbb{R}$. Entonces, son equivalentes:*

(a) *Alguna raíz de f se puede expresar por radicales reales sobre K.*

(b) *Todas las raíces de f se pueden expresar por radicales reales sobre K y la expresión solo incluye raíces cuadradas.*

(c) *La extensión L/K es radical.*

(d) *$[L : K]$ es una potencia de 2.*

Demostración. Empezamos probando las implicaciones más sencillas. Es trivial que $(b) \Rightarrow (a)$, y como $L \subseteq \mathbb{R}$, se tiene también que $(c) \Rightarrow (a)$.
Veamos que $(d) \Rightarrow (c)$. Suponemos que $[L : K] = 2^n$, con $n \in \mathbb{N}$. Entonces, $|G| = 2^n$, siendo $G = G(L/K)$ el grupo de Galois de la extensión, y por tanto, G es un grupo resoluble (pues si $|G| = p^n$, con p primo, entonces G es resoluble). Luego contiene una torre abeliana

$$\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G,$$

con $[G_i : G_{i-1}] = 2$. Consideramos, para $i = 0, \ldots, n$, el cuerpo fijo por G_{n-i}, $K_i = L^{G_{n-i}}$. Entonces, tenemos una torre de subcuerpos:

$$K \subseteq K_1 \subseteq \ldots \subseteq K_n = L,$$

donde $[K_i : K_{i-1}] = 2$ para cada i. Es decir, K_i se obtiene al adjuntar a K_{i-1} una raíz cuadrada. Por lo tanto, la extensión L/K es radical y queda probado $(d) \Rightarrow (c)$.
De hecho, también hemos demostrado que $(d) \Rightarrow (b)$, pues $L \subseteq \mathbb{R}$.
Falta probar que $(a) \Rightarrow (d)$.
Sea $f \in K[X]$ irreducible y $L \subseteq \mathbb{R}$ un cuerpo de descomposición de f en K. Sea α una raíz de f. Consideramos L'/K una extensión radical real tal que $\alpha \in L'$.
Razonamos por reducción al absurdo y supongamos que $[L : K] \neq 2^n$. Entonces existe p un primo impar que divide a $[L : K]$. Veamos primero que existe $\sigma \in G$ de orden p tal que $\sigma(\alpha) \neq \alpha$.
Puesto que p divide a $|G|$, existirá $\tau \in G$ de orden p. Denotamos por $\alpha_1 = \alpha, \ldots, \alpha_r$ las raíces de f (con $r = gr(f)$). Entonces $L = K(\alpha_1, \ldots, \alpha_r)$. Además. como τ no es la identidad, existe i tal que $\tau(\alpha_i) \neq \alpha_i$. Pero f es irreducible, y entonces existe $\sigma_i \in G$ tal que $\sigma_i(\alpha) = \alpha_i$. Se tiene que

$$(\sigma_i^{-1}\tau\sigma_i)(\alpha) = (\sigma_i^{-1}\tau)(\alpha_i) \neq \sigma_i^{-1}(\alpha_i) = \alpha,$$

siendo $\sigma_i^{-1}\tau\sigma_i \in G$ un elemento de orden p.
Ahora, consideramos $M = L^{\langle\sigma\rangle} \subseteq L$. La extensión L/M es de Galois y además

$$[L : M] = |G(L/M)| = |\langle\sigma\rangle| = p.$$

Entonces, por la proposición 5.4, L no puede estar contenido en una extensión radical real de M.
Se tiene que $\alpha \in L$, por ser L el cuerpo de descomposición de f, pero $\alpha \notin M$ pues $\sigma(\alpha) \neq \alpha$. Entonces, como $[L : M] = p$ es primo, tenemos que $L = M(\alpha)$. Consideramos E el mínimo subcuerpo que contenga a M y a L'. Entonces, $L = M(\alpha) \subseteq E$ (pues $\alpha \in L'$). Además, E/M es una extensión radical real, pues lo es L'/K. Es decir, L está contenido en una extensión radical real de M, lo cual es absurdo, pues la proposición 5.4 dice lo contrario.
Se concluye, que $[L/K]$ es una potencia de 2 y quedan probadas todas las equivalencias. □

Corolario 5.6. *Sean $K \subseteq \mathbb{R}$ y $f \in K[X]$ un polinomio irreducible, cuyo grado no sea potencia de 2. Si f se descompone completamente sobre $\mathbb{R}$, ninguna raíz de f se puede expresar por radicales reales sobre K.*

Demostración. Sea L un cuerpo de descomposición de f sobre K. Puesto que f se descompone completamente sobre $\mathbb{R}$, se tiene que $L \subseteq \mathbb{R}$. Consideramos $\alpha \in L$ una raíz de f. Se tiene la torre de cuerpos

$$K \subseteq K(\alpha) \subseteq L.$$

Además, por la fórmula de los grados (3.1), se tiene que

$$[L : K] = [L : K(\alpha)][K(\alpha) : K] \neq 2^k,$$

pues $[K(\alpha) : K] = gr(f)$. Es decir, $[L : K]$ no es una potencia de 2. Entonces, por el teorema 5.5, ninguna raíz de f se puede expresar en radicales reales sobre K. □

Ejemplo 5.7. Consideramos el polinomio

$$f = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X],$$

y sea L un cuerpo de descomposición de f sobre $\mathbb{Q}$. Observamos que f es irreducible sobre $\mathbb{Q}$ y $gr(f) = 3$ no es una potencia de 2. Vimos en el ejemplo 3.13 que las raíces de f son reales (pues $\Delta(f) > 0$), luego f se descompone completamente en $\mathbb{R}$.
Entonces, por el corolario 5.6, ninguna de sus raíces se pueden expresar en radicales reales sobre $\mathbb{Q}$. Esto coincide con lo que probamos en dicho ejemplo, es decir, la extensión $L/\mathbb{Q}$ es resoluble, pero no radical.

Bibliografía

[1] David A Cox. *Galois theory*. John Wiley & Sons, 2012.

[2] Félix Delgado de la Mata, Concepción Fuertes Fraile y Sebastián Xambó Descamps. *Introducción al álgebra. Vol. 2, Anillos, factorización y teoría de cuerpos*. Universidad de Valladolid, 1999.

[3] Sebastián Xambó Descamps, Félix Delgado y Concha Fuertes. *Introducción al álgebra*. Vol. 1. Editorial Complutense, 1993.

[4] Carlos Ivorra. *Las fórmulas de Cardano-Ferrari*. 2011.

[5] Joseph J Rotman. *Galois theory*. Springer, 1990.

[6] Martha Rzedowski Calderón. «La demostración de Abel». En: *Miscelánea Matemática* 63 (2016).

[7] Ian Stewart. *Galois theory*. Chapman y Hall/CRC, 2022.