



# **El icosaedro y la irreducibilidad de la quintica**

**Víctor Manuel Gómez Sousa**





## **El icosaedro y la irreducibilidad de la quintica**

Víctor Manuel Gómez Sousa

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Miguel Ángel Olalla Acosta



# Índice general

<b>English Abstract</b>	<b>1</b>
<b>1. Introducción</b>	<b>3</b>
<b>2. Los cinco sólidos platónicos</b>	<b>5</b>
2.1. Poliedros regulares . . . . .	5
2.2. Poliedro dual . . . . .	9
2.3. Grupos de simetría de los sólidos platónicos . . . . .	10
<b>3. El icosaedro y la irreducibilidad de la quinta</b>	<b>13</b>
3.1. Invariantes . . . . .	13
3.2. Ecuaciones poliédricas . . . . .	16
3.3. Funciones hipergeométricas . . . . .	18
3.4. La transformación de Tschirnhaus . . . . .	21
3.5. Resolventes quinticos de la ecuación icosaédrica . . . . .	24
3.6. Geometría de la ecuación canónica . . . . .	31



# English Abstract

According to Galois theory, every irreducible quintic whose Galois group is isomorphic to  $\mathcal{A}_5$  can not be solved by radicals, due to this group is not solvable. Since the symmetry group of the icosahedron is also isomorphic to  $\mathcal{A}_5$ , it is natural to think that there is any connection between the solutions of the irreducible quintic and the icosahedron. In this dissertation we will show up this connection.

One of the first things we will do is to build a polyhedral equation associated to the icosahedral Möbius group (the icosahedral equation) and we will study a method based on hypergeometric functions to solve it. After that, we will reduce the general quintic to a simplest form, the so called canonical form. Using the symmetries of the icosahedron, we will be able to build a suitable quintic resolvent whose roots coincide with those of the canonical quintic and can be expressed as a function of the solution of the icosahedral equation.





# 1 | Introducción

La resolución de ecuaciones polinómicas puede ser considerada como uno de los temas de estudio más antiguos de las matemáticas, siendo conocida la resolución de ecuaciones de segundo grado por los babilonios. Sin embargo, la fórmula para resolver ecuaciones de tercer grado utilizando radicales no fue publicada hasta 1545 por Gerolamo Cardano (1501-1576) en su obra *Ars Magna*. Esta fórmula fue descubierta por Scipione del Ferro (1465-1526) y Niccolò Fontana (conocido como Tartaglia, 1499-1557), quienes la mantuvieron en secreto. Tartaglia le confió el secreto a Cardano, quien más tarde lo reveló en su obra. Posteriormente, Ludovico Ferrari (1522-1565) dedujo la fórmula para el caso de cuarto grado.

El siguiente paso era intentar resolver la ecuación general de quinto grado, tarea que intentaron realizar generaciones de matemáticos sin éxito alguno. No fue hasta 1824 cuando Niels Henrik Abel (1802-1829) demostró que la ecuación general de quinto grado no podía resolverse por radicales. Posteriormente, y desconociendo la contribución de Abel, Évariste Galois (1811-1832) creó una nueva rama de las matemáticas (la teoría de Galois) con la que demostró la imposibilidad de resolver por radicales ecuaciones generales de grado mayor o igual a cinco. Sin embargo, esto no quiere decir que no puedan ser resueltas. El matemático francés Charles Hermite (1822-1901) logró dar una solución utilizando funciones modulares elípticas, y el matemático alemán Leopold Kronecker (1823-1891) obtuvo la misma solución utilizando teoría de grupos.

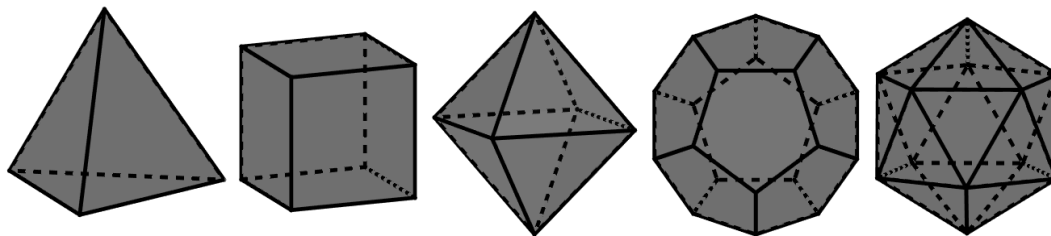
Todo este trabajo previo llevó a Felix Klein (1849-1925) a idear un método en el que relacionó las simetrías del icosaedro, la teoría de Galois y un tipo de funciones especiales denominadas funciones hipergeométricas. Este procedimiento fue publicado en 1884 en su libro *Lecciones sobre el icosaedro y la solución de ecuaciones de quinto grado*. Este método será nuestro principal tema de estudio, aunque en ocasiones recurriremos a deducciones más geométricas y tomaremos los razonamientos más cortos que nos lleven a los resultados principales.



## 2 | Los cinco sólidos platónicos

En este capítulo nos centraremos en el estudio de los famosos sólidos platónicos: el tetraedro, el cubo o hexaedro, el octaedro, el dodecaedro y el icosaedro. Estos cinco poliedros, que destacan por su simetría y especial belleza, fueron estudiados por primera vez en la antigua Grecia. Tal fue su trascendencia que se llegó a identificar al tetraedro, cubo, octaedro e icosaedro con los cuatro elementos de la naturaleza: fuego, tierra, aire y agua (en este orden). El dodecaedro se asoció al universo entero, correspondiéndose cada una de sus caras con un signo del Zodiaco.

En primer lugar veremos cuáles son las propiedades que los hacen únicos. A continuación explicaremos el concepto de dualidad, que nos permitirá relacionar a los sólidos platónicos entre sí y nos facilitará el trabajo para, finalmente, hacer un estudio de sus grupos de simetría.



### 2.1 Poliedros regulares

Comenzaremos recordando que un conjunto  $C \subset \mathbb{R}^n$  se dice convexo si el segmento que une dos puntos cualesquiera de  $C$  está contenido en  $C$ . Definimos el concepto de poliedro convexo  $K$  como cualquier región limitada de  $\mathbb{R}^3$  que se obtiene al intersecar un número finito de semiespacios cerrados. Llamaremos una *cara* de  $K$  a la intersección del poliedro convexo con cualquier plano que sea frontera de uno de

estos semiespacios. Cualquier lado común a dos caras será una *arista*, y los puntos finales de las aristas se llamarán *vértices* de  $K$ .

Antes de definir el concepto de regularidad vamos a detenernos en dos ideas importantes:

1. Diremos que una aplicación  $S : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  es una *isometría* si preserva las distancias, es decir,  $d(S(p), S(q)) = d(p, q)$  para todo  $p, q \in \mathbb{R}^3$ . Denotaremos por  $Iso(\mathbb{R}^3)$  al grupo de todas las isometrías espaciales y por  $Sim(K)$  al grupo de isometrías espaciales que dejan invariante a  $K$ .
2. Definimos una *bandera* de  $K$  como la tripleta  $(p, e, f)$  donde  $p$  es un vértice,  $e$  es una arista y  $f$  es una cara de  $K$ , cumpliendo que  $p \in e \subset f$ .

Una vez definidos estos conceptos, diremos que  $K$  es *regular* si dadas dos banderas  $(p_1, e_1, f_1)$  y  $(p_2, e_2, f_2)$  de  $K$ , existe una isometría  $S \in Sim(K)$  tal que  $S(p_1) = p_2$ ,  $S(e_1) = e_2$  y  $S(f_1) = f_2$ .

Si  $K$  es un poliedro convexo de vértices  $p_1, \dots, p_n$ , definimos el *centroide* de  $K$  como

$$c = \frac{p_1 + \dots + p_n}{n}.$$

Es decir, el punto cuyas coordenadas son la media aritmética de las de los vértices. Tenemos el siguiente resultado:

**Proposición 2.1.** Sea  $S \in Sim(K)$ . Entonces  $S(c) = c$ .

**Demostración.** Consideremos la función  $f : \mathbb{R}^3 \rightarrow \mathbb{R}$  dada por  $f(p) = \sum_{j=1}^n d(p, p_j)^2$ .

Sea  $S \in Sim(K)$ , sabemos que  $S$  permuta los vértices de  $K$ . Por lo tanto:

$$f(S(p)) = \sum_{j=1}^n d(S(p), p_j)^2 = \sum_{j=1}^n d(p, S^{-1}(p_j))^2 = \sum_{j=1}^n d(p, p_j)^2 = f(p).$$

Veamos que  $f$  tiene un mínimo global en  $c$ :

$$\begin{aligned} f(p) &= \sum_{j=1}^n d(p, p_j)^2 = \sum_{j=1}^n \|p - p_j\|^2 = \sum_{j=1}^n (\|p\|^2 - 2p \cdot p_j + \|p_j\|^2) = \\ &= n\|p\|^2 - 2np \cdot c + \sum_{j=1}^n \|p_j\|^2 = n\|p - c\|^2 - n\|c\|^2 + \sum_{j=1}^n \|p_j\|^2. \end{aligned}$$

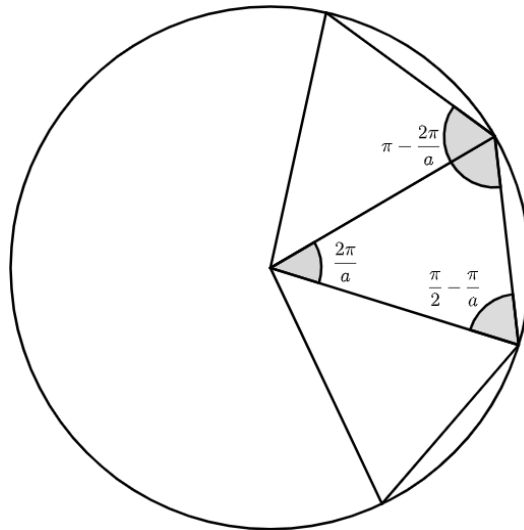
Como el único término que depende de  $p$  es el primero, está claro que  $f$  tiene un mínimo global donde lo tenga  $\|p - c\|^2$ , es decir, en  $c$ . La composición  $f \circ S^{-1}$  tiene

un mínimo global en  $S(c)$ , y como  $f \circ S^{-1} = f$ , estos mínimos tienen que coincidir, por lo que  $S(c) = c$ . |

**Corolario 2.1.** Si  $K$  es regular, su centroide es equidistante a cada vértice. Lo mismo ocurre con las aristas y las caras de  $K$ .

**Demostración.** Se deriva de que la regularidad de  $K$  asegura que dos vértices cualesquiera pueden ser intercambiados mediante una isometría de  $Sim(K)$  que deja fijo al centroide. |

Nuestro objetivo es ver cuántos poliedros regulares existen. Para ello definimos el *símbolo de Schläfli* de cada poliedro regular como  $\{a, b\}$ , donde  $a$  es el número de lados de una cara y  $b$  es el número de caras que se encuentran en un vértice. Cada cara es un polígono regular de  $a$  lados, por lo que el ángulo entre dos aristas de una misma cara y adyacentes es  $\pi - 2\pi/a$ . Para ver esto es suficiente dividir una cara en  $a$  triángulos isósceles conectando los vértices con el centro, y posteriormente medir los ángulos como se muestra en la siguiente figura:



Como en un vértice se encuentran  $b$  caras, la convexidad de  $K$  implica que la suma de los ángulos de dichas caras sea menor que  $2\pi$ . Es decir

$$b \left( \pi - \frac{2\pi}{a} \right) < 2\pi \Rightarrow b \left( 1 - \frac{2}{a} \right) < 2 \Rightarrow (a - 2)(b - 2) < 4.$$

Por definición  $a$  y  $b$  deben de ser mayores que 2, por lo que los casos posibles para el símbolo de Schläfli son:

$$\{3, 3\}, \{3, 4\}, \{4, 3\}, \{3, 5\}, \{5, 3\}.$$

Veamos ahora un conocido teorema que nos permitirá obtener el número de caras, aristas y vértices de cada poliedro regular.

**| Teorema 2.1 (Teorema de Euler para poliedros convexos).** *Sea  $K$  un poliedro convexo (no necesariamente regular). Sean  $V$ ,  $E$  y  $F$  el número de vértices, aristas y caras de  $K$ , respectivamente. Entonces*

$$V - E + F = 2.$$

*Demostración.* Podemos eliminar una de las caras del poliedro y deformar el resto hasta extenderlo sobre un plano. El resultado será un grafo planar conexo con el mismo número de vértices y aristas, pero con una cara menos. Por lo tanto solo es necesario probar que dado un grafo planar conexo se tiene la igualdad  $V - E + F = 1$ . Para ver esto construiremos el grafo paso a paso empezando por un grafo con un único vértice. Para este caso se tiene la igualdad  $V - E + F = 1$ , ya que  $V = 1$ ,  $E = 0$  y  $F = 0$ . Para construir el grafo, en cada paso hacemos una de las siguientes operaciones:

1. Añadimos una nueva arista que una un vértice existente con otro nuevo.
2. Añadimos una nueva arista que una dos vértices existentes, creando una cara.

Como ninguna de estas dos operaciones afecta al valor de la suma  $V - E + F$ , llegamos al resultado deseado. |

Observemos que dado un poliedro regular con símbolo de Schläfli  $\{a, b\}$  tenemos que  $bV = 2E = aF$ . Esto es debido a que si contamos las  $b$  aristas en cada vértice estamos contando las aristas dos veces. Lo mismo obtenemos al contar las  $a$  aristas en cada cara. Este hecho, junto a la igualdad  $V - E + F = 2$ , nos permite expresar  $V$ ,  $E$  y  $F$  en función de  $a$  y  $b$ :

$$V = \frac{4a}{2a + 2b - ab}, \quad E = \frac{2ab}{2a + 2b - ab}, \quad F = \frac{4b}{2a + 2b - ab}.$$

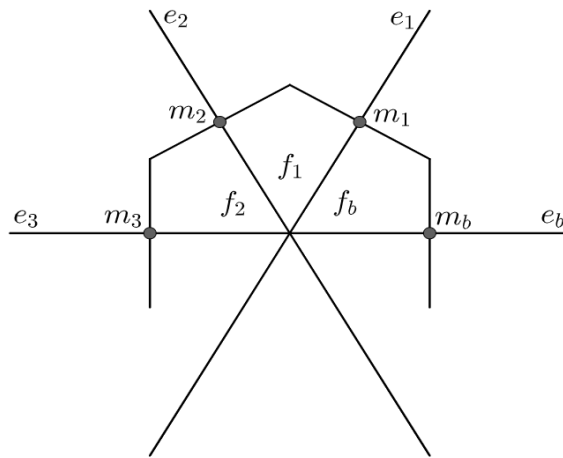
Sustituyendo los posibles valores del símbolo de Schläfli obtenemos los cinco sólidos platónicos:

Poliedro	$\{a, b\}$	$V$	$E$	$F$
Tetraedro	$\{3, 3\}$	4	6	4
Cubo	$\{4, 3\}$	8	12	6
Octaedro	$\{3, 4\}$	6	12	8
Dodecaedro	$\{5, 3\}$	20	30	12
Icosaedro	$\{3, 5\}$	12	30	20

## 2.2 Poliedro dual

Sea un poliedro regular  $P$  con símbolo de Schläfli  $\{a, b\}$  y sea  $p$  un vértice de  $P$ . Denotamos por  $e_1, \dots, e_b$  a las  $b$  aristas que llegan a  $p$ , y por  $f_1, \dots, f_b$  a las caras, de tal modo que  $e_1, e_2 \subset f_1, e_2, e_3 \subset f_2, \dots, e_b, e_1 \subset f_b$ . Sea  $S \in \text{Sim}(P)$  una isometría que lleva la bandera  $(p, e_1, f_1)$  en  $(p, e_2, f_2)$ . Como  $S$  deja fijo al centroide  $c$  y al vértice  $p$ , lo mismo debe pasarle a la recta  $l$  que pasa por estos dos puntos. Además, como  $S(e_2)$  es una arista de  $f_2 = S(f_1)$  distinta a  $e_2$ , tenemos que  $S(e_2) = e_3$ . Razonando de forma análoga tenemos que  $S^j(e_1) = e_{j+1}$  para  $j = 1, \dots, b-1$  y  $S^b(e_1) = e_1$ . Deducimos que  $S$  es una rotación de orden  $b$  y eje  $l$ . Además el grupo cíclico  $\langle S \rangle$  generado por  $S$  es el subgrupo de  $\text{Sim}(P)$  de las isometrías directas que dejan invariante a  $p$ .

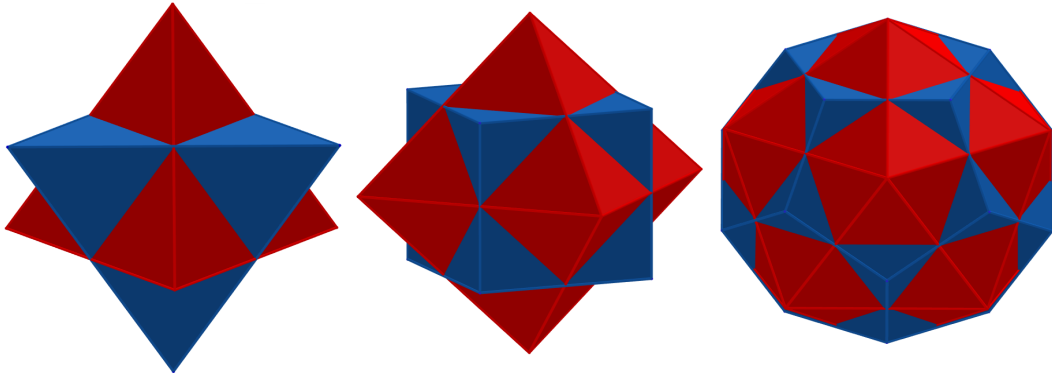
Denotemos por  $m_1, \dots, m_b$  los puntos medios de  $e_1, \dots, e_b$ . Como los vértices (distintos de  $p$ ) de cada  $e_j$  están en la órbita de  $S$ , también lo están los  $m_j$ . Por lo tanto los  $m_j$  pueden ser considerados como los puntos medios de las aristas de un polígono regular de  $b$  lados, como se muestra en la siguiente figura:



Si hacemos esto para los  $V$  vértices de  $P$  y unimos los polígonos resultantes obtenemos un poliedro regular  $P^0$  que llamaremos el dual de  $P$ . Durante la construcción del poliedro dual hemos visto que cada cara de  $P^0$  tiene  $b$  lados. Además, a cada vértice de  $P^0$  llegan  $a$  aristas, por lo que  $P^0$  tiene símbolo de Schläfli  $\{b, a\}$ .

Por consiguiente el dual del tetraedro es él mismo, mientras que el cubo y el oc-

taedro son duales, al igual que el dodecaedro y el icosaedro:



## 2.3 Grupos de simetría de los sólidos platónicos

En esta sección vamos a estudiar los grupos de simetría de los cinco sólidos platónicos. Gracias a la construcción de la sección anterior, es fácil ver que si dos poliedros son duales entonces tendrán el mismo grupo de simetría. Por lo tanto los casos a estudiar se reducen a tres: tetraedro, octaedro e icosaedro.

Consideremos un sólido platónico  $P$  con símbolo de Schläfli  $\{a, b\}$ . El eje de toda rotación debe pasar por un vértice, por el punto medio de una arista o por el centro de una cara. En el primer caso el ángulo de rotación sería un múltiplo entero de  $2\pi/b$ ; en el segundo, un múltiplo entero de  $\pi$ ; y en el tercero, un múltiplo entero de  $2\pi/a$ . Por lo tanto el número total de rotaciones no triviales es

$$\frac{1}{2}(V(b-1) + E + F(a-1)).$$

El factor  $1/2$  se debe a que todo eje rotacional pasa a través de dos de los puntos considerados. Utilizando que  $bV = 2E = aF$  y el teorema de Euler para poliedros convexos, llegamos a que el número total de rotaciones no triviales es  $2E - 1$ . Por lo tanto el orden de  $Sim^+(P)$  (el grupo de isometrías directas de  $P$ ) es  $2E$ .

Para el tetraedro este orden será 12, para el octaedro 24 y para el icosaedro 60. De esta forma el grupo de simetrías directas del tetraedro  $Sim^+(T)$  es isomorfo al grupo alternado  $\mathcal{A}_4$ , el del octaedro  $Sim^+(O)$  es isomorfo a  $\mathcal{S}_4$  y el del icosaedro  $Sim^+(I)$  es isomorfo al grupo alternado  $\mathcal{A}_5$ . Estos grupos se llamarán *grupo tetraédrico*, *octaédrico* e *icosaédrico*, respectivamente.



Ahora estudiaremos cada uno de los grupos de simetría de estos poliedros. Empezaremos con el tetraedro regular  $T$ . Las únicas simetrías planas que dejan invariante a  $T$  son aquellas cuyos planos pasan por una arista y por el punto medio de la arista opuesta. Hay exactamente seis de estos planos, uno por cada arista de  $T$ , por lo que  $Sim(T)$  contiene seis reflexiones. Si consideramos los cuatro vértices de  $T$ , cada elemento  $S \in Sim(T)$  permuta estos vértices, por lo que se puede asociar a una permutación de cuatro elementos. Como caso particular, una reflexión se asociaría a una transposición (permutación que intercambia dos elementos y fija los restantes). Como el grupo simétrico  $\mathcal{S}_4$  consiste en las permutaciones de cuatro elementos y tiene exactamente seis transposiciones, llegamos a que  $Sim(T) \cong \mathcal{S}_4$ .

Para el octaedro y el icosaedro razonamos de la siguiente forma: Sea  $G$  su grupo de simetría y  $G^+ \subset G$  el subgrupo de isometrías directas de  $G$ . Como la composición de dos isometrías indirectas es directa, se tiene que  $|G| = 2|G^+|$ . Es decir,  $G^+$  y cualquier elemento de  $G^- = G - G^+$  generan  $G$ . En nuestro caso la aplicación antipodal (simetría central respecto al centroide  $c$ )

$$\begin{aligned} -I : \mathbb{R}^3 &\rightarrow \mathbb{R}^3 \\ p &\mapsto 2c - p \end{aligned}$$

es un elemento de  $G$ , por lo que  $G^- = (-I) \cdot G^+$  (ya que el término de la derecha es un conjunto de  $|G^+|$  isometrías indirectas en  $G$ ). Como  $-I$  conmuta con los elementos de  $G$ , el subgrupo cíclico  $\{\pm I\} \subset G$  (isomorfo a  $C_2$ ) es normal. Como  $G^+ \subset G$  es normal (ya que es de índice 2), obtenemos que  $G \cong G^+ \times C_2$ .

Resumiendo todo lo que hemos visto hasta ahora:

$P$	$\{a, b\}$	$V$	$E$	$F$	$P^0$	$Sim^+(P)$	$Sim(P)$
Tetraedro	$\{3, 3\}$	4	6	4	Tetraedro	$\mathcal{A}_4$	$\mathcal{S}_4$
Cubo	$\{4, 3\}$	8	12	6	Octaedro	$\mathcal{S}_4$	$\mathcal{S}_4 \times C_2$
Octaedro	$\{3, 4\}$	6	12	8	Cubo	$\mathcal{S}_4$	$\mathcal{S}_4 \times C_2$
Dodecaedro	$\{5, 3\}$	20	30	12	Icosaedro	$\mathcal{A}_5$	$\mathcal{A}_5 \times C_2$
Icosaedro	$\{3, 5\}$	12	30	20	Dodecaedro	$\mathcal{A}_5$	$\mathcal{A}_5 \times C_2$



# 3 | El icosaedro y la irreducibilidad de la quinta

## 3.1 Invariantes

En esta sección daremos algunos resultados básicos sobre los cuales empezaremos a trabajar en las secciones posteriores.

Comenzaremos definiendo  $Möb(\hat{\mathbb{C}})$  como el grupo de Möbius sobre la esfera de Riemann (el plano complejo al que se le añade un punto en el infinito  $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ ), es decir, el grupo generado por las inversiones respecto a circunferencias y las simetrías axiales en  $\hat{\mathbb{C}}$ . Recordemos que los elementos de  $Möb(\hat{\mathbb{C}})$ , dependiendo de si son transformaciones directas o indirectas, son de la forma

$$\frac{az + b}{cz + d} \text{ o } \frac{a\bar{z} + b}{c\bar{z} + d} \text{ con } ad - bc = 1.$$

A los elementos de  $Möb^+(\hat{\mathbb{C}})$  los llamaremos transformaciones fraccionarias lineales o transformaciones de Möbius. Tenemos el siguiente isomorfismo:

$$Möb^+(\hat{\mathbb{C}}) \cong SL(2, \mathbb{C}) / \{\pm I\}$$
$$\frac{az + b}{cz + d} \leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

donde  $SL(2, \mathbb{C})$  denota al grupo lineal especial complejo de las matrices complejas de orden  $2 \times 2$  con determinante 1.

Denotemos por  $h_N : S^2 \rightarrow \hat{\mathbb{C}}$  a la proyección estereográfica desde el polo norte. Tenemos el siguiente resultado:

**| Teorema 3.1 (Teorema de Cayley).** Sea  $p_0 = (a_0, b_0, c_0) \in S^2$  y  $\theta \in \mathbb{R}$ . Sea  $R_\theta(p_0)$  la rotación de ángulo  $\theta$  cuyo eje pasa por el origen y  $p_0$ . Entonces

$$(h_N \circ R_\theta(p_0) \circ h_N^{-1})(z) = \frac{\lambda z - \bar{\mu}}{\mu z + \bar{\lambda}}, \quad z \in \hat{\mathbb{C}},$$

donde

$$\lambda = \cos\left(\frac{\theta}{2}\right) + \text{sen}\left(\frac{\theta}{2}\right) c_0 i, \quad \mu = \sin\left(\frac{\theta}{2}\right) (b_0 + a_0 i).$$

Bajo el isomorfismo  $Möb^+(\hat{\mathbb{C}}) \cong SL(2, \mathbb{C})/\{\pm I\}$ , las transformaciones de Möbius del teorema de Cayley se corresponden con el subgrupo de matrices unitarias  $SU(2, \mathbb{C}) \subset SL(2, \mathbb{C})$ .

Si inscribimos cualquier sólido platónico  $P$  en la esfera unidad y proyectamos desde el origen obtenemos una teselación de  $S^2$ . Aplicando el teorema de Cayley a  $Sim^+(P)$  obtenemos un subgrupo isomorfo en  $Möb^+(\hat{\mathbb{C}})$ ,  $G$ . Llamaremos a los correspondientes subgrupos *grupos tetraédrico, octaédrico e icosaédrico de Möbius*, y los denotaremos por  $\mathcal{T}$ ,  $\mathcal{O}$  y  $\mathcal{I}$ . Denotaremos por  $G^*$  a la imagen inversa de  $G$  bajo la proyección natural  $SU(2, \mathbb{C}) \rightarrow SU(2, \mathbb{C})/\{\pm I\}$ .  $G^*$  se llamará el *grupo binario asociado* a  $G$ , dándose la igualdad  $|G^*| = 2|G|$ .

Sea una función racional  $q : \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ . Definimos su grupo de invarianza  $G$  como aquel formado por los  $g \in Möb(\hat{\mathbb{C}})$  tales que  $q \circ g = q$ . Nuestro objetivo será encontrar una función racional cuyo grupo de invarianza sea un subgrupo  $G$  de  $Möb^+(\hat{\mathbb{C}})$ . Para ello comenzaremos definiendo una *forma* como un polinomio homogéneo  $F : \mathbb{C}^2 \rightarrow \mathbb{C}$ . Estudiaremos la invarianza de las formas bajo el grupo binario  $G^*$ . Diremos que  $F$  es  $G^*$ -invariante si existe un homomorfismo  $\chi_F : G^* \rightarrow \mathbb{C} \setminus \{0\}$  tal que

$$F \circ g = \chi_F(g) \cdot F, \quad g \in G^*.$$

Se dirá que  $F$  es un invariante absoluto de  $G^*$  si  $\chi_F = 1$ . Supongamos construidas dos formas  $P$  y  $Q$ ,  $G^*$ -invariantes, del mismo grado y con  $\chi_P = \chi_Q$ . Gracias a la homogeneidad el cociente  $P/Q$  definirá nuestra función racional  $q : \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$  como

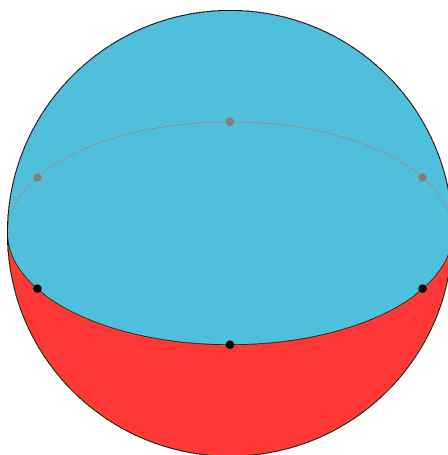
$$q(z) = \frac{P(z_1, z_2)}{Q(z_1, z_2)}, \quad z = \frac{z_1}{z_2}, \quad z_1, z_2 \in \mathbb{C}.$$

Para cada sólido platónico  $P$  con símbolo de Schläfli  $\{a, b\}$  existen tres formas  $F_0, F_1, F_2$  de grados  $|G|/\nu_0, |G|/\nu_1$  y  $|G|/\nu_2$  (donde  $\nu_0 = b, \nu_1 = 2$  y  $\nu_2 = a$ ) tales que  $F_0^{\nu_0}, F_1^{\nu_1}$  y  $F_2^{\nu_2}$  son linealmente dependientes: existen  $\lambda_0, \lambda_1$  y  $\lambda_2$  tales que

$$\lambda_0 F_0^{\nu_0} + \lambda_1 F_1^{\nu_1} + \lambda_2 F_2^{\nu_2} = 0.$$

Estas formas se caracterizan por anularse en ciertos puntos de  $\mathbb{P}^1(\mathbb{C})$ . Si identificamos  $z \in \mathbb{C}$  con el punto proyectivo  $(z : 1)$  y  $\infty \in \hat{\mathbb{C}}$  con  $(1 : 0)$ , entonces  $F_0$  se anula en la imagen por  $h_N$  de los vértices de la teselación de  $S^2$  dada por  $P$ ,  $F_1$  en los puntos medios de las aristas y  $F_2$  en los centros de las caras. Además, toda forma  $G^*$ -invariante puede escribirse como un polinomio en  $F_0$ ,  $F_1$  y  $F_2$ .

El mismo razonamiento es válido para el diedro, un poliedro esférico cuyos vértices son los  $n$  puntos de  $\hat{\mathbb{C}}$  soluciones de  $z^n = 1$ . Su símbolo de Schläfli es  $\{n, 2\}$  y su grupo de Möbius, que se denota por  $\mathcal{D}_n$ , tiene  $2n$  elementos.



También podemos considerar el grupo cíclico  $\mathcal{C}_n \subset \text{Möb}^+(\hat{\mathbb{C}})$  de las rotaciones  $z \mapsto e^{2k\pi i/n} z$  con  $k = 0, \dots, n-1$ , obteniéndose las formas  $z_1^n$  y  $z_2^n$ .

Las tres formas para el diedro son:

$$\alpha = \frac{z_1^n - z_2^n}{2}, \quad \beta = \frac{z_1^n + z_2^n}{2}, \quad \gamma = z_1 z_2.$$

Para el tetraedro son:

$$\Phi = z_1^4 - 2\sqrt{3}iz_1^2 z_2^2 + z_2^4, \quad \Omega = z_1 z_2 (z_1^4 - z_2^4), \quad \Psi = z_1^4 + 2\sqrt{3}iz_1^2 z_2^2 + z_2^4.$$

Para el octaedro son  $\Omega$ ,  $(\Phi^3 + \Psi^3)/2$  y  $\Phi\Psi$ , mientras que para el icosaedro tenemos los siguientes invariantes absolutos:

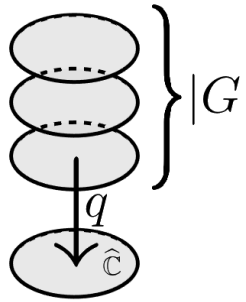
$$\begin{aligned} \mathcal{I} &= z_1 z_2 (z_1^{10} + 11z_1^5 z_2^5 - z_2^{10}), \\ \mathcal{J} &= (z_1^{30} + z_2^{30}) + 522(z_1^{25} z_2^5 - z_1^5 z_2^{25}) - 10005(z_1^{20} z_2^{10} + z_1^{10} z_2^{20}), \\ \mathcal{H} &= -(z_1^{20} + z_2^{20}) + 228(z_1^{15} z_2^5 - z_1^5 z_2^{15}) - 494z_1^{10} z_2^{10}. \end{aligned}$$

La dependencia lineal en cada caso es:

$$\begin{aligned} \alpha^2 - \beta^2 + \gamma^n &= 0, & \Phi^3 - 12\sqrt{3}i\Omega^2 - \Psi^3 &= 0, \\ 108\Omega^4 + \left(\frac{\Phi^3 + \Psi^3}{2}\right)^2 - (\Phi\Psi)^3 &= 0, & 1728\mathcal{I}^5 - \mathcal{J}^2 - \mathcal{H}^3 &= 0. \end{aligned}$$

### 3.2 Ecuaciones poliédricas

Sea un subgrupo finito  $G$  de  $Möb^+(\hat{\mathbb{C}})$  y una función racional  $q : \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$  que sea  $G$ -invariante. Como  $q \circ g = q$  si y solo si  $g \in G$ ,  $q$  puede ser considerada como la proyección de un recubrimiento cuyo número de ramas es  $|G|$ .



Los puntos de ramificación serán los puntos fijos de las transformaciones de Möbius de  $G$ . Equivalentemente,  $z \in \hat{\mathbb{C}}$  es un punto de ramificación si y solo si la  $G$ -órbita  $G(z)$  no es principal. En este caso  $|G(z)| = |G|/\nu$  y el número de ramificación asociado a  $z$  será  $\nu - 1$ . A  $q(z)$  se le denomina el valor de ramificación de  $z$ .

Para los sólidos platónicos  $q = (-\lambda_2 F_2^{\nu_2})/(\lambda_0 F_0^{\nu_0})$ . Los puntos de ramificación se dividen en tres órbitas: los vértices, los puntos medios de las aristas y los centros de las caras. Por lo tanto el número de ramificación asociado a cada vértice será  $\nu_0 - 1$ , el de los puntos medios de las aristas será  $\nu_1 - 1$  y el de los centros de las caras  $\nu_2 - 1$ . Los valores de ramificación son  $w = \infty$ ,  $w = 1$  y  $w = 0$ , respectivamente.

Si  $q = P/Q$ , dado  $w \in \mathbb{C}$ , la ecuación  $q(z) = w$  puede ser escrita como una ecuación polinomial de grado  $|G|$ :

$$P(z) - wQ(z) = 0.$$

Esta será llamada *la ecuación poliédrica asociada a  $G$* , la cual tiene  $|G|$  soluciones (contando multiplicidad).

Para el caso del grupo cíclico  $\mathcal{C}_n$  tenemos que  $q = (z_1^n)/(z_2^n) = z^n$  por lo que la ecuación asociada es  $z^n = w$ , cuyas soluciones son las raíces  $n$ -ésimas de  $w$ .

Para el diedro tenemos:

$$q_{\mathcal{D}_n}(z) = -\frac{\alpha(z_1, z_2)^2}{\gamma(z_1, z_2)^n} = -\frac{(z_1^n - z_2^n)^2}{4z_1^n z_2^n} = -\frac{(z^n - 1)^2}{4z^n} = w.$$

De esta forma obtenemos la ecuación del diedro:

$$4wz^n + (z^n - 1)^2 = 0.$$

Que se trata de una ecuación cuadrática en  $z^n$  cuyas  $2n$  soluciones son:

$$z = q_{\mathcal{D}_n}^{-1}(w) = \sqrt[n]{1 - 2w \pm 2\sqrt{w(w-1)}}.$$

Es decir, para invertir  $q_{\mathcal{D}_n}$  es necesario hacer una raíz cuadrada seguida de una  $n$ -ésima.

Para el tetraedro tenemos:

$$q_{\mathcal{T}}(z) = \frac{\Psi(z_1, z_2)^3}{\Phi(z_1, z_2)^3} = \left( \frac{z_1^4 + 2\sqrt{3}iz_1^2z_2^2 + z_2^4}{z_1^4 - 2\sqrt{3}iz_1^2z_2^2 + z_2^4} \right)^3 = \left( \frac{z^4 + 2\sqrt{3}iz^2 + 1}{z^4 - 2\sqrt{3}iz^2 + 1} \right)^3 = w.$$

Tomando raíces cúbicas en ambos lados llegamos a una ecuación cuadrática en  $z^2$  que puede ser fácilmente resuelta. Además, utilizando la expresión para  $q_{\mathcal{D}_2}$  podemos escribir  $q_{\mathcal{T}}$  como:

$$q_{\mathcal{T}}(z) = \left( \frac{q_{\mathcal{D}_2} - e^{\pi i/3}}{q_{\mathcal{D}_2} + e^{2\pi i/3}} \right)^3.$$

Por lo tanto para invertir  $q_{\mathcal{T}}$  es necesario el cálculo de una raíz cúbica seguida de dos raíces cuadradas.

Para el octaedro:

$$q_{\mathcal{O}}(z) = \frac{(\Phi\Psi)^3}{108\Omega^4} = w.$$

Por lo que:

$$\frac{w}{w-1} = \frac{q_{\mathcal{O}}(z)}{q_{\mathcal{O}}(z)-1} = \frac{(\Phi\Psi)^3}{(\Phi\Psi)^3 - 108\Omega^4} = \frac{(\Phi\Psi)^3}{\left(\frac{\Phi^3+\Psi^3}{2}\right)^2} = \frac{(\Psi/\Phi)^3}{\left(\frac{(\Psi/\Phi)^3+1}{2}\right)^2} = \frac{q_{\mathcal{T}}}{\left(\frac{q_{\mathcal{T}}+1}{2}\right)^2}.$$

De esta forma el invertir  $q_{\mathcal{O}}$  es equivalente a calcular una raíz cuadrada, una cúbica y posteriormente dos cuadradas. En vista de la teoría de Galois, notemos que esta

secuencia coincide con los índices de la serie de subgrupos normales  $\mathcal{S}_4 \supset \mathcal{A}_4 \supset D_2 \supset C_2 \supset \{1\}$ , la cual es 2, 3, 2, 2.

Para el icosaedro tenemos:

$$q_I(z) = \frac{\mathcal{H}^3}{1728\mathcal{I}^5} = w.$$

Por lo que la ecuación icosaédrica será:

$$\mathcal{H}^3(z, 1) - 1728w\mathcal{I}^5(z, 1) = 0,$$

$$\left((z^{20} + 1) - 228(z^{15} - z^5) + 494z^{10}\right)^3 + 1728wz^5(z^{10} + 11z^5 - 1)^5 = 0.$$

Como veremos en las próximas secciones, es imposible expresar sus soluciones mediante radicales.

### 3.3 Funciones hipergeométricas

Como la ecuación icosaédrica no se puede resolver por radicales, es necesario buscar otro procedimiento para expresar las soluciones de forma explícita. En esta sección veremos que cualquier solución de una ecuación poliédrica puede ser escrita como el cociente de dos soluciones linealmente independientes de una ecuación diferencial lineal homogénea de segundo orden con exactamente tres puntos singulares regulares. Estas ecuaciones diferenciales son llamadas *hipergeométricas*, y sus soluciones *funciones hipergeométricas*. Equivalentemente, veremos que la inversa  $q^{-1}$  es el cociente de dos funciones hipergeométricas.

Sea  $G \subset \text{Möb}^+(\hat{\mathbb{C}})$  el grupo de invarianza de  $q$ . Recordemos que  $q$  es la proyección de un recubrimiento de  $|G|$  ramas con valores de ramificación  $w_0 = 0$ ,  $w_1 = 1$  y  $w_2 = \infty$  y números de ramificación asociados  $\nu_2 - 1$ ,  $\nu_1 - 1$  y  $\nu_0 - 1$ , por lo que su inversa  $q^{-1}$  será una función multivaluada. Para pasar de una rama a otra solo es necesario componer  $q^{-1}$  con los elementos de  $G$ . Como la derivada Schwarziana

$$\mathcal{S}(f) = \left(\frac{f''}{f'}\right)' - \frac{1}{2} \left(\frac{f''}{f'}\right)^2$$

se caracteriza por ser invariante únicamente bajo transformaciones de Möbius,  $\mathcal{S}(q^{-1})$  debe ser una función univaluada racional  $s : \mathbb{C} \rightarrow \mathbb{C}$ . Determinaremos  $s$  explícitamente tomando su serie de Laurent en los polos.



Como  $q^{-1}$  es multivaluada, cerca de un valor de ramificación  $w_j$  con número de ramificación  $\nu_{2-j} - 1$  se tiene el desarrollo

$$q^{-1}(w) - q^{-1}(w_j) = \sum_{k=1}^{\infty} a_k (w - w_j)^{k/\nu_{2-j}},$$

donde  $q^{-1}(w_j)$  indica una de las  $|G|/\nu_{2-j}$  preimágenes y  $q^{-1}(w)$  está cerca de  $q^{-1}(w_j)$ . Cuando  $w_j = \infty$  en lugar de  $w - w_j$  ponemos  $1/w$ . Sustituyendo este desarrollo en la expresión de la derivada Schwarziana obtenemos los términos iniciales de la expansión de Laurent de  $s$  en  $w_0 = 0$ ,  $w_1 = 1$  y  $w_2 = \infty$ :

$$\frac{\nu_2^2 - 1}{2\nu_2^2 w^2}, \quad \frac{\nu_1^2 - 1}{2\nu_1^2 (w - 1)^2}, \quad \frac{\nu_0^2 - 1}{2\nu_0^2 w^2}.$$

Por lo tanto

$$s(w) = \frac{\nu_2^2 - 1}{2\nu_2^2 w^2} + \frac{A}{w} + \frac{\nu_1^2 - 1}{2\nu_1^2 (w - 1)^2} + \frac{B}{w - 1} + P(w),$$

donde  $A$  y  $B$  son números complejos y  $P$  es un polinomio. Al hacer el cambio de variable  $w \mapsto 1/w$ , el primer término de la expansión de Laurent es

$$\frac{\nu_0^2 - 1}{2\nu_0^2} w^2,$$

por lo que  $P$  debe ser nulo. Utilizando el mismo argumento con los demás sumandos de  $s$  llegamos a las restricciones:

$$A + B = 0, \quad \frac{\nu_2^2 - 1}{2\nu_2^2} + \frac{\nu_1^2 - 1}{2\nu_1^2} + B = \frac{\nu_0^2 - 1}{2\nu_0^2}.$$

Con todo esto tenemos que

$$\mathcal{S}(q^{-1}) = s(w) = \frac{\nu_2^2 - 1}{2\nu_2^2 w^2} + \frac{\nu_1^2 - 1}{2\nu_1^2 (w - 1)^2} + \frac{\frac{1}{\nu_1^2} + \frac{1}{\nu_2^2} - \frac{1}{\nu_0^2} - 1}{2w(w - 1)}.$$

La solución de esta ecuación coincide con el cociente de dos soluciones linealmente independientes de la ecuación diferencial hipergeométrica

$$z'' = p(w)z' + q(w)z,$$

donde  $p$  y  $q$  cumplen que

$$s = p' - \frac{1}{2}p^2 - 2q.$$

Tomando  $p(w) = -1/w$  y  $q$  tal que satisfaga lo anterior, llegamos a

$$z'' + \frac{1}{w}z' + \frac{-\frac{1}{\nu_2^2} + \left(\frac{1}{\nu_0^2} + \frac{1}{\nu_2^2} - \frac{1}{\nu_1^2} + 1\right)w - \frac{1}{\nu_0^2}w^2}{4w^2(w-1)^2}z = 0.$$

Este es un caso especial de la ecuación diferencial hipergeométrica

$$z'' - \frac{1 - \alpha_1 - \alpha_2 - (1 + \gamma_1 + \gamma_2)w}{w(w-1)}z' + \frac{\alpha_1\alpha_2 - (\alpha_1\alpha_2 - \beta_1\beta_2 + \gamma_1\gamma_2)w + \gamma_1\gamma_2w^2}{w^2(w-1)^2}z = 0,$$

donde

$$\alpha_1 = -\alpha_2 = \frac{1}{2\nu_2}, \quad \beta_1 = \frac{1}{2\nu_1}, \quad \beta_2 = \frac{\nu_1^2 - 1}{2\nu_1}, \quad \gamma_1 = -\gamma_2 = \frac{1}{2\nu_0},$$

ya que  $\nu_2 = 2$ . Sean

$$a = \alpha_1 + \beta_1 + \gamma_1, \quad b = \alpha_1 + \beta_1 + \gamma_2, \quad c = 1 + \alpha_1 - \alpha_2.$$

Entonces podemos escribir la ecuación diferencial como

$$w(1-w)z'' + (c - (a+b+1))z' - abz = 0.$$

Las soluciones de esta ecuación pueden ser expresadas en series de potencias centradas en 0, 1 o  $\infty$ . Para ello utilizaremos la serie hipergeométrica

$$F(a, b, c, w) = 1 + \frac{a \cdot b}{1 \cdot c}w + \frac{a(a+1) \cdot b(b+1)}{1 \cdot 2 \cdot c(c+1)}w^2 + \frac{a(a+1)(a+2) \cdot b(b+1)(b+2)}{1 \cdot 2 \cdot 3 \cdot c(c+1)(c+2)}w^3 + \dots,$$

que converge en  $|w| \leq 1$  si  $c$  no es un entero negativo y si  $Re(c-a-b) > 0$ , lo cual es cierto para todos los casos considerados. Dos soluciones linealmente independientes centradas en  $\infty$  son

$$F_1(w) = w^{-a}F(a, 1+a-c, 1+a-b, 1/w),$$

$$F_2(w) = w^{-b}F(b, 1+b-c, 1+b-a, 1/w).$$

Estas soluciones son válidas para  $|w| \geq 1$ . En los puntos donde la serie hipergeométrica diverge podemos utilizar la extensión analítica dada por

$$F(a, b, c, w) = \frac{\Gamma(c)\Gamma(b-a)}{\Gamma(b)\Gamma(c-a)}(-1)^{-a}F_1(w) + \frac{\Gamma(c)\Gamma(a-b)}{\Gamma(a)\Gamma(c-b)}(-1)^{-b}F_2(w).$$

Por lo tanto  $q^{-1}$  se obtiene al aplicar una transformación de Möbius al cociente de estas dos soluciones. Para el caso del icosaedro, obtenemos

$$q^{-1}(w) = \frac{F\left(\frac{31}{60}, \frac{11}{60}, \frac{6}{5}, \frac{1}{w}\right)}{(1728w)^{1/5}F\left(\frac{19}{60}, -\frac{1}{60}, \frac{4}{5}, \frac{1}{w}\right)}.$$

### 3.4 La transformación de Tschirnhaus

En esta sección reduciremos la quintica general

$$z^5 + a_1z^4 + a_2z^3 + a_3z^2 + a_4z + a_5 = 0$$

a una forma más simple

$$z^5 + \tilde{a}_1z^4 + \tilde{a}_2z^3 + \tilde{a}_3z^2 + \tilde{a}_4z + \tilde{a}_5 = 0,$$

donde algunos de los coeficientes son nulos. Para ello utilizaremos la llamada transformación de Tschirnhaus, dada por

$$\tilde{z} = \sum_{i=1}^4 \lambda_i z^{(i)},$$

donde los  $\lambda_i$  son a determinar y

$$z^{(i)} = z^i - \frac{1}{5} \sum_{j=1}^5 z_j^i,$$

donde  $z_1, \dots, z_5$  son las raíces de la quintica original. Como

$$z^5 + a_1z^4 + a_2z^3 + a_3z^2 + a_4z + a_5 = (z - z_1) \dots (z - z_5),$$

llegamos a la relación

$$a_k = (-1)^k \sum_{l_1 < \dots < l_k} z_{l_1} \dots z_{l_k} =: (-1)^k e_k(z_1, \dots, z_5).$$

Por el teorema fundamental de los polinomios simétricos, la suma de potencias que aparece en la expresión de  $z^{(i)}$  (que es un polinomio simétrico en las raíces) puede ser expresada como un polinomio en  $\{e_k(z_1, \dots, z_5)\}_{k=1}^5$ , y por lo tanto en los coeficientes  $a_1, \dots, a_5$ . Por ejemplo, como

$$\sum_{j=1}^5 z_j = -a_1, \quad \sum_{j=1}^5 z_j^2 = a_1^2 - 2a_2,$$

tenemos

$$z^{(1)} = z + \frac{a_1}{5}, \quad z^{(2)} = z^2 - \frac{1}{5} (a_1^2 - 2a_2).$$

De esta forma  $\tilde{z}$  es un polinomio en  $z$  de grado menor o igual a 4 con coeficientes en  $\mathbb{Q}[a_1, \dots, a_5]$  y que depende de las constantes  $\lambda_1, \dots, \lambda_4$ .

Tras aplicar la transformación de Tschirnhaus, la nueva quíntica reducida tendrá raíces  $\tilde{z}_1, \dots, \tilde{z}_5$ , donde

$$\tilde{z}_j = \sum_{i=1}^4 \lambda_i z_j^{(i)}, \quad j = 1, \dots, 5.$$

Además

$$\sum_{j=1}^5 \tilde{z}_j = \sum_{j=1}^5 \sum_{i=1}^4 \lambda_i z_j^{(i)} = \sum_{i=1}^4 \lambda_i \sum_{j=1}^5 z_j^{(i)} = 0$$

porque

$$\sum_{j=1}^5 z_j^{(i)} = \sum_{j=1}^5 \left( z_j^i - \frac{1}{5} \sum_{k=1}^5 z_k^i \right) = \sum_{j=1}^5 z_j^i - \sum_{k=1}^5 z_k^i = 0.$$

De esta forma, para cualquier transformación de Tschirnhaus

$$\tilde{a}_1 = - \sum_{j=1}^5 \tilde{z}_j = 0.$$

Buscaremos una transformación de Tschirnhaus en la que  $\tilde{a}_2 = 0$  de la forma

$$\tilde{z} = \lambda z^{(1)} + z^{(2)} = \lambda \left( z + \frac{a_1}{5} \right) + z^2 - \frac{1}{5} (a_1^2 - 2a_2),$$

donde hemos fijado  $\lambda_1 = \lambda$  a determinar,  $\lambda_2 = 1$ ,  $\lambda_3 = \lambda_4 = 0$ . Como

$$\sum_{j=1}^5 \tilde{z}_j^2 = \tilde{a}_1^2 - 2\tilde{a}_2 = -2\tilde{a}_2,$$

entonces  $\tilde{a}_2 = 0$  es equivalente a

$$0 = \sum_{j=1}^5 \tilde{z}_j^2 = \sum_{j=1}^5 \left( \lambda z_j^{(1)} + z_j^{(2)} \right)^2 = \lambda^2 \sum_{j=1}^5 \left( z_j^{(1)} \right)^2 + 2\lambda \sum_{j=1}^5 z_j^{(1)} z_j^{(2)} + \sum_{j=1}^5 \left( z_j^{(2)} \right)^2.$$

De nuevo por el teorema fundamental de los polinomio simétricos, los coeficientes de esta ecuación cuadrática en  $\lambda$  pueden ser escritos en términos de  $a_1, \dots, a_5$ :

$$\sum_{j=1}^5 \left( z_j^{(1)} \right)^2 = \frac{4}{5} a_1^2 - 2a_2, \quad \sum_{j=1}^5 z_j^{(1)} z_j^{(2)} = -\frac{4}{5} a_1^3 + \frac{13}{5} a_1 a_2 - 3a_3,$$

$$\sum_{j=1}^5 \left( z_j^{(2)} \right)^2 = \frac{4}{5} a_1^4 - \frac{16}{5} a_1^2 a_2 + \frac{6}{5} a_2^2 + 4a_1 a_3 - 4a_4.$$

Para calcular los dos valores de  $\lambda$  soluciones de esta ecuación es necesario hacer la raíz cuadrada de la expresión

$$4 \left( \sum_{j=1}^5 z_j^{(1)} z_j^{(2)} \right)^2 - 4 \left( \sum_{j=1}^5 \left( z_j^{(1)} \right)^2 \right) \left( \sum_{j=1}^5 \left( z_j^{(2)} \right)^2 \right),$$

o equivalentemente del discriminante  $\delta$  que se obtiene al dividir lo anterior por

$$\left( \sum_{j=1}^5 \left( z_j^{(1)} \right)^2 \right)^2.$$

El cuerpo más pequeño sobre el cual está definida la quintica original es  $k = \mathbb{Q}(a_1, \dots, a_5)$ . Sabemos que  $\delta \in k$ , pero generalmente  $\sqrt{\delta} \notin k$ , por lo que será necesaria una extensión cuadrática de  $k$ . De esta forma el problema de solubilidad de la quintica original se reduce a la solubilidad de

$$P(z) = z^5 + 5az^2 + 5bz + c,$$

donde hemos añadido factores constantes por conveniencia. Una quintica de esta forma se dice que es *canónica*. Por el teorema fundamental de los polinomios simétricos sabemos que su discriminante

$$\delta = \prod_{1 \leq i < j \leq 5} (z_i - z_j)^2$$

puede escribirse como un polinomio en  $a$ ,  $b$  y  $c$ :

$$\frac{\delta}{5^5} = 108a^5c - 135a^4b^2 + 90a^2bc^2 - 320ab^3c + 256b^5 + c^4.$$

Sean  $z_1, \dots, z_5$  las raíces de la quintica canónica. Consideremos el punto proyectivo complejo  $(z_1 : \dots : z_5) \in \mathbb{P}^4(\mathbb{C})$  (descartando el caso donde  $P(z) = z^5$  y  $z_1 = \dots = z_5 = 0$ ). A partir de este punto podemos recuperar las raíces utilizando las expresiones vistas anteriormente para el discriminante, por lo que no perdemos información al homogeneizar. Como no podemos fijar ningún orden genérico en las raíces, consideramos los 120 puntos proyectivos que forman una órbita en  $\mathbb{P}^4(\mathbb{C})$  bajo la acción de  $\mathcal{S}_5$ , que actúa permutando las coordenadas homogéneas.

Como nuestra ecuación es la canónica, las raíces satisfacen las relaciones

$$\sum_{j=1}^5 z_j = 0, \quad \sum_{j=1}^5 z_j^2 = 0.$$

Por lo tanto el punto  $(z_1 : \dots : z_5)$  se encuentra en

$$\mathcal{Q}_0 = \left\{ (z_1 : \dots : z_5) \in \mathbb{P}^4(\mathbb{C}) : \sum_{j=1}^5 z_j = \sum_{j=1}^5 z_j^2 = 0 \right\},$$

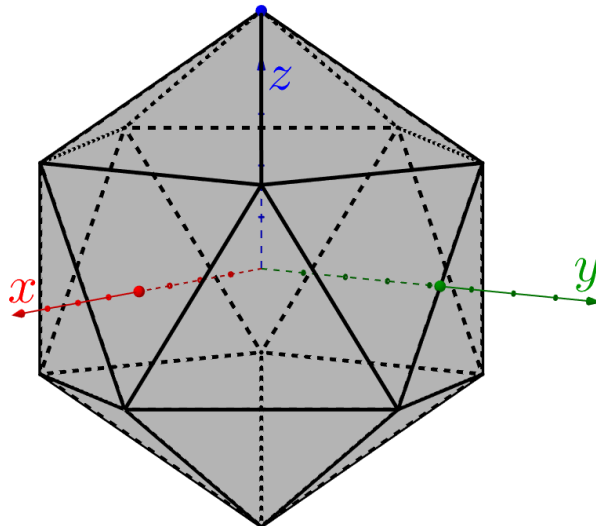
que se puede identificar con una cuádrlica proyectiva compleja en  $\mathbb{P}^3(\mathbb{C})$  una vez que identifiquemos  $\mathbb{P}^3(\mathbb{C})$  con el hiperplano proyectivo

$$\mathbb{P}_0^3(\mathbb{C}) = \left\{ (z_1 : \dots : z_5) \in \mathbb{P}^4(\mathbb{C}) : \sum_{j=1}^5 z_j = 0 \right\}.$$

La interpretación geométrica de la transformación de Tschirnhaus es la siguiente: empezamos con el punto proyectivo  $(z_1 : \dots : z_5) \in \mathbb{P}^4(\mathbb{C})$  cuyas coordenadas homogéneas son las raíces de la quintica general. Consideramos los puntos proyectivos  $(z_1^{(1)} : \dots : z_5^{(1)})$  y  $(z_1^{(2)} : \dots : z_5^{(2)})$  que se encuentran en  $\mathbb{P}_0^3(\mathbb{C})$  para posteriormente tomar una de las dos intersecciones de la recta proyectiva que pasa por estos dos puntos con la cuádrlica  $\mathcal{Q}_0$ . La transformación de Tschirnhaus asocia a  $(z_1 : \dots : z_5)$  este punto de intersección en  $\mathcal{Q}_0$ .

### 3.5 Resolventes quinticos de la ecuación icosaédrica

Podemos inscribir el icosaedro en  $S^2$  de forma que los polos norte y sur sean vértices y el segundo eje de coordenadas pase a través del punto medio de una arista, como se muestra en la siguiente imagen:



En esta posición los 60 elementos del grupo icosaédrico de Möbius  $\mathcal{I}$  son:

$$z \mapsto \omega^j z, \quad -\frac{1}{\omega^j z}, \quad \omega^j \frac{-(\omega - \omega^4)\omega^k z + (\omega^2 - \omega^3)}{(\omega^2 - \omega^3)\omega^k z + (\omega - \omega^4)},$$

$$\omega^j \frac{(\omega^2 - \omega^3)\omega^k z + (\omega - \omega^4)}{(\omega - \omega^4)\omega^k z - (\omega^2 - \omega^3)}, \quad j, k = 0, \dots, 4.$$

donde  $\omega = e^{2\pi i/5}$  es una raíz quinta primitiva de la unidad.

En esta sección trabajaremos en un cuerpo  $k \subset \mathbb{C}$  de característica cero y tal que  $\omega \in k$ , por lo que  $\mathbb{Q}(\omega) \subset k$ . Esto nos asegura que las transformaciones del grupo icosaédrico de Möbius  $\mathcal{I} = \mathcal{A}_5$  están definidas sobre  $k$ . Como en la ecuación icosaédrica aparece un parámetro arbitrario  $w \in \mathbb{C}$ , consideraremos esta ecuación definida sobre  $k(w)$ , el cuerpo de las funciones racionales en la variable  $w$  y con coeficientes en  $k$ . Sea  $z$  una solución de la ecuación icosaédrica. Como  $q(z) = w$ , el cuerpo  $k(z)$  contiene a  $k(w)$ .

Cada  $g \in \mathcal{I}$  define un automorfismo del cuerpo  $k(z)$  mediante sustitución, es decir, a cada  $r^* \in k(z)$  le hacemos corresponder  $r^* \circ g^{-1}$ . Como  $q$  es  $\mathcal{I}$ -invariante, estos automorfismos fijan el subcuerpo  $k(w)$ . De hecho  $k(w)$  es el mayor subcuerpo fijo por todos estos automorfismos. Por lo tanto la extensión  $k(z)/k(w)$  es de Galois, con grupo de Galois isomorfo a  $\mathcal{A}_5$ . Es más,  $k(z)$  es el cuerpo de descomposición de la ecuación icosaédrica sobre  $k(w)$ , siendo las soluciones los 60 elementos de  $k(z)$  que representan las transformaciones de  $\mathcal{I}$ . Además, como  $\mathcal{A}_5$  actúa transitivamente en estas soluciones, la ecuación icosaédrica es irreducible sobre  $k(w)$ .

Sea una extensión de Galois  $K/k$  cuyo grupo de Galois es  $G$ . Pongamos  $K$  como el cuerpo de descomposición de un polinomio  $P \in k[z]$  con raíces  $z_1, \dots, z_n$ . Llamaremos *polinomio resolvente de  $P$*  a cualquier polinomio de la forma

$$P^*(z) = \prod_{j=1}^{n^*} (z - z_j^*),$$

cuyas raíces  $\{z_1^*, \dots, z_{n^*}^*\}$  forman una  $G$ -órbita en  $K$ . Notemos que cada  $z_j^*$  es una función racional en  $z_1, \dots, z_n$ . En nuestro caso, un elemento  $r^* \in k(z) \setminus k(w)$  tiene polinomio resolvente

$$P^*(X) = \prod_{j=1}^{n^*} (X - r_j^*),$$

donde  $\mathcal{A}_5(r^*) = \{r_1^*, \dots, r_{n^*}^*\}$  es la órbita de  $r^*$ .  $P^*$  tiene coeficientes en  $k(w)$  y como  $\mathcal{I}$  es simple,  $k(z) = k(r_1^*, \dots, r_{n^*}^*)$ .

Nuestro objetivo principal es establecer una conexión entre la quintica en forma canónica

$$P(z) = z^5 + 5az^2 + 5bz + c$$

y las soluciones de la ecuación icosaédrica

$$\mathcal{H}^3(z, 1) - 1728w\mathcal{I}^5(z, 1) = 0.$$

Como esta última es una ecuación polinomial de grado 60, buscaremos un resolvente quintico adecuado de  $\mathcal{H}^3 - 1728w\mathcal{I}^5$  que sea directamente comparable con nuestra quintica canónica. Es decir, queremos encontrar un resolvente quintico en forma canónica que contenga, además de  $w$ , dos parámetros más,  $u$  y  $v$ :

$$P^*(z) = z^5 + 5a(u, v, w)z^2 + 5b(u, v, w)z + c(u, v, w).$$

Queremos que los coeficientes sean funciones racionales en  $u$ ,  $v$  y  $w$ . Además, como  $P^*$  es un resolvente icosaédrico, necesitamos poder expresar las raíces de  $P^*$  en términos de las soluciones de la ecuación icosaédrica (o equivalentemente, en términos de funciones hipergeométricas).

Una vez que tengamos  $P^*$ , la relación con la quintica  $P$  equivale a resolver el sistema

$$\begin{cases} a(u, v, w) = a, \\ b(u, v, w) = b, \\ c(u, v, w) = c. \end{cases}$$

junto con la restricción adicional

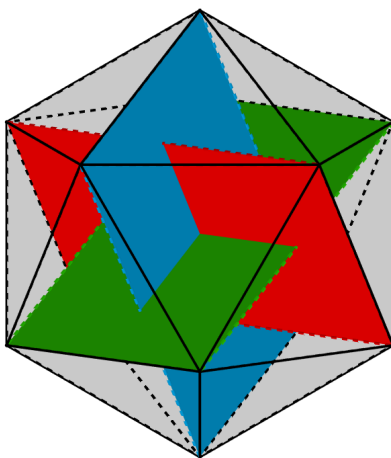
$$\sqrt{\delta(u, v, w)} = \sqrt{\delta},$$

donde  $\delta(u, v, w)$  es el discriminante de  $P^*$ . De este razonamiento deducimos que las raíces de  $P$  y  $P^*$  coinciden como conjuntos. Para obtener una correspondencia biunívoca tendremos que ver cómo actúa el grupo de Galois  $\mathcal{A}_5$  en cada conjunto de raíces.

Las cinco raíces de  $P^*$  constituyen una órbita de  $\mathcal{A}_5$  en la extensión  $k(z)/k(w)$ , por lo que necesitamos encontrar cinco funciones racionales en  $z$  que sean permutadas entre sí por las sustituciones icosaédricas. Como es mucho más fácil construir formas, nuestro propósito será encontrar una  $\mathcal{A}_5$ -órbita formada por cinco formas. Para ello consideraremos trios de rectángulos perpendiculares entre sí e inscritos en



el icosaedro, como se muestra en la siguiente figura:



Los 15 pares de aristas opuestas del icosaedro nos dan un total de 15 rectángulos inscritos. Agrupándolos de tres en tres obtenemos hasta cinco configuraciones de este tipo. En cada una de ellas hay 6 aristas del icosaedro. Tomando los puntos medios de estas aristas obtenemos los vértices de un octaedro regular. Para cada uno de estos octaedros construiremos una forma de grado 6 que se anula en sus vértices, vistos como puntos de  $\hat{C}$  (primero proyectamos a  $S^2$  desde el origen y después a  $\hat{C}$  mediante la proyección estereográfica). Estas formas serán las raíces de nuestro resolvente quíntico.

Consideremos los siguientes elementos de  $\mathcal{I}$ :

$$S : z \mapsto \omega z, \quad U : z \mapsto -\frac{1}{z}, \quad V : z \mapsto \frac{(\omega^2 - \omega^3)z + (\omega - \omega^4)}{(\omega - \omega^4)z - (\omega^2 - \omega^3)}, \quad W = UV$$

La transformación  $S$  se corresponde con una rotación de eje  $OZ$  de orden 5, mientras que las demás son de orden 2. El eje de  $U$  es el  $OY$ , mientras que el de  $V$  es perpendicular al de  $U$  y pasa por el punto medio de una de las aristas en la base de la pirámide pentagonal superior. El eje de  $W$  es perpendicular a los de  $U$  y  $V$ . Los ejes de estas tres últimas rotaciones definen una de las configuraciones de rectángulos perpendiculares vistas anteriormente. Tomaremos el primer octaedro (proyectado a  $\hat{C}$ ) con vértices en los puntos fijos de estas rotaciones.

Los puntos fijos de  $U$  son las soluciones de  $z^2 = -1$ , y la forma que se anula en estos puntos es  $z_1^2 + z_2^2$ . Para los puntos fijos de  $V$  consideramos

$$\frac{(\omega^2 - \omega^3)z_1 + (\omega - \omega^4)z_2}{(\omega - \omega^4)z_1 - (\omega^2 - \omega^3)z_2} = \frac{z_1}{z_2}.$$

Multiplicando nos queda

$$z_1^2 - 2(\omega + \omega^4)z_1z_2 - z_2^2 = 0.$$

Como  $\omega + \omega^4 = 1/\phi$ , donde  $\phi = (1 + \sqrt{5})/2$  es la razón áurea, obtenemos la forma

$$z_1^2 - \frac{2}{\phi}z_1z_2 - z_2^2.$$

Del mismo modo para  $W$  obtenemos la forma

$$z_1^2 + 2\phi z_1z_2 - z_2^2.$$

Multiplicando las tres formas anteriores obtenemos la primera forma octaédrica

$$\Omega_1(z_1, z_2) = (z_1^2 + z_2^2)(z_1^4 + 2z_1^3z_2 - 6z_1^2z_2^2 - 2z_1z_2^3 + z_2^4).$$

Las demás formas octaédricas  $\Omega_{j+1}$ ,  $j = 1, \dots, 4$ , se obtienen aplicando a  $\Omega_1$  las sustituciones homogéneas

$$z_1 \mapsto \pm\omega^{3j}z_1, \quad z_2 \mapsto \pm\omega^{2j}z_2, \quad j = 1, \dots, 4.$$

que corresponden a las rotaciones  $S^j$  dadas por  $z \mapsto \omega^j z$ . Las expresiones explícitas de estas cinco formas son

$$\Omega_{j+1}(z_1, z_2) = \omega^{3j}z_1^6 + 2\omega^{2j}z_1^5z_2 - 5\omega^jz_1^4z_2^2 - 5\omega^{4j}z_1^2z_2^4 - 2\omega^{3j}z_1z_2^5 + \omega^{2j}z_2^6.$$

Queremos ver cómo actúa  $\mathcal{A}_5$  en  $\{\Omega_1, \dots, \Omega_5\}$ . Para ello basta ver cómo los generadores icosaédricos  $S$  y  $W = UV$  actúan sobre estas formas. Por definición,  $S$  permuta cíclicamente. Por cómo hemos definido  $\Omega_1$ , sabemos que esta forma es fija para  $U$ ,  $V$  y  $W$ . Para  $U : z \mapsto -1/z$  hacemos la sustitución homogénea  $z_1 \mapsto z_2$ ,  $z_2 \mapsto -z_1$ . Mirando cómo afecta esta sustitución a los coeficientes líderes de las formas octaédricas, vemos que  $U$  actúa del siguiente modo:

$$U : \Omega_1 \mapsto \Omega_1, \quad \Omega_2 \leftrightarrow \Omega_5, \quad \Omega_3 \leftrightarrow \Omega_4.$$

Las cinco aristas que llegan al vértice superior del icosaedro son permutadas cíclicamente por  $S$ . Cada una de ellas forma parte de una configuración distinta de rectángulos perpendiculares. Si denotamos por  $e_j$  a la arista cuya configuración define  $\Omega_j$ , entonces el eje de la rotación  $V$  pasa a través del punto medio de la base de la cara formada por  $e_3$  y  $e_4$ . Aplicando  $V$ , vemos que  $V(e_3)$  y  $e_5$  son aristas en una misma configuración, al igual que  $V(e_4)$  y  $e_2$ . De esta forma  $V$  actúa como:

$$V : \Omega_1 \mapsto \Omega_1, \quad \Omega_2 \leftrightarrow \Omega_4, \quad \Omega_3 \leftrightarrow \Omega_5.$$

Por último  $W = UV$  actúa de la siguiente forma:

$$W : \Omega_1 \mapsto \Omega_1, \quad \Omega_2 \leftrightarrow \Omega_3, \quad \Omega_4 \leftrightarrow \Omega_5.$$

A pesar de haber construido estas formas, dado que  $\sum_{j=1}^5 \Omega_j^2 \neq 0$ , el resolvente icosaédrico construido a partir de ellas no será canónico. Sin embargo, podemos considerar el Hessiano

$$\Xi_j(z_1, z_2) = Hess(\Omega_j)(z_1, z_2) = \begin{vmatrix} \frac{\partial^2 \Omega_j}{\partial z_1^2} & \frac{\partial^2 \Omega_j}{\partial z_1 \partial z_2} \\ \frac{\partial^2 \Omega_j}{\partial z_2 \partial z_1} & \frac{\partial^2 \Omega_j}{\partial z_2^2} \end{vmatrix}, \quad j = 1, \dots, 5.$$

Cada  $\Xi_j$  es una forma de grado 8:

$$\begin{aligned} \Xi_{j+1} &= -\omega^{4j} z_1^8 + \omega^{3j} z_1^7 z_2 - 7\omega^{2j} z_1^6 z_2^2 - 7\omega^j z_1^5 z_2^3 + 7\omega^{4j} z_1^3 z_2^5 - 7\omega^{3j} z_1^2 z_2^6 - \omega^{2j} z_1 z_2^7 - \omega^j z_2^8 = \\ &= (\omega^{4j} z_1 - \omega^{3j} z_2)(-z_1^7 + 7z_1^2 z_2^5) + (\omega^{2j} z_1 + \omega^j z_2)(-7z_1^5 z_2^2 - z_2^7). \end{aligned}$$

El conjunto  $\{\Xi_1, \dots, \Xi_5\}$  también forma una  $\mathcal{A}_5$ -órbita. Además, tenemos que

$$\sum_{j=1}^5 \Xi_j = 0, \quad \sum_{j=1}^5 \Xi_j^2 = 0,$$

ya que no hay formas de grado 8 y 16 (recordemos que cualquier forma icosaédrica es un polinomio en  $\mathcal{I}$ ,  $\mathcal{J}$  y  $\mathcal{H}$ ). Por lo tanto el resolvente icosaédrico construido a partir de estas formas será canónico.

Para conseguir una familia de dos parámetros de estas formas solo basta notar que

$$\sum_{j=1}^5 \Omega_j \Xi_j = 0, \quad \sum_{j=1}^4 \Omega_j \Xi_j^2 = 0, \quad \sum_{j=1}^5 (\Omega_j \Xi_j)^2 = 0,$$

ya que no hay invariantes icosaédricos de grados 14, 22 y 28. La expresión explícita de estas formas es la siguiente:

$$\begin{aligned} \Omega_{j+1} \Xi_{j+1} &= (\omega^{4j} z_1 - \omega^{3j} z_2)(-26z_1^{10} z_2^3 + 39z_1^5 z_2^8 + z_2^{13}) + \\ &+ (\omega^{2j} z_1 + \omega^j z_2)(-z_1^{13} + 39z_1^8 z_2^5 + 26z_1^3 z_2^{10}). \end{aligned}$$

Busquemos un resolvente para la combinación lineal

$$\Upsilon_j = E\Xi_j + F\Omega_j \Xi_j, \quad j = 1, \dots, 5.$$

en la que por homogeneidad, los coeficientes  $E$  y  $F$  serán las formas de grado 30 y 24

$$E = 12u\mathcal{J} \quad F = 144v\mathcal{I}^2,$$

donde  $u$  y  $v$  son parámetros complejos. Escribimos el polinomio resolvente como

$$\prod_{j=1}^5 (\mathcal{X} - \Upsilon_j) = \mathcal{X}^5 + b_1\mathcal{X}^4 + b_2\mathcal{X}^3 + b_3\mathcal{X}^2 + b_4\mathcal{X} + b_5,$$

donde hemos usado  $\mathcal{X}$  como variable. Por lo visto anteriormente,  $b_1 = b_2 = 0$ . Utilizando el hecho de que los coeficientes deben ser invariantes (absolutos) de  $\mathcal{I}$  llegamos a

$$\begin{aligned} & \mathcal{X}^5 + 5\mathcal{X}^2(8E^3\mathcal{I}^2 + E^2F\mathcal{J} + 72EF^2\mathcal{I}^3 + F^3\mathcal{I}\mathcal{J}) + \\ & + 5\mathcal{X}(-E^4\mathcal{I}\mathcal{H} + 18E^2F^2\mathcal{I}^2\mathcal{H} + EF^3\mathcal{H}\mathcal{J} + 27F^4\mathcal{I}^3\mathcal{H}) + \\ & + (E^5\mathcal{H}^2 - 10E^3F^2\mathcal{I}\mathcal{H}^2 + 45EF^4\mathcal{I}^2\mathcal{H}^2 + F^5\mathcal{J}\mathcal{H}^2). \end{aligned}$$

Introducimos la nueva variable

$$X = \frac{\mathcal{I}}{\mathcal{J}\mathcal{H}}\mathcal{X},$$

junto con

$$r_j = 12\frac{\mathcal{I}^2}{\mathcal{J}}\Omega_j, \quad s_j = 12\frac{\mathcal{I}}{\mathcal{H}}\Xi_j, \quad j = 1, \dots, 5.$$

Comparando los grados de las formas involucradas vemos que  $r_j$  y  $s_j$  son funciones racionales en  $z = z_1/z_2$ . Con este cambio de variable:

$$t_j := \frac{\mathcal{I}}{\mathcal{J}\mathcal{H}}\Upsilon_j = us_j + vr_js_j, \quad j = 1, \dots, 5.$$

El polinomio resolvente resultante es:

$$\begin{aligned} P^*(X) &= \prod_{j=1}^5 (X - t_j) = X^5 + \frac{5X^2}{w} \left( 8u^3 + 12u^2v + \frac{6uv^2 + v^3}{1-w} \right) + \\ &+ \frac{15X}{w} \left( -4u^4 + \frac{6u^2v^2 + 4uv^3}{1-w} + \frac{3v^4}{4(1-w)^2} \right) + \frac{3}{w} \left( 48u^5 - \frac{40u^3v^2}{1-w} + \frac{15uv^4 + 4v^5}{(1-w)^2} \right). \end{aligned}$$

Este será llamado el *polinomio resolvente canónico* de la ecuación icosaédrica. Sus raíces  $\{t_j\}_{j=1}^5$  son funciones racionales en  $z = z_1/z_2$  y funciones lineales en  $u$  y  $v$ . Como en el caso de las formas octaédricas, los generadores icosaédricos  $S$  y  $W$  actúan en las raíces de la forma:

$$S : t_j \mapsto t_{j(\text{mod } 5)+1}, \quad j = 1, \dots, 5,$$

$$W : t_1 \mapsto t_1, \quad t_2 \leftrightarrow t_3, \quad t_4 \leftrightarrow t_5.$$

Como en el caso de la quinta canónica, los puntos proyectivos correspondientes a las raíces del resolvente canónico se encuentran en

$$\mathcal{Q}_0 = \left\{ (t_1 : \cdots : t_5) \in \mathbb{P}^4(\mathbb{C}) : \sum_{j=1}^5 t_j = \sum_{j=1}^5 t_j^2 = 0 \right\}.$$

Como el conjunto de soluciones contiene dos parámetros, es de esperar que estos puntos rellenen  $\mathcal{Q}_0$ . Veremos este hecho como una consecuencia de otros resultados en las secciones posteriores. De esta forma la cuádrica proyectiva  $\mathcal{Q}_0 \subset \mathbb{P}_0^3(\mathbb{C}) \subset \mathbb{P}^4(\mathbb{C})$  es un espacio parametrizable por las soluciones del resolvente canónico de la ecuación icosaédrica.

### 3.6 Geometría de la ecuación canónica

**| Teorema 3.2.** *Sea  $k$  un cuerpo satisfaciendo  $\mathbb{Q}(\omega) \subset k \subset \mathbb{C}$ . Sea  $K \subset \mathbb{C}$  una extensión de Galois de  $k$ , con grupo de Galois  $\mathcal{A}_5$ . Entonces, reemplazando  $k$  por una extensión cuadrática adecuada, existe  $w^* \in k$  tal que  $K$  está generado por cualquier solución  $z^*$  de la ecuación icosaédrica con parámetro  $w^* = q(z^*)$ . Además, cada solución  $z^*$  da lugar a un isomorfismo  $\varphi : \mathcal{A}_5 \rightarrow \mathcal{I}$  de forma que si  $\sigma \in \mathcal{A}_5$  es un  $k$ -automorfismo de  $K$  que es llevado bajo este isomorfismo a*

$$\varphi(\sigma) = \pm \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix},$$

entonces

$$\sigma^{-1}(z^*) = \varphi(\sigma)(z^*) = \frac{a(\sigma)z^* + b(\sigma)}{c(\sigma)z^* + d(\sigma)}.$$

Observemos que una extensión cuadrática no afecta a las hipótesis de este teorema. En efecto, si  $k'$  es una extensión cuadrática de  $k$ , entonces  $k'$  no está contenido en  $K$ , ya que el grupo de Galois  $\mathcal{A}_5$  de la extensión  $K/k$  no contiene ningún subgrupo de índice 2. Por lo tanto  $G(K \cdot k'/k') = G(K/k) = \mathcal{A}_5$ .

Toda quinta  $P(z) = z^5 + a_1z^4 + a_2z^3 + a_3z^2 + a_4z + a_5$  irreducible sobre  $k$ ,  $\mathbb{Q} \subset k \subset \mathbb{C}$ , con grupo de Galois  $\mathcal{A}_5$  tiene un cuerpo de descomposición como en el teorema 3.2. Recíprocamente, sea  $K/k$  como en este teorema, existe una quinta irreducible

sobre  $k$  cuyo cuerpo de descomposición es  $K$ , y cuyo grupo de Galois es  $\mathcal{A}_5$ . En efecto, consideremos un subgrupo de  $\mathcal{A}_5$  isomorfo a  $\mathcal{A}_4$ , el cual denotaremos de igual forma. El cuerpo  $k$  está contenido propiamente en el cuerpo fijo  $K^{\mathcal{A}_4}$ , por lo que existe  $z_1 \in K^{\mathcal{A}_4} \setminus k$ . Consideremos la  $\mathcal{A}_5$ -órbita de  $z_1$  formada por cinco elementos  $z_1, \dots, z_5$  (ya que  $\mathcal{A}_4$  es maximal en  $\mathcal{A}_5$ ). Sea  $P(z) = \prod_{j=1}^5 (z - z_j)$  el resolvente quíntico asociado a  $z_1$ . Entonces  $P$  es irreducible sobre  $k$ ,  $K$  es el cuerpo de descomposición de  $P$  sobre  $k$  y el grupo de Galois  $\mathcal{A}_5$  se puede identificar con el grupo de permutaciones pares de las raíces  $z_1, \dots, z_5$ .

Para probar el teorema 3.2, veremos  $K$  como el cuerpo de descomposición de una quíntica irreducible con grupo de Galois  $\mathcal{A}_5$ . La "extensión cuadrática adecuada" que aparece en este teorema se corresponde con la vista anteriormente para reducir la quíntica general a forma canónica.

Hemos visto que  $\mathcal{Q}_0$  es parametrizable tanto por las raíces del resolvente canónico de la ecuación icosaédrica como por las raíces de la quíntica irreducible en forma canónica. Nuestro objetivo es hacer coincidir estas dos parametrizaciones para obtener una prueba constructiva del teorema 3.2 y las fórmulas explícitas para resolver quínticas canónicas.

Comenzaremos considerando la llamada sustitución de Lagrange, dada por

$$\begin{aligned} \iota : \quad \mathbb{P}^3(\mathbb{C}) &\rightarrow \mathbb{P}^4(\mathbb{C}) \\ (\xi_1 : \dots : \xi_4) &\mapsto (z_1 : \dots : z_5) \end{aligned}$$

donde

$$z_j = \sum_{l=1}^4 \omega^{-(j-1)l} \xi_l, \quad j = 1, \dots, 5.$$

Como  $1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$ , tenemos que

$$\sum_{j=1}^5 z_j = \sum_{l=1}^4 \left( \sum_{j=1}^5 \omega^{-(j-1)l} \right) \xi_l = 0.$$

Por lo tanto  $\iota$  envía  $\mathbb{P}^3(\mathbb{C})$  en  $\mathbb{P}_0^3(\mathbb{C}) \subset \mathbb{P}^4(\mathbb{C})$ . De hecho,  $\iota$  es un isomorfismo lineal entre  $\mathbb{P}^3(\mathbb{C})$  y  $\mathbb{P}_0^3(\mathbb{C})$ , con inversa dada por

$$\xi_l = \frac{1}{5} \sum_{j=1}^5 \omega^{(j-1)l} z_j, \quad l = 1, \dots, 4.$$

Bajo este isomorfismo, la ecuación  $\sum_{j=1}^5 z_j^2 = 0$  de  $\mathcal{Q}_0$  se transforma en

$$0 = \sum_{j=1}^5 z_j^2 = \sum_{j=1}^5 \left( \sum_{l=1}^4 \omega^{-(j-1)l} \xi_l \right)^2 = \sum_{l,l'=1}^4 \left( \sum_{j=1}^5 \omega^{-(j-1)(l+l')} \right) \xi_l \xi_{l'} = 10(\xi_1 \xi_4 + \xi_2 \xi_3).$$

En la última igualdad hemos utilizado que  $\sum_{j=1}^5 \omega^{-(j-1)(l+l')} = 5$  si  $l+l' = 5$ , y cero en otro caso. Este razonamiento identifica  $\mathcal{Q}_0$  con la cuádrlica proyectiva

$$\mathcal{Q} = \{(\xi_1 : \dots : \xi_4) \in \mathbb{P}^3(\mathbb{C}) : \xi_1 \xi_4 + \xi_2 \xi_3 = 0\}.$$

Veamos la geometría de  $\mathcal{Q}$  como superficie doblemente reglada. Para cada valor  $c^* \in \hat{\mathbb{C}}$ , las ecuaciones

$$-\frac{\xi_1}{\xi_2} = \frac{\xi_3}{\xi_4} = c^*$$

definen una recta proyectiva contenida en  $\mathcal{Q}$ , que llamaremos *recta generadora de primer tipo* con parámetro  $c^*$ . De igual forma, para  $c^{**} \in \hat{\mathbb{C}}$ , las ecuaciones

$$\frac{\xi_1}{\xi_3} = -\frac{\xi_2}{\xi_4} = c^{**}$$

definirán una *recta generadora de segundo tipo* con parámetro  $c^{**}$ . Observando las ecuaciones que definen estas dos familias es fácil deducir las siguientes propiedades:

1. Cada punto de  $\mathcal{Q}$  es la intersección de dos rectas generadoras de diferentes tipos.
2. Dos rectas generadoras de distinto tipo se intersecan en un único punto de  $\mathcal{Q}$ .
3. Dos rectas generadoras distintas del mismo tipo son disjuntas.

Gracias a la equivalencia entre  $\mathcal{Q}$  y  $\mathcal{Q}_0$ , esta construcción puede ser llevada a nuestra cuádrlica inicial. Como las variables  $\xi_l$  dependen linealmente de  $z_1, \dots, z_5$ , los parámetros  $c^*$  y  $c^{**}$  tendrán dependencia racional en las variables  $z_1, \dots, z_5$ , sujeto a  $\sum_{j=1}^5 z_j = \sum_{j=1}^5 z_j^2 = 0$ .

Si fijamos un punto  $o \in \mathcal{Q}_0$  como el origen, entonces las rectas generadoras  $\mathbb{P}^*(\mathbb{C})$  y  $\mathbb{P}^{**}(\mathbb{C})$  de primer y segundo tipo a través de  $o$  pueden ser vistas como ejes de un sistema de coordenadas para  $\mathcal{Q}_0$ . Cualquier punto en  $\mathcal{Q}_0$  puede ser representado por un único par de coordenadas complejas  $(c^*, c^{**}) \in \mathbb{P}^*(\mathbb{C}) \times \mathbb{P}^{**}(\mathbb{C})$  de manera obvia. Esto nos da la equivalencia conforme

$$\mathcal{Q}_0 = \mathbb{P}^*(\mathbb{C}) \times \mathbb{P}^{**}(\mathbb{C})$$

Recordemos que el grupo simétrico  $\mathcal{S}_5$  actúa en  $\mathbb{P}^4(\mathbb{C})$  permutando las coordenadas homogéneas, por lo que deja invariante a  $\mathcal{Q}_0 \subset \mathbb{P}_0^3(\mathbb{C})$ . Cada permutación en  $\mathcal{S}_5$  lleva rectas generadoras en rectas generadoras. Esto es debido a que la acción de estos elementos es una homografía, ya que actúan en  $\mathbb{C}^5$  como una matriz de permutación, y toda homografía lleva rectas proyectivas en rectas proyectivas. Por continuidad, estas dos familias de rectas generadoras pueden ser intercambiadas o fijadas por los elementos de  $\mathcal{S}_5$ . Sea  $\mathcal{G} \subset \mathcal{S}_5$  el subgrupo que mantiene cada recta generadora en su familia. Está claro que el índice de  $\mathcal{G}$  en  $\mathcal{S}_5$  es como mucho 2. Como el grupo alternado  $\mathcal{A}_5$  es el único subgrupo de índice 2 en  $\mathcal{S}_5$ , llegamos a que  $\mathcal{G} = \mathcal{A}_5$  o  $\mathcal{G} = \mathcal{S}_5$ . Dado que la permutación impar

$$z_1 \mapsto z_1, \quad z_2 \mapsto z_4, \quad z_3 \mapsto z_2, \quad z_4 \mapsto z_5, \quad z_5 \mapsto z_3$$

actúa como

$$c^* = \frac{\xi_3}{\xi_4} = \frac{z_1 + \omega^3 z_2 + \omega z_3 + \omega^4 z_4 + \omega^2 z_5}{z_1 + \omega^4 z_2 + \omega^3 z_3 + \omega^2 z_4 + \omega z_5} \mapsto \frac{z_1 + \omega z_2 + \omega^2 z_3 + \omega^3 z_4 + \omega^4 z_5}{z_1 + \omega^3 z_2 + \omega z_3 + \omega^4 z_4 + \omega^2 z_5} = \frac{\xi_1}{\xi_3} = c^{**},$$

tenemos que  $\mathcal{G} = \mathcal{A}_5$ .

La equivalencia conforme vista anteriormente es  $\mathcal{A}_5$ -equivariante, es decir, el siguiente diagrama es conmutativo

$$\begin{array}{ccc} \mathcal{Q}_0 & \longrightarrow & \mathbb{P}^*(\mathbb{C}) \times \mathbb{P}^{**}(\mathbb{C}) \\ \downarrow \sigma & & \downarrow \sigma \\ \mathcal{Q}_0 & \longrightarrow & \mathbb{P}^*(\mathbb{C}) \times \mathbb{P}^{**}(\mathbb{C}) \end{array}$$

donde  $\sigma \in \mathcal{A}_5$  actúa en el producto  $\mathbb{P}^*(\mathbb{C}) \times \mathbb{P}^{**}(\mathbb{C})$  diagonalmente.

Dado que la acción de  $\mathcal{A}_5$  preserva las familias de rectas generadoras,  $\mathcal{A}_5$  se puede considerar como un subgrupo en  $Aut(\mathbb{P}^*(\mathbb{C}))$  y también en  $Aut(\mathbb{P}^{**}(\mathbb{C}))$ . De forma similar, una permutación impar de  $\mathcal{S}_5$  nos da una equivalencia conforme entre  $\mathbb{P}^*(\mathbb{C})$  y  $\mathbb{P}^{**}(\mathbb{C})$ . Conjugar  $\mathcal{A}_5$  con esta permutación impar hace que la acción de  $\mathcal{A}_5$  cambie de familia.

Consideremos las proyecciones  $\pi^* : \mathcal{Q}_0 \rightarrow \mathbb{P}^*(\mathbb{C})$  y  $\pi^{**} : \mathcal{Q}_0 \rightarrow \mathbb{P}^{**}(\mathbb{C})$ . Sea

$$\tilde{\mathcal{Q}}_0 = \left\{ (z_1, \dots, z_5) \in \mathbb{C}^5 \setminus \{0\} : \sum_{j=1}^5 z_j = \sum_{j=1}^5 z_j^2 = 0 \right\},$$

y definamos  $\pi : \tilde{\mathcal{Q}}_0 \rightarrow \mathcal{Q}_0$  como la restricción de la proyección canónica  $\mathbb{C}^5 \setminus \{0\} \rightarrow \mathbb{P}^4(\mathbb{C})$ . Sean  $z^* = \pi^* \circ \pi$  y  $z^{**} = \pi^{**} \circ \pi$ . Veamos que las transformaciones que  $z^*$  y  $z^{**}$



experimentan bajo la acción de  $\mathcal{A}_5$  en las variables  $z_1, \dots, z_5$  se pueden identificar con transformaciones de Möbius, obteniéndose un isomorfismo entre ambos grupos. Para ello es suficiente estudiar el caso de  $\pi^*$ , ya que las coordenadas homogéneas serán permutadas de igual forma por los elementos de  $\mathcal{A}_5$  (el caso de  $\pi^{**}$  será análogo). Además, dado que  $\mathcal{I} = \langle S, U, W \rangle$ , basta ver que se cumple para estos generadores.

La transformación  $S$  (multiplicar por  $\omega$ ) se corresponde con la permutación cíclica

$$S : z_j \mapsto z_{j(\bmod 5)+1}, \quad j = 1, \dots, 5.$$

Esto es debido a que esta permutación actúa como

$$c^* = -\frac{\xi_1}{\xi_2} = -\frac{\sum_{j=1}^5 \omega^{j-1} z_j}{\sum_{j=1}^5 \omega^{2(j-1)} z_j} \mapsto -\frac{\sum_{j=1}^5 \omega^{j-1} z_{j(\bmod 5)+1}}{\sum_{j=1}^5 \omega^{2(j-1)} z_{j(\bmod 5)+1}} = -\frac{\sum_{j=1}^5 \omega^{j-2} z_j}{\sum_{j=1}^5 \omega^{2(j-2)} z_j} = \omega c^*$$

De forma similar,  $U : z \mapsto -1/z$  se corresponde con la permutación

$$U : z_1 \mapsto z_1, \quad z_2 \leftrightarrow z_5, \quad z_3 \leftrightarrow z_4,$$

ya que actúa como

$$c^* = \frac{\xi_3}{\xi_4} = \frac{z_1 + \omega^3 z_2 + \omega z_3 + \omega^4 z_4 + \omega^2 z_5}{z_1 + \omega^4 z_2 + \omega^3 z_3 + \omega^2 z_4 + \omega z_5} \mapsto \frac{z_1 + \omega^2 z_2 + \omega^4 z_3 + \omega z_4 + \omega^3 z_5}{z_1 + \omega z_2 + \omega^2 z_3 + \omega^3 z_4 + \omega^4 z_5} = \frac{\xi_2}{\xi_1} = -\frac{1}{c^*}.$$

Por último,  $W$  se corresponde con la permutación

$$W : z_1 \mapsto z_1, \quad z_2 \leftrightarrow z_3, \quad z_4 \leftrightarrow z_5.$$

Para probar esto utilizaremos las siguientes igualdades:

$$\phi = \frac{\omega - \omega^4}{\omega^2 - \omega^3} = -(\omega^2 + \omega^3) = \frac{1}{\omega + \omega^4}, \quad \xi_1 \xi_4 + \xi_2 \xi_3 = 0,$$

$$1 + \frac{2}{\phi} = \sqrt{5}, \quad 3 - \phi = \frac{\sqrt{5}}{\phi}, \quad 3 + \frac{1}{\phi} = \sqrt{5}\phi, \quad 1 - 2\phi = -\sqrt{5}.$$

Permutando  $z_1, \dots, z_5$  de la forma indicada y escribiendo el cociente en término de  $\xi_1, \dots, \xi_4$ , obtenemos:

$$\begin{aligned} & -\frac{z_1 + \omega^2 z_2 + \omega z_3 + \omega^4 z_4 + \omega^3 z_5}{z_1 + \omega^4 z_2 + \omega^2 z_3 + \omega^3 z_4 + \omega z_5} = \\ & = -\frac{(1 + 2\omega + 2\omega^4)\xi_1 + (3 + \omega^2 + \omega^3)\xi_2 + (3 + \omega + \omega^4)\xi_3 + (1 + 2\omega^2 + 2\omega^3)\xi_4}{(3 + \omega^2 + \omega^3)\xi_1 + (1 + 2\omega^2 + 2\omega^3)\xi_2 + (1 + 2\omega + 2\omega^4)\xi_3 + (3 + \omega + \omega^4)\xi_4} = \end{aligned}$$

$$\begin{aligned}
 &= -\frac{(1 + \frac{2}{\phi})\xi_1 + (3 - \phi)\xi_2 + (3 + \frac{1}{\phi})\xi_3 + (1 - 2\phi)\xi_4}{(3 - \phi)\xi_1 + (1 - 2\phi)\xi_2 + (1 + \frac{2}{\phi})\xi_3 + (3 + \frac{1}{\phi})\xi_4} = -\frac{\xi_1 + \frac{\xi_2}{\phi} + \phi\xi_3 - \xi_4}{\frac{\xi_1}{\phi} - \xi_2 + \xi_3 + \phi\xi_4} = \\
 &= -\frac{(\phi\xi_1 + \xi_2)(\frac{1}{\phi} + \frac{\xi_3}{\xi_1})}{(\xi_1 - \phi\xi_2)(\frac{1}{\phi} + \frac{\xi_3}{\xi_1})} = -\frac{\phi\xi_1 + \xi_2}{\xi_1 - \phi\xi_2} = -\frac{(\omega - \omega^4)\xi_1 + (\omega^2 - \omega^3)\xi_2}{(\omega^2 - \omega^3)\xi_1 - (\omega - \omega^4)\xi_2} = Wc^*
 \end{aligned}$$

Estas correspondencias dan lugar a un isomorfismo  $\varphi : \mathcal{A}_5 \rightarrow \mathcal{I}$ , de forma que  $z^*$  es  $\varphi$ -equivariante, es decir, el siguiente diagrama es conmutativo

$$\begin{array}{ccc}
 \tilde{\mathcal{Q}}_0 & \xrightarrow{z^*} & \hat{\mathcal{C}} \\
 \downarrow \sigma & & \downarrow \varphi(\sigma) \\
 \tilde{\mathcal{Q}}_0 & \xrightarrow{z^*} & \hat{\mathcal{C}}
 \end{array}$$

para cualquier  $\sigma \in \mathcal{A}_5$ , donde  $\mathcal{A}_5$  actúa en  $\tilde{\mathcal{Q}}_0$  permutando las coordenadas, y  $\mathcal{I}$  actúa en  $\hat{\mathcal{C}}$  como el grupo icosaédrico de Möbius.

Cuando  $K$  es considerado como el cuerpo de descomposición de una quintica canónica  $P(z) = z^5 + az^2 + bz + c$  con raíces  $z_1, \dots, z_5$  y grupo de Galois  $\mathcal{A}_5$ , entonces  $z^*(z_1, \dots, z_5)$  se convierte en un elemento de  $K = k(z_1, \dots, z_5)$ , ya que  $z^*$  depende racionalmente de  $z_1, \dots, z_5$ . Como  $z^*$  es  $\varphi$ -equivariante, las 60 raíces de su polinomio resolvente coinciden con las transformaciones de  $\mathcal{I}$  aplicadas a  $z^*(z_1, \dots, z_5)$ . Resumiendo, hemos probado que  $z^*$  satisface la ecuación icosaédrica

$$q(z^*(z_1, \dots, z_5)) = w^*(a, b, c, \sqrt{\delta}),$$

donde  $z_1, \dots, z_5$  están sujetos a  $\sum_{j=1}^5 z_j = \sum_{j=1}^5 z_j^2 = 0$ , y el parámetro  $w^*$  depende de  $a, b, c$  y  $\sqrt{\delta}$  racionalmente. Para completar la prueba del teorema 3.2, necesitamos demostrar que  $z^*$  genera  $K$  sobre  $k$ . La situación es completamente análoga para las rectas generadoras de segundo tipo. Obtenemos un elemento  $z^{**}(z_1, \dots, z_5) \in K$  que satisface la ecuación icosaédrica

$$q(z^{**}(z_1, \dots, z_5)) = w^{**}(a, b, c, \sqrt{\delta}).$$

Los parámetros  $a, b$  y  $c$  son invariantes bajo el grupo simétrico  $\mathcal{S}_5$ , mientras que  $\sqrt{\delta}$  cambia su signo cuando las raíces son sometidas a permutaciones impares. Como las dos acciones de  $\mathcal{A}_5$  en  $\mathbb{P}^*(\mathbb{C})$  y  $\mathbb{P}^{**}(\mathbb{C})$  son conjugadas bajo permutaciones impares de  $\mathcal{S}_5$ , obtenemos

$$w^*(a, b, c, -\sqrt{\delta}) = w^{**}(a, b, c, \sqrt{\delta}).$$

Comparemos cómo  $S$  y  $W$  transforman  $z_1, \dots, z_5$  y  $t_1, \dots, t_5$ . Vemos que cuando  $z^*$  es sometido a una transformación de  $\mathcal{I}$ , esta acción puede ser entendida como una permutación par en las variables, exactamente de la misma forma que cuando actúa en las raíces  $t_1, \dots, t_5$  del resolvente icosaédrico. De esta forma se establece una correspondencia biunívoca y  $\mathcal{A}_5$ -equivariante  $z_j \leftrightarrow t_j, j = 1, \dots, 5$ , entre los conjuntos  $\{z_1, \dots, z_5\}$  y  $\{t_1, \dots, t_5\}$ :  $z_1$  y  $t_1$  son el único punto fijo de  $W$ , y  $z_{j+1} = S^j(z_1)$  se corresponde con  $t_{j+1} = S^j(t_1), j = 1, \dots, 4$ .

Para obtener un análisis más profundo de esta correspondencia, estudiaremos las rectas generadoras en términos de las raíces  $\{t_1, \dots, t_5\}$  del resolvente icosaédrico. En analogía con la sustitución de Lagrange, hacemos

$$t_j = \sum_{l=1}^4 \omega^{-(j-1)l} X_l, \quad j = 1, \dots, 5,$$

y

$$X_l = \frac{1}{5} \sum_{j=1}^5 \omega^{(j-1)l} t_j, \quad l = 1, \dots, 4.$$

Para calcular  $X_l$ , utilizaremos las expresiones explícitas de las formas  $\Xi_j$  y  $\Omega_j \Xi_j$  dadas en la sección anterior. De esta forma obtenemos

$$t_j = (\omega^{4(j-1)} z_1 - \omega^{3(j-1)} z_2) A + (\omega^{2(j-1)} z_1 + \omega^{j-1} z_2) B,$$

donde  $A$  y  $B$  son lineales en  $u$  y  $v$ . La inversa de la sustitución de Lagrange será

$$\begin{aligned} X_l &= \frac{1}{5} \sum_{j=1}^5 \omega^{(j-1)l} (\omega^{4(j-1)} z_1 - \omega^{3(j-1)} z_2) A + \frac{1}{5} \sum_{j=1}^5 \omega^{(j-1)l} (\omega^{2(j-1)} z_1 + \omega^{j-1} z_2) B = \\ &= (\delta_{1l} z_1 - \delta_{2l} z_2) A + (\delta_{3l} z_1 + \delta_{4l} z_2) B, \end{aligned}$$

donde hemos utilizado la función delta de Kronecker  $\delta_{jl}$  ( $= 1$  si  $j = l$  y cero en otro caso). Por lo tanto tenemos

$$X_1 = z_1 A, \quad X_2 = -z_2 A, \quad X_3 = z_1 B, \quad X_4 = z_2 B$$

Para los parámetros  $C^*$  y  $C^{**}$  de las rectas generadoras definidas por

$$-\frac{X_1}{X_2} = \frac{X_3}{X_4} = C^*, \quad \frac{X_1}{X_3} = -\frac{X_2}{X_4} = C^{**},$$

obtenemos

$$C^* = \frac{z_1}{z_2} = z, \quad C^{**} = \frac{A}{B}.$$

Como  $z^*$  y  $z^{**}$  vienen dadas por las proyecciones  $(C^*, C^{**}) \mapsto C^*$  y  $(C^*, C^{**}) \mapsto C^{**}$ , tenemos que

$$z^*(t_1, \dots, t_5) = z, \quad z^{**}(t_1, \dots, t_5) = \frac{A}{B}$$

Escribiendo el resolvente canónico como

$$P^*(X) = \prod_{j=1}^5 (X - t_j) = X^5 + 5a(u, v, w)X^2 + 5b(u, v, w)X + c(u, v, w),$$

tenemos

$$q(z^*(t_1, \dots, t_5)) = w^*(a(u, v, w), b(u, v, w), c(u, v, w), \sqrt{\delta(u, v, w)}) = q(z) = w,$$

donde  $\delta(u, v, w)$  es el discriminante del polinomio resolvente canónico.

El sistema

$$\begin{cases} a(u, v, w) = a, \\ b(u, v, w) = b, \\ c(u, v, w) = c. \end{cases}$$

puede ser invertido, siempre que también hagamos coincidir las raíces cuadradas de los discriminantes,  $\sqrt{\delta(u, v, w)} = \sqrt{\delta}$ :

$$\begin{cases} u = u(a, b, c, \sqrt{\delta}), \\ v = v(a, b, c, \sqrt{\delta}), \\ w = w(a, b, c, \sqrt{\delta}). \end{cases}$$

Usando las fórmulas explícitas de los coeficientes del polinomio resolvente canónico, el sistema inicial se puede expresar como

$$\begin{cases} w \cdot a = 8u^3 + 12u^2v + \frac{6uv^2 + v^3}{1-w}, \\ \frac{w \cdot b}{3} = -4u^4 + \frac{6u^2v^2 + 4uv^3}{1-w} + \frac{3v^4}{4(1-w)^2}, \\ \frac{w \cdot c}{3} = 48u^5 - \frac{40u^3v^2}{1-w} + \frac{15uv^4 + 4v^5}{(1-w)^2}. \end{cases}$$

Si multiplicamos la primera ecuación por  $-4v^2/(1-w)$  y la segunda por  $12u$  para posteriormente sumar las tres ecuaciones, todos los términos de la derecha se cancelan, por lo que

$$\frac{-4v^2wa}{1-w} + 4uwb + \frac{wc}{3} = 0 \implies \frac{v^2}{1-w} = \frac{12ub + c}{12a}.$$

Llamaremos a esta última igualdad la relación fundamental. De las dos últimas ecuaciones del sistema podemos obtener la igualdad

$$-uc + \frac{v^2}{1-w}b = -\frac{9}{4w} \left(4u^2 - \frac{v^2}{1-w}\right)^3, \quad (*)$$

mientras que de las dos primeras obtenemos

$$a^2 - \frac{4}{81} \frac{1-w}{v^2} (3ua + 2b)^2 = \frac{1}{w} \left(4u^2 - \frac{v^2}{1-w}\right)^3.$$

Combinando estas dos igualdades resulta

$$a^2 - \frac{4}{81} \frac{1-w}{v^2} (3ua + 2b)^2 = \frac{4}{9} \left(uc - \frac{v^2}{1-w}b\right).$$

Utilizando la relación fundamental, obtenemos

$$a^2 - \frac{16}{27} \frac{a}{12ub + c} (3ua + 2b)^2 = \frac{4}{9} \left(uc - \frac{12ub + c}{12a}b\right).$$

Esta ecuación cuadrática en  $u$  tiene como solución

$$u = u(a, b, c, \sqrt{\delta}) = \frac{(11a^3b + 2b^2c - ac^2) \pm a\sqrt{\delta}/(25\sqrt{5})}{24(a^4 - b^3 + abc)},$$

donde el signo en frente de  $\sqrt{\delta}$  debe ser determinado. Podemos utilizar la relación fundamental en la ecuación (\*) y despejar  $w$ , obteniendo

$$w = w(a, b, c, \sqrt{\delta}) = \frac{(48u^2a - 12ub - c)^3}{64a^2(12u(ac - b^2) - bc)}.$$

Finalmente, la primera ecuación de nuestro sistema puede ser escrita como

$$\left(12u^2 + \frac{v^2}{1-w}\right)v = wa - 8u^3 - 6u\frac{v^2}{1-w}.$$

Utilizando de nuevo la relación fundamental, llegamos a

$$v = v(a, b, c, \sqrt{\delta}) = -\frac{96u^3a + 72u^2b + 6uc - 12a^2w}{144u^2a + 12ub + c}.$$

Para determinar el signo de  $\sqrt{\delta}$  debemos hacer  $\sqrt{\delta} = \sqrt{\delta(u, v, w)}$ . Es suficiente estudiar el caso para  $u = 1$  y  $v = 0$ . Para estos valores, nuestro sistema se reduce a

$$a = \frac{8}{w}, \quad b = -\frac{12}{w}, \quad c = \frac{144}{w}.$$

Sustituyendo estos valores en la fórmula explícita de  $u$ , obtenemos

$$\pm\sqrt{\delta} = 12^4 \cdot 25\sqrt{5} \frac{1-w}{w^3}.$$

Por otro lado, para  $u = 1$  y  $v = 0$ ,  $t_j$  se reduce a  $s_j = 12(\mathcal{I}/\mathcal{H})\Xi_j$ , por lo que

$$\sqrt{\delta(1, 0, w)} = \prod_{1 \leq j < l \leq 5} (s_j - s_l) = 12^{10} \frac{\mathcal{I}^{10}}{\mathcal{H}^{10}} \prod_{1 \leq j < l \leq 5} (\Xi_j - \Xi_l).$$

Este último producto es un invariante icosaédrico de grado 80, por lo que debe ser combinación lineal de  $\mathcal{I}^5\mathcal{H}$ ,  $\mathcal{J}^2\mathcal{H}$  y  $\mathcal{H}^4$ . Comparando los coeficientes, llegamos a la igualdad

$$\prod_{1 \leq j < l \leq 5} (\Xi_j - \Xi_l) = -25\sqrt{5}\mathcal{J}^2\mathcal{H}.$$

Por lo tanto

$$\sqrt{\delta(1, 0, w)} = -12^{10} \cdot 25\sqrt{5} \left(\frac{\mathcal{I}^5}{\mathcal{H}^3}\right)^2 \left(\frac{\mathcal{J}^2}{\mathcal{H}^3}\right).$$

Finalmente, utilizando que  $q(z) = \mathcal{H}^3/(12^3\mathcal{I}^5) = w$ , obtenemos

$$\sqrt{\delta(1, 0, w)} = -12^4 \cdot 25\sqrt{5} \frac{1-w}{w^3}.$$

De esta forma, para que  $\sqrt{\delta} = \sqrt{\delta(1, 0, w)}$ , necesitamos elegir el signo negativo delante de  $\sqrt{\delta}$ .

Resolviendo este sistema hemos visto que las raíces de la quintica canónica  $P$  y las raíces del resolvente quintico  $P^*$  coinciden como conjuntos. Es más, hemos visto que existe una correspondencia  $\mathcal{A}_5$ -equivariante entre estos conjuntos de raíces, obteniéndose

$$z_j = t_j, \quad j = 1, \dots, 5.$$

Con esto podemos describir un procedimiento para resolver una quintica irreducible dada:

1. Utilizamos la transformación de Tschirnhaus para reducirla a la forma canónica  $P(z) = z^5 + 5az^2 + 5bz + c$ , lo que equivale a resolver una ecuación cuadrática.
2. Calculamos el discriminante  $\delta$  mediante la expresión explícita dada en la sección 4.
3. Obtenemos  $u$ ,  $v$  y  $w$  sustituyendo los valores de  $a$ ,  $b$ ,  $c$  y  $\delta$  en las fórmulas explícitas estudiadas recientemente.

4. Resolvemos la ecuación icosaédrica para este valor de  $w$  y obtenemos  $z = z_1/z_2$  como cociente de dos funciones hipergeométricas (sección 3).
5. Usando los valores de  $u, v$  y  $z$  calculamos  $\Omega_j, \Xi_j$  y  $t_j, j = 1, \dots, 5$ .
6. Como  $z_j = t_j$ , estas son las cinco raíces de la quinta canónica. Basta deshacer el cambio de variable dado por la transformación de Tschirnhaus.

Volviendo sobre nuestros pasos, vemos que  $z_1, \dots, z_5$  dependen racionalmente de  $z^*$ . En particular, cuando  $K = k(z_1, \dots, z_5)$  es el cuerpo de descomposición de la quinta canónica, obtenemos que  $z^*$  genera  $K$  sobre  $k$ . De esta forma completamos la prueba del teorema 3.2.





# Bibliografía

- [1] E.T. Whittaker, G.N. Watson. *A Course of Modern Analysis*.  
Cambridge University Press, 1996.
- [2] Felix Klein. *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*.  
Dover Publications, 2003.
- [3] Gabor Toth. *Glimpses of Algebra and Geometry*.  
Springer, 2002.
- [4] Oliver Nash. *On Klein's Icosahedral Solution of the Quintic*.  
2013.