MA–660: TEORÍA DE GALOIS

Joseph C. Várilly

Escuela de Matemática, Universidad de Costa Rica

II Ciclo Lectivo del 2006

Introducción

Un tema central del álgebra es la resolución de ecuaciones polinomiales. Los documentos escritos más antiguos, desde hace casi cuatro milenios, incluyen procedimientos para obtener soluciones de ecuaciones cuadráticas. En la época clásica de Grecia, el problema de la duplicación del cubo fue objeto de intenso estudio; modernamente, lo enfocamos como la resolución de la ecuación de tercer grado $X^3 = 2$. En el siglo XVI se logró obtener fórmulas para la resolución de la ecuación general de tercer o cuarto grado. A principios del siglo XIX, fue descubierto que no hay, ni puede haber, fórmulas algebraicas análogas para la ecuación general de quinto grado.

A partir de los estudios de Galois, se llegó a comprender que la solubilidad de una ecuación polinomial "por radicales" estaba ligado a la naturaleza del grupo de permutaciones de las raíces de la ecuación. Esto, por un lado, dio un gran impulso al estudio de los grupos como objetos abstractos. Alrededor de 1940, Artin y otros cambiaron el enfoque al estudio de las extensiones de cuerpos: al cuerpo base que incluye los coeficientes del polinomio $p(X)$, como por ejemplo el cuerpo $\mathbb{Q}$ de los números racionales, se le adjunta las raíces de la ecuación $p(X) = 0$. El teorema principal que une los dos conceptos, el de grupo de permutaciones y el de extensión de cuerpo, establece (en condiciones favorables) una *correspondencia de Galois* entre los subgrupos del grupo y los cuerpos intermedios de la extensión.

Por ende, la teoría de Galois es un puente entre el álgebra clásica —el estudio de ecuaciones polinomiales— y el álgebra moderna que enfatiza aspectos mas "estructurales" como cuerpos, anillos, grupos, etc. Hoy en día, se hacen investigaciones activas cuya meta es ampliar la correspondencia de Galois a un ámbito más general, usando nuevas herramientas algebraicas.

El curso empieza con un estudio sobre las propiedades de los polinomios con coeficientes enteros (o racionales). Luego se consideran cuerpos más grandes, al extender $\mathbb{Q}$ mediante la adjunción de números algebraicos, hasta llegar al concepto de una extensión normal de un cuerpo. En seguida se introducen los grupos de automorfismos de un cuerpo numérico y su relación con la resolución de las ecuaciones. Después se pasa al caso importante de un cuerpo con un número finito de elementos, clasificando sus extensiones con la ayuda de la teoría de grupos. Finalmente, se considera una variante moderna de las extensiones galoisianas, en donde el grupo de automorfismos se amplía a su "álgebra de grupo", cuya estructura permite dar una nueva mirada a las simetrías de cuerpos numéricos.

Indíce de materias

1 Polinomios y Resolución de Ecuaciones

1.1 Ecuaciones de tercer o cuarto grado

Un problema muy antiguo es la resolución de ecuaciones de segundo grado:

$$aX^2 + bX + c = 0, \quad \text{con} \quad a \neq 0.$$

Hoy en día, la solución general viene de la "fórmula cuadrática",

$$X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{1.1}$$

En la antigüedad, no se disponía de estas notaciones, pero se conocían procedimientos sistemáticos que son equivalentes a la aplicación de esta fórmula. Los más antiguos documentos matemáticos que conocemos vienen de la época babilonio, en los dos siglos 1800 a 1600 a.C., cuando la región de Mesopotamia fue unificada bajo la dinastía de Hammurabi. La administración contable de este reino grabó sus archivos en lápidas de arcilla; algunas lápidas que se conservan tienen contenido matemático, como tablas numéricas de cuadrados o de recíprocos, o bien exposiciones de problemas computacionales.[1] Un ejemplo es el siguiente:[2]

> El *igibum* excede el *igum* por 7, ¿cuáles son el *igibum* y el *igum*?

Según Neugebauer y Sachs, las palabras sumerianas *igum* e *igibum* denotan cantidades recíprocas, cuyo producto es 1 (o bien 60, ó 3600, etc., en el sistema sexagesimal). En notación moderna, se trata de la ecuación

$$X - \frac{60}{X} = 7,$$

equivalente a la ecuación cuadrática $X^2 - 7X - 60 = 0$. El problema se resuelve como sigue:[3]

> La mitad del exceso 7 es 3;30. Multiplíquese 3;30 por 3;30, esto da 12;15. Al 12;15 se le suma el producto [1,0], resultando 1,12;15. La raíz de 1,12;15 es 8;30. Colóquese 8;30 y 8;30. Restar 3;30 de uno y agregar 3;30 al otro. Ahora uno es 12, el otro es 5. El 12 es el *igibum*, el 5 es el *igum*.

Por la fórmula cuadrática (1.1), la ecuación $X^2 - 7X - 60 = 0$ tiene dos soluciones $X = 12$ y $X = -5$. Los babilonios no tenían el concepto de número negativo, así que obtuvieron $X = 12$ solamente. En el texto, $3;30 = 3\frac{30}{60} = 3\frac{1}{2}$, cuyo cuadrado es $12;15 = 12\frac{15}{60} = 12\frac{1}{4}$, el número siguiente es $1,12;15 = 60 + 12 + \frac{15}{60} = 72\frac{1}{4}$, que aparece en las tablas de cuadrados como el cuadrado de $8;30 = 8\frac{1}{2}$. El procedimiento es entonces equivalente a la fórmula

$$X \text{ y } \frac{1}{X} = \sqrt{\left(\frac{7}{2}\right)^2 + 60} \pm \frac{7}{2} = 12 \text{ y } 5.$$

[1] Véase: Otto Neugebauer, *The Exact Sciences in Antiquity*, Brown Univ. Press, Providence, RI, 1957.

[2] Tomado de una lápida que aparece con una traducción en: Otto Neugebauer y Abraham Sachs, *Mathematical Cuneiform Texts*, American Oriental Society, New Haven, CT, 1945.

[3] Tomado de una historia "popular" del álgebra: John Derbyshire, *Unknown Quantity*, Joseph Henry Press, Washington, DC, 2006; pp. 26–27, siguiendo a Neugebauer y Sachs.

Muchos siglos después, alrededor de 820 d.C., estos y otros procedimientos fueron recopilados por Muhammad ibn Musa al-Khwarizmi (en Baghdad, unos 100 km al norte de la antigua Babilonia, en el otro río), en un famoso tratado sobre "compleción y reducción" (*al-jabr wa'l-muqabala*, de ahí la palabra "álgebra") para la resolución de ecuaciones.

► En notación moderna, la ecuación general de segundo grado,

$$aX^2+bX+c=0, \quad \text{con} \quad a\neq 0,$$

puede expresarse como *polinomio mónico* al dividir por a:

$$X^2+pX+q=0, \quad \text{con} \quad p=\frac{b}{a}, \quad q=\frac{c}{a}.$$

La sustitución $Y=X+\frac{1}{2}p$ simplifica la ecuación:

$$\begin{aligned}
(X+\tfrac{1}{2}p)^2-\tfrac{1}{4}p^2+q&=0,\\
Y^2+q&=\tfrac{1}{4}p^2 && \textit{al-jabr}: \text{sumar } \tfrac{1}{4}p^2 \text{ a cada lado},\\
Y^2&=\tfrac{1}{4}p^2-q && \textit{al-muqabala}: \text{restar } q \text{ de cada lado}.
\end{aligned}$$

Ahora $Y=\pm\sqrt{\frac{1}{4}p^2-q}$, así que

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

Luego, el paso de Y^2 a Y (hay dos raíces cuadrados) conduce a la fórmula cuadrática (1.1).

► Par la resolución de las ecuaciones de tercer grado, podemos comenzar de una vez con un polinomio mónico:

$$Z^3+aZ^2+bZ+c=0.$$

Ahora la sustitución $X=Z+\frac{1}{3}a$ simplifica la ecuación en

$$\begin{aligned}
Z^3+aZ^2+bZ+c&=\left(Z^3+aZ^2+\frac{a^2}{3}Z+\frac{a^3}{27}\right)+\left(b-\frac{a^2}{3}\right)Z+\left(c-\frac{a^3}{27}\right)\\
&=X^3+\left(b-\frac{a^2}{3}\right)X+\left(c-\frac{ab}{3}+\frac{a^3}{27}\right)\\
&=:X^3+pX+q,
\end{aligned}$$

al poner

$$p:=b-\frac{a^2}{3}, \qquad q:=c-\frac{ab}{3}+\frac{a^3}{27}.$$

Ahora se trata de buscar la solución general de

$$X^3+pX+q=0. \tag{1.2}$$

Esta ecuación fue resulta por los italianos en el siglo XVI, en buena parte debido a la disponibilidad de la prensa escrita. Recordemos que Gutenberg estrenó su prensa tipográfica en Mainz alrededor de 1450. Para 1490, Teobaldo Manucci (latinizado a Aldus Manutius) tenía una prensa en Venecia que producía libros con "letra itálica", fáciles de leer. Scipione del Ferro, profesor de matemáticas en Bologna, supuestamente resolvió las ecuaciones de tipo $aX^3 + cX = d$ antes de su muerte en 1526, pero no publicó la solución.[4] Nicolo Tartaglia, de Venecia, logró resolver ecuaciones[5] de tipo $aX^3 + bX^2 = d$ y para 1535 obtuvo una solución del caso anterior también. Discutió sus soluciones con Girolamo Cardano de Milano en 1539; éste, junto con su asistente Lodovico Ferrari, logró sistematizar el procedimiento y además resolver la ecuación general de cuarto grado. Cardano publicó su solución en 1545, donde estrenó las *fórmulas de Cardano*, que son notables por la inclusión de números imaginarios.[6]

Considérese la ecuación (1.2). Cardano sugirió poner $X =: U + V$, donde U, V son *dos* cantidades por determinar. Entonces,

$$U^3 + 3U^2V + 3UV^2 + V^3 + pU + pV + q = 0$$

o bien

$$(U^3 + V^3) + (U + V)(3UV + p) + q = 0.$$

Si ahora elegimos U, V de modo que $3UV + p = 0$, tendremos

$$U^3 + V^3 = -q \quad \text{y a la vez} \quad U^3 + V^3 = -\frac{p^3}{27}.$$

De ahí, U^3 y V^3 son soluciones de la ecuación *cuadrática*:

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

El discriminante de esta ecuación cuadrática es $D = 4d$, donde

$$d = \frac{q^2}{4} + \frac{p^3}{27}.$$

En consecuencia, $T = -\frac{1}{2}q \pm \sqrt{d}$, lo cual da

$$U^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \qquad V^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

[4] Los coeficientes a, c, d son números *positivos*; aun no se aceptaban operaciones con números negativos. Además, tampoco se escribía la letra X: para los italianos de ese siglo, la cantidad incógnita era *cosa*, su cuadrado era *censo* (que significa propiedad o potencia) y su cubo era *cubo*. El caso resuelto por del Ferro se llamaba *il cubo e le cose*.

[5] Con a, b, d positivos: el caso de *il cubo ed i censi*.

[6] Girolamo Cardano, *Artis magnae sive de regulis algebraicis liber unus*, Nürnberg, 1545. El libro, cuyo título se traduce como "Del gran arte, o bien el primer libro de las reglas del álgebra" se conoce comúnmente como *Ars Magna*.

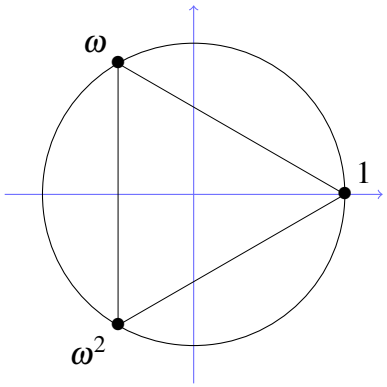


Figura 1: Las tres raíces cúbicas de 1

Sean ahora u, v raíces cúbicas de las expresiones al lado derecho, elegidos de modo que $3uv = -p$. Hay que recordar que un número no cero (real o complejo) tiene tres raíces cúbicas: las raíces cúbicas de 1 son $1, \omega, \omega^2$, donde

$$\omega := \frac{-1+i\sqrt{3}}{2}, \qquad \omega^2 = \frac{-1-i\sqrt{3}}{2},$$

que cumplen $(\omega^2)^2 = \omega$ y $1+\omega+\omega^2 = 0$ (véase la Figura 1). Las tres raíces cúbicas de $(-\frac{1}{2}q + \sqrt{d})$ tienen la forma de $u, \omega u, \omega^2 u$ para algún número complejo u; las tres raíces cúbicas de $(-\frac{1}{2}q + \sqrt{d})$ tiene la forma $v, \omega v, \omega^2 v$ para algún v. Dependiendo de cómo elegimos estas raíces, la cantidad $3uv$ cuyo cubo es $-p^3$, puede ser $-p$, $-\omega p$ ó $-\omega^2 p$ pero nada más. En todo caso, podemos elegir un candidato de cada lista de modo que tres veces su producto es $-p$, en efecto. Entonces las tres soluciones de (1.2) tienen la forma

$$X = u+v, \qquad X = \omega u + \omega^2 v, \qquad X = \omega^2 u + \omega v. \tag{1.4}$$

A veces se escribe estas fórmulas de Cardano en la forma

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

en donde el símbolo $\sqrt[3]{\ }$ es *ambiguo*. En principio, el lado derecho puede tomar 9 valores y para reducirlos a tres valores hay que agregar la regla $3uv = -p$.

► Ferrari logró reducir la ecuación general de cuarto grado a una ecuación cúbica. Con un cambio $X = Z + \frac{1}{4}a$, la ecuación $Z^4 + aZ^3 + bZ^2 + cZ + d = 0$ se transforma en

$$X^4 + pX^2 + qX + r = 0, \tag{1.5}$$

para algunas coeficientes p, q, r. Si fuera posible encontrar un polinomio $sX + t$ de manera que $(sX+t)^2 = -pX^2 - qX - r$, entonces (1.5) se transformaría en $X^4 = (sX+t)^2$, de donde

$$X^2 = sX + t \quad \text{o bien} \quad X^2 = -sX - t,$$

y este par de ecuaciones cuadráticas se resolvería enseguida.

En general, el polinomio $-pX^2 - qX - r$ no es un cuadrado perfecto. Pero se puede lograr el mismo propósito al introducir un parámetro y, sumando a ambos lados (*al-jabr* de nuevo) la misma cantidad $(yX^2 + \frac{1}{4}y^2)$ para obtener

$$(X^2 + \tfrac{1}{2}y)^2 = (y-p)X^2 - qX + (\tfrac{1}{4}y^2 - r). \tag{1.6}$$

El objetivo es elegir y de modo que el lado derecho de esta ecuación tenga la forma $(sX+t)^2 = s^2 + 2stX + t^2$. Como $(2st)^2 = 4s^2t^2$, la condición que y debe satisfacer es

$$q^2 = (y-p)(y^2 - 4r),$$

o bien

$$y^3 - py^2 - 4ry + (4pr - q^2) = 0.$$

Si esta condición se verifica, entonces el lado derecho de (1.6) es igual a

$$(y-p)\left(X - \frac{q}{2(y-p)}\right)^2.$$

En consecuencia, (1.6) se convierte en un par de ecuaciones de segunda grado:

$$X^2 = -\frac{y}{2} + \sqrt{y-p}\left(X - \frac{q}{2(y-p)}\right), \quad \text{o bien} \quad X^2 = -\frac{y}{2} - \sqrt{y-p}\left(X - \frac{q}{2(y-p)}\right). \tag{1.7}$$

Dos aplicaciones de la fórmula cuadrática proporcionan las cuatro expresiones deseadas para X. En ellas, el parámetro y debe sustituirse por *una* de las fórmulas de Cardano que resuelven esta ecuación auxiliar de tercer grado:

$$Y^3 - pY^2 - 4rY + (4pr - q^2) = 0. \tag{1.8}$$

Las raíces $X = \alpha_1, \alpha_2, \alpha_3, \alpha_4$, obtenidas por la fórmula cuadrática a partir de las dos ecuaciones (1.7), obviamente *dependen de la elección de* y entre las tres raíces de (1.8). Volviendo a las fórmulas de Cardano (1.4), sean u, v las expresiones tales que y sea una de $(u+v)$, $(\omega u + \omega^2 v)$, $(\omega^2 u + \omega v)$. Una elección diferente de y entre estas tres expresiones no puede producir nuevas raíces de la ecuación original (1.5), aunque sí *puede alterar el orden* en el que $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ se presentan.

Recordemos que

$$(X-\alpha_1)(X-\alpha_2) = X^2 - (\alpha_1+\alpha_2)X + \alpha_1\alpha_2,$$
$$(X-\alpha_3)(X-\alpha_4) = X^2 - (\alpha_3+\alpha_4)X + \alpha_3\alpha_4,$$

de donde sigue que

$$\alpha_1\alpha_2 = \frac{y}{2} + \frac{q}{2\sqrt{y-p}}, \qquad \alpha_3\alpha_4 = \frac{y}{2} - \frac{q}{2\sqrt{y-p}}.$$

Resulta entonces que

$$y = \alpha_1\alpha_2 + \alpha_3\alpha_4. \tag{1.9}$$

Ahora puede observarse que una permutación de las raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ puede alterar la función $\alpha_1\alpha_2 + \alpha_3\alpha_4$, pero esta función toma a lo sumo *tres valores distintos*. En detalle: las tres combinaciones $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, $\alpha_1\alpha_4 + \alpha_2\alpha_3$ pueden ser distintas. Esto concuerda con la ambigüedad ternaria del parámetro y como solución de la ecuación cúbica (1.8).

► Hubo varios intentos posteriores de obtener procedimientos análogas para la solución de ecuaciones de grado 5 o superior; en vano. Una teoría general[7] fue propuesta por Lagrange en 1771. Su idea fue convertir la ecuación general de grado n, $f(X)=0$, en una ecuación más sencilla para una variable auxiliar t, llamado "resolvente de Lagrange", que *podría expresarse como polinomio en las raíces* de la ecuación $f(X)=0$. Como ejemplo, la y de Ferrari es el polinomio cuadrático (1.9).

Para ilustrar la teoría de Lagrange, consideremos la ecuación (1.2) de tercer grado. Sean $\alpha_1,\alpha_2,\alpha_3$ las raíces de esta ecuación, dadas por la factorización:

$$X^3+pX+q=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3).$$

Sea r una combinación lineal cualquiera de las raíces:

$$r=c_1\alpha_1+c_2\alpha_2+c_3\alpha_3,$$

con ciertos coeficientes complejos c_1,c_2,c_3. Al permutar las raíces, obtenemos 6 combinaciones:

$$\begin{aligned} r_0&=c_1\alpha_1+c_2\alpha_2+c_3\alpha_3, & r_2&=c_1\alpha_2+c_2\alpha_3+c_3\alpha_1, & r_4&=c_1\alpha_3+c_2\alpha_1+c_3\alpha_2,\\ r_1&=c_1\alpha_1+c_2\alpha_3+c_3\alpha_2, & r_3&=c_1\alpha_3+c_2\alpha_2+c_3\alpha_1, & r_5&=c_1\alpha_2+c_2\alpha_1+c_3\alpha_3. \end{aligned}$$

Estas 6 expresiones cumplen una ecuación de sexto grado:

$$(R-r_0)(R-r_1)(R-r_2)(R-r_3)(R-r_4)(R-r_5)=0. \tag{1.10}$$

Una elección astuta de los coeficientes puede simplificar esta última ecuación. Tomemos $c_1:=1$, $c_2:=\omega$, $c_3:=\omega^2$. El *resolvente de Lagrange* para la ecuación cubica (1.2) es

$$r:=\alpha_1+\omega\alpha_2+\omega^2\alpha_3. \tag{1.11}$$

Entonces $r_2=\alpha_2+\omega\alpha_3+\omega^2\alpha_1=\omega^2(\omega\alpha_2+\omega^2\alpha_3+\alpha_1)=\omega^2 r_0$; también $r_4=\omega r_0$, $r_3=\omega^2 r_1$ y $r_5=\omega r_1$: las seis permutaciones de r son r_0, ωr_0, $\omega^2 r_0$, r_1, ωr_1, $\omega^2 r_1$. Al notar que $(R-r_0)(R-\omega r_0)(R-\omega^2 r_0)=R^3-r_0^3$, la ecuación (1.10) se convierte en

$$(R^3-r_0^3)(R^3-r_1^3)=R^6-(r_0^3+r_1^3)R^3+r_0^3r_1^3=0.$$

Hay que resolver esta ecuación cuadrática para R^3. Ahora bien: *sus coeficientes pueden expresarse explícitamente en términos de los coeficientes p,q de la ecuación original.* En efecto,

$$\begin{aligned} r_0r_1&=(\alpha_1+\omega\alpha_2+\omega^2\alpha_3)(\alpha_1+\omega^2\alpha_2+\omega\alpha_3)\\ &=\alpha_1^2+\alpha_2^2+\alpha_3^2-\alpha_1\alpha_2-\alpha_2\alpha_3-\alpha_3\alpha_1\\ &=(\alpha_1+\alpha_2+\alpha_3)^2-3(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)=-3p,\\ r_0^3+r_1^3&=2(\alpha_1^3+\alpha_2^3+\alpha_3^3)-3(\alpha_1^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1+\alpha_1\alpha_2^2+\alpha_2\alpha_3^2+\alpha_3\alpha_1^2)+12\alpha_1\alpha_2\alpha_3\\ &=2(\alpha_1+\alpha_2+\alpha_3)^3-9(\alpha_1+\alpha_2+\alpha_3)(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)+27\alpha_1\alpha_2\alpha_3=-27q, \end{aligned}$$

[7] Joseph-Louis Lagrange, *Réflexions sur la résolution algébrique des équations*, Mém. Acad. Royale des Sciences et Belles-lettres de Berlin, 1771. Lagrange, nacido Guiseppe Lodovico Lagrangia en Torino, 1736, escribió todas sus obras en francés.

así que $R^6 + 27qR^3 - 27p^3 = 0$. Al poner $T = (R/3)^3$, se recupera la ecuación cuadrática (1.3); por ende, las soluciones son $R = 3u$, $R = 3v$, donde u, v son los ingredientes de la solución de Cardano. Para obtener la raíz α_1, por ejemplo, se usa

$$\alpha_1 = \tfrac{1}{3}(3\alpha_1) = \tfrac{1}{3}(2\alpha - \alpha_2 - \alpha_3) = \tfrac{1}{3}(r_0 + r_1) = u + v,$$

y de igual manera $\alpha_2 = \omega^2 u + \omega v$, $\alpha_3 = \omega u + \omega^2 v$.

En resumen: el método de Lagrange conduce de modo sistemático a la solución por las fórmulas de Cardano e indica que la sustitución $X = U + V$ puede obtenerse de una teoría general. La clave de esa teoría general es la elección de una función de las raíces, en este caso $r^3 = (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3$, que toma mucho menos que $n!$ valores bajo permutaciones de estas raíces.

Lagrange trató de encontrar un resolvente adecuado para la ecuación general de quinto grado, pero sin éxito. La imposibilidad de encontrar dicho resolvente fue demostrado por Galois (1831) mediante un análisis novedoso de las propiedades de las permutaciones de las raíces.[8] De este nuevo método surgió el concepto de *grupo* (de permutaciones, inicialmente) y sus implicaciones algebraicas se conoce hoy en día como la "teoría de Galois".

1.2 Anillos de polinomios

Para abordar la teoría de Galois en una forma sistemática, debemos comenzar con ciertos propiedades elementales de polinomios.

Notación. Por lo general, A denotará un *anillo conmutativo*. Supondremos siempre[9] que A contiene una identidad multiplicativa 1. La letra F denotará un *cuerpo*,[10] es decir, un anillo conmutativo en donde cada elemento $a \neq 0$ posee un inverso multiplicativo $a^{-1} = 1/a \in F$.

Los cuerpos más familiares son $\mathbb{Q}$, de números racionales; $\mathbb{R}$, de números reales; $\mathbb{C}$, de números complejos; y el cuerpo finito $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$, de residuos de enteros bajo división por un número *primo* p.

A veces se escribe $\mathbb{Z}_p$ en vez de $\mathbb{F}_p$ como sinónimo de $\mathbb{Z}/p\mathbb{Z}$. Sin embargo, en la teoría algebraica de números, la notación $\mathbb{Z}_p$ está reservado para el anillo de enteros p-ádicos. En este curso, usaremos la notación $\mathbb{F}_p$ para este cuerpo finito de p elementos.

Los siguientes anillos conmutativos no son cuerpos: (a) $\mathbb{Z}$, los números enteros; (b) el anillo de "enteros gaussianos" $\mathbb{Z}[i] := \{m + ni : m, n \in \mathbb{Z}\}$; y (c) el anillo de residuos $\mathbb{Z}/n\mathbb{Z}$ si $n \in \mathbb{N}$ no es primo.

Este último anillo $\mathbb{Z}/n\mathbb{Z}$ contiene "divisores de cero": si $n = rs$ es una factorización de n en $\mathbb{N}$, entonces $\overline{r}\,\overline{s} = \overline{0}$ en $\mathbb{Z}/n\mathbb{Z}$. Para excluir este fenómeno, introducimos el concepto de "anillo entero".

[8] Galois murió el año siguiente al perder un duelo con pistolas, a la edad de 20 años. Su artículo había sido rechazado por la Academia Francesa, pero fue publicado posteriormente por Liouville, en su *Journal de Mathématiques Pures et Appliqueés*, en 1846.

[9] Al demandar que $1 \in A$, seguimos la usanza de Bourbaki.

[10] El nombre viene del alemán *Körper*, un término introducido por Richard Dedekind en 1871; se llama *corps* en francés, *cuerpo* en español, *corp* en rumano, etc., pero en inglés se llama *field*. En español, no debe usarse la traducción secundaria "campo", reservada para campos vectoriales, campos magnéticos, etc.

Definición 1.1. Se dice que un anillo conmutativo A con identidad es un **anillo entero** si $ab = 0$ en $A \implies a = 0$ o bien $b = 0$; es decir, A no contiene divisores de cero.[11]

Por supuesto, $\mathbb{Z}$ es un anillo entero. Cualquier cuerpo es evidentemente un anillo entero. Resulta que $\mathbb{Z}[i]$ también es entero.

Definición 1.2. Si A es un anillo entero, se puede definir su **cuerpo de fracciones** F, como sigue. Declárese una relación de equivalencia entre pares $(a,b) \in A$ con $b \neq 0$ por $(a_1,b_1) \sim (a_2,b_2)$ si y sólo si $a_1b_2 = a_2b_1$; denótese la clase de equivalencia por a/b. Entonces

$$F := \{\, a/b : a,b \in A,\ b \neq 0 \,\},$$

con las operaciones $a_1/b_1 + a_2/b_2 := (a_1b_2 + a_2b_1)/b_1b_2$ y $(a_1/b_1)\,(a_2/b_2) := a_1a_2/b_1b_2$. F incluye una copia de A al identificar $a \in A$ con $a/1 \in F$. Fíjese que $a/b \neq 0$ en F si y sólo si $a \neq 0$ en A, en cuyo caso $(a/b)^{-1} = b/a$.

Es evidente que el cuerpo de fracciones de $\mathbb{Z}$ es el cuerpo $\mathbb{Q}$.

Definición 1.3. Si A es un anillo conmutativo, se denota por $\underline{A[X]}$ el anillo (también conmutativo) de **polinomios** en una indeterminada X, cuyos elementos tienen la forma

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

para algún $n \in \mathbb{N}$;[12] si $f(X) \neq 0$, el mayor exponente n tal que el coeficiente a_n de X^n no es cero se llama el **grado** del polinomio: $n = \operatorname{gr} f(X)$. No se define el grado del polinomio cero. Cuando $a_n = 1$, se dice que $f(X)$ es un *polinomio mónico*.

Formalmente, un polinomio es una sucesión $(a_n)_{n\in\mathbb{N}}$ con valores en A donde solamente un número finito de entradas no son ceros; es cuestión de definir la suma y producto de tales sucesiones apropiadamente. De este punto de vista, la X no es más que una notación cómoda para escribir estas sucesiones, de modo que el producto se ve en forma transparente:

$$\left(\sum_{i=0}^{n} a_iX^i\right)\left(\sum_{j=0}^{m} b_jX^j\right) := \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_ib_j\right)X^k. \tag{1.12}$$

Por inducción, se definen polinomios con más indeterminados: $A[X_1,X_2] := (A[X_1])[X_2]$ y en general $A[X_1,\ldots,X_n] := (A[X_1,\ldots,X_{n-1}])[X_n]$.

Lema 1.4. *Si A es un anillo entero, entonces $A[X]$ es un anillo entero. En particular, $F[X]$ es un anillo entero cuando F es un cuerpo.*

Demostración. Si $f(X) = a_0 + a_1X + \cdots + a_nX^n$ y $g(X) = b_0 + b_1X + \cdots + b_mX^m$ son dos polinomios no nulos, con $a_n \neq 0$ y $b_m \neq 0$, entonces $a_nb_m \neq 0$ porque A es entero. Pero a_nb_m es el coeficiente de X^{m+n} en el producto $f(X)g(X)$, así que $f(X)g(X) \neq 0$ en $A[X]$. □

[11] En francés, *anneau entier*; pero en inglés, *integral domain*. Serge Lang, *Algebra*, 3a edición (Springer, New York, 2002) usa el término *entire ring*. Un "dominio de Dedekind" es una clase de anillos más amplio que los anillos enteros. Es de notar que Kronecker (1881) llamó "dominio de racionalidad" a lo que ahora se llama cuerpo. Huyan de los textos en español que hablan de "dominio íntegro" o "dominio de integridad".

[12] Es oportuno aclarar que usamos el convenio de que $\mathbb{N}$ incluye 0, es decir, $\mathbb{N} = \{0,1,2,3,\ldots\}$.

Definición 1.5. Si F es un cuerpo, se denota por $\overline{F(X)}$ el cuerpo de fracciones del anillo entero $F[X]$. Sus elementos se llaman **funciones racionales** sobre F. Cada función racional es un cociente de dos polinomios $f(X)/g(X)$, con $g(X) \neq 0$.

Proposición 1.6. *Sean A y S dos anillos conmutativos y sea $\varphi\colon A \to S$ un homomorfismo de anillos, es decir, una aplicación que cumple*

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\,\varphi(b) \quad \text{si } a,b \in A; \text{ y} \quad \varphi(1_A) = 1_S.$$

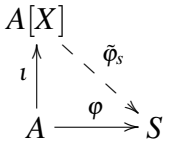
Para todo $s \in S$, hay un único homomorfismo $\tilde{\varphi}_s\colon A[X] \to S$ tal que $\tilde{\varphi}_s(a) = \varphi(a)$ cuando $a \in A$ y además $\tilde{\varphi}_s(X) = s$.

Demostración. Tomando en cuenta la inclusión $A \hookrightarrow A[X]$ que identifica elementos de A con polinomios de grado 0, se dice que "$\tilde{\varphi}_s$ extiende φ a $A[X]$" toda vez que $\tilde{\varphi}_s(a) = \varphi(a)$ cuando $a \in A$. La extensión buscada, que además debe cumplir $\tilde{\varphi}_s(X) = s$, necesariamente obedece

$$\tilde{\varphi}_s(a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) := \varphi(a_0) + \varphi(a_1)s + \varphi(a_2)s^2 + \cdots + \varphi(a_n)s^n.$$

Se verifica fácilmente que esta receta es un homomorfismo de $A[X]$ en S. □

Esta extensión se puede representar mediante el siguiente diagrama, en donde la flecha quebrada (cuya existencia se propone) muestra la *propiedad universal* del anillo de polinomios:



en donde $\iota\colon A \to A[X]$ denota la inclusión.

Corolario 1.7. *Si $\varphi\colon A \to S$ es un homomorfismo y $s_1, \ldots, s_n \in S$, hay un único homomorfismo $\tilde{\varphi}_{s_1,\ldots,s_n}\colon A[X_1,\ldots,X_n] \to S$ que extiende φ tal que $\tilde{\varphi}_{s_1,\ldots,s_n}(X_j) = s_j$ para $j = 1,\ldots,n$.* ⊟

► Repasemos las propiedades de divisibilidad en el anillo $\mathbb{Z}$. Si $m,n \in \mathbb{Z}$, se dice que m *divide* n, escrito $m \setminus n$, si hay $q \in \mathbb{Z}$ tal que $n = qm$.[13] Las propiedades esenciales para que $k \in \mathbb{Z}$ sea un **máximo común divisor** de m y n son:

1. $k \setminus m$, $k \setminus n$;
2. si $t \setminus m$ y $t \setminus n$, entonces $t \setminus k$.

Si además se exige $k > 0$, entonces k es único y se llama *el* máximo común divisor de m y n; se escribe $k = \overline{\mathrm{mcd}(m,n)}$.

Para calcular $\mathrm{mcd}(m,n)$ para dos enteros dados, se usa el *algoritmo euclidiano*.[14]

[13] Esta notación se prefiere sobre la más usual $m \mid n$, por recomendación de Graham, Knuth y Patashnik, *Concrete Mathematics*, Addison-Wesley, Reading, MA, 1989.

[14] El procedimiento se encuentra en el libro VII de los *Elementos* de Euclides.

Lema 1.8. *Si $m,n \in \mathbb{Z}$ con $m > 0$, $n > 0$, entonces hay enteros únicos q,r tales que*

$$n = qm + r, \quad con \quad 0 \le r < m. \tag{1.13}$$

Demostración. Si $m > n$, tómese $q := 0$, $r := n$. En cambio, si $m \le n$, considérese la sucesión de enteros $n, n-m, n-2m, \ldots$. Por la propiedad arquimediano de los enteros, hay $q \in \mathbb{N}$ (único) tal que $n - qm \ge 0$ pero $n - (q+1)m < 0$; tómese $r := n - qm$. □

Proposición 1.9 (Algoritmo euclidiano en $\mathbb{Z}$)**.** *Si $m,n \in \mathbb{Z}$ con $m > 0$, $n > 0$, su máximo común divisor se encuentra como sigue. Defínase dos sucesiones de enteros (q_j), (r_j) así:*

$$\begin{aligned}
n &= q_1 m + r_1 \quad con \quad 0 < r_1 < m,\\
m &= q_2 r_1 + r_2 \quad con \quad 0 < r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3 \quad con \quad 0 < r_3 < r_2,\\
\vdots &= \qquad \vdots \\
r_{k-2} &= q_k r_{k-1} + r_k \quad con \quad 0 < r_k < r_{k-1},\\
r_{k-1} &= q_{k+1} r_k + 0.
\end{aligned}$$

Entonces $\mathrm{mcd}(m,n) = r_k$*, el último residuo no cero en estas divisiones. Además, se verifica la siguiente relación:*

$$\mathrm{mcd}(m,n) = am + bn \quad para\ algunos \quad a,b \in \mathbb{Z}. \tag{1.14}$$

Demostración. Para ver que $r_k \setminus n$, obsérvese que

$$n = q_1 m + r_1 = q_1(q_2 r_1 + r_2) + r_1 = (q_1 q_2 + 1) r_1 + q_1 r_2.$$

Sustituyendo $m, r_1, r_2, \ldots, r_{k-2}$ uno por uno por los lados derechos que aparecen en el enunciado de la Proposición, se llega a $n = c r_{k-1} + d r_k$ para algunos $c,d \in \mathbb{Z}$, así que $n = (c q_{k+1} + d) r_k$ y por tanto $r_k \setminus n$. El mismo proceso muestra que $r_k \setminus m$.

Ahora, si $t \in \mathbb{N}$ es tal que $t \setminus m$ y $t \setminus n$, entonces t divide $n - q_1 m = r_1$. En seguida, $t \setminus (m - q_2 r_1) = r_2$ y así sucesivamente hasta ver que $t \setminus (r_{k-2} - q_k r_{k-1}) = r_k$. Se concluye que $r_k = \mathrm{mcd}(m,n)$.

Para comprobar (1.14), fíjese que $r_1 = n - q_1 m$; que $r_2 = m - q_2 r_1 = m - q_2(n - q_1 m) = (q_1 q_2 + 1)m - q_2 n$; por sustitución repetida, se encuentran $a_j, b_j \in \mathbb{Z}$ con $r_j = a_j m + b_j n$, para $j = 1, 2, \ldots, k$. □

Corolario 1.10. *Dos enteros $m,n \in \mathbb{N}$ son* relativamente primos*, es decir,* $\mathrm{mcd}(m,n) = 1$*, si y solo si existen $a,b \in \mathbb{Z}$ tales que $am + bn = 1$.* □

► Sea F un cuerpo cualquiera. El anillo entero tiene propiedades de divisibilidad análogas a las de $\mathbb{Z}$. Un polinomio $g(X)$ divide un polinomio $f(X)$ si hay un polinomio $q(X)$ tal que $f(X) = q(X)g(X)$. El *máximo común divisor* $k(X) = \mathrm{mcd}(f(X), g(X))$ es el (único) polinomio *mónico* tal que: (i) $k(X) \setminus f(X)$, $k(X) \setminus g(X)$; y (ii) si $h(X) \setminus f(X)$ y $h(X) \setminus g(X)$, entonces $h(X) \setminus k(X)$.

La existencia y también el cálculo explícito del máximo común divisor está garantizado por el algoritmo euclidiano, una vez que se comprueba la siguiente propiedad de divisibilidad.

Lema 1.11. *Si $f(X)$ y $g(X)$ son dos polinomios en $F[X]$ con $g(X) \neq 0$, entonces hay un único par de polinomios $q(X)$, $r(X)$ tales que*

$$f(X) = q(X)g(X) + r(X), \quad con \quad \begin{cases} \operatorname{gr} r(X) < \operatorname{gr} g(X), \\ o\ bien\ \ r(X) = 0. \end{cases} \tag{1.15}$$

Demostración. Escríbase $f(X) = a_0 + a_1X + \cdots + a_nX^n$ y $g(X) = b_0 + b_1X + \cdots + b_mX^m$. Si $m > n$, tómese $q(X) := 0$, $r(X) := f(X)$.

En cambio, si $m \leq n$, entonces

$$f(X) - \frac{a_n}{b_m} X^{n-m} g(X) =: f_1(X)$$

es un polinomio con $\operatorname{gr} f_1(X) < n$. Invoquemos inducción sobre n, para poder suponer que $f_1(X) = q_1(X)g(X) + r_1(X)$, con $\operatorname{gr} r(X) < m$ o bien $r(X) = 0$. Entonces

$$f(X) = \left(\frac{a_n}{b_m} X^{n-m} + q_1(X)\right) g(X) + r(X),$$

y el resultado (1.15) sigue por la inducción sobre n.

Para la unicidad de $q(X)$ y $r(X)$, obsérvese que si $q(X)g(X) + r(X) = \tilde{q}(X)g(X) + \tilde{r}(X)$, entonces $\big(q(X) - \tilde{q}(X)\big)g(X) = \tilde{r}(X) - r(X)$. Si los lados de esta ecuación no se anulan, entonces al lado izquierdo el grado sería $\geq m$, mientras al lado derecho el grado sería $< m$, lo cual es imposible. Por tanto $\tilde{r}(X) = r(X)$ y $\big(q(X) - \tilde{q}(X)\big)g(X) = 0$. Como $F[X]$ es un anillo entero y $g(X) \neq 0$, se concluye que $\tilde{q}(X) = q(X)$. □

Ejemplo 1.12. Hay que notar que el resultado $r_k(X)$ de aplicar el algoritmo euclidiano a dos polinomios $f(X)$, $g(X)$ no es necesario mónico, pero siempre será *un* máximo común divisor de los dos polinomios originales. Por ejemplo, si $f(X) = X^{12} - 1$ y $g(X) = (X^2 - X + 1)^4$, el resultado de aplicar el algoritmo —usando *Mathematica*— es el siguiente:

$$\begin{aligned}
r_1(X) &= 2(7 - 30X + 72X^2 - 110X^3 + 120X^4 - 90X^5 + 45X^6 - 12X^7), \\
r_2(X) &= \frac{1}{48}(41 - 134X + 288X^2 - 370X^3 + 352X^4 - 198X^5 + 75X^6), \\
r_3(X) &= \frac{32}{625}(-11 + 14X - 23X^2 + 70X^3 - 67X^4 + 58X^5), \\
r_4(X) &= \frac{625}{161472}(107 - 500X + 1215X^2 - 1108X^3 + 715X^4), \\
r_5(X) &= \frac{861184}{319515625}(-274 + 405X - 405X^2 + 131X^3), \\
r_6(X) &= \frac{8626921875}{923673664}(1 - X + X^2).
\end{aligned}$$

Además, $r_7(X) = 0$, así que $r_6(X)$ es un máximo común divisor de $f(X)$ y $g(X)$. Al reemplazar $r_6(X)$ por el polinomio mónico asociado, se llega al resultado deseado:

$$\operatorname{mcd}\big(X^{12} - 1, (X^2 - X + 1)^4\big) = X^2 - X + 1.$$

► Un polinomio $f(X) \in F[X]$ se llama *irreducible* si no posee factores propios, es decir, si no es posible expresar $f(X) = h(X)k(X)$ con $\operatorname{gr} h(X) < \operatorname{gr} f(X)$ y $\operatorname{gr} k(X) < \operatorname{gr} f(X)$. La reducibilidad de un polinomio depende del cuerpo F de coeficientes. El resultado básico en esta materia es la siguiente proposición (no demostrada): con coeficientes complejos, cualquier polinomio es completamente reducible.

Proposición 1.13 (Teorema Fundamental del Álgebra)**.** *Cada polinomio irreducible en $\mathbb{C}[X]$ es de primer grado. Si $f(X) \in \mathbb{C}[X]$, entonces*

$$f(X) = a_n (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n), \tag{1.16}$$

*para algunos $\alpha_1, \dots, \alpha_n \in \mathbb{C}$. Los α_j se llaman **raíces** del polinomio $f(X)$, o bien de la ecuación $f(X) = 0$.* ⊟

Cuando se considera coeficientes *reales*, los polinomios irreducibles en $\mathbb{R}[X]$ son de primer o segundo grado. Por ejemplo, $X^2 + 1$ es irreducible en $\mathbb{R}[X]$ pero no en $\mathbb{C}[X]$: de hecho, $X^2 + 1 = (X - i)(X + i)$. Si $f(X)$ tiene coeficientes reales $a_0, a_1, \dots, a_n \in \mathbb{R}$, entonces $f(X)$ es invariante bajo conjugación compleja:

$$a_n (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n) = a_n (X - \bar{\alpha}_1)(X - \bar{\alpha}_2) \dots (X - \bar{\alpha}_n).$$

Entonces, tras una permutación adecuada, los α_j o bien son reales o se agrupan en pares conjugadas: se puede suponer que para algún r con $0 \le 2r \le n$, vale $\bar{\alpha}_{2j} = \alpha_{2j-1}$ para $j = 1, \dots, r$; y $\alpha_k \in \mathbb{R}$ para $k > 2r$. En tal caso,

$$(X - \alpha_{2j-1})(X - \alpha_{2j}) = (X - \bar{\alpha}_{2j})(X - \alpha_{2j}) = X^2 - (2\Re\alpha_{2j})X + |\alpha_{2j}|^2$$

es un polinomio cuadrático real irreducible.

Ejemplo 1.14. Cada polinomio de cuarto grado en $\mathbb{R}[X]$ es reducible. Por ejemplo,

$$X^4 + 1 = (X^4 + 2X^2 + 1) - 2X^2 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1).$$

El caso de la factorización de polinomios con *coeficientes racionales* es mucho más intrincado. Si $f(X) = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{Q}[X]$, sea $c \in \mathbb{N}$ el mínimo común denominador de $a_0, a_1, \dots, a_n$. Entonces $c f(X) \in \mathbb{Z}[X]$, con coeficientes enteros. Por otro lado, si $d = \operatorname{mcd}(ca_0, ca_1, \dots, ca_n)$, entonces $(c/d) f(X) \in \mathbb{Z}[X]$ es un polinomio *primitivo*, es decir, sus coeficientes no tienen factor común.

Lema 1.15. *El producto de dos polinomios primitivos en $\mathbb{Z}[X]$ es primitivo.*

Demostración. Si $f(X) = a_0 + a_1 X + \dots + a_n X^n$ y $g(X) = b_0 + b_1 X + \dots + b_m X^m$ son primitivos en $\mathbb{Z}[X]$, supóngase que hay un número primo p que divide cada coeficiente $c_k := \sum_{i+j=k} a_i b_j$ de su producto (1.12). Sean a_r, b_s los primeros coeficientes de $f(X)$, $g(X)$ respectivamente que *no* son divisibles por p. Entonces

$$c_{r+s} = (a_0 b_{r+s} + \dots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \dots + a_{r+s} b_0),$$

en donde $p \setminus a_i$ para $i = 0, \dots, r-1$, $p \setminus b_j$ para $j = 0, \dots, s-1$ y $p \setminus c_{r+s}$. Por tanto, $p \setminus a_r b_s$, y en consecuencia $p \setminus a_r$ o bien $p \setminus b_s$, contrario a hipótesis. Se concluye que $c_0, c_1, \dots, c_{n+m}$ no pueden tener factor común. □

Proposición 1.16 (Lema de Gauss)**.** *Sea $f(X) \in \mathbb{Z}[X]$ un polinomio con coeficientes enteros. Entonces $f(X)$ se factoriza en $\mathbb{Q}[X]$ si y sólo si se factoriza en $\mathbb{Z}[X]$.*[15]

Demostración. Se puede suponer que $f(X)$ es primitivo. Sea $f(X) = h(X)\,k(X)$ una factorización en $\mathbb{Q}[X]$ con $\operatorname{gr} h(X) \geq 1$, $\operatorname{gr} k(X) \geq 1$. Al sacar denominadores comunes, hay $a,b,c,d \in \mathbb{Z}$ tales que $h(X) = (a/b)\,\tilde{h}(X)$ y $k(X) = (c/d)\,\tilde{k}(X)$, donde $\tilde{h}(X)$ y $\tilde{k}(X)$ son polinomios primitivos en $\mathbb{Z}[X]$. Ahora se verifica

$$bd\,f(X) = ac\,\tilde{h}(X)\,\tilde{k}(X) \quad \text{en} \quad \mathbb{Z}[X].$$

El máximo común divisor de los coeficientes de $bd\,f(X)$ es bd. Como $\tilde{h}(X)\tilde{k}(X)$ es primitivo, por el lema anterior, el máximo factor común al lado derecho es ac. Luego $bd = ac$, así que $f(X) = (ac/bd)\,\tilde{h}(X)\,\tilde{k}(X) = \tilde{h}(X)\,\tilde{k}(X)$ factoriza $f(X)$ en $\mathbb{Z}[X]$. □

Determinar si un polinomio dado en $\mathbb{Z}[X]$ es irreducible o no puede ser difícil en la práctica. Un criterio que es bastante útil en algunos casos es el siguiente.

Proposición 1.17 (Criterio de Eisenstein)**.** *Sea $f(X) = a_0 + a_1X + \cdots + a_nX^n$ un polinomio en $\mathbb{Z}[X]$. Si hay un número primo p tal que*

- *p divide $a_0, a_1, \ldots, a_{n-1}$;*
- *p no divide a_n; y p^2 no divide a_0;*

entonces $f(X)$ es irreducible en $\mathbb{Z}[X]$.

Demostración. Supóngase que $f(X) = g(X)\,h(X)$ es una factorización no trivial en $\mathbb{Z}[X]$, donde $g(X) = b_0 + b_1X + \cdots + b_mX^m$ y $h(X) = c_0 + c_1X + \cdots + c_{n-m}X^{n-m}$. Ahora $a_0 = b_0c_0$. Como $p \setminus a_0$ pero $p^2 \nmid a_0$, resulta entonces que p divide uno y sólo uno de b_0 y c_0: digamos que $p \setminus b_0$ pero $p \nmid c_0$.

Como p no puede dividir todos los b_j, porque entonces sería un factor escalar de $g(X)$ y por ende de $f(X)$, sea b_r el primer coeficiente de $g(X)$ tal que $p \nmid b_r$. Entonces

$$a_r = b_0c_r + \cdots + b_{r-1}c_1 + b_rc_0,$$

en donde $p \setminus b_j$ para $j = 0, \ldots, r-1$ y $p \setminus a_r$. Por tanto, $p \setminus b_rc_0$, lo cual contradice $p \nmid b_r$ y $p \nmid c_0$. Se concluye que no hay tal factorización de $f(X)$. □

Ejemplo 1.18. Si $p \in \mathbb{N}$ es primo, entonces $X^n - p$ es irreducible en $\mathbb{Z}[X]$ para todo $n = 1, 2, 3, \ldots$; en efecto, este polinomio cumple el criterio de Eisenstein para el mismo número primo p.

[15] Este es el inciso 42 en: Carl Friedrich Gauß, *Disquisitiones Arithmeticae*, Leipzig, 1801. Hay una traducción al español, editado por Hugo Barrantes, Michael Josephy y Ángel Ruiz (Academia Colombiana de Ciencias, Santafé de Bogotá, 1995).

Ejemplo 1.19. Si $p \in \mathbb{N}$ es un número primo, considérese el polinomio

$$h(X) = 1 + X + X^2 + X^3 + \cdots + X^{p-1}. \tag{1.17}$$

Fíjese que $h(X) = (X^p - 1)/(X - 1)$. No puede aplicarse el criterio de Eisenstein en forma directa a $h(X)$. Pero obsérvese que

$$\begin{aligned} g(X) := h(X+1) &= \frac{(X+1)^p - 1}{(X+1) - 1} \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + \binom{p}{2} X^{p-3} + \cdots + \binom{p}{p-2} X + \binom{p}{p-1}. \end{aligned}$$

Se sabe que p divide $\binom{p}{k}$ para $k = 1, 2, \ldots, p-1$ y que $\binom{p}{p-1} = \binom{p}{p-1} = p$. Ahora el criterio de Eisenstein permite concluir que $g(X)$ es irreducible. Esto conlleva la irreducibilidad de $h(X)$, porque una factorización $h(X) = k(X)\,l(X)$ implicaría $g(X) = k(X+1)\,l(X+1)$. Por lo tanto, el polinomio (1.17) es también irreducible.

1.3 Polinomios simétricos

Definición 1.20. Una *permutación* del conjunto $\{1, 2, \ldots, n\}$ es una biyección de este conjunto en sí mismo. Las permutaciones forman un grupo (no conmutativo) bajo composición de funciones. Este grupo se denota S_n y contiene $n!$ elementos.

Definición 1.21. Si $\sigma \in S_n$, se puede definir un automorfismo φ_σ del anillo $A[X_1, \ldots, X_n]$ por

$$\varphi_\sigma(f(X_1, \ldots, X_n)) := f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}). \tag{1.18}$$

Obsérvese que φ_σ es la extensión del homomorfismo de inclusión $\iota : A \to A[X_1, \ldots, X_n]$ determinado por $\varphi_\sigma(X_j) := X_{\sigma(j)}$. Su existencia sigue del Corolario 1.7, con $S = A[X_1, \ldots, X_n]$. Es evidente que φ_σ es biyectivo, con inverso $\varphi_{\sigma^{-1}}$.

Un polinomio $f = f(X_1, \ldots, X_n)$ se llama **polinomio simétrico** si $\varphi_\sigma(f) = f$ para toda permutación $\sigma \in S_n$.

Ejemplo 1.22. Los siguientes polinomios de grado 3 en tres variables son simétricos:

$$X_1^3 + X_2^3 + X_3^3, \qquad X_1^2X_2 + X_1^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2, \qquad X_1X_2X_3.$$

Por otro lado, $X_1^2X_2 + X_2^2X_3 + X_3^2X_1$ no es simétrico.

Definición 1.23. Para cada n fijo, y para cada $k = 1, 2, \ldots, n$, se define el **polinomio simétrico elemental** $\underline{s_k}$ de grado k en n variables por

$$s_k(X_1, \ldots, X_n) := \sum_{\substack{J \subset \{1,2,\ldots,n\} \\ |J| = k}} \left(\prod_{j \in J} X_j \right).$$

Para $n = 3$, los polinomios simétricos elementales son:

$$s_1 := X_1 + X_2 + X_3, \qquad s_2 := X_1X_2 + X_1X_3 + X_2X_3, \qquad s_3 := X_1X_2X_3.$$

El polinomio $s_k(X_1, \ldots, X_n)$ es entonces la suma de todos los posibles productos de k de las indeterminadas, sin repetición.

Si Z es otra indeterminada, en el anillo $\mathbb{Z}[X_1, \ldots, X_n, Z]$ se verifica

$$(Z - X_1)(Z - X_2)\ldots(Z - X_n) = Z^n - s_1 Z^{n-1} + s_2 Z^{n-2} + \cdots + (-1)^n s_n, \tag{1.19}$$

la cual sirve como definición alternativa de los $s_k = s_k(X_1, \ldots, X_n)$.

Proposición 1.24. *Si $p(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n \in F[X]$ es un polinomio* mónico *con raíces $\alpha_1, \ldots, \alpha_n \in F$, entonces sus coeficientes cumplen*

$$a_{n-k} = (-1)^k s_k(\alpha_1, \ldots, \alpha_n). \tag{1.20}$$

Demostración. Hay un homomorfismo estándar $\varphi\colon \mathbb{Z} \to F[X]$ determinado por $\varphi(1) := 1_F \in F[X]$. Por el Corolario 1.7, éste se extiende a un homomorfismo $\tilde{\varphi}\colon \mathbb{Z}[X_1, \ldots, X_n, Z] \to F[X]$, de manera única, al poner $\tilde{\varphi}(X_j) := \alpha_j$ para cada j y $\tilde{\varphi}(Z) := X$. Al aplicar $\tilde{\varphi}$ a ambos lados de la ecuación (1.19), se obtiene

$$p(X) = X^n - s_1(\alpha_1, \ldots, \alpha_n)X^{n-1} + s_2(\alpha_1, \ldots, \alpha_n)X^{n-2} + \cdots + (-1)^n s_n(\alpha_1, \ldots, \alpha_n), \tag{1.21}$$

de donde las identidades (1.20) son evidentes. □

En particular, en la factorización $X^3 + aX^2 + bX + c = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ se obtiene

$$-a = \alpha_1 + \alpha_2 + \alpha_3, \qquad b = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \qquad -c = \alpha_1\alpha_2\alpha_3.$$

Cualquier polinomio simétrico puede expresarse en función de los polinomios simétricos elementales. Por ejemplo,

$$X_1^2 + \cdots + X_n^2 = (X_1 + \cdots + X_n)^2 - 2(X_1X_2 + \cdots + X_{n-1}X_n) = s_1^2 - 2s_2.$$

Para $n = 3$, otro ejemplo es

$$\begin{aligned} X_1^3 + X_2^3 + X_3^3 &= (X_1 + X_2 + X_3)^3 - 3(X_1 + X_2 + X_3)(X_1X_2 + X_1X_3 + X_2X_3) + 3X_1X_2X_3 \\ &= s_1^3 - 3s_1s_2 + 3s_3. \end{aligned}$$

En $F[X_1, \ldots, X_n]$, el producto $s_1^{k_1}s_2^{k_2}\ldots s_n^{k_n}$ es una suma simétrica de monomios cuyo primer término es $X_1^{k_1+k_2+\cdots+k_n}X_2^{k_2+\cdots+k_n}\ldots X_{n-1}^{k_{n-1}+k_n}X_n^{k_n}$. Su grado, como elemento de $F[X_1, \ldots, X_n]$, es $k_1 + 2k_2 + \cdots + nk_n$: esta cantidad puede llamarse el "peso" del monomio $s_1^{k_1}s_2^{k_2}\ldots s_n^{k_n}$.

Los polinomios simétricos generan una *subálgebra* de $F[X_1, \ldots, X_n]$. El siguiente resultado dice que los polinomios simétricos *elementales* generan esta subálgebra.[16]

[16] Un *álgebra* sobre un cuerpo F es un anillo que es a su vez un espacio vectorial sobre F.

Proposición 1.25. *Si $f(X_1,\dots,X_n)$ es un polinomio simétrico en $F[X_1,\dots,X_n]$ de grado r, entonces hay un único polinomio p de n variables, de peso $\leq r$, tal que $f(X_1,\dots,X_n) = p(s_1,\dots,s_n)$.*

Demostración. Si se pone $X_n = 0$ en la relación (1.19), se obtiene

$$(Z-X_1)\dots(Z-X_{n-1})Z = Z^n - \tilde{s}_1 Z^{n-1} + \cdots + (-1)^n \tilde{s}_{n-1} Z,$$

donde los $\tilde{s}_k(X_1,\dots,X_{n-1}) = s_k(X_1,\dots,X_{n-1},0)$ son los polinomios simétricos elementales en $(n-1)$ variables.

Ahora se puede hacer una doble inducción sobre n (el caso $n=1$ es trivial) y sobre el grado r (el caso $r=0$ es trivial). Supóngase, entonces, que el enunciado sea válido para polinomios de menos de n variables, y para polinomios de n variables de grado $< r$. Luego, hay un polinomio g de $n-1$ variables, de peso $\leq r$, tal que

$$f(X_1,\dots,X_{n-1},0) = g(\tilde{s}_1,\dots,\tilde{s}_{n-1}).$$

En ese caso, el polinomio

$$f_1(X_1,\dots,X_n) := f(X_1,\dots,X_n) - g(s_1,\dots,s_{n-1}) \quad \in F[X_1,\dots,X_n]$$

tiene grado $\leq r$, es simétrico en $X_1,\dots,X_n$ y satisface $f_1(X_1,\dots,X_{n-1},0) = 0$. Por tanto, este polinomio es divisible por X_n. Por su simetría, también es divisible por $X_1,\dots,X_{n-1}$, y en consecuencia es divisible por $s_n = X_1\dots X_n$. Resulta, entonces, que

$$f_1(X_1,\dots,X_n) = s_n\, h(X_1,\dots,X_n)$$

para algún polinomio h con $\operatorname{gr} h(X_1,\dots,X_n) \leq r-n$. la hipótesis inductiva asegura que hay un polinomio g_1 de n variables con $h(X_1,\dots,X_n) = g_1(s_1,\dots,s_n)$. Entonces

$$f(X_1,\dots,X_n) = g(s_1,\dots,s_{n-1}) + s_n\, g_1(s_1,\dots,s_n),$$

en donde cada monomio al lado derecho tiene peso $\leq r$.

Para la *unicidad*, basta mostrar que no puede haber un polinomio q de grado ≥ 1 tal que $q(s_1,\dots,s_n) = 0$. En el caso contrario, tómese q del menor grado posible. Al desarrollar q con respecto a la variable X_n, se obtiene

$$q(X_1,\dots,X_n) = q_0(X_1,\dots,X_{n-1}) + q_1(X_1,\dots,X_{n-1})X_n + \cdots + q_k(X_1,\dots,X_{n-1})X_n^k,$$

en donde $q_0(X_1,\dots,X_{n-1}) \neq 0$. (Porque si no, sería $q(X_1,\dots,X_n) = X_n\, k(X_1,\dots,X_n)$ y por ende $s_n\, k(s_1,\dots,s_n) = 0$, lo cual implicaría $k(s_1,\dots,s_n) = 0$ con $\operatorname{gr} k < \operatorname{gr} q$.) Entonces

$$q_0(s_1,\dots,s_{n-1}) + \cdots + q_k(s_1,\dots,s_{n-1})\, s_n^k = 0,$$

y la sustitución $X_n \mapsto 0$, que conlleva $s_n \mapsto 0$, produce la relación $q_0(\tilde{s}_1,\dots,\tilde{s}_{n-1}) = 0$. Se ve que este es una relación no trivial entre los polinomios simétricos elementales en $(n-1)$ variables. La ausencia de tales relaciones sigue por inducción sobre n. □

Al no haber una relación polinomial no trivial entre $s_1,\dots,s_n$, se dice que éstos son *algebraicamente independientes*. La conclusión es que la subálgebra de polinomios simétricos en $F[X_1,\dots,X_n]$ es también un álgebra polinomial: se identifica con $F[s_1,\dots,s_n]$.

Corolario 1.26. *Si $F \subseteq \mathbb{C}$, sean $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ las raíces del polinomio $f(X) \in F[X]$. Si h es cualquier polinomio simétrico de n variables, entonces $h(\alpha_1, \ldots, \alpha_n) \in F$.*

Demostración. Por la Proposición 1.25, basta tomar $h = s_k$, uno de los polinomios simétricos elementales. Si $f(X) = a_0 + a_1 X + \ldots + a_n X^n$, la Proposición 1.24 dice que $h(\alpha_1, \ldots, \alpha_n) = (-1)^k a_{n-k}/a_n \in F$. □

► A veces es importante saber si dos polinomios tienen una raíz común, antes de calcular las raíces explícitamente. Hay una cantidad escalar que depende solamente de los coeficientes de los dos polinomios y que detecta la presencia de una raíz común.

Definición 1.27. Sean $f(X) = a_0 + a_1 X + \cdots + a_n X^n$, $g(X) = b_0 + b_1 X + \cdots + b_m X^m$ dos polinomios en $F[X]$, donde $F \subseteq \mathbb{C}$. Sean

$$f(X) = a_n (X - \alpha_1) \ldots (X - \alpha_n), \qquad g(X) = b_m (X - \beta_1) \ldots (X - \beta_m)$$

sus factorizaciones en $\mathbb{C}[X]$. El **resultante** de estos dos polinomios es

$$\operatorname{Res}(f, g) := a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j). \tag{1.22}$$

Si $f(X) = 0$ ó $g(X) = 0$, se define $\operatorname{Res}(f, g) := 0$.

Obsérvese que $\operatorname{Res}(g, f) = (-1)^{mn} \operatorname{Res}(f, g)$. Además, es claro que

$$\operatorname{Res}(f, g) := a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} f(\beta_j). \tag{1.23}$$

Para el caso de polinomios constantes ($n = 0$ ó $m = 0$), estas fórmulas son consistentes can $\operatorname{Res}(a_0, g) := a_0^m$, $\operatorname{Res}(f, b_0) := b_0^n$.

Lema 1.28. *El resultante se anula, $\operatorname{Res}(f, g) = 0$, si y sólo si $f(X)$ y $g(X)$ tienen una raíz común (en $\mathbb{C}$), si y sólo si el máximo común divisor de $f(X)$ y $g(X)$ tiene grado al menos* 1.

Demostración. Está claro que la cantidad (1.22) es cero si y sólo si una de las α_i coincide con una de las β_j. Por otra parte, si $h(X) := \operatorname{mcd}(f(X), g(X))$ en $F[X]$ es de grado mayor que cero, hay algún $\zeta \in \mathbb{C}$ con $h(\zeta) = 0$ y por ende $f(\zeta) = 0$ y $g(\zeta) = 0$: este ζ es una raíz común de $f(X)$ y $g(X)$. En cambio, si $f(\eta) = g(\eta) = 0$ para algún $\eta \in \mathbb{C}$, la relación $h(X) = a(X) f(X) + b(X) g(X)$ muestra que $h(\eta) = 0$ también, así que $(X - \eta)$ es un factor de $h(X)$ en $\mathbb{C}[X]$: se concluye que $\operatorname{gr} h(X) \geq 1$. □

Lema 1.29. *Si $f(X) = q(X) g(X) + r(X)$ en $f[X]$, en donde $k = \operatorname{gr} r(X) < \operatorname{gr} g(X)$ o bien $r(X) = 0$, entonces*

$$\operatorname{Res}(f, g) = (-1)^{mn} b_m^{n-k} \operatorname{Res}(g, r). \tag{1.24}$$

En consecuencia, se puede calcular $\operatorname{Res}(f, g)$ con el algoritmo euclidiano.

Demostración. Al aplicar las dos fórmulas en (1.23), se ve que

$$\begin{aligned}\operatorname{Res}(f,g) &= \operatorname{Res}(qg+r,g) = (-1)^{mn} b_m^n \prod_{j=1}^{m} q(\beta_j)\, g(\beta_j) + r(\beta_j) \\ &= (-1)^{mn} b_m^n \prod_{j=1}^{m} r(\beta_j) = (-1)^{mn} b_m^{n-k} b_m^k \prod_{j=1}^{m} r(\beta_j) \\ &= (-1)^{mn} b_m^{n-k} \operatorname{Res}(g,r).\end{aligned}$$

□

Ejemplo 1.30. Los polinomios $3X^5+X+2$, $2X^3-1$ no tienen raíz común, porque

$$\begin{aligned}\operatorname{Res}(2+X+3X^5,-1+2X^3) &= (-1)^{15}2^{5-2}\operatorname{Res}(-1+2X^3,2+X+\tfrac{3}{2}X^2) \\ &= -8(-1)^6(\tfrac{3}{2})^{3-1}\operatorname{Res}(2+X+\tfrac{3}{2}X^2,\tfrac{7}{9}-\tfrac{16}{9}X) \\ &= -18(-1)^2(-\tfrac{16}{9})^{2-0}\operatorname{Res}(\tfrac{7}{9}-\tfrac{16}{9}X,\tfrac{1395}{512}) \\ &= -\tfrac{512}{9}\,(\tfrac{1395}{512})^1 = -155.\end{aligned}$$

Hay una fórmula para el resultante[17] en términos de los coeficientes de los polinomios:

$$\operatorname{Res}(f,g) = \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_0 & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_0 & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & b_m & b_{m-1} & \dots & b_0 \end{vmatrix} \tag{1.25}$$

En este determinante, las primeras m filas contienen los coeficientes de $f(X)$, las últimas n filas contienen los coeficientes de $g(X)$, y hay $m+n$ columnas; las entradas no indicadas son ceros. Por ejemplo,

$$\operatorname{Res}(3X^5+X+2,2X^3-1) = \begin{vmatrix} 3 & 0 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 1 & 2 \\ 2 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & -1 \end{vmatrix} = -155.$$

Para averiguar si un polinomio tenga una raíz doble, se toma el resultante de ese polinomio con su derivada.

[17] Para una demostración de la igualdad de esta fórmula con (1.22), véase, por ejemplo: A. G. Kurosh, *Curso de Álgebra Superior*, Mir, Moscú, 1977; art. 54.

Definición 1.31. Si $f(X) = a_0 + a_1X + \cdots + a_nX^n$ es un polinomio en $F[X]$, su **derivada** es el polinomio

$$f'(X) := a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}.$$

Para el caso $f(X) = a_0$, se define $f'(X) := 0$. Es fácil comprobar que la correspondencia $f(X) \mapsto f'(X)$ es una *derivación* del álgebra $F[X]$, es decir, una aplicación lineal que cumple la *regla de Leibniz*: la derivada de $f(X)\,g(X)$ es $f'(X)\,g(X) + f(X)\,g'(X)$.

El **discriminante** de $f(X)$ es el escalar

$$D(f(X)) := \frac{(-1)^{n(n-1)/2}}{a_n} \operatorname{Res}(f, f') \quad \in F. \tag{1.26}$$

Lema 1.32. *Sea $f(X) \in F[X]$, con $F \subseteq \mathbb{C}$. El discriminante $D(f(X))$ se anula si y sólo si $f(X)$ tiene una raíz doble.*

Demostración. Sea $f(X) = a_n(X - \alpha_1)\ldots(X - \alpha_n)$ en $\mathbb{C}[X]$. La fórmula (1.23) muestra la identidad $\operatorname{Res}(f, f') = a_n^{n-1} \prod_{i=1}^n f'(\alpha_i)$.

La regla de Leibniz muestra que

$$f'(X) = a_n \sum_{i=1}^{n} (X - \alpha_1)\ldots(X - \alpha_{i-1})(X - \alpha_{i+1})\ldots(X - \alpha_n),$$

así que

$$f'(\alpha_i) = a_n(\alpha_i - \alpha_1)\ldots(\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1})\ldots(\alpha_i - \alpha_n) = a_n \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Por tanto, $\operatorname{Res}(f, f') = a_n^{2n-1} \prod_{i \neq j} (\alpha_i - \alpha_j)$ vale 0 si y sólo si dos de los α_i son iguales. □

La demostración del lema pone en evidencia la fórmula

$$D(f(X)) = (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

El signo se puede suprimir al cambiar el término $(\alpha_r - \alpha_s)$ a $-(\alpha_s - \alpha_r)$ toda vez que $r > s$; de esta forma, se obtiene

$$D(f(X)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \tag{1.27}$$

Cualquier permutación de los α_i sólo puede cambiar el signo de estos productos. Por tanto, si $D(f(X))^2$ es un *polinomio simétrico* en las raíces de $f(X)$.

Ejemplo 1.33. El discriminante del polinomio $aX^2 + bX + c$ es

$$\begin{aligned} D(aX^2 + bX + c) &= -\frac{1}{a} \operatorname{Res}(aX^2 + bX + c, 2aX + b) \\ &= -\frac{1}{a}(2a)^2 \operatorname{Res}\left(2aX + b, c - \frac{b^2}{4a}\right) = -4a\left(c - \frac{b^2}{4a}\right) = b^2 - 4ac. \end{aligned}$$

De igual manera, el discriminante del polinomio X^3+pX+q es

$$\begin{aligned} D(X^3+pX+q) &= -\operatorname{Res}(X^3+pX+q, 3X^2+p) = -3^2\operatorname{Res}(3X^2+p, \tfrac{2}{3}pX+q) \\ &= -9\left(\frac{2p}{3}\right)^2 \operatorname{Res}\left(\frac{2p}{3}X+q, p+\frac{27q^2}{4p^2}\right) = -4p^2\left(p+\frac{27q^2}{4p^2}\right) \\ &= -4p^3-27q^2. \end{aligned}$$

1.4 Ejercicios sobre polinomios

Ejercicio 1.1. Resolver la ecuación $X^3-6X+9=0$ por el método de Cardano.

Ejercicio 1.2. Resolver la ecuación $X^3-15X^2-33X+847=0$ por el método de Cardano; las raíces son números enteros.

Ejercicio 1.3. Encontrar, por inspección, tres raíces enteros de la ecuación

$$X^3-7X+6=0.$$

En seguida, explicar en detalle cómo obtener estas raíces enteras por el método de Cardano.

Ejercicio 1.4. Resolver, por el método de Ferrari, la ecuación

$$X^4+X^2+4X-3=0.$$

⟦ Indicación: Tratar de encontrar una raíz de la ecuación cúbica auxiliar por inspección. ⟧

Ejercicio 1.5. Hallar el máximo común divisor $h(X)$ de los polinomios

$$f(X)=X^4+3X^3-X^2-4X-3, \qquad g(X)=3X^3+10X^2+2X-3.$$

En seguida, encontrar $a(X)$, $b(X)$ en $\mathbb{Q}[X]$ tales que $a(X)f(X)+b(X)g(X)=h(X)$.

Ejercicio 1.6. Sea F un cuerpo cualquiera. Demostrar el "teorema del residuo": *si $\alpha\in F$, el residuo de la división de un polinomio $f(X)\in F[X]$ por $(X-\alpha)$ es igual a $f(\alpha)$.*

(Una consecuencia inmediata es el "teorema del factor": *$f(X)$ tiene $(X-\alpha)$ como factor de primer grado si y sólo si $f(\alpha)=0$.*)

¿Siguen válidos estos "teoremas" si reemplazamos F por $\mathbb{Z}$?

Ejercicio 1.7. Dos polinomios $f(X)$ y $g(X)$ en $F[X]$ se llaman *asociados* si hay un escalar no cero $c\in F$ tal que $f(X)=c\,g(X)$. (Debe de ser evidente que esta es una relación de equivalencia entre polinomios.) Explicar cómo se podría modificar el algoritmo euclidiano para polinomios en $\mathbb{Z}[X]$, de manera que todos los cocientes y residuos intermedios $q_j(X)$ y $r_j(X)$ tengan coeficientes en $\mathbb{Z}$. Con esta modificación, hallar $\operatorname{mcd}(X^{12}-1,(X^2-X+1)^4)$ mediante un cálculo ejecutado en $\mathbb{Z}[X]$.

Ejercicio 1.8. Sean $f(X)$, $g(X)$ dos polinomios en $F[X]$ y sea $h(X) = \mathrm{mcd}(f(X), g(X))$. Mostrar, con todo detalle, que existen polinomios $a(X), b(X) \in F[X]$ tales que

$$a(X)\, f(X) + b(X)\, g(X) = h(X).$$

⟦ Indicación: Adaptar la demostración del resultado análogo en $\mathbb{Z}$, con base en la propiedad de divisibilidad con residuo. ⟧

Ejercicio 1.9. Sea F un cuerpo. Se sabe que $F[X]$ es un *anillo principal*, es decir, un anillo entero en donde cada ideal es generado por un sólo elemento. Si A es un anillo conmutativo y $c_1, \ldots, c_n \in A$, se denota por $(c_1, \ldots, c_n) := \{\, a_1c_1 + a_2c_2 + \cdots + a_nc_n : a_1, \ldots, a_n \in A \,\}$ el ideal que estos elementos generan. Mostrar que $(f(X), g(X)) = (h(X))$ como ideales de $F[X]$ si y sólo si $h(X)$ es un asociado del máximo común divisor $\mathrm{mcd}(f(X), g(X))$.

Ejercicio 1.10 (Lema de Euclides)**.** Dos polinomios $f(X)$ y $g(X)$ en $F[X]$ se llaman *relativamente primos* si $\mathrm{mcd}(f(X), g(X)) = 1$. En tal caso, mostrar que si $k(X) \in F[X]$ y si $f(X)$ divide $g(X)\, k(X)$, entonces $f(X)$ divide $k(X)$.

Ejercicio 1.11. El polinomio $2X^4 + 21X^3 - 6X^2 + 9X - 3$ es irreducible en $\mathbb{Z}[X]$. Verificar la irreducibilidad con el criterio de Eisenstein.

Ejercicio 1.12. El Lema de Gauss muestra que los factores de un polinomio primitivo en $\mathbb{Z}[X]$ quedan también en $\mathbb{Z}[X]$. Para el polinomio $X^4 + X + 1$, mostrar que las posibles factorizaciones

$$X^4 + X + 1 = (X \pm 1)(X^3 + ax^2 + bX \pm 1) = (X^2 + cX \pm 1)(x^2 + dX \pm 1)$$

no pueden realizarse con $a, b, c, d \in \mathbb{Z}$, así que $X^4 + X + 1$ es irreducible en $\mathbb{Z}[X]$.

Del mismo modo, comprobar que $X^5 + 5X^2 + 4X + 7$ es irreducible en $\mathbb{Z}[X]$.

Ejercicio 1.13. Se sabe que el polinomio $X^4 + X^3 + X^2 + X + 1$ es irreducible en $\mathbb{Q}[X]$, pero reducible en $\mathbb{R}[X]$. Encontrar su factorización en $\mathbb{R}[X]$.

⟦ Indicación: Recordar la fórmula de de Moivre: $(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos n\theta + i\,\mathrm{sen}\, n\theta$. ⟧

Ejercicio 1.14. Si $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ tiene una raíz racional $\alpha = r/s \in \mathbb{Q}$, donde $r, s \in \mathbb{Z}$ con $s \neq 0$ y $\mathrm{mcd}(r, s) = 1$, comprobar que $r \setminus a_0$ y $s \setminus a_n$.

Usar este criterio para factorizar $2X^3 - 8X^2 - 9X + 5$ en $\mathbb{Z}[X]$.

2 Extensiones de Cuerpos

2.1 Cuerpos y subcuerpos

Definición 2.1. Sean F, K dos cuerpos tales que $F \subseteq K$ como subanillo. Entonces se dice que F es un *subcuerpo* de K y que K es una **extensión** de F. Se escribe $\underline{K \mid F}$ para indicar que K es una extensión de F.[1]

En particular, K es un *espacio vectorial* sobre F. De hecho, si $a \in F$, entonces la correspondencia $b \mapsto ab$ entre elementos de K es una "multiplicación escalar" por ese elemento de F. La *dimensión* de K como espacio vectorial sobre F se denota $[K\colon F]$ y se llama el **grado** de la extensión.

Ejemplo 2.2. El grado de una extensión puede ser finita o infinita; si $[K\colon F]$ es finita, se dice que K es una *extensión finita* de F.

1. La extensión $\mathbb{C} \mid \mathbb{R}$ es finita, con $[\mathbb{C}\colon \mathbb{R}] = 2$. En efecto, como cada elemento de $\mathbb{C}$ es de la forma $a + bi$ con $a, b \in \mathbb{R}$, es evidente que $\{1, i\}$ es una base de $\mathbb{C}$ como espacio vectorial sobre $\mathbb{R}$.

2. Las extensiones $\mathbb{R} \mid \mathbb{Q}$ y $\mathbb{C} \mid \mathbb{Q}$ son infinitas. De hecho, como $\mathbb{Q}$ es enumerable pero $\mathbb{R}$ no lo es, cualquier base de $\mathbb{R}$ como espacio vectorial sobre $\mathbb{Q}$ es no enumerable: por lo tanto, no se puede exhibir una sola de esas "bases de Hamel", aunque se sabe que existen.[2]

3. Si F es un cuerpo cualquiera, sea $F(X)$ el cuerpo de funciones racionales en una variable. Está claro que $[F(X)\colon F] = \infty$.

4. Sea $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Este es obviamente un anillo entero; de hecho, es un cuerpo, porque si $a \neq 0$ ó $b \neq 0$, se ve que $(a + b\sqrt{2})^{-1} = (a - b\sqrt{2})/(a^2 - 2b^2)$ queda en $\mathbb{Q}(\sqrt{2})$. Es evidente, además, que $\{1, \sqrt{2}\}$ es una base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Por tanto, $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = 2$.

Proposición 2.3. *Si $F \subseteq K \subseteq L$ es una* torre *de dos extensiones, entonces*

$$[L\colon F] = [L\colon K]\,[K\colon F]. \tag{2.1}$$

Demostración. Sean $y_1, \ldots, y_s \in L$ linealmente independientes sobre K; y sean $x_1, \ldots, x_r \in K$ linealmente independientes sobre F. Entonces los elementos $\{x_i y_j : i = 1, \ldots, r;\ j = 1, \ldots, s\}$ de L son linealmente independientes sobre F. En efecto, si hay coeficientes $c_{ij} \in F$ con $\sum_{i,j} c_{ij} x_i y_j = 0$, entonces

$$\sum_{j=1}^{s} \left(\sum_{i=1}^{r} c_{ij} x_i \right) y_j = 0 \quad \text{en } L,$$

[1] En la mayoría de los textos, se usa "K/F" en vez de "$K \mid F$" para indicar una extensión; pero esta notación no es muy compatible con la designación de cocientes (de cuerpos, anillos o grupos). Aquí reservamos la raya vertical para extensiones.

[2] La existencia de una base en cualquier espacio vectorial fue señalada por Georg Hamel en 1905, como una de las primeras consecuencias de la "axioma de elección" formulado por Ernst Zermelo en 1904.

lo cual implica que $\sum_{i=1}^{r} c_{ij} x_i = 0$ en K para cada $j = 1, \ldots, s$; lo cual a su vez implica que $c_{ij} = 0$ en F para cada i, j. Se concluye que $[L\colon F] \geq rs$. En consecuencia, se ve que $[L\colon F] \geq [L\colon K]\,[K\colon F]$.

Si $[L\colon K] = \infty$ ó $[K\colon F] = \infty$, entonces $[L\colon F] = \infty$ y la relación (2.1) vale como igualdad entre dos infinitudes.

Si $L \,|\, K$ y $K \,|\, F$ son extensiones finitas, entonces puede tomarse $r = [K\colon F]$ y $s = [L\colon K]$, en cuyo caso $\{x_1, \ldots, x_r\}$ es una base para K sobre F y $\{y_1, \ldots, y_s\}$ es una base para L sobre K. Si $z \in L$, entonces $z = \sum_{j=1}^{s} b_j y_j$ para algunos $b_j \in K$ y además $b_j = \sum_{i=1}^{r} a_{ij} x_i$ para algunos $a_{ij} \in F$. Por tanto, $z = \sum_{i,j} a_{ij} x_i y_j$. La conclusión es que $\{x_i y_j : i = 1, \ldots, r;\ j = 1, \ldots, s\}$ genera L como espacio vectorial sobre F; por ende, este conjunto es una base de L sobre F. Luego $[L\colon F] = rs = [L\colon K]\,[K\colon F]$. □

Notación. Sea $K \,|\, F$ una extensión de cuerpos y sean $\alpha_1, \ldots, \alpha_n \in K$. El subanillo de K generado por $F \cup \{\alpha_1, \ldots, \alpha_n\}$ se llama $\underline{F[\alpha_1, \ldots, \alpha_n]}$.[3] Este subanillo es la imagen del homomorfismo $\varphi_{\alpha_1,\ldots,\alpha_n}\colon F[X_1, \ldots, X_n] \to K$ que extiende la inclusión $F \hookrightarrow K$ y obedece $\varphi_{\alpha_1,\ldots,\alpha_n}(X_j) = \alpha_j$ para $j = 1, \ldots, n$. Informalmente, $F[\alpha_1, \ldots, \alpha_n]$ consta de "polinomios en $\alpha_1, \ldots, \alpha_n$ con coeficientes en F".

El *subcuerpo* de K generado por $F \cup \{\alpha_1, \ldots, \alpha_n\}$ se denota por $\underline{F(\alpha_1, \ldots, \alpha_n)}$. Es evidente que $F(\alpha_1, \ldots, \alpha_n) = \{\, a/b : a, b \in F[\alpha_1, \ldots, \alpha_n],\ b \neq 0 \,\}$.

Si $n = 1$, se dice que

$$F(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} : f(X), g(X) \in F[X],\ g(\alpha) \neq 0 \right\} \tag{2.2}$$

es una *extensión simple* de F.

Definición 2.4. Sea $K \,|\, F$ una extensión de cuerpos y sea $\alpha \in K$. Se dice que α es un **elemento trascendente** sobre F si $f(\alpha) \neq 0$ para todo $f(X) \in F[X]$. En este caso, el homomorfismo $\varphi_\alpha\colon F[X] \to F[\alpha]$, tal que $\varphi_\alpha(a) = a$ para $a \in F$ y $\varphi_\alpha(X) = \alpha$, se extiende a un homomorfismo *inyectivo* $\psi_\alpha\colon F(X) \to F(\alpha)$ al definir $\psi_\alpha(f(X)/g(X)) := f(\alpha)/g(\alpha)$.

Definición 2.5. Sea $K \,|\, F$ una extensión de cuerpos y sea $\alpha \in K$. Se dice que α es un **elemento algebraico** sobre F si existe un polinomio no constante $f(X) \in F[X]$ tal que $f(\alpha) = 0$. En este caso,

$$\ker \varphi_\alpha = \{\, f(X) \in F[X] : f(\alpha) = 0 \,\}$$

es un ideal de $F[X]$. Como todo ideal de $F[X]$ es principal, hay un polinomio mónico $p(X)$ tal que $\ker \varphi_\alpha = (p(X))$. Este polinomio $p(X)$ es *irreducible*: si $p(X) = g(X)\,h(X)$ fuera una factorización no trivial en dos factores mónicos, entonces sería $g(\alpha)\,h(\alpha) = p(\alpha) = 0$ así que $g(\alpha) = 0$ o bien $h(\alpha) = 0$; pero entonces sería $g(X) \in \ker \varphi_\alpha$ o bien $h(X) \in \ker \varphi_\alpha$, aunque ninguna de estos dos polinomios es divisible por $p(X)$. Este polinomio mónico irreducible $p(X)$ se llama el **polinomio mínimo**[4] del elemento algebraico α.

[3] Este es, por definición, la intersección de todos los subanillos de K que incluyen $F \cup \{\alpha_1, \ldots, \alpha_n\}$: su existencia es automática.

[4] La *unicidad* de $p(X)$ se verifica fácilmente.

Lema 2.6. *Sea $K \mid F$ una extensión de cuerpos y sea $\alpha \in K$ algebraico sobre F con polinomio mínimo $p(X)$. Sea $\beta \in K$ cualquier otro raíz de $p(X)$. Entonces β es algebraico sobre F y su polinomio mínimo es $p(X)$ también.*

Demostración. Como $p(\beta) = 0$ por hipótesis, β es algebraico sobre F. Sea $q(X)$ el polinomio mínimo de β, el cual es mónico e irreducible. La igualdad $p(\beta) = 0$ implica que $q(X) \setminus p(X)$; pero $p(X)$ es irreducible, así que $q(X) = c\,p(X)$ para algún $c \in F$, $c \neq 0$. Ahora, tanto $p(X)$ como $q(X)$ es mónico, por ende $c = 1$ y $q(X) = p(X)$. □

Lema 2.7. *Si $K \mid F$ es una extensión de cuerpos y si $\alpha \in K$ es un elemento algebraico sobre F, entonces $F(\alpha) = F[\alpha]$.*

Demostración. Sea $p(X)$ el polinomio mínimo de α en $F[X]$. Si $h(X) \in F[X]$ es un polinomio con $h(\alpha) \neq 0$, entonces $p(X)$ no divide $h(X)$. Como $p(X)$ es irreducible, se concluye que $\operatorname{mcd}(p(X), h(X)) = 1$. El resultado del Corolario 1.10 es válido tanto en $\mathbb{Z}$ como en el anillo de polinomios $F[X]$ (se lo demuestra por el mismo algoritmo euclidiano en ambos casos) y de ahí pueden encontrarse dos polinomios $a(X)$, $b(X)$ tales que

$$a(X)\,p(X) + b(X)\,h(X) = 1. \tag{2.3}$$

Al evaluar estos polinomios[5] en α, se obtiene $b(\alpha)\,h(\alpha) = 1$ en $F[X]$. Luego se puede escribir $g(\alpha)/h(\alpha) = g(\alpha)\,b(\alpha) \in F[\alpha]$ para todo $g(\alpha) \in F[\alpha]$. □

Lema 2.8. *Si $\alpha \in K$ es un elemento algebraico sobre el subcuerpo F de K, entonces la extensión $F(\alpha) \mid F$ es finita.*

Demostración. Sea n el grado del polinomio mínimo $p(X)$ de α. Si $f(X) \in F[X]$, hay polinomios $q(X)$, $r(X)$ en $F[X]$ tales que $f(X) = q(X)\,p(X) + r(X)$, con $\operatorname{gr} r(X) < n$ o bien $r(X) = 0$. Al evaluar estos polinomios en α, se obtiene

$$f(\alpha) = q(\alpha)\,p(\alpha) + r(\alpha) = r(\alpha),$$

y en consecuencia,

$$F(\alpha) = F[\alpha] = \{0\} \cup \{\, r(\alpha) \in K : \operatorname{gr} r(X) < n \,\}.$$

Entonces, $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ generan $F(\alpha)$ como espacio vectorial sobre F. Estos elementos de K también son linealmente independientes sobre F, porque si no, una combinación lineal de entre ellos produciría un polinomio $h(X)$ de grado $< n$ tal que $h(\alpha) = 0$, contrario a la minimalidad de $p(X)$. Luego $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base de $F(\alpha)$ sobre F, de donde $[F(\alpha) : F] = n$. □

En vista de este resultado, se dice que *un elemento algebraico α es de grado n* sobre F si n es el grado de su polinomio mínimo $p(X)$, que coincide con el grado $[F(\alpha) : F]$ de la extensión $F(\alpha) \mid F$.

[5] Dicha "evaluación" consiste en la aplicación del homomorfismo $\varphi_\alpha : F[X] \to F[\alpha]$.

Definición 2.9. Una extensión de cuerpos $K \mid F$ es una **extensión algebraica** si cada elemento de K es algebraico sobre F.

Ejemplo 2.10. La extensión $\mathbb{C} \mid \mathbb{R}$ es algebraica, porque cada elemento $a+bi \in \mathbb{C}$ con $a, b \in \mathbb{R}$ es una raíz del polinomio $X^2 - 2aX + a^2 + b^2$. Este es su polinomio mínimo si $b \neq 0$.

Lema 2.11. *Cada extensión finita $K \mid F$ es una extensión algebraica.*

Demostración. Sea $n = [K\colon F]$. Si $\beta \in K \setminus F$, entonces el conjunto $\{1, \beta, \beta^2, \ldots, \beta^n\}$ no es linealmente independiente sobre F: si sus elementos son distintos, hay $(n+1)$ de ellos; y si no son distintos, hay una relación lineal $\beta^k - 1 = 0$ para algún $k \in \{2, \ldots, n\}$. Luego, hay un polinomio no constante $f(X) \in F[X]$ con $\operatorname{gr} f(X) = n$ tal que $f(\beta) = 0$. Esto dice que β es algebraica sobre F, de grado $\leq n$. □

Ejemplo 2.12. No toda extensión algebraica es una extensión finita. Por el "teorema fundamental del álgebra", cada polinomio en $\mathbb{Q}[X]$ tiene todos sus raíces en $\mathbb{C}$. Defínase $\overline{\mathbb{Q}}$ como la unión de todas las raíces en $\mathbb{C}$ de todos los polinomios en $\mathbb{Q}[X]$. Resulta que $\overline{\mathbb{Q}}$ es un cuerpo (¿por qué?) y que hay elementos de $\mathbb{C}$ que no pertenecen a $\mathbb{Q}$, los llamados *números trascendentes*.[6] Por construcción, $\overline{\mathbb{Q}}$ es una extensión algebraica de $\mathbb{Q}$. Pero se sabe (véase el Ejemplo 1.19) que hay polinomios irreducibles en $\mathbb{Q}[X]$ de cualquier grado primo p, cuyas raíces son números algebraicos de grado p sobre $\mathbb{Q}$. Por tanto, no puede haber cota finita para el grado $[\overline{\mathbb{Q}}\colon \mathbb{Q}]$.

Lema 2.13. *Si $K \mid F$ es una extensión de cuerpos y si $\alpha, \beta \in K$ son algebraicos sobre F, entonces $\alpha \pm \beta$, $\alpha\beta$ y α/β (si $\beta \neq 0$) son algebraicos sobre F.*

Demostración. Sea $E := F(\alpha)$, de modo que $F(\alpha, \beta) = E(\beta)$. Sean $p(X), q(X) \in F[X]$ los respectivos polinomios mínimos de α y β sobre F. Escríbase $n = [F(\alpha)\colon F] = \operatorname{gr} p(X)$, $m = [F(\beta)\colon F] = \operatorname{gr} q(X)$. Ahora $q(X) \in E[X]$ porque $F \subseteq E$, con $q(\beta) = 0$ en K: eso dice que β es algebraico sobre E y que $[E(\beta)\colon E] \leq m$. (Obsérvese que $q(X)$, aunque irreducible en $F[X]$, podría ser reducible en $E[X]$, en cuyo caso el polinomio mínimo de β sobre E sería un factor propio de $q(X)$, de grado $< m$.) Entonces

$$[F(\alpha, \beta)\colon F] = [F(\alpha, \beta)\colon F(\alpha)]\,[F(\alpha)\colon F] = [E(\beta)\colon E]\,[F(\alpha)\colon F] \leq mn.$$

Por lo tanto $F(\alpha, \beta)$ es una extensión finita de F y como tal es una extensión algebraica, por el Lema 2.11. En particular, $\alpha \pm \beta$, $\alpha\beta$ y α/β (si $\beta \neq 0$) son elementos de $F(\alpha, \beta)$ y luego son algebraicos sobre F. □

Llamemos *cuerpo intermedio* de una extensión $K \mid F$ un cuerpo E tal que $F \subseteq E \subseteq K$.

Corolario 2.14. *Si $K \mid F$ es una extensión de cuerpos cualquiera, los elementos de K que son algebraicos sobre F forman un cuerpo intermedio de esta extensión.* ⊟

[6] Los números trascendentes existen, porque $\overline{\mathbb{Q}}$ es enumerable mientras $\mathbb{C}$ no lo es. Es menos fácil *exhibir* un número trascendente, aunque ya se sabe que π, e son trascendentes. Liouville, en 1844, produjo una familia (no enumerable) de números trascendentes, entre ellos $\sum_{k=1}^{\infty} 10^{-k!} = 0.11000100000000000000000100\ldots$. Para su construcción, véase el Capítulo 2 de: John C. Oxtoby, *Measure and Category*, Springer, New York, 1971.

Ejemplo 2.15. Considérese la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})\,|\,\mathbb{Q}$. Tiene un cuerpo intermedio $\mathbb{Q}(\sqrt{2})$, que cumple $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = 2$. De hecho, el polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es el polinomio cuadrático X^2-2.

Es fácil ver que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Si hubiera $p,q \in \mathbb{Q}$ con $\sqrt{3} = p+q\sqrt{2}$, entonces sería $3 = p^2+2q^2+2pq\sqrt{2}$: como $\{1,\sqrt{2}\}$ es linealmente independiente sobre $\mathbb{Q}$, se tendría $p^2+2q^2 = 3$ y $2pq = 0$ en $\mathbb{Q}$; de ahí $p = 0$, $2q^2 = 3$ o bien $q = 0$, $p^2 = 3$, pero estas ecuaciones no tienen soluciones racionales.

Entonces $\mathbb{Q}(\sqrt{2},\sqrt{3})\,|\,\mathbb{Q}(\sqrt{2})$ es una extensión de grado > 1 y el polinomio X^2-3 es irreducible en $\mathbb{Q}(\sqrt{2})[X]$. Este es, entonces, el polinomio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$. Por tanto, es $[\mathbb{Q}(\sqrt{2},\sqrt{3})\colon \mathbb{Q}(\sqrt{2})] = 2$. Se concluye que $[\mathbb{Q}(\sqrt{2},\sqrt{3})\colon \mathbb{Q}] = 4$.

Ahora $\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$. Además, $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ es una base de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ como espacio vectorial sobre $\mathbb{Q}$. Si no fuera así, habría $a,b,c,d \in \mathbb{Q}$, no todos cero, tales que

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = 0.$$

Después de multiplicar por un denominador común y dividir por algún entero, se puede suponer que $a,b,c,d \in \mathbb{Z}$ y que no tienen factor común. Ahora $a+b\sqrt{2} = -c\sqrt{3}-d\sqrt{6}$, así que $a^2+2b^2+2ab\sqrt{2} = 3c^2+6d^2+6cd\sqrt{2}$ y por ende,

$$a^2+2b^2 = 3(c^2+2d^2), \qquad ab = 3cd.$$

Al tomar residuos módulo 3, se obtiene $a^2+2b^2 \equiv 0 \bmod 3$, $ab \equiv 0 \bmod 3$. Esto sólo es posible si $a \equiv b \equiv 0 \bmod 3$, de modo que $a = 3m$, $b = 3n$ con $m,n \in \mathbb{Z}$. Pero esto implicaría que $c^2+2d^2 = 3(m^2+2n^2)$ y $cd = 3mn$. El mismo proceso lleva a $c \equiv d \equiv 0 \bmod 3$, contrario a la suposición de que $\mathrm{mcd}(a,b,c,d) = 1$.

Sea $\alpha := \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$. Entonces $\alpha^2 = 5+2\sqrt{6}$ y luego no hay $p,q,r \in \mathbb{Q}$, no todos cero, tales que $p\alpha^2+q\alpha+r = 0$. El polinomio mínimo de α sobre $\mathbb{Q}$ tiene grado mayor que 2, así que ese grado debe ser 4. Ahora $\alpha^4 = (5+2\sqrt{6})^2 = 49+20\sqrt{6} = 10\alpha^2-1$, se ve que ese polinomio mínimo es $p(X) := X^4-10X^2+1$.

El criterio de Eisenstein no es útil para verificar que X^4-10X^2+1 es irreducible sobre $\mathbb{Q}$. Pero podemos ensayar una factorización directa. La fórmula cuadrática muestra que

$$X^4-10X^2+1 = 0 \implies X^2 = 5\pm 2\sqrt{6} = (\sqrt{2}\pm\sqrt{3})^2,$$

de donde se obtiene la factorización completa en $\mathbb{Q}(\sqrt{2},\sqrt{3})$:

$$X^4-10X^2+1 = (X-\sqrt{2}-\sqrt{3})(X-\sqrt{2}+\sqrt{3})(X+\sqrt{2}-\sqrt{3})(X+\sqrt{2}+\sqrt{3}).$$

Se concluye que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

2.2 Cuerpos de escisión

Lema 2.16. *Sea $p(X)$ un polinomio irreducible en $F[X]$, y sea $J := (p(X))$ el ideal principal de $F[X]$ generado por $p(X)$. Entonces el anillo cociente $F[X]/J = \{\, f(X)+J : f(X) \in F[X] \,\}$ es un cuerpo.*

Demostración. Los elementos del anillo cociente son 'coclases' de la forma $f(X)+J$. Por división, como en la demostración del Lema 2.8, se puede escribir $f(X) = q(X)\,p(X)+r(X)$, con $\operatorname{gr} r(X) < \operatorname{gr} p(X)$ o bien $r(X) = 0$. Entonces $f(X)+J = r(X)+J$: cada coclase se representa por el residuo bajo división por $p(X)$.

Si $r(X) \neq 0$, entonces $\operatorname{mcd}(p(X), r(X)) = 1$, así que hay polinomios $a(X), b(X) \in F[X]$ tales que

$$a(X)\,p(X)+b(X)\,r(X) = 1.$$

Es claro que $b(X) \neq 0$, porque $q(X)\,p(X) = 1$ es imposible por conteo de grados. Puede suponerse que $\operatorname{gr} b(X) < \operatorname{gr} p(X)$, porque de lo contrario habría $q_1(X)$, $b_1(X)$ con $\operatorname{gr} b_1(X) < \operatorname{gr} p(X)$ tales que $b(X) = q_1(X)\,p(X)+b_1(X)$; y entonces

$$(a(X)+q_1(X)\,r(X))\,p(X)+b_1(X)\,r(X) = 1.$$

Pasando al anillo cociente, se obtiene

$$(b(X)+J)(r(X)+J) = 1-a(X)\,p(X)+J = 1+J.$$

Ahora $1+J$ es la identidad en el anillo conmutativo $F[X]/J$; el cero de este anillo es la coclase J. Se concluye que cada coclase no nula $r(X)+J$ tiene un inverso multiplicativo $b(X)+J$; en otras palabras, $F[X]/J$ es un cuerpo. □

Teorema 2.17 (Kronecker)**.** *Sea F un cuerpo cualquiera y sea $f(X) \in F[X]$ un polinomio no constante. Entonces hay una extensión $E \mid F$ tal que $f(X)$ posee una raíz en E.*

Demostración. Sea $p(X)$ un factor irreducible de $f(X)$, y sea $J = (p(X))$ el ideal principal de $F[X]$ generado por $p(X)$. Por el lema anterior, sabemos que $L := F[X]/J$ es un cuerpo.

La aplicación $\sigma\colon F \to L$ dado por $\sigma(a) := a+J$ es un homomorfismo inyectivo, porque si $a \neq 0$ en F, entonces $a \notin J$ así que $a+J \neq J$ en L. Entonces el (único) homomorfismo $\eta\colon F[X] \to L$ que extiende σ y cumple $\eta(X) := X+J$ es la *aplicación cociente*, definido como $\eta\colon F[X] \to F[X]/J : h(X) \mapsto h(X)+J$.

Ahora, si $p(X) = a_0+a_1X+\cdots+a_nX^n$, entonces

$$p(X+J) = a_0+a_1X+\cdots+a_nX^n+J = p(X)+J = J,$$

así que $X+J$ es una raíz de $p(X)$ en $L = F[X]/J$.

Por la demostración del Lema 2.16, se sabe que $L = \{\, r(X)+J : r(X) = 0 \text{ ó } \operatorname{gr} r(X) < n \,\}$. Sea S un conjunto de la misma cardinalidad que $\{\, r(X) : 1 \leq \operatorname{gr} r(X) < n \,\}$ y defínase $E := F \uplus S$ (unión disjunta); entonces la inyección $\sigma\colon F \hookrightarrow L$ puede extenderse a una biyección $\sigma\colon E \to L$. La estructura de cuerpo de L se transfiere a E mediante esta biyección:

$$\alpha+\beta := \sigma^{-1}(\sigma(\alpha)+\sigma(\beta)), \qquad \alpha\beta := \sigma^{-1}(\sigma(\alpha)\,\sigma(\beta)).$$

Entonces $E \mid F$ es una extensión (finita) de cuerpos. Sea $\xi := \sigma^{-1}(X+J) \in E$. Entonces $\sigma(p(\xi)) = p(X+J) = J$ en L implica que $p(\xi) = 0$ en E. Luego $\xi \in E$ es una raíz de $p(X)$ y también de $f(X)$. □

Corolario 2.18. *Sea F un cuerpo cualquiera y sea $f(X) \in F[X]$ un polinomio de grado $n \geq 1$. Entonces hay una extensión $K \mid F$ tal que $f(X)$ posee n raíces (no necesariamente distintas) en K.*

Demostración. Por inducción sobre $n = \operatorname{gr} f(X)$. No hace falta extender F si $n = 1$.

Por el teorema anterior, hay una extensión $E \mid F$ y un elemento $\alpha_1 \in E$ tal que $f(\alpha_1) = 0$ en E. Entonces $f(X) = (X - \alpha_1) f_1(X)$ con $f_1(X) \in E[X]$, de grado $(n-1)$. Por la hipótesis inductiva, hay una extensión $K \mid E$ y hay elementos $\alpha_2, \ldots, \alpha_n$ tales que $f(\alpha_j) = 0$ para $j = 2, \ldots, n$. Luego $f_1(X) = a_n(X - \alpha_2) \ldots (X - \alpha_n)$ para algún $a_n \neq 0$ en E. Por tanto, K extiende F, es $a_n \in F$ y vale

$$f(X) = a_n(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n).$$

Es decir, $f(X)$ posee una factorización completa en $K[X]$. □

Definición 2.19. Sea F un cuerpo cualquiera y sea $f(X) \in F[X]$ un polinomio de grado $n \geq 1$. Un cuerpo K se llama un **cuerpo de escisión** para $f(X)$ sobre F si:

(a) K es una extensión de F y $f(X)$ *escinde* en $K[X]$, es decir, hay n raíces $\alpha_1, \ldots, \alpha_n \in K$ tales que

$$f(X) = a_n(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n) \quad \text{en } K[X]. \tag{2.4}$$

(b) $K = F(\alpha_1, \ldots, \alpha_n)$; esto es, las raíces generan la extensión $K \mid F$.

Definición 2.20. Un homomorfismo[7] biyectivo $\varphi\colon F \to F'$ entre dos cuerpos se llama un **isomorfismo** entre F y F'; si hay al menos un isomorfismo entre ellos, se escribe $F \simeq F'$ y se dice que F y F' son *isomorfos*. El homomorfismo inverso $\varphi^{-1}\colon F' \to F$ establece que $F' \simeq F$; y si hay un isomorfismo $\psi\colon F' \to F''$, entonces $\psi \circ \varphi\colon F \to F''$ es también un isomorfismo. De esta forma, se ve que el isomorfismo entre cuerpos es una relación de equivalencia.

Ejemplo 2.21. Si F es un cuerpo cualquiera y si $p(X) \in F[X]$ es irreducible, el Teorema 2.17 muestra que hay una extensión $E \mid F$ y un elemento $\alpha \in E$ tales que $p(\alpha) = 0$ en E. Si $J = (p(X))$, el homomorfismo $\varphi_\alpha\colon F[X] \to F(\alpha)$ que deja fijo F y cumple $\varphi_\alpha(X) = \alpha$ da lugar a un homomorfismo $\psi_\alpha\colon F[X]/J \to F(\alpha)$ por

$$\psi_\alpha(h(X) + J) := \varphi_\alpha(h(X)) = h(\alpha).$$

Claramente, ψ_α es sobreyectivo; es también inyectivo porque

$$\begin{aligned} h(X) + J \in \ker \psi_\alpha &\iff h(\alpha) = 0 \text{ en } E \iff p(X) \setminus h(X) \text{ en } F[X] \\ &\iff h(X) \in (p(X)) = J \iff h(X) + J = J. \end{aligned}$$

Por lo tanto, $F(\alpha) \simeq F[X]/J$.

[7] Hay que recordar el convenio de que, entre dos anillos con identidad, cada homomorfismo $\varphi\colon A \to B$ debe cumplir $\varphi(1_A) = 1_B$.

Proposición 2.22. *Si $\varphi\colon F \to F'$ es un isomorfismo y si $p(X) = a_0 + a_1X + \cdots + a_nX^n$ es irreducible en $F[X]$, escríbase $p^\varphi(X) := \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n \in F'[X]$. Sean $K \,|\, F$ y $K' \,|\, F'$ dos extensiones que contienen $\alpha \in K$ con $p(\alpha) = 0$ y $\beta \in K'$ con $p^\varphi(\beta) = 0$. Entonces hay un (único) isomorfismo $\psi\colon F(\alpha) \to F'(\beta)$ que extiende φ tal que $\psi(\alpha) = \beta$.*

Demostración. El polinomio $p^\varphi(X)$ es irreducible en $F'[X]$, porque cualquier factorización en $F'[X]$ es de la forma $p^\varphi(X) = h^\varphi(X)\,k^\varphi(X)$ para una factorización correspondiente $p(X) = h(X)\,k(X)$ en $F[X]$.

Del ejemplo anterior, sabemos que hay dos isomorfismos $\psi_\alpha\colon F[X]/(p(X)) \to F(\alpha)$ y $\psi'_\beta\colon F'[X]/(p^\varphi(X)) \to F'(\beta)$ tales que $\psi_\alpha\colon X + (p(X)) \mapsto \alpha$ y $\psi'_\beta\colon X + (p^\varphi(X)) \mapsto \beta$.

Sean $\eta\colon F[X] \to F[X]/(p(X))$ y $\eta'\colon F'[X] \to F'[X]/(p^\varphi(X))$ los mapas cocientes.

La aplicación $h(X) \mapsto h^\varphi(X)$ es un homomorfismo biyectivo $\hat\varphi\colon F[X] \to F'[X]$ (entre anillos). La composición $\eta' \circ \hat\varphi\colon F[X] \to F'[X]/(p^\varphi(X))$ es un homomorfismo cuyo núcleo es $\ker(\eta' \circ \hat\varphi) = \{\, h(X) : p^\varphi(X) \setminus h^\varphi(X) \,\} = \{\, h(X) : p(X) \setminus h(X) \,\}$. Por tanto, hay un isomorfismo $\tilde\varphi\colon F[X]/(p(X)) \to F'[X]/(p^\varphi(X))$ que hace conmutar al siguiente diagrama:

$$\begin{array}{ccc} F[X] & \xrightarrow{\quad\hat\varphi\quad} & F'[X] \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta'} \\ F[X]/(p(X)) & \xrightarrow{\quad\tilde\varphi\quad} & F'[X]/(p^\varphi(X)) \end{array}$$

y en particular, $\tilde\varphi\colon X + (p(X)) \mapsto X + (p^\varphi(X))$. El isomorfismo deseado es entonces la aplicación que hace conmutar al diagrama

$$\begin{array}{ccc} F[X]/(p(X)) & \xrightarrow{\quad\tilde\varphi\quad} & F'[X]/(p^\varphi(X)) \\ {\scriptstyle\psi_\alpha}\downarrow & & \downarrow{\scriptstyle\psi'_\beta} \\ F(\alpha) & \xrightarrow{\quad\psi\quad} & F'(\beta) \end{array}$$

que es evidentemente $\psi := \psi'_\beta \circ \tilde\varphi \circ \psi_\alpha^{-1}$. Se ve que $\psi(a) = \varphi(a)$ si $a \in F$ y $\psi(\alpha) = \beta$. □

Corolario 2.23. *Si $K \,|\, F$ es una extensión de cuerpos, si $p(X) \in F[X]$ es irreducible y $\alpha, \beta \in K$ son dos raíces de $p(X)$, entonces la correspondencia $h(\alpha) \mapsto h(\beta)$ define un isomorfismo entre $F(\alpha)$ y $F(\beta)$ que deja fijo el cuerpo F.* ⊟

Proposición 2.24. *Si $\varphi\colon F \to F'$ es un isomorfismo de cuerpos, si K es un cuerpo de escisión para un polinomio $f(X) \in F[X]$ y si K' es un cuerpo de escisión para $f^\varphi(X) \in F'[X]$, entonces hay un isomorfismo $\psi\colon K \to K'$ que extiende φ.*

Demostración. Por inducción sobre el grado $[K\colon F]$. El caso $[K\colon F] = 1$ ocurre cuando $f(X)$ ya escinde en F, es decir, la factorización (2.4) puede realizarse con $\alpha_1, \ldots, \alpha_n \in F$. Ahora $K' = F(\beta_1, \ldots, \beta_n)$ donde $\beta_1, \ldots, \beta_n \in K$ son raíces de $f^\varphi(X)$ en $K'[X]$: por tanto, $\{\beta_1, \ldots, \beta_n\} \supseteq \{\varphi(\alpha_1, \ldots, \varphi(\alpha_n)\}$ y por conteo estos dos juegos de raíces son iguales. Luego $K' = F'(\beta_1, \ldots, \beta_n) = F'$, es $[K'\colon F'] = 1$ y se puede tomar $\psi := \varphi$.

Supóngase ahora que la Proposición vale para extensiones de grado menor que $[K\colon F]$. Sea $p(X)$ un factor irreducible de $f(X)$; entonces $p^\varphi(X)$ es un factor irreducible de $f^\varphi(X)$ en $F'[X]$. Sea $\alpha_1 \in K \setminus F$, $\beta_1 \in K' \setminus F'$ dos elementos tales que $p(\alpha_1) = 0$ en K y $p^\varphi(\beta_1) = 0$ en K'. Por la Proposición 2.22 hay un isomorfismo $\psi_1\colon F(\alpha_1) \to F'(\beta_1)$ que extiende φ, tal que $\psi_1(\alpha_1) = \beta_1$.

Ahora $K = F(\alpha_1,\ldots,\alpha_n) = \underline{F(\alpha_1)}(\alpha_2,\ldots,\alpha_n)$ y de igual manera $K' = F(\beta_1,\ldots,\beta_n) = \underline{F(\beta_1)}(\beta_2,\ldots,\beta_n)$, así que K es un cuerpo de escisión para $f(X)$ en $F(\alpha_1)[X]$ y K' es un cuerpo de escisión para $f^\varphi(X)$ en $F(\beta_1)[X]$. Como

$$[K\colon F(\alpha_1)] = \frac{[K\colon F]}{[F(\alpha_1)\colon F]} < [K\colon F],$$

la hipótesis inductiva produce un isomorfismo $\psi\colon K \to K'$ que extiende ψ_1. □

Corolario 2.25. *Si K y K' son dos cuerpos de escisión para un polinomio $f(X) \in F[X]$, entonces hay un isomorfismo $\psi\colon K \to K'$ que deja fijo F.*

Obsérvese que en la Proposición y el Corolario anteriores, el isomorfismo ψ no es único: su construcción depende de la elección de una biyección entre las raíces de los polinomios que se escinden; en el caso del Corolario, éste es una permutación de las raíces del polinomio $f(X)$. Para contar las posibilidades, hay que tomar en cuenta la posibilidad de raíces múltiples.

Definición 2.26. Sea $f(X) \in F[X]$ un polinomio que posee una factorización completa (2.4) en $K[X]$, para alguna extensión $K \,|\, F$. La **multiplicidad** de una raíz $\beta \in \{\alpha_1,\ldots,\alpha_n\}$ es el número de factores $(X-\alpha_j)$ en (2.4) que coinciden con $(X-\beta)$.

En otros términos: sean $\beta_1,\ldots,\beta_r$ los elementos *distintos* de entre $\alpha_1,\ldots,\alpha_n$, así que

$$(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n) = (X-\beta_1)^{k_1}(X-\beta_2)^{k_2}\ldots(X-\beta_r)^{k_r}$$

con $k_1+\cdots+k_r = n$; en donde k_j es la multiplicidad de la raíz β_j.

Definición 2.27. Sea F un subcuerpo[8] de $\mathbb{C}$ y sea $\alpha \in \mathbb{C}$ algebraico sobre F. Sea $p(X) \in F[X]$ el polinomio mínimo de α sobre F. Cualquier raíz β de $p(X)$ se llama un **conjugado** de α sobre F.

Ejemplo 2.28. (a) Si $a+bi \in bC$ con $a,b \in \mathbb{R}$, $b \neq 0$, entonces $a-bi$ es un conjugado de $a+bi$ sobre $\mathbb{R}$. En efecto, estos dos números complejos son las dos raíces del polinomio $X^2 - 2aX + a^2 + b^2$, que es irreducible en $\mathbb{R}[X]$. De este modo, el "conjugado complejo" es un conjugado en el sentido de la Definición 2.27, asociado con la extensión $\mathbb{C} \,|\, \mathbb{R}$.

(b) Si $\omega := \frac{1}{2}(-1+i\sqrt{3}) = e^{2\pi i/3}$, una raíz cúbica de 1, entonces los conjugados de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ son $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$, pues éstas son las tres raíces del polinomio irreducible X^3-2.

(c) En vista del Ejemplo 2.15, los conjugados de $\sqrt{2}+\sqrt{3}$ sobre $\mathbb{Q}$ son los cuatro números $\pm\sqrt{2} \pm \sqrt{3}$, por ser éstos las raíces de $X^4 - 10X^2 + 1$.

[8] La inclusión $F \subseteq \mathbb{C}$ sólo es necesario para garantizar la existencia de α. Eventualmente se podrá reemplazar $\mathbb{C}$ por una clausura algebraica de F.

Definición 2.29. Una extensión $K \mid F$ se llama una **extensión normal** si es algebraica y si todo polinomio irreducible $p(X) \in F[X]$ que posee *una* raíz en K tiene *todas* sus raíces en K.

Ejemplo 2.30. La extensión $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ *no es normal*, porque $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ pero el polinomio mínimo $X^3 - 2$ de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ posee dos raíces no reales. De hecho,

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \omega^2\sqrt[3]{2}) = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$$

donde el lado derecho es la factorización de $X^3 - 2$ en el cuerpo $\mathbb{Q}(\sqrt[3]{2})$. En este cuerpo, el polinomio $X^3 - 2$ tiene una raíz pero no escinde en factores de primer grado.

Obsérvese que $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ es una *base* de $\mathbb{Q}(\sqrt[3]{2})$ como espacio vectorial sobre $\mathbb{Q}$. Sólo es necesario comprobar su independencia lineal. Ahora, si hubiera $a, b, c \in \mathbb{Q}$, no todos cero, tales que $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$, entonces $g(X) := a + bX + cX^2$ sería un polinomio no cero en $\mathbb{Q}[X]$ con $g(\sqrt[3]{2}) = 0$; como tal, sería un factor propio de $X^3 - 2$, lo cual es imposible.

Lema 2.31. *Sea K un cuerpo de escisión de $f[X] \in F[X]$ y sea $L \mid K$ una extensión. Si $\sigma\colon K \to L$ es un homomorfismo inyectivo que deja fijo F, entonces $\sigma(K) = K$ (es decir, σ es también sobreyectivo).*

Demostración. Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $f(X)$ en K, de modo que $K = F(\alpha_1, \ldots, \alpha_n)$. Ahora $f^\sigma(X) = f(X)$ porque $f(X)$ tiene coeficientes en F y σ los deja fijos. Por lo tanto, cada $\sigma(\alpha_i) \in L$ es una raíz de $f(X)$ y en consecuencia $\sigma(\alpha_i) = \alpha_j$ para algún j. Como σ es inyectivo, lo que hace es permutar las raíces de $f(X)$. En particular,

$$\sigma(K) = F(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = F(\alpha_1, \ldots, \alpha_n) = K. \qquad \square$$

Proposición 2.32. *Si K es un cuerpo de escisión de un polinomio en $F[X]$, entonces la extensión $K \mid F$ es una extensión normal.*

Demostración. Sea $K = F(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_1, \ldots, \alpha_n$ son todas las raíces de $f(X) \in F[X]$. Sea $g(X) \in F[X]$ algún polinomio irreducible que contenga una raíz β en K. Hay un cuerpo de escisión L para $g(X)$ sobre K; sea $\beta' \in L$ otra raíz de $g(X)$. Para garantizar que $K \mid F$ es normal, debemos comprobar que $\beta' \in K$.

Por la Proposición 2.22, hay un homomorfismo $\varphi\colon F(\beta) \to F(\beta')$ que deja fijo F tal que $\varphi(\beta) = \beta'$. Ahora, el cuerpo de escisión de $f(X)$ sobre $F(\beta)$ es $F(\beta, \alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n) = K$ en vista de que $\beta \in K$. Por otra parte, el cuerpo de escisión de $f(X) = f^\sigma(X)$ sobre $F(\beta')$ es $F(\beta', \alpha_1, \ldots, \alpha_n) = K(\beta')$.

La Proposición 2.24 ahora garantiza que hay un isomorfismo $\psi\colon K \to K(\beta')$ que extiende φ; entre otras cosas, ψ deja fijo F. El Lema anterior muestra que $\psi(K) = K$, así que $K(\beta') = K$, lo que dice que $\beta' \in K$. $\square$

2.3 F-morfismos

Definición 2.33. Sean $K \mid F$ y $L \mid F$ dos extensiones del mismo cuerpo F. Un **F-morfismo** de K en L es un homomorfismo $\varphi\colon K \to L$ que deja F fijo, es decir, $\varphi(a) = a$ para todo $a \in F$. La totalidad de F-morfismos de K en L se denota por $\mathrm{Hom}_F(K, L)$.

Estos F-morfismos tienen las siguientes propiedades:

1. Cada F-morfismo es inyectivo, porque $\varphi(1) = 1$ ya que $1 \in F$ y el ideal $\ker\varphi$ de K es necesariamente nulo. Por tanto, φ es un isomorfismo entre K y L si y sólo si φ es sobreyectivo. Si $L = K$ y si $\varphi(K) = K$, se dice que φ es un **F-automorfismo** de K.

2. De todos modos, la imagen $\varphi(K)$ es un subcuerpo de L que es isomorfo a K.

3. Cada $\varphi \in \mathrm{Hom}_F(K,L)$ es en particular una transformación F-lineal entre los espacios F-vectoriales K y L.

4. Si $[K\colon F]$ es finito, cada $\varphi \in \mathrm{Hom}_F(K,K)$ es F-lineal e inyectivo y por tanto es también sobreyectivo, así que φ es un F-automorfismo de K.

5. Si $K = F(\alpha_1,\ldots,\alpha_n)$, entonces cada $\varphi \in \mathrm{Hom}_F(K,L)$ queda determinado por sus valores $\varphi(\alpha_1),\ldots,\varphi(\alpha_n) \in L$.

Lema 2.34. *Si $F \subseteq K \subseteq \mathbb{C}$ y si $\varphi \in \mathrm{Hom}_F(K,\mathbb{C})$, entonces $\varphi(\alpha)$ es un conjugado de α sobre F, para cada $\alpha \in K$. Inversamente, si $\alpha,\beta \in K$ son conjugados sobre F, entonces hay un único F-morfismo $\varphi\colon F(\alpha) \to \mathbb{C}$ tal que $\varphi(\alpha) = \beta$.*

Demostración. Sea $p(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ el polinomio mínimo en $F[X]$ de $\alpha \in K$. Entonces

$$\begin{aligned} p(\varphi(\alpha)) &= a_0 + a_1\varphi(\alpha) + \cdots + a_{n-1}\varphi(\alpha)^{n-1} + \varphi(\alpha)^n \\ &= \varphi(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n) \\ &= \varphi(p(\alpha)) = \varphi(0) = 0. \end{aligned} \tag{2.5}$$

Luego $\varphi(\alpha)$ es una raíz (en $\mathbb{C}$) de $p(X)$, es decir, es un conjugado de α sobre F.

Para la parte inversa, dadas dos raíces $\alpha,\beta \in \mathbb{C}$ de un polinomio irreducible $p(X) \in F[X]$, el Corolario 2.23 proporciona un F-isomorfismo $\varphi\colon F(\alpha) \to F(\beta)$, el cual es también un F-morfismo de $F(\alpha)$ en $\mathbb{C}$, que cumple $\varphi(\alpha) = \beta$. Este $\varphi \in \mathrm{Hom}_F(F(\alpha),\mathbb{C})$ es único porque queda determinado por el valor $\varphi(\alpha)$. □

Ejemplo 2.35. (a) Si $a + bi \in \mathbb{C}$ con $a,b \in \mathbb{R}$, sus únicos conjugados sobre $\mathbb{R}$ son $a + bi$ mismo y su "conjugado complejo" $a - bi$ (véase el Ejemplo 2.28); estos coinciden si y sólo si $b = 0$. Entonces sólo hay dos $\mathbb{R}$-automorfismos de $\mathbb{C}$: la aplicación identidad $\mathrm{id}_{\mathbb{C}}$ y la conjugación compleja $a + bi \mapsto a - bi$.

(b) Como $X^3 - 2$ es irreducible sobre $\mathbb{Q}[X]$ y tiene tres raíces distintas en $\mathbb{C}$, hay exactamente 3 $\mathbb{Q}$-morfismos $\{\varphi_0,\varphi_1,\varphi_2\}$ de $\mathbb{Q}(\sqrt[3]{2})$ en $\mathbb{C}$. Aquí φ_0 es la inclusión $\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$ y los otros son dados explícitamente por

$$\varphi_1(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{4}, \tag{2.6a}$$

$$\varphi_2(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a + b\omega^2\sqrt[3]{2} + c\omega\sqrt[3]{4}, \tag{2.6b}$$

para $a,b,c \in \mathbb{Q}$; recuérdese que $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ es una base vectorial de $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$.

Proposición 2.36. *Si $F \subseteq K \subseteq \mathbb{C}$ con $[K\colon F] = n$ finito y si $\varphi \in \mathrm{Hom}_F(K,\mathbb{C})$, entonces hay exactamente n homomorfismos $\psi\colon K \to \mathbb{C}$ que extienden φ.*

Demostración. Por inducción sobre n. En el caso $n = 1$, es $K = F$ y entonces $\psi := \varphi$ es la única posibilidad.

Sea $n > 1$ y supóngase que el teorema es válido para extensiones de grado menor que n. Tómese $\alpha \in K \setminus F$. Por ser $K \,|\, F$ una extensión finita, se sabe que α es algebraica sobre F y que $F \subset F(\alpha) \subseteq K$. Sea $p(X) \in F[X]$ el polinomio mínimo de α sobre F, de grado m con $1 < m \leq n$.

Sea $E := \varphi(F)$, un subcuerpo de $\mathbb{C}$. El isomorfismo de cuerpos $\varphi\colon F \to E$ determina un isomorfismo de anillos $F[X] \to E[X]$ que lleva $p(X)$ en $p^{\varphi}(X)$. Luego $p^{\varphi}(X)$ es irreducible en $E(X)$, de grado m; como tal, tiene m raíces *distintas* en $\mathbb{C}$.

En el caso de que $m = n$, entonces $[F(\alpha)\colon F] = n = [K\colon F]$, así que $K = F(\alpha)$. Para extender φ, es necesario y suficiente encontrar el elemento $\psi(\alpha) \in \mathbb{C}$. Una leve modificación del cálculo (2.5) muestra que

$$\begin{aligned} p^{\varphi}(\psi(\alpha)) &= \varphi(a_0) + \varphi(a_1)\psi(\alpha) + \cdots + \varphi(a_{m-1})\psi(\alpha)^{m-1} + \psi(\alpha)^m \\ &= \psi(a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} + \alpha^m) \\ &= \psi(p(\alpha)) = \psi(0) = 0, \end{aligned}$$

por tanto $\psi(\alpha)$ es una raíz de $p^{\varphi}(X)$ en $E[X]$. La elección de esta raíz da lugar a exactamente $m = n$ posibilidades para ψ.

En el caso de que $m < n$, entonces $F \subset F(\alpha) \subset K$ con inclusiones estrictas; si $r := [K\colon F(\alpha)]$, entonces

$$n = [K\colon F] = [K\colon F(\alpha)]\,[F(\alpha)\colon F] = rm.$$

Por la hipótesis inductiva, hay r posibles homomorfismos $\varphi_1, \ldots, \varphi_r\colon F(\alpha) \to \mathbb{C}$ que extienden φ, y además cada una de ellas tiene m posibles extensiones de K en $\mathbb{C}$. Luego hay un total de $rm = n$ posibles extensiones de φ hasta K. □

Corolario 2.37. *Si $F \subseteq K \subseteq \mathbb{C}$ con $[K\colon F] = n$ finito, hay exactamente n F-morfismos en la colección* $\mathrm{Hom}_F(K,\mathbb{C})$. ⊟

El teorema que sigue dice que una extensión finita que queda dentro del cuerpo $\mathbb{C}$ es necesariamente simple. Para mostrarlo, se puede usar el siguiente lema de álgebra lineal, que tiene cierto interés propio.

Lema 2.38. *Si V es un espacio vectorial sobre un cuerpo infinito F, entonces V no es la unión de un número finito de subespacios propios.*

Demostración. Si $H_1, \ldots, H_r$ son subespacios de V con $H_j \neq V$ en cada caso, hay que mostrar que $H_1 \cup \cdots \cup H_r \neq V$.

Esto se hace por inducción sobre el número r de subespacios dados. En el caso $r = 1$, queda claro que $H_1 \neq V$ por ser H_1 un subespacio propio.

Sea $r > 1$ y supóngase que el lema es válido para el caso $(r-1)$. Para obtener una contradicción, tomemos una colección de r subespacios propios H_j con $H_1 \cup \cdots \cup H_r = V$. Ahora $H_1 \cup \cdots \cup H_{r-1} \neq V$ por la hipótesis inductiva, así que debe haber un vector $x \in H_r$ tal que $x \notin H_1 \cup \cdots \cup H_{r-1}$. Por otro lado, como H_r es un subespacio, debe haber otro vector $y \in V \setminus H_r$, de modo que $y \in H_1 \cup \cdots \cup H_{r-1}$. Está claro que $y \neq x$.

La recta que pasa por los dos puntos x, y es $\{\, (1-t)x + ty : t \in F \,\}$ que se parametriza biyectivamente por los escalares $t \in F$. Como F tiene infinitos elementos, el principio de los palomares[9] indica que debe haber al menos un subespacio H_k de la lista que contenga dos puntos distintos de la recta. Es decir, hay $t_0, t_1 \in F$ con $t_0 \neq t_1$ tales que $(1-t_0)x + t_0 y \in H_k$, $(1-t_1)x + t_1 y \in H_k$. La diferencia es $(t_1 - t_0)(y - x) \in H_k$; al dividir por $(t_1 - t_0)$, se obtiene $(y - x) \in H_k$.

Ahora, si $k = r$, entonces $(y - x) \in H_r$, $x \in H_r$ implica $y \in H_r$, lo cual es falso. Pero si $k < r$, entonces $(x - y) \in H_k$, $y \in H_k$ implica $x \in H_k$, igualmente falso. La suposición de que $H_1 \cup \cdots \cup H_r = V$ entonces resulta contradictoria. □

El siguiente resultado se conoce como el *Teorema del Elemento Primitivo*. La hipótesis de que la extensión sea un subcuerpo de $\mathbb{C}$ no es esencial: más adelante, veremos otras hipótesis en donde se puede obtener la misma conclusión.

Teorema 2.39. *Sea $K \mid F$ una extensión finita en donde $K \subseteq \mathbb{C}$. Entonces hay un elemento $\alpha \in K$ tal que $K = F(\alpha)$.*

Demostración. Del Corolario 2.37, se sabe que $\mathrm{Hom}_F(K, \mathbb{C})$ consta de exactamente n F-morfismos $\{\psi_1, \ldots, \psi_n\}$, donde ψ_1 es la inclusión $K \hookrightarrow \mathbb{C}$. Para cada par ordenado (i, j) con $1 \leq i < j \leq n$, la diferencia $\psi_i - \psi_j$ es una aplicación F-lineal no nula de K en $\mathbb{C}$; su núcleo $H_{ij} := \ker(\psi_i - \psi_j)$ es un subespacio propio de K.

Por ser $F \subseteq \mathbb{C}$, tenemos $\{0, 1\} \subset F$, de donde $\mathbb{Z} \subset F$ e inclusive $\mathbb{Q} \subseteq F$. Entre otras cosas, esto dice que F tiene infinitos elementos. Ahora el Lema 2.38 garantiza que la unión de los subespacios H_{ij} no es todo K. Por ende, hay un elemento $\alpha \in K$ tal que $\alpha \notin \ker(\psi_i - \psi_j)$ cada vez que $i < j$ en $\{1, 2, \ldots, n\}$. En otras palabras, $\psi_i(\alpha) \neq \psi_j(\alpha)$ para $i < j$. Dicho de modo más sencillo, los elementos $\psi_1(\alpha), \ldots, \psi_n(\alpha) \in \mathbb{C}$ son distintos.

Ahora $\psi_1(\alpha) = \alpha$ y el Lema 2.34 dice que cada $\psi_j(\alpha)$ es un conjugado de α. Por lo tanto, el elemento $\alpha \in K$ tiene n conjugados *distintos*, así que el grado de su polinomio mínimo es al menos n. Por otro lado, como $[K\colon F] = n$, este grado no puede exceder n, y se concluye que $F \subseteq F(\alpha) \subseteq K$ con $[F(\alpha)\colon F] = n$. En consecuencia, es $F(\alpha) = K$. □

2.4 Números constructibles

Una de las consecuencias más llamativas de la teoría de extensiones de cuerpos es la imposibilidad de resolver, en forma positiva, los tres problemas más famosas de la época griega antigua: la *duplicación del cubo*, la *trisección del ángulo* y la *cuadratura del círculo*, con el uso de la regla y el compás.

[9] Este es el *Schubfachsprinzip*, formulado por Dirichlet: al meter $(n+1)$ palomas en n palomares, debe haber al menos un palomar que contenga al menos dos palomas.

Los primeros dos problemas fueron parcialmente resueltos, usando otros instrumentos que exceden el ámbito de la regla y el compás, por diversos sabios, desde Eudoxos hasta Apolonio, entre 350 y 200 a.C.[10] La cuadratura del círculo (construir un cuadrado que tenga la misma área que un círculo dado) resistió a sus esfuerzos. Su imposibilidad fue finalmente comprobado en 1881, cuando Ferdinand Lindemann demostró que π es trascendente sobre $\mathbb{Q}$.

Los otros dos problemas involucran la construcción, en el sentido explicado más adelante, de ciertos números algebraicos. La duplicación del cubo (hallar el lado de un cubo cuyo volumen es el doble de un cubo dado) pide la construcción de $\sqrt[3]{2}$, mientras la trisección de un ángulo de 60° (digamos) pide la construcción de $\cos 20^\circ$ y $\operatorname{sen} 20^\circ$.

Cualquier cuerpo tiene al menos dos elementos, 0 y 1. Consideremos el plano $\mathbb{R}^2$, identificado con el cuerpo $\mathbb{C}$, junto con las posiciones marcados de 0 y 1. La distancia entre estos dos puntos proporciona una unidad de medición que puede compararse con otras distancias en el plano. La *regla* es un instrumento que permite trazar la recta que une dos puntos distintos en el plano. El *compás* es un instrumento que permite trazar el círculo cuyo centro es un punto dado y que pasa por otro punto dado. Las primeras proposiciones del Libro I de Euclides[11] muestran que, con instrumentos de esta naturaleza, puede trazarse un círculo con centro dado, cuyo radio es la distancia entre cualquier par de puntos conocidos: es decir, que se puede asumir que el compás es *rígido*, de modo que puede trazarse un círculo "con centro dado y radio dado". Finalmente, se agregan los puntos de intersección de las curvas trazadas con éstos instrumentos al catálogo de puntos ya construidos, partiendo de $\{0,1\}$, para así formar el conjunto de todos los "puntos constructibles" del plano euclidiano.

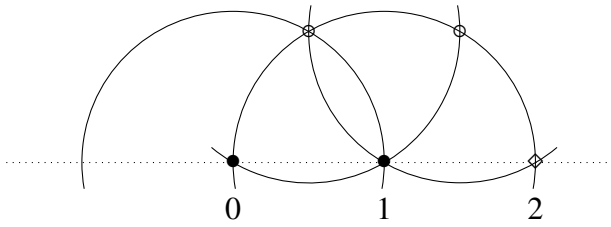


Figura 2: Construcción de 2 a partir de $\{0,1\}$ con compás solamente

Algunas construcciones pueden efectuarse con sólo el compás. Por ejemplo, a partir de 0 y 1, mediante la ubicación intermedia de los dos puntos $\frac{1}{2}(1+\sqrt{3}\,i)$ y $\frac{1}{2}(3+\sqrt{3}\,i)$, se puede encontar 2 como una intersección de dos círculos: Véase la Figura 2. Es evidente que al repetir esta construcción, se puede ubicar los puntos $3,4,5,\ldots$ y también $-1,-2,-3,\ldots$, de

[10] Para una descripción detallada de éstas y otras investigaciones en el tercer siglo a.C., véase: Wilbur R. Knorr, *The Ancient Tradition of Geometric Problems*, Dover, New York, 1986.

[11] El tratado de Euclides, titulado Στοιχεῖα (que significa *Elementos*) se divide en 13 "libros" sobre temas afines, desde la geometría de triángulos (Libro I), pasando por la teoría de proporciones (Libro V), la teoría de números (Libro VII), construcciones de irracionales (Libro X), hasta la contrucción de los cinco poliedros regulares convexos (Libro XIII). Entre las traducciones modernos, se recomienda: Thomas L. Heath, *The Thirteen Books of Euclid's Elements*, en 3 tomos, Dover, New York, 1956.

modo que todo $n \in \mathbb{Z}$ es constructible con compás solamente.[12]

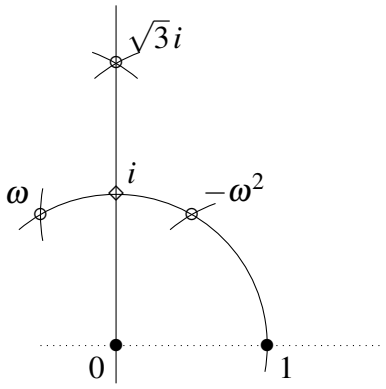


Figura 3: Construcción de i a partir de $\{0,1\}$ con regla y compás

Una construcción de i exige cinco círculos y una recta, con la ubicación de tres puntos intermedios $-\omega^2 = \frac{1}{2}(1+\sqrt{3}\,i)$, ω, $\sqrt{3}\,i$: véase la Figura 3.

Con regla y compás, se puede construir:

- una recta paralela a una recta dada, a través de un punto dado;
- un tríangulo semejante a un triángulo dado, cuyo lado sea un segmento dado;
- el lado de un cuadrado cuya área es igual a la de un rectángulo dado.[13]

De esta forma, si $p,q \in \mathbb{R}$ son puntos ya ubicados, puede ubicarse también la suma $p+q$, el negativo $-p$, el producto pq, el cociente p/q si $q \neq 0$ y la raíz cuadrada $\sqrt{q}$ si $q > 0$. Se concluye que *los puntos constructibles de* $\mathbb{R}$ *forman un subcuerpo de* $\mathbb{R}$ *que extiende* $\mathbb{Q}$. Al agregar los correspondientes de i (fíjese que $\{0, p, p\,i\}$ son los vértices de un triángulo isósceles), se ve que todos los puntos constructibles del plano forman un cuerpo K_{cons} tal que $\mathbb{Q}(i) \subset K_{\text{cons}} \subset \mathbb{C}$.

Definición 2.40. Sea F un subcuerpo de $\mathbb{C}$. Entonces $F = \{\, a+bi \in \mathbb{C} : a,b \in F \cap \mathbb{R} \,\}$ se identifica con la totalidad de puntos $(a,b) \in \mathbb{R}^2$ con coordenadas en $F \cap \mathbb{R}$. Un número $z \in \mathbb{C}$ es **constructible en un paso** a partir de los elementos de F, si z queda en al menos uno de éstos tres casos:

(i) el punto de intersección de dos rectas:

$$\begin{aligned} a_1x + b_1y + c_1 &= 0 \\ a_2x + b_2y + c_2 &= 0 \end{aligned} \qquad \text{con} \quad a_1,b_1,c_1,a_2,b_2,c_2 \in F \cap \mathbb{R}; \tag{2.7}$$

[12] Se sabe que cualquier construcción por regla y compás puede efectuarse con compás solamente. Esto fue demostrado por Lorenzo Mascheroni, *Geometria del Compasso*, Pavia, 1797.

[13] Para los procedimientos explícitos que efectúan estas construcciones, véase el Capítulo 1 de: Joseph C. Várilly, *Elementos de Geometría Plana*, Editorial de la UCR, San José, 1988.

(ii) un punto de intersección de una recta y un círculo:

$$\begin{aligned} ax+by+c &= 0 \\ x^2+y^2+2gx+2fy+e &= 0 \end{aligned} \qquad \text{con} \quad a,b,c,e,f,g \in F\cap\mathbb{R}; \tag{2.8}$$

(iii) un punto de intersección de dos círculos:

$$\begin{aligned} x^2+y^2+2g_1x+2f_1y+e_1 &= 0 \\ x^2+y^2+2g_2x+2f_2y+e_2 &= 0 \end{aligned} \qquad \text{con} \quad e_1,f_1,g_1,e_2,f_2,g_2 \in F\cap\mathbb{R}.$$

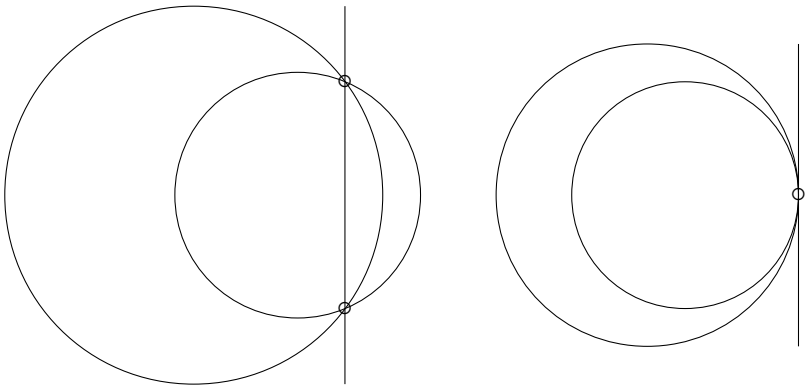


Figura 4: Las intersecciones de dos círculos determinan una recta

Obsérvese que en el tercer caso, los dos puntos de intersección de los círculos coinciden con la intersección del primer círculo con la recta

$$2(g_1-g_2)x+2(f_1-f_2)y+(e_1-e_2)=0,$$

obtenida al restar las ecuaciones de los círculos:[14] véase la Figura 4. Por tanto, el caso (iii) es redundante.

Proposición 2.41. *Si un número $z=x+yi\in\mathbb{C}$ es constructible en un paso a partir de elementos de un subcuerpo F de $\mathbb{C}$, entonces z es algebraico sobre F con $[F(z)\colon F]=1$ ó 2.*

Demostración. En el caso (i), se obtiene, la intersección de las dos rectas (2.7) por la regla de Cramer:

$$x=\frac{b_1c_2-b_2c_1}{a_1b_2-a_2b_1}\in F\cap\mathbb{R}, \qquad y=\frac{c_1a_2-c_2a_1}{a_1b_2-a_2b_1}\in F\cap\mathbb{R}.$$

(Obsérvese que $a_1b_2-a_2b_1=0$ si y sólo si las dos rectas son iguales o paralelos.) Por tanto, $z=x+yi$ pertenece también a F y $F(z)=F$.

[14] Esta recta se llama el *eje radical* de los dos círculos.

Considérese ahora la intersección (2.8) de una recta y un círculo. Al eliminar x por $x = -(by+c)/a$ si $a \neq 0$, se obtiene de la ecuación del círculo:

$$(b^2+1)y^2 + 2(bc - abg + a^2 f)y + (c^2 - 2acg + a^2 e) = 0.$$

Entonces se ve que $x, y, z \in F(\sqrt{\Delta})$, donde Δ es el discriminante del lado izquierdo de esta ecuación cuadrática para y. Hay dos posibilidades: si Δ es un cuadrado en F, entonces $F(z) = F(\sqrt{\Delta}) = F$; en cambio, si Δ no es un cuadrado en F, entonces y y también x son raíces de polinomios cuadráticos irreducibles sobre F y por ende $[F(z)\colon F] = [F(\sqrt{\Delta})\colon F] = 2$.

Si fuera $a = 0$, entonces $y = -c/b$ y se obtiene una ecuación cuadrática para x, susceptible al mismo análisis. □

Corolario 2.42. *Si $z \in \mathbb{C}$ es un número constructible en una cadena finita de pasos a partir de 0 y 1, entonces z es algebraico sobre $\mathbb{Q}$ con $[\mathbb{Q}(z)\colon \mathbb{Q}] = 2^m$ para algún $m \in \mathbb{N}$.*

Demostración. Cada elemento de $\mathbb{Q}$ —o bien de $\mathbb{Q}(i)$— es constructible en un número finito de pasos. Si $z \notin \mathbb{Q}$, su construcción pasa por una torre finita de extensiones

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k,$$

con $F_k = \mathbb{Q}(z)$, donde $[F_i\colon F_{i-1}] = 1$ ó 2 para $i = 1, 2, \ldots, k$. Al multiplicar estos grados, se obtiene $[\mathbb{Q}(z)\colon \mathbb{Q}] = 2^m$ para algún $m \in \{0, 1, \ldots, k\}$. □

Corolario 2.43. *Si $z \in \mathbb{C}$ es tal que $[\mathbb{Q}(z)\colon \mathbb{Q}]$ es divisible por un número primo* impar*, entonces z no es constructible por regla y compás.* ⊟

Corolario 2.44. *La duplicación del cubo por regla y compás es imposible.*

Demostración. Para duplicar el cubo cuyo lado es el segmento $[0,1]$, hay que obtener un segmento de la misma longitud que el segmento $[0, \sqrt[3]{2}]$; es decir, hay que construir el número $\sqrt[3]{2}$. Pero el polinomio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ es $X^3 - 2$, así que $[\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}] = 3$. El Corolario anterior muestra que $\sqrt[3]{2}$ no es constructible por regla y compás.[15] □

Proposición 2.45. *La trisección del ángulo $\frac{\pi}{3} = 60^\circ$ no es posible por regla y compás.*[16]

Demostración. Se tarea de verificar que el número $e^{\pi i/9} = \cos\frac{\pi}{9} + i\,\mathrm{sen}\,\frac{\pi}{9}$ no es constructible, para lo cual basta comprobar que $\cos\frac{\pi}{9} = \cos 20^\circ$ no es constructible.

Hay que recordar la fórmula para el coseno del ángulo triple:

$$\begin{aligned}
\cos 3\theta &= \cos 2\theta \cos\theta - \mathrm{sen}\,2\theta\,\mathrm{sen}\,\theta \\
&= (2\cos^2\theta - 1)\cos\theta - 2\,\mathrm{sen}^2\theta\cos\theta \\
&= 2\cos^3\theta - \cos\theta - 2(1-\cos^2\theta)\cos\theta \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

[15] Para una discusión de su construcción por otros instrumentos, véase el libro de Knorr antes citado.

[16] Este resultado no ha percolado todavía a la cultura popular, que ya ha tomado conciencia de que la cuadratura del círculo es imposible. Un recuento de las actividades de "los trisectores" y la psicología de sus labores se encuentra en: Underwood Dudley, *A Budget of Trisections*, Springer, New York, 1987.

Ahora $\cos 60^\circ = \frac{1}{2}$, por lo tanto $\cos 20^\circ$ es una raíz del polinomio cúbico $8X^3 - 6X - 1 = 0$.

Hace falta comprobar que este polinomio es irreducible en $\mathbb{Q}[X]$. Por el Lema de Gauss, basta verificar que no tiene una factorización propia en $\mathbb{Z}[X]$. Consideremos cuatro posibilidades:

$$8X^3 - 6X - 1 = \begin{cases} (X \pm 1)(8X^2 + aX \mp 1) & \Longrightarrow \quad a \pm 8 = 0, \quad \pm a \mp 1 = -6; \\ (2X \pm 1)(4X^2 + bX \mp 1) & \Longrightarrow \; 2b \pm 4 = 0, \quad \pm b \mp 2 = -6; \\ (4X \pm 1)(2X^2 + cX \mp 1) & \Longrightarrow \; 4c \pm 2 = 0, \quad \pm c \mp 4 = -6; \\ (8X \pm 1)(X^2 + dX \mp 1) & \Longrightarrow \; 8d \pm 1 = 0, \quad \pm d \mp 8 = -6. \end{cases}$$

Las ecuaciones a la derecha corresponden a los coeficientes de X^2 y X en el producto de los posibles factores. Se ve que no hay solución alguna con $a, b, c, d \in \mathbb{Z}$. Por tanto, este polinomio cúbico es irreducible en $\mathbb{Z}[X]$. En consecuencia, $[\mathbb{Q}(\cos 20^\circ) \colon \mathbb{Q}] = 3$, lo cual conlleva que $\cos 20^\circ$ no es constructible. □

2.5 Ejercicios sobre extensiones de cuerpos

Ejercicio 2.1. Determinar los grados de las extensiones $K \,|\, \mathbb{Q}$ para los casos

$$\text{(a)} \quad K = \mathbb{Q}(\omega); \qquad \text{(b)} \quad K = \mathbb{Q}(i); \qquad \text{(c)} \quad K = \mathbb{Q}(\sqrt[3]{2});$$

donde $\omega = e^{2\pi i/3}$ es una raíz cúbica compleja de 1. En cada caso, exhibir una base para K como espacio vectorial sobre $\mathbb{Q}$.

Ejercicio 2.2. Determinar el grado $[\mathbb{Q}(\sqrt{3}, i) \colon \mathbb{Q}]$ y encontrar tres cuerpos intermedios E con $\mathbb{Q} \subsetneq E \subsetneq \mathbb{Q}(\sqrt{3}, i)$. ¿Será posible encontrar otro cuerpo intermedio, distinto de éstos tres?

Ejercicio 2.3. (a) Demostrar que $X^n - 2$ es irreducible en $\mathbb{Z}[X]$, para $n = 1, 2, 3, \ldots$. Sea $F_n := \mathbb{Q}(2^{1/n})$ para $n \in \mathbb{N} \setminus \{0\}$; mostrar que $[F_n \colon \mathbb{Q}] = n$.

(b) Si $m \in \mathbb{N} \setminus \{0\}$ con $m \setminus n$, mostrar que $F_m \subseteq F_n$ y calcular el grado $[F_n \colon F_m]$.

(c) En cambio, si $\mathrm{mcd}(m, n) = 1$, mostrar que $F_{mn} = \mathbb{Q}(2^{1/m}, 2^{1/n})$.

Ejercicio 2.4. Calcular el grado de extensión $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \colon \mathbb{Q}]$.

Ejercicio 2.5. Factorizar $X^6 - 1$ en $\mathbb{Z}[X]$. Usar esta factorización para encontrar el cuerpo de escisión de $X^6 - 1$ sobre $\mathbb{Q}$ como una extensión simple $\mathbb{Q}(\alpha)$, para un número $\alpha \in \mathbb{C}$ apropiado.

Ejercicio 2.6. Sea $p(X)$ un polinomio irreducible en $\mathbb{Q}[X]$ y sea $K \subset \mathbb{C}$ el cuerpo de escisión para $p(X)$ sobre $\mathbb{Q}$. Mostrar que todas las raíces de $p(X)$ en K son distintas.

⟦ Indicación: ¿Qué pasaría si $p(X)$ tuviera una raíz doble en K? ⟧

Ejercicio 2.7. Encontrar un elemento $\alpha \in \mathbb{Q}(\sqrt{3}, i)$ tal que $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\alpha)$. Calcular el polinomio mínimo de este elemento α sobre $\mathbb{Q}$. Exhibir todos los elementos conjugados de α sobre $\mathbb{Q}$.

Ejercicio 2.8. Hallar un cuerpo de escisión K para $(X^2-2)(X^2+X+1)$ sobre $\mathbb{Q}$ y encontrar $\beta \in K$ tal que $\mathbb{Q}(\beta) = K$.

Ejercicio 2.9. (a) Si hay un homomorfismo $\varphi\colon K \to L$ entre dos extensiones $K \,|\, \mathbb{Q}$ y $L \,|\, \mathbb{Q}$, mostrar que $\varphi(a) = a$ para todo $a \in \mathbb{Q}$.

(b) Explicar por qué los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$ no son isomorfos.

Ejercicio 2.10. Si $K \,|\, F$ es una extensión cuadrática — es decir, $[K\colon F] = 2$ — mostrar que esta extensión es normal.

Ejercicio 2.11. Si $p \in \mathbb{N}$ es primo y si K es el cuerpo de escisión de $f(X) := X^p - 1$ sobre $\mathbb{Q}$, mostrar que $[K\colon \mathbb{Q}] = p-1$. Además, encontrar elementos $\alpha_1, \ldots, \alpha_{p-1} \in \mathbb{C}$ tales que $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_{p-1})$.

Ejercicio 2.12. (a) Demostrar que un polinomio $f(X) \in \mathbb{Z}[X]$ cuyo discriminante se anula — es decir, $D(f(X)) = 0$ — debe ser reducible.

(b) En el caso $f(X) = X^4 - 4X^3 - 4X^2 + 16X + 16$, verificar que $D(f(X)) = 0$.

(c) Concluir que este polinomio o bien tiene un factor de la forma $(X-a)^2$ con $a \in \mathbb{Z}$, o bien $f(X) = (X^2 + bX + c)^2$ con $b, c \in \mathbb{Z}$.

(d) Decidir entre las dos alternativas en (c), para obtener la factorización completa de $X^4 - 4X^3 - 4X^2 + 16X + 16$ en $\mathbb{Z}[X]$.

Ejercicio 2.13. (a) Factorizar el polinomio $h(X) = 16X^4 + 16X^3 - 4X^2 - 4X + 1$ en $\mathbb{Z}[X]$.

(b) Verificar la identidad trigonométrica:

$$\cos 5\theta = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta.$$

(c) Concluir que $h(\cos\frac{2\pi}{5}) = 0$ y obtener el polinomio mínimo de $\cos\frac{2\pi}{5}$ sobre $\mathbb{Q}$.

(d) Deducir que $[\mathbb{Q}(\cos\frac{2\pi}{5})\colon \mathbb{Q}] = 2$.

Ejercicio 2.14. (a) Sea $\zeta_5 := e^{2\pi i/5} = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\,\frac{2\pi}{5}$. Encontrar el polinomio mínimo de ζ_5 sobre $\mathbb{Q}$ y concluir que $[\mathbb{Q}(\zeta_5)\colon \mathbb{Q}] = 4$.

(b) Mostrar que $\cos\frac{2\pi}{5} \in \mathbb{Q}(\zeta_5)$. Deducir que $[\mathbb{Q}(\zeta_5)\colon \mathbb{Q}(\cos\frac{2\pi}{5})] = 2$.

(c) Encontrar el polinomio mínimo de ζ_5 sobre $\mathbb{Q}(\cos\frac{2\pi}{5})$.

3 Grupos de Galois

El tema central de la teoría de Galois es la relación entre extensiones de cuerpos y ciertos grupos de automorfismos de cuerpos. A cada extensión $K \mid F$ se puede asociar el grupo de automorfismos de K que deja fijo el subcuerpo F; en cambio, a cada grupo G de automorfismos de un cuerpo K se puede asociar el subcuerpo de elementos fijos de K bajo la acción de los automorfismos en G. En este capítulo exploramos hasta donde estas aplicaciones definen una correspondencia recíproca y las consecuencias que tiene dicha reciprocidad para la estructura de los cuerpos.

3.1 La correspondencia de Galois

Definición 3.1. Sea $K \mid F$ una extensión de cuerpos. La totalidad de F-automorfismos de K (es decir, los automorfismos $\sigma\colon K \to K$ tales que $\sigma(a) = a$ para todo $a \in F$) es un *grupo* $\underline{\mathrm{Gal}(K \mid F)}$, llamado el **grupo de Galois** de la extensión.

La identidad de este grupo es la aplicación identidad $\mathrm{id}\colon K \to K$ y la operación del grupo es la composición funcional de los automorfismos.

Notación. Si G es un grupo finito, $|G|$ denota el número de elementos en G.

Proposición 3.2. *Sea $F \subseteq K \subseteq \mathbb{C}$ con $[K\colon F]$ finito. Entonces*

$$\big|\mathrm{Gal}(K \mid F)\big| \leq [K\colon F]. \tag{3.1}$$

Demostración. Del Teorema 2.39, la hipótesis de que $F \subseteq K \subseteq \mathbb{C}$ y la finitud de $n = [K\colon F]$ implican que hay un elemento "primitivo" $\alpha \in K$ tal que $K = F(\alpha)$. El polinomio mínimo $p(X)$ de α sobre F tiene grado n.

Si $\sigma \in \mathrm{Gal}(K \mid F)$, entonces $p^\sigma(X) = p(X)$ porque σ deja fijo cada coeficiente de $p(X)$. Luego

$$p(\sigma(\alpha)) = p^\sigma(\sigma(\alpha)) = \sigma(p(\alpha)) = \sigma(0) = 0,$$

así que $\sigma(\alpha) \in K$ es un conjugado de α sobre F. Ahora α tiene exactamente n conjugados en $\mathbb{C}$, a saber, las n raíces distintas de $p(X)$.

Denótese por $\imath\colon K \to \mathbb{C}$ la inclusión de K en $\mathbb{C}$. Entonces $\imath\sigma \in \mathrm{Hom}_F(K, \mathbb{C})$ para todo $\sigma \in \mathrm{Gal}(K \mid F)$ y σ queda determinado por $\sigma(\alpha) = \imath(\sigma(\alpha))$. Por otro lado, sabemos por el Corolario 2.37 que cada conjugado $\beta \in \mathbb{C}$ de α determina un elemento $\varphi \in \mathrm{Hom}_F(K, \mathbb{C})$ que cumple $\varphi(\alpha) = \beta$. De ahí se concluye que[1]

$$\mathrm{Gal}(K \mid F) \leftrightarrow \{\, \varphi \in \mathrm{Hom}_F(K, \mathbb{C}) : \varphi(\alpha) \in K \,\} \tag{3.2}$$

y el orden de este grupo es el número de conjugados de α que pertenecen a K. Por lo tanto, $|\mathrm{Gal}(K \mid F)| \leq n$. □

El caso más interesante ocurre cuando $|\mathrm{Gal}(K \mid F)|$ coincide con $[K\colon F]$. Resulta que la condición necesaria (y suficiente, si $K \subseteq \mathbb{C}$) es la normalidad de la extensión. Antes de comprobarlo, es útil notar que las extensiones normales finitos son cuerpos de escisión.

[1] La notación '$A \leftrightarrow B$' significa que hay una biyección entre los conjuntos A y B.

Proposición 3.3. *Si $F \subseteq K \subseteq \mathbb{C}$ con $[K\colon F]$ finito, entonces las siguientes condiciones son equivalentes:*

(a) la extensión $K \,|\, F$ es normal;

(b) K es el cuerpo de escisión de un polinomio $f(X) \in F[X]$;

(c) K es el cuerpo de escisión de un polinomio irreducible $p(X) \in F[X]$.

Demostración. La implicación (c) $\Longrightarrow$ (b) es trivial, y la implicación (b) $\Longrightarrow$ (a) es la Proposición 2.32. Sólo hace falta comprobar (a) $\Longrightarrow$ (c).

Del Teorema 2.39, se sabe que hay $\beta \in K$ tal que $K = F(\beta)$. Sea $q(X)$ el polinomio mínimo de β sobre F y sea $n = [K\colon F] = \operatorname{gr} q(X)$. Supóngase que $K \,|\, F$ es normal. Como $q(X)$ es irreducible y β es una de sus raíces, todos sus conjugados $\beta = \beta_1, \beta_2, \ldots, \beta_n$ pertenecen a K. Luego

$$q(X) = (X - \beta_1)(X - \beta_2)\ldots(X - \beta_n) \quad \text{en} \quad K[X].$$

Por tanto, $K = F(\beta) = F(\beta_1) \subseteq F(\beta_1, \ldots, \beta_n) \subseteq K$, así que $K = F(\beta_1, \ldots, \beta_n)$. En otras palabras, K es el cuerpo de escisión del polinomio irreducible $q(X) \in F[X]$. □

Corolario 3.4. *Si $F \subseteq K \subseteq \mathbb{C}$ con $[K\colon F]$ finito, entonces*

$$\big|\mathrm{Gal}(K \,|\, F)\big| = [K\colon F] \quad \textit{si y sólo si} \quad K \,|\, F \textit{ es normal.}$$

► Ahora considérese la situación donde se presenta un cuerpo K con un juego de automorfismos dados. Nada se pierde al agregar el automorfismo trivial (la identidad sobre K) y los inversos y compuestos de los automorfismos dados inicialmente. Entonces, podemos suponer que los automorfismos dados forman un *grupo*.

Definición 3.5. Si K es un cuerpo y si G es un grupo de automorfismos de K, sea

$$K^G := \{\, a \in K : \sigma(a) = a \text{ para todo } \sigma \in G \,\},$$

el cual se llama el **cuerpo fijo** de K bajo la acción de G.

Es fácil comprobar que K^G es un subcuerpo de K. Fíjese que $0, 1 \in K^G$ porque $\sigma(0) = 0$ y $\sigma(1) = 1$ para todo automorfismo de K. Además, si $a, b \in K^G$, se verifica

$$\begin{aligned} \sigma(a+b) &= \sigma(a) + \sigma(b) = a + b, \\ \sigma(-a) &= -\sigma(a) = -a, \\ \sigma(ab) &= \sigma(a)\,\sigma(b) = ab, \\ \sigma(a/b) &= \sigma(a)/\sigma(b) = a/b \quad \text{si} \quad b \neq 0, \end{aligned}$$

para todo $\sigma \in G$, de modo que $a+b$, $-a$, ab, y a/b (si $b \neq 0$) están también en K^G.

Si $K \subseteq \mathbb{C}$ y si σ es un automorfismo de K, entonces $\sigma(1) = 1$ conlleva $\sigma(n) = n$ para $n \in \mathbb{Z}$ ya que σ es aditivo; en seguida, $\sigma(m/n) = \sigma(m)/\sigma(n) = m/n$ para $m, n \in \mathbb{Z}$ con $n \neq 0$ ya que σ es multiplicativo. Si G es un grupo de automorfismos de K, el cuerpo fijo K^G incluye al menos el subcuerpo mínimo $\mathbb{Q}$.

Ejemplo 3.6. La conjugación compleja $\kappa\colon z \mapsto \bar{z}$ es un automorfismo de $\mathbb{C}$ tal que $\kappa^2 = \mathrm{id}$. Luego $\{\mathrm{id}, \kappa\}$ es un grupo de automorfismos de $\mathbb{C}$ cuyo cuerpo fijo es $\mathbb{R} = \{z \in \mathbb{C} : \bar{z} = z\}$.

Ejemplo 3.7. ¿Cuáles son los automorfismos de $\mathbb{Q}(\sqrt[3]{2})$? Cada elemento $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ es de la forma $\alpha = p + q\sqrt[3]{2} + r\sqrt[3]{4}$ con $p, q, r \in \mathbb{Q}$. Si σ es un automorfismo de $\mathbb{Q}(\sqrt[3]{2})$, entonces

$$\sigma(p + q\sqrt[3]{2} + r\sqrt[3]{4}) = p + q\,\sigma(\sqrt[3]{2}) + r\,\sigma(\sqrt[3]{2})^2$$

porque σ deja fijo cada elemento de $\mathbb{Q}$. De este modo, se ve que σ queda determinado por $\sigma(\sqrt[3]{2})$. Además, el cubo de este elemento es $\sigma(\sqrt[3]{2})^3 = \sigma((\sqrt[3]{2})^3) = \sigma(2) = 2$, así que $\sigma(\sqrt[3]{2})$ es una raíz del polinomio $X^3 - 2$. De entre las tres raíces $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$ de este polinomio, sólo la primera pertenece a $\mathbb{Q}(\sqrt[3]{2})$. Por tanto $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, así que $\sigma = \mathrm{id}$: el único automorfismo de $\mathbb{Q}(\sqrt[3]{2})$ es la identidad.

Ejemplo 3.8. Sea $\zeta_5 := e^{2\pi i/5}$, una raíz quinta de 1. Se sabe que $[\mathbb{Q}(\zeta_5)\colon \mathbb{Q}] = 4$ porque el polinomio mínimo de ζ_5 sobre $\mathbb{Q}$ es $p(X) = X^4 + X^3 + X^2 + X + 1$. Cada automorfismo σ de $\mathbb{Q}(\zeta_5)$ deja fijo $\mathbb{Q}$ y por tanto queda determinado por $\sigma(\zeta_5)$. Ahora, $(\zeta_5^k)^5 = \zeta_5^{5k} = 1^k = 1$ para $k = 0, 1, 2, 3, 4$, así que

$$X^5 - 1 = (X-1)(X-\zeta_5)(X-\zeta_5^2)(X-\zeta_5^3)(X-\zeta_5^4).$$

Entonces el polinomio $p(X)$ escinde en $\mathbb{Q}(\zeta_5)$:

$$X^4 + X^3 + X^2 + X + 1 = \frac{X^5 - 1}{X - 1} = (X-\zeta_5)(X-\zeta_5^2)(X-\zeta_5^3)(X-\zeta_5^4).$$

Como $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4)$ de manera trivial, se ve que $\mathbb{Q}(\zeta_5)$ es el cuerpo de escisión de $p(X)$ sobre $\mathbb{Q}$ y por ende la extensión $\mathbb{Q}(\zeta_5) \,|\, \mathbb{Q}$ es normal.

Sea σ_k el automorfismo de $\mathbb{Q}(\zeta_5)$ determinado por $\sigma_k(\zeta_5) := \zeta_5^k$, para $k = 1, 2, 3, 4$. Entonces $\sigma_1 = \mathrm{id}$ y $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ es un grupo de orden 4. De hecho,

$$\begin{aligned}
\sigma_2^2(\zeta_5) &= \sigma_2(\sigma_2(\zeta_5)) = \sigma_2(\zeta_5^2) = \zeta_5^4,\\
\sigma_2^3(\zeta_5) &= \sigma_2(\zeta_5^4) = \zeta_5^8 = \zeta_5^3,\\
\sigma_2^4(\zeta_5) &= \sigma_2(\zeta_5^3) = \zeta_5^6 = \zeta_5.
\end{aligned}$$

Se concluye que $\sigma_2^2 = \sigma_4$, $\sigma_2^3 = \sigma_3$, $\sigma_2^4 = \mathrm{id}$. Por lo tanto, G es un grupo cíclico, generado por σ_2.

Fíjese que $\zeta_5^4 = e^{8\pi i/5} = e^{-2\pi i/5} = \bar{\zeta}_5$ y $\zeta_5^3 = e^{6\pi i/5} = e^{-4\pi i/5} = \bar{\zeta}_5^2$. Luego σ_4 coincide con la conjugación compleja κ sobre $\mathbb{Q}(\zeta_5)$.

Un elemento $\alpha = p + q\zeta_5 + r\zeta_5^2 + s\zeta_5^3 + t\zeta_5^4$ en $\mathbb{Q}(\zeta_5)$ queda en el cuerpo fijo $\mathbb{Q}(\zeta_5)^G$ si y sólo si $\sigma_2(\alpha) = \alpha$. Pero $\sigma_2(\alpha) = p + s\zeta_5 + q\zeta_5^2 + t\zeta_5^3 + r\zeta_5^4$ y $\{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$ es una base de $\mathbb{Q}(\zeta_5)$ sobre $\mathbb{Q}$, luego $\sigma_2(\alpha) = \alpha$ si y sólo si $q = s = t = r$, si y sólo si $\alpha = p + q(\zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4) = p - q \in \mathbb{Q}$. Por lo tanto, $\mathbb{Q}(\zeta_5)^G = \mathbb{Q}$.

► Los siguientes dos teoremas forman el corazón de la teoría de Galois. En sus enunciados se mantiene la condición de que todos los cuerpos en discusión son subcuerpos de $\mathbb{C}$. Más adelante, se ampliará el ámbito de estos teoremas al reemplazar esta hipótesis por la condición de "separabilidad".

Teorema 3.9 (Artin)**.** *Sea $K \subseteq \mathbb{C}$ y sea H un grupo finito de automorfismos de H. Entonces la extensión $K \mid K^H$ es normal y* $\mathrm{Gal}(K \mid K^H) = H$.

Demostración. Sea $\alpha \in K$ y sea $n := |H|$. Entonces $S := \{\, \sigma(\alpha) : \sigma \in H \,\}$ es un parta finita de K y su cardinalidad m cumple $m \leq n$. Sean $\sigma_1, \ldots, \sigma_m \in H$ unos automorfismos, con $\sigma_1 = \mathrm{id}$, tales que $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$ sean distintos, en cuyo caso $S = \{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}$. Si $\tau \in H$, entonces $S = \{\tau\sigma_1(\alpha), \ldots, \tau\sigma_m(\alpha)\}$ también, porque

$$\tau\sigma_i(\alpha) = \tau\sigma_j(\alpha) \implies \tau^{-1}(\tau\sigma_i(\alpha)) = \tau^{-1}(\tau\sigma_j(\alpha)) \implies \sigma_i(\alpha) = \sigma_j(\alpha) \implies i = j.$$

Defínase un polinomio $q(X) \in K[X]$, de grado m, por

$$q(X) := (X - \sigma_1(\alpha)) \ldots (X - \sigma_m(\alpha)) = \prod_{i=1}^{m} (X - \sigma_i(\alpha)).$$

Entonces $q^\tau(X) = \prod_{i=1}^m (X - \tau\sigma_i(\alpha)) = q(X)$ para cada $\tau \in H$, así que los coeficientes de $q(X)$ quedan fijos bajo cada τ, es decir, $q(X) \in K^H[X]$. Como $\sigma_1 = \mathrm{id}$, se ve que $(X - \alpha) \setminus q(X)$, de modo que $q(\alpha) = 0$. Se concluye que α es *algebraico* sobre el subcuerpo K^H, de grado no mayor que n. En fin, la extensión $K \mid K^H$ es algebraica.

Sea E un cuerpo con $K^H \subseteq E \subseteq K$ y $[E\colon K^H]$ finito. Entonces $E = K^H(\beta)$ para algún $\beta \in K$, por el Teorema 2.39. Luego $[E\colon K^H]$, que es el grado de β sobre K^H, cumple $[E\colon K^H] \leq n$. Entre todos estos cuerpos intermedios E, elíjase una tal que $[E\colon K^H]$ tenga el mayor valor posible. Si $\gamma \in K$, entonces $E(\gamma) = K^H(\beta, \gamma)$ es una extensión finita de K^H, porque $[E(\gamma)\colon K^H] = [E(\gamma)\colon E]\,[E\colon K^H]$ y γ es algebraica sobre K^H y por ende sobre E. La maximalidad de $[E\colon K^H]$ implica que $[E(\gamma)\colon K^H] = [E\colon K^H]$ y en consecuencia $[E(\gamma)\colon E] = 1$, es decir, $E(\gamma) = E$ o más simplemente, $\gamma \in E$. Se concluye que $E = K$ y por ende $[K\colon K^H]$ es *finito*.

Se puede entonces suponer que α es un elemento primitivo de la extensión $K \mid K^H$, con $K = K^H(\alpha)$. Los distintos automorfismos $\sigma \in H$ están determinados por sus valores $\sigma(\alpha)$, que deben ser distintos. En este caso, pues, $m = n$ y las n raíces de $q(X)$ son los conjugados de α sobre K^H. Por tanto, $q(X)$ es el polinomio mínimo de α sobre K^H y K es el cuerpo de escisión de $q(X) \in K^H(X)$, con $[K\colon K^H] = n$. Por la Proposición 3.3, la extensión $K \mid K^H$ es *normal*.

El Corolario 3.4 entonces muestra que $|\mathrm{Gal}(K \mid K^H)| = [K\colon K^H] = n = |H|$. Pero cada elemento de H es un K^H-automorfismo de K, así que H es un subgrupo de $\mathrm{Gal}(K \mid K^H)$. El conteo de los órdenes de los grupos muestra que $\mathrm{Gal}(K \mid K^H) = H$. □

Corolario 3.10. *Si $F \subseteq K \subseteq \mathbb{C}$ con $[K\colon F]$ finito, y si $G = \mathrm{Gal}(K \mid F)$, entonces la extensión $K \mid F$ es normal si y sólo si $K^G = F$.*

Demostración. Del Corolario 3.4 se obtiene $|G| \leq [K\colon F]$ con igualdad si y sólo si $K \,|\, F$ es normal. Del Teorema anterior, es $|G| = [K\colon K^G]$ y $K \,|\, K^G$ es normal. Cada $\sigma \in G$ deja F fijo, así que $F \subseteq K^G$ y por ende $[K\colon K^G] \leq [K\colon F]$, con igualdad si y sólo si $|G| = [K\colon F]$, si y sólo si $K \,|\, F$ es normal. □

Lema 3.11. *Si $F \subseteq E \subseteq K \subseteq \mathbb{C}$ y si $K \,|\, F$ es una extensión normal y finita, entonces la extensión $K \,|\, E$ es también normal y finita.*

Demostración. El grado $[K\colon E]$ es finito porque $[K\colon E]\,[E\colon F] = [K\colon F]$ es finito.

Como $K \,|\, F$ es normal, hay un polinomio $f(X) \in F[X]$ con raíces $\alpha_1, \ldots, \alpha_n \in K$ tal que $K = F(\alpha_1, \ldots, \alpha_n)$. Pero $f(X)$ es también un polinomio en $E[X]$ porque $F \subseteq E$ y $K = E(\alpha_1, \ldots, \alpha_n)$ también. Luego K es el cuerpo de escisión de un polinomio en $E[X]$, así que $K \,|\, E$ es normal. □

► Hay que recordar algunos conceptos básicos de la teoría de grupos. Si G es un grupo y si H es un subgrupo de G, se escribe $H \leq G$. El menor subgrupo posible es $\mathbf{1} = \{1\} \leq G$, que consta de la identidad $1 \in G$ y nada más; el mayor subgrupo es G mismo. Dado un subgrupo $H \leq G$ se puede formar "coclases" de H a la izquierda o bien a la derecha:

$$gH := \{\, gh : h \in G \,\}, \qquad Hg := \{\, hg : h \in G \,\},$$

para cada $g \in G$. Considérese el conjunto $G/H := \{\, gH : g \in G \,\}$ de coclases a la izquierda. Este es el cociente del conjunto G bajo la relación de equivalencia $R = \{\, (g, g') \in G \times G : g^{-1}g' \in H \,\}$ porque las coclases gH son las clases de equivalencia para R y por eso son disjuntos. El número de estas coclases se llama el *índice* $[G\colon H]$. Si G es un grupo finito, es evidente que $[G\colon H] = |G|/|H|$.

Definición 3.12. Un subgrupo $H \leq G$ es un **subgrupo normal** de G, escrito $H \trianglelefteq G$, si vale $gH = Hg$ para cada $g \in G$, o equivalentemente, si $g^{-1}Hg = H$ para todo $g \in G$.

Aquí $g^{-1}Hg := \{\, g^{-1}hg : h \in H \,\}$ es un subgrupo de G, llamado *subgrupo conjugado* de H. Entonces $H \trianglelefteq G$ si y sólo si el único subgrupo conjugado de H es H mismo. Fíjese que $gH = Hg$ si y sólo si cada producto hg con $h \in H$ es de la forma gh' para algún $h' \in H$. Evidentemente,

$$hg = gh' \iff h' = g^{-1}hg,$$

así que $gH = Hg$ si y sólo si $g^{-1}Hg = H$.

Si G es un grupo *abeliano* (es decir, conmutativo), cualquier subgrupo de G es normal.

Si $H \trianglelefteq G$, entonces el conjunto G/H tiene una estructura de grupo, llamado el *grupo cociente* de G por H, al definir el producto $(g_1H)(g_2H) := g_1g_2H$. Para que este producto esté bien definido, se requiere que para cada $h_1, h_2 \in H$ haya un elemento $h_3 \in H$ tal que

$$(g_1h_1)(g_2h_2) = g_1(h_1g_2)h_2 = g_1(g_2h_3)h_2 = g_1g_2(h_3h_2) \in g_1g_2H,$$

dado necesariamente por $h_3 = g_2^{-1}h_1g_2 \in g_2^{-1}Hg_2$. El orden del grupo cociente es el índice del subgrupo, es decir, $|G/H| = [G\colon H]$.

Con estos preparativos, podemos abordar el resultado central del curso.

Teorema 3.13 (Teorema Principal de la Teoría de Galois)**.** *Sea $K \mid F$ una extensión normal y finita (con $K \subseteq \mathbb{C}$, por ahora). Entonces hay una biyección $\Phi_{K|F}$ entre los cuerpos intermedios E con $F \subseteq E \subseteq K$ y los subgrupos $H \leq \mathrm{Gal}(K \mid F)$, dado por $\Phi_{K|F} \colon E \mapsto \mathrm{Gal}(K \mid E)$ y en el sentido inverso por $\Phi_{K|F}^{-1} = \Psi_{K|F} \colon H \mapsto K^H$, con las siguientes propiedades:*

(a) $E = K^{\mathrm{Gal}(K|E)}$;

(b) $H = \mathrm{Gal}(K \mid K^H)$;

(c) $[K : E] = \big|\mathrm{Gal}(K \mid E)\big|$;

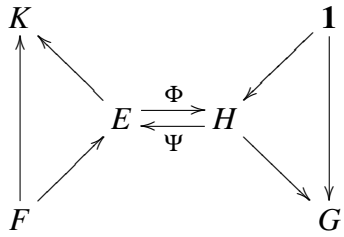
(d) $[E : F] = [\mathrm{Gal}(K \mid F) : \mathrm{Gal}(K \mid E)]$;

(e) $E \mid F$ *es normal si y sólo si* $\mathrm{Gal}(K \mid E) \trianglelefteq \mathrm{Gal}(K \mid F)$;

(f) $\mathrm{Gal}(E \mid F) \simeq \mathrm{Gal}(K \mid F) \big/ \mathrm{Gal}(K \mid E)$ *si* $E \mid F$ *es normal.*

Demostración. Primero, debe notarse que (a) es equivalente a la relación $\Psi_{K|F} \circ \Phi_{K|F} = \mathrm{id}$ sobre la familia de cuerpos intermedios de la extensión $K \mid F$; y que (b) es equivalente a la relación $\Phi_{K|F} \circ \Psi_{K|F} = \mathrm{id}$ sobre la familia de subgrupos de $\mathrm{Gal}(K \mid F)$. Por lo tanto, la comprobación de (a) y (b) establecerá que $\Phi_{K|F}$ y $\Psi_{K|F}$ son biyecciones mutuamente inversos.

Esta correspondencia entre cuerpos intermedios y subgrupos puede ilustrarse con el siguiente esquema, en donde $G := \mathrm{Gal}(K \mid F)$.



(3.3)

Ad (a): Fíjese que $\mathrm{Gal}(K \mid E)$ es un subgrupo de $\mathrm{Gal}(K \mid F)$, porque consta de automorfismos de K que dejan E fijo y luego dejan F fijo también. Como $K \mid F$ es normal, el Lema 3.11 muestra que $K \mid E$ es normal, y entonces el Corolario 3.10 asegura que $K^{\mathrm{Gal}(K|E)} = E$.

Ad (b): Este es el Teorema 3.9.

Obsérvese que $\Phi_{K|F}$ es sobreyectivo, porque si $H \leq G$, entonces $F \subseteq K^H \subseteq K$ y la parte (b) muestra que $\Phi_{K|F}(K^H) = \mathrm{Gal}(K \mid K^H) = H$.

También, $\Phi_{K|F}$ es inyectivo, porque si E y E' son cuerpos intermedios de $K \mid F$, la parte (a) muestra que

$$\Phi_{K|F}(E) = \Phi_{K|F}(E') \implies \mathrm{Gal}(K \mid E) = \mathrm{Gal}(K \mid E') \implies K^{\mathrm{Gal}(K|E)} = K^{\mathrm{Gal}(K|E')} \implies E = E'.$$

Ad (c): Sigue del Corolario 3.4 porque $K \mid E$ es normal, por el Lema 3.11.

Ad (d): De la Proposición 2.3 y la parte (c) se obtiene

$$[E:F] = \frac{[K:F]}{[K:E]} = \frac{|\operatorname{Gal}(K\,|\,F)|}{|\operatorname{Gal}(K\,|\,E)|} = [\operatorname{Gal}(K\,|\,F) : \operatorname{Gal}(K\,|\,E)].$$

Ad (e): La extensión $E\,|\,F$ es finita, porque $[E:F] \leq [K:F]$. Si es también normal, entonces hay un elemento $\alpha \in E$ tal que $E = F(\alpha)$ y todos los conjugados de α (sobre F) están en E.

Sea $\sigma \in \operatorname{Gal}(K\,|\,F)$. Entonces la restricción $\sigma|_E$ es un homomorfismo de E en K que deja F fijo, es decir, $\sigma|_E \in \operatorname{Hom}_F(E,K)$. Además, σ queda determinado por $\sigma(\alpha)$, que es un conjugado de α. Por tanto, $\sigma|_E$ lleva E en E.

Ahora, si $\tau \in \operatorname{Gal}(K\,|\,E)$, entonces $\sigma^{-1}\tau\sigma\colon K \to K$ es un F-automorfismo de K tal que

$$\sigma^{-1}\tau\sigma(\alpha) = \sigma^{-1}(\tau(\sigma(\alpha))) = \sigma^{-1}(\sigma(\alpha)) = \alpha$$

ya que τ deja E fijo y $\sigma(\alpha) \in E$. Entonces $\sigma^{-1}\tau\sigma$ deja fijo a todo $F(\alpha) = E$ y por ende $\sigma^{-1}\tau\sigma \in \operatorname{Gal}(K\,|\,E)$. La implicación

$$\tau \in \operatorname{Gal}(K\,|\,E) \implies \sigma^{-1}\tau\sigma \in \operatorname{Gal}(K\,|\,E) \quad \text{para todo} \quad \sigma \in \operatorname{Gal}(K\,|\,F)$$

dice precisamente que $\operatorname{Gal}(K\,|\,E) \trianglelefteq \operatorname{Gal}(K\,|\,F)$.

Ad (f): Si la extensión $E\,|\,F$ es normal, la aplicación de restricción $\theta(\sigma) := \sigma|_E$ es un *homomorfismo de grupos* $\theta\colon \operatorname{Gal}(K\,|\,F) \to \operatorname{Gal}(E\,|\,F)$. Ahora,

$$\sigma \in \ker\theta \iff \sigma|_E = \mathrm{id}_E \iff \sigma \text{ deja } E \text{ fijo} \iff \sigma \in \operatorname{Gal}(K\,|\,E).$$

Hay un isomorfismo[2] de grupos $\operatorname{Gal}(K\,|\,F)\big/\ker\theta \simeq \operatorname{im}\theta$. Por conteo de órdenes de grupos y grados de extensiones, se obtiene

$$|\operatorname{im}\theta| = \frac{|\operatorname{Gal}(K\,|\,F)|}{|\ker\theta|} = \frac{|\operatorname{Gal}(K\,|\,F)|}{|\operatorname{Gal}(K\,|\,E)|} = \frac{[K:F]}{[K:E]} = [E:F] = |\operatorname{Gal}(E\,|\,F)|,$$

donde la última igualdad sigue de la normalidad de $E\,|\,F$. Por lo tanto, θ es sobreyectivo y el isomorfismo canónico produce $\operatorname{Gal}(K\,|\,F)\big/\operatorname{Gal}(K\,|\,E) \simeq \operatorname{Gal}(E\,|\,F)$. □

Corolario 3.14. *Sea $K\,|\,F$ una extensión normal y finita, con $K \subseteq \mathbb{C}$. Entonces la cantidad de cuerpos intermedios distintos es finita.*

Demostración. Por el Teorema anterior, basta observar que la cantidad de subgrupos del grupo finito $\operatorname{Gal}(K\,|\,F)$ es finita. □

Lema 3.15. *Sea $K\,|\,F$ una extensión normal y finita, con $K \subseteq \mathbb{C}$. Las correspondencias de Galois $\Phi_{K|F}$ y $\Phi_{K|F}$ son decrecientes: si $F \subseteq E \subseteq E' \subseteq K$, entonces $\operatorname{Gal}(K\,|\,E') \leq \operatorname{Gal}(K\,|\,E)$; y si $H \leq H' \leq \operatorname{Gal}(K\,|\,F)$, entonces $K^{H'} \subseteq K^H$.* ⊟

[2] Si $\theta\colon G \to G'$ es un homomorfismo de grupos, hay un isomorfismo canónico $\operatorname{im}\theta \simeq G/\ker\theta$. Este es el llamado "primer teorema de isomorfismo de grupos".

3.2 Grupo de Galois de un polinomio

Definición 3.16. Sea $f(X) \in F[X]$, donde F es un subcuerpo de $\mathbb{C}$, tal que $f(X)$ tenga raíces distintas en $\mathbb{C}$. Sea K_f el cuerpo de escisión de $f(X)$ sobre F. Entonces $\mathrm{Gal}(K_f \,|\, F)$ se llama el **grupo de Galois del polinomio** $f(X)$ sobre F.

Lema 3.17. *Si* $G = \mathrm{Gal}(K_f \,|\, F)$ *y si* $\operatorname{gr} f(X) = m$, *entonces* $|G| \leq m!$.

Demostración. Sea $f(X) = a_m(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_m)$ la descomposición en $K_f[X]$ de $f(X)$ en factores de primer grado. Entonces $\alpha_1, \dots, \alpha_m \in K_f$ son distintas y es $K_f = F(\alpha_1, \dots, \alpha_m)$. Cada elemento $\sigma \in G$ queda determinado por los valores $\sigma(\alpha_1), \dots, \sigma(\alpha_m)$. Se sabe que cada $\sigma(\alpha_j)$ es un conjugado de α_j sobre F, así que $\sigma(\alpha_j) \in \{\alpha_1, \dots, \alpha_m\}$ para cada $j = 1, \dots, m$.

Denótese por S_m el grupo de permutaciones de m cosas distintas: concretamente, se puede identificar S_m con las biyecciones del conjunto de m elementos $\{\alpha_1, \dots, \alpha_m\}$ en sí mismo. Defínase una aplicación $\theta\colon G \to S_m$ por

$$\theta(\sigma) := \sigma\big|_{\{\alpha_1,\dots,\alpha_m\}}.$$

La operación de restricción preserva la composición de funciones: en particular, $\theta(\sigma\tau) = \theta(\sigma) \circ \theta(\tau)$ para $\sigma, \tau \in G$. Por tanto, $\theta\colon G \to S_m$ es un homomorfismo de grupos. Como σ es determinado por $\sigma(\alpha_1), \dots, \sigma(\alpha_m)$, se ve que θ es inyectivo. Por ende, θ es un isomorfismo del grupo G en el subgrupo $\theta(G)$ de S_m. Se concluye que

$$|G| = |\theta(G)| \leq |S_m| = m!\,. \qquad \square$$

Ejemplo 3.18. ¿Cuál es el grupo de Galois de $f(X) = \underline{X^3 - 2}$ sobre $\mathbb{Q}$?

Ya se sabe que $K_f = \mathbb{Q}(\sqrt[3]{2}, \omega)$ donde $\omega = \frac{1}{2}(-1 + \sqrt{3}\,i) = e^{2\pi i/3}$ es una raíz cúbica de 1. El Lema anterior dice que $|G| \leq 3! = 6$; por otro lado, sabemos que

$$|G| = [\mathbb{Q}(\sqrt[3]{2}, \omega)\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega)\colon \mathbb{Q}(\sqrt[3]{2})]\,[\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}] = 2 \cdot 3 = 6.$$

(Si $E = \mathbb{Q}(\sqrt[3]{2})$, es $[E(\omega)\colon E] = 2$ ya que $X^2 + X + 1$ es el polinomio mínimo de ω sobre E.)

Cada $\sigma \in G$ está determinado por sus valores $\sigma(\sqrt[3]{2})$, $\sigma(\omega)$ en los generadores de K_f sobre $\mathbb{Q}$. Además, como $\sigma(\alpha)$ es un conjugado de α sobre $\mathbb{Q}$ para los dos casos $\alpha = \sqrt[3]{2}$ y $\alpha = \omega$, se obtiene:

$$\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}, \qquad \sigma(\omega) \in \{\omega, \omega^2\}.$$

Hay exactamente 6 maneras de elegir $\sigma(\sqrt[3]{2})$ y $\sigma(\omega)$ en estos conjuntos, que determinan los 6 elementos de G. Denotando $\sigma_0 = \mathrm{id}$, podemos exhibirlos en la Tabla 1.

Para calcular el isomorfismo $\theta\colon G \to S_3$, se observa el efecto de cada σ_j sobre las tres raíces $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, $\alpha_3 = \omega^2\sqrt[3]{2}$ de $X^3 - 2$. Por ejemplo,

$$\begin{aligned}
\sigma_4(\sqrt[3]{2}) &= \omega^2\sqrt[3]{2},\\
\sigma_4(\omega\sqrt[3]{2}) &= \sigma_4(\omega)\,\sigma_4(\sqrt[3]{2}) = \omega \cdot \omega^2\sqrt[3]{2} = \sqrt[3]{2},\\
\sigma_4(\omega^2\sqrt[3]{2}) &= \sigma_4(\omega^2)\,\sigma_4(\sqrt[3]{2}) = \omega^2 \cdot \omega^2\sqrt[3]{2} = \omega\sqrt[3]{2},
\end{aligned}$$

Tabla 1: Grupo de Galois de X^3-2

$\sigma \in G$	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
$\sigma(\sqrt[3]{2})$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$
$\sigma(\omega)$	ω	ω^2	ω	ω^2	ω	ω^2
$\theta(\sigma) \in S_3$	id	(23)	(123)	(12)	(132)	(13)

o bien $\sigma_4(\alpha_1)=\alpha_3$, $\sigma_4(\alpha_3)=\alpha_2$, $\sigma_4(\alpha_2)=\alpha_1$. Es decir, la permutación $\theta(\sigma_4)$ es el ciclo (132). Las demás entradas de la última fila de la Tabla 1 se calculan de manera similar.

► Antes de seguir, es oportuno hacer un pequeño catálogo de los grupos finitos finitos más conocidos. Cualquier grupo finito tiene una *presentación por generadores y relaciones*, en la forma

$$G = \langle x_1, \ldots, x_m : R_1, \ldots, R_p \rangle,$$

donde los generadores $x_1, \ldots, x_m$ son elementos de G y cada R_j es una relación entre estos generadores.

Definición 3.19. Si n es un número entero positivo, el **grupo cíclico** de n elementos, con generador g, es

$$C_n = \{1, g, g^2, \ldots, g^{n-1}\} = \langle g : g^n = 1 \rangle.$$

En este caso, sólo se requiere un generador y una relación $g^n = 1$. Fíjese que si $\mathrm{mcd}(k,n) = 1$ con $k \in \{1, \ldots, n-1\}$, entonces las n potencias de g^k son distintas, y se puede escribir $C_n = \{1, g^k, g^{2k}, \ldots, g^{(n-1)k}\}$ también: luego, g^k es otro generador de C_n.

Un ejemplo concreto de este grupo abstracto es el grupo de las n raíces n-ésimas de 1, que también[3] se denota por C_n:

$$C_n = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} = \{\, e^{2k\pi i/n} : k = 0, 1, \ldots, n-1 \,\}. \tag{3.4}$$

Otra instancia de este grupo abstracto es el grupo *aditivo* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ de los residuos de división por n.

Definición 3.20. El **grupo de permutaciones** S_n del conjunto $\{1, 2, \ldots, n\}$ cumple $|S_n| = n!$ por definición del factorial.

Una *transposición* es una permutación que cambia dos objetos entre sí, dejando fijos a los demás: la transposición $j \leftrightarrow k$ se denota (jk). Cualquier permutación en S_n es un producto de transposiciones (de varias maneras). Una permutación se llama *par* si es el producto de

[3] Este es un típico "abuso de notación", en donde la etiqueta C_n se usa para denotar un objeto abstracto y también una de sus manifestaciones concretas.

un número par de transposiciones. Para ver que el concepto de paridad está bien definido, considérese el polinomio

$$h(X_1,\ldots,X_n) := \prod_{1\le i<j\le n}(X_i - X_j).$$

Si $\sigma \in S_n$, entonces, al aplicar φ_σ de (1.18):

$$\begin{aligned}\varphi_\sigma(h(X_1,\ldots,X_n)) &= h(X_{\sigma(1)},\ldots,X_{\sigma(n)}) = \prod_{i<j}(X_{\sigma(i)} - X_{\sigma(j)}) \\ &= \pm\prod_{r<s}(X_r - X_s) = \pm h(X_1,\ldots,X_n),\end{aligned}$$

en donde el signo $\pm$ es $+$ si y sólo si la permutación σ es par; denótese este signo $\pm$ por $(-1)^\sigma$. Como $\varphi_{\sigma\tau} = \varphi_\sigma \circ \varphi_\tau$, se obtiene de esta manera un homomorfismo $\sigma \mapsto (-1)^\sigma$ de S_n en el grupo $\{+1,-1\} = C_2$. El *núcleo* de este homomorfismo es el subgrupo A_n de las permutaciones pares, llamado el **grupo alternante** de n objetos. En cuanto núcleo de un homomorfismo, es un subgrupo normal: $A_n \lhd S_n$.

Como $S_n/A_n \simeq C_2$ por el isomorfismo canónico, se ve que $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}\,n!$.

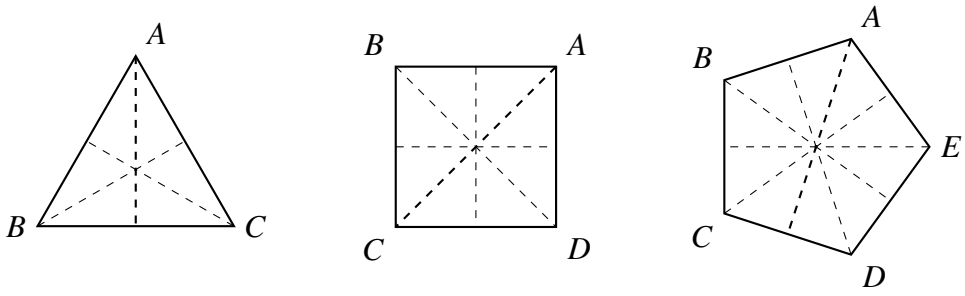


Figura 5: Ejes de reflexión de polígonos regulares

Definición 3.21. El **grupo diédrico** D_n es el grupo de isometrías de un polígono regular de n vértices. El centro del polígono es un punto fijo de cualquier isometría. Las isometrías son de dos tipos: rotaciones y reflexiones. Si los vértices son $A,B,C,\ldots,K$ en un orden contrario a reloj alrededor del centro, sea r la rotación por un ángulo $2\pi/n$ que lleva A a B, B a C, etc. Sea s la reflexión que deja fija el vértice A (véase la Figura 3.21). Entonces rsr^{-1} es una reflexión que deja fijo el vértice B. Se puede ver que el grupo D_n es generado por los dos elementos r y s y que no es abeliano.

Las reflexiones en D_n son los elementos $s, rs, r^2s, \ldots, r^{n-1}s$. Para ver que esta lista es completa, fíjese que el elemento srs es la rotación que lleva B en A, porque $srs(B) = sr(K) = s(A) = A$ y $srs(A) = sr(A) = s(B) = K$; por ende, $srs = r^{-1} = r^{n-1}$. Luego, $sr = (srs)s^{-1} = (srs)s = r^{n-1}s$. En resumen,

$$D_n = \langle r,s : r^n = 1,\ s^2 = 1,\ sr = r^{n-1}s\rangle. \tag{3.5}$$

En consecuencia, $D_n = \{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$, porque la tercera relación permite escribir cualquier producto de los generadores en la forma $r^k s^l$ y las otras relaciones obligan $k < n$ y $l < 2$. En fin, $|D_n| = 2n$.

Definición 3.22. Si G y H son dos grupos, el **producto directo** $G \times H$ es el producto cartesiano de los conjuntos G y H, con la operación de grupo $(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$.

Definición 3.23. Hay 5 grupos no isomorfos de orden 8. Uno de ellos es C_8 y el grupo diédrico D_4 es otro. Los productos directos $C_2 \times C_4$ y $C_2 \times C_2 \times C_2$ son otros dos grupos, ambos abelianos, de orden 8. Para completar la lista, se introduce el **grupo de cuaterniones**

$$Q := \{1, -1, i, -i, j, -j, k, -k\}, \quad \text{con} \quad i^2 = j^2 = k^2 = ijk = -1.$$

De estas igualdades se obtiene $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$. Este Q es un grupo no abeliano, que no es isomorfo a D_4 porque Q posee seis elementos de orden 4 y uno de orden 2, mientras D_4 posee dos elementos de orden 4 y cinco de orden 2. Una posible presentación de Q es

$$Q = \langle i, j : i^4 = 1,\ j^4 = 1,\ ji = i^3 j \rangle.$$

► Continuamos con otro ejemplo de la identificación de un grupo de Galois de un polinomio.

Ejemplo 3.24. ¿Cuál es el grupo de Galois de $f(X) = \underline{X^4 + 2}$ sobre $\mathbb{Q}$?

Sea $\zeta := \zeta_8 = e^{\pi i/4}$, una raíz octava de 1, Obsérvese que $\zeta^2 = i$ y que $\zeta = (1+i)/\sqrt{2}$, por la trigonometría del círculo de radio 1. La factorización de $X^4 + 2$ en $\mathbb{C}[X]$ es

$$X^4 + 2 = (X^2 - i\sqrt{2})(X^2 + i\sqrt{2}) = (X - \zeta\sqrt[4]{2})(X + \zeta\sqrt[4]{2})(X - i\zeta\sqrt[4]{2})(X + i\zeta\sqrt[4]{2}). \quad (3.6)$$

Fíjese que $\mathbb{Q}(\sqrt[4]{2}, \zeta) = \mathbb{Q}(\sqrt[4]{2}, i)$ porque $i = \zeta(\sqrt[4]{2})^2 - 1$ mientras $\zeta = \frac{1}{2}(1+i)(\sqrt[4]{2})^2$. Es evidente que $K_f \subseteq \mathbb{Q}(\sqrt[4]{2}, \zeta)$. No es difícil expresar $\sqrt[4]{2}$ y también i como polinomios en las raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ que aparecen al lado derecho de (3.6). Se concluye que $K_f = \mathbb{Q}(\sqrt[4]{2}, i)$.

Cada $\sigma \in G = \mathrm{Gal}(K_f \,|\, \mathbb{Q})$ queda determinado por sus valores en los generadores, $\sigma(\sqrt[4]{2})$ y $\sigma(i)$. Los polinomios mínimos de los generadores sobre $\mathbb{Q}$ son $X^4 - 2$ y $X^2 + 1$, respectivamente. De ahí se obtiene sus conjugados, para concluir que

$$\sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}, \qquad \sigma(i) \in \{i, -i\}.$$

Hay exactamente 8 maneras de elegir $\sigma(\sqrt[4]{2})$ y $\sigma(i)$ en estos conjuntos, que determinan los 8 elementos de G. Defínase $\sigma, \tau \in G$ por

$$\begin{aligned} \sigma(\sqrt[4]{2}) &:= i\sqrt[4]{2}, \qquad & \sigma(i) &:= i, \\ \tau(\sqrt[4]{2}) &:= \sqrt[4]{2}, \qquad & \tau(i) &:= -i. \end{aligned}$$

Es evidente que $\sigma^4 = \mathrm{id}$ y que $\tau^2 = \mathrm{id}$, mientras $\sigma^2 \neq \mathrm{id}$: el elemento σ es de orden 4 en G y τ es de orden 2. Además,

$$\begin{aligned} \tau\sigma(\sqrt[4]{2}) &= -i\sqrt[4]{2}, \qquad & \tau\sigma(i) &= -i, \\ \sigma^3\tau(\sqrt[4]{2}) &= i^3\sqrt[4]{2}, \qquad & \sigma^3\tau(i) &= -i. \end{aligned}$$

Luego $\tau\sigma = \sigma^3\tau$ en G.

Por lo tanto, los elementos σ y τ cumplen las relaciones (3.5) que definen el grupo D_4. En consecuencia, hay un homomorfismo $\eta : D_4 \to G$ determinado por $\eta(r) := \sigma$, $\eta(s) := \tau$. Es evidente que $G = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$, así que η es sobreyectivo. La inyectividad de η sigue del isomorfismo canónico $D_4/\ker\eta \simeq \operatorname{im}\eta = G$, porque $|D_4| = 8 = |G|$ conlleva $|\ker\eta| = 1$. Por tanto, η es un isomorfismo de grupos y G es una copia del grupo diédrico D_4.

3.3 Extensiones ciclotómicas

Definición 3.25. Sea $n \in \mathbb{N}$ con $n \geq 2$. Un residuo $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ es una *unidad* si posee un inverso multiplicativo $\overline{l}$ tal que $\overline{k}\,\overline{l} = \overline{1}$. Si $k \in \mathbb{N}$, es evidente que $\overline{k}$ es una unidad en $\mathbb{Z}/n\mathbb{Z}$ si y sólo si $\mathrm{mcd}(k,n) = 1$. Las unidades forman un grupo bajo multiplicación:

$$U_n := \{\, \overline{k} \in \mathbb{Z}/n\mathbb{Z} : \mathrm{mcd}(k,n) = 1 \,\}. \tag{3.7}$$

Obsérvese que U_n es un grupo abeliano, ya que $\mathbb{Z}/n\mathbb{Z}$ es un anillo conmutativo.

La llamada **función tociente** de Euler[4] es la función $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ definido[5] por $\varphi(1) := 1$ y $\varphi(n) := |U_n|$ si $n \geq 2$.

Lema 3.26. *La función tociente tiene las siguientes propiedades:*

(a) Si p es primo y si $r \in \mathbb{N}^*$, entonces $\varphi(p^r) = p^r - p^{r-1}$.

(b) Si $m,n \in \mathbb{N}^*$ con $\mathrm{mcd}(m,n) = 1$, entonces $\varphi(mn) = \varphi(m)\,\varphi(n)$.

Demostración. Ad (a): Si $k \in \{0,1,\ldots,p^r-1\}$, entonces $\mathrm{mcd}(k,p^r) = 1$ si y sólo si $p \nmid k$. Fíjese que hay p^{r-1} múltiplos de p en $\{0,1,\ldots,p^r-1\}$.

Ad (b): Sea $k \in \{1,\ldots,mn-1\}$. Tómese $a,b \in \mathbb{Z}$ tales que $am + bn = 1$. Entonces $k = \overline{amk + bnk}$. Por división, hay $r \in \{0,1,\ldots,m-1\}$ y $s \in \{0,1,\ldots,n-1\}$ únicos tales que $bnk \equiv r \bmod m$, $amk \equiv s \bmod n$. Entonces $k \equiv r \bmod m$, $k \equiv s \bmod n$, y la correspondencia $\overline{k} \leftrightarrow (\overline{r},\overline{s})$ es un isomorfismo de anillos entre $\mathbb{Z}/mn\mathbb{Z}$ y $(\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$.

Ahora, si $\mathrm{mcd}(k,mn) = 1$, entonces $\mathrm{mcd}(k,m) = 1$ y $\mathrm{mcd}(k,n) = 1$. Además,

$$\mathrm{mcd}(r,m) = \mathrm{mcd}(bnk,m) = \mathrm{mcd}(k,m) = 1,$$

y de modo similar $\mathrm{mcd}(s,n) = \mathrm{mcd}(amk,n) = \mathrm{mcd}(k,n) = 1$. Por restricción, la correspondencia $\overline{k} \leftrightarrow (\overline{r},\overline{s})$ también define un isomorfismo de grupos entre U_{mn} y $U_m \times U_n$. Por ende, $\varphi(mn) = |U_{mn}| = |U_m|\,|U_n| = \varphi(m)\varphi(n)$. □

Si $n \in \mathbb{N}$ con $n \geq 2$ tiene la factorización prima $n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$, entonces el valor $\varphi(n)$ de la función tociente es

$$\varphi(n) = \prod_{j=1}^{k} p_j^{r_j-1}(p_j - 1) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right).$$

[4] La palabra "tociente" (más bien, *totient* en inglés) fue inventada por James Joseph Sylvester en 1883 para designar la función de Euler.

[5] Aquí se sigue el convenio francés para los números naturales: $\mathbb{N} = \{0,1,2,\ldots\}$ y $\mathbb{N}^* = \{1,2,\ldots\} = \mathbb{N}\setminus\{0\}$.

Definición 3.27. Sea $n \in \mathbb{N}^*$. Un número complejo $\zeta \in \mathbb{C}$ es una **raíz n-ésima primitiva de 1** si $\zeta^n = 1$ y si $\zeta^m \neq 1$ cuando $m \setminus n$ con $1 < m < n$.

Escríbase $\zeta_n := e^{2\pi i/n}$. Entonces ζ es una raíz n-ésima primitiva de 1 si y sólo si $\zeta = \zeta_n^k$ con $\mathrm{mcd}(k,n) = 1$, si y sólo si ζ es un generador del grupo C_n de todas las raíces n-ésimas de 1.

Definición 3.28. Sea $n \in \mathbb{N}^*$. El **polinomio ciclotómico** $\Phi_n(X) \in \mathbb{C}[X]$ se define como[6]

$$\Phi_n(X) := \prod_{\substack{\zeta^n=1 \\ \zeta \text{ primitiva}}} (X - \zeta) = \prod_{\overline{k} \in U_n} (X - \zeta_n^k).$$

Es evidente que $\mathrm{gr}\,\Phi_n = \varphi(n)$.

Ejemplo 3.29. Como $\zeta_1 = 1$, $\zeta_2 = -1$, $\zeta_3 = \omega$, $\zeta_4 = i$ y $\zeta_6 = \frac{1}{2}(1 + \sqrt{3}\,i)$, se obtiene

$$\begin{aligned}
\Phi_1(X) &= X - 1, \\
\Phi_2(X) &= X + 1, \\
\Phi_3(X) &= (X - \omega)(X - \omega^2) = X^2 + X + 1, \\
\Phi_4(X) &= (X - i)(X + i) = X^2 + 1, \\
\Phi_5(X) &= (X - \zeta_5)(X - \zeta_5^2)(X - \zeta_5^3)(X - \zeta_5^4) = X^4 + X^3 + X^2 + X + 1, \\
\Phi_6(X) &= (X - \zeta_6)(X - \zeta_6^5) = X^2 - 2(\Re\zeta_6)X + 1 = X^2 - X + 1.
\end{aligned}$$

Lema 3.30. *Sea $n \in \mathbb{N}^*$. En $\mathbb{C}[X]$, se cumple la identidad*

$$X^n - 1 = \prod_{d \setminus n} \Phi_d(X). \tag{3.8}$$

Demostración. Si $k \in \{0, 1, \ldots, n-1\}$, el orden de ζ_n^k como elemento del grupo C_n es d si $\zeta_n^{dk} = 1$ pero $\zeta_n^{ck} \neq 1$ para $c = 1, \ldots, d-1$. Se escribe $o(\zeta_n^k) = d$ para denotar este hecho: es evidente que d es un divisor de n, por el teorema de Lagrange. De igual manera pero con la notación aditiva, se escribe $o(\overline{k}) = d$ para $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ si $dk \equiv 0 \bmod n$ pero $ck \not\equiv 0 \bmod n$ cuando $c = 1, \ldots, d-1$.

Ahora se puede descomponer el polinomio $X^n - 1$ así:

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \zeta_n^k) = \prod_{d \setminus n} \Big(\prod_{o(\overline{k})=d} (X - \zeta_n^k) \Big). \tag{3.9}$$

Si $o(\overline{k}) = d$, entonces $(\zeta_n^k)^d = 1$, así que ζ_n^k es una potencia de ζ_d. Hay una igualdad de conjuntos

$$\{1, \zeta_n^k, \zeta_n^{2k}, \ldots, \zeta_n^{(d-1)k}\} = \{1, \zeta_d, \zeta_d^2, \ldots, \zeta_d^{d-1}\}$$

y los elementos de orden exactamente d del lado izquierdo son los elementos primitivos del lado derecho. Luego, el término entre paréntesis en (3.9) es igual a $\Phi_d(X)$. □

[6] La palabra *ciclotómico* viene del verbo griego κυκλοτόμειν, que significa "cortar el círculo": guarda relación, como luego se verá, con el proceso de dividir la circunferencia del círculo en n arcos iguales.

Corolario 3.31. *Para todo $n \in \mathbb{N}^*$, el polinomio $\Phi_n(X)$ pertenece a $\mathbb{Z}[X]$.*

Demostración. La fórmula (3.8) permite un *cálculo recursivo* de $\Phi_n(X)$, porque

$$\Phi_n(X) = (X^n - 1) \Big/ \prod_{d \backslash n,\ d<n} \Phi_d(X)$$

y el destino de la recursión es $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.

De esta última fórmula, se ve por inducción sobre n que $\Phi_n(X) \in \mathbb{Q}[X]$: el lado derecho es (por la hipótesis inductiva) un cociente de polinomios en $\mathbb{Q}[X]$, que coincide con un polinomio $\Phi_n(X)$. Denotando el denominador a la derecha por $g(X)$, se obtiene $X^n - 1 = \Phi_n(X)\, g(X)$. Esta es una división en el anillo $\mathbb{Q}[X]$, sin residuo: el divisor es $g(X)$, el cociente es $\Phi_n(X)$.

Ahora, tanto el dividendo $X^n - 1$ como el divisor $g(X)$ son polinomios *mónicos* en $\mathbb{Z}[X]$ — la hipótesis inductiva permite afirmar que $g(X) \in \mathbb{Z}[X]$— así que el cociente $\Phi_n(X)$ también tiene coeficientes enteros. □

Como ejemplos de esta recursión, se puede calcular ahora:

$$\begin{aligned}
\Phi_2(X) &= \frac{X^2-1}{X-1} = X+1, \\
\Phi_3(X) &= \frac{X^3-1}{X-1} = X^2+X+1, \\
\Phi_4(X) &= \frac{X^4-1}{\Phi_1(X)\,\Phi_2(X)} = \frac{X^4-1}{(X-1)(X+1)} = X^2+1, \\
\Phi_5(X) &= \frac{X^5-1}{X-1} = X^4+X^3+X^2+X+1, \\
\Phi_6(X) &= \frac{X^6-1}{\Phi_1(X)\,\Phi_2(X)\,\Phi_3(X)} = \frac{X^6-1}{(X-1)(X+1)(X^2+X+1)} = X^2-X+1.
\end{aligned}$$

Proposición 3.32. *El polinomio $\Phi_n(X)$ es irreducible en $\mathbb{Z}[X]$, para todo n.*

Demostración. Sea $\zeta \in \mathbb{C}$ una raíz n-ésima primitiva de 1. Entonces $\Phi_n(\zeta) = 0$ porque $(X - \zeta)$ es un factor de $\Phi_n(X)$, por definición.

Sea p un primo tal que $p \backslash n$. Entonces ζ^p es otra raíz n-ésima de 1, la cual también es primitiva, porque $\mathrm{mcd}(k,n) = 1$ implica $\mathrm{mcd}(pk,n) = 1$. Por tanto, $\Phi_n(\zeta^p) = 0$.

Sea $q(X)$ el polinomio mínimo de ζ sobre $\mathbb{Q}$, así que $q(X) \setminus \Phi_n(X)$. Si $q(\zeta^p) \neq 0$, entonces $q(X)$ es un factor propio de $\Phi_n(X)$, y por eso hay un polinomio $h(X) \in \mathbb{Z}[X]$ (por ser cociente de dos polinomios mónicos) con $\mathrm{gr}\, h(X) \geq 1$, tal que $\Phi_n(X) = h(X)\, q(X)$.

Puesto que $q(\zeta^p) \neq 0$, se obtiene $h(\zeta^p) = 0$, de modo que ζ es una raíz del polinomio $X \mapsto h(X^p)$. En consecuencia, hay $k(X) \in \mathbb{Z}[X]$ tal que $h(X^p) = k(X)\, q(X)$.

El siguiente paso es la reducción de los coeficientes de estos polinomios a sus residuos módulo p. Sea $\theta : \mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ el homomorfismo cociente (de anillos): concretamente, $\theta(k) = \overline{k} \in \mathbb{F}_p$. A cada polinomio $f(X) \in \mathbb{Z}[X]$ le corresponde un polinomio $f^\theta(X) \in \mathbb{F}_p[X]$,

y la correspondencia $f(X) \mapsto f^\theta(X)$ es un homomorfismo de anillos de $\mathbb{Z}[X]$ en $\mathbb{F}_p[X]$. Por ejemplo, vale $h^\theta(X^p) = k^\theta(X)\,q^\theta(X)$ en el anillo $\mathbb{F}_p[X]$. Si $h(X) = a_0 + a_1X + \cdots + a_mX^m$, entonces

$$\begin{aligned} h(X)^p &\equiv (a_0 + a_1X + a_2X^2 + \cdots + a_mX^m)^p \\ &\equiv a_0^p + a_1^pX^p + a_2^pX^{2p} + \cdots + a_m^pX^{mp} \\ &\equiv a_0 + a_1X^p + a_2X^{2p} + \cdots + a_mX^{mp} \equiv h(X^p) \bmod p, \end{aligned}$$

donde el segundo renglón sigue porque $\binom{p}{k} \equiv 0 \bmod p$ para $k = 1, \ldots, p-1$, mientras el tercer renglón es consecuencia de la conocida[7] relación: $a^p \equiv a \bmod p$ para $a \in \mathbb{Z}$. En otras palabras, vale $h^\theta(X)^p = h^\theta(X^p)$ en $\mathbb{F}_p[X]$.

Ahora, la relación $h^\theta(X)^p = k^\theta(X)\,q^\theta(X)$ dice que $\operatorname{mcd}(h^\theta(X), q^\theta(X)) \neq 1$ en el anillo entero $\mathbb{F}_p[X]$. Si $g^\theta(X)$ es un factor común de $h^\theta(X)$ y $q^\theta(X)$ con $\operatorname{gr} g^\theta(X) \geq 1$, entonces

$$g^\theta(X)^2 \setminus \Phi_n^\theta(X) \setminus (X^n - \overline{1}) \quad \text{en} \quad \mathbb{F}_p[X].$$

Por tanto, $g^\theta(X)$ divide la derivada $\overline{n}X^{n-1}$ de $(X^n - \overline{1})$. Pero $\overline{n} \neq \overline{0}$ en $\mathbb{F}_p$, porque $p \setminus n$ por hipótesis. Sin embargo, esto implicaría que $g^\theta(X)$ divide $\operatorname{mcd}(X^{n-1}, X^n - \overline{1}) = 1$, lo cual es imposible porque $g^\theta(X)$ no es constante.

Esta contradicción muestra que $q(\zeta^p) = 0$ toda vez que p es primo con $p \setminus n$. Cada k con $\operatorname{mcd}(k,n) = 1$ es un producto $k = p_1p_2 \ldots p_s$, donde $p_j \setminus n$ para $j = 1, \ldots, s$. El argumento anterior muestra que $q(\zeta^{p_1}) = 0$. Al reemplazar ζ por ζ^{p_1}, también primitivo, y ζ^{p_1} por su potencia $\zeta^{p_1p_2}$, se obtiene $q(\zeta^{p_1p_2}) = 0$. Repitiendo este proceso s veces, se llega a que $q(\zeta^k) = 0$. En fin, cada raíz primitiva n-ésima de 1 es una raíz de $q(X)$. Se concluye que $q(X) = \Phi_n(X)$ y, en particular, que $\Phi_n(X)$ es irreducible. □

Corolario 3.33. *Si ζ es una raíz n-ésima primitiva de 1, entonces $\Phi_n(X)$ es el polinomio mínimo de ζ sobre $\mathbb{Q}$.* □

Corolario 3.34. *Si ζ es una raíz n-ésima primitiva de 1, entonces $\mathbb{Q}(\zeta)$ es el cuerpo de escisión de $\Phi_n(X)$ sobre $\mathbb{Q}$. La extensión $\mathbb{Q}(\zeta) \,|\, \mathbb{Q}$ es normal, con $[\mathbb{Q}(\zeta) \colon \mathbb{Q}] = \varphi(n)$.* □

Definición 3.35. Si ζ es una raíz n-ésima primitiva de 1, la extensión $\mathbb{Q}(\zeta) \,|\, \mathbb{Q}$ se llama una **extensión ciclotómica** de $\mathbb{Q}$.

Proposición 3.36. *Si ζ es una raíz n-ésima primitiva de 1, entonces* $\operatorname{Gal}(\mathbb{Q}(\zeta) \,|\, \mathbb{Q}) \simeq U_n$.

Demostración. Sea $\sigma \in G = \operatorname{Gal}(\mathbb{Q}(\zeta) \,|\, \mathbb{Q})$; obsérvese que σ queda determinado por el valor $\sigma(\zeta)$. Este valor es un conjugado de ζ sobre $\mathbb{Q}$ y como tal, es también un generador del grupo C_n de raíces n-ésimas de 1. Por tanto, $\sigma(\zeta) = \zeta^k$ donde $k \in \mathbb{N}$ con $\operatorname{mcd}(k,n) = 1$.

Defínase un homomorfismo de grupos $\theta \colon G \to U_n$ por $\theta(\sigma) := \overline{k}$. En efecto, si $\tau \in G$ con $\theta(\tau) = \overline{l}$, entonces $\sigma\tau(\zeta) = \sigma(\zeta^l) = \zeta^{kl}$, así que $\theta(\sigma\tau) = \overline{kl} = \overline{k}\,\overline{l} = \theta(\sigma)\theta(\tau)$.

Ahora, si $\sigma \in \ker\theta$, entonces $\overline{k} = \overline{1}$, así que $\zeta^k = \zeta$ y por tanto $\sigma = \mathrm{id}$. Luego, θ es inyectivo. Como $|G| = [\mathbb{Q}(\zeta) \colon \mathbb{Q}] = \varphi(n) = |U_n|$, la aplicación θ es además biyectivo. Luego θ es el isomorfismo deseado entre G y U_n. □

[7] La relación $a^p \equiv a \bmod p$ fue observado por Fermat. En su forma equivalente: $a^{p-1} \equiv 1 \bmod p$ si $\operatorname{mcd}(a,p) = 1$, es una consecuencia del Teorema de Lagrange porque el grupo U_p cumple $|U_p| = p - 1$.

Proposición 3.37. *Sea $\zeta \in \mathbb{C}$ una raíz n-ésima primitiva de 1. Entonces ζ es constructible (por regla y compás) sólo si $n = 2^m p_1 p_2 \dots p_k$ donde los p_j son primos impares distintos, de la forma $p = 2^{2^l} + 1$: por ejemplo, $p = 3, 5, 17, 257$ ó 65537.*

Demostración. Por el Corolario 2.42, la condición necesaria para constructibilidad de ζ es que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^s$ para algún $s \in \mathbb{N}$. El Corolario 3.34 transforma este criterio en la ecuación numérica $\varphi(n) = 2^s$.

Ahora, sea $n = 2^m p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ la factorización prima de n, donde $p_1, \dots, p_k$ son los primos impares distintos que dividen n. Del Lema 3.26 se obtiene

$$\varphi(n) = \varphi(2^m)\,\varphi(p_1^{r_1}) \dots \varphi(p_k^{r_k}) = 2^{m-1}\, p_1^{r_1-1}(p_1 - 1) \dots p_k^{r_k-1}(p_k - 1).$$

Se requiere que este producto no contenga factores impares. Para eso, es necesario y suficiente que cada $r_j = 1$ (cada factor primo impar de n aparece una sola vez) y que cada p_j sea de la forma $2^t + 1$.

Ahora, si $t = uv$ donde $u \neq 1$ es impar, $2^t + 1$ no es primo, porque

$$2^t + 1 = (2^v)^u + 1 = (2^v + 1)(2^{v(u-1)} - 2^{v(u-2)} + \dots + 2^{2v} - 2^v + 1),$$

en donde los u términos del segundo factor a la derecha tienen signos alternantes. Luego $2^t + 1$ puede ser primo sólo si t mismo es de la forma $t = 2^l$ para algún $l \in \mathbb{N}$. Los casos $l = 0, 1, 2, 3, 4$ dan $2^{2^l} + 1 = 3, 5, 17, 257, 65537$, los cuales son números primos. □

Fermat especuló que $2^{2^5} + 1 = 2^{32} + 1 = 4294967297$ sería primo, pero no pudo demostrarlo. Euler logró demostrar lo contrario: este número es divisible por $641 = 10 \cdot 2^6 + 1$; de hecho, $2^{32} + 1 = 641 \cdot 6700417$ es un producto de dos primos.[8] Se sabe que $2^{2^l} + 1$ no es primo para $l = 5, 6, \dots, 32$; en cada caso, tiene un factor de la forma $k 2^{l+1} + 1$.

El inverso de la Proposición 3.37 también es cierto: dado n de la forma permitida, hay una construcción por regla y compás de un n-gono regular. En primer lugar, es fácil bisecar un arco de círculo dado, lo cual permite fabricar un $2n$-gono regular a partir de un n-gono regular; por tanto, basta examinar el caso en donde n es impar. En segundo lugar, si $\mathrm{mcd}(m, n) = 1$ y si $am + bn = 1$, entonces $2\pi/mn = a(2\pi/n) + b(2\pi/m)$; de ahí, los vértices del m-gono y del n-gono regulares determinan los vértices del mn-gono regular. Basta, entonces, examinar el caso $n = 2^{2^l} + 1$ sea un primo de Fermat. En este caso, como $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p) \,|\, \mathbb{Q}) \simeq U_{2^{2^l}}$, hay una cadena de subgrupos $G = G_0 \geq G_1 \geq \dots \geq G_r = \mathbf{1}$ donde cada $[G_i : G_{i-1}] = 2$. Por tanto, hay una torre de subcuerpos $\mathbb{Q} = E_0 \subset E_1 \subset \dots \subset E_r = \mathbb{Q}(\zeta_n)$ tal que cada $E_i \,|\, E_{i-1}$ es una extensión de grado 2: se puede construir elementos de E_i a partir de elementos de E_{i-1} por regla y compás.

Las construcciones para los casos $n = 3$ y $n = 5$ (triángulo y pentágono regulares) aparecen en los *Elementos* de Euclides (Proposiciones I.1 y IV.11, respectivamente.) El caso $n = 17$ fue resuelto por Gauss (*Disquisitiones Arithmeticae*, arts. 354 y 363).[9]

[8] Los números $3, 5, 17, 257, 65537$ se llaman *primos de Fermat*; fueron mencionados en una carta de Pierre de Fermat a Marin Mersenne, escrito el 25 de diciembre de 1640. No se sabe aún (en el 2006) si $2^{2^{33}} + 1$ es primo o compuesto. Para el estado actual de la cuestión, véase el sitio `http://www.prothsearch.net/fermat.html`.

[9] Véase también: Felix Klein, *Famous Problems of Elementary Geometry* (1895); Dover, New York, 1956.

3.4 Extensiones cíclicas

Definición 3.38. Sea $K \mid F$ una extensión normal y finita con $K \subseteq \mathbb{C}$. Se dice que $K \mid F$ es una *extensión abeliana* si $\mathrm{Gal}(K \mid F)$ es un grupo abeliano. Se dice que $K \mid F$ es una **extensión cíclica** si $\mathrm{Gal}(K \mid F)$ es un *grupo cíclico*.

Cada extensión ciclotómica $\mathbb{Q}(\zeta) \mid \mathbb{Q}$ es abeliana. De hecho, si ζ es una raíz n-ésima primitiva de 1, el grupo $\mathrm{Gal}(\mathbb{Q}(\zeta) \mid \mathbb{Q}) \simeq U_n$ es abeliano. Además, si $E \mid \mathbb{Q}$ es normal, con $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\zeta)$, el grupo $\mathrm{Gal}(E \mid \mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta) \mid \mathbb{Q}) \,/\, \mathrm{Gal}(\mathbb{Q}(\zeta) \mid E)$ es abeliano. Un famoso teorema de Kronecker y Weber, que no se demuestra aquí, dice que toda extensión abeliana de $\mathbb{Q}$ es un cuerpo intermedio de alguna extensión ciclotómica.

El grupo U_n es cíclico para algunos n, pero no para todos. Por ejemplo, si $n = 2^k$ con $k \geq 2$, se sabe que $U_n \simeq C_{2^{k-1}} \times C_2 \not\simeq C_{2^k}$. Para n primo, el grupo U_n sí es cíclico, en vista de la Proposición siguiente.

Lema 3.39. *Si* $\mathrm{mcd}(m,n) = 1$*, entonces* $C_m \times C_n \simeq C_{mn}$.

Demostración. Sea h un generador de C_m y sea k un generador de C_n. Entonces $h^r = 1$ en C_m si y sólo si $m \setminus r$; también, $k^s = 1$ en C_n si y sólo si $n \setminus s$.

En el producto directo $C_m \times C_n$, la potencia $(h,k)^t = (h^t, k^t)$ es igual a la identidad $(1,1)$ si y sólo si $h^t = 1$ y $k^t = 1$, si y sólo si $m \setminus t$ y $n \setminus t$. Esta condición es equivalente a que $mn \setminus t$, porque $\mathrm{mcd}(m,n) = 1$. Entonces $C_m \times C_n$ es un grupo abeliano de orden mn que posee un elemento (h,k) de orden mn. Por tanto, este grupo es cíclico, con generador (h,k).

Por otro lado, en el grupo cíclico C_{mn}, sea z un generador y considérese los subgrupos

$$H := \{ x \in C_{mn} : x^m = 1 \} = \{1, z^n, z^{2n}, \ldots, z^{(m-1)n}\} \simeq C_m,$$
$$K := \{ y \in C_{mn} : y^n = 1 \} = \{1, z^m, z^{2m}, \ldots, z^{m(n-1)}\} \simeq C_n.$$

Al escribir $1 = am + bn$ con $a, b \in \mathbb{Z}$, se ve que $z^k = z^{kbn} z^{kam}$ para todo $k = 0, 1, \ldots, mn-1$. Es fácil comprobar que la aplicación $z^k \mapsto (z^{kbn}, z^{kam})$ es un isomorfismo de grupos que lleva C_{mn} en $H \times K \simeq C_m \times C_n$. □

Proposición 3.40. *Sea F un cuerpo finito y sea $F^\times := F \setminus \{0\}$ su grupo multiplicativo. Entonces $F^\times$ es un grupo cíclico.*

Demostración. El grupo multiplicativo $F^\times$ es abeliano porque F es un anillo conmutativo. Si $|F^\times| = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$, sea $H_j := \{ a \in F : a^{p_j^{r_j}} = 1 \}$ para $j = 1, \ldots, k$. Entonces cada H_j es un subgrupo de $F^\times$ y no es difícil comprobar que $F^\times \simeq H_1 \times H_2 \times \cdots \times H_k$.

Ahora sea H un subgrupo de $F^\times$ de orden p^r, para algún primo p que divide $|F^\times|$. El orden de cada elemento de H es un divisor de p^r: sea $b \in H$ de orden máximo p^s, con $s \leq r$. Entonces $a^{p^s} = 1$ para todo $a \in H$. Esto dice que el polinomio $X^{p^s} - 1 \in F[X]$ tiene al menos p^r raíces, las cuales son todos los elementos de H. Por tanto $s = r$, y el grupo H es cíclico con generador b.

Se concluye que cada H_j es un subgrupo cíclico de $F^\times$, con órdenes relativamente primos entre sí. El Lema anterior muestra que $F^\times \simeq H_1 \times H_2 \times \cdots \times H_k$ también es cíclico. □

Corolario 3.41. *Si p es primo, entonces $U_p = \mathbb{F}_p^\times \simeq C_{p-1}$.* □

Proposición 3.42. *Sea ζ una raíz n-ésima primitiva de 1. Sea $F \subseteq \mathbb{C}$ un cuerpo tal que $\zeta \in F$ y sea $a \in F$. Si $\beta \in \mathbb{C}$ es una raíz del polinomio $X^n - a$, entonces $F(\beta) \,|\, F$ es una extensión cíclica. Si $d = [F(\beta)\colon F]$, entonces $\beta^d \in F$.*

Demostración. Por definición, β es una raíz n-ésima de a. Todas las raíces n-ésimas de a son $\{\, \zeta^k\beta : k = 0, 1, \ldots, n-1 \,\} \subset F(\beta)$. Por lo tanto, $F(\beta) = F(\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta)$ es el cuerpo de escisión de $X^n - a$ sobre F. Por la Proposición 3.3, la extensión $F(\beta) \,|\, F$ es normal.

Si $G = \mathrm{Gal}(F(\beta) \,|\, F)$, cada $\sigma \in G$ queda determinado por $\sigma(\beta)$ y además $\sigma(\beta) = \zeta^k\beta$ para algún $k \in \{0, 1, \ldots, n-1\}$. Defínase una aplicación $\theta\colon G \to C_n$ por $\theta(\sigma) := \zeta^k$. Si $\tau(\beta) = \zeta^l\beta$, entonces

$$\sigma\tau(\beta) = \sigma(\tau(\beta)) = \sigma(\zeta^l\beta) = \zeta^l\,\sigma(\beta) = \zeta^l\zeta^k\beta = \zeta^{k+l}\beta,$$

así que $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$: entonces θ es un homomorfismo de grupos. Fíjese que en este cálculo $\sigma(\zeta^l) = \zeta^l$ porque $\zeta^l \in F$.

Ahora θ es inyectivo, porque

$$\sigma \in \ker\theta \implies \theta(\sigma) = 1 \implies \sigma(\beta) = \beta \implies \sigma = \mathrm{id}\,.$$

Luego $G \simeq \theta(G) \leq C_n$. Como subgrupo de un grupo cíclico, G también es un grupo cíclico y por ende la extensión $F(\beta) \,|\, F$ es cíclica.

Si σ es un generador de G, sea d el orden de σ, de modo que $\zeta^{dk} = 1$ pero $\zeta^{ck} \neq 1$ para $c = 1, \ldots, d-1$. Obsérvese que $d \setminus n$ ya que $dk \setminus n$. Ahora,

$$\sigma(\beta^d) = \sigma(\beta)^d = (\zeta^k\beta)^d = \zeta^{dk}\beta^d = \beta^d,$$

por ende $\sigma^r(\beta^d) = \beta^d$ para todo $\sigma^r \in G$. Esto dice que $\beta^d \in F(\beta)^G = F$. □

Corolario 3.43. *Si el polinomio $X^n - a$ es irreducible en $F[X]$, entonces* $\mathrm{Gal}(F(\beta) \,|\, F) \simeq C_n$.

Demostración. En este caso, $X^n - a$ es el polinomio mínimo de β sobre F, así que $|G| = n$ y el homomorfismo $\theta\colon G \to C_n$ es biyectivo. □

La Proposición 3.42 dice que si $\mathbb{Q}(\zeta) \subseteq F$, entonces una extensión de F por una raíz n-ésima de $a \in F$ es una extensión cíclica. En seguida mostraremos un resultado inverso, que una extensión cíclica de F es generado por una raíz n-ésima de algún $a \in F$, en el caso de que n sea un número primo.

Proposición 3.44. *Sean $p \in \mathbb{N}$ un número primo, ζ una raíz p-ésima de 1, y $F \subseteq \mathbb{C}$ un cuerpo tal que $\zeta \in F$. Si $K \,|\, F$ es una extensión cíclica con $[K\colon F] = p$, entonces $K = F(\beta)$ donde $\beta^p \in F$.*

Demostración. Sea $\alpha \in K$ con $\alpha \notin F$. Si $f(X) \in F[X]$ es el polinomio mínimo de α sobre F, entonces $\mathrm{gr}\, f(X) > 1$ y $\mathrm{gr}\, f(X) \setminus p$, así que $\mathrm{gr}\, f(X) = p$ y por ende $F(\alpha) = K$.

Sea σ un generador de $\mathrm{Gal}(K \,|\, F) \simeq C_p$. Para $j = 1, \ldots, p$, defínase $\alpha_j = \sigma^{j-1}(\alpha)$. Fíjese que $\sigma(\alpha_j) = \alpha_{j+1}$ para $j = 1, \ldots, p-1$ y que $\sigma(\alpha_p) = \alpha = \alpha_1$.

Para cada $k = 0, 1, \ldots, p-1$, considérese el *resolvente de Lagrange*:

$$\lambda_k := \alpha_1 + \zeta^k \alpha_2 + \zeta^{2k} \alpha_3 + \cdots + \zeta^{(p-1)k} \alpha_p. \tag{3.10}$$

Al aplicar σ a este elemento de K, se obtiene

$$\begin{aligned}\sigma(\lambda_k) &= \sigma(\alpha_1) + \zeta^k \sigma(\alpha_2) + \zeta^{2k} \sigma(\alpha_2) + \cdots + \zeta^{(p-1)k} \sigma(\alpha_p) \\ &= \alpha_2 + \zeta^k \alpha_3 + \zeta^{2k} \alpha_4 + \cdots + \zeta^{(p-1)k} \alpha_1 = \zeta^{-k} \lambda_k,\end{aligned}$$

y en consecuencia, $\sigma(\lambda_k^p) = \zeta^{-kp} \lambda_k^p = \lambda_k^p$, lo cual implica que $\lambda_k^p \in K^G = F$.

Las fórmulas (3.10), para $k = 0, 1, \ldots, p-1$, definen un sistema de ecuaciones lineales para las incógnitas $\alpha_1, \ldots, \alpha_p$. Al enumerar las raíces p-ésimas de 1 como $\{\zeta_1, \zeta_2, \ldots, \zeta_p\} := \{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\}$, este sistema tiene la siguiente forma:

$$\begin{aligned}
\alpha_1 + \zeta_1 \alpha_2 + \zeta_1^2 \alpha_3 + \cdots + \zeta_1^{p-1} \alpha_p &= \lambda_0, \\
\alpha_1 + \zeta_2 \alpha_2 + \zeta_2^2 \alpha_3 + \cdots + \zeta_2^{p-1} \alpha_p &= \lambda_1, \\
\alpha_1 + \zeta_3 \alpha_2 + \zeta_3^2 \alpha_3 + \cdots + \zeta_3^{p-1} \alpha_p &= \lambda_2, \\
\vdots \qquad\qquad & \qquad \vdots \\
\alpha_1 + \zeta_p \alpha_2 + \zeta_p^2 \alpha_3 + \cdots + \zeta_p^{p-1} \alpha_p &= \lambda_{p-1}.
\end{aligned}$$

El determinante de la matriz de coeficientes es un *determinante de Vandermonde*:[10]

$$\begin{vmatrix} 1 & \zeta_1 & \zeta_1^2 & \cdots & \zeta_1^{p-1} \\ 1 & \zeta_2 & \zeta_2^2 & \cdots & \zeta_2^{p-1} \\ 1 & \zeta_3 & \zeta_3^2 & \cdots & \zeta_3^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_p & \zeta_p^2 & \cdots & \zeta_p^{p-1} \end{vmatrix} = \prod_{i<j} (\zeta_j - \zeta_i). \tag{3.11}$$

Para el cálculo de este determinante, obsérvese que:

(a) se puede reemplazar la fila j por la diferencia (fila j − fila i) sin afectar el valor del determinante;

(b) $(\zeta_j - \zeta_i)$ es un factor de esta nueva fila y por ende es un factor del determinante;

(c) entonces el producto al lado derecho es un divisor del determinante;

(d) por la expansión en la fila j, el determinante es un polinomio de grado $p-1$ en cada variable ζ_j, así que es un múltiplo constante del lado derecho;

(e) el coeficiente del término diagonal $\zeta_2 \zeta_3^2 \ldots \zeta_p^{p-1}$ en la expansión del lado derecho es $+1$, así que dicha constante también es $+1$.

[10] Este determinante fue usado por Alexandre Vandermonde en 1770, precisamente para invertir las expresiones (3.10) que Lagrange en su monografía de 1771 llamó "resolventes".

Como $\zeta_1, \ldots, \zeta_n$ son distintos, se ve que $\prod_{i<j}(\zeta_j - \zeta_i) \neq 0$. Por tanto, el sistema de ecuaciones (3.10) tiene solución única, de la forma

$$\alpha_j = c_{j0}\,\lambda_0 + c_{j1}\,\lambda_1 + \cdots + c_{j,p-1}\,\lambda_{p-1} \quad \text{con cada} \quad c_{jk} \in F.$$

Ahora, $\alpha_1 = \alpha \notin F$, así que al menos un índice k con $\lambda_k \notin F$; colóquese $\beta := \lambda_k$. Entonces $F(\beta) = K$, por el argumento al inicio de esta demostración, y también $\beta^p = \lambda_k^p \in F$. □

► Podemos aplicar esta teoría de extensiones cíclicas a la solución de la ecuación cúbica $X^3 + pX + q = 0$, con $p, q \in F \subseteq \mathbb{C}$. Supóngase que este polinomio es irreducible en $F[X]$, lo cual implica que sus raíces $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ son distintas. Obsérvese que $\alpha_1 + \alpha_2 + \alpha_3 = 0$. El discriminante de este polinomio mónico es

$$D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 = -4p^3 - 27q^2 \in F,$$

por la fórmula (1.27) y el Ejemplo 1.33.

Lema 3.45. *Si $X^3 + pX + q$ es irreducible en $F[X]$, con raíces $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, y si*

$$\delta := (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1),$$

entonces el cuerpo de escisión de $X^3 + pX + q$ sobre F es $F(\alpha_1, \delta)$, con $[F(\alpha_1, \delta) : F] = 3$ si $\delta \in F$, mientras $[F(\alpha_1, \delta) : F] = 6$ si $\delta \notin F$.

Demostración. El cuerpo de escisión de $X^3 + pX + q$ sobre F es $K = F(\alpha_1, \alpha_2, \alpha_3)$. Fíjese que $\delta^2 = D$. Además, $\alpha_1 \notin F$ porque $X^3 + pX + q$ es irreducible en $F[X]$; en particular, es $\alpha_1 \neq 0$. Ahora bien,

$$(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_1) = \alpha_1(\alpha_2 + \alpha_3) - \alpha_1^2 - \alpha_2\alpha_3 = -2\alpha_1^2 + \frac{q}{\alpha_1} \in F(\alpha_1),$$

luego $\alpha_2 - \alpha_3 = \delta/(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_1) \in F(\alpha_1, \delta)$. También, $\alpha_2 + \alpha_3 = -\alpha_1 \in F(\alpha_1)$: se concluye que $\alpha_2, \alpha_3 \in F(\alpha_1, \delta)$ y por ende $K = F(\alpha_1, \delta)$.

Como $X^3 + pX + q$ es el polinomio mínimo de α_1, se ve que $[F(\alpha_1) : F] = 3$. Si $\delta \in F$, entonces $K = F(\alpha_1)$ es de grado 3 sobre F. Si $\delta \notin F$, entonces $[F(\delta) : F] = 2$ porque $\delta^2 = D \in F$. Luego $[K : F]$ es divisible por 2, $\delta \notin F(\alpha_1)$ y $[K : F(\alpha_1)] = 2$ también, por ende $[K : F] = 6$. □

Como $\delta^2 = D$, de modo que $\delta = \pm\sqrt{D}$, el grado es 6 si y sólo si D no es un cuadrado en F. En este caso, la extensión $K \,|\, F$ es normal y finita, el grupo $G = \mathrm{Gal}(K \,|\, F)$ permuta las raíces $\alpha_1, \alpha_2, \alpha_3$ y es de orden 6: es evidente que $G \simeq S_3$. El subgrupo A_3 de permutaciones pares es un grupo cíclico de orden 3 generado por el automorfismo σ determinado por

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

Se ve que $\sigma(\delta) = \delta$, así que $E := F(\delta)$ es el cuerpo fijo del subgrupo $H := \{\mathrm{id}, \sigma, \sigma^2\} \simeq A_3$. Entonces $[E : F] = [G : H] = 2$. En consonancia con la Proposición 3.44 para $p = 2$, se ve que $E = F(\delta)$ y $\delta^2 \in F$.

Supóngase ahora que $\omega = e^{2\pi i/3} \in F$. Como la extensión $K \mid E$ es normal, se obtiene $\mathrm{Gal}(K \mid E) = \mathrm{Gal}(K \mid K^H) = H$, el cual es un grupo cíclico de orden 3. La Proposición 3.44 garantiza que hay $\beta \in K$ tal que $K = E(\beta)$ y $\beta^3 \in E$. Además, se puede elegir β entre los tres resolventes de Lagrange para el polinomio cúbico $X^3 + pX + q$. En el caso presente, es $\lambda_0 = \alpha_1 + \alpha_2 + \alpha_3 = 0$, de modo que debe tomarse $\beta := \lambda_1 = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$ (alternativamente, se puede tomar $\beta' = \lambda_2 = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$).

Para calcular $\beta^3 \in E$, se usa la tecnología de los polinomios simétricos. En efecto, usando la relación $\delta = \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 - \alpha_1^2\alpha_2 - \alpha_2^2\alpha_3 - \alpha_3^2\alpha_1$ se obtiene

$$\begin{aligned}
\beta^3 &= (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3 \\
&= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) + 6\alpha_1\alpha_2\alpha_3 \\
&= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 - \frac{3}{2}(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 + \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) - \frac{3\sqrt{3}\,i}{2}\delta + 6\alpha_1\alpha_2\alpha_3 \\
&= -\frac{27}{2}q - \frac{3}{2}(\omega - \omega^2)\delta \in E.
\end{aligned}$$

La alternativa $\beta' = \lambda_2$ conduce a $\beta'^3 = -\frac{27}{2}q + \frac{3}{2}(\omega - \omega^2)\delta$.

Las raíces cúbicas de β^3 son β, $\omega\beta$ y $\omega^2\beta$. Al tomar $\alpha_1 = \frac{1}{2}(\lambda_1 + \lambda_2)$, etc., se obtienen $\alpha_1, \alpha_2, \alpha_3$ en términos de q y δ. Finalmente, como $i\delta = \pm\sqrt{-D} = \pm\sqrt{4p^3 + 27q^2}$, se recuperan las fórmulas de Cardano para $\alpha_1, \alpha_2, \alpha_3$.

3.5 Resolución de ecuaciones por radicales

El trabajo principal de Évariste Galois, escrito entre los años 1829 y 1831 y publicado póstumamente en 1846, contiene un criterio para decidir si una ecuación polinomial es o no es resoluble por radicales. Brevemente, una "resolución por radicales" quiere decir la exhibición de una fórmula para las raíces, similar a la fórmula cuadrática y las fórmulas de Cardano y Ferrari, en términos de los coeficientes del polinomio, mediante las cuatro operaciones aritméticas básicas y la extracción de un número finito de raíces. Desde Ferrari a Galois, se buscaba una fórmula para resolver la ecuación *general* de quinto grado, hasta que los trabajos de Paolo Ruffini (1799) y Niels Henrik Abel (1824) señalaron que esa fórmula general no existía. Galois logró confirmar sus resultados, pero a la vez señaló un método para obtener resoluciones de algunas clases particulares de ecuaciones de alto grado.

Galois usó un *resolvente* más general de los resolventes de Lagrange. En lenguaje moderno, su resolvente es una función racional (eventualmente, un polinomio) $\beta = g(\alpha_1, \ldots, \alpha_n)$ de las raíces α_j de la ecuación, que es un *elemento primitivo* del cuerpo de escisión, es decir, que $F(\beta) = F(\alpha_1, \ldots, \alpha_n)$. Para hallar un resolvente de este tipo, él estudio el efecto de someter β a un juego de permutaciones o "sustituciones" de las raíces que él llamaba *grupo* de sustituciones. Reconoció que, dependiendo de la ecuación polinomial dada, no hace falta usar todas las sustituciones posibles, siempre que sea posible combinar e invertir las sustituciones del grupo elegido. En breve, identificó lo que hoy en día se llama el "grupo de Galois" del polinomio dado. En seguida, la estructura de este grupo fue la clave para descifrar la ecuación.

► Antes de seguir, conviene repasar algunos conceptos de la teoría de grupos finitos.

Definición 3.46. Un grupo G es un **grupo resoluble** si hay una cadena decreciente finita de subgrupos

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r = \mathbf{1}, \tag{3.12}$$

tal que $G_i \trianglelefteq G_{i-1}$ para $i = 1, 2, \ldots, r$, y cada grupo cociente G_{i-1}/G_i es un grupo *abeliano*.

Ejemplo 3.47. (a) Cualquier grupo abeliano es resoluble. La cadena trivial $G \trianglerighteq \mathbf{1}$ sirve para el caso abeliano.

(b) El grupo S_3 es resoluble, con cadena $S_3 \triangleright A_3 \triangleright \mathbf{1}$, ya que los cocientes $S_3/A_3 \simeq C_2$ y $A_3/\mathbf{1} = A_3 \simeq C_3$ son abelianos.

(c) El grupo S_4 es resoluble, con cadena $S_4 \triangleright A_4 \triangleright V \triangleright \mathbf{1}$, donde el tercer subgrupo es $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Los cocientes son $S_4/A_4 \simeq C_2$, $A_4/V \simeq C_3$ y $V \simeq C_2 \times C_2$.

(d) El grupo diédrico D_n es resoluble, con cadena $D_n \triangleright C_n \triangleright \mathbf{1}$. Los cocientes abelianos son $D_n/C_n \simeq C_2$ y C_n.

Si $H \trianglelefteq G$, entonces G/H es abeliano si y sólo si $(gH)(hH) = (hH)(gH)$ o bien $ghH = hgH$ para todo $g, h \in G$, si y sólo si $ghg^{-1}h^{-1}H = H$ o bien $ghg^{-1}h^{-1} \in H$ para todo $g, h \in G$.

Definición 3.48. Para cualquier grupo G, el *subgrupo derivado* G' es el subgrupo generado por todos los elementos de la forma $ghg^{-1}h^{-1}$, para $g, h \in G$. Obsérvese que $G' = \mathbf{1}$ si y sólo si G es abeliano; y que

$$k(ghg^{-1}h^{-1})k^{-1} = kgk^{-1}\,khk^{-1}\,kg^{-1}k^{-1}\,kh^{-1}k^{-1} = (kgk^{-1})(khk^{-1})(kgk^{-1})^{-1}(khk^{-1})^{-1},$$

para todo $k \in G$, así que $G' \trianglelefteq G$. Se escribe $G^{(2)} = G'' := (G')'$, $G^{(3)} = G''' := (G'')'$ y en general $G^{(r+1)} := (G^{(r)})'$.

Fíjese que el grupo G/G' es abeliano, por la observación anterior. Además, si $H \trianglelefteq G$ con cociente abeliano G/H, entonces $G' \leq H$.

Por otro lado, si $G' \leq H \trianglelefteq G$, entonces $G' \trianglelefteq H$ y $G/H \simeq (G/G')\big/(H/G')$ por un isomorfismo canónico, así que G/H es abeliano, por ser isomorfo a un cociente del grupo abeliano G/G'. En resumen, G' es el menor subgrupo normal de G con cociente abeliano.

Proposición 3.49. *Un grupo G es resoluble si y sólo si hay $s \in \mathbb{N}^*$ tal que $G^{(s)} = \mathbf{1}$.*

Demostración. Si $G^{(s)} = \mathbf{1}$, hay una cadena decreciente finita con inclusiones normales y cocientes abelianos:

$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots \trianglerighteq G^{(s)} = \mathbf{1},$$

lo que muestra que G es resoluble.

Por otro lado, si G es resoluble, entonces en la cadena (3.12) es $G' \leq G_1$ por ser G/G_1 abeliano. *Afirmación*: $G^{(i)} \leq G_i$ para todo i; esto puede comprobarse por inducción sobre i. En efecto, si $G^{(i-1)} \leq G_{i-1}$, entonces por ser G_{i-1}/G_i abeliano, se obtiene

$$G^{(i)} = (G^{(i-1)})' \leq (G_{i-1})' \leq G_i.$$

En particular, $G^{(r)} \leq G_r = \mathbf{1}$, como era requerido. □

Si $\theta\colon G \to K$ es un homomorfismo de grupos, es $\theta(ghg^{-1}h^{-1}) = \theta(g)\theta(h)\theta(g)^{-1}\theta(h)^{-1}$ para todo $g,h \in G$. Luego $\theta(G') \leq K'$, con igualdad si θ es sobreyectivo.

Proposición 3.50. *Sea G un grupo y $H \leq G$. Si G es resoluble, entonces H también es resoluble. Si $H \trianglelefteq G$, entonces G es resoluble si y sólo si H y G/H son resolubles.*

Demostración. Si G es resoluble con $G^{(s)} = \mathbf{1}$, entonces $H^{(i)} \leq G^{(i)}$ para todo i, así que $H^{(s)} = \mathbf{1}$ también, lo que muestra que H es resoluble.

En el caso de que $H \trianglelefteq G$, sea $\eta\colon G \to G/H$ el homomorfismo cociente; entonces $\eta(G') = (G/H)'$. Por inducción, se ve que $\eta(G^{(i)}) = (G/H)^{(i)}$ para todo i. Si G es resoluble con $G^{(s)} = \mathbf{1}$, entonces $(G/H)^{(s)} = \eta(\mathbf{1}) = H$, el subgrupo trivial de G/H. Se concluye que G/H es resoluble.

Por otro lado, si $H \trianglelefteq G$ y si H y G/H son resolubles, entonces hay $r,s \in \mathbb{N}^*$ con $H^{(s)} = \mathbf{1}$ y $\eta(G^{(r)}) = (G/H)^{(r)} = H$. Por tanto, $G^{(r)} \leq H$ y en consecuencia $G^{(r+s)} = \mathbf{1}$. Se concluye que G también es resoluble. □

Si $H \trianglelefteq G$, y si $M \leq G/H$, defínase $K := \eta^{-1}(M)$, de modo que $H \leq K \leq G$. Si $M \trianglelefteq G/H$, entonces $K \trianglelefteq G$, porque $\eta(gkg^{-1}) = \eta(g)\eta(k)\eta(g)^{-1} \in M$ para $k \in K$, $g \in G$. Si además G/H es abeliano, entonces G/K y K/H son también abelianos.

Un grupo es *simple* si no tiene subgrupo normal propio. Los únicos grupos finitos que sean simples y abelianos son los grupos cíclicos C_p de orden primo. Si un grupo finito simple G no es abeliano, entonces $G' = G$ (porque $G' \trianglelefteq G$ y $G' \neq \mathbf{1}$). Por tanto, $G^{(i)} = G$ para todo $i \in \mathbb{N}^*$ y por ende G no es resoluble. Veremos más adelante que si $n \geq 5$, entonces el grupo alternante A_n es simple.[11]

Si en la cadena (3.12) el cociente G_{i-1}/G_i no es simple, entonces se puede intercalar un subgrupo H tal que $G_{i-1} \rhd H \rhd G_i$ y los cocientes G_i/H y H/G_{i-1} son también abelianos. Entonces *cada grupo finito G posee una cadena de máxima longitud, en donde cada cociente es un grupo cíclico de orden primo*.

⟦ Aun si el grupo G no fuera resoluble, siempre puede formarse una cadena de máxima longitud con cocientes simples. El *teorema de Jordan y Hölder* asegura que cada cadena máxima, llamada "serie de composición" de G, tiene la misma longitud y el mismo juego de grupos cocientes, aunque la cadena no sea única por cuanto estos cocientes pueden aparecer en posiciones permutadas. En este lenguaje, un grupo finito es resoluble si y sólo si sus series de composición tiene cocientes C_{p_i} para ciertos números primos p_i. ⟧

► El análisis de la ecuación cúbica irreducible, al final de la última subsección, pone en evidencia que la generación de fórmulas análogas a las de Cardano consiste, en última instancia, en ampliar el cuerpo F por una torre de extensiones cíclicas, que permite expresar las raíces del polinomio dado en términos de un juego de raíces cuadradas, cúbicas, etc., encajadas, aplicadas a los coeficientes del polinomio. Esta intuición se formaliza en las siguientes dos definiciones.

[11] Los grupos finitos simples fueron clasificados alrededor de 1980. Aparte de las dos familias mencionadas $\{C_p : p \text{ primo}\}$ y $\{A_n : n = 5,6,\dots\}$, hay 16 familias infinitas de "grupos de tipo Lie" (constituidos por matrices sobre cuerpos finitos) y hay otros 26 "grupos esporádicos". Para la lista completa, véase `http://en.wikipedia.org/wiki/List_of_finite_simple_groups`.

Definición 3.51. Sea $F \subseteq L \subseteq \mathbb{C}$. Entonces $L \mid F$ es una **extensión radical** si hay una torre de cuerpos intermedios $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = L$ tal que

$$F_i = F_{i-1}(\alpha_i) \quad \text{con} \quad \alpha_i^{n_i} \in F_{i-1}, \quad \text{para algunos} \quad n_1, \ldots, n_r \in \mathbb{N}^*. \tag{3.13}$$

Definición 3.52. Sea $F \subseteq \mathbb{C}$. Sea K_f el cuerpo de escisión de un polinomio $f(X) \in F[X]$. Se dice que $f(X)$ es **resoluble por radicales** si hay una extensión radical $L \mid F$ tal que $K_f \subseteq L$.

Fíjese que una extensión radical es finita pero no es necesariamente normal, así que el teorema fundamental no es directamente aplicable a este caso. En seguida se verá que esta situación puede remendarse, porque siempre será posible reemplazar $L \mid F$ para una extensión radical mayor que sí es normal.

Lema 3.53. *Si $L \mid F$ es una extensión radical y si n es el mínimo común múltiplo de los exponentes $n_1, \ldots, n_r$ de* (3.13)*, sea ζ una raíz n-ésima primitiva de* 1*. Si $\zeta \notin F$, entonces $L(\zeta) \mid F$ es también una extensión radical de F, en donde cada extensión intermedia es una extensión abeliana.*

Demostración. Por la definición de mínimo común múltiplo, se sabe que $n_i \setminus n$ para todo i y que cualquier $m \in \mathbb{N}^*$ tal que $n_i \setminus m$ para todo i cumple $n \setminus m$. En particular, $n = k_i n_i$ para algunos $k_1, \ldots, k_r \in \mathbb{N}^*$. En cada caso, ζ^{k_i} es una raíz primitiva n_i-ésima de 1.

Considérese la torre de cuerpos

$$F \subseteq F(\zeta) \subseteq F_1(\zeta) \subseteq \cdots \subseteq F_r(\zeta) = L(\zeta).$$

Para $i = 1, \ldots, r$, es $F_i(\zeta) = F_{i-1}(\alpha_i, \zeta) = F_{i-1}(\zeta)(\alpha_i)$. Sea $c_{i-1} := \alpha_i^{n_i} \in F_{i-1}$. Entonces la extensión $F_i(\zeta) \mid F_{i-1}(\zeta)$, generada por una raíz del polinomio $X^{n_i} - c_{i-1}$, es una extensión cíclica por la Proposición 3.42, ya que $\zeta^{k_i} \in F_{i-1}(\zeta)$. En particular, esta extensión es abeliana.

El primer piso de esta torre es excepcional: la extensión $F(\zeta) \mid F$ no es necesariamente cíclica. Pero sí es una extensión ciclotómica, por ende es normal y finita con grupo de Galois $\mathrm{Gal}(F(\zeta) \mid F) \leq U_n$, que es un grupo abeliano. □

Lema 3.54. *Si $L \mid F$ es una extensión radical, entonces hay una extensión $K \mid L$ tal que $K \mid F$ sea una extensión radical normal, en donde cada extensión intermedia es abeliana.*

Demostración. En la notación del lema anterior, sea ζ una raíz n-ésima primitiva de 1 y sean $\alpha_1, \ldots, \alpha_r$ los elementos que generan la torre de extensiones intermedias de $L \mid F$, como en (3.13). Para $i = 1, \ldots, r$, sea $\{\beta_{i1}, \beta_{i2}, \ldots, \beta_{im_i}\}$ el juego de conjugados de α_i sobre F, con $\beta_{i1} = \alpha_i$. Defínase

$$E_i := F(\zeta, \beta_{11}, \ldots, \beta_{1m_1}, \beta_{21}, \ldots, \beta_{2m_2}, \ldots, \beta_{i1}, \ldots, \beta_{im_i}).$$

Sea $p_i(X)$ el polinomio mínimo de α_i sobre F. La extensión $E_i \mid F$ es normal y finita, por ser el cuerpo de escisión del polinomio $(X^n - 1)p_1(X)p_2(X)\ldots p_i(X)$. Está claro que $F_i(\zeta) \subseteq E_i$ para cada i. Sea $K := E_r$; entonces $L(\zeta) \subseteq K$ y la extensión $K \mid F$ es normal y finita.

Para ver que $K \,|\, F$ es una extensión radical, es suficiente mostrar que $\beta_{ij}^{n_i} \in E_{i-1}$ en cada caso. Por el Lema 2.34, hay un F-morfismo $\varphi_{ij}\colon F(\alpha_i) \to \mathbb{C}$ con $\varphi_{ij}(\alpha_i) = \beta_{ij}$. Como $[E_i\colon F(\alpha_i)]$ es finita, éste se puede extender a un F-morfismo $\widetilde{\varphi}_{ij}\colon E_i \to \mathbb{C}$.

Ahora $\beta_{ij}^{n_i} = \widetilde{\varphi}_{ij}(\alpha_i^{n_i}) = \widetilde{\varphi}_{ij}(c_{i-1})$ es un conjugado de c_{i-1}, por el Lema 2.34 de nuevo. Pero E_{i-1} es normal sobre F y por tanto contiene todos los conjugados de c_{i-1}. Luego, es $\beta_{ij}^{n_i} \in E_{i-1}$.

Sea $\widetilde{F}_0 := F$, $\widetilde{F}_1 := F(\zeta)$, $\widetilde{F}_k := E_{i-1}(\beta_{i1}, \ldots, \beta_{ij})$ para $k = 1 + m_1 + \cdots + m_{i-1} + j$. Entonces $\widetilde{F}_k = \widetilde{F}_{k-1}(\beta_{ij})$ y $\beta_{ij}^{n_i} \in \widetilde{F}_{k-1}$, por ende la torre

$$F = \widetilde{F}_0 \subseteq \widetilde{F}_1 \subseteq \cdots \subseteq \widetilde{F}_k \subseteq \cdots \subseteq K$$

muestra que $K \,|\, F$ es una extensión radical. El primer piso de esta torre es una extensión ciclotómica y los demás pisos son extensiones cíclicas, por la demostración del lema anterior. Por tanto, todas las extensiones intermedias son abelianas. □

Teorema 3.55. *Sea $F \subseteq \mathbb{C}$. Sea $f(X) \in F[X]$ y sea K su cuerpo de escisión sobre F. Si $f(X)$ es resoluble por radicales, entonces* $\mathrm{Gal}(K \,|\, F)$ *es un grupo resoluble.*

Demostración. Por hipótesis, hay una extensión radical $L \,|\, F$ tal que $K \subseteq L$, con una torre de cuerpos intermedios que cumplen relaciones de tipo (3.13). En vista del Lema 3.54, se puede suponer, sin perder generalidad, que la extensión $L \,|\, F$ es normal y que las extensiones intermedias son abelianas.

Sea $H := \mathrm{Gal}(L \,|\, F)$ y sea $H_i := \mathrm{Gal}(L \,|\, F_i)$ para $i = 0, 1, \ldots, r$. En vista del Teorema 3.13, la torre de cuerpos intermedios de $L \,|\, F$ induce una cadena de subgrupos de H, así:

$$\begin{array}{c} F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = L \\ \Updownarrow \\ H = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_r = \mathbf{1} \end{array} \tag{3.14}$$

En particular, $H_i \trianglelefteq H_{i-1}$ porque $F_i \,|\, F_{i-1}$ es una extensión normal, para $i = 1, \ldots, r$. El Teorema 3.13(f) permite concluir que

$$\mathrm{Gal}(F_i \,|\, F_{i-1}) \simeq \mathrm{Gal}(L \,|\, F_{i-1}) \big/ \mathrm{Gal}(L \,|\, F_i) = H_{i-1}/H_i,$$

y el cociente H_{i-1}/H_i es un grupo abeliano porque la extensión $F_i \,|\, F_{i-1}$ es abeliana. La cadena de subgrupos (3.14) entonces muestra que H es resoluble.

Ahora $F \subseteq K \subseteq L$ y la extensión $K \,|\, F$ es normal porque K es un cuerpo de escisión sobre F. Si $G = \mathrm{Gal}(K \,|\, F)$, el Teorema 3.13(e,f) implica que $\mathrm{Gal}(L \,|\, K) \trianglelefteq \mathrm{Gal}(L \,|\, F) = H$ y que $G \simeq H \big/ \mathrm{Gal}(L \,|\, K)$. La Proposición 3.50 muestra que G es resoluble, por ser cociente del grupo resoluble H. □

Teorema 3.56. *Sea $f(X) \in F[X]$ y sea K su cuerpo de escisión sobre F, con $F \subseteq \mathbb{C}$. Si* $\mathrm{Gal}(K \,|\, F)$ *es un grupo resoluble, entonces el polinomio $f(X)$ es resoluble por radicales sobre F.*

Demostración. Escríbase $G = \mathrm{Gal}(K \mid F)$. Entonces hay una cadena de subgrupos (3.12) en donde cada cociente G_{i-1}/G_i es un grupo cíclico de orden primo p_i.

Supóngase primero que F contiene ζ, una raíz n-ésima primitiva de 1, donde $n = [K\colon F]$.

Sea $F_i := K^{G_i}$. Por el Teorema 3.13, esta cadena de subgrupos induce una torre de cuerpos intermedios de $K \mid F$, así:

$$\begin{array}{ccc} G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_r = \mathbf{1} \\ \Updownarrow \\ F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K \end{array}$$

Para cada $i = 1, \ldots, r$, es $\mathrm{Gal}(K \mid F_i) = G_i \trianglelefteq G_{i-1} = \mathrm{Gal}(K \mid F_{i-1})$, y por ende la extensión $F_i \mid F_{i-1}$ es normal.

Además, $\mathrm{Gal}(F_i \mid F_{i-1}) \simeq C_{p_i}$. Fíjese que

$$p_1 p_2 \ldots p_r = [F_1\colon F]\,[F_2\colon F_1] \ldots [K\colon F_{r-1}] = [K\colon F] = n,$$

así que $p_i \setminus n$ para cada i. El cuerpo F_{i-1} contiene una raíz p_i-ésima de 1, de la forma ζ^{k_i} con $k_i = p_1 p_2 \ldots p_{i-1}$. Ahora la Proposición 3.44 muestra que $F_i = F_{i-1}(\alpha_i)$ para algún $\alpha_i \in F_i$ que cumple $\alpha_i^{p_i} \in F_{i-1}$. Se concluye que $K \mid F$ es una extensión radical.

En el caso contrario, de que $\zeta \notin F$, la extensión $K(\zeta) \mid F$ es normal porque $K(\zeta)$ es el cuerpo de escisión de $(X^n - 1)f(X)$ sobre F. Ahora $\mathrm{Gal}(K(\zeta) \mid K)$ es abeliano, en particular es resoluble, y $\mathrm{Gal}(K \mid F)$ es resoluble. En vista de que

$$\mathrm{Gal}(K \mid F) \simeq \mathrm{Gal}(K(\zeta) \mid F) \big/ \mathrm{Gal}(K(\zeta) \mid K),$$

se concluye de la Proposición 3.50 que $\mathrm{Gal}(K(\zeta) \mid F)$ es también un grupo resoluble.

El caso anterior muestra que la extensión $K(\zeta) \mid F$ es radical, y $K \subseteq K(\zeta)$ obviamente. Por tanto, $f(X)$ es resoluble por radicales sobre F también en este caso. □

Los dos teoremas anteriores se pueden combinar en el **Teorema de Galois**: *un polinomio $f(X)$ es resoluble por radicales si y sólo si el grupo de Galois de su cuerpo de escisión es un grupo resoluble*.

Para explicar la imposibilidad de resolver por radicales la ecuación general de quinto grado, Galois demostró además que el grupo correspondiente, que es S_5, *no es* resoluble. En efecto, la serie de composición de S_5 es $S_5 \triangleright A_5 \triangleright \mathbf{1}$, en donde el segundo cociente no es abeliano: eso es una consecuencia inmediata del teorema siguiente.

Teorema 3.57. *El grupo alternante A_n es simple, para $n \geq 5$.*

Demostración. Tómese $n \in \mathbb{N}$ con $n \geq 5$. Sea $H \trianglelefteq A_n$ un subgrupo normal, con $H \neq \mathbf{1}$. Hay que mostrar que $H = A_n$.

Elíjase un elemento $\tau \in H$ que, como permutación de $\{1, 2, \ldots, n\}$, desplaza la menor cantidad posible de cifras. Se puede escribir $\tau = \tau_1 \tau_2 \ldots \tau_r$ como producto de ciclos disjuntos.

Caso 1 Supóngase que dos de estos ciclos, digamos τ_1 y τ_2, son transposiciones (hay que notar que dos ciclos disjuntos conmutan). Se puede asumir, sin perder generalidad, que $\tau_1 = (12)$ y $\tau_2 = (34)$. Sea $\sigma = \tau_3 \dots \tau_r$, de modo que $\tau = (12)(34)\sigma$.

El 3-ciclo (123) queda en A_n. Entonces H contiene

$$(123)\tau(123)^{-1} = (123)(12)(34)\sigma(132) = (123)(12)(34)(132)\sigma = (14)(23)\sigma,$$

y luego

$$\tau\big((14)(23)\sigma\big)^{-1} = (12)(34)\sigma\sigma^{-1}(23)(14) = (13)(24) \in H.$$

Ahora $(13)(24)$ desplaza cuatro cifras solamente. Luego $\sigma = \mathrm{id}$ y $H \ni (12)(34)$.

Como $n \geq 5$, es $(125) \in A_n$. Luego

$$(125)(12)(34)(125)^{-1} = (125)(12)(34)(152) = (25)(34) \in H,$$

así que $(12)(34)\,(25)(34) = (125) \in H$. Se concluye que H contiene un 3-ciclo.

Caso 2 Si en el producto $\tau = \tau_1\tau_2 \dots \tau_r$ aparece exactamente una transposición τ_j, entonces $r > 1$ porque τ_j es una permutación impar: $\tau_j \notin A_n$. Debe haber otro ciclo impar de longitud al menos 4. Sin perder generalidad, puede asumirse que $\tau_1 = (1234\dots k)$ con $k \geq 4$.

Ahora $H \ni (123)\tau(123)^{-1} = (2314\dots k)\tau_2 \dots \tau_r$ y por ende

$$H \ni \tau\big((2314\dots k)\tau_2 \dots \tau_r\big)^{-1} = (1234\dots k)\,(k\dots 4132) = (142). \tag{3.15}$$

También en este caso, H contiene un 3-ciclo.

Caso 3 Si en el producto $\tau = \tau_1\tau_2 \dots \tau_r$ no aparecen transposiciones, sea k la longitud del ciclo más largo τ_j. Si $k \geq 4$, entonces el cálculo (3.15) muestra que hay un 3-ciclo en H.

Si $k = 3$ y $r \geq 2$, se puede suponer que $\tau = (123)(456)\tau_3 \dots \tau_r$; por tanto, H contiene el elemento $(124)\tau(124)^{-1} = (156)(243)\tau_3 \dots \tau_r$ y por ende

$$H \ni \tau\big((156)(243)\tau_3 \dots \tau_r\big)^{-1} = (123)(456)\,(234)(165) = (14352),$$

lo cual contradice $k = 3$. Finalmente, si $k = 3$ y $r = 1$, entonces τ ya es un 3-ciclo.

En todos los casos, hay un 3-ciclo en H. Al reenumerar si fuera necesario, se puede asumir que $(123) \in H$. Entonces

$$\begin{aligned}
a \notin \{1,2,3\} &\implies (12a)(123)(12a)^{-1} = (2a3) \in H,\\
c \notin \{2,3,a\} &\implies (2ac)(2a3)(2ac)^{-1} = (3ac) \in H,\\
b \notin \{3,a,c\} &\implies (3ab)(3ac)(3ab)^{-1} = (abc) \in H.
\end{aligned}$$

Se concluye que H contiene *todos* los 3-ciclos en A_n.

Cada elemento de A_n es un producto de pares de transposiciones $(ab)(cd)$. Si $a = c$, $b = d$, o bien si $a = d$, $b = c$, entonces $(ab)(cd) = \mathrm{id} \in H$. Si $a = c$, $b \neq d$, entonces $(ab)(cd) =$

$(ab)(ad) = (adb) \in H$. Si $a \neq c$, $b = d$, entonces $(ab)(cd) = (ab)(bc) = (abc) \in H$. Finalmente, si a,b, c, d son distintos, entonces

$$(ab)(cd) = (ab)(ac)(ac)(cd) = (acb)\,(acd) \in H.$$

En resumen, $(ab)(cd) \in H$ en todos los casos. Por tanto, $A_n = H$. □

Corolario 3.58. *El grupo de permutaciones S_n no es resoluble, para $n \geq 5$.*

Demostración. Como $S_n/A_n \simeq C_2$ es abeliano, la Proposición 3.50 muestra que S_n es resoluble si y sólo si A_n es resoluble. Del teorema anterior, A_n es resoluble si y sólo si $n = 1,2,3,4$. □

Lema 3.59. *Si p es primo, $p \geq 3$, el grupo S_p es generado por una transposición y un ciclo de longitud p.*

Demostración. Considérese S_p como el grupo de permutaciones del conjunto $\{1,2,\ldots,p\}$. Se puede suponer que la transposición es (12). Si σ es el p-ciclo, entonces alguna potencia σ^k cumple $\sigma^k(1) = 2$; basta entonces comprobar el lema para el caso en donde $\sigma(1) = 2$. Sin perder generalidad, se puede suponer que $\sigma = (123\ldots p)$.

Ahora, en el subgrupo H generado por (12) y σ, se encuentran

$$\sigma(12)\sigma^{-1} = (123\ldots p)(12)(p\ldots 321) = (23),$$
$$\sigma(23)\sigma^{-1} = (23\ldots p1)(23)(1p\ldots 32) = (34), \quad \text{etc.}$$

Al repetir este cálculo, se obtiene $\sigma^{k-1}(12)\sigma^{1-k} = (k, k+1) \in H$ para $k = 1,\ldots,p-1$. Por tanto, H contiene las transposiciones (12), (23),…, $(p-1,\, p)$. Pero *toda* transposición es un producto de éstas; por ejemplo, es $(25) = (34)(23)(34)(23)(45)(34)(23)$. Como cualquier permutación es un producto de transposiciones, se concluye que $H = S_p$. □

Ejemplo 3.60. El polinomio $f(X) = X^5 - 80X + 5$ no es resoluble por radicales sobre $\mathbb{Q}$.

En efecto, $f(X)$ es irreducible en $\mathbb{Z}[X]$ y por ende en $\mathbb{Q}[X]$, por el criterio de Eisenstein con $p = 5$. Su derivada es $f'(X) = 5(X^4 - 16) = 5(X^2+4)(X-2)(X+2)$ que tiene exactamente dos raíces reales, -2 y 2. De la tabla de valores:

a	-4	-2	2	4
$f(a)$	-699	133	-123	709

se ve que $f(X)$ tiene tres raíces reales $\alpha_1, \alpha_2, \alpha_3$, con $-4 < \alpha_1 < -2 < \alpha_2 < 2 < \alpha_3 < 4$. Por el teorema de Rolle, no puede haber más raíces reales: las otras dos raíces forman un par de conjugados complejos, $\alpha_5 = \overline{\alpha}_4$.

Si $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ es el cuerpo de escisión de $f(X)$ sobre $\mathbb{Q}$, entonces la conjugación compleja κ define un elemento de $G = \mathrm{Gal}(K \mid \mathbb{Q})$, de orden 2, que transpone α_4 con α_5 y deja fijas las raíces reales. Al considerar G como subgrupo del grupo S_5 de permutaciones de las raíces, se obtiene $\kappa|_K = (45) \in G$. Por otro lado, como $\mathbb{Q}(\alpha_1) \subseteq K$, con $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 5$ por la irreducibilidad de $f(X)$, se ve que $5 \setminus |G| = [K : \mathbb{Q}]$. Por tanto, G contiene un elemento de orden 5, que es necesariamente un 5-ciclo en S_5. El Lema 3.59 entonces muestra que $G = S_5$, que es un grupo no resoluble.

Ejemplo 3.61. Sean $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ números complejos algebraicamente independientes: es decir, α_1 es trascendente sobre $\mathbb{Q}$ y α_j es trascendente sobre $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$ para $j = 2, \ldots, n$. Si $h(X) := (X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$, la ecuación $h(X) = 0$ se llama la *ecuación general de n-ésimo grado* sobre $\mathbb{Q}$. Por la Proposición 1.24, si $a_{n-k} := (-1)^k s_k(\alpha_1, \ldots, \alpha_n)$ son los polinomios simétricos en estas raíces (con un ajuste de signos), se obtiene de la fórmula (1.19):

$$h(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1 X + a_0, \tag{3.16}$$

el polinomio mónico "general" con coeficientes en $\mathbb{C}$.

Decir que los $\alpha_1, \ldots, \alpha_n$ son algebraicamente independientes es afirmar que no cumplen relación polinomial alguna, o bien que el homomorfismo $f \mapsto f(\alpha_1, \ldots, \alpha_n)$ de $\mathbb{Q}[X_1, \ldots, X_n]$ en $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ es *inyectivo*. Pasando a los cuerpos de fracciones, se obtiene un homomorfismo inyectivo de $\theta : \mathbb{Q}(X_1, \ldots, X_n) \to \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

El cuerpo $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ es el cuerpo de escisión de $h(X)$ sobre $\mathbb{Q}$. Sea $F := \mathbb{Q}(a_1, \ldots, a_n)$ el cuerpo generado por los coeficientes de (3.16). Entonces $f(X) \in F[X]$ y la extensión $K \,|\, F$ es normal y finita. Sea $G := \mathrm{Gal}(K \,|\, F)$. Cada permutación σ de $\{\alpha_1, \ldots, \alpha_n\}$ se extiende a un $\mathbb{Q}$-automorfismo (también llamado σ) de K que deja fijos los polinomios simétricos en los α_j. Por tanto, $\sigma(a_i) = a_i$ para cada i, así que σ es un F-automorfismo de K. De esta forma, hay una de inclusión S_n como subgrupo de G.

El grupo S_n también actúa sobre el cuerpo $\mathbb{Q}(X_1, \ldots, X_n)$ por permutación de los indeterminados $X_1, \ldots, X_n$. La Proposición 1.25 muestra que el cuerpo fijo para esta acción es exactamente el cuerpo de funciones racionales $\mathbb{Q}(s_1, \ldots, s_n)$. Al aplicar el homomorfismo inyectivo θ que entrelaza las dos acciones de S_n, se obtiene

$$K^{S_n} = \theta\big(\mathbb{Q}(s_1, \ldots, s_n)\big) = \mathbb{Q}(a_1, \ldots, a_n) = F.$$

Por tanto, $[K\colon F] = |S_n| = n!$.

Por otro lado, el Lema 3.17 muestra que $|G| = |\mathrm{Gal}(K \,|\, F)| \leq n!$ porque $\mathrm{gr}\, h(X) = n$. Se concluye que el subgrupo S_n es todo G, es decir, que $G = S_n$.

Finalmente, la no resolubilidad de S_n permite concluir que *la ecuación general de n-ésimo grado, $h(X) = 0$, no es resoluble por radicales, si $n \geq 5$*. Esta es la forma moderna de demostrar el teorema de Ruffini y Abel, y es una consecuencia directa del trabajo de Galois.

3.6 Ejercicios sobre grupos de Galois y extensiones ciclotómicas y radicales

En los problemas que siguen, cuando $f(X)$ es un polinomio en $\mathbb{Q}[X]$, K_f denotará el cuerpo de escisión de $f(X)$ sobre $\mathbb{Q}$.

Ejercicio 3.1. Sean $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}(\sqrt[4]{2})$. Mostrar que las extensiones $K \,|\, E$ y $E \,|\, F$ son normales, pero que $K \,|\, F$ no es normal. (Esto dice que la normalidad de una extensión no es una propiedad transitiva.)

Ejercicio 3.2. Si $f(X) = X^5 - 2$, hallar K_f y calcular el grado $[K_f\colon \mathbb{Q}]$.

Ejercicio 3.3. Mostrar que X^6+X^3+1 es irreducible en $\mathbb{Q}[X]$. Usar este resultado para comprobar que la extensión $\mathbb{Q}(e^{2\pi i/9}) \,|\, \mathbb{Q}$ es normal y que $[\mathbb{Q}(e^{2\pi i/9}) \colon \mathbb{Q}] = 6$.

Ejercicio 3.4. En cada uno de los casos siguientes: hallar el cuerpo K_f, calcular $[K_f \colon \mathbb{Q}]$, determinar el grupo $\mathrm{Gal}(K_f \,|\, \mathbb{Q})$ y encontrar los cuerpos intermedios E con $\mathbb{Q} \subset E \subset K_f$, si:

$$\text{(a) } f(X) = X^2 - 2, \qquad \text{(b) } f(X) = X^4 - 1, \qquad \text{(c) } f(X) = X^4 + 1.$$

Ejercicio 3.5. Si $f(X) = X^4 - 2X^2 - 1$, mostrar que $[K_f \colon \mathbb{Q}] = 8$ y que $\mathrm{Gal}(K_f \,|\, \mathbb{Q})$ es isomorfo al grupo diédrico D_4.

Ejercicio 3.6. Si $F = \mathbb{Q}(\sqrt{3})$ y $K = \mathbb{Q}(\sqrt{3} + \sqrt[4]{3})$, hallar el grupo de Galois $\mathrm{Gal}(K \,|\, F)$, identificando cada uno de sus elementos como F-automorfismo de K.

Ejercicio 3.7. (a) Sea $\alpha = \sqrt{2+\sqrt{2+\sqrt{2}}}$. Encontrar el polinomio mínimo $p(X)$ de α sobre $\mathbb{Q}$, usando el criterio de Eisenstein para verificar su irreducibilidad. ¿Cuáles son los conjugados de α sobre $\mathbb{Q}$?

(b) Verificar que el cuerpo de escisión K_p es $\mathbb{Q}(\alpha)$. Si $\tau \in \mathrm{Gal}(\mathbb{Q}(\alpha) \,|\, \mathbb{Q})$ es determinado por $\tau(\alpha) := \sqrt{2+\sqrt{2-\sqrt{2}}}$, describir el efecto de τ como permutación de las raíces de $p(X)$.

(c) Hallar el grupo $\mathrm{Gal}(\mathbb{Q}(\alpha) \,|\, \mathbb{Q})$.

Ejercicio 3.8. Hallar una extensión *normal* de $\mathbb{Q}$ de grado 3 (con una verificación de su normalidad). ⟦ Indicación: Buscar un polinomio cuyas raíces sean $\cos\frac{2\pi}{7}$, $\cos\frac{4\pi}{7}$, $\cos\frac{6\pi}{7}$. ⟧

Ejercicio 3.9. Si $f(X) = (X^3-2)(X^3-3)$, determinar el grupo $\mathrm{Gal}(K_f \,|\, \mathbb{Q})$ y hallar el subgrupo cuyo cuerpo fijo es $\mathbb{Q}(\omega)$, donde $\omega = \frac{1}{2}(-1+i\sqrt{3}) = e^{2\pi i/3}$.

Ejercicio 3.10. Un *retículo* es un conjunto parcialmente ordenado L, en donde cada par de elementos x, y posee un *ínfimo* $x \wedge y$ y un *supremo* $x \vee y$, y además L posee un elemento mínimo $\overline{0}$ y un elemento máximo $\overline{1}$. Si $K \,|\, F$ es una extensión normal y finita con $K \subseteq \mathbb{C}$, sea $\mathcal{E}_{K|F} := \{E : F \subseteq E \subseteq K\}$ el conjunto de cuerpos intermedios de esta extensión; y si $G = \mathrm{Gal}(K \,|\, F)$, sea $\mathcal{H}_{K|F} := \{H : H \leq G\}$ el conjunto de subgrupos de G.

(a) Comprobar que $\mathcal{E}_{K|F}$ y $\mathcal{H}_{K|F}$ son retículos, describiendo sus operaciones $\wedge$ y $\vee$.

(b) Si $\Phi \colon \mathcal{E}_{K|F} \to \mathcal{H}_{K|F}$ es la correspondencia de Galois, y si $E, E' \in \mathcal{E}_{K|F}$, demostrar en detalle que $\Phi(E \wedge E') = \Phi(E) \vee \Phi(E')$ y $\Phi(E \vee E') = \Phi(E) \wedge \Phi(E')$.

Ejercicio 3.11 (Artin)**.** (a) Si $F(t)$ es el cuerpo de funciones racionales sobre F, sean σ, τ las aplicaciones de $F(t)$ en $F(t)$ definidas por[12]

$$\sigma(f(t)) := f\left(\frac{1}{1-t}\right), \qquad \tau(f(t)) := f\left(\frac{1}{t}\right).$$

Mostrar que σ y τ son F-automorfismos de $F(t)$ y que generan un grupo H de 6 elementos, isomorfo a S_3.

[12] Este ejercicio está tomado del libro de Artin, pp. 38–39.

(b) Verificar que $s := \dfrac{(t^2-t+1)^3}{t^2(t-1)^2} \in F(t)$ queda fijo bajo los automorfismos en H.

(c) Demostrar que el cuerpo fijo $F(t)^H$ es precisamente $F(s)$.

Ejercicio 3.12. Un teorema de Kaplansky dice que si $f(X) = X^4 + aX^2 + b \in \mathbb{Z}[X]$ es irreducible, entonces el grupo $\mathrm{Gal}(K_f \,|\, \mathbb{Q})$ es uno de los siguientes tres grupos: el *Vierergruppe* $V = C_2 \times C_2$, el grupo cíclico C_4, o bien el grupo diédrico D_4 (de 8 elementos). Hallar este grupo de Galois en los tres casos:

$$\text{(a)}\ \ f(X) = X^4 + 1, \qquad \text{(b)}\ \ f(X) = X^4 + 4X^2 + 2, \qquad \text{(c)}\ \ f(X) = X^4 + 2X^2 + 2,$$

para comprobar que los tres grupos admisibles se realizan.[13]

Ejercicio 3.13. (a) Sean $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $K = E\Big(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\Big)$. Verificar que $[K\colon E] = 2$.

(b) Demostrar que $E \,|\, \mathbb{Q}$ es normal y que $\mathrm{Gal}(E \,|\, \mathbb{Q}) \simeq C_2 \times C_2$.

(c) Demostrar que $K \,|\, \mathbb{Q}$ es normal y que $\mathrm{Gal}(K \,|\, \mathbb{Q}) \simeq Q$, donde

$$Q := \{1, -1, i, -i, j, -j, k, -k\} \quad \text{con} \quad i^2 = j^2 = k^2 = ijk = -1$$

es el *grupo de cuaterniones* de 8 elementos.[14]

Ejercicio 3.14. Sea $\Phi_n(X)$ el polinomio ciclotómico tal que $\Phi_n(e^{2\pi i/n}) = 0$.

(a) Si p es un número primo tal que $p \nmid n$, mostrar que $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$. ⟦ Indicación: inducción sobre n. ⟧

(b) Si p es un número primo tal que $p \mid n$, mostrar que $\Phi_{pn}(X) = \Phi_n(X^p)$.

Ejercicio 3.15. Si $n \in \mathbb{N}$ es impar con $n > 1$, demostrar que $\Phi_{2n}(X) = \Phi_n(-X)$.

Ejercicio 3.16. Calcular los polinomios ciclotómicos $\Phi_8(X)$, $\Phi_{12}(X)$, $\Phi_{24}(X)$, $\Phi_{30}(X)$ y $\Phi_{81}(X)$.

Ejercicio 3.17. (a) Sea $n = 2^k$ con $k \geq 2$. Mostrar que $5^{2^r} \equiv 1 + 2^{r+2} \bmod 2^{r+3}$ para $r \in \mathbb{N}$. ⟦ Indicación: El teorema binomial. ⟧ Concluir que el orden del elemento $\overline{5} \in U_n$ es 2^{k-2}.

(b) Demostrar que $5^m \not\equiv -1 \bmod 2^k$ para todo $m \in \mathbb{N}$. Concluir que U_n es isomorfo al grupo $C_{2^{k-2}} \times C_2$.

Ejercicio 3.18. Sean $\zeta := e^{2\pi i/17}$, $K := \mathbb{Q}(\zeta)$ y $G := \mathrm{Gal}(K \,|\, \mathbb{Q})$. Se sabe que $G \simeq U_{17} \simeq C_{16}$. Sea $\sigma_k \in G$ el automorfismo de $\mathbb{Q}(\zeta)$ que corresponde a $\overline{k} \in U_{17}$.

(a) Mostrar que $2^8 \equiv 1 \bmod 17$ y que $3^8 \not\equiv 1 \bmod 17$ (así que σ_3 es un generador del grupo cíclico G pero σ_2 no es un generador). Escribir la lista de las potencias de $\overline{3}$ en U_{17}.

[13] Ejercicio tomado de los apuntes de Baker: ver la bibliografía.

[14] Ejercicio tomado de los apuntes de Milne: ver la bibliografía.

(b) Verificar que el retículo $\mathcal{H}_{K|\mathbb{Q}}$ es una *cadena*, isomorfa a $C_{16} \trianglerighteq C_8 \trianglerighteq C_4 \trianglerighteq C_2 \trianglerighteq \mathbf{1}$. Comprobar que el retículo $\mathcal{E}_{K|\mathbb{Q}}$ viene dado por

$$\mathbb{Q} = K^{\langle\sigma_3\rangle} \subset K^{\langle\sigma_9\rangle} \subset K^{\langle\sigma_{13}\rangle} \subset K^{\langle\sigma_{16}\rangle} \subset K = \mathbb{Q}(\zeta).$$

(c) Sea $\alpha := \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16}$. Encontrar $\sigma \in G$ tal que $\sigma(\alpha) \neq \alpha$ pero $\sigma(\sigma(\alpha)) = \alpha$. Mostrar que $[\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 2$ y obtener el polinomio mínimo de α sobre $\mathbb{Q}$. Concluir que $\{\alpha, \sigma(\alpha)\} = \frac{1}{2}(-1 \pm \sqrt{17})$.

(d) Verificar que $\cos(2\pi/17) > \cos(4\pi/17) > \sqrt{2}/2$ y $\cos(8\pi/17) > 0$. Concluir que $\alpha \in \mathbb{R}$ con $\alpha > 0$, así que $\alpha = \frac{1}{2}(-1 + \sqrt{17})$. Explicar cómo construir α, a partir de 0 y 1, por regla y compás.

[Nota: De la misma forma, se puede hallar $\beta, \gamma \in \mathbb{C}$ tales que $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha,\beta) \subset \mathbb{Q}(\alpha,\beta,\gamma) \subset \mathbb{Q}(\zeta)$ es una torre de extensiones de grado 2 cada una. Se puede construir $\alpha, \beta, \gamma, \zeta$ sucesivamente por regla y compás. Los cálculos omitidos son largos y tediosos.][15]

Los tres ejercicios siguientes culminan con una "fórmula cerrada" para el polinomio $\Phi_n(X)$.

Ejercicio 3.19 (Gian-Carlo Rota, 1964)**.** Sea N un conjunto parcialmente ordenado con un elemento mínimo t, tal que cada "intervalo" $\{z \in N : x \leq z \leq y\}$ sea finito. Sea A un grupo abeliano con una operación aditiva, y sea $\mathcal{F}$ el conjunto de funciones $F\colon N \times N \to A$ tales que $f(x,y) = 0$ cuando $x \not\leq y$. La *convolución* $F * G$ de $F, G \in \mathcal{F}$ se define por

$$F * G(x,y) := \sum_{x \leq z \leq y} F(x,z)\, G(z,y).$$

(a) Verificar que $(\mathcal{F}, +, *)$ es un anillo con identidad D, donde $D(x,x) := 1$, $D(x,y) := 0$ si $x \neq y$.

(b) Defínase la *función zeta* en $\mathcal{F}$ por $Z(x,y) := 1$ toda vez que $x \leq y$. Defínase otro elemento $M \in \mathcal{F}$ por inducción, así: $M(x,x) := 1$; y si $M(x,z)$ está definida para $x \leq z < y$, entonces

$$M(x,y) := -\sum_{x \leq z < y} M(x,z).$$

Verificar esta *función de Möbius*[16] M invierte Z, es decir, que $M * Z = D = Z * M$.

(c) Si $f, g\colon N \to A$ son dos funciones, mostrar que

$$g(x) = \sum_{t \leq w \leq x} f(w) \quad \text{si y sólo si} \quad f(y) = \sum_{t \leq x \leq y} g(x) M(x,y).$$

[15] Ejercicio tomado del libro de Escofier, que incluye esos cálculos tediosos.

[16] Esta generalización de la función de Möbius para $\mathbb{N}$ es una pieza clave de la teoría general de la combinatoria, esbozada en el artículo de Gian-Carlo Rota, "On the foundations of combinatorial theory I. Theory of Möbius functions", Zeitschrift für Wahrscheinlichkeitstheorie 2 (1964), 340–368.

Ejercicio 3.20. Tómese $N := \mathbb{N}^* = \{1,2,3,\dots\}$, parcialmente ordenado por divisibilidad, al emplear el orden parcial "$k \setminus m$" en lugar de "$k \le m$". Sea $\mathcal{F}' \subset \mathcal{F}$ el subanillo de funciones que cumplen $F(k,m) = F(1,m/k) =: f(m/k)$ cuando $k \setminus m$.

(a) Comprobar que $\mathcal{F}'$ queda cerrada bajo convolución y que la relación $F * G = H$ es equivalente a relación

$$h(m) = \sum_{k\setminus m} f(k)\, g(m/k).$$

(b) Sea $\mu(n) := M(1,n)$ la función de Möbius para $\mathbb{N}$. Comprobar la *fórmula de inversión*:

$$g(n) = \sum_{m\setminus n} f(m) \quad \text{si y sólo si} \quad f(m) = \sum_{k\setminus m} g(k)\,\mu(m/k).$$

Nota: si se reemplaza el grupo aditivo A por un grupo multiplicativo en la definición de $\mathcal{F}$ y $\mathcal{F}'$, esta fórmula debe ser reemplazado por su versión multiplicativa:

$$g(n) = \prod_{m\setminus n} f(m) \quad \text{si y sólo si} \quad f(m) = \prod_{k\setminus m} g(k)^{\mu(m/k)}.$$

(c) Verificar la siguiente fórmula para la función de Möbius μ. Sea $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ la factorización prima de n, donde $p_1,\dots,p_k$ son primos distintos. Entonces

$$\mu(n) = \begin{cases} (-1)^k, & \text{si cada } r_i = 1, \\ 0, & \text{si algún } r_i > 1. \end{cases}$$

⟦ Indicación: Considerar la expansión binomial de $(1-1)^k = 0$. ⟧

Ejercicio 3.21. Sea A el grupo multiplicativo $\mathbb{C}(X)\setminus\{0\}$ de funciones racionales no nulos con coeficientes complejos. Usar la fórmula de inversión de Móbius para comprobar la fórmula

$$\Phi_n(X) = \prod_{d\setminus n} (X^d - 1)^{\mu(n/d)}.$$

Usar esta fórmula para calcular los polinomios ciclotómicos $\Phi_8(X)$, $\Phi_{12}(X)$, $\Phi_{24}(X)$, $\Phi_{30}(X)$ y $\Phi_{81}(X)$.

Ejercicio 3.22. Sea ζ una raíz n-ésima primitiva de 1 y sea F un subcuerpo de $\mathbb{C}$.

(a) Mostrar que $F(\zeta)$ es una extensión normal de F.

(b) Sea $G = \mathrm{Gal}(F(\zeta)\,|\,F)$ su grupo de Galois. Si $U_n = \mathrm{Gal}(\mathbb{Q}(\zeta)\,|\,\mathbb{Q})$, mostrar que la restricción $\theta(\sigma) := \sigma\big|_{\mathbb{Q}(\zeta)}$ define un homomorfismo inyectivo $\theta\colon G \to U_n$.

(c) Concluir que la extensión $F(\zeta)\,|\,F$ es abeliana.

Ejercicio 3.23. Mostrar que la extensión $\mathbb{Q}\big(\sqrt{2}, \sqrt{\sqrt[3]{3}+\sqrt[3]{5}}\big)\,|\,\mathbb{Q}$ es una extensión radical, al exhibir una torre de extensiónes intermedias cuyos grupos de Galois son cíclicos de orden primo.

Ejercicio 3.24. Sea $f(X) \in \mathbb{Z}[X]$ un polinomio y sea $D = D(f(X))$ su discriminante. Si $n = \operatorname{gr} f(X)$, considérese $\operatorname{Gal}(K_f \,|\, \mathbb{Q})$ como subgrupo del grupo S_n de permutaciones de las raíces (en K_f). Mostrar que $\operatorname{Gal}(K_f \,|\, \mathbb{Q}) \leq A_n$ si y sólo si D es un cuadrado en $\mathbb{Q}$.

Ejercicio 3.25. Mostrar que el polinomio $X^3 - 3X + 1$ es irreducible en $\mathbb{Z}[X]$ y que su grupo de Galois sobre $\mathbb{Q}$ es isomorfo a C_3.

Ejercicio 3.26. (a) Mostrar que el polinomio $f(X) = X^3 - 5$ es irreducible en $\mathbb{Z}[X]$ y que su grupo de Galois sobre $\mathbb{Q}$ es isomorfo a S_3.

(b) Encontrar un cuerpo intermedio E con $\mathbb{Q} \subset E \subset K_f$ tal que $\operatorname{Gal}(E \,|\, \mathbb{Q}) \simeq C_3$.

Ejercicio 3.27. Comprobar que el discriminante del polinomio $X^3 + aX^2 + bX + c$ es

$$D = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2.$$

Concluir que el grupo de Galois (sobre $\mathbb{Q}$) del polinomio $X^3 + 10X^2 - 24X - 256$ es isomorfo a C_3.

Ejercicio 3.28. (a) Mostrar que $f(X) = X^4 - 10X^2 - 4X + 6$ es irreducible en $\mathbb{Z}[X]$.[17]

(b) Si sus raíces son $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{C}$, sean

$$\beta_1 := \alpha_1\alpha_2 + \alpha_3\alpha_4, \qquad \beta_2 := \alpha_1\alpha_3 + \alpha_2\alpha_4, \qquad \beta_3 := \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Usar el método de Ferrari para obtener el polinomio mínimo de β_1. En seguida, verificar que $\operatorname{Gal}(\mathbb{Q}(\beta_1) \,|\, \mathbb{Q}) \simeq C_3$.

(c) Comprobar que el grupo de Galois $G = \operatorname{Gal}(K_f \,|\, \mathbb{Q})$ permuta $\beta_1, \beta_2, \beta_3$ *cíclicamente* y por ende no contiene transposiciones. Concluir que $G \simeq A_4$.

Ejercicio 3.29. (a) Verificar que el grupo A_4 no incluye un subgrupo de orden 6.

(b) Usar el resultado del Ejercicio anterior para mostrar que las raíces del polinomio $f(X) = X^4 - 10X^2 - 4X + 6$ no son números constructibles con regla y compás.

Ejercicio 3.30. Un teorema de la teoría de grupos finitos asegura que cualquier grupo finito G de orden p^r, con p primo, tiene un subgrupo normal $H \lhd G$ tal que $[G\colon H] = p$.

Si $K \,|\, \mathbb{Q}$ es una extensión normal finita de grado p^r, mostrar que $K \,|\, \mathbb{Q}$ es una extensión radical, con una torre de extensiones $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K$ tal que cada extensión intermedia $F_i \,|\, F_{i-1}$ es cíclica de orden p.

Ejercicio 3.31. Sea $f(X) \in \mathbb{Z}[X]$ un polinomio de grado 4, que tenga exactamente 2 raíces reales. Mostrar que su grupo de Galois sobre $\mathbb{Q}$ es S_4 ó D_4.

Ejercicio 3.32. (a) Mostrar que el polinomio $f(X) = X^5 - 5X + 1$ es irreducible en $\mathbb{Z}[X]$.

(b) Verificar que $f(X)$ tiene exactamente tres raíces reales. Concluir que su grupo de Galois sobre $\mathbb{Q}$ es S_5.

[17] Ejercicio tomado de los apuntes de Chamizo: ver la bibliografía.

Ejercicio 3.33. La notación F_{20} denota el *grupo de Frobenius* de orden 20. Este es el grupo abstracto

$$F_{20} := \langle a, b : a^5 = 1,\ b^4 = 1,\ ba = a^2 b \rangle.$$

(a) Verificar que los ciclos $a = (12345)$, $b = (2354)$ realizan F_{20} como subgrupo de S_5 y mostrar que F_{20} es un grupo resoluble.

(b) Encontrar el cuerpo de escisión K_f para el polinomio $f(X) = X^5 - 2$ sobre $\mathbb{Q}$.

(c) Mostrar que $\mathrm{Gal}(K_f \,|\, \mathbb{Q}) \simeq F_{20}$.

(d) Expresar la extensión $K_f \,|\, \mathbb{Q}$ como extensión radical, al exhibir una torre de extensiones cíclicas intermedias.[18]

[18] Ejercicio tomado de los apuntes de Milne.

4 Cuerpos Finitos

Hasta ahora, se ha estudiado la teoría de Galois mayormente para cuerpos incluidos en $\mathbb{C}$. Buena parte de los resultados ya vistos son válidos en otros cuerpos, como por ejemplo el cuerpo de funciones racionales $\mathbb{Q}(X)$. En este capítulo se considera el caso general, con atención a los cuerpos con un número finito de elementos. Aparece un fenómeno nuevo, de *inseparabilidad*: la existencia de polinomios irreducibles con raíces repetidas.

4.1 Cuerpos de característica prima

Sea F un cuerpo cualquiera. Si $a \in F$ y $n \in \mathbb{Z}$ con $n > 0$, escríbase $n \cdot a := a + a + \cdots + a$ (n sumandos). También sean $(-n) \cdot a := n \cdot (-a)$ y $0 \cdot a := 0 \in F$. Entonces la expresión $\iota(n) := n \cdot 1$ define un homomorfismo de anillos $\iota : \mathbb{Z} \to F$.

Supóngase que $\iota : \mathbb{Z} \to F$ es inyectivo. Este es el caso cuando $n \cdot 1 \neq 0$ en F para $n \neq 0$ en $\mathbb{Z}$. Entonces ι se extiende a un homomorfismo inyectivo $\tilde{\iota} : \mathbb{Q} \to F$ por

$$\tilde{\iota}\left(\frac{m}{n}\right) := \frac{m \cdot 1}{n \cdot 1} \in F,$$

cuando $m, n \in \mathbb{Z}$ con $n \neq 0$. Es inmediata que $\mathbb{Q} \simeq \tilde{\iota}(\mathbb{Q}) \subseteq F$.

Ahora considérese el caso contrario, cuando $\iota : \mathbb{Z} \to F$ no es inyectivo. En este caso, hay $n > 0$ con $n \cdot 1 = 0$ en F. Si $n = rs$ con $r > 1$, $s > 1$ en $\mathbb{N}$, entonces

$$0 = n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ veces}} = (\underbrace{1 + \cdots + 1}_{r \text{ veces}})(\underbrace{1 + \cdots + 1}_{s \text{ veces}}) = (r \cdot 1)(s \cdot 1),$$

así que $r \cdot 1 = 0$ o bien $s \cdot 1 = 0$ en F. Sea p el *menor* entero positivo tal que $p \cdot 1 = 0$; entonces p es un número primo. Luego $\mathbb{F}_p \simeq \iota(\mathbb{Z}) \subseteq F$.

Definición 4.1. El cuerpo F es **de característica 0** si $\iota : \mathbb{Z} \to F$ es inyectivo. El *subcuerpo primo* de F es el subcuerpo generado por 1, que es $\tilde{\iota}(\mathbb{Q}) \simeq \mathbb{Q}$.

Sea p un número primo. Un cuerpo F es **de característica p** si $\iota : \mathbb{Z} \to F$ no es inyectivo y si p es el menor entero positivo tal que $p \cdot 1 = 0$. El *subcuerpo primo* de F es el subcuerpo generado por 1, que es $\iota(\mathbb{Z}) \simeq \mathbb{F}_p$.

Lema 4.2. *Si F es un cuerpo finito con q elementos, entonces $q = p^r$ para algún número primo p y algún $r \in \mathbb{N}^*$.*

Demostración. Por ser F finito, no puede incluir un subcuerpo infinito y por tanto no puede tener característica 0. Si su característica es p, su cuerpo primo es (isomorfo a) $\mathbb{F}_p$.

Sea $r := [F : \mathbb{F}_p]$. Sea $x_1, \ldots, x_r$ una base de F como espacio vectorial sobre $\mathbb{F}_p$. Los distintos elementos de F son combinaciones lineales $c_1 x_1 + \cdots + c_r x_r$ con $c_1, \ldots, c_r \in \mathbb{F}_p$. Hay exactamente p^r formas de elegir estos coeficientes, por lo tanto $q = p^r$. □

Proposición 4.3. *Si F es un cuerpo finito con p^r elementos, entonces F es un cuerpo de escisión del polinomio $X^{p^r} - X$ sobre su cuerpo primo.*

Demostración. Sea $F^\times := F \setminus \{0\}$. Entonces $F^\times$ es un grupo finito multiplicativo (de hecho, un grupo cíclico, por la Proposición 3.40) con $p^r - 1$ elementos. Por lo tanto, es $a^{p^r-1} = 1$ para $a \in F^\times$ con $a \neq 0$. Luego *todo* $a \in F$, inclusive el caso $a = 0$, cumple la ecuación $a^{p^r} = a$. En otras palabras, cada $a \in F$ es una raíz del polinomio $X^{p^r} - X$. Este polinomio tiene coeficientes 1, -1 y 0, los cuales pertenecen al cuerpo primo.

Ahora $X^{p^r} - X$ tiene grado p^r, luego tiene a lo sumo p^r raíces distintas en un cuerpo cualquiera. Los elementos del cuerpo F son p^r raíces de este polinomio y son distintas. En síntesis, este polinomio escinde en $F[X]$:

$$X^{p^r} - X = \prod_{a \in F} (X - a). \tag{4.1}$$

Es evidente y trivial que F es generado, sobre su cuerpo primo, por el conjunto de raíces $\{\, a : a \in F \,\}$, así que F es un cuerpo de escisión de $X^{p^r} - X$. □

Teorema 4.4. *Si $q = p^r$ es una potencia de un primo, existe un cuerpo finito, único hasta isomorfismo, con q elementos.*

Demostración. Considérese el polinomio $f(X) := X^{p^r} - X \in \mathbb{F}_p[X]$. Por el Corolario 2.18 al teorema de Kronecker, hay una extensión $K \,|\, \mathbb{F}_p$ tal que $f(X)$ escinde en K. Se puede suponer, sin perder generalidad, que K está generado sobre $\mathbb{F}_p$ por las raíces de $f(X)$, de modo que K es un cuerpo de escisión para $f(X)$ sobre $\mathbb{F}_p$. El Corolario 2.25 dice que K es único, hasta un $\mathbb{F}_p$-isomorfismo.

La derivada de $f(X)$ es $f'(X) = p^r X^{p^r-1} - \overline{1} = -\overline{1}$ en $\mathbb{F}_p[X]$. El discriminante de $f(X)$ es entonces $D(f(X)) = (-1)^{p^r-1} \operatorname{Res}(f(X), -\overline{1}) = \pm\overline{1} \neq 0$. Por el Lema 1.32, las raíces de $f(X)$ son distintas.

(Fíjese que ese Lema, y las propiedades de resultantes que lo demuestran, fueron enunciados para subcuerpos de $\mathbb{C}$, pero son igualmente válidos en un cuerpo como $\mathbb{F}_p$ que admite una extensión que contenga todas las raíces de $f(X)$ y de $f'(X)$.)

Sea $E \subseteq K$ el conjunto de las p^r raíces (distintas) de $f(X)$. Si $\alpha, \beta \in E$, entonces $(\alpha\beta)^{p^r} = \alpha^{p^r}\beta^{p^r} = \alpha\beta$, así que $\alpha\beta \in E$; también, $(-\alpha)^{p^r} = -\alpha^{p^r} = -\alpha$, así que $-\alpha \in E$. (Obsérvese que $-\alpha = +\alpha$ si $p = 2$.) Además, por el teorema binomial, es

$$(\alpha+\beta)^{p^r} = \alpha^{p^r} + \binom{p^r}{1}\alpha^{p^r-1}\beta + \cdots + \binom{p^r}{p^r-1}\alpha\beta^{p^r-1} + \beta^{p^r} = \alpha^{p^r} + \beta^{p^r} = \alpha + \beta, \tag{4.2}$$

porque $p \setminus \binom{p^r}{k}$ si $k = 1, \ldots, p^r - 1$. Por tanto, $\alpha + \beta \in E$ también. Se concluye que E es un *subcuerpo* de K con p^r elementos. La Proposición 4.3 implica que $E = K$. □

Definición 4.5. Si $q = p^r$ es una potencia de un primo, sea $\mathbb{F}_q$ el cuerpo finito (único) con q elementos.

Si $q = p$ es primo, este $\mathbb{F}_p$ es el cuerpo $\mathbb{Z}/p\mathbb{Z}$ de antes. Si σ es un *automorfismo* de $\mathbb{F}_p$, entonces $\sigma(\overline{1}) = \overline{1}$ necesariamente, luego $\sigma(\overline{k}) = \overline{k}$ para $k = 0, 1, \ldots, p-1$ por la aditividad de σ. Se concluye que el único automorfismo de $\mathbb{F}_p$ es $\sigma = \mathrm{id}$.

Definición 4.6. Sea F un cuerpo de característica $p \neq 0$. El **endomorfismo de Frobenius**[1] $\varphi\colon F \to F$ es la aplicación definida por $\varphi(a) := a^p$.

La fórmula (4.2), para $r = 1$, muestra que φ es aditivo; es obviamente multiplicativo y por ende es un homomorfismo, necesariamente inyectivo, que deja fijo el cuerpo primo $\mathbb{F}_p$.

Si F es un cuerpo *finito* de característica p, entonces φ es biyectivo. En tal caso, φ se llama el **automorfismo de Frobenius** de F.

Proposición 4.7. *Si $q = p^r$ es una potencia de un primo, el grupo de automorfismos* $\mathrm{Aut}(\mathbb{F}_q)$ *del cuerpo $\mathbb{F}_q$ es un grupo cíclico de orden r, generado por el automorfismo de Frobenius.*

Demostración. Sea φ el automorfismo de Frobenius de $\mathbb{F}_q$. Entonces $\varphi^r(a) = a^{p^r} = a$ para todo $a \in \mathbb{F}_q$, lo cual dice que $\varphi^r = \mathrm{id}$ en $\mathrm{Aut}(\mathbb{F}_q)$. Si φ fuera de orden s con $s < r$, entonces $a^{p^s} = a$ para todo $a \in \mathbb{F}_q$, de modo que $\mathbb{F}_q$ contendría p^r raíces distintas del polinomio $X^{p^s} - X$, lo cual es imposible. Por lo tanto, el subgrupo cíclico de $\mathrm{Aut}(\mathbb{F}_q)$ generado por φ tiene r elementos.

Ahora el grupo multiplicativo $\mathbb{F}_q^\times$ es cíclico, por la Proposición 3.40. Si $\alpha \in \mathbb{F}_q^\times$ es un generador de este grupo, entonces las potencias $\{\, \alpha^{p^k} : k = 0, 1, \ldots, r-1 \,\}$ son distintas. Sea $g(X) \in \mathbb{F}_p[X]$ el polinomio mínimo de α, cuyo grado divide $[\mathbb{F}_q\colon \mathbb{F}_p] = r$. Entonces para $k = 0, 1, \ldots, r-1$, es

$$g(\alpha^{p^k}) = g(\varphi^k(\alpha)) = \varphi^k(g(\alpha)) = \varphi^k(0) = 0,$$

de modo que los α^{p^k} son r raíces *distintas* de $g(X)$. Luego $\operatorname{gr} g(X) = r$ y además $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

Cada $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ deja fijo el cuerpo primo $\mathbb{F}_p$, así que $\mathrm{Aut}(\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_q \,|\, \mathbb{F}_p)$. En particular, σ queda determinado por $\sigma(\alpha)$. Pero $g(\sigma(\alpha)) = \sigma(g(\alpha)) = \sigma(0) = 0$, así que $\sigma(\alpha)$ es una raíz de $g(X)$. Luego $\sigma(\alpha) = \alpha^{p^k} = \varphi^k(\alpha)$ para algún k. Se concluye que el grupo cíclico generado por φ es todo $\mathrm{Aut}(\mathbb{F}_q)$. □

Corolario 4.8. *Si $q = p^r$ es una potencia de un primo, la extensión $\mathbb{F}_q \,|\, \mathbb{F}_p$ es cíclica y posee un elemento primitivo.*

Demostración. La extensión $\mathbb{F}_q \,|\, \mathbb{F}_p$ es obviamente finita, de grado r, y la Proposición anterior muestra que $\mathrm{Gal}(\mathbb{F}_q \,|\, \mathbb{F}_p) \simeq C_r$. Cualquier generador α del grupo cíclico $\mathbb{F}_q^\times$ es un elemento primitivo de la extensión, pues $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

Para ver que la extensión es normal, es cuestión de notar que $\mathbb{F}_q$ es el cuerpo de escisión sobre $\mathbb{F}_p$ del polinomio mínimo de α, cuyas raíces son $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{r-1}}$. La Proposición 2.32 garantiza la normalidad de $\mathbb{F}_q \,|\, \mathbb{F}_p$. □

Corolario 4.9. *Si $K \,|\, \mathbb{F}_q$ es una extensión finita del cuerpo finito $\mathbb{F}_q$, entonces $K \,|\, \mathbb{F}_q$ es cíclica y posee un elemento primitivo.*

Demostración. Si $[K\colon \mathbb{F}_q] = s$, entonces $K \simeq \mathbb{F}_{q^s}$ y las demostraciones de la Proposición 4.7 y el Corolario 4.8 ofrecen el resultado, al cambiar $q \mapsto q^s$, $p \mapsto q$ y $\varphi \mapsto \varphi_q$ donde $\varphi_q(a) := a^q$ para $a \in K$. □

[1] Un *endomorfismo* de un anillo A es un homomorfismo de A en sí mismo. No es necesariamente inyectivo (cuando A no es un cuerpo) ni sobreyectivo.

4.2 Extensiones separables y de Galois

En cuerpos de característica prima, se presenta un fenómeno curioso, de la existencia de polinomios irreducibles con raíces repetidas.

Ejemplo 4.10. Sea $K := \mathbb{F}_p(t)$ el cuerpo de funciones racionales en una variable t con coeficientes en $\mathbb{F}_p$. En este caso, por ser t trascendente sobre $\mathbb{F}_p$, el cuerpo K es infinito y su endomorfismo de Frobenius $\varphi\colon \alpha \mapsto \alpha^p$ no es sobreyectivo. Sea $F := \varphi(K)$ la imagen de este endomorfismo, que es un subcuerpo de K. Si $h(t) \in \mathbb{F}_p(t)$, es fácil ver que $\varphi(h(t)) = h(t^p)$, porque φ deja fijo el cuerpo primo $\mathbb{F}_p$.

Sea $\beta := \varphi(t) = t^p \in F$. Entonces $t \in K$ es un elemento algebraico sobre F, porque es una raíz del polinomio $X^p - \beta \in F[X]$. Luego K es una extensión algebraica de F. Si $\tilde{\varphi}\colon K[X] \to F[X] : f(X) \mapsto f^{\varphi}(X)$ es el isomorfismo de anillos que extiende el isomorfismo de cuerpos $\varphi\colon K \to F$, entonces $X^p - \beta = X^p - t^p = \tilde{\varphi}(X^p - t)$, así que los factores de $X^p - \beta$ en $F[X]$ son imágenes bajo $\tilde{\varphi}$ de los factores de $X^p - t$ en $K[X]$.

Pero el polinomio $X^p - t$ es irreducible en $K[X]$. Una manera de verificar esto es *aplicar el criterio de Eisenstein*: t es un elemento irreducible en el anillo entero $\mathbb{F}_p[t]$, cuyo cuerpo de fracciones es $\mathbb{F}_p(t)$; ahora el Lema de Gauss y el criterio de Eisenstein extienden al presente caso, al reemplazar $\mathbb{Z}$ por $\mathbb{F}_p[t]$, $\mathbb{Q}$ por $K = \mathbb{F}_p(t)$ y el primo p por el irreducible t. Se concluye que $X^p - \beta$ es irreducible en $F[X]$.

Luego, $t \in K$ es algebraico de grado p sobre F, con polinomio mínimo $X^p - \beta$. Ahora

$$X^p - \beta = X^p - t^p = (X - t)^p \quad \text{en } K[X].$$

Luego t es la única raíz en K, p veces repetida, del polinomio irreducible $X^p - \beta$ en $F[X]$.

Definición 4.11. Sea F un cuerpo cualquiera. Un polinomio *irreducible* $h(X) \in F[X]$ se llama **separable** sus raíces son distintas. En cambio, se dice que $h(X)$ es *puramente inseparable* si sus raíces son todas iguales.

Sea $K \mid F$ una extensión. Un elemento algebraico $\alpha \in K$ es *separable sobre* F si su polinomio mínimo es separable en $K[X]$, es decir, no tiene raíces múltiples. Además, $K \mid F$ es una **extensión separable** si cada elemento de K es separable sobre F.

En cambio, la extensión $K \mid F$ es **puramente inseparable** si cada elemento de K es puramente inseparable sobre F.

Proposición 4.12. *Una extensión algebraica $K \mid F$ es separable en los siguientes casos:*

(a) si F es de característica 0;

(b) si F es de característica p y el endomorfismo de Frobenius de F es sobreyectivo; en particular, si F es un cuerpo finito.

Demostración. Sea $\alpha \in K$ y sea $h(X) \in F[X]$ su polinomio mínimo.

Ad (a): Si $h(X) = (X - \alpha)^m f(X)$ en $K[X]$ con $m > 1$, $f(\alpha) \neq 0$, entonces su derivada es

$$h'(X) = m(X - \alpha)^{m-1} f(X) + (X - \alpha)^m f'(X),$$

y por tanto $h'(\alpha) = 0$. Pero $\operatorname{gr} h'(X) = \operatorname{gr} h(X) - 1$ y $h'(X)$ no es el polinomio nulo en $F[X]$: la ecuación $h'(\alpha) = 0$ contradice la minimalidad del polinomio $h(X)$. Se concluye que todo $\alpha \in K$ es una raíz simple de su polinomio mínimo.

Ad (b): Si α no es separable sobre F, sea $h(X) = (X - \alpha)\, l(X)$ en $K[X]$, donde $l(\alpha) = 0$. Entonces $h'(X) = l(X) + (X - \alpha)\, l'(X)$ cumple $h'(\alpha) = 0$. La minimalidad de $h(X)$ en este caso muestra que $h'(X) = 0$ en $F[X]$.

Obsérvese que la derivada del monomio X^p es $pX^{p-1} = 0$ en $F[X]$ por ser F de característica p. En general, un polinomio en $F[X]$ tiene derivada nula si y sólo si es de la forma

$$h(X) = g(X^p) = c_0 + c_p X^p + c_{2p} X^{2p} + \cdots + c_{kp} X^{kp}.$$

Como φ es sobreyectivo, hay $a_j \in F$ tal que $c_{jp} = \varphi(a_j) = a_j^p$ para $j = 0, 1, \ldots, k$. Luego,

$$h(X) = a_0^p + a_1^p X^p + a_2^p X^{2p} + \cdots + a_k^p X^{kp} = (a_0 + a_1 X + a_2 X^2 + \cdots + a_k X^k)^p =: (q(X))^p.$$

Pero entonces $h(X)$ tiene $q(X)$ como factor propio, lo cual contradice su irreducibilidad en $F[X]$. Se concluye que cada $\alpha \in K$ es separable sobre F. □

Definición 4.13. Una extensión algebraica $K \mid F$ es una **extensión de Galois** si es *normal y separable*.

► Antes de completar la discusión de las extensiones de Galois, es necesario revisar los argumentos y demostraciones anteriores en los lugares en donde se adujo la hipótesis de que un cuerpo K fuera un subcuerpo de $\mathbb{C}$. En todos esos casos, el papel del cuerpo $\mathbb{C}$, que es algebraicamente cerrado, es el de garantizar la existencia de raíces de un polinomio dado. Pero esta formulación es inadecuada para cuerpos de característica prima, que no están incluidos en $\mathbb{C}$, y para cuerpos como $\mathbb{Q}(X)$ que son de característica 0 pero tampoco caben dentro de $\mathbb{C}$.

Definición 4.14. Un cuerpo L es **algebraicamente cerrado** si todo polinomio en $L[X]$ escinde en L. Por el algoritmo de división, es suficiente que todo polinomio en $L[X]$ tenga al menos una raíz en L. Por el "teorema fundamental del álgebra", el cuerpo $\mathbb{C}$ es algebraicamente cerrado.

Si F es un cuerpo cualquiera, se dice que un cuerpo $\overline{F}$ es una **clausura algebraica** de F si (a) $F \subseteq \overline{F}$ y la extensión $\overline{F} \mid F$ es algebraica; y (b) $\overline{F}$ es algebraicamente cerrado.

La existencia de una clausura algebraica requiere una inducción transfinita. Sea $\mathcal{F}$ la familia de extensiones algebraicas de F.[2] Esta familia está parcialmente ordenado por inclusión, y la unión de una cadena creciente de extensiones algebraicas es una extensión algebraica. El Lema de Zorn garantiza que $\mathcal{F}$ contenga un elemento maximal $\overline{F}$ y su maximalidad asegura que $\overline{F}$ sea algebraicamente cerrado.

[2] Para guardar los protocolos de la teoría de conjuntos, se requiere que $\mathcal{F}$ sea parte de un universo no demasiado grande, para que sea un conjunto. Esto se puede garantizar de varias formas. Véase, por ejemplo, el libro de Serge Lang: *Algebra*, 3ª edición, Addison-Wesley, 1993, sección V.2.

Si $\iota\colon F \to \overline{F}$ es la inclusión y si $K\,|\,F$ es una extensión algebraica, entonces se puede extender ι a un homomorfismo inyectivo $\tilde{\iota}\colon K \to \overline{F}$, mediante otra Zornicación. Si K también es algebraicamente cerrada, entonces este homomorfismo es biyectivo, porque $\overline{F}$ es una extensión algebraica de $\tilde{\iota}(K)$. Por lo tanto, dos clausuras algebraicas de F son isomorfas (aunque no de manera canónica) y es permisible hablar de "la" clausura algebraica de F.

Repasemos brevemente los lugares en donde se ha usado la hipótesis $F \subseteq \mathbb{C}$ o bien $K \subseteq \mathbb{C}$.

En la Definición 2.27 de *elemento conjugado de* α como raíz del polinomio mínimo de α, dicha raíz puede tomarse en $\overline{F}$: los conjugados de α son elementos de $\overline{F}$, en general.

El Lema 2.34 debe decir que $\varphi(\alpha)$ es un conjugado de α para todo $\varphi \in \mathrm{Hom}_F(K,\overline{F})$; y que, para un conjugado dado $\beta \in \overline{F}$ de α, existe un único F-morfismo $\varphi\colon F(\alpha) \to \overline{F}$ con $\varphi(\alpha) = \beta$.

En la Proposición 2.36, el enunciado modificado es el siguiente: *Si $K\,|\,F$ es una extensión* ***separable*** *de grado finito n y si $\varphi \in \mathrm{Hom}_F(K,\overline{F})$, entonces hay exactamente n homomorfismos $\psi\colon K \to \overline{F}$ que extienden φ*. La separabilidad es esencial porque en la demostración se usó la propiedad de que las raíces de un polinomio irreducible son distintas. Para característica prima, esta propiedad no es automática: hace falta obligar que dicho polinomio sea separable.

El *Teorema del Elemento Primitivo* merece un nuevo tratamiento.

Teorema 4.15. *Sea $K\,|\,F$ una extensión finita* ***y separable****. Entonces hay un elemento $\alpha \in K$ tal que $K = F(\alpha)$.*

Demostración. Si el cuerpo F es infinito, la demostración del Teorema 2.39 es aplicable, *mutatis mutandis*.[3] Concretamente: se reemplaza $\mathrm{Hom}_F(K,\mathbb{C})$ por $\mathrm{Hom}_F(K,\overline{F})$ y se omite el argumento de que $\mathbb{Q} \subseteq F$: por ser F infinito por hipótesis, el Lema 2.38 se usa directamente. La separabilidad es esencial porque se arguye que los conjugados del elemento primitivo α deben ser distintos.

En cambio, si el cuerpo F es finito, con $|F| = q = p^r$ y $|K| = q^s$, basta tomar α como cualquier generador del grupo cíclico $K^\times$. Entonces $K = \{0\} \cup \{\, \alpha^k : k = 1,\dots,q^s-1 \,\}$, así que $K = \mathbb{F}_p(\alpha) = F(\alpha)$. □

En la Proposición 3.2, la desigualdad $\big|\mathrm{Gal}(K\,|\,F)\big| \leq [K\colon F]$ vale para cualquier extensión $K\,|\,F$ que sea finita **y separable**. (En su demostración, se exige que los conjugados de un elemento de K sean distintas, aunque no todas pertenezcan a K.)

En el Corolario 3.4, se obtiene la igualdad $\big|\mathrm{Gal}(K\,|\,F)\big| = [K\colon F]$ cuando la extensión $K\,|\,F$ es finita, separable y normal.

En el Teorema 3.9 de Artin, no se necesita que $K \subseteq \mathbb{C}$. En su desarrollo, se llega a demostrar que el polinomio $q(X)$ que define K como cuerpo de escisión sobre K^H *tiene raíces distintas*. Luego la extensión $K\,|\,K^H$ no es sólo normal sino también separable. El enunciado general es el siguiente.

Teorema 4.16 (Artin)**.** *Sea K un cuerpo cualquiera y sea H un grupo finito de automorfismos de H. Entonces la extensión $K\,|\,K^H$* ***es de Galois*** *y $\mathrm{Gal}(K\,|\,K^H) = H$.* ⊟

[3] Este latinajo significa: *cambiando lo que haya que cambiar*.

El Corolario 3.10 merece una nueva mirada.

Corolario 4.17. *Si $K\,|\,F$ es una extensión finita, con grupo de Galois $G = \mathrm{Gal}(K\,|\,F)$, entonces la extensión $K\,|\,F$ es de Galois si y sólo si $K^G = F$.*

Demostración. Si $K\,|\,F$ es de Galois, es decir, normal y separable, entonces $|G| = [K\colon F]$; en particular, G es un grupo finito. Por el teorema anterior, es $|G| = [K\colon K^G]$ por la misma razón. La definición de G implica que $F \subseteq K^G$. Luego $[K^G\colon F] = [K\colon F]\big/[K\colon K^G] = 1$ y por ende $K^G = F$.

Por otro lado, si $K^G = F$, entonces $K\,|\,F$ es de Galois como consecuencia inmediata del Teorema de Artin. □

Algunos autores toman la condición de que $K^G = F$ como la definición de "extensión de Galois" y luego demuestran que tales extensiones son normales y separables. En todo caso, la *correspondencia de Galois*, fruto del Teorema Principal, sigue válida para estas extensiones. En definitiva, se puede modificar el enunciado del Teorema 3.13 como sigue.
Si $K\,|\,F$ es una extensión finita ***de Galois****, las correspondencias $\Phi_{K|F}\colon E \mapsto \mathrm{Gal}(K\,|\,E)$ y $\Psi_{K|F}\colon H \mapsto K^H$ entre cuerpos intermedios de $K\,|\,F$ y subgrupos de $\mathrm{Gal}(K\,|\,F)$ son biyecciones inversas que cumplen las propiedades (a) – (f) del Teorema 3.13.*

4.3 Ejercicios sobre cuerpos finitos

En los problemas que siguen, p es un número primo. Si $q = p^r$ con $r \in \mathbb{N}^*$, $\mathbb{F}_q$ denotará el cuerpo finito con q elementos.

Ejercicio 4.1. (a) Mostrar que $\mathbb{F}_{p^r}$ es isomorfo a un subcuerpo de $\mathbb{F}_{p^s}$ si y sólo si $r \setminus s$.

(b) Exhibir el retículo de cuerpos intermedios de la extensión $\mathbb{F}_{p^{24}}\,|\,\mathbb{F}_p$.

(c) ¿Cuál es el grupo de Galois $\mathrm{Gal}(\mathbb{F}_{p^{24}}\,|\,\mathbb{F}_p)$? cuáles son todos sus subgrupos?

Ejercicio 4.2. (a) Si $p \equiv 3 \bmod 4$, mostrar que X^2+1 es irreducible en $\mathbb{F}_p[X]$.

(b) Si $p \equiv 1 \bmod 4$, mostrar que X^2+1 escinde en $\mathbb{F}_p[X]$.[4]

Ejercicio 4.3. Si $q = p^r$ con $r > 1$, y si $s > 1$, mostrar que $\mathrm{Gal}(\mathbb{F}_{q^s}\,|\,\mathbb{F}_q)$ es un grupo cíclico.

Ejercicio 4.4. (a) Si F es un cuerpo finito de característica p, sea $f(X) := X^p - X - 1 \in F[X]$. Si $\alpha \in F$ es una raíz de este $f(X)$, comprobar que $(\alpha + \overline{k})$ es una raíz de $f(X)$ para todo $\overline{k}$ en el cuerpo primo $\mathbb{F}_p$.

(b) Concluir que $f(X)$ es irreducible en $F[X]$, o bien $f(X)$ escinde en $F[X]$.

(c) Mostrar que el polinomio $X^p - X - 1$ es irreducible en $\mathbb{F}_p[X]$.

Ejercicio 4.5. (a) Si $f(X)$ es un polinomio mónico en $\mathbb{Z}[X]$, sea $\overline{f}(X) \in \mathbb{F}_p[X]$ su reducción módulo p, obtenida al reemplazar cada coeficiente a_k de $f(X)$ por su residuo $\overline{a_k} \in \mathbb{F}_p$. Si $\overline{f}[X]$ es irreducible en $\mathbb{F}_p[X]$, mostrar que $f(X)$ es irreducible en $\mathbb{Z}[X]$.

(b) Concluir que $X^p - X - 1$ es irreducible en $\mathbb{Z}[X]$ para todo primo p.

(c) Sea $h(X) := X^5 - 5X^4 - 6X - 1$. ¿Es $h(X)$ reducible o irreducible en $\mathbb{Z}[X]$?

[4] Ejercicio tomado de los apuntes de Baker.

Ejercicio 4.6. (a) Si $h(X) \in \mathbb{F}_p[X]$ es un factor irreducible de $X^{p^r} - X$ con $\operatorname{gr} h(X) = m$, mostrar que $m \setminus r$.

⟦ Indicación: Considerar el cuerpo de escisión de $h(X)$ sobre $\mathbb{F}_p$. ⟧

(b) Factorizar $X^9 - X$ en $\mathbb{F}_3[X]$.

Ejercicio 4.7. Mostrar que el polinomio $f(X) = X^4 - 10X^2 + 1$ es irreducible en $\mathbb{Z}[X]$, pero es reducible en $\mathbb{F}_p[X]$ para todo primo p.

Para la reducción en $\mathbb{F}_p[X]$, considérese las siguientes factorizaciones en $\mathbb{R}[X]$:[5]

$$\begin{aligned} X^4 - 10X^2 + 1 &= (X^2 - 2\sqrt{2}X - 1)(X^2 + 2\sqrt{2}X - 1) \\ &= (X^2 - 2\sqrt{3}X + 1)(X^2 + 2\sqrt{3}X + 1) \\ &= (X^2 - (5 + 2\sqrt{6}))(X^2 - (5 - 2\sqrt{6})). \end{aligned}$$

Mostrar que si $\overline{k}$ y $\overline{l}$ no son cuadrados en $\mathbb{F}_p$, entonces su producto $\overline{kl}$ sí es un cuadrado en $\mathbb{F}_p$. ⟦ Indicación: El grupo $\mathbb{F}_p^\times$ es cíclico. ⟧ Concluir que al menos uno de entre $\overline{2}$, $\overline{3}$, $\overline{6}$ es un cuadrado en $\mathbb{F}_p$ para todo primo p.

[5] Ejercicio tomado de los apuntes de Milne.

5 Extensiones de Hopf–Galois

El teorema principal de la teoría de Galois establece una correspondencia entre los cuerpos intermedios de una extensión $K \mid F$ y los subgrupos de su grupo de Galois $\mathrm{Gal}(K \mid F)$. Su validez depende fuertemente de que esta extensión sea de Galois, es decir, separable y normal. Si la extensión no es normal, el grupo de Galois suele ser demasiado pequeño: no hay suficientes F-automorfismos de K para obtener la correspondencia. Sin embargo, en algunos casos se puede emplear "automorfismos generalizados" de $K \mid F$ que son aditivos pero no multiplicativos. Estos casos sugieren que sería provechosa reemplazar el grupo de Galois por una estructura algebraica más flexible.

Otra motivación para ampliar el concepto de extensión de Galois es la de clasificar extensiones de álgebras o anillos que no necesariamente son cuerpos. La teoría general de estas extensiones para álgebras conmutativas fue desarrollada a partir de 1965.[1] Hoy en día hay una intensa actividad de investigación en la clasificación de extensiones de álgebras y anillos no necesariamente conmutativos.

5.1 Endomorfismos de una extensión

Definición 5.1. Sea $K \mid F$ una extensión de cuerpos. Si una aplicación $\sigma\colon K \to K$ cumple

$$\left\{ \begin{array}{c} \varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta) \\ \varphi(c\alpha) = c\,\varphi(\alpha) \end{array} \right\} \qquad \text{si } \alpha, \beta \in K,\ c \in F,$$

(es decir, σ es *F-lineal*) se dice que σ es un F-**endomorfismo** de K. La totalidad $\mathrm{End}_F(K)$ de tales F-endomorfismos es un álgebra sobre F, de dimensión $[K\colon F]^2$.

Es importante señalar que un F-endomorfismo no es necesariamente multiplicativo, es decir, que $\varphi(\alpha\beta) \neq \varphi(\alpha)\,\varphi(\beta)$ en general.[2] Para cada $\alpha \in K$, el "operador de multiplicación" $\mu(\alpha) : \beta \mapsto \alpha\beta$ es evidentemente F-lineal. Esto define una inyección $\mu\colon K \to \mathrm{End}_F(K)$.

Ejemplo 5.2. La extensión $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ es separable pero no es normal, y su grupo de Galois es trivial. Escríbase $\xi := \sqrt[3]{2}$ para mayor comodidad; entonces $\{1, \xi, \xi^2\}$ es una base de $K = \mathbb{Q}(\xi)$ como espacio vectorial sobre $\mathbb{Q}$. Defínase dos $\mathbb{Q}$-endomorfismos c, s de $\mathbb{Q}(\xi)$ por su acción sobre esta base:

$$\begin{array}{lll} c(1) := 1, & c(\xi) := -\frac{1}{2}\xi, & c(\xi^2) := -\frac{1}{2}\xi^2, \\ s(1) := 0, & s(\xi) := +\frac{1}{2}\xi, & s(\xi^2) := -\frac{1}{2}\xi^2. \end{array}$$

[1] Las fuentes primarias son el artículo de Stephen U. Chase, David K. Harrison y Alex Rosenberg, "Galois theory and Galois cohomology of commutative rings", Memoirs of the AMS 52 (1965), 15–33; y la monografía de Stephen U. Chase y Moss E. Sweedler, *Hopf Algebras and Galois Theory*, Lecture Notes in Mathematics 97, Springer, New York, 1969.

[2] Anteriormente, se llamó "F-morfismo" a una aplicación entre dos extensiones de F que fuera F-lineal y también multiplicativa. Esta usanza es inconsistente con el actual uso de la palabra "endomorfismo", por lo que se ruega disculpas del lector. En la literatura del álgebra superior, esta palabra se usa en ambos sentidos, a menudo sin previo aviso. *Caveat lector*.

Obsérvese que para $\alpha \in K$, es $\alpha \in \mathbb{Q}$ si y sólo si $c(\alpha) = \alpha$ y $s(\alpha) = 0$.

Sea $\underline{H := \mathbb{Q}(c,s)} \subset \mathrm{End}_{\mathbb{Q}}(K)$. Fíjese que

$$cs = sc, \quad c^2 + 3s^2 = \mathrm{id}, \quad (2c+\mathrm{id})s = 0, \quad (2c+\mathrm{id})(c-\mathrm{id}) = 0.$$

Luego $H \simeq \mathbb{Q}[X,Y]\big/\big(X^2+3Y^2-1,\ (2X+1)Y,\ (2X+1)(X-1)\big)$ es una subálgebra conmutativa de $\mathrm{End}_{\mathbb{Q}}(K)$, de dimensión 3. En efecto, como cs, c^2, s^2 pueden expresarse como combinaciones lineales de $\{\mathrm{id}, c, s\}$ y éstos son linealmente independientes entre sí, es $\dim_{\mathbb{Q}} H = 3$. Es fácil comprobar que $\mu(K)H = \mathrm{End}_{\mathbb{Q}}(K)$ como espacio $\mathbb{Q}$-vectorial.[3]

Es evidente que las aplicaciones lineales c y s no son automorfismos de $\mathbb{Q}(\sqrt[3]{2})$; la s ni siquiera es sobreyectiva. Sin embargo, como pareja cumplen las siguientes fórmulas, parecidas a las reglas de adición para las funciones trigonométricas coseno y seno:

$$\begin{aligned} c(\alpha\beta) &= c(\alpha)\,c(\beta) - 3\,s(\alpha)\,s(\beta), \\ s(\alpha\beta) &= s(\alpha)\,c(\beta) + c(\alpha)\,s(\beta). \end{aligned} \tag{5.1}$$

Estas igualdades son evidentes si $\alpha = 1$ o bien $\beta = 1$, y es fácil comprobarlos para $\alpha, \beta \in \{\xi, \xi^2\}$. Por ejemplo, para el caso $\alpha = \beta = \xi$ es inmediato que

$$c(\xi)^2 - 3\,s(\xi)^2 = \tfrac{1}{4}\xi^2 - \tfrac{3}{4}\xi^2 = -\tfrac{1}{2}\xi^2 = c(\xi^2), \qquad 2\,s(\xi)\,c(\xi) = -\tfrac{1}{2}\xi^2 = s(\xi^2).$$

Por linealidad, (5.1) se verifica para todo $\alpha, \beta \in \mathbb{Q}(\xi)$. En la próxima subsección, se introduce un formalismo que permite deducir estas relaciones a partir de un "coproducto" en H, de modo que (5.1) se presenta así:

$$\Delta(c) = c \otimes c - 3\,s \otimes s, \qquad \Delta(s) = s \otimes c + c \otimes s. \tag{5.2}$$

En ese formalismo, un automorfismo φ, que obedece $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$, cumple la relación $\Delta(\varphi) = \varphi \otimes \varphi$. Los endomorfismos id, c y s generan una *coálgebra* que reemplaza el grupo de Galois.

5.2 Algebras de Hopf

Definición 5.3. Sean U y V dos espacios vectoriales sobre un cuerpo F. Sea $B(U,V)$ la totalidad de aplicaciones bilineales $s\colon U \times V \to F$. Si $u \in U$, $v \in V$, entonces $u \otimes v : s \mapsto s(u,v)$ es F-lineal, así que pertenece al espacio dual $B(U,V)^*$. El subespacio de $B(U,V)^*$ generado por estos elementos se denota $\underline{U \otimes V}$ y se llama el **producto tensorial** de U y V sobre F. Cualquier elemento de $U \otimes V$ es una suma finita $\sum_j u_j \otimes v_j$ de estos "tensores simples", que cumplen las siguientes propiedades de combinación:

$$\begin{aligned} (u_1 + u_2) \otimes v &= u_1 \otimes v + u_2 \otimes v, \\ u \otimes (v_1 + v_2) &= u \otimes v_1 + u \otimes v_2, \\ a(u \otimes v) &= au \otimes v = u \otimes av, \end{aligned}$$

si $u, u_1, u_2 \in U$, $v, v_1, v_2 \in V$ y $a \in F$.

[3] Este ejemplo está tomado del artículo: Cornelius Greither y Bodo Pareigis, "Hopf Galois theory for separable field extensions", J. Algebra 106 (1987), 239–258. Este trabajo es una pieza clave de la teoría aquí esbozado.

La expresión $\sum_{j=1}^{r} u_j \otimes v_j$ para un elemento de $U \otimes V$ no es única, pero se puede suponer que los $u_1, \ldots, u_r$ son linealmente independientes en U y que los $v_1, \ldots, v_r$ son linealmente independientes en V. En consecuencia, se ve que $\dim_F(U \otimes V) = (\dim_F U)\,(\dim_F V)$ cuando estas dimensiones son finitas.

El producto tensorial posee *una propiedad universal*: si W es otro espacio vectorial sobre F, entonces cualquier aplicación *bilineal* $s\colon U \times V \to W$ determina una única aplicación *lineal* $\tilde{s}\colon U \otimes V \to W$ por $\tilde{s}(u \otimes v) := s(u, v)$. En un diagrama:

$$\begin{array}{ccc} U \otimes V & \overset{\tilde{s}}{\searrow} & \\ \uparrow & & W \\ U \times V & \underset{s}{\nearrow} & \end{array} \tag{5.3}$$

Dados tres espacios vectoriales U, V, W sobre F, es fácil comprobar que hay un isomorfismo F-lineal único de $(U \otimes V) \otimes W$ en $U \otimes (V \otimes W)$ tal que $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$ para $u \in U$, $v \in V$, $w \in W$. Por lo tanto, se escribe $U \otimes V \otimes W$ sin paréntesis, con elementos $u \otimes v \otimes w$. De igual modo, hay un isomorfismo F-lineal único

$$\tau\colon U \otimes V \to V \otimes U \quad \text{dado por} \quad \tau(u \otimes v) := v \otimes u. \tag{5.4}$$

También se identifica, $F \otimes U \simeq U \simeq U \otimes F$, porque $\dim_F F = 1$, mediante las isomorfismos naturales $1 \otimes u \leftrightarrow u \leftrightarrow u \otimes 1$.

Definición 5.4. Sea F un cuerpo. Un **álgebra** sobre F es un anillo A (con identidad 1_A) que es a la vez un espacio vectorial sobre F, tal que el producto asociativo $A \times A \to A$ sea bilineal. En vista de (5.3), el producto puede considerarse alternativamente como una aplicación *lineal* $m\colon A \otimes A \to A$. La presencia de $1_A \in A$ determina una inclusión $\eta\colon F \to A$ por $\eta(c) := c\,1_A$, que es trivialmente lineal. De este modo, un álgebra sobre F puede definirse como un triplete (A, m, η), en donde A es un espacio F-vectorial, m y η son aplicaciones F-lineales, y se exigen las siguientes dos propiedades:

1. Asociatividad: $m(m \otimes \mathrm{id}) = m(\mathrm{id} \otimes m) : A \otimes A \otimes A \to A$;
2. Unidad: $m(\eta \otimes \mathrm{id}) = m(\mathrm{id} \otimes \eta) = \mathrm{id} : A \to A$.

Estas propiedades pueden ilustrarse mediante dos diagramas conmutativas:

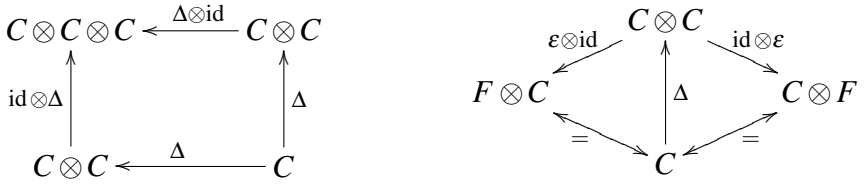
$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{m \otimes \mathrm{id}} & A \otimes A \\ \downarrow{\scriptstyle \mathrm{id} \otimes m} & & \downarrow{\scriptstyle m} \\ A \otimes A & \xrightarrow{m} & A \end{array} \qquad \begin{array}{ccccc} & \overset{\eta \otimes \mathrm{id}}{\nearrow} & A \otimes A & \overset{\mathrm{id} \otimes \eta}{\nwarrow} & \\ F \otimes A & & \downarrow{\scriptstyle m} & & A \otimes F \\ & \underset{=}{\searrow} & & \underset{=}{\swarrow} & \\ & & A & & \end{array} \tag{5.5}$$

El concepto dual de un álgebra, en el sentido categórico, es una "coálgebra", obtenido formalmente por reversión de las flechas en los diagramas (5.5).

Definición 5.5. Una **coálgebra** sobre un cuerpo F es triplete (C,Δ,ε), en donde C es un espacio F-vectorial y $\Delta\colon C\to C\otimes C$ y $\varepsilon\colon C\to F$ son aplicaciones F-lineales que cumplen las siguientes dos propiedades:

1. Coasociatividad: $(\Delta\otimes\mathrm{id})\Delta=(\mathrm{id}\otimes\Delta)\Delta : C\to C\otimes C\otimes C$;
2. Counidad: $(\varepsilon\otimes\mathrm{id})\Delta=(\mathrm{id}\otimes\varepsilon)\Delta=\mathrm{id} : C\to C$.

Se dice que Δ es un **coproducto** sobre C y que ε es una **counidad** para C. Fíjese que Δ es necesariamente inyectivo porque posee un inverso a la izquierda. Estas propiedades se exhiben en dos diagramas conmutativas:



(5.6)

Ejemplo 5.6. Un producto *agrega* dos objetos en un uno; un coproducto *reparte* un objeto en dos. Para comprender su significado, considérese el álgebra de polinomios $F[X]$. Posee un producto bilineal, que sólo necesita definirse sobre la base vectorial de los monomios: $m(X^k\otimes X^l):=X^{k+l}$, como ya se sabe. Pero resulta que $F[X]$ también es una coálgebra, bajo el coproducto definido por

$$\Delta(X^n):=\sum_{k=0}^{n}\binom{n}{k}X^k\otimes X^{n-k}. \tag{5.7}$$

La counidad es $\varepsilon(X^n):=0$, $\varepsilon(1):=1$, extendido por linealidad. Esta estructura se llama la *coálgebra binomial*, con diversas aplicaciones combinatoriales.[4]

Obsérvese que las dos estructuras de $F[X]$ son compatibles, porque tanto Δ como ε respetan el producto, es decir, son homomorfismos sobre el álgebra $F[X]$. En efecto,

$$\begin{aligned}\Delta(X^m)\Delta(X^n)&=\sum_{j=0}^{m}\sum_{k=0}^{n}\binom{m}{j}\binom{n}{k}X^jX^k\otimes X^{m-j}X^{n-k}\\&=\sum_{r=0}^{m+n}\sum_{j+k=r}\binom{m}{j}\binom{n}{k}X^{j+k}\otimes X^{m+n-j-k}\\&=\sum_{r=0}^{m+n}\binom{m+n}{r}X^r\otimes X^{m+n-r}=\Delta(X^{m+n}),\end{aligned}$$

al usar la identidad de Vandermonde. En otras palabras, $F[X]$ es una *biálgebra*.

[4]La reformulación de problemas combinatoriales en el lenguaje de las coálgebras fue uno de los grandes temas del trabajo de Gian-Carlo Rota. Véase: Saj-Nicole Joni y Gian-Carlo Rota, "Coalgebras and bialgebras in combinatorics", en el libro *Umbral Calculus and Hopf Algebras*, AMS, Providence, RI, 1979, pp. 1–47.

Definición 5.7. Una **biálgebra** sobre F es un quinteto $(A, m, \eta, \Delta, \varepsilon)$, tal que (A, m, η) es un álgebra, (A, Δ, ε) es una coálgebra, y tanto $\Delta\colon A \to A \otimes A$ como $\varepsilon\colon A \to F$ son homomorfismos de álgebras.

La manera de denotar un producto es conocido: se escribe $ab := m(a \otimes b)$, por yuxtaposición. Hay una notación generalmente aceptada, introducido por Sweedler, para denotar un coproducto. Se escribe

$$\Delta(a) =: \sum a_{(1)} \otimes a_{(2)}. \tag{5.8}$$

El símbolo $\sum$ toma cuenta de que el lado derecho generalmente no es un tensor simple, sino una suma finita de tensores simples; véase (5.7), por ejemplo. Sin embargo, se suele omitir el índice de esta sumatoria. La coasociatividad de Δ se expresa por la relación

$$\sum a_{(1)(1)} \otimes a_{(1)(2)} \otimes a_{(2)} = \sum a_{(1)} \otimes a_{(2)(1)} \otimes a_{(2)(2)},$$

la cual puede reescribirse, sin ambigüedad, como

$$(\Delta \otimes \mathrm{id})(\Delta(a)) = (\mathrm{id} \otimes \Delta)(\Delta(a)) =: \sum a_{(1)} \otimes a_{(2)} \otimes a_{(3)}. \tag{5.9}$$

La propiedad de counidad se expresa en notación de Sweedler mediante

$$\sum \varepsilon(a_{(1)})\, a_{(2)} = \sum a_{(1)}\, \varepsilon(a_{(2)}) = a \in A. \tag{5.10}$$

Ejemplo 5.8. Sea G un grupo finito, F un cuerpo. El **álgebra de grupo** $F[G]$ es la totalidad de sumas $\sum_{g \in G} a_g \cdot g$ con cada $a_g \in F$. En otras palabras, $F[G]$ es un espacio vectorial sobre F, de dimensión $|G|$, con una base etiquetada por los elementos de G. El producto en $F[G]$ se define así:

$$\left(\sum_{g \in G} a_g \cdot g\right)\left(\sum_{h \in G} b_h \cdot h\right) := \sum_{g,h \in G} a_g b_h \cdot gh = \sum_{k \in G}\left(\sum_{gh=k} a_g b_h\right) \cdot k.$$

En otras palabras, se extiende bilinealmente la multiplicación del grupo G; sería equivalente definir $m(g \otimes h) := gh$ sobre los elementos de la base vectorial de $F[G] \otimes F[G]$.

El coproducto Δ y la counidad sobre $F[G]$ se definen sobre los elementos de la base por

$$\Delta(g) := g \otimes g, \quad \varepsilon(g) := 1, \quad \text{para todo} \quad g \in G. \tag{5.11}$$

Como $\Delta(gh) = gh \otimes gh = (g \otimes g)(h \otimes h) = \Delta(g)\Delta(h)$ y $\varepsilon(gh) = 1 = \varepsilon(g)\varepsilon(h)$, es evidente que $F[G]$ es una biálgebra.

Si G es un grupo no abeliano, entonces el álgebra $F[G]$ no es conmutativa. Abstractamente, un álgebra (A, m, η) es conmutativa si $ab = ba$ o bien $m(a \otimes b) = m(b \otimes a)$ para todo $a, b \in A$. En términos de la aplicación de trueque τ de (5.4), la conmutatividad se expresa por la relación $m \circ \tau = m$.

Dualmente, se dice que una coálgebra C es *coconmutativo* si $\tau \circ \Delta = \Delta : C \to C \otimes C$. En notación de Sweedler, esta condición es

$$\sum a_{(1)} \otimes a_{(2)} = \sum a_{(2)} \otimes a_{(1)} \quad \text{para todo} \quad a \in C.$$

Es evidente de (5.11) que $F[G]$ es coconmutativo.

Ejemplo 5.9. Sea G un grupo finito, F un cuerpo. La **biálgebra de funciones** $\mathcal{O}(G)$, a veces denotado por F^G, es la totalidad de funciones $f\colon G \to F$ con la suma y producto usuales, es decir,

$$(f+l)(g) := f(g)+l(g), \qquad (fl)(g) := f(g)\,l(g).$$

Es un espacio vectorial sobre F, de dimensión $|G|$, con una base $\{\, e_g : g \in G\,\}$ donde $e_g(h) := \delta_{g,h}$ con la delta de Kronecker. El producto obedece $m(e_g \otimes e_h) = \delta_{g,h}\, e_g$.

Si $g \in G$, la evaluación $f \mapsto f(g) \in F$ es una función lineal sobre $\mathcal{O}(G)$. Si $f, l \in \mathcal{O}(G)$, la Definición 5.3 permite identificar $f \otimes l$ con la función de dos variables $(g,h) \mapsto f(g)\,l(h)$. Esta identificación lleva el producto tensorial $\mathcal{O}(G) \otimes \mathcal{O}(G)$ en el álgebra de funciones $\mathcal{O}(G \times G)$ sobre el producto directo $G \times G$ de dos copias de G.

El coproducto $\Delta\colon \mathcal{O}(G) \to \mathcal{O}(G \times G)$ se define por transponer la multiplicación en G, así:

$$\Delta(f)(g,h) := f(gh), \quad \text{para todo} \quad g,h \in G. \tag{5.12}$$

La coasociatividad de $\mathcal{O}(G)$ es consecuencia de la asociatividad de G:

$$\begin{aligned}(\Delta \otimes \mathrm{id})(\Delta(f))(g,h,k) &= \Delta(f)(gh,k) = f((gh)k) = f(g(hk)) \\ &= \Delta(f)(g,hk) = (\mathrm{id} \otimes \Delta)(\Delta(f))(g,h,k).\end{aligned}$$

La counidad en $\mathcal{O}(G)$ es dado por $\varepsilon(f) := f(1_G)$. Luego $\mathcal{O}(G)$ es una biálgebra. Si G es un grupo no abeliano, esta biálgebra es conmutativa pero no es coconmutativa.

Ejemplo 5.10. Sea H el álgebra tridimensional sobre $\mathbb{Q}$ generado por id, c, s, introducida en el Ejemplo 5.2. Defínase $\Delta\colon H \to H \otimes H$ por $\Delta(\mathrm{id}) := \mathrm{id} \otimes \mathrm{id}$ y $\Delta(c)$, $\Delta(s)$ dados por la fórmula (5.2), extendiendo por linealidad sobre $\mathbb{Q}$. Defínase $\varepsilon(\mathrm{id}) = \varepsilon(c) := 1$ y $\varepsilon(s) := 0$. Es fácil verificar que H es una biálgebra con estas operaciones.

Definición 5.11. Sea (A, m, η) un álgebra y (C, Δ, ε) una coálgebra sobre F. Denótese por $\mathrm{Hom}(C,A)$ el espacio F-vectorial de aplicaciones lineales $f\colon C \to A$. La **convolución** de dos elementos f, h de este espacio es el elemento $f * h \in \mathrm{Hom}(C,A)$ dado por

$$f * g := m(f \otimes g)\Delta : C \to A. \tag{5.13}$$

En la notación de Sweedler, esta fórmula es

$$(f * g)(c) := \sum f(c_{(1)})\, h(c_{(2)}) \in A, \quad \text{para todo} \quad c \in C.$$

La convolución es una operación asociativa:

$$\begin{aligned}((f * h) * k)(c) &= \sum (f * h)(c_{(1)})\, k(c_{(2)}) = \sum f(c_{(1)})\, h(c_{(2)})\, k(c_{(3)}) \\ &= \sum f(c_{(1)})\, (h * k)(c_{(2)}) = (f * (h * k))(c),\end{aligned}$$

donde la coasociatividad de C ha sido usado, mediante (5.9), en la enumeración de las "patas" de c; y la asociatividad de A ha sido usado de una forma igualmente implícita.

La convolución hace de $\mathrm{Hom}(C,A)$ un álgebra sobre F. Su elemento identidad es la aplicación $\eta\varepsilon\colon C \to F \to A$. En efecto, se ve que para todo $c \in C$,

$$\begin{aligned}(f * \eta\varepsilon)(c) &= \sum f(c_{(1)})\, \varepsilon(c_{(2)}) = f\big(\textstyle\sum c_{(1)}\, \varepsilon(c_{(2)})\big) = f(c), \\ (\eta\varepsilon * f)(c) &= \sum \varepsilon(c_{(1)})\, f(c_{(2)}) = f\big(\textstyle\sum \varepsilon(c_{(1)})\, c_{(2)}\big) = f(c).\end{aligned}$$

Si A es una biálgebra, entonces los endomorfismos (lineales, no necesariamente multiplicativas) forman un álgebra $\mathrm{End}(A) = \mathrm{Hom}(A,A)$ bajo convolución. En este caso, la aplicación identidad $\underline{\mathrm{id}}\colon A \to A$ pertenece a $\mathrm{End}(A)$ pero no es la identidad de este álgebra (la composición de aplicaciones lineales y la convolución son operaciones diferentes). Se plantea la inversibilidad de $\underline{\mathrm{id}}$ bajo convolución.

Definición 5.12. Un **álgebra de Hopf** es una biálgebra $(H, m, \eta, \Delta, \varepsilon)$ sobre un cuerpo F tal que $\mathrm{End}(H)$ contiene un elemento S, necesariamente único, que es un inverso de convolución para el elemento $\underline{\mathrm{id}}$:

$$\mathrm{id} * S = m(\mathrm{id} \otimes S)\Delta = \eta\varepsilon, \qquad S * \mathrm{id} = m(S \otimes \mathrm{id})\Delta = \eta\varepsilon. \tag{5.14}$$

Esta aplicación lineal $S\colon H \to H$ se llama el **antípoda** de H. En la notación de Sweedler, sus propiedades son:

$$\sum a_{(1)} S(a_{(2)}) = \sum S(a_{(1)}) a_{(2)} = \varepsilon(a)\, 1_H \quad \text{para todo} \quad a \in H. \tag{5.15}$$

Ejemplo 5.13. En el álgebra de grupo $F[G]$, el antípoda se define por

$$S(g) := g^{-1} \quad \text{para todo} \quad g \in G,$$

extendido por linealidad. La fórmula (5.15) se reduce a $g\,g^{-1} = g^{-1}\,g = 1$ en el grupo G.

Ejemplo 5.14. En la biálgebra de funciones $\mathcal{O}(G)$, el antípoda transpone la inversión en el grupo:

$$S(f)(g) := f(g^{-1}), \quad \text{para todo} \quad g \in G,\ f \in \mathcal{O}(G).$$

La fórmula (5.14) se reduce a la relación $f(g\,g^{-1}) = f(g^{-1}\,g) = f(1)$ en $\mathcal{O}(G)$.

Ejemplo 5.15. Para el ejemplo $H = \mathrm{lin}\langle \mathrm{id}, c, s\rangle$, se comprueba que la aplicación $S\colon H \to H$ determinado por $S(\mathrm{id}) := \mathrm{id}$, $S(c) := c$, $S(s) := -s$, cumple (5.15) y por ende es una antípoda para H.

Los Ejemplos 5.13 y 5.14 ponen en evidencia un concepto importante, el de la *dualidad* entre álgebras de Hopf. Ya se sabe que cada espacio vectorial V sobre F *de dimensión finita* posee un *espacio dual* $V^* := \mathrm{Hom}(V,F)$, que es la totalidad de aplicaciones F-lineales[5] de V en F. Resulta que $\dim_F V^* = \dim_F V$, así que los espacios V y V^* son linealmente isomorfos, aunque no de modo natural (se requiere elegir una base en cada espacio para definir un isomorfismo entre ellos). Por otro lado, el dual doble $V^{**} := \mathrm{Hom}(V^*,F)$ es isomorfo a V de modo canónico: si $v \in V$, la evaluación $\hat{v}(f) := f(v)$ es un elemento $\hat{v} \in V^{**}$, cuya definición no requiere una elección de bases, y (por conteo de dimensiones)[6] la correspondencia $v \mapsto \hat{v}$ es un isomorfismo lineal entre V y V^{**}.

Cuando H es una biálgebra finitodimensional sobre F, el espacio dual H^* también es una biálgebra, mediante la siguiente definición.

[5] Los elementos de V^* también se conocen como *formas lineales* sobre V.

[6] Si $\dim_F V = \infty$, la correspondencia $v \mapsto \hat{v}$ es inyectiva pero no es sobreyectiva.

Definición 5.16. Sea V un espacio vectorial finitodimensional sobre F; sea $V^* := \mathrm{Hom}(V,F)$ su espacio dual. Conviene usar la notación

$$\langle u, v\rangle := u(v) \in F, \quad \text{para todo} \quad u \in V^*,\ v \in V. \tag{5.16}$$

Si W es otro espacio F-vectorial de dimensión finita, cada aplicación lineal $R\colon V \to W$ posee una *transpuesta* $R^t\colon W^* \to V^*$ dada por

$$\langle R^t(x), v\rangle := \langle x, R(v)\rangle, \quad \text{para} \quad x \in W^*,\ v \in V.$$

Los espacios vectoriales $V^* \otimes V^*$ y $(V \otimes V)^*$, ambos de dimensión $(\dim_F V)^2$, se identifican mediante la dualidad[7]

$$\langle u \otimes u', v \otimes v'\rangle := \langle u, v\rangle \langle u', v'\rangle = u(v)\, u'(v')$$

si $v \otimes v' \in V \otimes V$ y si $u \otimes u' \in V^* \otimes V^*$.

Definición 5.17. Sea $(H, m, \eta, \Delta, \varepsilon)$ una biálgebra sobre F de dimensión finita. Entonces $m' := \Delta^t\colon H^* \otimes H^* \to H^*$ es asociativa y $\eta' := \varepsilon^t\colon F \to H^*$ es una counidad, de modo que (H^*, m', η') es un *álgebra* dual a la coálgebra (H, Δ, ε). También, $\Delta' := m^t\colon H^* \to H^* \otimes H^*$ es coasociativa[8] y $\varepsilon' := \eta^t\colon H^* \to F$ es una aplicación unidad, de modo que $(H^*, \Delta', \varepsilon')$ es una *coálgebra* dual al álgebra (H, m, η).

En la notación de Sweedler, todas estas relaciones se resumen así:

$$\begin{aligned} \langle uv, a\rangle &= \textstyle\sum \langle u \otimes v, a_{(1)} \otimes a_{(2)}\rangle, & \varepsilon(a) &= \langle 1_{H^*}, a\rangle, \\ \langle u, ab\rangle &= \textstyle\sum \langle u_{(1)} \otimes u_{(2)}, a \otimes b\rangle, & \varepsilon'(u) &= \langle u, 1_H\rangle. \end{aligned} \tag{5.17}$$

Si H es un álgebra de Hopf con antípoda S, entonces H^* es también un álgebra de Hopf con antípoda $S' := S^t\colon H^* \to H^*$, así:

$$\langle S'(u), a\rangle := \langle u, S(a)\rangle \quad \text{para todo} \quad a \in H,\ u \in H^*. \tag{5.18}$$

Proposición 5.18. *Sea F un cuerpo, G un grupo finito. Entonces las álgebras de Hopf $F[G]$ y $\mathcal{O}(G)$ son mutuamente duales.*

Demostración. Si $|G| = n$, tanto $F[G]$ como $\mathcal{O}(G)$ son espacios vectoriales n-dimensionales sobre F. Sus bases respectivas, $\{\, g : g \in G\,\}$ para $F[G]$ y $\{\, e_k : k \in G\,\}$ para $\mathcal{O}(G)$, son *bases duales*, ya que

$$\langle e_k, g\rangle := e_k(g) = \delta_{k,g} \quad \text{para todo} \quad g, k \in G.$$

[7] En el caso infinitodimensional, la dualidad define una inyección de $V^* \otimes V^*$ en el espacio $(V \otimes V)^*$, la cual no es sobreyectiva.

[8] En el caso infinitodimensional, dado que $H^* \otimes H^* \subset (H \otimes H)^*$ sin igualdad, la imagen $m^t(H^*)$ no es parte de $H^* \otimes H^*$ en general: el dual de una coálgebra es un álgebra, pero el dual de un álgebra no siempre es una coálgebra. Para recuperar la simetría entre ambas situaciones, es necesario reemplazar H^* por el subespacio $H^\circ := \{\, u \in H^* : m^t(u) \in H^* \otimes H^*\,\}$, conocido como el "dual de Sweedler" de H. Estas complicaciones no aparecen cuando la dimensión de H es finita.

De ahí, el espacio dual $F[G]^*$ se identifica con $\mathcal{O}(G)$.

Para ver que son duales como álgebras de Hopf, basta comprobar las relaciones (5.17) y (5.18) en este caso. Como todos los operadores de estructura son lineales, es suficiente comprobarlas para elementos básicos. En efecto,

$$\begin{aligned}
\langle e_k e_l, g\rangle &= (e_k e_l)(g) = e_k(g)\, e_l(g) = \langle e_k \otimes e_l, g \otimes g\rangle = \langle e_k \otimes e_l, \Delta(g)\rangle,\\
\langle e_k, gh\rangle &= e_k(gh) = \Delta(e_k)(g,h) = \langle \Delta(e_k), g \otimes h\rangle,\\
\varepsilon(g) &= 1 = \mathbf{1}(g) = \langle \mathbf{1}, g\rangle,\\
\varepsilon(e_k) &= e_k(1_G) = \langle e_k, 1_G\rangle,\\
\langle S(e_k), g\rangle &= S(e_k)(g) = e_k(g^{-1}) = e_k(S(g)) = \langle e_k, S(g)\rangle,
\end{aligned}$$

donde $\mathbf{1} = \sum_{k\in G} e_k$ es la función constante de valor 1, que es la identidad de $\mathcal{O}(G)$, mientras 1_G es el elemento identidad de G que es también la identidad del álgebra $F[G]$. □

¿Por qué las álgebras de Hopf se llaman por ese nombre? Una de sus fuentes originales fue las investigaciones de Heinz Hopf sobre la topología de los grupos topológicos compactos: resulta que la cohomología (sobre $\mathbb{R}$) de un tal grupo es una biálgebra con antípoda. Hoy en día es un amplio subtema del álgebra abstracta.[9]

5.3 Acciones y coacciones

Uno de los resultados más sencillos de la teoría de grupos finitos es la observación, por Arthur Cayley, de que cualquier grupo finito G es un subgrupo de un grupo de permutaciones S_n para algún n. En efecto, si $n = |G|$ con $G = \{g_1, \ldots, g_n\}$, la multiplicación a la izquierda $\Lambda(g)\colon g_j \mapsto g g_j$ es una permutación del conjunto G para cada $g \in G$, y así se define un homomorfismo inyectivo $\Lambda\colon G \to S_n$.

Más generalmente, un homomorfismo desde un grupo G al grupo de permutaciones de un conjunto X se llama una *acción* de G sobre X. Es conveniente formalizar este concepto en términos de una aplicación del producto cartesiano $G \times X$ en X.

Definición 5.19. Sea X un conjunto y G un grupo. Una **acción a la izquierda** de G sobre X es una función $\lambda : G \times X \to X$, que cumple:

(a) $\lambda(g, \lambda(h,x)) = \lambda(gh, x)$ para todo $g, h \in G$, $x \in X$.

(b) $\lambda(1_G, x) = x$ para todo $x \in X$.

Obsérvese que la aplicación $\Lambda(g)\colon x \mapsto \lambda(g,x)$ es una biyección sobre X para cada $g \in G$, cuya biyección inversa es $\Lambda(g^{-1})$. Las propiedades (a) y (b) dicen que $\Lambda(g) \circ \Lambda(h) = \Lambda(gh)$ y $\Lambda(1_G) = \mathrm{id}_X$, de modo que Λ es un homomorfismo desde G al grupo de permutaciones del conjunto X.[10]

[9] Un buen resumen de esa teoría es la primera parte del artículo: Héctor Figueroa y José M. Gracia-Bondía, "Combinatorial Hopf algebras in quantum field theory I", *Reviews in Mathematical Physics* 17 (2005), 881–976; también disponible en `http://arxiv.org/abs/hep-th/0408145/`.

[10] Si G y X son conjuntos infinitos, es apropiado dotarlos de topologías. En este caso, se suele requerir que la aplicación $\lambda : G \times X \to X$ sea continua, en cuyo caso se dice que "la acción es continua".

Escríbase $\underline{g \triangleright x} := \lambda(g,x)$. Entonces las propiedades de una acción se expresan mediante las fórmulas:

$$g \triangleright (h \triangleright x) = gh \triangleright x, \quad 1_G \triangleright x = x, \quad \text{para} \quad g,h \in G,\ x \in X. \tag{5.19}$$

En particular, si $X = G$ y $\lambda(g,h) = g \triangleright h := gh$, de modo que $\Lambda(g)$ es la "traslación a la izquierda" $h \mapsto gh$, esta es una acción porque el grupo G es asociativo.

De modo similar, puede definirse una *acción a la derecha* de un grupo G sobre un conjunto Y, como una función $\rho : Y \times G \to Y$, que cumple

$$\rho(\rho(y,h),g) = \rho(y,hg), \quad \rho(y,1_G) = y, \quad \text{para} \quad g,h \in G,\ y \in Y.$$

Con la abreviatura $\underline{y \triangleleft g} := \rho(y,g)$, estas propiedades son $(y \triangleleft h) \triangleleft g = y \triangleleft hg$, $y \triangleleft 1_G = y$. Por ejemplo, las traslaciones a la derecha $h \mapsto hg$ determinan una acción a la derecha de G sobre sí mismo.

Definición 5.20. Una acción (a la izquierda) $\lambda : G \times X \to X$ es **libre** si $g \triangleright x = x$ únicamente cuando $g = 1_G$. En este caso, para cada *órbita* $\underline{G \triangleright x} := \{ g \triangleright x : g \in G \} \subseteq X$ la aplicación $g \mapsto g \triangleright x$ es una biyección entre $G \triangleright x$ y X.

Una acción $\lambda : G \times X \to X$ es **transitiva** si hay una sola órbita, es decir, si $G \triangleright x = X$ para todo $x \in X$. Fíjese que λ es transitiva si y sólo si para cada dos elementos $x,y \in X$, hay al menos un elemento $g \in G$ tal que $g \triangleright x = y$.

Definición 5.21. Sea $\lambda : G \times X \to X$ una acción de G sobre X. La **aplicación canónica** asociada a λ es la función

$$\gamma\colon G \times X \to X \times X : (g,x) \mapsto (x, g \triangleright x). \tag{5.20}$$

Lema 5.22. *Sea $\lambda : G \times X \to X$ una acción de G sobre X. Entonces su aplicación canónica γ es inyectiva si y sólo si λ es libre; además, γ es sobreyectiva si y sólo si λ es transitiva.*

Demostración. Es evidente de (5.20) que γ es inyectiva si y sólo si $g \triangleright x = h \triangleright x$ implica $g = h$, para cada $x \in X$; si y sólo si $h^{-1}g \triangleright x = x$ implica $h^{-1}g = 1_G$, para cada $x \in X$; si y sólo si la acción λ es libre.

También es evidente de (5.20) que γ es sobreyectiva si y sólo si cada $(x,y) \in X \times X$ es de la forma $(x, g \triangleright x)$ para algún $g \in G$; si y sólo si la acción λ es transitiva. □

Ejemplo 5.23. (a) La acción de G sobre sí mismo por traslación es una acción libre y transitiva. Aquí $g \triangleright h := gh$ y por ende $\gamma(g,h) = (g,gh) \in G \times G$, la cual es biyectiva.

(b) Hay *otra* acción de G sobre sí mismo, dado por *conjugación*, donde $g \triangleright h := ghg^{-1}$. Esta acción no es libre porque $g \triangleright 1_G = 1_G$ para *todo* $g \in G$. Tampoco es transitiva, porque $G \triangleright 1_G = \{1_G\}$: la identidad 1_G es un punto fijo de esta acción. (Las órbitas, en este caso, son las clases de conjugación del grupo G.)

(c) Si $H \leq G$ es un subgrupo (no necesariamente normal), G actúa sobre el conjunto G/H de las coclases por $g \triangleright g'H := gg'H$. Esta acción es transitiva pero no es libre si $H \neq \mathbf{1}$, porque $g \triangleright H = H$ si y sólo si $g \in H$.

(d) Si $H \leq G$ es un subgrupo, entonces H actúa sobre G por $h \triangleright g := gh^{-1}$. Esta acción es libre, pero no es transitiva si $H \neq G$: las órbitas son precisamente las coclases $H \triangleright g := gH$.

Hay un concepto más amplio de acción, en donde se reemplaza el conjunto X por una álgebra A sobre un cuerpo F, se reemplaza el grupo G por una biálgebra H, se promueve el producto cartesiano $G \times X$ a un producto tensorial $H \otimes A$ y todas las operaciones son F-lineales. Cuando $H = F[G]$ es el álgebra del grupo G y $A = F^X$ es el álgebra de funciones $f : X \to F$, se recupera una versión "linealizado" de la acción $G \times X \to X$.

Definición 5.24. Si (A, m, η) es un álgebra y V es un espacio vectorial sobre un cuerpo F, una **acción** (a la izquierda) *de A sobre V* es una aplicación lineal $\theta : A \otimes V \to V$ tal que

$$\begin{aligned} \theta(\mathrm{id}_A \otimes \theta) &= \theta(m \otimes \mathrm{id}_V) : A \otimes A \otimes V \to V; \\ \theta(\eta \otimes \mathrm{id}_V) &= \mathrm{id}_V : V \to V. \end{aligned} \tag{5.21}$$

Escríbase $\theta(a \otimes v) := a \triangleright v \in V$ para $a \in A$, $v \in V$. La fórmula (5.19) se mantiene:

$$a \triangleright (b \triangleright v) = ab \triangleright v, \quad 1_A \triangleright v = v, \quad \text{para} \quad a, b \in A,\ v \in V.$$

pero ahora θ, $\mathrm{id}_A \otimes \theta$, etc., son operaciones F-lineales entre espacios vectoriales. Si además se escribe $\Theta(a) : v \mapsto \theta(a \otimes v)$, entonces las condiciones (5.21) dicen que $\Theta : A \to \mathrm{End}(V)$ es un homomorfismo de álgebras sobre F.

Definición 5.25. Si H es una biálgebra y A es un álgebra sobre un cuerpo F, una **acción de Hopf** (a la izquierda) de H sobre A es una acción del álgebra (H, m, η) sobre el espacio vectorial A, que cumple las siguientes propiedades:

$$\left\{ \begin{array}{l} h \triangleright (ab) = \sum (h_{(1)} \triangleright a)\,(h_{(2)} \triangleright b) \\ h \triangleright 1_A = \varepsilon(h)\, 1_A \end{array} \right\} \qquad \text{si } a, b \in A,\ h \in H. \tag{5.22}$$

Para comprender el significado de las reglas (5.22), considérese dos casos especiales. Primero, si $\Delta(h) = h \otimes h$ y $\varepsilon(h) = 1$, como ocurre con las generadores de la biálgebra $F[G]$, entonces estas reglas se reducen a

$$h \triangleright (ab) = (h \triangleright a)\,(h \triangleright b), \quad h \triangleright 1_A = 1_A,$$

de modo que el elemento $\Theta(h) \in \mathrm{End}(A)$ es un *homomorfismo de álgebras*.

En segundo lugar, si $\Delta(h) = h \otimes 1 + 1 \otimes h$ y $\varepsilon(h) = 0$ (un tal elemento de H se llama "primitivo"), entonces (5.22) dice que

$$h \triangleright (ab) = (h \triangleright a)\, b + a\, (h \triangleright b), \quad h \triangleright 1_A = 0,$$

la cual es una *regla de Leibniz*: la aplicación $\Theta(h) \in \mathrm{End}(A)$ es una *derivación* del álgebra A.

Por lo tanto, una acción de Hopf de una biálgebra H sobre un álgebra A representa H como "homomorfismos generalizados" de A.

▶ Por dualidad, una acción de un álgebra sobre un espacio vectorial da lugar a la noción simétrica de "una coacción de una coálgebra sobre un espacio vectorial". Como las coálgebras son quizás menos rutinarias que las álgebras, vale la pena mirar ese concepto con detalle.

Definición 5.26. Si (C,Δ,ε) es una coálgebra y V es un espacio vectorial sobre un cuerpo F, una **coacción** (a la derecha) *de C sobre V* es una aplicación lineal $\delta\colon V\to V\otimes C$ tal que

$$\begin{aligned}(\delta\otimes\mathrm{id}_C)\delta &= (\mathrm{id}_V\otimes\Delta)\delta : V\to V\otimes C\otimes C;\\ (\mathrm{id}_V\otimes\varepsilon)\delta &= \mathrm{id}_V : V\to V.\end{aligned}\tag{5.23}$$

Para calcular el efecto de una coacción, es conveniente introducir una variante de la notación de Sweedler:

$$\delta(v) =: \textstyle\sum v_{(0)}\otimes v_{(1)}\in V\otimes C.\tag{5.24}$$

Aquí, por convenio, $v_{(0)}$ denota un elemento del espacio vectorial V, mientras $v_{(1)}$, $v_{(2)}$, etc., serán elementos de la coálgebra C. Por ejemplo, la primera propiedad de (5.23) se puede expresar así:

$$\textstyle\sum v_{(0)(0)}\otimes v_{(0)(1)}\otimes v_{(1)} = \sum v_{(0)}\otimes v_{(1)(1)}\otimes v_{(1)(2)},$$

la cual puede reescribirse, sin ambigüedad, por analogía con (5.9), como

$$(\delta\otimes\mathrm{id}_C)(\delta(v)) = (\mathrm{id}_V\otimes\Delta)(\delta(v)) =: \textstyle\sum v_{(0)}\otimes v_{(1)}\otimes v_{(2)}.$$

La segunda propiedad de (5.23) dice que $\sum v_{(0)}\,\varepsilon(v_{(1)}) = v\in V$.

Lema 5.27. *Si $\delta\colon V\to V\otimes C$ es una coacción a la derecha de una coálgebra C sobre un espacio F-vectorial V, entonces hay una acción a la izquierda del álgebra dual C^* sobre V.*

Demostración. El dual de la coálgebra (C,Δ,ε) es el álgebra $(C^*,\Delta^t,\varepsilon^t)$, donde C^* es el espacio F-vectorial dual de C y sus operaciones son las aplicaciones transpuestas de Δ, ε respectivamente.

La acción $\theta\colon C^*\otimes V\to V$ se define por la fórmula

$$f\triangleright v := \textstyle\sum v_{(0)}\,\langle f, v_{(1)}\rangle = \sum\langle f, v_{(1)}\rangle\, v_{(0)},$$

en donde $\langle f,c\rangle := f(c)$ para $f\in C^*$, $c\in C$, y la coacción δ se expresa mediante la fórmula (5.24). Alternativamente, la definición de la acción es $\theta(f\otimes v) := (\mathrm{id}_V\otimes f)(\delta(v))$ o bien $\Theta(f) := (\mathrm{id}_V\otimes f)\delta$.

Si $f,h\in C^*$, entonces $\Delta^t(f\otimes h) = (f\otimes h)\circ\Delta$ es la convolución $f*h$ — fíjese que $C^* = \mathrm{Hom}(C,F)$ donde se puede considerar F como un álgebra unidimensional. Ahora

$$\begin{aligned}(f*h)\triangleright v &= \textstyle\sum v_{(0)}\,(f*h)(v_{(1)}) = \sum v_{(0)}\,f(v_{(1)(1)})\,h(v_{(1)(2)})\\ &= \textstyle\sum v_{(0)(0)}\,f(v_{(0)(1)})\,h(v_{(1)}) = \sum f\triangleright v_{(0)}\,h(v_{(1)}) = f\triangleright(h\triangleright v),\end{aligned}$$

y además $1_{C^*}\triangleright v = \sum v_{(0)}\,\varepsilon(v_{(1)}) = v$ para $v\in V$. Por tanto $v\mapsto f\triangleright v$ es una acción a la izquierda del álgebra C^*. □

Lema 5.28. *Si $\theta\colon A\otimes V\to V$ es una acción a la izquierda de un álgebra finitodimensional A sobre un espacio vectorial V con $\dim_F V$ finita, entonces hay una coacción a la derecha de la coálgebra dual A^* sobre V.*

Demostración. Sea $\{h_1,\dots,h_n\}$ una base de A como espacio F-vectorial y sea $\{f_1,\dots,f_n\}$ la base dual de A^*. Fíjese que cualquier elemento $g\in A$ se expresa en términos de estas bases como

$$g=\sum_{k=1}^{n}\langle f_k,g\rangle\, h_k.$$

Defínase una aplicación lineal $\delta\colon V\to V\otimes A^*$ por

$$\delta(v):=\sum_{j=1}^{n}(h_j\triangleright v)\otimes f_j. \tag{5.25}$$

Obsérvese que esta definición es independiente de la base de A: si $\{h'_1,\dots,h'_n\}$ es otra base de A, con base dual correspondiente $\{f'_1,\dots,f'_n\}$ de A^*, entonces es fácil ver que el lado derecho de (5.25) es igual a $\sum_{i=1}^{n}(h'_i\triangleright v)\otimes f'_i$.

Resulta que la aplicación (5.25) es una coacción. En efecto, si $v\in V$, entonces

$$(\mathrm{id}\otimes\varepsilon)(\delta(v))=\sum_{j=1}^{n}(h_j\triangleright v)\,\varepsilon(f_j)=\left(\sum_{j=1}^{n}\langle f_j,1\rangle\, h_j\right)\triangleright v=1\triangleright v=v.$$

Además,

$$\begin{aligned}(\mathrm{id}\otimes\Delta)(\delta(v))&=\sum_{k=1}^{n}(h_k\triangleright v)\otimes\Delta(f_k)=\sum_{i,j,k=1}^{n}(h_k\triangleright v)\otimes f_i\otimes f_j\,\langle\Delta(f_k),h_i\otimes h_j\rangle\\&=\sum_{i,j,k=1}^{n}\langle f_k,h_ih_j\rangle\,(h_k\triangleright v)\otimes f_i\otimes f_j=\sum_{i,j=1}^{n}(h_ih_j\triangleright v)\otimes f_i\otimes f_j\\&=\sum_{j=1}^{n}\left(\sum_{i=1}^{n}(h_i\triangleright(h_j\triangleright v))\otimes f_i\right)\otimes f_j=\sum_{j=1}^{n}\delta(h_j\triangleright v)\otimes f_j\\&=(\delta\otimes\mathrm{id})\sum_{j=1}^{n}(h_j\triangleright v)\otimes f_j=(\delta\otimes\mathrm{id})(\delta(v)).\end{aligned}$$

En vista de la Definición 5.26, δ es una coacción de A^* sobre V. □

Proposición 5.29. *Si $\theta\colon H\otimes A\to A$ es una acción de una biálgebra H sobre A y si $\delta\colon A\to A\otimes H^*$ es la coacción dual dada por* (5.25)*, entonces θ es una acción de Hopf si y sólo si δ es un homomorfismo de álgebras.*

Demostración. Si la acción θ cumple la propiedad (5.22) de acciones de Hopf, entonces la coacción dual δ obedece

$$\delta(1_A)=\sum_{k=1}^{n}(h_k\triangleright 1_A)\otimes f_k=\sum_{k=1}^{n}\varepsilon(h_k)\,1_A\otimes f_k=\sum_{k=1}^{n}1_A\otimes\langle 1_{H^*},h_k\rangle\, f_k=1_A\otimes 1_{H^*}.$$

También, para todo $a,b \in A$, se verifica

$$\begin{aligned}
\delta(ab) &= \sum_{k=1}^{n} (h_k \triangleright ab) \otimes f_k = \sum_{k=1}^{n} \sum (h_{k(1)} \triangleright a)(h_{k(2)} \triangleright b) \otimes f_k \\
&= \sum_{i,j,k=1}^{n} (\langle f_i, h_{k(1)} \rangle h_i \triangleright a)(\langle f_j, h_{k(2)} \rangle h_j \triangleright b) \otimes f_k \\
&= \sum_{i,j,k=1}^{n} \langle f_i \otimes f_j, h_{k(1)} \otimes h_{k(2)} \rangle (h_i \triangleright a)(h_j \triangleright b) \otimes f_k \\
&= \sum_{i,j,k=1}^{n} (h_i \triangleright a)(h_j \triangleright b) \otimes f_k \langle f_i f_j, h_k \rangle = \sum_{i,j=1}^{n} (h_i \triangleright a)(h_j \triangleright b) \otimes f_i f_j \\
&= \left(\sum_{i,=1}^{n} (h_i \triangleright a) \otimes f_i \right) \left(\sum_{j=1}^{n} (h_j \triangleright b) \otimes f_j \right) = \delta(a)\, \delta(b).
\end{aligned}$$

Luego, δ es un homomorfismo de álgebras.

Inversamente, si δ es un homomorfismo, entonces la acción dual θ cumple $h \triangleright 1_A = 1_A \langle 1_{H^*}, h \rangle = \varepsilon(h)\, 1_A$ porque $\delta(1_A) = 1_A \otimes 1_{H^*}$. Además, para $a,b \in A$ se verifica

$$\begin{aligned}
h \triangleright ab &= \sum (ab)_{(0)} \langle (ab)_{(1)}, h \rangle = \sum a_{(0)} b_{(0)} \langle a_{(1)} b_{(1)}, h \rangle \\
&= \sum a_{(0)} b_{(0)} \langle a_{(1)}, h_{(1)} \rangle \langle b_{(1)}, h_{(2)} \rangle = \big(\sum a_{(0)} \langle a_{(1)}, h_{(1)} \rangle \big) \big(\sum b_{(0)} \langle b_{(1)}, h_{(2)} \rangle \big) \\
&= \sum (h_{(1)} \triangleright a)\, (h_{(2)} \triangleright b).
\end{aligned}$$

Aquí las identidades $(ab)_{(0)} = a_{(0)} b_{(0)}$ y $(ab)_{(1)} = a_{(1)} b_{(1)}$ expresan la propiedad multiplicativa de la coacción, $\delta(ab) = \delta(a)\, \delta(b)$. □

Para una acción de Hopf $\theta : H \otimes A \to A$, el subespacio vectorial

$$A^H := \{\, a \in A : h \triangleright a = \varepsilon(h)\, a, \text{ para todo } h \in H \,\}$$

es una subálgebra, porque $h \triangleright ab = \sum \varepsilon(h_{(1)}) \varepsilon(h_{(2)}) ab = \varepsilon\big(\sum h_{(1)} \varepsilon(h_{(2)}) \big) ab = \varepsilon(h) ab$ para $a,b \in A^H$. Esta A^H se llama la *subálgebra invariante* de A bajo la acción de H. En el caso $H = F[G]$, en donde $\varepsilon(g) = 1$ para todo $g \in G$, $A^{F[G]} =: A^G$ consta de los $a \in A$ que son *fijos* bajo la acción del grupo G. En particular, si K es una extensión del cuerpo F y el grupo G actúa por automorfismos de K, entonces K^G es precisamente el *cuerpo fijo* de K bajo la acción de G.

Hay una noción dual de subálgebra coinvariante bajo una coacción, cuya definición es, de hecho, más sencilla que la de subálgebra invariante.

Definición 5.30. Sea $\delta : A \to A \otimes H$ una *coacción de álgebras*, es decir, una coacción de una biálgebra H sobre un álgebra A que es a la vez un homomorfismo de álgebras. La **subálgebra coinvariante** de A bajo δ es[11]

$$A^{\mathrm{co}H} := \{\, a \in A : \delta(a) = a \otimes 1_H \,\}.$$

[11] La notación $A^{\mathrm{co}H}$ es inelegante, pero universalmente aceptado.

Definición 5.31. Sea A un álgebra sobre un cuerpo F y sea B una subálgebra de A, Sea J el ideal de $A \otimes A$ generado por los elementos $ab \otimes a' - a \otimes ba'$, para $a, a' \in A$ y $b \in B$. Sea $\underline{A \otimes_B A}$ el álgebra cociente $(A \otimes A)/J$. La notación $a \otimes_B a'$ denota la *coclase* de $a \otimes a'$ en este cociente. Es evidente que $ab \otimes_B a' = a \otimes_B ba'$ si $b \in B$.

Definición 5.32. Sea $\delta : A \to A \otimes H$ una coacción de F-álgebras, de una biálgebra H sobre un álgebra A. Sea $B = A^{\mathrm{co}H}$ la subálgebra coinvariante. La **aplicación canónica** asociada a δ es la aplicación F-lineal

$$\beta : A \otimes_B A \to A \otimes H : c \otimes_B a \mapsto \sum ca_{(0)} \otimes a_{(1)}. \tag{5.26}$$

Alternativamente, se puede definir $\beta := (m_A \otimes \mathrm{id}_H)(\mathrm{id}_A \otimes \delta)$.

Esta aplicación está bien definida, porque si $b \in B$, entonces $\sum b_{(0)} \otimes b_{(1)} = \delta(b) = b \otimes 1$ y por ende

$$\sum c(ba)_{(0)} \otimes (ba)_{(1)} = \sum cb_{(0)}a_{(0)} \otimes b_{(1)}a_{(1)} = \sum cba_{(0)} \otimes a_{(1)},$$

de modo que la aplicación $\tilde{\beta} : c \otimes a \mapsto \sum ca_{(0)} \otimes a_{(1)}$, definida inicialmente sobre $A \otimes A$, cumple $\tilde{\beta}(c \otimes ba) = \tilde{\beta}(cb \otimes a)$ si $b \in B$. Esto dice que $\tilde{\beta}$ se anula sobre el ideal J y luego determina una aplicación β, definida en $A \otimes_B A$.

5.4 La aplicación canónica en la teoría de Galois

El formalismo desarrollado en la subsección anterior fue concebido históricamente para poder extender la correspondencia de Galois más allá del ámbito de las extensiones de cuerpos. En esta última subsección, se estudia la aplicación del formalismo al contexto original, para poder entender el por qué de dicha generalización.

Ejemplo 5.33. Sea $K \,|\, F$ una extensión finita de cuerpos, no necesariamente normal. Sea G un grupo finito isomorfo a $\mathrm{Gal}(K \,|\, F)$, para poder escribir $\mathrm{Gal}(K \,|\, F) = \{\, \sigma_g : g \in G \,\}$. Para $\alpha \in K$, sea $g \triangleright \alpha := \sigma_g(\alpha)$. De este modo, se obtiene una acción de grupo (a la izquierda) de G sobre K. Si $h = \sum_{g \in G} a_g \cdot g \in F[G]$, defínase

$$h \triangleright \alpha := \sum_{g \in G} a_g (g \triangleright \alpha) = \sum_{g \in G} a_g \, \sigma_g(\alpha) \in K.$$

Esta es una acción del álgebra de Hopf $F[G]$ sobre K, obtenida como extensión F-lineal de la acción de G. Como $\Delta(g) = g \otimes g$ para $g \in G$, esta es una acción de Hopf, porque $g \triangleright \alpha\beta = \sigma_g(\alpha\beta) = \sigma_g(\alpha)\,\sigma_g(\beta) = (g \triangleright \alpha)\,(g \triangleright \beta)$ para $\alpha, \beta \in K$.

La coacción dual es un homomorfismo $\delta : K \to K \otimes \mathcal{O}(G)$, dado por

$$\delta(\alpha) = \sum_{g \in G} \sigma_g(\alpha) \otimes e_g,$$

en vista de (5.25). La subálgebra coinvariante en este caso es un subcuerpo de K. En efecto, es $\alpha \in K^{\mathrm{co}\,\mathcal{O}(G)}$ si y sólo si $\sum_{g \in G} \sigma_g(\alpha) \otimes e_g = \alpha \otimes \mathbf{1}$; pero la función constante $\mathbf{1}$ es igual a

la suma $\sum_{g\in G} e_g$, de modo que $\alpha\otimes\mathbf{1} = \sum_{g\in G}\alpha\otimes e_g$. Como los e_g son linealmente independientes en $\mathcal{O}(G)$, se concluye que $\alpha\in K^{\mathrm{co}\,\mathcal{O}(G)}$ si y sólo si $\sigma_g(\alpha)=\alpha$ para todo $g\in G$. En otras palabras, $K^{\mathrm{co}\,\mathcal{O}(G)} = K^G$ es el *cuerpo fijo* de K bajo la acción de G.

Sea $E := K^G$. Entonces $K\otimes_E K$ puede identificarse con el producto tensorial de dos copias de K *como espacio vectorial sobre* E, al poner $c(\omega\otimes_E\alpha) := c\omega\otimes_E\alpha = \omega\otimes_E c\alpha$ para $c\in E$, $\omega,\alpha\in K$. Sin embargo, al considerarlo como espacio vectorial sobre el cuerpo F, su dimensión es

$$\dim_F(K\otimes_E K) = [E\colon F]\dim_E(K\otimes_E K) = [E\colon F]\,[K\colon E]^2 = [K\colon F]\,[K\colon E]. \tag{5.27a}$$

Por otro lado, el teorema de Artin garantiza que $|G| = [K\colon K^G] = [K\colon E]$, y por tanto

$$\dim_F(K\otimes\mathcal{O}(G)) = \dim_F(K)\dim_F(\mathcal{O}(G)) = [K\colon F]\,|G| = [K\colon F]\,[K\colon E]. \tag{5.27b}$$

En este caso, la aplicación canónica

$$\beta\colon K\otimes_E K\to K\otimes\mathcal{O}(G)\colon \omega\otimes_E\alpha\mapsto\sum_{g\in G}\omega\,\sigma_g(\alpha)\otimes e_g \tag{5.28}$$

es una aplicación F-lineal entre dos espacios vectoriales de la misma dimensión.

Para una acción de un grupo finito G sobre un conjunto finito X, la aplicación canónica γ de (5.20) es inyectiva si y sólo si la acción es libre.[12] Dualmente, para las aplicaciones canónicas (5.26) y (5.28) asociados con coacciones de biálgebras, lo que interesa saber es si β es sobreyectiva. En el caso de una extensión de cuerpos, la inyectividad de β sigue como consecuencia de la igualdad de dimensiones (5.27).

Resulta que la acción canónica (5.28) es efectivamente biyectiva, en virtud de un famoso resultado de Dedekind, ampliado y mejorado por Artin, acerca de la independencia lineal de caracteres.

Definición 5.34. Sea G un grupo, K un cuerpo. Un **carácter** de G en K es un homomorfismo de grupos $\chi\colon G\to K^\times$.

Proposición 5.35 (Artin)**.** *Si G es un grupo y si $\chi_1,\dots,\chi_n$ son caracteres distintos de G en un cuerpo K, ellos son linealmente independientes sobre K, en el sentido de que la relación $\alpha_1\chi_1+\alpha_2\chi_2+\cdots+\alpha_n\chi_n=0$, con $\alpha_1,\dots,\alpha_n\in K$, sólo se verifica si $\alpha_1=\alpha_2=\cdots=\alpha_n=0$.*

Demostración. Un solo carácter χ cumple $\alpha\chi=0$ (como función de G en K) si y sólo si $\alpha=\alpha\chi(1)=0$ en K.

Si $\chi_1,\dots,\chi_n$ no son linealmente independientes, hay $\alpha_1,\dots,\alpha_n\in K$, no todos cero, con

$$\alpha_1\chi_1+\alpha_2\chi_2+\cdots+\alpha_n\chi_n=0.$$

[12] La sobreyectividad de γ es menos importante: si la acción de G sobre X no es transitiva, entonces X es la unión de varias órbitas. Si Z es la colección de órbitas y $\pi\colon X\to Z : x\mapsto G\triangleright x$ es la aplicación cociente, la notación $X\times_Z X$ denota $\{\,(x,y)\in X\times X : \pi(x)=\pi(y)\,\}\subseteq X\times X$. Si se considera γ como aplicación de $G\times X$ en $X\times_Z X$, entonces γ es automáticamente sobreyectiva.

Se puede suponer, reenumerando los χ_i si fuera necesario, que el número n de sumandos es el menor posible: en particular, que $\alpha_i \neq 0$ para $i = 1, \ldots, n$. Como $\chi_1 \neq \chi_2$ por hipótesis, hay un elemento $g \in G$ tal que $\chi_1(g) \neq \chi_2(g)$.

Para todo $h \in G$, se verifica

$$\alpha_1\chi_1(h) + \alpha_2\chi_2(h) + \cdots + \alpha_n\chi_n(h) = 0 \quad \text{en } F. \tag{5.29a}$$

Además,

$$\alpha_1\chi_1(gh) + \cdots + \alpha_n\chi_n(gh) = \alpha_1\chi_1(g)\chi_1(h) + \cdots + \alpha_n\chi_n(g)\chi_n(h) = 0. \tag{5.29b}$$

Al multiplicar (5.29a) por $\chi_1(g)$ y al restar (5.29b), se obtiene

$$\alpha_2\big(\chi_1(g) - \chi_2(g)\big)\chi_2 + \cdots + \alpha_n\big(\chi_1(g) - \chi_n(g)\big)\chi_n = 0.$$

Esta es una relación lineal entre $\chi_2, \ldots, \chi_n$. Por la minimalidad de n, se concluye que

$$\alpha_2\big(\chi_1(g) - \chi_2(g)\big) = \cdots = \alpha_n\big(\chi_1(g) - \chi_n(g)\big) = 0.$$

Pero $\alpha_2 \neq 0$, $\chi_1(g) \neq \chi_2(g)$ desde antes: se ha llegado a una contradicción. □

Corolario 5.36. *En el caso de que $G = K^\times$, donde $K \mid F$ es una extensión, los elementos de* $\mathrm{Gal}(K \mid F)$ *son linealmente independientes sobre K.* ⊟

Proposición 5.37 (Dedekind)**.** *Sea $G = \{\sigma_1, \ldots, \sigma_n\}$ un grupo finito de automorfismos de un cuerpo K, y sea $\{c_1, \ldots, c_n\}$ una base vectorial de K sobre el cuerpo fijo K^G. Entonces la matriz $[\sigma_i(c_j)] \in M_n(K)$ es inversible.*[13]

Demostración. Fíjese que $[K\colon K^G] = |G| = n$, por el Teorema 3.9 de Artin, así que $[\sigma_i(c_j)]$ es una matriz cuadrada $n \times n$. Bastaría, entonces, comprobar que $\det[\sigma_i(c_j)] \neq 0$.

Si esta matriz no es inversible, es decir, si $\det[\sigma_i(c_j)] = 0$, entonces hay $\alpha_1, \ldots, \alpha_n \in K$, no todos cero, tal que

$$\begin{bmatrix}\alpha_1 & \alpha_2 & \ldots & \alpha_n\end{bmatrix}\begin{bmatrix}\sigma_1(c_1) & \sigma_1(c_2) & \ldots & \sigma_1(c_n)\\ \sigma_2(c_1) & \sigma_2(c_2) & \ldots & \sigma_2(c_n)\\ \vdots & \vdots & \ddots & \vdots\\ \sigma_n(c_1) & \sigma_n(c_2) & \ldots & \sigma_n(c_n)\end{bmatrix} = \begin{bmatrix}0 & 0 & \ldots & 0\end{bmatrix}$$

o bien $\sum_{i=1}^n \alpha_i\sigma_i(c_j) = 0$ para $j = 1, \ldots, n$. Como $\{c_1, \ldots, c_n\}$ es una base de K sobre K^G, estas relaciones dicen que $\sum_{i=1}^n \alpha_i\sigma_i = 0$ como aplicación lineal de K en K. Ahora, la Proposición 5.35 implica que $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$, contrario a hipótesis. Se concluye que $[\sigma_i(c_j)]$ es inversible. □

Teorema 5.38. *Sea $K \mid F$ una extensión finita de cuerpos, $G = \mathrm{Gal}(K \mid F)$ y $E = K^G$. Entonces la aplicación canónica $\beta\colon K \otimes_E K \to K \otimes \mathcal{O}(G)$ es biyectiva.*

[13] Aquí $M_n(K)$ denota la totalidad de matrices $n \times n$ con entradas en K.

Demostración. Por la igualdad de dimensiones (5.27), basta comprobar que β es inyectiva.

Como $|G| = [K\colon E] = n$, se puede escribir $G = \{\sigma_1, \dots, \sigma_n\}$ y a la vez encontrar una base vectorial $\{\alpha_1, \dots, \alpha_n\}$ de K sobre E. Cualquier elemento de $\ker\beta \subseteq K \otimes_E K$ es de la forma $\sum_{j=1}^n \omega_j \otimes_E \alpha_j$, para ciertos elementos $\omega_1, \dots, \omega_n \in K$. Entonces

$$\beta\left(\sum_{j=1}^n \omega_j \otimes_E \alpha_j\right) = \sum_{j=1}^n \sum_{i=1}^n \omega_j \sigma_i(\alpha_j) \otimes e_{\sigma_i} = 0 \quad \text{en} \quad K \otimes \mathcal{O}(G).$$

Ahora $\{e_{\sigma_1}, \dots, e_{\sigma_n}\}$ es linealmente independiente en el espacio F-vectorial $\mathcal{O}(G)$; por tanto, es $\sum_{j=1}^n \omega_j \sigma_i(\alpha_j) = 0$ en K para cada $i = 1, \dots, n$.

Pero la matriz $[\sigma_i(\alpha_j)]$ es inversible por la Proposición 5.37 de Dedekind. Se concluye que $\omega_1 = \cdots = \omega_n = 0$, y por ende $\sum_{j=1}^n \omega_j \otimes_E \alpha_j = 0$. Esto muestra que $\ker\beta = \{0\}$. □

Corolario 5.39. *La extensión finita $K \mid F$ es una extensión de Galois si y sólo si la aplicación $\tilde{\beta}\colon K \otimes K \to K \otimes \mathcal{O}(G)$ es biyectiva.*

Demostración. Por el Corolario 4.17, la extensión finita $K \mid F$ es de Galois (esto es, normal y separable) si y sólo si $K^G = F$. En ese caso, y sólo en eso caso, la subálgebra coinvariante $E = K^G$ coincide con F, y el producto tensorial $K \otimes_E K$ se reduce al producto tensorial ordinario $K \otimes K$ sobre F. □

► Vale la pena reformular esta aplicación canónica en términos de acción del $F[G]$ (o de cualquier otra álgebra de Hopf) sobre K. Resulta bastante complicado hacerlo en el caso general $E \neq F$, es decir, cuando la extensión no es de Galois —esto es una de las razones para preferir la versión dual de una coacción de $\mathcal{O}(G)$. Ahora bien: si la extensión $K \mid F$ es de Galois, de modo que el dominio de β es el espacio $K \otimes K$ de dimensión $[K\colon F]^2$, la situación es más sencilla. Antes de abordarla, se requiere un lema de dualidad en álgebra lineal.

Lema 5.40. *Sean U, V dos espacios vectoriales sobre F, de dimensión finita. Sean U^*, V^* sus respectivos espacios duales. Hay una correspondencia lineal natural*[14] *entre las aplicaciones lineales $P\colon U \otimes U \to U \otimes V^*$ y las aplicaciones lineales $Q\colon U \otimes V \to U^* \otimes U = \mathrm{End}(U)$. Si $\dim_F U = \dim_F V$, esta correspondencia preserva las aplicaciones biyectivas.*

Demostración. Sean $\{u_1, \dots, u_m\}$, $\{g_1, \dots, g_m\}$ bases duales para U y U^*, y sean $\{v_1, \dots, v_n\}$, $\{f_1, \dots, f_n\}$ bases duales para V y V^*. Para P y Q del enunciado, defínase

$$P^\sharp : U \otimes V \to U^* \otimes U : u \otimes v \longmapsto \sum_{i=1}^m g_i \otimes (\mathrm{id} \otimes \hat{v})(P(u \otimes u_i)),$$

$$Q^\flat : U \otimes U \to U \otimes V^* : x \otimes y \longmapsto \sum_{j=1}^n (\hat{y} \otimes \mathrm{id})(Q(x \otimes v_j)) \otimes f_j.$$

donde $\hat{v}\colon V^* \to F : f \mapsto \langle f, v\rangle$ y $\hat{y}\colon U^* \to F : g \mapsto \langle g, u\rangle$ son evaluaciones.

[14] La biyección es "natural" porque su definición no depende de la elección de bases en U y en V.

Las correspondencias lineales $P \mapsto P^\sharp$ y $Q \mapsto Q^\flat$ son inversas. (Obsérvese que el dominio y el rango en ambos casos son espacios vectoriales de dimensión m^3n.) Por ejemplo,

$$\begin{aligned}(P^\sharp)^\flat(x\otimes y) &= \sum_{j=1}^{n} (\hat{y}\otimes \mathrm{id})(P^\sharp(x\otimes v_j))\otimes f_j \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} \langle g_i, y\rangle\, (\mathrm{id}\otimes \hat{v}_j)(P(x\otimes u_i))\otimes f_j \\ &= \sum_{i=1}^{m} \langle g_i, y\rangle\, P(x\otimes u_i) = P\left(\sum_{i=1}^{m} x\otimes \langle g_i, y\rangle\, u_i\right) = P(x\otimes y).\end{aligned}$$

En este cálculo, se ha empleado la fórmula

$$\sum_{j=1}^{n} (\mathrm{id}\otimes \hat{v}_j)(u\otimes f)\otimes f_j = u\otimes \sum_{j=1}^{n} \langle f, v_j\rangle\, f_j = u\otimes f$$

cuando $u\otimes f \in U\otimes V^*$, para obtener la tercera igualdad. De igual manera, se comprueba que

$$\begin{aligned}(Q^\flat)^\sharp(u\otimes v) &= \sum_{i=1}^{m} g_i\otimes (\mathrm{id}\otimes \hat{v})(Q^\flat(u\otimes u_i)) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} \langle f_j, v\rangle\, g_i\otimes (\hat{u}_i\otimes \mathrm{id})(Q(u\otimes v_j)) \\ &= \sum_{j=1}^{n} \langle f_j, v\rangle\, Q(u\otimes v_j) = Q(u\otimes v),\end{aligned}$$

en vista de la fórmula

$$\sum_{i=1}^{m} g_i\otimes (\hat{u}_i\otimes \mathrm{id})(g\otimes u) = \sum_{i=1}^{m} \langle g, u_i\rangle\, g_i\otimes u = g\otimes u \in U^*\otimes U.$$

Con respecto a las bases elegidas, la matrices de P y Q se obtienen de las identidades $P(u_k\otimes u_l) =: \sum_{i,j} p_{kl}^{ij}\, u_i\otimes f_j$ y también $Q(u_t\otimes v_z) =: \sum_{r,s} q_{tz}^{rs}\, g_r\otimes u_s$. Se ve que $P = Q^\flat$ si y sólo si $q_{kj}^{li} = p_{kl}^{ij}$. Cuando $m = n$, estas son matrices cuadradas $n^2\times n^2$, y puede comprobarse que $\det[q_{kj}^{li}] = \det[q_{kl}^{ij}]$. En particular, Q es bijectiva si y sólo si este determinante no es cero, si y sólo si $Q^\flat$ es biyectiva. □

Corolario 5.41. *Si $\theta\colon H\otimes A\to A$ es una acción de Hopf de una biálgebra finitodimensional H sobre una álgebra finitodimensional A, si $\delta\colon A\to A\otimes H^*$ es su coacción de álgebras dual, si $A^{\mathrm{co}H^*} = F$ y si la aplicación canónica β es una biyección de $A\otimes A$ en $A\otimes H^*$, entonces hay una biyección correspondiente $\beta^\sharp\colon A\otimes H\to \mathrm{End}(A)$, dado por*

$$\beta^\sharp(c\otimes h)[a] := c\,(h\triangleright a). \tag{5.30}$$

Demostración. La biyectividad de $\beta^\sharp$ es consecuencia del lema anterior. Para verificar la fórmula para $\beta^\sharp$, elíjase bases duales $\{u_1,\dots,u_m\}$ para A y $\{g_1,\dots,g_m\}$ para A^*. Entonces

$$\begin{aligned}\beta^\sharp(c\otimes h)[a] &= \sum_{i=1}^{m}\langle g_i,a\rangle\,(\mathrm{id}\otimes\hat{h})(\beta(c\otimes u_i)) = (\mathrm{id}\otimes\hat{h})(\beta(c\otimes a))\\ &= \textstyle\sum c\,a_{(0)}\,\langle a_{(1)},h\rangle = c\,(h\triangleright a),\end{aligned}$$

a partir de la definición de la acción de H (véase la demostración del Lema 5.27). □

En el contexto de las extensiones finitas de cuerpos, esta reformulación conduce a la definición siguiente.

Definición 5.42. Sea $K\,|\,F$ una extensión finita de cuerpos. Sea H un álgebra de Hopf, finitodimensional sobre F, que posee una acción de Hopf sobre K. Entonces $K\,|\,F$ es una **extensión H–Galois**, o bien una *extensión de Hopf–Galois* mediante H, si la aplicación $\beta^\sharp\colon K\otimes H\to \mathrm{End}(K)$ dada por (5.30) es biyectiva.[15]

En esta definición, H es un álgebra de Hopf, es decir, una biálgebra con antípoda. La existencia de la antípoda es automática cuando la aplicación canónica es biyectiva. Véase el Apéndice, a continuación, para la razón de este fenómeno.

Ejemplo 5.43. En el Ejemplo 5.2, se introdujo un álgebra de Hopf $H=\mathrm{lin}\langle \mathrm{id},c,s\rangle$ actuando sobre $K=\mathbb{Q}(\sqrt[3]{2})$ por multiplicación de matrices 3×3, pues H es un subespacio 3-dimensional de $\mathrm{End}(K)$: en este caso, es $F=\mathbb{Q}$. Los operadores de multiplicación $\mu(c)\colon \alpha\mapsto c\alpha$ forman otro subespacio 3-dimensional de $\mathrm{End}(K)$. Es fácil comprobar que $\mu(K)\cap H=\mathbb{Q}\mathrm{id}$, que $\mu(K)H=\mathrm{End}(K)$ y que la aplicación lineal

$$c\otimes h\mapsto \mu(c)h$$

es una biyección de $K\otimes H$ en $\mathrm{End}(K)$, al contar dimensiones. Esta aplicación es precisamente la $\beta^\sharp$ de (5.30). Por lo tanto, $\mathbb{Q}(\sqrt[3]{2})\,|\,\mathbb{Q}$ es una extensión de Hopf–Galois mediante H.

En fin, las acciones o coacciones de Hopf con aplicación canónica biyectiva dilatan el concepto de grupo de Galois al caso de extensiones de cuerpos no necesariamente normales (ni separables). ¿Será siempre posible encontrar un tal H para una extensión finita cualquiera? Resulta que no: para $\mathbb{Q}(\alpha)$ donde α posee un polinomio mínimo $f(X)$ de grado 5, cuyo cuerpo de escisión K_f cumple $\mathrm{Gal}(K_f\,|\,\mathbb{Q})\simeq S_5$, como ocurre en el Ejemplo 3.60, no hay álgebra de Hopf H alguna para la cual la extensión $\mathbb{Q}(\alpha)\,|\,\mathbb{Q}$ sea H–Galois.[16]

La motivación original para reformular la teoría de Galois en términos de coacciones de álgebras de Hopf fue la búsqueda de una correspondencia de Galois para extensiones de álgebras que no fueran cuerpos. Una versión del Teorema Principal en ese contexto fue dada por Chase y Sweedler.[17] Dada una coacción de H sobre una F-álgebra conmutativa A con

[15] Debido al mayor alcance de la aplicación canónica β en contraste con su versión transpuesta $\beta^\sharp$, algunos autores dirían que $K\,|\,F$ es una extensión H^*–Galois. Es cuestión de gustos.

[16] Para los detalles sobre este contraejemplo, véase el artículo de Greither y Pareigis, *op. cit.*, inciso 2.4.

[17] Este es esencialmente el Teorema 7.6 en la monografía de Chase y Sweedler, *op. cit.*

coinvariantes $A^{\mathrm{co}H} = F$ y con aplicación canónica biyectiva, a cada subálgebra de Hopf $J \leq H$ le corresponde una única F-subálgebra $B \subseteq A$ tal que $A^{\mathrm{co}J} = B$. (Esta correspondencia no es biunívoca en todos los casos.) La demostración de este teorema está fuera del ámbito de este curso.

5.5 Apéndice: el papel de la antípoda

Cualquier biálgebra H tiene una coacción sobre sí mismo: el *coproducto* $\Delta\colon H \to H \otimes H$ es un ejemplo especial de una coacción. Además, por ser H una biálgebra, Δ es un homomorfismo de álgebras. ¿Qué puede decirse acerca de la aplicación canónica asociada?

La subálgebra coinvariante $H^{\mathrm{co}H}$ consta de los elementos $h \in H$ tales que $\Delta(h) = h \otimes 1$. Pero tales elementos obedecen

$$h = (\varepsilon \otimes \mathrm{id})(\Delta(h)) = (\varepsilon \otimes \mathrm{id})(h \otimes 1) = \varepsilon(h)\,1,$$

así que $H^{\mathrm{co}H} = F$, el cuerpo de escalares. La aplicación canónica para Δ es entonces

$$\beta_H : H \otimes H \to H \otimes H : g \otimes h \mapsto \textstyle\sum g h_{(1)} \otimes h_{(2)}. \tag{5.31}$$

Lema 5.44. *Si H es un álgebra de Hopf, la aplicación canónica β_H es biyectiva.*

Demostración. Si $S\colon H \to H$ es la antípoda de H, considérese la aplicación $\alpha_H \in \mathrm{End}(H \otimes H)$ definida por

$$\alpha_H(g \otimes h) := \textstyle\sum g\, S(h_{(1)}) \otimes h_{(2)}. \tag{5.32}$$

La fórmula (5.15) de la definición de antípoda y la coasociatividad de Δ muestran que

$$\begin{aligned}
\beta_H(\alpha_H(g \otimes h)) &= \textstyle\sum g\, S(h_{(1)}) h_{(2)(1)} \otimes h_{(2)(2)} = \sum g\, S(h_{(1)(1)}) h_{(1)(2)} \otimes h_{(2)} \\
&= \textstyle\sum g\, \varepsilon(h_{(1)}) \otimes h_{(2)} = \sum g \otimes \varepsilon(h_{(1)})\, h_{(2)} = g \otimes h, \\
\alpha_H(\beta_H(g \otimes h)) &= \textstyle\sum g\, h_{(1)} S(h_{(2)(1)}) \otimes h_{(2)(2)} = \sum g\, h_{(1)(1)} S(h_{(1)(2)}) \otimes h_{(2)} \\
&= \textstyle\sum g\, \varepsilon(h_{(1)}) \otimes h_{(2)} = \sum g \otimes \varepsilon(h_{(1)})\, h_{(2)} = g \otimes h,
\end{aligned}$$

para todo $g, h \in H$. Por lo tanto, β_H es biyectiva y α_H es su aplicación inversa. □

El resultado inverso, de que la biyectividad de β_H conlleva la existencia de una antípoda, requiere un resultado previo que tiene su propio interés.[18]

Lema 5.45 (Koppinen)**.** *Sea A un álgebra y C una coálgebra sobre un cuerpo F. Sea $\mathrm{End}_A^C(A \otimes C)$ la subálgebra de $\mathrm{End}(A \otimes C)$ cuyos elementos Λ conmutan con el producto de A a la izquierda y con el coproducto de C a la derecha:*

$$\begin{aligned}
(m \otimes \mathrm{id}_C)(\mathrm{id}_A \otimes \Lambda) &= \Lambda(m \otimes \mathrm{id}_C) : A \otimes A \otimes C \to A \otimes C \\
(\Lambda \otimes \mathrm{id}_C)(\mathrm{id}_A \otimes \Delta) &= (\mathrm{id}_A \otimes \Delta)\Lambda : A \otimes C \to A \otimes C \otimes C.
\end{aligned} \tag{5.33}$$

Entonces $\mathrm{End}_A^C(A \otimes C)$ es antiisomorfo[19] *al álgebra $\mathrm{Hom}(C, A)$ con convolución.*

[18] El lema apareció originalmente en el artículo de Markku Koppinen, "A Skolem–Noether theorem for coalgebra measurings", Archiv der Mathematik 57 (1991), 34–40.

[19] Un *antihomomorfismo* entre dos álgebras es una aplicación lineal que revierte el orden de los productos.

Demostración. Las propiedades de conmutación de Λ se expresan más concretamente así:

$$\begin{aligned} a'\Lambda(a\otimes c) &= \Lambda(a'a\otimes c) \quad \text{para todo} \quad a',a\in A,\ c\in C;\\ \textstyle\sum \Lambda(a\otimes c_{(1)})\otimes c_{(2)} &= (\mathrm{id}_A\otimes\Delta)(\Lambda(a\otimes c)) \quad \text{para todo} \quad a\in A,\ c\in C. \end{aligned} \tag{5.34}$$

Fíjese que Λ queda determinado por sus valores $\Lambda(1\otimes c)$ porque $\Lambda(a\otimes c)=a\Lambda(1\otimes c)$.

Para cada $T\in \mathrm{Hom}(C,A)$, defínase $\widetilde{T}\in \mathrm{End}(A\otimes C)$ por

$$\widetilde{T}(a\otimes c) := \textstyle\sum aT(c_{(1)})\otimes c_{(2)}.$$

Es evidente que $\widetilde{T}$ cumple las dos propiedades (5.34); el valor de la segunda igualdad es $\sum aT(c_{(1)})\otimes c_{(2)}\otimes c_{(3)}$. Además, para todo $c\in H$, se verifica

$$(\mathrm{id}_A\otimes\varepsilon)(\widetilde{T}(1\otimes c)) = \textstyle\sum T(c_{(1)})\,\varepsilon(c_{(2)}) = T\big(\sum c_{(1)}\,\varepsilon(c_{(2)})\big) = T(c).$$

Sea $T_\Lambda := (\mathrm{id}_A\otimes\varepsilon)\Lambda(\eta\otimes\mathrm{id}_C)\in\mathrm{Hom}(C,A)$ para $\Lambda\in \mathrm{End}_A^C(A\otimes C)$. Entonces

$$\begin{aligned} \widetilde{T_\Lambda}(A\otimes c) &= \textstyle\sum aT_\Lambda(c_{(1)})\otimes c_{(2)} = \sum(\mathrm{id}_A\otimes\varepsilon)\big(\Lambda(a\otimes c_{(1)})\big)\otimes c_{(2)}\\ &= (\mathrm{id}_A\otimes\varepsilon\otimes\mathrm{id}_C)(\mathrm{id}_A\otimes\Delta)(\Lambda(a\otimes c)) = \Lambda(a\otimes c), \end{aligned}$$

porque $(\varepsilon\otimes\mathrm{id}_C)\Delta=\mathrm{id}_C$. Esto muestra que la correspondencia $T\mapsto\widetilde{T}$ de $\mathrm{Hom}(C,A)$ en $\mathrm{End}_A^C(A\otimes C)$ es biyectiva: la correspondencia inversa es $\Lambda\mapsto T_\Lambda$.

Ahora, si $R,T\in\mathrm{Hom}(C,A)$, entonces

$$\begin{aligned} \widetilde{R}(\widetilde{T}(a\otimes c)) &= \textstyle\sum\widetilde{R}\big(aT(c_{(1)})\otimes c_{(2)}\big)\\ &= \textstyle\sum aT(c_{(1)})R(c_{(2)(1)})\otimes c_{(2)(2)} = \sum aT(c_{(1)(1)})R(c_{(1)(2)})\otimes c_{(2)}\\ &= \textstyle\sum a(T*R)(c_{(1)})\otimes c_{(2)} = (T*R)\widetilde{\ }(a\otimes c). \end{aligned}$$

Esto es $\widetilde{R}\circ\widetilde{T} = (T*R)\widetilde{\ }$ así que la biyección lineal $T\mapsto\widetilde{T}$ es un antihomomorfismo. □

Proposición 5.46. *Una biálgebra H para la cual la aplicación canónica β_H es biyectiva es un álgebra de Hopf.*

Demostración. En la terminología del lema anterior, las álgebras $\mathrm{End}(H)$, con convolución, y $\mathrm{End}_H^H(H\otimes H)$, con composición, son antiisomorfos. Es evidente de (5.31) que β_H queda en $\mathrm{End}_H^H(H\otimes H)$, con $\beta_H=\widetilde{\mathrm{id}}$. Si β_H es biyectiva, sea $\alpha_H := \beta_H^{-1}\in\mathrm{End}(H\otimes H)$. Este α_H también cumple las relaciones (5.33); en efecto,

$$\begin{aligned} \beta_H\big[(m\otimes\mathrm{id})(\mathrm{id}\otimes\alpha_H)-\alpha_H(m\otimes\mathrm{id})\big](\mathrm{id}\otimes\beta_H) &= \beta_H(m\otimes\mathrm{id})-(m\otimes\mathrm{id})(\mathrm{id}\otimes\beta_H)=0,\\ (\beta_H\otimes\mathrm{id})\big[(\alpha_H\otimes\mathrm{id})(\mathrm{id}\otimes\Delta)-(\mathrm{id}\otimes\Delta)\alpha_H\big]\beta_H &= (\mathrm{id}\otimes\Delta)\beta_H-(\beta_H\otimes\mathrm{id})(\mathrm{id}\otimes\Delta)=0, \end{aligned}$$

y se obtiene (5.33) para $\Lambda=\alpha_H$ puesto que β_H, $(\mathrm{id}\otimes\beta_H)$ y $(\beta_H\otimes\mathrm{id})$ son biyectivos.

Se deduce que hay un único $S\in\mathrm{End}(H)$ tal que $\alpha_H=\widetilde{S}$. Las relaciones $\alpha_H\circ\beta_H=\beta_H\circ\alpha_H=\mathrm{id}_{H\otimes H}$ entonces implican que $\mathrm{id}*S=S*\mathrm{id}=\eta\varepsilon$ en $\mathrm{End}(H)$, lo cual significa que S es una antípoda para H. □

Obsérvese que esta demostración proporciona una fórmula para β_H^{-1}. De hecho, es

$$\beta_H^{-1}(g\otimes h) = \sum g\, S(h_{(1)})\otimes h_{(2)} \quad \text{para todo} \quad g,h\in H.$$

También, se ve que $S(h) = (\mathrm{id}\otimes\varepsilon)(\beta_H^{-1}(1\otimes h))$ para todo $h\in H$.

► Después de la Definición 5.42, se observó que una acción de Hopf de una biálgebra finitodimensional, cuya aplicación canónica es biyectiva, sólo puede existir si la biálgebra es de Hopf, es decir, posee una antípoda. Es hora de justificar esta afirmación.

En primer lugar, si H es un álgebra de Hopf con antípoda $S\in \mathrm{End}(H)$, entonces su transpuesta $S'\in\mathrm{End}(H^*)$ de (5.18) es una antípoda para la biálgebra dual H^* y viceversa. Basta entonces considerar el caso de una coacción de álgebras $\delta\colon A\to A\otimes H$, cuya aplicación canónica viene dada por (5.26). En este caso, el álgebra de coinvariantes $B = A^{\mathrm{co}H}$ no tiene que ser igual a F.

El siguiente resultado generaliza la Proposición 5.46 a otras coacciones con β biyectiva.[20]

Proposición 5.47 (Schauenburg)**.** *Sea H una biálgebra finitodimensional sobre un cuerpo F y supóngase que hay una coacción de álgebras $\delta\colon A\to A\otimes H$, con A finitodimensional sobre F, cuya aplicación canónica β es biyectiva. Entonces H es un álgebra de Hopf.*

Demostración. Hay que mostrar que H posee una antípoda. En virtud del Lema 5.44 y la Proposición 5.46, basta comprobar que la aplicación β_H es inversible en $\mathrm{End}(H\otimes H)$.

Considérese la aplicación ampliada

$$(\mathrm{id}_A\otimes\beta_H)\colon A\otimes H\otimes H\to A\otimes H\otimes H.$$

Obviamente, esta aplicación es biyectiva si β_H es biyectiva. Inversamente, si $\mathrm{id}_A\otimes\beta_H$ es biyectiva, se puede eliminar[21] el factor tensorial A por medio del espacio dual A^*. En efecto, si $\sum_j g_j\otimes h_j\in\ker\beta_H$, entonces

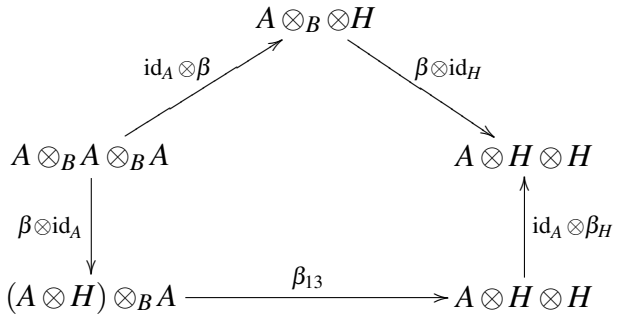
$$\begin{aligned}
(\mathrm{id}_A\otimes\beta_H)\big(\textstyle\sum_j a\otimes g_j\otimes h_j\big) = 0, &\quad \text{para todo} \quad a\in A\\
\Longrightarrow \textstyle\sum_j a\otimes g_j\otimes h_j = 0, &\quad \text{para todo} \quad a\in A\\
\Longrightarrow \langle f,a\rangle\textstyle\sum_j g_j\otimes h_j = 0, &\quad \text{para todo} \quad a\in A,\ f\in A^*\\
\Longrightarrow \textstyle\sum_j g_j\otimes h_j = 0,&
\end{aligned}$$

así que β_H es inyectiva. Un argumento similar muestra que β_H es sobreyectiva.

[20] Véase el artículo de Peter Schauenburg, "A bialgebra that admits a Hopf–Galois extension is a Hopf algebra", *Proceedings of the AMS* 125 (1997), 83–85. La demostración simplificada, debido a Mitsuhiro Takeuchi, se encuentra en: Peter Schauenburg, "Hopf–Galois and bi-Galois extensions", en *Galois Theory, Hopf Algebras and Semiabelian Categories*, AMS, 2004, pp. 469–515.

[21] Todas estas construcciones tienen sentido en el contexto más amplio de álgebras y coálgebras sobre un anillo conmutativo R en vez de un cuerpo F: en lugar de espacios F-vectoriales, se habla de R-módulos. En ese contexto, hay que prevenir fenómenos de torsión en los productos tensoriales. Para poder cancelar el factor tensorial A en este argumento, hay que postular que A sea *un R-módulo fielmente plano*. Véase el libro de Lang, *op. cit.*, capítulo XVI.

Considérese ahora el diagrama "pentagonal" siguiente:



donde $\beta_{13}(c \otimes h \otimes_B a) := \sum c\, a_{(0)} \otimes h \otimes a_{(1)}$ es el producto tensorial de β con id_H "de en medio". Este diagrama conmuta, porque

$$\begin{aligned}(\beta \otimes \mathrm{id}_H)(\mathrm{id}_A \otimes \beta)(a \otimes_B b \otimes_B c) &= (\beta \otimes \mathrm{id}_H)\big(\textstyle\sum a \otimes_B bc_{(0)} \otimes c_{(1)}\big) \\ &= \textstyle\sum ab_{(0)}c_{(0)(0)} \otimes b_{(1)}c_{(0)(1)} \otimes c_{(1)} \\ &= \textstyle\sum ab_{(0)}c_{(0)} \otimes b_{(1)}c_{(1)(1)} \otimes c_{(1)(2)},\end{aligned}$$

a la vez que

$$\begin{aligned}(\mathrm{id}_A \otimes \beta_H)\beta_{13}(\beta \otimes \mathrm{id}_A)(a \otimes_B b \otimes_B c) &= (\mathrm{id}_A \otimes \beta_H)\beta_{13}\big(\textstyle\sum ab_{(0)} \otimes b_{(1)} \otimes_B c\big) \\ &= (\mathrm{id}_A \otimes \beta_H)\big(\textstyle\sum ab_{(0)}c_{(0)} \otimes b_{(1)} \otimes c_{(1)}\big) \\ &= \textstyle\sum ab_{(0)}c_{(0)} \otimes b_{(1)}c_{(1)(1)} \otimes c_{(1)(2)}.\end{aligned}$$

Ahora la hipótesis de la biyectividad de $\beta\colon A \otimes_B A \to A \otimes H$ implica que cada flecha del diagrama es una biyección, con la posible excepción de la flecha $\mathrm{id}_A \otimes \beta_H$. La conmutatividad del diagrama obliga a que $\mathrm{id}_A \otimes \beta_H$ sea también una biyección. Luego, por los argumentos iniciales, β_H es biyectiva y H posee una antípoda. □

Corolario 5.48. *Si H una biálgebra finitodimensional que posee una acción de Hopf sobre un álgebra finitodimensional A, y si la aplicación lineal $c \otimes h \mapsto \big(a \mapsto c\,(h \triangleright a)\big)$ de $A \otimes H$ en* $\mathrm{End}(H)$ *es biyectiva, entonces H es un álgebra de Hopf.*

Demostración. La coacción dual $\delta\colon A \to A \otimes H^*$ tiene aplicación canónica biyectiva, debido al Lema 5.40. La Proposición anterior garantiza que H^* tiene una antípoda S', cuya transpuesta S es una antípoda para H. □

5.6 Ejercicios sobre álgebras de Hopf

Ejercicio 5.1. (a) Sea $K = \mathbb{Q}(\sqrt[4]{2})$. Mostrar que $G = \mathrm{Gal}(K \,|\, \mathbb{Q})$ es isomorfo a C_2 y determinar el cuerpo fijo K^G.

(b) Si $\xi := \sqrt[4]{2}$, tómese $\{1, \xi, \xi^2, \xi^3\}$ como base de K sobre $\mathbb{Q}$. Si $\mu(\alpha) : \beta \mapsto \alpha\beta$ para $\alpha, \beta \in K$, comprobar que $\mu(K)$ y $\mathbb{Q}[G]$ generan un subespacio de dimensión 8 de $\mathrm{End}_{\mathbb{Q}}(K)$.

Ejercicio 5.2. Sean $K = \mathbb{Q}(\sqrt[4]{2})$, $\xi := \sqrt[4]{2}$ de nuevo. Defínase dos aplicaciones $\mathbb{Q}$-lineales $c, s \in \mathrm{End}_{\mathbb{Q}}(K)$ por

$$\begin{aligned} c(1) &:= 1, & c(\xi) &:= 0, & c(\xi^2) &:= -\xi^2, & c(\xi^3) &:= 0, \\ s(1) &:= 0, & s(\xi) &:= -\xi, & s(\xi^2) &:= 0, & s(\xi^3) &:= \xi^3. \end{aligned}$$

(a) Verificar que $c^2 + s^2 = \mathrm{id}$ y $cs = 0$. Si H es la *subálgebra* de $\mathrm{End}_{\mathbb{Q}}(K)$ generada por c, s y sus potencias, mostrar que $\dim_{\mathbb{Q}} H = 4$.

(b) Comprobar que $\mu(K)H = \mathrm{End}_{\mathbb{Q}}(K)$ en este caso.

(c) Expresar $c(\alpha\beta)$ y $s(\alpha\beta)$ en términos de $c(\alpha)$, $c(\beta)$, $s(\alpha)$ y $s(\beta)$ para todo $\alpha, \beta \in K$. Usar las reglas $\Delta(f)(\alpha\beta) = \sum f_{(1)}(\alpha) f_{(2)}(\beta)$ y $\varepsilon(f) := f(1)$ para justificar las fórmulas

$$\Delta(c) = c \otimes c - s \otimes s, \quad \Delta(s) = s \otimes c + c \otimes s, \quad \varepsilon(c) = 1, \quad \varepsilon(s) = 0.$$

(d) Comprobar que la biálgebra H posee una antípoda S tal que $S(c) = c$ y $S(s) = -s$, al resolver el sistema de ecuaciones

$$\sum a_{(1)} S(a_{(2)}) = \sum S(a_{(1)}) a_{(2)} = \varepsilon(a)\, 1_H \quad \text{para todo} \quad a \in H.$$

¿Cuanto vale $S(c^2)$?

Ejercicio 5.3. Sea C un espacio vectorial sobre un cuerpo F de dimensión n^2, con base $\{x_{ij} : i, j = 1, 2, \ldots, n\}$. Defínase las aplicaciones lineales $\Delta\colon C \to C \otimes C$ y $\varepsilon\colon C \to F$ por

$$\Delta(x_{ij}) := \sum_{k=1}^{n} x_{ik} \otimes x_{kj}, \qquad \varepsilon(x_{ij}) := \delta_{i,j},$$

donde $\delta_{i,j}$ es la delta de Kronecker. Verificar que (C, Δ, ε) es una coálgebra sobre F, es decir, comprobar las propiedades de coasociatividad y counidad. ¿Cuál es el álgebra dual C^*?

Ejercicio 5.4. Sea $\lambda\colon G \times X \to X : (g, x) \mapsto g \triangleright x$ una acción a la izquierda de un grupo finito G sobre un conjunto finito X. Denótese por $\mathcal{O}(X)$ la totalidad de funciones $f\colon X \to F$, que es un álgebra sobre F con la suma y producto usuales de funciones.

(a) Mostrar que la aplicación lineal $\delta : \mathcal{O}(X) \to \mathcal{O}(X) \otimes \mathcal{O}(G) = \mathcal{O}(X \times G)$, definida por $\delta(f)(x, g) := f(g^{-1} \triangleright x)$, es una coacción de álgebras de $\mathcal{O}(G)$ sobre $\mathcal{O}(X)$.

(b) Si $\mathbf{1}$ es la función constante de valor 1 sobre G, mostrar que $\delta(f) = f \otimes \mathbf{1}$ si y sólo si la función f es constante sobre cada órbita $G \triangleright x$.

(b) Si la acción λ es transitiva, mostrar que la aplicación canónica asociada a δ es

$$\beta(\ell)(x, g) = \ell(x, g^{-1} \triangleright x), \quad \text{para} \quad \ell \in \mathcal{O}(X \times X).$$

Concluir que β es inyectiva si y sólo si la acción λ es libre.

Nota bibliográfica

Hay pocos libros en español dedicados al tema de este curso, aunque buena parte de la materia se encuentra en los libros generales sobre álgebra abstracta. En las lecciones se ha mencionado, de paso, algunos libros y artículos de revistas, dignos de considerar. También se encuentran en la red varios cursos sobre la teoría de Galois, desde diversos puntos de vista.

De entre los libros dedicados exclusivamente a la teoría de Galois, los siguientes son dignos de mencionar.

1. Emil Artin y Arthur N. Milgram, *Galois Theory*, University of Notre Dame Press, 1942.
   Una joya de exposición matemática, breve y concisa.

2. Richard Brauer, *Galois Theory*, Harvard University Lecture Notes, Cambridge, MA, 1964.
   Una edición rústica de un curso de Brauer en Harvard.

3. Harold M. Edwards, *Galois Theory*, Graduate Texts in Mathematics 101, Springer, New York, 1984.
   Una monografía histórica sobre los trabajos de Lagrange y Galois. Un complemento interesante al enfoque "artiniano" moderno.

4. Jean-Pierre Escofier, *Galois Theory*, Graduate Texts in Mathematics 204, Springer, Berlin, 2001.
   Un curso muy ameno, traducido del francés. En estas lecciones hemos seguido el enfoque de Escofier, en particular la decisión de desarrollar la teoría para subcuerpos de $\mathbb{C}$, antes de abordar cuerpos de característica prima.

5. Lisl Gaal, *Classical Galois Theory*, Chelsea, New York, 1973.
   Un texto *sui generis*, con gran cantidad de ejemplos.

6. Charles R. Hadlock, *Field Theory and its Classical Problems*, Carus Mathematical Monographs **19**, MAA, Washington, DC, 1978.
   El prólogo del libro enuncia: "I wrote this book for myself." Una exposición clara y detallada de las bases de la teoría.

7. Héctor A. Merklen, *Estructuras Algebraicas V (Teoría de Cuerpos)*, Serie OEA de Matemática, Washington, DC, 1979.
   El único texto en español que hemos encontrado. Un desarrollo muy competente, con un estilo algo abstracto.

8. M. Pavaman-Murthy, K. G. Ramanathan, C. S. Seshadri, U. Shukla y R. Sridharan, *Galois Theory*, Tata Institute for Fundamental Research, Bombay, 1965.
   Un breve curso de estilo *Satz-Beweis*, sin muchos ejemplos pero con demostraciones muy elegantes.

9. Joseph J. Rotman, *Galois Theory*, Universitext, Springer, Berlin, 1990.
   Un curso conciso y útil, pero sin la claridad del libro de Artin.

10. Ian N. Stewart, *Galois Theory*, Chapman & Hall/CRC, 3ra edición, 2003.
El texto favorito de los estudiantes, desde la primera edición en 1973.

Todos los libros comprensivos de álgebra traen uno o más capítulos dedicados a la teoría de Galois. Entre ellos, se destacan los siguientes.

11. John Derbyshire, *Unknown Quantity*, Joseph Henry Press, Washington, DC, 2006.
Un libro para el público (educado) general, que trata de contar la historia del álgebra. Los capítulos sobre la resolución de ecuaciones y la teoría de grupos son muy informativos.

12. Israel N. Herstein, *Topics in Algebra*, Blaisdell, New York, 1964.
El capítulo sobre la teoría de cuerpos trae pruebas muy detalladas.

13. Nathan Jacobson, *Basic Algebra I*, W. H. Freeman, New York, 1985.
Un tratado comprehensivo de álgebra abstracta, con un excelente exposición de la teoría de Galois.

14. Serge Lang, *Algebra*, tercera edición, Springer, New York, 2002.
Lang fue estudiante y discípulo de Artin. Sus capítulos sobre polinomios, extensiones algebraicas y teoría de Galois son un homenaje al maestro.

15. Bartel L. van der Waerden, *Modern Algebra 1*, Frederick Ungar, New York, 1953.
Una traducción y reedición del libro *Moderne Algebra* de 1930. Un tratado general de álgebra muy influyente, basado en su colaboración con Emmy Noether. Las secciones sobre la teoría de Galois son notablemente modernas.

16. H. Weber, *Lehrbuch der Algebra*, tomo 1, Friedrich Vieweg, Braunschweig, 1898; reimpreso por Chelsea, New York, 1979.
Un tratado de álgebra de la época "pre-artiniana", que trae un extenso estudio de las extensiones cíclicas y ciclotómicas.

Una búsqueda por internet encuentra un surtido de cursos sobre la teoría de Galois. Entre ellos, los siguientes han sido fuentes de algunos de los ejercicios para este curso.

17. Andrew Baker, *An Introduction to Galois Theory*, curso en la Universidad de Glasgow, 2006. URL: <www.maths.gla.ac.uk/~ajb/dvi-ps/Galois.pdf>.

18. Fernando Chamizo Lorente, *¡Qué bonita es la teoría de Galois!*, curso en la Universidad Autónoma de Madrid, 2004. URL:
<http://www.uam.es/personal_pdi/ciencias/fchamizo/algebraIIn.html>.

19. James S. Milne, *Fields and Galois Theory*, curso de posgrado en la Universidad de Michigan. Versión 4, 2005. URL:
<http://www.jmilne.org/math/CourseNotes/math594f.html>.

20. Miles Reid, *MA3D5 Galois Theory*, curso en la Universidad de Warwick, 2004. URL:
<http://www.maths.warwick.ac.uk/~miles/MA3D5/>.

Indíce alfabético