UNIVERSIDAD NACIONAL DE LA MATANZA

Departamento de Formación Continua

Tesis de Licenciatura

Sobre la imposibilidad de resolver algebraicamente la ecuación general de quinto grado y de grados superiores

Ricardo Bernabé Baloni

Director de Tesis: Lic. Miguel Calzón

Fecha de presentación: 23 de febrero de 2011

Índice general

Introducción.....4

1 Campos de Extensiones.....8

§ 1. Extensiones simples.....8

§ 2. Elementos algebraicos y trascendentes.....12

§ 3. Extensiones finitas.....17

§ 4. Extensiones Algebraicas.....20

§ 5. Extensiones Normales y Campos de Descomposición.....24

§ 6. Extensiones separables.....33

2 Grupos Resolubles. El Grupo simétrico S_n.....39

§ 1. Resultados necesarios de la teoría de grupos.....39

§ 2. Grupos resolubles.....43

§ 3. El grupo simétrico S_n.....47

3 Teoría de Galois.....59

§ 1. El Grupo de Galois.....59

§ 2. El orden del Grupo de Galois.....69

§ 3. La correspondencia de Galois.....75

§ 4. El Teorema Fundamental de la Teoría de Galois……..….78

§ 5. Permutación de las raíces y el Grupo de Galois……89

4 Grupos y ecuaciones……..92

§ 1. Polinomios simétricos elementales……...……..92

§ 2. Polinomio simétricos……..96

§ 3. El Grupo de Galois y el grupo simétrico S_n……..…...102

§ 4. Solubilidad por radicales……105

§ 5. El resultado final……...…109

Bibliografía……...…117

Introducción

En la historia de la Matemática ha habido varios problemas que involucraron a grandes matemáticos. Un ejemplo de estos problemas es el que concierne a la demostración de célebre Último Teorema de Fermat, postulado en 1637 por Pierre de Fermat y demostrado "recién" en 1995 por Andrew Wiles. En ciertos casos la distancia entre los resultados matemáticos y su demostración final consiste en unos cuantos cientos de años.

En el mismo sentido que en el caso anterior existen varios ejemplos de resultados escurridizos y aparentemente indemostrables, como por ejemplo la Hipótesis de Riemann, que desvelaron y siguen desvelando a las mentes de ayer y de hoy.

En particular, resulta atractiva la historia de uno de ellos, no solo por lo que significó su resolución para la Matemática sino también por sus protagonistas. El mismo es el que tiene que ver con la solución por radicales de la ecuación de quinto grado.

Es sabido que las ecuaciones de primer y segundo grado fueron resueltas de forma eficaz por los antiguos babilonios hacia el año 2000 a. C. Por su parte, la solución las ecuaciones de tercer y cuarto grado se hicieron esperar un poco más. En cuanto a la primera, Scipione del Ferro (1465 - 1526) en 1515 y Nicolo "tartaglia" Fontana (c 1500 - 1557) en 1535 resolvieron algunos casos particulares y finalmente en 1545 Girolamo Cardano (1501 - 1576), en su *Ars Magna*, publicó los trabajos Tartaglia y algunos avances hechos por él mismo llegando finalmente a la conocida Fórmula de Cardano para la ecuación de tercer grado. En cuanto a la ecuación de cuarto grado, Lodovico Ferrari (1522 - 1565), alumno de Cardano, consiguió hallar su solución basada en los métodos presentados por Tartaglia. Los trabajos hechos por Ferrari también fueron publicados en el *Ars Magna* de su maestro.

Era de esperarse que algo parecido ocurriese con la ecuación de quinto grado.

Desde ese momento la búsqueda de la solución de la ecuación de quinto grado y de grados más elevados se convirtió en el objetivo principal de los matemáticos de esa época. Una de las publicaciones más importantes sobre la teoría de ecuaciones fue *Réflexions sur la Résolution Algébrique des Équations* (1770 – 1771) del brillante J. L. Lagrange (1736 - 1813). Por su parte, casi al mismo tiempo que Lagrange, Alexandre Vandermonde (1735 – 1736) publicó en 1770 su *Mémoire sur la Résolution des Équations.*

A pesar de haber avanzado increíblemente en la Teoría de Ecuaciones, la solución de la quíntica seguía sin aparecer.

En 1799 Paolo Ruffini publicó su *Teoría Generale delle Equazioni: in cui si demostra impossibile La Soluzione Algebraica delle Equazioni Generale di Grado Superiore al Quarto.* Ruffini aseguraba haber demostrado la imposibilidad de resolver algebraicamente, es decir por radicales, la ecuación general de quinto grado y de grados superiores, sin embargo su demostración resulto estar incompleta.

Finalmente en 1824 el matemático noruego Niels Henrik Abel en su *Mémoire sur les Équations Algébriques: où on demontre l´impossibilité de la résolution de l´équation générale du cinquième dégré*, logro demostrar al fin que la ecuación general de quinto grado no es resoluble por radicales.

La idea de Abel consistió en considerar la expresión general de lo que él llamo las expresiones algebraicas. Luego de hallar y demostrar la generalidad de esta expresión, supuso que si la ecuación general de quinto grado fuese resoluble por radicales, entonces cada raíz debería poder representarse por una determinada expresión algebraica de este tipo. A partir de allí, Abel reemplazó esta expresión por la incógnita en la ecuación general de quinto grado y llego a una contradicción.

El traspié en la prueba de Ruffini fue utilizar esta expresión sin haberla demostrado.

Más tarde, en 1832, de manera independiente y con una estrategia muy distinta a la de Abel, el joven matemático francés Evariste Galois llego a la misma conclusión sobre la quíntica. Las ideas utilizadas por Galois en su demostración involucraron de manera rudimentaria, elementos del Álgebra Abstracta, tales como el concepto de grupo y los campos de extensión. En cuanto a este último

tema, Galois introdujo el concepto de la adjunción de elementos a un campo base, lo cual es fundamental el la teoría de campos. En este sentido, los trabajos de Galois originalmente destinados a la Teoría de Ecuaciones fueron más significativos que los de Abel, sin que esto signifique un desmerito para Abel, puesto que sus ideas fueron el comienzo del Álgebra Abstracta, que aun hoy sigue siendo un fructífero campo de investigación.

En las páginas siguientes, desde un enfoque moderno, desarrollaremos algunos conceptos de la Teoría de Galois necesarios para llegar finalmente a la demostración de la imposibilidad de resolver por radicales la ecuación general de quinto grado y de grados superiores.

Evariste Galois a la edad de 15 años

"Pide a Jacobi o a Gauss

que den públicamente su opinión,

no en cuanto a la veracidad,

sino a la importancia de estos teoremas.

Más tarde habrá gente, espero, que

verá conveniente descifrar todo este embrollo"

Fragmento de la carta de Evariste Galois a su amigo Auguste Chevalier, 29 de mayo de 1832.

Capítulo 1

Campos de extensión

La teoría original de Galois fue pensada en términos de los polinomios sobre el campo de los Números Complejos. Luego, con el avance del Álgebra se generalizaron estas ideas a campos arbitrarios. Empecemos entonces recordando algunos conceptos concernientes a la Teoría de Campos que serán claves para abordar los conceptos principales de la Teoría de Galois, expuesta en los capítulos siguientes. En este primer capítulo comenzaremos por definir lo que se llama campo de extensión.

§ 1 Extensiones simples.

Definición 1. Sean K y L dos campos y sea $\varphi: K \to L$ un monomorfismo entre K y L. Diremos que L es una *extensión* de K (o campo de extensión) vía φ.

Si identificamos a K con su imagen en L, la cual denotamos por $\varphi(K)$, es claro que

$$\varphi: K \to \varphi(K)$$

Es un isomorfismo, esto es, K es isomorfo a un subcampo de L. Bajo estas circunstancias podemos considerar que K es un subcampo de L, i.e. $K \subset L$.

Si L es una extensión de K (o sobre K), se denota $L:K$ o L/K y se dice que K es el campo base.

Sean L y K dos campos de manera que L es una extensión de K. Se define la extensión generada por $\alpha \in L$ sobre K como conjunto

$$K(\alpha) = \left\{\frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], \alpha \in L, g(\alpha) \neq 0\right\}$$

Dado que todo elemento de $K[x]$ también está en $L[x]$ y como $\alpha \in L$, si $f \in K[x]$ entonces $f(\alpha) \in L$. Del mismo modo, si $g \in K[x]$ entonces $g(\alpha) \in L$, y si además $g(\alpha) \neq 0$, luego existe $g(\alpha)^{-1} \in L$, asi pues $\frac{f(\alpha)}{g(\alpha)} = f(\alpha)g(\alpha)^{-1} \in L$ y es $K(\alpha) \subset L$.

El conjunto $K(\alpha)$ es el conjunto de todas las expresiones racionales en α con coeficientes en K. Como $K \subset L$, se sigue que $K(\alpha) \subset L(\alpha)$. Por otra parte, teniendo en cuenta que $L(\alpha)$ es el campo de cocientes de $L[\alpha]$, restringiendo las operaciones del campo $L(\alpha)$ a $K(\alpha) \subset L(\alpha)$, es fácil probar que $K(\alpha)$ es un campo.

Sean $f(x) = a$, con $a \in K$, y sea $g(x) = 1$, entonces $\frac{f(\alpha)}{g(\alpha)} = \frac{a}{1} = a$, para todo $a \in K$. Esto muestra que todo elemento de a de K esta en $K(\alpha)$. Por otra parte sea $f(x) = x$, entonces $\frac{f(\alpha)}{g(\alpha)} = \frac{\alpha}{1} = \alpha$. Esto es, $\alpha \in K(\alpha)$ y dado que $\alpha \in L$, pero no necesariamente pertenece a K, vemos que $K \subset K(\alpha)$.

Por otra parte, dado que L es un campo y por lo tanto el campo cociente de L es el mismo L y que el campo de cocientes de un dominio entero (de hecho L es un dominio entero por ser campo) es el menor campo que lo contiene, no queda otra que $K(\alpha) \subset L$. Luego tenemos que $K(\alpha)$ es una extensión de K y que L es una extensión de $K(\alpha)$.

Definición 2. Un campo de extensión L de un campo K es una *extensión simple* de K si $L = K(\alpha)$ para algún $\alpha \in L$.

Es claro que $K = K(\alpha)$ si $\alpha \in K$.

Teorema 3. Sea $L = K(\alpha)$ una extensión simple de K. Entonces $K(\alpha)$ es la menor extensión que contiene a K y a α.

Demostración: Supongamos que H es una extensión de K de modo tal que $\alpha \in H$. Dado que $K(\alpha) = \left\{\frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], \alpha \in L, g(\alpha) \neq 0\right\}$ y $K \subset H$, si $f, g \in K[x]$, entonces $f, g \in H[x]$, y dado que $\alpha \in H$, sigue que $f(\alpha), g(\alpha) \in H[\alpha]$. Por último, como H es un campo, si $g(\alpha) \neq 0$, entonces existe $g(\alpha)^{-1} \in H$, por ende $\frac{f(\alpha)}{g(\alpha)} \in H$. Luego $K(\alpha) \subset H$. Queda entonces demostrado que $F(\alpha)$ es la menor extensión que contiene a F y a α.

A este proceso se le denomina, *adjunción* del elemento α al cuerpo K.

Sea L un campo de extensión del campo K, y sean α_1, α_2 elementos de L. Según lo que vimos antes, $K(\alpha_1)$ es la menor extensión de K en L que contiene al elemento $\alpha_1$de L. En forma análoga, $\big(K(\alpha_1)\big)(\alpha_2)$ puede considerarse como la menor extensión de K en L que contiene a α_2. Tambien podíamos haber comenzado con α_2, de modo que claramente $\big(K(\alpha_1)\big)(\alpha_2) = \big(K(\alpha_2)\big)(\alpha_1)$. Denotamos a este campo por $K(\alpha_1\ \alpha_2)$. De manera análoga, para $\alpha_1, \dots, \alpha_n \in L$, $K(\alpha_1, \dots, \alpha_n)$ es el menor campo de extensión de K en L, que contiene a $\alpha_1, \dots, \alpha_n$. De esta forma se obtiene el campo $K(\alpha_1, \dots, \alpha_n)$ mediante la adjunción de los elementos $\alpha_1, \dots, \alpha_n \in L$ a K.

Teorema 4. $K(\alpha_1, \dots, \alpha_n)$ es el menor subcampo de L que contiene a K y a $\alpha_1, \dots, \alpha_n$.

Demostración: De forma análoga en que mostramos que $K(\alpha)$, con $\alpha \in L$, es un subcampo del campo L, en la página anterior, se muestra que $F(\alpha_1, \dots, \alpha_n)$, con $\alpha_1, \dots, \alpha_n \in L$, es un subcampo de L. Entonces para demostrar el teorema debemos mostrar que si E es un subcampo de L que contiene a $\alpha_1, \dots, \alpha_n$ y a K entonces $K(\alpha_1, \dots, \alpha_n) \subset E$. Entonces supongamos que $E \subset L$ contiene a $\alpha_1, \dots, \alpha_n$ y a K. Luego para cualquier $p \in K[x_1 \dots, x_n]$, debe suceder que $p(\alpha_1, \dots, \alpha_n) \in E$, dado que E es cerrado bajo la suma y la multiplicación. Esto muestra que

$F[\alpha_1, \dots, \alpha_n] \subset E$. De esto se sigue inmediatamente que $K(\alpha_1, \dots, \alpha_n) \subset E$, debido a que E es un campo.

Dado que $K(\alpha_1, \dots, \alpha_n)$ es un subcampo de L que contiene a K, obtenemos las extensiones

$$K \subset K(\alpha_1, \dots, \alpha_n) \subset L$$

Corolario 5. Si $K \subset L$ y $\alpha_1, \dots, \alpha_n \in L$, entonces

$$K(\alpha_1, \dots, \alpha_n) = (K(\alpha_1, \dots, \alpha_r))(\alpha_{r+1}, \dots, \alpha_n)$$

para cualquier $1 \leq r \leq n - 1$.

Demostración: Para que se cumpla la igualdad de estos conjuntos debemos probar la doble inclusión. Veamos. El campo $(K(\alpha_1, \dots, \alpha_r))(\alpha_{r+1}, \dots, \alpha_n)$ se obtiene a partir de la adjunción de los elementos $\alpha_1, \dots, \alpha_r \in L$ a K y luego la adjunción de los elementos $\alpha_{r+1}, \dots, \alpha_n \in L$ al campo $K(\alpha_1, \dots, \alpha_r)$. El campo $(K(\alpha_1, \dots, \alpha_r))(\alpha_{r+1}, \dots, \alpha_n)$ obviamente contiene a K y a $\alpha_1, \dots, \alpha_r, \alpha_{r+1}, \dots, \alpha_n \in L$. Luego el Teorema 4 implica que

$$K(\alpha_1, \dots, \alpha_n) \subset (K(\alpha_1, \dots, \alpha_r))(\alpha_{r+1}, \dots, \alpha_n)$$

Ahora. Dado el campo K y los elementos $\alpha_1, \dots, \alpha_r \in K(\alpha_1, \dots, \alpha_n)$, el Teorema 4 implica que $K(\alpha_1, \dots, \alpha_r)$ es el menor campo que contiene a K y a los elementos $\alpha_1, \dots, \alpha_r \in K(\alpha_1, \dots, \alpha_n)$. Nuevamente, dado el campo $K(\alpha_1, \dots, \alpha_r)$ y los elementos $\alpha_{r+1}, \dots, \alpha_n \in K(\alpha_1, \dots, \alpha_n)$, se sigue del Teorema 4, que $(K(\alpha_1, \dots, \alpha_r))(\alpha_{r+1}, \dots, \alpha_n)$ es el menor subcampo de $K(\alpha_1, \dots, \alpha_n)$ que contiene a $\alpha_{r+1}, \dots, \alpha_n$ y a $K(\alpha_1, \dots, \alpha_r)$, y por ende $\big(K(\alpha_1, \dots, \alpha_r)\big)(\alpha_{r+1}, \dots, \alpha_n) \subset K(\alpha_1, \dots, \alpha_n)$.

De esto resulta que

$$K(\alpha_1, \dots, \alpha_n) = (K(\alpha_1, \dots, \alpha_r))(\alpha_{r+1}, \dots, \alpha_n)$$

Tal como dijimos al principio.

§ 2 Elementos algebraicos y trascendentes.

Si pensamos en hallar las raíces de un polinomio sobre el campo de los números racionales, una de las preguntas que podemos hacernos es ¿Qué clase de números cumplen con esta condición? O a veces mucho mejor aun es ¿Qué clase de números cumplen "no" con esta condición? Como sabemos, en general las raíces de un polinomio tal son reales pertenecientes a $\mathbb{R} \setminus \mathbb{Q}$ o complejas del tipo$\mathbb{C} \setminus \mathbb{R}$. El problema inverso sería, dado un número real o complejo cualquiera, de los mencionados anteriormente, ¿Existe un polinomio que tenga a este número como raíz? Lamentablemente hay que decir que estos problemas son extremadamente difíciles de resolver en ciertos casos. Para convencernos de esto podríamos intentar hallar un polinomio sobre los racionales que tenga a $\frac{\pi+1}{\sqrt{17}}$ como raíz.

Definición 1. Sea L una extensión del campo K y sea α un elemento de L. Diremos que α es *algebraico* sobre K si existe un polinomio no constante $f \in K[x]$ tal que $f(\alpha) = 0$. Si α no es algebraico sobre K, diremos que α es trascendente sobre K.

Por ejemplo, $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, puesto que es raíz del polinomio $f = x^2 - 2 \in \mathbb{Q}[x]$, sin embargo se ha demostrado que los números π y e son trascendentes sobre $\mathbb{Q}$[1]. Notemos también que cualquier número de la forma $\sqrt{a} + \sqrt{b}$, con a, b primos es algebraico sobre $\mathbb{Q}$. En efecto, poniendo

$$x = \sqrt{a} + \sqrt{b}$$

Al elevar al cuadrado esta igualdad tenemos la siguiente expresión

$$x^2 - a - b = 2\sqrt{a}\sqrt{b}$$

1- La trascendencia del número e fue demostrada por Charles Hermite en 1873 y en 1882, Ferdinand Lindemann logro adaptar el planteamiento de Hermite para demostrar la trascendencia del número π.

Elevando al cuadrado una vez más hallamos

$$x^4 - 2x^2(a+b) + (a+b)^2 = 4ab$$

Luego

$$x^4 - 2x^2(a+b) + a^2 + b^2 - 2ab = 0$$

Esto muestra que el número $\sqrt{a} + \sqrt{b}$ es raíz del polinomio $f = x^4 - 2x^2(a+b) + a^2 + b^2 - 2ab \in \mathbb{Q}[x]$.

Si el elemento α de L es algebraico sobre K, pueden haber infinitos polinomios no constantes en $K[x]$ para los cuales α es una raíz. Uno de estos polinomios es de particular importancia.

Teorema 2. Si α de L es algebraico sobre el campo K, entonces hay un único polinomio mónico no constante $p \in K[x]$ con las siguientes dos propiedades:

1. α es raíz de p, esto es $p(\alpha) = 0$

2. Si $f \in K[x]$ y además $f(\alpha) = 0$, entonces f es un múltiplo de p.

Demostración: De entre todos los polinomios no constantes en $K[x]$ para los que α es una raíz, debe haber uno de menor grado. Tomemos este polinomio y llamémoslo p. Dado que K es campo, no se pierde generalidad si se supone que p es monico. De hecho, si no lo fuese, al multiplicar por una constante adecuada se obtiene el polinomio mónico deseado. Esta claro que p satisface la primera propiedad. Supongamos ahora que $f(\alpha) = 0$ para algún $f \in K[x]$. El conocido Algoritmo de la División[1] en $F[x]$ nos da dos polinomios q y r en $K[x]$, tales que

$$f = q \cdot p + r$$

1- El Algoritmo de la División es abordado en cualquier libro de álgebra. Véase por ejemplo Álgebra Abstracta de J. Fraleigh.

Con $r = 0$ o $\mathrm{Grad}(r) < \mathrm{Grad}(p)$. Evaluando estos polinomios en α tenemos

$$f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha) = 0$$

Dado que $p(\alpha) = 0$, entonces $r(\alpha) = 0$. Pero si es $\mathrm{Grad}(r) < \mathrm{Grad}(p)$, se contradice el hecho de que p es el polinomio de menor grado para el cual $p(\alpha) = 0$. Luego tiene que ser $r = 0$. Por lo tanto p satisface la segunda propiedad.

Definición 3. Sea $\alpha \in L$. Si α es algebraico sobre K. Entonces el polinomio del teorema 2 se llama *polinomio minimal* de α sobre K. Un polinomio no constante $f \in K[x]$ se llama *irreducible* sobre K si no es un producto de polinomios en $K[x]$ de grado estrictamente menor.

Teorema 4. Sea $\alpha \in L$ algebraico sobre K, y sea $p \in K[x]$ su polinomio minimal. Si $f \in K[x]$ es un polinomio monico no cosnstante, entonces:

1. $f = p \Leftrightarrow f$ es un polinomio de grado minimal que cumple $f(\alpha) = 0$

2. $f = p \Leftrightarrow f$ es irreducible sobre K y $f(\alpha) = 0$.

Demostración: La primera equivalencia sigue de la demostración del Teorema 2. Para la segunda, probaremos que el polinomio minimal p es irreducible sobre K. Si $p = gh$, donde $g, h \in K[x]$ tienen grado estrictamente menor que p, entonces $0 = p(\alpha) = g(\alpha)h(\alpha)$ lo cual implica que $g(\alpha) = 0$ o $h(\alpha) = 0$, lo cual contradice la primer equivalencia.

Por el contrario, supongamos que $f(\alpha) = 0$ y que f es irreducible. Entonces p divide a f por el Teorema 2, así que $f = ph$, con $h \in K[x]$. Dado que f es irreducible y p es no constante, h debe ser constante, entonces sigue que $f = p$ debido a que f y p son polinomios mónicos.

Dado que $K[x]$ es un anillo, se pueden considerar ideales del mismo. Sea $p \in K[x]$, entonces se demuestra muy fácilmente que el conjunto

$$\langle p \rangle = \{hp : h \in K[x]\}$$

es el ideal del anillo $K[x]$, generado por p[1]. El siguiente teorema relaciona esta clase de ideales con los campos de extensión.

Teorema 5. Sea L un campo de extensión del campo K, y sea $\alpha \in L$ algebraico sobre K, con polinomio minimal $p \in K[x]$. Entonces existe un único isomorfismo de anillo

$$K[\alpha] \simeq K[x]/\langle p \rangle$$

que es la identidad sobre K y envía a α a la clase lareral $x + \langle p \rangle$.

Demostración: Considere el homomorfismo de anillos $\varphi : K[x] \to L$ que envía $h(x) \in K[x]$ a $h(\alpha) \in L$. Por definición, la imagen de $K[\alpha]$. Para el Kernel, afirmamos que $\mathrm{Ker}(\varphi) = \langle p \rangle$. Para probar esto, primero notemos que $g \in K[x]$ implica que

$$\varphi(gp) = \varphi(g)\varphi(p) = g(\alpha)p(\alpha) = g(\alpha)0 = 0$$

Esto muestra que $\langle p \rangle \subset \mathrm{Ker}(\varphi)$. Para la otra inclusión, supongamos que $f \in \mathrm{Ker}(\varphi)$. Entonces $f(\alpha) = 0$, lo cual, por la segunda parte del Teorema 2 implica que f es múltiplo de p. Entonces $\mathrm{Ker}(\varphi) \subset \langle p \rangle$, y entonces sigue que:

$$\mathrm{Ker}(\varphi) = \langle p \rangle$$

Dado que conocemos la imagen y el Kernel de φ, el Primer Teorema del Homomorfismo de Anillos[2] tenemos que

$$K[x]/\langle p \rangle \simeq K[\alpha]$$

1- Un estudio breve sobre los ideales de un anillo de polinomios puede encontrarse por ejemplo Ideals Varieties and Algorithms de D. Cox, J. Little y D. O´Shea Ed. 2007.

2- El Primer Teorema del Homomorfismo de Anillos es un resultado clásico de la Teoría de Anillos. En el capítulo 2 demostraremos la versión de este teorema para grupos. Para un estudio detallado del Primer, segundo y tercer Teorema del Homomorfismo de anillos, véase por ejemplo Álgebra Abstracta de Herstein, Teorema 4.3.3, pág. 141.

Este isomorfismo es la identidad sobre K y envía la clase $x + \langle p \rangle$ a α. Su inverso es el isomorfismo descripto en el enunciado del teorema.

Finalmente, la unicidad sigue, dado que todo homomorfismo definido sobre $K[\alpha]$ está unívocamente determinado por los valores sobre K y α.

Este teorema muestra como representar a $K[\alpha]$ como un anillo cociente. Por otra parte dado que $p \in K[x]$ es el polinomio minimal de α, es entonces irreducible por el Teorema 4. Por otra parte, se demuestra que si p es irreducible, entonces $K[x]/\langle p \rangle$ es un campo[1]. Luego por el Teorema 5, $K[\alpha]$ es un campo, cuando α es algebraico sobre K.

Teorema 6. Supongamos que L es un campo de extensión del campo K, y sea $\alpha \in L$. Entonces α es algebraico sobre K si y solo si $K[\alpha] = K(\alpha)$.

Demostración: Cuando α es algebraico sobre K, la observación hecha en el párrafo anterior muestra que $K[\alpha]$ es un campo que contiene a K y a α. Por el Teorema 3, sección 1, sabemos que $K(\alpha)$ es el menor subcampo de L que contiene a K y a α, sigue entonces que $K(\alpha) \subset K[\alpha]$. La inclusión opuesta es siempre verdadera. De este modo, $K[\alpha] = K(\alpha)$ cuando α es algebraico sobre K.

Para la otra implicación, supongamos que $K[\alpha] = K(\alpha)$. Debemos tomar $\alpha \neq 0$, puesto que obviamente 0 es algebraico sobre K. Entonces $1/\alpha \in K(\alpha) = K[\alpha]$ implica que

$$1/\alpha = a_0 + a_1\alpha + \cdots + a_m\alpha^m$$

Para algunos elementos $a_0, \ldots, a_n \in K$. Entonces

$$0 = -1 + a_0\alpha + a_1\alpha^2 + \cdots + a_m\alpha^{m+1}$$

Lo cual demuestra que α es algebraico sobre K.

1- Véase Galois Theory de D. Cox, Proposición 3.1.1 p. 57.

Veamos a continuación una generalizacion natural del teorema anterior.

Teorema 7. Sea L es un campo de extensión del campo K, y sean $\alpha_1, \dots, \alpha_n \in L$ algebraicos sobre K. Entonces

$$K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$$

Demostración: Por el argumento utilizado en la demostración del Teorema 6, es suficiente probar que $K[\alpha_1, \dots, \alpha_n]$ es un campo. Hagamos esto por inducción. El caso $n = 1$ es verdadero por el Teorema 6. Ahora supongamos que $n > 1$ y que y que $K[\alpha_1, \dots, \alpha_n]$ es un campo. Sabemos que $f(\alpha_n) = 0$ para algún $f \in K[x]$. Ahora podemos considerar a f como a un polinomio con coeficientes en el campo más grande $K[\alpha_1, \dots, \alpha_{n-1}]$, tal que α_n es algebraico sobre $K[\alpha_1, \dots, \alpha_{n-1}]$. Entonces el Teorema 6 implica que

$$K[\alpha_1, \dots, \alpha_{n-1}][\alpha_n]$$

Es un campo. Puesto que

$$K[\alpha_1, \dots, \alpha_{n-1}][\alpha_n] = K[\alpha_1, \dots, \alpha_n]$$

Finalmente queda demostrado el teorema.

§ 3 Extensiones finitas.

Hay una relación entre un campo K y una extensión L del mismo que hasta ahora no se ha considerado pero que es muy fácil de ver. Supongamos que L es una extensión del campo K. Dado que L es un campo, entonces es un grupo abeliano bajo la suma definida en el. Por otra parte dado que $K \subset L$, para cualquier elemento α de K y para cualquier elemento β de L se cumple que $\alpha\beta \in L$. De esta forma podemos definir una multiplicación a izquierda por un escalar, la cual vimos es cerrada, y considerar a L como un espacio vectorial sobre el campo K. De esta forma se define otro tipo de extensión.

Definición 1. Sea L un campo de extensión de K. L es una *extensión finita* de K si L es un espacio vectorial de dimencion finita sobre K. Si L es una extensión finita sobre K, el *grado* de L sobre K, denotado por $[L:K]$, es la dimension de L como espacio vectorial sobre K.

Por ejemplo, si pensamos en $\mathbb{C}$ y en $\mathbb{R}$, y teniendo en cuenta que todo número complejo se puede expresar en la forma $z = p + q \cdot i, p, q \in \mathbb{R}$, vemos que 1 y i forman una base para $\mathbb{C}$, como espacio vectorial sobre $\mathbb{R}$. Luego $[\mathbb{C}:\mathbb{R}] = 2$.

Teorema 2. Sea L una extensión finita de K, entonces $[L:K] = 1$ si y solo si $L = K$.

Demostración: Si $[L:K] = 1$ entonces cualquier elemento de L, digamos $1 \in L$ es una base, entonces $L = \{a \cdot 1 : a \in K\} = K$. El reciproco es obvio.

Teorema 3. (Teorema de la Torre de extensiones) Si E es un campo de extensión finita de K y L es un campo de extensión finita de E. Entonces L es un campo de extensión finita de K y además

$$[L:K] = [L:E][E:K]$$

Demostración: Sea $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ una base para E como espacio vectorial sobre K y sea $\{\beta_1, \beta_2, \dots, \beta_n\}$ una base para L como espacio vectorial sobre E. El teorema quedará probado si podemos mostrar que los mn elementos $\alpha_i\beta_j$ con $0 \leq i \leq n$ y $0 \leq j \leq m$ forman una base para L considerado como espacio vectorial sobre K.

Entonces, sea γ cualquier elemento de L. Como las β_j forman una base para L sobre E, tenemos

$$\gamma = \sum_{j=1}^{m} b_j\beta_j$$

Para $b_j \in E$. Como las α_i forman una base para E sobre K, tenemos

$$b_j = \sum_{i=1}^{n} a_{ij}\alpha_i$$

Para $a_{ij} \in K$. Entonces,

$$\gamma = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\alpha_i\right)\beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j)$$

De modo que los mn vectores $\alpha_i\beta_j$ generan L sobre K.

Falta mostrar que los mn elementos $\alpha_i\beta_j$ son independientes sobre K. Supongamos que $\sum_{i,j} c_{ij}(\alpha_i\beta_j) = 0$, con $c_{ij} \in K$. Entonces,

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{n} c_{ij}\alpha_i\right)\beta_j = 0$$

Y $\left(\sum_{i=1}^{n} c_{ij}\alpha_i\right) \in E$. Como los elementos β_j son independientes sobre E, debemos tener

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0$$

Para todas las j. Pero ahora las α_i son independientes sobre K, de modo que $\sum_{i=1}^{n} c_{ij}\alpha_i = 0$ implica que $c_{ij} = 0$ para todas las i y j. Así, las $\alpha_i\beta_j$ no solo generan L sobre K, sino que además, son independientes sobre K. Asi forman una base para L sobre K.

Teorema 4. (Teorema de la Torre de extensiones generalizado) Si K_i es un campo para $i = 1, \dots, r$ y K_{i+1} es una extensión finita de K_i, entonces K_r es una extensión finita de K_1 y

$$[K_r : K_1] = [K_r : K_{r-1}][K_{r-1} : K_{r-2}] \cdots [K_2 : K_1]$$

Demostración: La demostración de este teorema se basa en una simple extensión por inducción del Teorema 3.

§ 4 Extensiones Algebraicas.

En esta sección seguiremos estudiando algunas propiedades de los elementos algebraicos sobre un campo. En principio notemos que dado un campo K y un número finito de elementos algebraicos sobre K, digamos $\alpha_1, \dots \alpha_n$ pertenecientes a un campo L que contiene a K, el campo obtenido a partir de la adjunción de $\alpha_1, \dots \alpha_n$ a K, cumple la condición de que todo elemento α de L es algebraico sobre K. Este es un caso especial de campo de extensión que se define a continuación.

Definición 1. Una extensión L del campo K es una *extensión algebraica* si cada elemento α de L es algebraico sobre K.

Teorema 2. Supongamos que L es una extensión del campo K y sea α un elemento de L.

1. α es algebraico sobre K si y solo si $[K(\alpha): K]$ es finito.

2. Sea α algebraico sobre K. Si n es el grado del polinomio minimal de α sobre K, entonces $\{1, \alpha, \dots, \alpha^{n-1}\}$ forma una base de $K(\alpha)$ sobre K. Entonces $[K(\alpha): K] = n$.

Demostración: Primero supongamos que α es algebraico sobre K con polinomio minimal p, donde $\mathrm{Grad}(p) = n$. Necesitamos mostrar que $\{1, \alpha, \dots, \alpha^{n-1}\}$ forma una base de $K(\alpha)$ sobre K. Dado que $K(\alpha) = K[\alpha]$, cada elemento de $K(\alpha)$ es de la forma $g(\alpha)$ para algún $g \in K[x]$. Dividiendo g por p, tenemos:

$$g = qp + a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

donde $q \in K[x]$ y $a_0, \dots, a_{n-1} \in K$, y evaluando esta expresión en $x = \alpha$ queda:

$$g(\alpha) = a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} \tag{1.1}$$

puesto que $p(\alpha) = 0$. Entonces $\{1, \alpha, \dots, \alpha^{n-1}\}$ extienden $K(\alpha)$ sobre K.

Para mostrar la independencia lineal, supongamos que

$$0 = a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1}$$

donde $a_0, \dots, a_{n-1} \in K$. Entonces α es la raíz de $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in K[x]$. Pero dado que el polinomio minimal de α posee grado n, este debe ser el polinomio nulo. Esto es, $a_i = 0$ para todo i, y entonces la independencia lineal queda probada. Entonces $[K(\alpha): K] = n$.

Esto prueba la parte 2 y una implicación de 1. Queda entonces por considerar el caso cuando $[K(\alpha): K]$ es finito. Si suponemos que $[K(\alpha): K] = n$, entonces $K(\alpha)$ es un espacio vectorial n −dimensional sobre K. Esto implica que cualquier colleccion de $n + 1$ elementos de $K(\alpha)$ es linealmente dependiente. En particular, los elementos de $\{1, \alpha, \dots, \alpha^{n-1}, \alpha^n\}$ son linealmente dependientes sobre K. Por lo tanto existen $a_0, \dots, a_n \in K$, no todos cero, tales que

$$a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_n \alpha^n = 0$$

Luego, como en el párrafo anterior, sigue que α es una raíz del polinomio

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in K[x]$$

El cual es no nulo, puesto que a_i no son todos cero. Por lo tanto α es algebraico sobre K, y el teorema queda demostrado.

Corolario 3. Si L es un campo de extensión de K, y $\in L$ es algebraico sobre K y $\beta \in K(\alpha)$, entonces el grado del polinomio minimal de β sobre K divide al grado del polinomio minimal de α sobre K.

Demostración: Acordemos en denotar al grado del polinomio minimal de α sobre

K mediante el símbolo $\mathrm{Grad}(\alpha, K)$ y lo mismo para β. Por el Teorema 2, tenemos que $\mathrm{Grad}(\alpha, K) = [K(\alpha): K]$ y $\mathrm{Grad}(\beta, K) = [K(\beta): K]$. Además se cumple que $K \subset K(\beta) \subset K(\alpha)$, luego por el Teorema 3, sección 3, sigue que $[K(\beta): K]$ divide a $[K(\alpha): K]$.

El siguiente ejemplo muestra como funciona el teorema de la torre de extensiones o sus corolarios.

Por el Corolario 3, no hay elementos de $\mathbb{Q}(\sqrt{2})$ que sea un cero de $x^3 - 2$. Notemos que $\mathrm{Grad}(\sqrt{2}, \mathbb{Q}) = 2$ mientras que un cero de $x^3 - 2$ es de grado 3 sobre $\mathbb{Q}$, pero 3 no divide a 2.

Teorema 4. Sea L una extensión finita del campo K, entonces

1. L es una extensión algebraica del campo K.

2. Si $\alpha \in L$, entonces el grado del polinomio minimal de α sobre K divide a $[L: K]$.

Demostración: Un elemento $\alpha \in L$ nos da $K \subset K(\alpha) \subset L$, y por el Teorema de la Torre de Extensiones tenemos que $[K(\alpha): K]$ es finito y divide a $[L: K]$. Entonces 1 y 2 siguen inmediatamente del Teorema 2. En efecto, dado que L una extensión finita del campo K, entonces cualquier elemento de L es algebraico sobre K, luego L es una extensión algebraica de K. A su vez, $[K(\alpha): K]$ es el grado del polinomio minimal. Y como dijimos, ciertamente divide a $[L: K]$.

Teorema 5. Sea L una extensión del campo K. Entonces $[L: K]$ es finito si y solo si existen $\alpha_1, \dots, \alpha_m \in L$ tales que cada α_i es algebraico sobre K y $L = K(\alpha_1, \dots, \alpha_m)$.

Demostración: Primero supongamos que $[L: K]$ es finito. Sean $\alpha_1, \dots, \alpha_m \in L$ una base de L como un espacio vectorial sobre K. De este modo la dimensión de L como un espacio vectorial sobre K es m. Entonces:

$$L = \{a_1\alpha_1 + \cdots + a_m\alpha_m : a_1, \dots, a_m \in K\} \subset K(\alpha_1, \dots, \alpha_m) \subset L$$

lo cual prueba que $L = K(\alpha_1, \dots, \alpha_m)$. Cada α_i es algebraico sobre K por el Teorema 4.

Por el contrario supongamos que $L = K(\alpha_1, \dots, \alpha_m)$ donde cada α_i es algebraico sobre K. Sea $L_0 = K$, y $L_i = K(\alpha_1, \dots, \alpha_i)$ para $1 \leq i \leq m$. Entonces hemos construido la siguiente cadena de extensiones de campos:

$$K = L_0 \subset L_1 \subset \cdots \subset L_m = L \tag{1.2}$$

y el Corolario 5 de la sección 1, muestra que

$$L_i = K(\alpha_1, \dots, \alpha_{i-1}, \alpha_i) = K(\alpha_1, \dots, \alpha_{i-1})(\alpha_i) = L_{i-1}(\alpha_i)$$

para $1 \leq i \leq m$. Puesto que α_i es algebraico sobre K, también es algebraico sobre el campo mas grande:

$$K =\subset L_{i-1}$$

En virtud del Teorema 2, tenemos que

$$[L_i : L_{i-1}] = [L_{i-1}(\alpha_i) : L_{i-1}]$$

es finito.

Así que cada extensión sucesiva en (1.2) posee grado finito. Entonces por el Teorema Generalizado de la Torre de Extensiones implica que

$$[L : K] = [L_m : L_0] = [L_m : L_{m-1}] \cdots [L_1 : L_0]$$

es una cantidad finita. Esto demuestra el teorema.

Teorema 6. Sea L un campo de extensión de K. Si $\alpha, \beta \in L$ son algebraicos sobre K. Entonces $\alpha + \beta$ y $\alpha\beta$ son algebraicos sobre K.

Demostración: El teorema 5 implica que $K \subset K(\alpha, \beta)$ es una extensión finita y por

lo tanto es una extensión algebraica por el Teorema 4. Entonces cada elemento de $K(\alpha, \beta)$ es algebraica sobre K. Puesto que $\alpha + \beta, \alpha\beta \in K(\alpha, \beta)$, y de esta forma queda demostrado el teorema.

Teorema 7. Sea $K \subset E \subset L$. Si $\alpha \in L$ es algebraico sobre E y E es una extensión algebraica sobre K. Entonces α es algebraico sobre K.

Demostración: Sea α una raíz de $f = \beta_n x^n + \cdots + \beta_0 \in E[x]$, donde $\beta_n, \dots, \beta_0 \in E$ no son todos nulos. Por hipótesis, cada β_i es algebraico sobre K. Entonces $M = K(\beta_n, \dots, \beta_0)$ es una extensión finita de K por el Teorema 5. Lo que es más M esta construida por la base $\{\beta_n, \dots, \beta_0\}$, luego $f \in M[x]$ y además α es algebraico sobre sobre M. Lo cual implica que $M \subset M(\alpha)$ es una extensión finita, y por el Teorema de la Torre de Extensiones tenemos:

$$[M(\alpha): K] = [M(\alpha): M][M: K]$$

Es una cantidad finita, entonces $K \subset M(\alpha)$ es una extensión finita y por ende algebraica. Esto significa que cada elemento de $M(\alpha)$, incluido α es algebraico sobre K.

Del Teorema anterior siguen inmediatamente el siguiente resultado.

Corolario 8. Sean $K \subset E \subset L$, donde L es algebraica sobre E y E es algebraica sobre K. Entonces L es una extensión algebraica de K.

§ 5 Extensiones Normales y campos de descomposición.

En esta sección comenzaremos a ver algunas propiedades importantes de las extensiones de un campo. En principio, veremos algunas cuestiones relacionadas con los campos de descomposición, que son extensiones obtenidas a partir de la adjunción de las raíces de un cierto polinomio a un campo dado. Trataremos el concepto de normalidad de una extensión, el cual junto con el concepto de separabilidad de un campo juega un papel fundamental en la Teoría de Galois.

Definición 1. Sea el polinomio $f \in K[x]$ de grado n. Entonces una extensión L del campo K es un campo de descomposición de f sobre K si:

1. $f = c(x - \alpha_1) \cdots (x - \alpha_n)$, donde $c \in K$ y $\alpha_i \in L$ y

2. $L = K(\alpha_1 \cdots \alpha_n)$

La definición, en pocas palabras dice que un campo de descomposición es el menor campo en el que el polinomio f se descompone completamente en factores lineales.

Definición 2. Una extensión algebraica L del campo K es *normal* si cada polinomio irreducible en $K[x]$ que posee una raíz en L, se descompone completamente sobre L.

Veamos ahora algunos resultados concernientes a las extensiones normales y los campos de descomposición.

Teorema 3. Sea $f \in K[x]$ un polinomio de grado $n > 0$, y sea L un campo de descomposición para f sobre K. Entonces $[L: K] \leq n!$.

Demostración: Probaremos el teorema por inducción sobre n. Cuando $n = 1$, $f = ax + b$ tiene una raíz $-b/a$ siendo $a \neq 0$. Entonces $F = L$ y sigue fácilmente

$$[L: K] \leq 1!.$$

Ahora supongamos que f tiene grado $n > 1$, y sea $L = K(\alpha_1, \dots, \alpha_n)$ un campo de descomposición de f sobre K. Si escribimos $f = (x - \alpha_1)g$, entonces el Algoritmo de la División implica que $g \in K(\alpha_1)[x]$. Lo que es más, las raíces de g son precisamente $\alpha_2, \dots, \alpha_n$, asi que un campo de descomposicion de g sobre $K(\alpha_1)$ esta dado por

$$K(\alpha_1)(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_n) = L$$

Donde la primera igualdad sigue del Corolario 5, sección 1. Dado que $g \in F(\alpha_1)[x]$, tiene grado $n - 1$, por hipótesis inductiva, esto implica que

$$[L: K(\alpha_1)] \leq (n-1)!$$

Notemos que en estas circunstancias,

$$K \subset K(\alpha_1) \subset L$$

Luego aplicando el Teorema de la Torre de Extensiones tenemos que

$$[L: K] = [L: K(\alpha_1)][K(\alpha_1): K] \leq (n-1)!\,[K(\alpha_1): K]$$

Por otra parte sabemos que $[K(\alpha_1): K]$ es el grado del polinomio minimal de α_1 sobre K (Teorema 2, sección 4). Dado que $f(\alpha_1) = 0$, tenemos que $[K(\alpha_1): K] \leq n$, y de aquí sigue que

$$[L: K] \leq n!$$

Hemos demostrado entonces, el teorema.

Un polinomio $f \in K[x]$ puede tener distintos campos de descomposición. Por ejemplo, debido a los Teoremas 5 y 6 de la sección 2, tenemos que $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ son ambos campos de descomposición del polinomio $f = x^2 - 2$ sobre $\mathbb{Q}$. La clave esta en que si bien no son iguales, son isomorfos.

Con el fin de probar este resultado para polinomios en general, necesitamos probar algo más general. Supongamos que tenemos un isomorfismo de campos $\varphi: K_1 \to K_2$, y sea $f_1 \in K_1[x]$ un polinomio de grado $n > 0$. Aplicando φ a los coeficientes de f_1 obtenemos un polinomio $f_2 \in K_2[x]$. A su vez, sean L_1 y L_2 los campos de descomposición de f_1 sobre K_1 y f_2 sobre K_2 respectivamente. Aunque

los campos de descomposición L_1 y L_2 puedan ser construidos de diferentes formas, probaremos a continuación que los mismos son isomorfos.

Lema 4. Sean los campos K, K', y sea $\varphi: K \to K'$ un isomorfismo. Sea $\hat{\varphi}$ una función de $K[x]$ en $K'[x]$ definida como sigue:

$$\hat{\varphi}(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$$

Sea $f = a_0 + a_1x + \cdots + a_nx^n$ un polinomio irreducible de grado n con coeficientes en K , y sea $f^{'} = \hat{\varphi}(f) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$. Sea L una extensión de K que contiene una raíz α de f, y sea $L^{'}$ una extensión de $K^{'}$ que contiene una raíz $\alpha^{'}$ de $f^{'}$. Entonces existe un isomorfismo ψ de $K[\alpha]$ sobre $K[\alpha^{'}]$, una extensión de φ.

Demostración: Es rutina mostrar que $\hat{\varphi}$ es un isomorfismo de $K[x]$ en $K^{'}[x]$.

El campo $K[\alpha]$ esta constituido por todos los polinomios de la forma $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, con la suma habitual, y donde la multiplicación es efectuada utilizando la ecuación:

$$\alpha^n = -\frac{1}{a^n}(a_{n-1}\alpha^{n-1} + \cdots + a_0)$$

La función ψ esta definida por

$$\psi(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}) = \varphi(b_0) + \varphi(b_1)\alpha^{'} + \cdots + \varphi(b_{n-1})\left(\alpha^{'}\right)^{n-1}$$

En una notación mas compacta, tenemos que, para cada polinomio $u \in K[x]$ con $\mathrm{Grad}(u) < n$,

$$\psi\big(u(\alpha)\big) = \big(\hat{\varphi}(u)\big)\big(\alpha^{'}\big)$$

Es claro que ψ es biyectivo, y que extiende el isomorfismo $\varphi: K \to K^{'}$.

Sean $u, v \in K[x]$, donde $\mathrm{Grad}(u), \mathrm{Grad}(v) \leq n - 1$. Entonces es claro que

$$\psi\big(u(\alpha) + v(\alpha)\big) = \psi\big(u(\alpha)\big) + \psi\big(v(\alpha)\big)$$

La igualdad correspondiente para la multiplicación es un tanto más complicada. Multipliquemos $u(\alpha)$ y $v(\alpha)$ y usemos el polinomio minimal m para reducir nuestra respuesta, digamos a un polinomio $w(\alpha)$, donde $\mathrm{Grad}(w) \leq n - 1$. Utilizando el Algoritmo de la División para escribir $uv = qm + w$, donde $\mathrm{Grad}(w) < n$ por lo tanto

$$\psi\big(u(\alpha)v(\alpha)\big) = \psi\big(w(\alpha)\big) = \big(\hat{\varphi}(w)\big)\big(\alpha^{'}\big) \tag{1.3}$$

El isomorfismo $\hat{\varphi}$ asegura que el Algoritmo de la División en $K^{'}[x]$ da

$$\hat{\varphi}(u)\hat{\varphi}(v) = \hat{\varphi}(q)\hat{\varphi}(m) + \hat{\varphi}(w) \tag{1.4}$$

Por lo tanto

$$\psi\big(u(\alpha)\big)\psi\big(v(\alpha)\big) = \big(\hat{\varphi}(u)\big)\big(\alpha^{\prime}\big)\big(\hat{\varphi}(v)\big)\big(\alpha^{\prime}\big) = \big(\hat{\varphi}(u)\hat{\varphi}(v)\big)\big(\alpha^{\prime}\big)$$

Según (1.4) esto se puede escribir en la forma

$$\big(\hat{\varphi}(q)\hat{\varphi}(m) + \hat{\varphi}(w)\big)\big(\alpha^{\prime}\big) = \big(\hat{\varphi}(q)\big)\big(\alpha^{\prime}\big)\big(\hat{\varphi}(m)\big)\big(\alpha^{\prime}\big) + \big(\hat{\varphi}(w)\big)\big(\alpha^{\prime}\big) =$$

$$= \big(\hat{\varphi}(w)\big)\big(\alpha^{\prime}\big)$$

Esto último se debe a que $\big(\hat{\varphi}(m)\big)\big(\alpha^{\prime}\big) = 0$. Comparando con (1.3) llegamos al resultado buscado.

Teorema 5. Sean los campos Sean los campos $K, K^{\prime}$ y sea $\varphi: K \to K^{\prime}$ un isomorfismo, que se extiende a un isomorfismo $\hat{\varphi}: K[x] \to K^{\prime}[x]$. Sea $f \in K[x]$, y sean $L, L^{\prime}$ campos de descomposición de f sobre K y $\hat{\varphi}(f)$ sobre $K^{\prime}$, respectivamente. Entonces existe un isomorfismo $\varphi^{*}: L \to L^{\prime}$ que extiende φ.

Demostración: Supongamos que $\mathrm{Grad}(f)$ y que en $L[x]$ tenemos la que f se descompone en factores como sigue

$$f = \alpha(x - \alpha_1)(x - \alpha_1) \cdots (x - \alpha_1)$$

donde α, el coeficiente principal de f, esta en K, y $\alpha_1, \dots, \alpha_n \in L$. Podemos suponer que, para algún $m \in \{0,1,..,n\}$, las raíces $\alpha_1, \dots, \alpha_m$ no están en K, y

$\alpha_{m+1}, \dots, \alpha_n \in K$. Probaremos el teorema por inducción sobre m.

Si $m = 0$, entonces todas las raíces están en K, y entonces K mismo es un campo de descomposición para f. Por lo tanto, en $K^{\prime}[x]$, tenemos

$$\hat{\varphi}(f) = \varphi(\alpha)(x - \varphi(\alpha_1))(x - (\varphi\alpha_1)) \cdots (x - (\varphi\alpha_1))$$

Entonces $K^{\prime}$ es un campo de descomposición para $\hat{\varphi}(f)$, y $\varphi^{*} = \varphi$.

Supongamos ahora que $m > 0$. Nuestra hipótesis inductiva establece que, para cada campo E y cada polinomio $g \in E[x]$ con menos de m raíces fuera de E en una campo de descomposición L de g, cada isomorfismo de E puede extenderse a un isomorfismo de L.

Nuestra suposición de que $m > 0$ implica que los factores irreducibles de f en $K[x]$ no son todos lineales. Sea f_1 un factor no lineal e irreducible de f. Entonces $\hat{\varphi}(f_1)$ es un factor irreducible de $\varphi(f_1)$ en K'. Las raíces de f_1 en el campo de descomposición L estan incluidas entre $\alpha_1, \dots, \alpha_n$, y podemos suponer, sin perder generalidad, que α_1 es una raíz de f_1. Similarmente, la lista $\varphi(\alpha_1), \dots, \varphi(\alpha_n)$ de raíces de $\hat{\varphi}(f)$ incluye una raíz $\beta_1 = \varphi(\alpha_i)$ de $\hat{\varphi}(f_1)$. En este caso no se puede asumir que $i = 1$. Por el lema 4, existe un isomorfismo $\varphi': K(\alpha_1) \to K'(\beta_1)$ que extiende φ. Dado que ahora f posee menos de m raíces fuera de $K(\alpha_1)$, podemos usar nuestra hipótesis inductiva para asegurar la existencia de un isomorfismo $\varphi^*: L \to L'$, que extiende a $\varphi': K(\alpha_1) \to K'(\beta_1)$, y por lo tanto extiende $\varphi: K \to K'$.

Corolario 6. Si L_1 y L_2 son campos de descomposicion de $f \in K[x]$, entonces existe un isomorfismo $L_1 \simeq L_2$ que es la identidad en K.

Teorema 7. Sea L el campo de descomposición de $f \in K[x]$, y sea $g \in K[x]$ un polinomio irreducible. Si g tiene una raíz en L, entonces se descompone completamente sobre L.

Demostración: Podemos asumir que f y g son polinomios mónicos. Entonces $L = K(\alpha_1, \dots, \alpha_n)$, donde $f = (x - \alpha_1) \cdots (x - \alpha_n)$. Si $\beta \in L$ es una raíz de g, entonces g es el polinomio minimal de β dado que g es mónico e irreducible. Debemos probar entonces que todas las raíces de g estan en L.

El Teorema 7 de la sección 2, implica que $L = K(\alpha_1, \dots, \alpha_n) = K[\alpha_1, \dots, \alpha_n]$, asi que β es un polinomio en α_i, esto es, $\beta = h(\alpha_1, \dots, \alpha_n)$ para algún h en $K[x_1, \dots, x_n]$. Ahora consideremos el polinomio

$$s(x) = \prod_{\sigma \in S_n} \left(x - h\left(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}\right)\right) \in L[x]$$

Es claro que el polinomio $s(x)$ tiene todas sus raíces en L. Lo que es más, el factor correspondiente a $\sigma = e$ es $x - h(\alpha_1, \dots, \alpha_n) = x - \beta$, asi que β es una raíz de $s(x)$.

Si pudiéramos probar que $s(x)$ esta en $K[x]$, entonces $g|s$ seguiría inmediatamente puesto que g es el polinomio minimal de β. Como s se descompone completamente en L, esto implicaría que g tambien se descompone completamente sobre L.

Entonces es suficiente con mostrar que $s \in K[x]$. Notemos que el polinomio

$$s(x) = \prod_{\sigma \in S_n} \left(x - h\left(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}\right)\right)$$

Tiene coeficientes en $K[x_1, \dots, x_n]$, lo que es más, permutando $x_1, \dots, x_n$ se permutan los factores de s. Ahora, si expandimos la expresión de s tenemos la expresión

$$s(x) = \sum_{i=0}^{n!} p_i(x_1, \dots, x_n) x^i$$

Donde cada $p_i(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ es un polinomio simétrico[1] y según el Teorema Fundamental de los Polinomio Simétricos[2], p_i se puede escribir como un polinomio en los Polinomio Simétricos Elementales $\sigma_r(x_1, \dots, x_n)$ con coeficientes en K. Por otra parte $\sigma_r(\alpha_1, \dots, \alpha_n)$, salvo el signo, son los coeficientes de $f \in K[x]$.

1- Un Polinomio Simétrico es aquel que queda invariante ante cualquier permutación de sus variables.

2- El Teorema fundamental de los Polinomios Simétricos establece que un polinomio se puede expresar en término de los Polinomios Simétricos Elementales si y solo si es simétrico. Véase su demostración en la sección 2 del capítulo 4.

3- Véase la definición de los Polinomios Simétricos Elementales en la sección 1 del capítulo 4.

Notemos que los $\sigma_r(\alpha_1, \dots, \alpha_n)$ son precisamente los Polinomios Simétricos Elementales evaluados en $\alpha_1, \dots, \alpha_n$. Según lo dicho tenemos que los $\sigma_r(\alpha_1, \dots, \alpha_n) \in K$. Esto implica que cada $p_i(\alpha_1, \dots, \alpha_n) \in K$. Entonces concluimos que

$$s(x) = \sum_{i=0}^{n!} p_i(x_1, \dots, x_n)x^i \in K[x]$$

Luego, según la explicación dada mas arriba, sigue el teorema.

El siguiente resultado muestra la estrecha relación que existe entre los campos de descomposición y las extensiones normales. Veamos de qué se trata.

Teorema 8. Supongamos que L es una extensión de K. Entonces L es el campo de descomposición de algún polinomio $f \in K[x]$ si y solo si la extensión L es normal y finita.

Demostración: Supongamos que L es el campo de descomposición de $f \in K[x]$, entonces por el Teorema 3, L es una extensión finita, y por el Teorema 7, es normal. Por el contrario supongamos que la extensión L del campo K es normal y finita. Supongamos que $\alpha_1, \dots, \alpha_m \in L$ forman una base para L como espacio vectorial sobre K, entonces podemos escribir

$$L = K(\alpha_1, \dots, \alpha_m)$$

Por otra parte, dado que la extensión L es finita, entonces es algebraica y por ende cada $\alpha_i \in L$ es algebraico sobre K. Sea $p_i \in K[x]$ es polinomio minimal de α_i y sea

$$f = p_1 \cdots p_m$$

Mostraremos que L es el campo de descomposición de f sobre K.

Para probar esto, observemos que cada p_i se descompone completamente sobre L,

dado que la extensión L es normal y $p_i \in K[x]$ es irreducible con raíz $\alpha_i \in L$. Sigue que f se descompone completamente sobre L. Ahora sea $L' \subset L$ el campo generado por K y las raíces de f. Dado que las raíces de incluyen a $\alpha_1, \dots, \alpha_m$, tenemos que

$$L = K(\alpha_1, \dots, \alpha_m) \subset L' \subset L$$

Esto muestra que $L' = L$, asi que L es el campo de descomposición de f sobre K. Esto concluye la demostración del teorema.

Cuando una extensión de un campo no es normal, podemos recuperar la normalidad considerando extensiones más grandes.

Definición 9. Sea L una extensión finita del campo K. Un campo N que contiene a L se llama *clausura normal de* L *sobre* K si:

1. N es una extensión normal de K.

2. Si $L \subseteq M \subseteq N$ y M es una extensión normal de K, entonces $M = N$.

Evidentemente si L una extensión finita y normal del campo K, entonces L es su propia clausura normal.

Definición 10: Supongamos que tenemos un campo L y dos subcampos $K_1 \subset L$ y $K_2 \subset L$. Entonces *compuesto* de K_1 y K_2 en L es el menor subcampo de L que contiene a K_1 y K_2. Denotamos el compuesto por $K_1 \vee K_2$.

Puede probarse que este conjunto consiste en la intersección de todos los subcampos de L que contienen a K_1 y K_2. Además, si $K_1 = F(\alpha_1, \dots, \alpha_n) \subset L$ y $K_2 = F(\beta_1, \dots, \beta_n) \subset L$, el compuesto de K_1 y K_2 es

$$K_1 \vee K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n)$$

Teorema 11. Sea L una extensión finita de K y sea N la clausura normal de L. Entonces

$$N = L_1 \vee \cdots \vee L_k$$

Donde $L_1, \dots, L_k$ son campos que contienen a K, cada uno isomorfo a L.

Demostración: Dado que L una extensión finita de K, por el Teorema 5 de la sección 4, podemos suponer que $L = K(z_1, \dots, z_n)$, donde $\{z_1, \dots, z_n\}$ es una base para L sobre K cada z_i es algebraico sobre K, con polinomio minimal m_i, y N es el campo de descomposicion sobre K del polinomio $m = m_1 \cdot m_2 \cdots m_n$. Sea $i \in \{1, \dots, n\}$, y sea $z_i^{'}$ una raíz de m_i. Entonces para todas las elecciones de i y $z_i^{'}$, el campo

$$K\left(z_1, \dots, z_i^{'}, \dots, z_n\right) \tag{1.5}$$

es isomorfo a L. El campo N es generado sobre K por el conjunto $\{\alpha_1, \dots, \alpha_k\}$ de todas las raíces de todos los polinomios $m_1, \dots, m_n$, y por lo tanto por los campos de la forma (1.5).

§ 6 Extensiones separables.

Más adelante veremos que el estudio de las permutaciones de las raíces de un polinomio f sobre un anillo es la base de toda Teoría de Galois[1]. Por el momento, notemos que la permutación de las raíces se torna problemática si el polinomio en cuestión posee raíces repetidas. Principalmente porque distintas permutaciones podrían conducirnos a resultados iguales. Para evitar esto es conveniente entonces considerar campos de descomposición en los que las raíces del polinomio sean todas distintas, es claro que este es el caso más general posible. Veamos entonces que de esto trata el concepto de separabilidad.

1- Véase Œuvres Mathématiques d'Évariste Galois de Emile Picard.

Definición 1. Un polinomio no constante $f \in K[x]$ es *separable* si sus raíces en un campo de factorización son todas simples.

En otras palabras, f es separable si todas sus raíces son distintas.

Definición 2. Sea L una extensión algebraica del campo K.

1. $\alpha \in L$ es *separable* sobre K si su polinomio minimal sobre K es separable.

2. L es una *extensión separable* de K si cada $\alpha \in L$ es separable sobre K.

Definición 3. Sea $f = a_0 + a_1x + \cdots + a_nx^n$ un polinomio en $K[x]$. Se define la *derivada formal* Df, de f como el polinomio

$$Df = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

Aunque este sea un procedimiento formal y nada tenga que ver con el proceso de diferenciación del Análisis, se deducen igualmente las siguientes propiedades:

1. $D(kf) = kD(f)$

2. $D(f + g) = D(f) + D(g)$

3. $D(fg) = D(f)g + fD(g)$

4. $D[(x - \alpha)^n] = n(x - \alpha)^{n-1}$

Donde $f, g \in K[x]$ y $k \in K$.

A continuación veamos un resultado que relaciona las raíces del polinomio f con las de Df.

Teorema 4. Sea el polinomio $f \in K[x]$ y sea L el campo de descomposicion de f sobre K. Entonces las raíces de f en L son todas distintas si y solo si f y Df no poseen factores no constantes comunes.

Demostración: Supongamos que f posee una raíz α repetida en L, asi que $f = (x-\alpha)^r g$, donde $r \geq 2$. Entonces, por las propiedades 3 y 4, tenemos

$$Df = (x-\alpha)^r (Dg) + r(x-\alpha)^{r-1} g$$

De este modo vemos que f y Df tienen el factor $x - \alpha$ en común.

Por el contrario, supongamos que f no posee raíces repetidas, Entonces, para cada raiz α de f, tenemos $f = (x-\alpha)g$, donde $g(\alpha) \neq 0$. Entonces por la propiedad 3, sigue

$$Df = g + (x-\alpha)(Dg)$$

De este modo, $(Df)(\alpha) = g(\alpha) \neq 0$. Entonces, por el conocido Teorema del Resto, $(x-\alpha) \nmid Df$. Esto vale para cada factor de f en $L[x]$, asi que f y Df deben ser coprimos.

Teorema 5. Un polinomio no constante $f \in K[x]$ es separable si y solo si f es el producto de polinomios irreducibles, cada uno de los cuales es separable y nos hay dos de los cuales sean múltiplos uno del otro.

Demostración: Primero supongamos que f es separable. Si un factor de no posee raíces distintas en un campo de descomposición, evidentemente, lo mismo sucede con f. Entonces cada factor irreducible de f debe ser separable. Además, si la factorización de f en irreducibles incluye dos factores que sean múltiplos uno del otro, entonces el producto de estos factores será un divisor no separable de f. Entonces la factorización de f debe estar constituida por polinomios irreducibles y no debe haber dos de los cuales sean múltiplos uno del otro.

Por el contrario, sea $f = g_1, \dots, g_s$, donde $g_1, \dots, g_s$ son separables e irreducibles. Y no hay dos que sean múltiplos uno del otro. Entonces en el campo de factorización de f, cada g_i posee raíces distintas. Lo que es más, supongamos que

g_i y g_j comparten una raíz α para algún $i \neq j$. Dado que g_i y g_j son irreducibles, esto implicaría que cada uno fuese una constante y a la vez el polinomio minimal de α, lo cual es una contradicción. Por lo tanto f es separable.

Teorema 6. Sea $f \in K[x]$ un polinomio irreducible de grado $n > 1$.

1. Si K posee característica cero, entonces f es separable sobre el campo K.

2. Si K tiene característica finita p, entonces f es separable a menos que sea de la forma

$$b_0 + b_1 x^p + b_2 x^{2p} + \cdots + b_m x^{mp}$$

Demostración: Sea $f = a_0 + a_1 x + \cdots + a_n x^n$, con $\mathrm{Grad}(f) = n > 1$, y supongamos que f no es separable. Entonces f y Df poseen un factor común d de grado, por lo menos 1. Dado que f es irreducible, el factor común d debe ser un múltiplo constante de f, y este no puede dividir a Df, a menos que

$$Df = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

sea el polinomio nulo. Entonces,

$$a_1 = 2a_2 = \cdots = n a_n = 0$$

Si K posee característica cero, esto implica que $f$es la constante a_0, y entonces llegamos a una contradicción. Entonces f debe ser separable.

Supongamos ahora que la característica de K es p. Entonces $r a_r = 0$ implica que $a_r = 0$ si y solo si $p \nmid r$. Por ende, los únicos términos no nulos de f son de la forma $a_{kp} x^{kp}$, para $k = 0,1,2 \ldots$. Escribiendo a_{kp} como b_k llegamos a la conclusión requerida.

Con los resultados anteriores podemos recopilar la siguiente información en cuanto a la separabilidad y los campos de característica cero. En principio que todo polinomio irreducible es separable. Por otra parte, dado que las separabilidad de un campo implica la existencia de un polinomio para cada elemento del mismo,

sigue de inmediato que toda extensión finita es separable, lo que es más, toda extensión algebraica es separable. Y por último que todo polinomio no constante es separable si y solo si es el producto de polinomios irreducibles y no hay dos de ellos que sean múltiplos el uno del otro. Juntemos toda esta información en el siguiente corolario.

Corolario 7. Si K es un campo de característica cero, entonces:

1. Todo polinomio irreducible en $K[x]$ es separable.

2. Toda extensión algebraica de K es separable.

3. Un polinomio no constante $f \in K[x]$ es separable si y solo si f es el producto de polinomios irreducibles, y no hay dos que sean múltiplos uno del otro.

Demostración: La parte 1 sigue inmediatamente del Teorema 6, y esto implica la parte 2 por definición de extensión separable. Finalmente 3 sigue de la parte 1 y el Teorema 6.

En relación al Corolario 7, veamos el concepto de campo perfecto.

Definición 8. Un campo K es perfecto si toda extensión finita es separable.

Corolario 9. Todo campo de característica cero es perfecto.

Demostración: Por el Teorema 4, de la sección 4, sabemos que toda extensión finita es algebraica. Entonces sigue del Corolario 7 toda extensión finita es separable. Luego, en base a la Definición 8 obtenemos el resultado buscado.

Del Corolario 9, sigue que el campo de los Números Complejos es perfecto, por lo tanto la separabilidad en él no es un problema. Gran parte de los teoremas importantes de la Teoría de Galois que veremos en el capítulo 3 exigen que los campos cumplan con las condiciones de normalidad y separabilidad, por este

motivo es necesario tener en cuenta algunos resultados de la teoría de las extensiones separables al trabajar con campos arbitrarios. Dados que los trabajos originales de Evariste Galois se realizaron en base al campo de los Complejos, la separabilidad no era necesaria. Esto último ocurre en algunos textos que estudian la Teoría de Galois referida únicamente al campo de los Complejos.

Teorema 10. Sea L una extensión finita y separable de K y sea E un campo tal que $K \subset E \subset L$. Entonces L una extensión separable de E.

Demostración: Sea $\alpha \in L$ y sea m_K y m_E el polinomio minimal de α sobre K y sobre E respectivamente. Supongamos que m_K es separable. Usando el Algoritmo de la División en $E[x]$ tenemos que

$$m_K = qm_E + r$$

siendo $\mathrm{Grad(r)} < Grad(m_E)$. Sigue entonces que:

$$r(\alpha) = m_K(\alpha) - q(\alpha)m_E(\alpha) = 0 - 0 = 0$$

Esto contradice la minimalidad del polinomio m_E, a menos que sea $r = 0$. En este caso, debe ser si o si, $m_K = qm_E$ en el anillo $E[x]$.

Si m_E no es separable, entonces existe un polinomio g que divide a m_E y a Dm_E. Puesto que $Dm_K = qDm_E + m_E Dq$, sigue que g divide a m_K y a Dm_K. Pero esto puede suceder únicamente si m_K tiene una raíz repetida en un campo de descomposición, y esto contradice el hecho de que m_K es separable. Por lo tanto, m_E es separable. Luego L una extensión separable de E.

Capítulo 2

Grupos Resolubles. El Grupo Simétrico S_n.

En este capítulo recopilaremos algunos resultados de la Teoría de Grupos necesarios para alcanzar nuestro objetivo final. En primer lugar daremos la definición de grupo resoluble y analizaremos bajo que condiciones el grupo simétrico es resoluble. Como veremos esto último tiene gran importancia en la Teoría de Galois dado que en ciertos casos, este último es isomorfo al grupo simétrico.

§ 1 Resultados necesarios de la teoría de grupos.

Definición 1. Sea G un grupo y $g, h \in G$. Definimos el conjugado de h por g como el elemento $h^g = g^{-1}hg \in G$. Definimos el homomorfismo $\alpha_g: G \to G$ dado por $\alpha_g(h) = g^{-1}hg$.

Es fácil ver que α_g es un automorfismo de G. Por otra parte es evidente que $h^g = h$ si y solo si $hg = gh$.

Si $A \subset G$, escribiremos $A^g = \alpha_g(A) = \{a^g : a \in A\}$.

Es fácil probar que $gH = Hg$ equivale a $H = g^{-1}Hg = H^g$, Esto es cuando H es un subgrupo normal de G.

Teorema 2. Sea G un grupo y $N \lhd G$.

1. Si $N \leq H \leq G$, entonces $H/N \leq G/N$.

2. Si $K \leq G/N$, entonces existe un subgrupo H de G tal que $N \leq H \leq G$ y $K = H/N$.

3. Si $N \leq H \leq G$, entonces $H/N \lhd G/N$ si y solo si $H \lhd G$

4. Las correspondencias descriptas en los apartador 1 y 2 determinan una biyección entre los subgrupos de G/N y los subgrupos de G que contienen a N. Los subgrupos normales de G se corresponden con los subgrupos normales de G/N.

Demostración: 1 es inmediato. Los elementos de H/N son las clases hN con $h \in H$ y los de G/N son las clases gN con $g \in G$. La operación es la misma.

2. Consideremos el epimorfismo[1] $\pi: G \to G/N$ dado por $\pi(g) = gN$. Dado un subconjunto K de G/N, definimos el conjunto $H = \pi^{-1}(K) = \{g \in G : \pi(g) \in K\}$. Es fácil probar que $\pi^{-1}(K) \leq G$. De este modo $N = \pi^{-1}(\{eN\})$ y claramente $N \leq H$. Asi, $H/N = \{hN : h \in H\} = \pi(H) = \pi(\pi^{-1}(K)) = K$.

3. Si $H/N \lhd G/N$, entonces al conjugar un elemento de $h \in H$ por un elemento $g \in G$ se cumple que:

$$h^g N = g^{-1}hgN = (g^{-1}N)(hN)(gN) = (gN)^{-1}(hN)(gN) = (hN)^{gN} \in H/N$$

Luego $h^g \in H$ y asi $H \lhd G$. El reciproco es análogo.

1- Un epimorfismo es un homomorfismo sobreyectivo.

4. Si $H/N = H^{\prime}/N$, entonces $H = \pi^{-1}(H/N) = \pi^{-1}\left(H^{\prime}/N\right) = H^{\prime}$, luego la correspondencia es inyectiva y por 2 es sobreyectiva.

Teorema 3. (Primer Teorema del Homomorfismo). Sean G y $G^{\prime}$ dos grupos y sea φ un homomorfismo de G sobre $G^{\prime}$ con núcleo $K = \mathrm{Ker}(\varphi)$. Entonces

$$G^{\prime} \simeq \frac{G}{\mathrm{K}}$$

y el isomorfismo entre ellos es efectuado por la aplicación

$$\psi: \frac{G}{\mathrm{K}} \to G^{\prime}$$

definida por $\psi(aK) = \varphi(a)$.

Demostración: Definamos $\psi: G/K \to G^{\prime}$ por $\psi(aK) = \varphi(a)$ para $a \in G$. Demostremos ahora que ψ está bien definida, es decir que si $aK = bK$, entonces $\psi(aK) = \psi(bK)$. Es claro que según la definición de ψ, esto se reduce a demostrar que si $aK = bK$ entonces debe ser $\varphi(a) = \varphi(b)$. Pero si $aK = bK$, entonces $a = bk$ para algún $k \in K$, por consiguiente $\varphi(a) = \varphi(bk) = \varphi(b)\varphi(k)$ sin embargo, dado que $k \in K$, el Kernel de φ, sigue que $\varphi(k) = e^{\prime}$, el elemento identidad de $G^{\prime}$, de este modo resulta que $\varphi(a) = \varphi(b)$. Esto muestra que la aplicación ψ está bien definida.

En virtud de que φ es sobreyectiva sobre $G^{\prime}$, dado un elemento $x \in G^{\prime}$, sigue que $x = \varphi(a)$ para algún $a \in G$, así que $x = \varphi(a) = \psi(aK)$. Esto demuestra que ψ aplica G/K sobre $G^{\prime}$, en otras palabras, ψ es sobreyectiva.

Supongamos ahora que $\psi(aK) = \psi(bK)$; entonces $\varphi(a) = \psi(aK) = \psi(bK) = \varphi(b)$, por lo tanto $e^{\prime} = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$. De este modo resulta que ab^{-1} esta en el Kernel de φ, entonces $ab^{-1} \in K = \mathrm{Ker}(\varphi)$. Esto implica que $aK = bK$. De esta manera se vemos que ψ es inyectiva.

Queda por demostrar que ψ es un homomorfismo de G/K sobre G'. Teniendo en cuenta que φ es un homomorfismo y que $(aK)(bK) = (ab)K$, tenemos que $\psi[(aK)(bK)] = \psi[(ab)K] = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aK)\psi(bK)$. Hemos

probado entonces que ψ es un isomorfismo de G/K sobre G', de este modo concluye la demostración.

Notemos que en el enunciado del teorema anterior se puede considerar un homomorfismo φ cualquiera, no necesariamente sobreyectivo, del grupo G en otro grupo H; y luego considerar a G' como la imagen de φ.

Teorema 4 (de Cauchy para grupos abelianos). Si G es un grupo abeliano finito de orden $|G|$ y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p.

Demostración: Se procede por inducción en $|G|$. Si $|G| = 1$, no existe tal p y el teorema necesariamente es cierto por vacuidad. Sin embargo para evitar esta situación podemos suponer que $|G| = 2$ y en este caso tenemos necesariamente $p = 2$, y el teorema sigue siendo cierto.

Supongamos ahora que existe un subgrupo distinto N de G, con $\{e\} \neq N \neq G$, puesto que $|N| < |G|$, si p divide a $|N|$, por la hipótesis inductiva, debe existir un elemento de orden p en N y por consiguiente en G, entonces en este caso el teorema es válido. Supongamos ahora que p no divide a $|N|$. Puesto que G es abeliano, todo subgrupo es normal, asi que se puede formar el cociente G/N. Debido a que p divide a $|G|$ y p no divide a $|N|$ y a que $|G/N| = |G|/|N|$, se tiene que p divide a $|G/N|$. El grupo G/N es abeliano, puesto que G lo es, y puesto que $\{e\} \neq N$, $|N| > 1$, así que $|G/N| = |G|/|N| < |G|$. Por consiguiente, otra vez por inducción, existe un elemento en G/N de orden p. Esto se traduce en: existe $a \in G$ tal que $[aN]^p = [eN]$, pero $[aN] \neq [eN]$. Puesto que $[eN] = [aN]^p = [a^pN]$, sigue que $a^p \in N$, con $a \notin N$. Así que si $m = |N|$, entonces, puesto que $a^p \in N$, sigue que $(a^p)^m = e$. De modo que $(a^m)^p = e$. Si se pudiese demostrar que

$b = a^m \neq e$, entonces b sería el elemento requerido de orden p en G. Pero si $a^m = e$, entonces $[a^m N] = [eN]$, y puesto que $[aN]$ tiene orden p, p divide a m. Pero por hipótesis p no divide a m. De este modo concluye la demostración si G posee un subgrupo no trivial.

Pero si G no posee subgrupos no triviales, debe ser cíclico de orden primo p, debido a que por hipótesis p divide a $|G|$, y en este caso debe ser $p = |G|$. Pero entonces cualquier elemento $a \neq e \in G$ satisface $a^p = e$ y por ende es de orden p. Esto completa la demostración del teorema.

§ 2 Grupos resolubles.

Definición 1. Un grupo finito G es resoluble si existe una secuencia de subgrupos

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$$

Tal que para todo $i, 0 \leq i \leq m-1$, G_i es un subgrupo normal de G_{i+1} y además $|G_{i+1}|/|G_i|$ es primo.

Puesto que G_i es normal en G_{i+1}, el hecho de que $|G_{i+1}|/|G_i|$ es primo se puede reemplazar diciendo que G_{i+1}/G_i sea un grupo cíclico de orden primo[1].

Con los resultados de la sección anterior, estamos en condiciones de demostrar algunas propiedades de los grupos resolubles.

Teorema 2. Sea G un grupo resoluble finito, entonces todo subgrupo H de G es resoluble.

1- Véase Álgebra Abstracta de Herstein. Teorema 2.6.3, p 80.

Demostración: Si G es un grupo resoluble entonces existe una secuencia de subgrupos de G

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$$

que cumplen las condiciones de la definición 1. Sea H un subgrupo de G. Sean los conjuntos $H_{i+1} = G_{i+1} \cap H$. Notemos que

$$H_m = G_m \cap H = G \cap H = H$$

$$H_0 = G_0 \cap H = \{e\} \cap H = \{e\}$$

Entonces consideremos el homomorfismo de grupo

$$\pi: H_{i+1} \to G_{i+1}/G_i$$

que envía cada $h \in H_{i+1}$ a la clase lateral $hG_i \in G_{i+1}/G_i$. Observemos que $h \in H_{i+1}$ esta en el $Ker(\pi)$ si y solo si $hG_i = G_i$. Pero esto ocurre si y solo si

$$h \in H_{i+1} \cap G_i = (G_{i+1} \cap H) \cap G_i = G_i \cap H = H_i$$

Esto muestra que $Ker(\pi) = H_i$. Y teniendo en cuenta que el Kernel de un homomorfismo de grupos de A en B es un subgrupo normal del grupo A, tenemos que H_i es un subgrupo normal de H_{i+1}. Luego por el Teorema Fundamental del Homomorfismo de Grupos, hallamos el isomorfismo

$$H_{i+1}/H_i = H_{i+1}/Ker(\pi) \simeq Im(\pi) \subset G_{i+1}/G_i$$

Como G_{i+1}/G_i es cíclico de orden primo, no queda otra que H_{i+1}/H_i sea trivial o isomorfo a G_{i+1}/G_i. Esto es, $H_{i+1} = H_i$ ó $|H_{i+1}|/|H_i|$ primo. De esta forma, descartando los casos en que ocurra la primera posibilidad, hallamos la secuencia de grupos

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_i \subset H_{i+1} \subset \cdots \subset H_m = H$$

con las propiedades indicadas.

Teorema 3. Sea G un grupo finito y H un subgrupo normal de G. Entonces G es resoluble si y solo si H y G/H son resolubles.

Demostración: Primero supongamos que supongamos que G es resoluble. Por el teorema anterior, H es resoluble. Para mostrar que G/H es resoluble suponga que G_i son los subgrupos de G, de la Definición 1 de grupo resoluble, y sea

$$\pi: G \to G/H$$

El homomorfismo de grupo que asocia a cada $g \in G$ con la clase lateral gG. Entonces sea $\tilde{G}_i = \pi(G_i)$. Esto es, $\tilde{G}_i$ es la imagen de G_i en G/H.

Notemos que

$$\tilde{G}_0 = \pi(G_0) = \pi(\{e\}) = \{eH\} \quad \text{y} \quad \tilde{G}_m = \pi(G_m) = \pi(G) = G/H$$

Ahora consideremos el homomorfismo

$$\vartheta: G_{i+1}/G_i \to \tilde{G}_{i+1}/\tilde{G}_i$$

definido por

$$\vartheta(gG_i) = \pi(g)\tilde{G}_i$$

Evidentemente ϑ es sobreyectivo. Esto se sigue dado que π lo es. De este modo vemos que:

$$Im(G_{i+1}/G_i) = \tilde{G}_{i+1}/\tilde{G}_i$$

Pero dado que G_{i+1}/G_i es cíclico de orden primo, $\tilde{G}_{i+1}/\tilde{G}_i$ debe ser trivial o de orden primo. Es decir: $\tilde{G}_{i+1} = \tilde{G}_i$ o $\left|\tilde{G}_{i+1}\right|/\left|\tilde{G}_i\right|$ es primo. Además, dado que $G_i \lhd G_{i+1}$, por el Teorema 2 de la sección 1 sigue que $\tilde{G}_i \lhd \tilde{G}_{i+1}$.

Como en la demostración del teorema anterior, descartando los duplicados entre los subgrupos, hallamos la secuencia

$$\{eH\} = \tilde{G}_0 \subset \tilde{G}_1 \subset \cdots \subset \tilde{G}_i \subset \tilde{G}_{i+1} \subset \cdots \subset \tilde{G}_m = G/H$$

Luego G/H es resoluble.

Supongamos ahora que H y G/H son resolubles. Entonces existe la secuencia se subgrupos de H que cumplen con las condiciones de la Definición 1.

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_i \subset H_{i+1} \subset \cdots \subset H_l = H$$

De la misma forma, sean

$$\{eH\} = N_0/H \subset N_1/H \subset \cdots \subset N_i/H \subset N_{i+1}/H \subset \cdots \subset N_m/H = G/H$$

Una secuencia de subgrupos de G/H que cumplen con las condiciones especificadas en la definición 1.

Según el Teorema 2 de la sección 1, la secuencia de subgrupos de G que muestran que este es resoluble es:

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_i \subset H_{i+1} \subset \cdots \subset H_l = H = N_0 \subset N_1 \subset \cdots \subset N_i \subset N_{i+1} \subset \cdots \subset N_m = G$$

De esta forma el teorema queda demostrado.

A continuación, Utilizamos los resultados de los teoremas anteriores para mostrar que los grupos abelianos finitos son resolubles.

Teorema 4. Todo grupo abeliano finito G es resoluble.

Demostración. Probaremos el teorema por inducción sobre $n = |G|$. El caso $n = 1$ es trivial. Asumamos ahora que G es un grupo abeliano finito de orden $n > 1$ y que el resultado es válido para todo grupo abeliano finito de orden menor que n.

Sea p un divisor primo de $|G|$. Si $p = |G|$, entonces G es cíclico de orden primo y por ende resoluble. Si $p < |G|$, entonces por el Teorema de Cauchy para Grupos Abelianos, podemos encontrar un elemento $g \in G$ de orden p. Ahora sea H el subgrupo de G generado por g. Entonces H es normal, dado que G es abeliano y $|H| = p < G$. Sigue que los órdenes de H y de G/H son estrictamente menores que $|G| = n$. Por lo tanto, por hipótesis inductiva, H y de G/H son resolubles. Luego, por el Teorema 3 sigue que G es resoluble.

§ 3 El grupo simétrico S_n.

En esta sección estudiaremos algunas propiedades referidas al grupo simétrico S_n que serán claves en lo que respecta a nuestro objetivo final. El resultado más importante que demostraremos en este segmento de trabajo tiene que ver con insolubilidad S_n para $n \geq 5$. Sin embargo, para llegar a tal punto necesitamos algunos resultados previos.

Teorema 1. Sea el conjunto $N = \{1,2,\dots,n\}$ y sea S_n el conjunto de todas las permutaciones de N. Entonces S_n es un grupo bajo la multiplicación de permutaciones.

Demostración: Sean σ_1 y σ_2 dos permutaciones de N. Por definición ambas son funciones biyectivas de N en N. Es claro que $\sigma_1 \cdot \sigma_2$ esta definida de N en N, por lo que solamente debemos probar que $\sigma_1 \cdot \sigma_2$ es biyectiva, es decir, debemos probar que $\sigma_1 \cdot \sigma_2$ es también una permutación de N. Para esto veamos que si

$$(a_1)[\sigma_1 \cdot \sigma_2] = (a_2)[\sigma_1 \cdot \sigma_2] \Longrightarrow \big((a_1)\sigma_1\big)\sigma_2 = \big((a_2)\sigma_1\big)\sigma_2$$

Dado que σ_1 es biyectiva, $\big((a_1)\sigma_1\big)\sigma_2 = \big((a_2)\sigma_1\big)\sigma_2$ implica que $(a_1)\,\sigma_1 = (a_2)\,\sigma_1$ y ahora dado que σ_2 es biyectiva, $(a_1)\,\sigma_1 = (a_2)\,\sigma_1$ implica que $a_1 = a_2$. Esto muestra que $\sigma_1 \cdot \sigma_2$ es inyectiva. Por otra dado que parte, para todo $a \in N, \exists a' \in N: (a')\sigma_2 = a$. A su vez, para $a' \in N$, $\exists a'' \in N: (a'')\sigma_1 = a'$. Por lo tanto

$$(a')\sigma_2 = \big((a'')\sigma_1\big)\sigma_2 = (a'')[\sigma_1 \cdot \sigma_2] = a$$

Luego $\sigma_1 \cdot \sigma_2$ es sobreyectiva y por lo tanto $\sigma_1 \cdot \sigma_2$ es biyectiva, así que $\sigma_1 \cdot \sigma_2$ es una permutación de N, esto es $\sigma_1 \cdot \sigma_2 \in S_n$.

Probemos ahora que se cumple la asociatividad, para esto, sean $\sigma_1, \sigma_2, \sigma_3 \in S_n$ y $a \in N$. Debemos probar que:

$$(a)[(\sigma_1 \cdot \sigma_2) \cdot \sigma_3] = (a)[\sigma_1 \cdot (\sigma_2 \cdot \sigma_3)]$$

En efecto,

$$(a)[(\sigma_1 \cdot \sigma_2) \cdot \sigma_3] = \big((a)[\sigma_1 \cdot \sigma_2]\big)(\sigma_3) = \big(\big((a)\sigma_1\big)\sigma_2\big)\sigma_2 = ((a)\sigma_1)[\sigma_2 \cdot \sigma_3] =$$

$$= (a)[\sigma_1 \cdot (\sigma_2 \cdot \sigma_3)]$$

Vemos entonces que se cumple la asociatividad.

La permutación Id tal que $(a)Id = a$ para todo $a \in N$ obviamente actúa como elemento identidad, por lo que existe inverso.

Por último, para una permutación $\sigma \in S_n$, definamos σ^{-1} como la permutación que invierte la dirección de la transformación σ, esto es $(a)\ \sigma^{-1}$será el elemento $a^{\acute{}}$ se S_n tal que $\big(a^{\acute{}}\big)\sigma = a$. La existencia de de exactamente un elemento $a^{\acute{}}$ con esa característica se debe a que, como función, σ es biyectiva. Es claro que

$$(a)Id = a = \big(a^{\acute{}}\big)\sigma = \big((a)\sigma^{-1}\big)\sigma = (a)(\sigma\sigma^{-1})$$

Y tambien que

$$\big(a^{\acute{}}\big)Id = a^{\acute{}} = (a)\sigma^{-1} = \big[\big(a^{\acute{}}\big)\sigma\big]\sigma^{-1} = \big(a^{\acute{}}\big)(\sigma^{-1}\sigma)$$

De modo que $\sigma\sigma^{-1}$ y $\sigma^{-1}\sigma$ son ambas permutaciones de Id, luego se satisface el axioma de la existencia de inverso.

De todo esto concluimos la propiedad requerida. Hemos finalizado la demostración.

Definición 2. Sea el conjunto $N = \{1,2, \dots, n\}$, entonces el grupo de todas las permutaciones de N es el grupo simétrico de "n" elementos y se denota por S_n.

Definición 3. Una permutación σ de de un conjunto A se llama *ciclo de longitud* n, denotado por $\sigma = (a_1, a_2, \dots, a_n)$, si existen $a_1, a_2, \dots, a_n \in A$ tales que

$$(a_1)\sigma = a_2, \qquad (a_2)\sigma = a_3\ , \dots , (a_{n-1})\sigma = a_n, \quad (a_n)\sigma = a_1$$

y $(a)\sigma = a$ para todo $a \notin \{a_1, a_2, \dots, a_n\}$. Un ciclo de longitud 2 se denomina *transposición.* Dos ciclos son ajenos (o disjuntos) si no poseen elementos el común.

Por ejemplo, $(1,3,5)$ y $(4,2,6,7)$ son ciclos ajenos de S_7.

Teorema 4. Toda permutación $\sigma \in S_n$ se puede expresar como un producto de ciclos ajenos. El orden de σ es el mínimo común múltiplo de las longitudes de los ciclos.

Demostración: Sea x_1 un elemento arbitrario de $\{1, \dots, n\}$. Si $(x_1)\sigma = x_1$, entonces (x_1) es a si mismo un ciclo, de otro modo escribamos $(x_1)\sigma = x_2$. Continuamos con la secuencia:

$$x_1, \qquad x_2 = (x_1)\sigma, \qquad x_3 = (x_2)\sigma, \dots$$

y dado que el conjunto $\{1, \dots, n\}$ es finito, eventualmente debe haber una repetición: supongamos que la primera repetición es $(x_k)\sigma = x_j$, con $k > j$. Si $j \neq 1$ tenemos una contradicción dado que $(x_k)\sigma = (x_{j-1})\sigma = x_j$; luego $j = 1$, y la restricción de σ a $\{x_1, \dots, x_k\}$ es el ciclo $(x_1, \dots, x_k)$.

Entonces al elegir un y_1 que no este en $\{x_1, \dots, x_k\}$ y repitiendo este procedimiento otra vez, obtenemos el ciclo $(y_1, \dots, y_l)$. Eventualmente el procedimiento debe terminar y así obtenemos la descomposición de σ en ciclos ajenos.

Es claro que el orden de un ciclo coincide con su longitud, por ejemplo si $\sigma = (1,3,4)$ en S_4, tenemos entonces que $(1)\sigma = 3, (1)\sigma^2 = (3)\sigma = 4, (1)\sigma^3 = (4)\sigma = 1$, es lo mismo empezando con otro elemento, y así se cumple lo que afirmamos. Por otra parte también es fácil ver que dado dos ciclos disjuntos, estos conmutan el uno con el otro. Por lo tanto, si σ es el producto $\sigma_1 \cdots \sigma_r$ de ciclos ajenos de longitudes $\lambda_1, \dots, \lambda_r$, entonces para cada $m \geq 1$,

$$\sigma^m = \sigma_1^m \cdots \sigma_r^m$$

Y esto es igual a la permutación idéntica si y solo si m es un múltiplo de cada uno de los enteros $\lambda_1, \dots, \lambda_r$.

Del teorema 4 se deduce fácilmente el siguiente corolario:

Corolario 5. Toda permutación $\sigma \in S_n$ se puede expresar como un producto de transposiciones.

Demostración: En vista del Teorema 4, basta con mostrar que un ciclo es el producto de transposiciones. Un simple cálculo directo muestra que

$$(a_1, \dots, a_k) = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_k)$$

A continuación veremos que las permutaciones se pueden clasificar en dos categorías: *pares* e *impares*. Si bien existen varias formas de definir cada una, tal vez sería conveniente aquí considerar el polinomio

$$\Delta(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3) \cdots (x_{n-1} - x_n)$$

$$(x_2 - x_3) \cdots (x_2 - x_n)$$

$$\dots\dots$$

$$(x_{n-1} - x_n)$$

en n indeterminadas. Para cada permutación $\sigma \in S_n$, podemos definir

$$\sigma(\Delta) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Los factores en $\sigma(\Delta)$ son los mismos que los factores en Δ, excepto que están en diferente orden, y alguno de ellos puede estar invertido. Por ejemplo, si σ es la transposición $(1,2)$, el factor $x_1 - x_2$ se convierte en $x_2 - x_1$, y los otros factores permanecen inalterados, entonces en este caso tenemos que $\sigma(\Delta) = -\Delta$. Por otro lado si

$$\sigma = (1,2,3) = (1,2)(1,3)$$

Dos factores, digamos, $(x_1 - x_2)$ y $(x_1 - x_3)$, cambian de signo, y entonces $\sigma(\Delta) = \Delta$. Una permutación σ es *par* o *impar* si $\sigma(\Delta) = \Delta$ o $\sigma(\Delta) = -\Delta$, respectivamente. Vemos también que σ es par (impar) si y solo si se puede

expresar como la composición de un número de transposiciones pares (impares). De esto sigue que:

$$par\ o\ par = par, \quad impar\ o\ impar = impar$$

$$par\ o\ impar = impar\ o\ par = impar,$$

Como consecuencia de esto, el conjunto de todas las permutaciones pares es un subgrupo, de hecho un subgrupo normal de S_n, llamado *Grupo Alternante* y se denota con el símbolo A_n.[1]

Notemos además que según la forma en que definimos las permutaciones en par o impar, se tiene que dada una permutación $\sigma \in S_n$, σ es par o bien, es impar.

Definamos ahora la función $\theta: S_n \to E = \{-1,1\}$ del siguiente modo.

$$\theta(\sigma) = \begin{cases} 1 \text{ si } \sigma \text{ es par} \\ -1 \text{si } \sigma \text{ es impar} \end{cases}$$

Según las reglas precedentes relativas a los productos tenemos que $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$, de manera que θ es un homomorfismo de S_n sobre el grupo $E = \{-1,1\}$ de orden 2 respecto a la multiplicación. En virtud de la propia definición de A_n, se ve que $\mathrm{Ker}(\theta) = A_n$. Así que por el Primer Teorema del Homomorfismo,

$$E \simeq S_n/A_n$$

De esta manera $2 = |E| = |S_n/A_n| = |S_n|/|A_n|$, si $n > 1$. Esto da por resultado que

$$|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$$

Por lo tanto llegamos a que S_n contiene $1/2\,n!$ permutaciones pares y $1/2\,n!$ permutaciones impares. Este planteo muestra evidentemente que el índice de A_n es 2.[2]

1- Véase Álgebra Abstracta de Herstein. Teorema 3.3.3, p 122.

2- Dado el grupo G y un subgrupo H del mismo, el número de clases laterales izquierdas (derechas) de H en G es el índice de H en G.

Por otra parte, en cuanto a la afirmación hecha antes en cuanto a la normalidad del grupo alternante A_n en S_n, se demuestra sin dificultad que todo subgrupo H de un grupo G de índice 2 es un subgrupo normal.

Más adelante veremos la importancia del grupo alternante A_n cuando $n \geq 5$. Antes de esto pongamos nuestra atención a los siguientes dos teoremas.

Teorema 6. El grupo simétrico S_3 es resoluble.

Demostración: Los elementos de S_3 son

$$e = Id, \quad a_1 = (1,2,3), \quad a_2 = (1,3,2), \quad a_3 = (2,3), \quad a_4 = (1,3), \quad a_5 = (1,2)$$

S_3 tiene un subgrupo normal $H = \{e, a_1, a_2\}$ y tanto H como S/H son cíclicos. Entonces S_3 es resoluble.

El siguiente resultado no es tan evidente como el anterior.

Teorema 7. El grupo simétrico S_4 es resoluble.

Demostración: El grupo alternante A_4 es un subgrupo de índice 2 y ciertamente normal. No obstante, el cociente S_4 / A_4, siendo un grupo de orden 2, es ciertamente abeliano.[1] El grupo alternante esta constituido por la identidad, junto con los 11 elementos

$$(1,2,3),(1,2,4),(1,3,2),(1,3,4),(1.4.2),(1.4.3),(2.3.4),(2.4.3),\ (1.2)(3.4),$$
$$(1.3)(2.4),\ (1.4)(2,3)$$

El conjunto $V = \{e, (1.2)(3.4), (1.3)(2.4), (1.4)(2,3)\}$ es un subgrupo abeliano de A_4 (Grupo de Klein). Sus clases laterales izquierdas y derechas son

1- Se demuestra sin dificultad que todo grupo de orden menor o igual a 5 es abeliano. Para orden 2,3 y 5 es cierto estos son números primos. Para orden 4 se llega fácilmente teniendo en cuenta el conocido Teorema de Lagrange.

$$V, \qquad V(1,2,3) = (1,2,3)V = \{(1,2,3), (1,3,4), (1.4.2), (2.4.3)\},$$

$$V(1,2,4) = (1,2,4)V = \{(1,2,4), (1,3,2), (1.4.3), (2.3.4)\}$$

y se cumple $V \lhd A_4$. El cociente A_4/V, siendo de orden 3, es abeliano. Entonces tenemos

$$e \subseteq V \subseteq A_4 \subseteq S_4$$

con

$$e \lhd V, \;\; V \lhd A_4, \;\; A_4 \lhd S_4$$

y además

V/e, A_4/V, $S_4\,/A_4$ son todos abelianos, y entonces, por el Teorema 3 y el Teorema 4 de la sección 2, sigue que S_4 es resoluble.

Para determinar cuando es resoluble el grupo S_n, cuando $n \geq 5$, es conveniente estudiar el grupo alternante A_n. Empecemos con el siguiente resultado.

Teorema 8. Para todo $n \geq 3$, el grupo alternante A_n es generado por el conjunto de todos los ciclos de longitud 3.

Demostración: Es claro que el grupo alternante A_n por el conjunto de elementos del tipo $(a,b)(c,d)$. Si las dos transposiciones son iguales, su producto es la identidad. Si el producto es de la forma $(a,b)(a,c)$, donde a,b,c son distintos, entonces vemos que

$$(a,b)(a,c) = (a,b,c)$$

y si a,b,c,d son todos distintos, entonces

$$(a,b)(c,d) = [(a,b)(a,c)][(c,a)(c,d)] = (a,b,c)(c,a,d)$$

El siguiente resultado acerca del grupo alternante requiere que recordemos la siguiente definición:

Definición 9. Un grupo G es *simple* si sus únicos subgrupos normales son $\{e\}$ y el mismo G.

Teorema 10. Para todo $n \geq 5$, el grupo alternante A_n es simple.

Demostración: Sea $N \neq \{e\}$ un subgrupo normal de A_n; Mostraremos que N contiene a cada ciclo de longitud 3, y por consiguiente seguirá del teorema anterior que $N = A_n$.

Caso 1. Supongamos primero que N contiene un ciclo (a, b, c) de longitud 3. Sean x, y, z elementos distintos de $\{1, \dots, n\}$, y sea

$$\alpha = \begin{pmatrix} a\ b\ c \\ x\ y\ z \end{pmatrix}$$

entonces $\alpha^{-1}(a, b, c)\alpha = (x, y, z)$. Si α es par, entonces $(x, y, z) \in N$; si α es impar, la reemplazamos por la permutación par $\beta = (d, e)\alpha$, donde $d, e \notin \{a, b, c\}$ (siendo esto posible puesto que $n \geq 5$) y observemos que $\beta^{-1}(a, b, c)\beta = (x, y, z)$. Por lo tanto N contiene todos los ciclos de longitud 3, por lo cual $N = A_n$.

Caso 2. Supongamos ahora que N contiene un elemento σ el cual se descompone en ciclos ajenos del siguiente modo

$$\sigma = k_1 \cdots k_r$$

y supongamos que uno de los ciclos, lo podemos hacer sin perder generalidad, digamos k_1, es de longitud $s \geq 4$:

$$k_1 = (a_1, \dots, a_s)$$

Sea $\alpha = (a_1, a_2, a_3)$; entonces $\alpha^{-1}\sigma\alpha = \alpha^{-1}k_1\alpha k_2 \cdots k_r$, dado que solamente k_1 es afectado por la conjungacion y

$$\alpha^{-1}k_1\alpha = (a_1, a_3, a_2)(a_1, \dots, a_s)(a_1, a_2, a_3) = (a_2 a_3 a_1 a_4 a_5, \dots, a_s)$$

El elemento $\sigma^{-1}\alpha^{-1}\sigma\alpha$ pertenece a N, y

$$\sigma^{-1}\alpha^{-1}\sigma\alpha = k_1^{-1}\alpha^{-1}k_1\alpha = (a_s, a_{s-1}, \dots, a_1)(a_2, a_3, a_1, a_4, a_5, \dots, a_s)$$
$$= (a_1, a_2, a_4)$$

De este modo volvemos al Caso 1, asi que $N = A_n$.

Queda por considerar el caso donde todos los elementos de N poseen ciclos que involucran solamente ciclos de longitud 2 y 3. Si σ contiene solamente un ciclo (a, b, c) de longitud 3 (siendo los demas, ciclos de longitud 2), entonces $\sigma^2 = (a, c, b) \in N$, y entonces volvemos al Caso 1. Entonces supongamos que σ contiene por lo menos dos ciclos ajenos (a, b, c) y (d, e, f) de longitud 3. Entonces N contiene a

$$\sigma' = (e, d, c)\sigma(e, c, d)$$
$$= (e, d, c)(a, b, c)(d, e, f)(e, c, d)\cdots$$
$$= (a, b, d)(c, f, e)\cdots$$

y entonces contiene a

$$\sigma\sigma' = (a, b, c)(d, e, f)\cdots(a, b, d)(c, f, e)\cdots$$
$$= (a, d, c, b, f,)\cdots$$

De este modo volvemosal Caso 2, asi que $N = A_n$.

El caso final es cuando σ es el producto de un (necesariamente par) número de transposiciones. Supongamos primero que son solamente dos: $\sigma = (a, b)(c, d)$. Entonces existe al menos otro simbolo e, dado que asumimos que $n \geq 5$, y N contiene al elemento

$$\sigma[(a, b, e)^{-1}\sigma(a, b, e)] = (a, b)(c, d)(a, e, b)(a, b)(c, d)(a, b, e) = (a, e, b)$$

Y otra vez regresamos al Caso 1.

Supongamos finalmente que $\sigma = (a, b)(c, d)(e, f)(g, h)\cdots$. Entonces N contiene al elemento

$$\sigma[(b,c)^{-1}(d,e)^{-1}\sigma(d,e)(b,c)] = \sigma(b,c)(d,e)\sigma(d,e)(b,c)$$
$$= (a,e,d)(b,c,f)\cdots$$

y otra vez volvemos a un caso ya considerado. Así concluye la demostración.

Del teorema anterior sigue inmediatamente el siguiente corolario:

Corolario 11. El grupo simétrico S_n con $n \geq 5$ no es resoluble.

Demostración: Si S_n fuese resoluble, entonces todos sus subgrupos deberían ser resolubles, y sabemos que A_n, siendo simple, no es resoluble.

Lema 12. Sea la transposición $\phi = (1,2)$ y el ciclo $\psi = (1,2,\dots,n)$, ambos en S_n. Se cumple que

$$\psi^{-k}\phi\psi^{k} = (\psi^{k}(1), \psi^{k}(2)) = (k+1, k+2); (\text{mod } n), k \geq 1$$

Demostración: Procederemos por inducción sobre k. Supongamos que $k = 1$. Con un simple cálculo vemos que

$$\psi^{-1}\phi\psi^{1} = (1,2,\dots,n)^{-1}(1,2)(1,2,\dots,n)^{1} = (2,3) = (\psi^{1}(1), \psi^{1}(2))$$

Supongamos ahora que la propiedad es valida para $k = m$. Debemos demostrar entonces que la propiedad se cumple para $m+1$. Según nuestra hipótesis inductiva, es verdad que:

$$\psi^{-k}\phi\psi^{k} = (1,2,\dots,n)^{-k}(1,2)(1,2,\dots,n)^{k} = (k+1, k+2)$$

Veamos ahora que

$$\psi^{-(k+1)}\phi\psi^{k+1} = (1,2,\dots,n)^{-(k+1)}(1,2)(1,2,\dots,n)^{k+1}$$

Dado que estamos trabajando en un grupo, sigue que $\psi^{-(k+1)}\phi\psi^{k+1}$ se puede escribir en la forma:

$$\psi^{-1}(\psi^{-k}\phi\psi^{k})\psi^{1}$$

Siendo

$$\psi^{-k}\phi\psi^{k} = (k+1, k+2)$$

tenemos entonces que

$$\psi^{-1}(\psi^{-k}\phi\psi^{k})\psi^{1} = \psi^{-1}(k+1, k+2)\psi^{1}$$

Realizando esta composición, sin dificultad llegamos a que:

$$\psi^{-1}(\psi^{-k}\phi\psi^{k})\psi^{1} = \psi^{-1}(k+1, k+2)\psi^{1} = (k+2, k+3)$$

Esto es:

$$\psi^{-(k+1)}\phi\psi^{k+1} = \left(\psi^{k+1}(1), \psi^{k+1}(2)\right)$$

De esta forma queda demostrado el teorema.

El teorema anterior muestra como generar las transposiciones de la forma $(x, x+1)$, con $1 \leq x \leq n-1$, a partir de la transposición $\phi = (1,2)$ y el ciclo $\psi = (1,2, \dots, n)$, de S_n. En realidad puede demostrarse que el grupo simétrico es generado justamente por $\phi = (1,2)$ y $\psi = (1,2, \dots, n)$.

Para llegar a ese punto necesitamos el siguiente resultado.

Teorema 13. Si $n \geq 2$, entonces las $n-1$ transposiciones $\{(1, i): 2 \leq i \leq n\}$ generan S_n.

Demostración: Si $n = 2$, el resultado es inmediato. Supongamos ahora que el resultado es válido para $n-1 \geq 2$ y sea $\tau \in S_n$. Supongamos que $\tau(n) = m$, con $1 \leq m \leq n$. Entonces el elemento

$$s = \tau(1, m)(1, n)$$

verifica $s(n) = n$, por lo tanto, podemos pensar a s como una permutación en S_{n-1} y así utilizar nuestra hipótesis inductiva. Entonces, s se escribe como el producto de elementos de la forma $(1, i)$ con $2 \leq i \leq n - 1$, y en consecuencia

$$\tau = s(1, n)(1, m)$$

Se escribe como producto de las transposiciones citadas.

Corolario 14. El grupo simétrico S_n es generado por la transposición $\phi = (1,2)$ y el ciclo $\psi = (1,2, \dots, n)$.

Demostración: Demostraremos que toda transposición de la forma $(1, i)$ con $2 \leq i \leq n$ puede obtenerse a partir de $\phi = (1,2)$ y $\psi = (1,2, \dots, n)$. Si $i = 2$, entonces $(1, i) = \psi$ y no hay nada que demostrar.

Supongamos entonces ya obtenidas las $(1,2), (1,3), \dots, (1, i)$ a partir de ϕ y ψ. Veamos cono hacer lo mismo con $(1, i + 1)$. En vista del Lema 12, las transposiciones de la forma $(i, i + 1)$ son generadas a partir de ϕ y ψ, entonces, observando que:

$$(1, i)(i, i + 1)(1, i) = (1, i + 1)$$

Concluimos que la transposición $(1, i + 1)$ puede obtenerse a partir de ϕ y ψ, y como S_n es generado por esta clase de transposiciones, por el Teorema 13, sigue el resultado buscado.

Otra propiedad importante que muestra como generar cualquier tipo de transposición a partir de transposiciones de la forma $(1, i)$ y $(1, r)$ es la siguiente:

$$(1, r)(1, i)(1, r) = (r, i).$$

Capítulo 3

Teoría de Galois

Es este capítulo desarrollaremos algunos de los conceptos claves de la Teoría de Galois que nos servirán en lo que sigue para llegar al resultado principal de este trabajo, la demostración de la imposibilidad de resolver mediante radicales la ecuación general de quinto grado y de grados superiores. Comenzaremos por definir el Grupo de Galois de una extensión.

§ 1 El Grupo de Galois.

Definición 1. Sea L una extensión del campo K. Un isomorfismo α del campo L en si mismo es un *automorfismo* del campo L. Todo automorfismo α de L tal que $\alpha(x) = x$, para todo $x \in K$ se llama $K -$*automorfismo* de L.

Teorema 2. Sea L un campo y sea $\mathrm{Aut}(L)$ el conjunto de todos los automorfismos de L. Entoces $\mathrm{Aut}(L)$ es un grupo bajo la composición de funciones.

Demostración: La composición de funciones siempre es asociativa, dado que para todo $x \in L$ y para todo $\alpha, \beta, \gamma \in \mathrm{Aut}(L)$ se tiene

$$[(\alpha o\beta)o\gamma](x) = (\alpha o\beta)[\gamma(x)] = \alpha\left(\beta\left(\gamma(x)\right)\right)$$

$$[\alpha o(\beta o\gamma)](x) = \alpha([\beta o\gamma](x)) = \alpha\left(\beta\left(\gamma(x)\right)\right)$$

Por otra parte, existe un automorfismo identidad definido de la siguiente forma:

$$i(x) = x, x \in L$$

Y es claro que $io\alpha = \alpha oi = \alpha$, para todo $\alpha \in \mathrm{Aut}(L)$. Finalmente, para todo para todo $\alpha \in \mathrm{Aut}(L)$, existe una función inversa α^{-1} definida mediante la propiedad de que $\alpha^{-1}(z) = x$, y x es el único elemento en L tal que $\alpha(x) = z$. Veamos ahora que α^{-1} esta en $\mathrm{Aut}(L)$. Sean $y, z \in K$ y sean $\alpha^{-1}(z) = x$ y $\alpha^{-1}(t) = y$. Entonces $\alpha(x) = z$ y $\alpha(y) = t$ y además $\alpha(x + y) = z + t$. Luego

$$\alpha^{-1}(z) + \alpha^{-1}(t) = x + y = \alpha^{-1}\left(\alpha(x + y)\right) = \alpha^{-1}(z + t)$$

De la misma forma podemos demostrar que

$$(\alpha^{-1}(z))(\alpha^{-1}(t)) = \alpha^{-1}(zt)$$

Luego α^{-1} esta en $\mathrm{Aut}(L)$, y tiene la propiedade que $\alpha o\alpha^{-1} = \alpha^{-1}o\alpha = i$. De esta forma queda demostrado el teorema.

Teorema 3. Sea L una extensión normal y de grado finito sobre el campo K, y sea E un subcampo de L que contiene a K. Entonces cada $K -$ automorfismo de E en L se puede extender a un $K -$ automorfismo de L.

Demostración: Sea δ un $K -$ automorfismo de E en L. Por el Teorema 8, seccion 2, capítulo 1, existe un polinomio f tal que L es el campo de descomposicion de f sobre K. L es tambien el campo de descomposición para f sobre cada uno de los campos E y $\varphi(E)$. Por el Teorema 5, sección 5 del capítulo 1, con $L = L'$, deducimos que existe un $K -$ automorfismo φ^* de L que extiende φ.

Teorema 4. Sea L una extensión normal y de grado finito sobre el campo K. Si z_1 y z_2 son raices de un mismo polinomio irreducible en $K[x]$. Entonces esiste un $K-$ automorfismo θ de L tal que $\theta(z_1) = z_2$.

Demostración: Por el Lema 4, seccion 5, capítulo 1, que existe un $K-$ automorfismo de $K(z_1)$ sobre $K(z_2)$. Por el Teorema 3, este se extiende a un $K-$ automorfismo θ de L.

Teorema 5. Sea L una extensión normal finita del campo K, y sea E un subcampo de L que contiene a K. Entonces E es una extensión normal de si y solo si cada $K-$automorfismo de E en L es un $K-$automorfismo de E.

Demostración: Supongamos primero que E es una extensión normal, entonces E es su propia clausura normal. Sea φ un $K-$automorfismo de E en L, y sea $z \in E$. Sea $m = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ el polinomio minimal de z sobre K. Entonces

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0$$

Y por ende, aplicando φ a esta igualdad, tenemos:

$$\big(\varphi(z)\big)^n + a_{n-1}\big(\varphi(z)\big)^{n-1} + \cdots + a_1\big(\varphi(z)\big) + a_0 = 0$$

Entonces, $\varphi(z)$ tambien es una raíz de m en L. Pero z, un elemento de E, es una raíz del polinomio irreducible m, y entonces, puesto que E es normal, m se descompone completamente sobre E. Sigue que $\varphi(z) \in E$, entonces $\varphi(E)$ es un campo contenido en E. Sigue que $K \subset \varphi(E) \subset E$. Entonces por el Teorema de la Torre de Extensiones tenemos que:

$$[E: K] = [E: \varphi(E)][\varphi(E): K]$$

Supongamos que $[E: K] = n$. Este número representa a la dimensión de E como espacio vectorial sobre K. De la misma forma,

$$[\varphi(E): K] = \frac{n}{[E: \varphi(E)]}$$

Representa la dimensión de $\varphi(E)$ como espacio vectorial sobre K. Dado que φ es un monomorfismo y además $\varphi(K) = K$, podemos ver a φ como una tranformación lineal de E en L, donde $\mathrm{Im}(\varphi) = \varphi(E)$. Por otra parte, es claro que $\varphi(z) = 0$ si y solo si $z = 0$, puesto que $0 \in K$, esto es $\mathrm{Ker}(\varphi) = \{0\}$. Luego por el conocido Teorema de la Dimensión que establece que:

$$\mathrm{Dim}\big(\mathrm{Ker}(\varphi)\big) + \mathrm{Dim}\big(\mathrm{Im}(\varphi)\big) = \mathrm{Dim}(\mathrm{E})$$

En nuestro caso es:

$$0 + \frac{n}{[E:\varphi(E)]} = n$$

Entonces

$$[E:\varphi(E)] = 1$$

Y por el teorema 2, sección 3, capítulo 1, es:

$$E = \varphi(E)$$

Entonces tenemos que φ es un K −automorfismo de E.

Por el contrario supongamos que cada K −automorfismo de E en L es un K −automorfismo de E. Sea f un polinomio irreducible en $K[x]$ que posee una raíz $z \in E$. Para establecer que E es una extensión normal de K, necesitamos mostrar que f se descompone completamente sobre E. Ciertamente, puesto que L es normal, f se descompone completamente sobre L. Sea z' otra raíz de f en L. Entonces por el teorema 4, existe un K −automorfismo ψ de L tal que $\psi(z) = z'$. Sea ψ^* la restricción de ψ a E. Entonces ψ^* es un K −automorfismo de E en L, y también, por lo que asumimos, es un K −automorfismo de E. Entonces $z' = \psi(z) = \psi^*(z) \in E$, y entonces llegamos a que E es normal.

Definición 6. El conjunto de todos los K −automorfismos de L se llama el *Grupo de Galois* de L sobre K y se denota por $\mathrm{Gal}(L/K)$.

El siguiente teorema nos dirá la razón por la cual $\mathrm{Gal}(L/K)$ se llama Grupo Galois.

Teorema 7. Sea el campo de extensión L/K. Entonces el conjunto $\mathrm{Gal}(L/K)$ de todos los automorfismos de L es un subgrupo de $\mathrm{Aut}(K)$.

Demostración: Ciertamente $i \in \mathrm{Gal}(L/K)$. Sean $\alpha, \beta \in \mathrm{Gal}(L/K)$, entonces para todo $x \in K$

$$x = \beta(x) = \beta^{-1}\big(\beta(x)\big) = \beta^{-1}(x)$$

Esto muestra que $\beta^{-1} \in \mathrm{Gal}(L/K)$. Luego

$$(\alpha o \beta^{-1})(x) = \alpha(\beta^{-1}(x)) = \alpha(x) = x$$

Esto es, $\alpha o \beta^{-1}$ $\mathrm{Gal}(L/K)$. Por lo tanto $\mathrm{Gal}(L/K)$ es un subgrupo de $\mathrm{Aut}(K)$.

En relación a la Definición 6, y que los polinomios juegan un papel importante en cuanto a la generación de los campos de descomposición, que como vimos son extensiones, tenemos la siguiente definición:

Definición 8. Sea el polinomio $f \in K[x]$ y sea $L = K(\alpha_1, \dots, \alpha_n)$ el campo de descomposición de f sobre K. Se define el Grupo de Galois de f, denotado por $\mathrm{Gal}(f)$, como el grupo $\mathrm{Gal}(L/K)$.

Los siguientes teoremas muestran cómo se comportan los elementos del Grupo de Galois.

Teorema 9. Sea L una extensión finita sobre el campo K y σ un elemento de $\mathrm{Gal}(L/K)$. Dado un polinomio $h \in K[x_1, \dots, x_n]$ y los elementos $\beta_1, \dots, \beta_n \in L$, entonces

$$\sigma(h(\beta_1, \dots, \beta_n)) = h(\sigma(\beta_1), \dots, \sigma(\beta_n))$$

En particular si $h \in K[x]$ y $\beta \in L$, entonces

$$\sigma(h(\beta)) = h\big(\sigma(\beta)\big)$$

Demostración: Se sigue inmediatamente de la definición de automorfismo de σ y ademas que por ser σ un elemento de $\mathrm{Gal}(L/K)$, $\sigma(x) = x$ para todo $x \in K$.

A partir de este resultado es claro que si $\beta \in L$ es raíz de un polinomio $h \in L[x]$, entonces $\sigma(\beta)$ lo es también. Esto se muestra en el siguiente teorema.

Teorema 10. Sea L una extensión finita del campo K y sea $\sigma \in \mathrm{Gal}(L/K)$, entonces:

1. si $h \in K[x]$ es un polinomio no constante y $\alpha \in L$ es una raíz del mismo, entonces $\sigma(\alpha) \in L$ también es una raíz de h.

2. Si $L = K(\alpha_1, \dots, \alpha_n)$, entonces σ queda unívocamente determinado por sus valores en $\alpha_1, \dots, \alpha_n$.

Demostración: Por el Teorema 9, si $h \in K[x]$ y $h(\alpha) = 0$ implica que

$$0 = \sigma(0) = \sigma\big(h(\alpha)\big) = h(\sigma(\alpha))$$

Esto muestra que $\sigma(\alpha) \in K$, es también una raíz de h. Queda demostrada asi la parte 1.

Ahora notemos que $L = K[\alpha_1, \dots, \alpha_n]$, puesto que $L = K(\alpha_1, \dots, \alpha_n)$ es una extensión finita de K, por el Teorema 7, sección 2 del capítulo 1. Por lo que cualquier $\beta \in K$ puede escribirse en la forma

$$\beta = h(\alpha_1, \dots, \alpha_n)$$

Para algún $h \in K[x_1, \dots, x_n]$. Luego, por el Teorema 9,

$$\sigma(\beta) = \sigma(h(\alpha_1, \dots, \alpha_n)) = h(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$$

De esto sigue que $\sigma: L \to L$ queda unívocamente determinado por

$$\sigma(\alpha_1), \dots, \sigma(\alpha_n).$$

Este teorema nos conduce a nuestro primer resultado sobre la estructura del Grupo de Galois.

Corolario 11. Sea L una extensión finita sobre el campo K, entonces su Grupo de Galois, $\mathrm{Gal}(L/K)$ es finito.

Demostración: Dado que L una extensión finita, $L = K(\alpha_1, \dots, \alpha_n)$, donde cada α_i es algebraico sobre K. Ahora suponga que $\sigma \in \mathrm{Gal}(L/K)$. Por la parte 2 del Teorema 10, σ queda unívocamente determinado por $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$. Lo que es mas, si $p_i \in F[x]$ es el polinomio minimal de α_i, entonces la parte 1 del Teorema 10 dice que hay a lo sumo $\mathrm{Grad}(p_i)$ valores distintos que puede asumir $\sigma(\alpha_i)$. La finitud del Grupo de Galois $\mathrm{Gal}(L/K)$, se sigue de inmediato.

Teorema 12. Sean los siguientes campos $K \subset E \subset L$. Supongamos que E es una extensión finita de K y que L es una extensión finita de E. Entonces $\mathrm{Gal}(L/E)$ es un subgrupo de $\mathrm{Gal}(L/K)$.

Demostración: Cada $\sigma \in \mathrm{Gal}(L/E)$ es un automorfismo de L que es la identidad sobre E, entonces $\sigma \in \mathrm{Gal}(L/K)$ sigue de $K \subset E$; por lo tanto $\mathrm{Gal}(L/E) \subset \mathrm{Gal}(L/K)$. Puesto que ambos son grupos bajo la composición, concluimos que $\mathrm{Gal}(L/E)$ es un subgrupo de $\mathrm{Gal}(L/K)$.

Ahora introduciremos una importante idea que relaciona los subcampos E del campo L que contienen al campo K y los subgrupos H del grupo de Galois $\mathrm{Gal}(L/K)$. Para cada E definimos:

$$\Gamma(E) = \{\alpha \in \mathrm{Aut}(L): \alpha(z) = z, \forall z \in E\} \tag{3.1}$$

Y para cada H definimos

$$\Phi(\mathrm{H}) = \{x \in \mathrm{L}: \alpha(x) = x, \forall\, \sigma \in H\} \tag{3.2}$$

Mas adelante veremos que estos dos conjuntos son fundamentales en la Teoría de Galois. Ahora veamos dos propiedades de estos conjuntos.

Teorema 13. Sea L un campo de extensión del campo K.

1. Para cada subcampo E de L que contiene a K, el conjunto $\Gamma(E)$ es un subgrupo de $\mathrm{Gal}(L/K)$.

2. Para cada subgrupo H de $\mathrm{Gal}(L/K)$, el conjunto $\Phi(\mathrm{H})$ es un subcampo de L que contiene a K.

Demostración: 1. Ciertamente $\Gamma(E) \neq \emptyset$, dado que contiene a i, el automorfismo identidad. También $\Gamma(E) \subseteq \mathrm{Gal}(L/K)$, dado que todo automorfismo que deje fijos todos los elementos de E, automáticamente deja fijo los elementos de K, puesto que $K \subset E$.

Sean $\alpha, \beta \in \Gamma(E)$. Entonces para $z \in E$.

$$(\alpha o \beta^{-1})(z) = \alpha\big(\beta^{-1}(z)\big) = \alpha\left(\beta^{-1}\big(\beta(z)\big)\right) = \alpha(z) = z$$

Por lo tanto $\alpha o \beta^{-1} \in \Gamma(E)$. Entonces $\Gamma(E)$ es un subgrupo.[1]

2. Es claro que $K \subseteq \Phi(\mathrm{H})$ puesto que todo automorfismo en $\mathrm{Gal}(L/K)$ dejan fijos los elementos de K. Sean $x, y \in \Phi(\mathrm{H})$, entonces para todo $\alpha \in H$,

$$\alpha(x - y) = \alpha(x) - \alpha(y) = x - y$$

Así que $x - y \in \Phi(\mathrm{H})$. Si $y \neq 0$, entonces, para todo $\alpha \in H$

$$\alpha(xy^{-1}) = \alpha(x)\alpha(y^{-1}) = \alpha(x)(\alpha(x))^{-1} = xy^{-1}$$

1- Existen varias criterios para determinar cuándo, dado un grupo G y un subconjunto H de G, H es un subgrupo de G. En este caso, basta con demostrar que H no es vacio y que dados a, b en H, esto implica que ab^{-1} tambien está en H. Véase por ejemplo Álgebra Abstracta de Herstein pág. 51 para ver condiciones de subgrupo.

Así que $xy^{-1} \in \Phi(\mathrm{H})$. Entonces $\Phi(\mathrm{H})$ es un subcampo de L.[1]

Según el teorema anterior, $\Gamma(E)$ es el grupo de todos los E −automorfismos de L. Esto es, $\Gamma(E) = \mathrm{Gal}(L/E)$.

Por otra parte, diremos que $\Phi(\mathrm{H})$ es el campo fijo de H. En algunos textos, cuando L es una extensión de K, el campo fijo de un subconjunto H, tal como se definió aquí, se suele denotar por los símbolos L_H, o $\mathrm{Fix}(\mathrm{H})$.[2]

Teorema 14. Sea el campo de extensión L/K.

1. Si E_1 y E_2 son subcampo de L que contienen a K, entonces

$$E_1 \subseteq E_2 \Longrightarrow \Gamma(E_1) \supseteq \Gamma(E_2)$$

2. Si H_1 y H_2 son subgrupos de $\mathrm{Gal}(L/K)$, entonces

$$H_1 \subseteq H_2 \Longrightarrow \Phi(H_1) \supseteq \Phi(H_2)$$

Demostración: 1. Supongamos que $E_1 \subseteq E_2$, y sea $\alpha \in \Gamma(E_2)$, entonces α deja fijo cada elemento de E_2 de tal modo que también deja fijo cada elemento de E_1. Por lo tanto $\alpha \in \Gamma(E_1)$.

2. Supongamos que $H_1 \subseteq H_2$, y sea $z \in \Phi(H_2)$, entonces $\alpha(z) = z$ para cada α en H_2, y por lo tanto también para cada α en H_1, Por lo tanto $z \in \Phi(H_1)$.

Los dos teorema precedentes dejan en claro la estrecha relación de Γ y Φ. Sin embargo no es necesariamente cierto que ambos conjuntos sean siempre

1- Si R es un campo y F un subconjunto de R, se demuestra sin dificultad que F es un subcampo de R si y solo si: $0 \in F$, $(a - b) \in F$ y $ab^{-1} \in F$, para todo $a, b \in F$.

2- Véase por ejemplo Galois Theory de D. Cox, Cap. 7, pág. 147.

mutuamente inversos. Esto es, Dados los campos $K \subset E \subset L$ y los grupos H y $\mathrm{Gal}(L/K)$, no necesariamente se cumplen a la vez las siguientes relaciones:

$$\Gamma(\mathrm{E}) = \mathrm{H} \text{ y } \Phi(H) = E$$

Que también se pueden escribir como

$$\Gamma\big(\Phi(H)\big) = \mathrm{H} \text{ y } \Phi\big(\Gamma(\mathrm{E})\big) = E$$

Más adelante veremos bajo qué condiciones esto es cierto. Por el momento, veamos un ejemplo en el que se cumple esta propiedad.

Ejemplo: Sea $\mathbb{Q} \subset L = \mathbb{Q}\big(\sqrt[3]{2}\big)$. El polinomio minimal de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ es $x^3 - 2$, el cual tiene raíces $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, donde $\omega = e^{2\pi i/3}$. Los últimas dos raíces no son reales por lo que no pueden estar en $\mathbb{Q}\big(\sqrt[3]{2}\big)$. Por lo tanto cada $\sigma \in \mathrm{Gal}\big(\mathbb{Q}\big(\sqrt[3]{2}\big)/\mathbb{Q}\big)$ de cumplir que $\sigma\big(\sqrt[3]{2}\big) = \sqrt[3]{2}$. Puesto que σ esta unívocamente determinado por $\sigma\big(\sqrt[3]{2}\big)$, debe ser la identidad. Por lo tanto $\mathrm{Gal}\big(\mathbb{Q}\big(\sqrt[3]{2}\big)/\mathbb{Q}\big) = \{i\}$. Por esta razón es

$$\Gamma\left(\mathbb{Q}\big(\sqrt[3]{2}\big)\right) = \{i\}$$

De esta forma

$$\Phi(\{i\}) = \mathbb{Q}\big(\sqrt[3]{2}\big)$$

Y así se cumple la propiedad en cuestión.

Ejemplo: Descripción de $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Sea $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, entonces $\sigma(x) = x$ para todo $x \in \mathbb{R}$. Sea $\sigma(i) = j$. Entonces

$$j^2 = \sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$$

De este modo, $j = \pm i$. Si $j = i$ entonces, para todo $(x + yi) \in \mathbb{C}$, con $x, y \in \mathbb{R}$,

$$\sigma(x+yi) = \sigma(x) + \sigma(y)\sigma(i) = x + yi$$

Y de esta forma σ es el automorfismo identidad. Si $j = -i$, entonces

$$\sigma(x+yi) = x - yi$$

Evidentemente esta función deja fijo los elementos de $\mathbb{R}$. Notemos que a su vez, también es un automorfismo, pues

$$\begin{aligned}\sigma\big((x+yi)+(u+vi)\big) &= \sigma\big((x+u)+(y+v)i\big) = (x+u)-(y+v)i \\ &= (x-yi)+(u-vi) = \sigma(x+yi)+\sigma(u+vi)\end{aligned}$$

y

$$\begin{aligned}\sigma\big((x+yi)(u+vi)\big) &= \sigma\big((xu-yv)+(xv+yu)i\big) = (xu-yv)-(xv+yu)i \\ &= (x-yi)(u-vi) = (\sigma(x+yi))(\sigma(u+vi))\end{aligned}$$

De esto deducimos que $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ es el grupo $\{Id, k\}$ de orden 2, donde k es la función de conjugación compleja, la cual asocia cada $(x+yi) \in \mathbb{C}$ a $(x-yi) \in \mathbb{C}$. Dado que $[\mathbb{C}:\mathbb{R}] = 2$, un número primo, no pueden haber campos intermedios entre $\mathbb{C}$ y $\mathbb{R}$. Luego tenemos

$$\Phi(\{Id\}) = \mathbb{C} \quad \text{y} \quad \Phi(\{Id, k\}) = \mathbb{R}$$

§ 2 El orden del Grupo de Galois.

Con el fin de seguir avanzando en nuestro estudio de la Teoría de Galois, veamos ahora algunas características del orden del Grupo de Galois. Nos encargaremos en esta sección de calcular el orden del Grupo de Galois.

Teorema 1. Sea L una extensión finita de K y sea G un subgrupo del Grupo de Galois $\mathrm{Gal}(L/K)$. Entonces $|L:\Phi(G)| = |G|$.

Demostración. Sea $|G| = n$ y supongamos que los elementos de G son $\sigma_1, \dots, \sigma_n$, donde σ_1 es la identidad en K.

1. Supongamos que $[L: \Phi(G)] = m < n$. Sea $\{x_1, \dots, x_m\}$ una base para L como espacio vectorial de $\Phi(G)$ Es sabido, del Algebra Lineal que existen $y_1, \dots, y_n \in K$ no todos iguales a cero, tales que

$$y_1\sigma_1(x_j) + \cdots + y_n\sigma_n(x_j) = 0 \tag{2.3}$$

Para $j = 1, \dots, m$. Sea x algún elemento de L. Entonces

$$x = \alpha_1 x_1 + \cdots + \alpha_m x_m$$

Donde $\alpha_1, \dots, \alpha_m \in \Phi(G)$. Entonces

$$y_1\sigma_1(x) + \cdots + y_n\sigma_n(x) = y_1\sigma_1\left(\sum_l \alpha_l x_l\right) + \cdots + y_n\sigma_n\left(\sum_l \alpha_l x_l\right)$$
$$= \sum_l \alpha_l[y_1\sigma_1(x_l) + \cdots + y_n\sigma_n(x_l)] = 0$$

Entonces los distintos monomorfismo $\sigma_1, \dots, \sigma_n$ son linealmente dependientes, esto contradice el Lema de Dedekind (1831-1916), el cual establece que si L y K son dos campos y $\sigma_1, \dots, \sigma_n$ monomorfismos distintos de K en L, entonces $\sigma_1, \dots, \sigma_n$ son linealmente independiente sobre L.[1] Entonces llegamos a la conclusión de que debe ser si o si $m \geq n$.

2. Supongamos ahora que $[L: \Phi(G)] > n$. Entonces existe un conjunto de $n + 1$ elementos de L que son linealmente independientes sobre $\Phi(G)$; digamos $\{x_1, \dots, x_{n+1}\}$. Entonces existen $y_1, \dots, y_{n+1} \in L$, no todos iguales a cero, tales que para $j = 1, \dots, n$

$$y_1\sigma_j(x_1) + \cdots + y_{n+1}\sigma_j(x_{n+1}) = 0 \tag{3.3}$$

Elijamos las $y_1, \dots, y_{n+1}$ de modo tal que el menor número de ellas sea igual a cero

1- Véase la demostración del Lema de Dedekind en Fields and Galois Theory de J. Howie, Teorema 7.1, pág. 92.

y reenumeremos estas cantidades en la siguiente forma

$$y_1, \dots, y_r \neq 0 \quad \text{y} \quad y_{r+1}, \dots, y_{n+1} = 0$$

Entonces la ecuación (3.3) se convierte en:

$$y_1\sigma_j(x_1) + \cdots + y_r\sigma_j(x_r) = 0 \tag{3.4}$$

Sea $\sigma \in G$. Apliquemos σ a la ecuación (3.4). De esto resulta:

$$\sigma(y_1)\sigma\left(\sigma_j(x_1)\right) + \cdots + \sigma(y_r)\sigma\left(\sigma_j(x_r)\right) = 0 \tag{3.5}$$

Notemos que si $\sigma \in G = \{\sigma_1, \dots, \sigma_n\}$, la función $\sigma_i \mapsto \sigma\sigma_i$ es un isomorfismo de G. En efecto, si $h \in G$, entonces $\sigma^{-1}h = \sigma_j$, para algún j y $h = \sigma\sigma_j$. Ahora si $\sigma\sigma_i = \sigma\sigma_j$, entonces $\sigma_i = \sigma^{-1}\sigma\sigma_j = \sigma_j$. De esto, $\sigma_i \mapsto \sigma\sigma_i$ es una biyección de $G \to G$ y comprobamos el resultado indicado. Esto nos muestra que el sistema (3.5) es igual a

$$\sigma(y_1)\sigma_j(x_1) + \cdots + \sigma(y_r)\sigma_j(x_r) = 0 \tag{3.6}$$

Multiplicando la ecuación (3.4) por $\sigma(y_1)$ y la ecuación (3.6) por y_1 y luego restando ambas ecuaciones, entonces tenemos la siguiente ecuación:

$$[y_2\sigma(y_1) - \sigma(y_2)y_1]\sigma_j(x_2) + \cdots + [y_r\sigma(y_1) - \sigma(y_r)y_1]\sigma_j(x_r) = 0$$

Este es un sistema de ecuaciones como el (3.4), pero con menos términos, lo cual conduce a una contradicción a menos que todos los coeficientes

$$y_i\sigma(y_1) - y_1\sigma(y_i)$$

sean cero. Si esto ocurre, tenemos entonces que

$$y_i y_1^{-1} = \sigma(y_i y_1^{-1})$$

Para todo $\sigma \in G$. Así que $y_i y_1^{-1} \in K_0$. Entonces existen $z_1, \dots, z_r \in \Phi(G)$ y un elemento $(3.4) \in L$ tal que $y_i = kz_i$ para todo i. Entonces, haciendo $j = 1$, la ecuación (3.4) se convierte en:

$$x_1kz_1 + \cdots + x_rkz_r = 0$$

y dado que $k \neq 0$, podemos dividir por k, lo cual muestra que los x_i son linealmente dependientes sobre $\Phi(G)$. Esto es una contradicción.

Por lo tanto $[L: \Phi(G)]$ no es mayor que n, y puesto que tampoco puede ser menor que n por la primera parte de la demostración, debe cumplirse que $[L: \Phi(G)] = n = |G|$. Esto es:

$$[L: \Phi(G)] = |\mathrm{G}|$$

Así concluye la demostración del teorema.

Si bien sabemos que el Grupo de Galois el grupo formado por todos los K −automorfismo de L que dejan fijos todos elementos x de K, es otras palabras, que dejan fijo al campo claro que K, no podemos pretender en este momento aplicar el Teorema 1 a dicho grupo. Entre otras cosas porque no esta claro aun si el campo que queda fijo por la acción del grupo $\mathrm{Gal(L/K)}$ sobre el campo L es precisamente K, podemos decir sin embargo que tal campo debe contener o ser igual a K. Veremos entonces que el resultado anterior es válido siempre que L sea una extensión normal y separable de K. Con tal motivo, pasemos a demostrar el siguiente teorema.

Teorema 2. Sea L una extensión separable del campo K, de grado finito n. Entonces hay precisamente n K −monomorfismos distintos de L en la clausura normal N de L sobre K.

Demostración: Usemos inducción sobre el grado $[L: K]$. Si $[L: K] = 1$, entonces $L = K = N$, y el único K −monomorfismo de K en N es la función identidad.

Supongamos ahora que el resultado es valido para todo $n \leq k - 1$, y supongamos también que $[L: K] = k > 1$. Sea $z_1 \in L \setminus K$, y sea m (con $\mathrm{Grad(m)} = \mathrm{r} \geq 2$) el polinomio minimal de z_1 sobre K. Entonces $K \subset K(z_1) \subseteq L$, y $[K(z_1): K] = r$. Entonces, siendo m irreducible y teniendo una raíz z_1 en la extensión normal N, se descompone completamente sobre N. Dado que L es separable, las raíces de m

son todas distintas: supongamos que las raíces son $z_1, \dots, z_r$. Sea $[L: K(z_1)] = s$; entonces $1 \leq s \leq k$ y $rs = k$.

El campo N es una clausura normal de L sobre $K(z_1)$, y entonces, por la hipótesis inductiva, hemos supuesto que el número de $K(z_1)$ −monomorfismos de L en N es precisamente s: denotemoslos $\mu_1, \dots, \mu_s$. Por el Teorema 4, sección 1, existen r K −automorfismos distintos, digamos, $\lambda_1, \dots, \lambda_r$ de N, donde $\lambda_i(z_1) = z_i$ $(i = 1,2, \dots, r)$. Definamos la función $\varphi_{ij}: L \to N$ por:

$$\varphi_{ij}(x) = \lambda_i\big(\mu_j(x)\big) \tag{3.7}$$

donde $x \in L, i = 1, \dots, r; j = 1, \dots, s$.

Las definiciones muestran claramente que las funciones son todas K −monomorfismos.

Mostraremos que las funciones φ_{ij} son todas distintas. Primero observe que

$$\varphi_{ij}(z_1) = \lambda_i\big(\mu_j(z_1)\big) = \lambda_i(z_1) = z_i \tag{3.8}$$

Por lo tanto, si $\varphi_{ij} = \varphi_{pq}$, sigue que $i = p$. Supongamos ahora que $\varphi_{ij} = \varphi_{pq}$. Entonces, para todo $x \in L$,

$$\lambda_i\big(\mu_j(x)\big) = \lambda_i\big(\mu_q(x)\big)$$

Dado que λ_i es biyectivo, sigue que $\mu_j(x) = \mu_q(x)$ para todo $x \in L$, y entonces $j = q$. Entonces las funciones φ_{ij} son todas distintas, y de (3.7) deducimos que hay al menos $rs = k$ K −monomorfismos distintos de L en N.

Para mostrar que no hay más de k K −monomorfismos distintos de L en N, debemos mostrar que cada K −monomorfismos ψ de L en N coincide con una de las funciones φ_{ij}. En otras palabras, ψ debe transformar a z_1 en otra raíz z_i de m en N. Sea $\chi: L \to N$ una función definida por:

$$\chi(x) = {\lambda_i}^{-1}(\psi(x))$$

Ciertamente se trata de un K −monomorfismo; de hecho, dado que

$$\chi(z_1) = \lambda_i^{-1}\big(\psi(z_1)\big) = \lambda_i^{-1}(z_i) = z_1$$

con $x \in L$, tenemos que es un $K(z_1)$ −monomorfismo, y entonces coincide con uno de los $\mu_1, \dots, \mu_s$, digamos μ_j. Entonces para todo $x \in L$,

$$\mu_j = \lambda_i^{-1}\big(\psi(x)\big)$$

Y entonces $\psi(x) = \lambda_i\big(\mu_j(x)\big)$. Por lo tanto $\psi = \varphi_{ij}$.

En algunos de los resultados importantes que se detallan en las páginas siguientes, será necesario que las extensiones cumplan con la condición de ser normales y separables a la vez. Esto motiva la siguiente definición:

Definición 3. Se llama *extensión de Galois* a toda extensión que sea simultáneamente normal y separable.

Notemos que si en el enunciado del Teorema 2, suponemos que L es una extensión normal y separable, i.e. una extensión de Galois, luego L es su propia clausura normal, y entonces obtenemos el siguiente corolario de gran importancia en lo que sigue:

Corolario 4. Sea L una extensión de Galois del campo K, y sea G el Grupo de Galois $\mathrm{Gal(L/K)}$. Entonces:

$$|\mathrm{Gal(L/K)}| = [L: K]$$

§ 3 La correspondencia de Galois.

En la sección 1 definimos los conjuntos:

$$\Gamma(E) = \{\alpha \in \mathrm{Aut}(L): \alpha(z) = z, \forall z \in E\}$$

$$\Phi(\mathrm{H}) = \{\mathrm{x} \in \mathrm{L}: \alpha(x) = x, \forall\, \sigma \in H\}$$

En los cuales se relacionan los subcampos E del campo L que contienen al campo K, o subcampos intermedios, y los subgrupos H del grupo de Galois $\mathrm{Gal}(L/K)$. Ahora, si consideramos los campos

$$K \subseteq E_1 \subseteq E_2 \subseteq L$$

Según la definición de Γ es

$$\Gamma(K) = \mathrm{Gal}(L/K) \text{ y } \Gamma(L) = \{i\}$$

y según el Teorema 14 de la sección 1, si $E_1 \subseteq E_2$ se cumplen las inclusiones reversas $\Gamma(E_1) \supseteq \Gamma(E_2)$. Por esta razón tenemos:

$$\{i\} \subseteq \Gamma(E_2) \subseteq \Gamma(E_1) \subseteq \mathrm{Gal}(L/K)$$

Algo parecido podemos hacer con Φ. Tenemos $\Phi(\{i\}) = L$ y $\Phi\big(\mathrm{Gal}(L/K)\big) = K_0 \supseteq K$, y dados

$$\{i\} \subseteq H_1 \subseteq \mathrm{Gal}(L/K)$$

Se cumple, por el Teorema 14 de la sección 1, que

$$K \subseteq K_0 \subseteq \Phi(H_1) \subseteq L$$

Si llamamos $\mathcal{F}$ al conjunto de todos los subcampos E de L que contienen a K, y $\mathcal{G}$ al conjunto de todos los subconjuntos de $\mathrm{Gal}(L/K)$. Podemos der a Γ y a Φ como las funciones

$\Gamma: \mathcal{F} \to \mathcal{G}$ y $\Phi: \mathcal{G} \to \mathcal{F}$

Esta relación se conoce como *La Correspondencia de Galois* entre $\mathcal{F}$ y $\mathcal{G}$. Veremos a continuación que condiciones deben cumplirse para que Γ y Φ sean mutuamente inversas, esto es para que se establezca una biyección entre $\mathcal{F}$ y $\mathcal{G}$.

Antes de llegar a esto veamos el siguiente resultado.

Teorema 1. Sea L una extensión del campo K y sea E un subcampo de L que contiene a K y sea H un subgrupo del grupo de Galois $\mathrm{Gal}(L/K)$, entonces:

$$E \subseteq \Phi\big(\Gamma(E)\big), \qquad H \subseteq \Gamma(\Phi(H))$$

Demostración: Sea $z \in E$. El grupo $\Gamma(E)$ es el grupo de todos los automorfismos que dejan fijo cada elemento de E. Por tal razón, z es dejado fijo por algún automorfismo en $\Gamma(E)$. Por lo tanto $z \in \Phi\big(\Gamma(E)\big)$. Luego $E \subseteq \Phi\big(\Gamma(E)\big)$.

Sea $\alpha \in H$. El campo $\Phi(H)$ es el conjunto de todos los elementos de L que son dejados fijos por todos los elementos de H, y por eso α deja fijo a cada elemento de $\Phi(H)$, esto es $\alpha \in \Gamma(\Phi(H))$. Por lo tanto, $H \subseteq \Gamma(\Phi(H))$. De esta forma queda demostrado el teorema.

El siguiente teorema establece las condiciones que deben cumplirse para que el campo que queda fijo por la acción del Grupo de Galois $\mathrm{Gal}(L/K)$ sobre L, sea K.

Teorema 2. Sea L una extensión finita de K y sea G el Grupo de Galois $\mathrm{Gal(L/K)}$. Entonces el campo que queda fijo por la acción de G es K, i.e: $\Phi\big(\mathrm{Gal(L/K)}\big) = K$, si y solo si L es una extensión normal y separable de K.

Demostración: Sea K_0 el campo fijo de G, y sea $[L:K] = n$. El Corolario 4 de la sección 2 implica que $|G| = n$. Luego por el Teorema 1 de la sección 2 tenemos que $[L:K_0] = n$. Por el Teorema 1 es $K \subseteq K_0$, según el teorema de la Torre de Extensiones tenemos la siguiente relación

$$[L:K_0] = [L:K][K_0:K]$$

Pero según lo anterior, es $[L:K_0] = [L:K]$ y por ende, $[K_0:K] = 1$ y según el Teorema 2, sección 3 del capitulo 1, debe ser $K = K_0$.

Por el contrario, supongamos ahora que K es el campo fijo de $\mathrm{Gal(L/K)}$ y sea $\alpha \in L$. Hallaremos el polinomio minimal de α sobre K usando una construcción debida a Lagrange. Sea $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r$ los distintos elementos de L obtenidos al aplicar los elementos de $\mathrm{Gal(L/K)}$ a α. Entonces considere el polinomio:

$$h(x) = \prod_{i=1}^{r} (x - \alpha_i) \in L[x]$$

Mostraremos que $h \in K[x]$ y que h es irreducible sobre K.

Primero mostremos que $\sigma \in \mathrm{Gal(L/K)}$ permuta los elementos α_i. Por definición tenemos que $\alpha_i = \tau(\alpha)$, para algún $\tau \in \mathrm{Gal(L/K)}$, entonces $\sigma(\alpha_i.) = \sigma\big(\tau(\alpha)\big) = (\sigma\tau)(\alpha_i.)$, el cual es α_j para algún j. Entonces σ transforma $\{\alpha_1, \dots, \alpha_r\}$ en si mismo, lo cual da una permutación dado que σ es biyectiva.

Puesto que σ permuta los elementos α_i, también permuta los factores $(x - \alpha_i)$ de h, esto muestra que los coeficientes de h quedan fijos por $\mathrm{Gal(L/K)}$, y por lo tanto están en el campo fijo, el cual es L según lo dijimos antes. Entonces $h \in K[x]$, según se dijo.

A continuación, sea $g \in K[x]$ el factor irreducible de h que se anula en α. Por el Teorema 10 de la sección 1 sabemos que $\sigma(\alpha)$ tambien es una raíz de g para todo $\sigma \in \mathrm{Gal(L/K)}$. Dado que los α_i son elementos distintos de L obtenidos mediante la acción de $\mathrm{Gal(L/K)}$, tenemos que $h|g$. Sigue entonces que h es irreducible sobre F, puesto que g es el factor irreducible de h.

Concluimos entonces que $h \in K[x]$ es el polinomio minimal de α sobre K, puesto que h es irreducible sobre K y tiene a α como raíz. Entonces, si $f \in K[x]$ es irreducible y tiene a $\alpha \in L$ como raíz, entonces f es, salvo una constante, el polinomio h definido anteriormente. Entonces f se descompone completamente sobre L, sigue entonces que L es una extensión normal de K. Por otro lado, si $\alpha \in L$, su polinomio minimal es el polinomio h. Entonces α es separable sobre K,

dado que h lo es. Sigue entonces que L es una extensión separable de K. Esto completa la demostración del teorema.

§ 4 El teorema fundamental de la Teoría de Galois.

El objetivo principal de esta sección es demostrar el Teorema Fundamental da la Teoría de Galois, el cual describe precisamente la relación entre los subcampos de L que contienen a K y los subgrupos H del Grupo de Galois $\mathrm{Gal(L/K)}$.

Teorema 1. Sea L una extensión de Galois de un campo K, y sea E un campo de L que contiene a K. Si $\delta \in \mathrm{Gal(L/K)}$, entonces $\Gamma\big(\delta(E)\big) = \delta\Gamma(E)\delta^{-1}$.

Demostración: Escribamos $\delta(E) = E^{\prime}$, $\Gamma(E) = H$ y $\Gamma\big(E^{\prime}\big) = H^{\prime}$. Debemos mostrar que $H^{\prime} = \delta H \delta^{-1}$. En este sentido, sea $\theta \in H$; mostraremos que $\delta\theta\delta^{-1} \in H^{\prime}$. Sea $z^{\prime} \in E^{\prime}$ y sea z el único elemento de E tal que $\delta(z) = z^{\prime}$. Entonces, dado que θ fija todos los elementos de E,

$$(\delta\theta\delta^{-1})\big(z^{\prime}\big) = (\delta\theta\delta^{-1}\delta)(z) = \delta\big(\theta(z)\big) = \delta(z) = z^{\prime}$$

y entonces $\delta\theta\delta^{-1} \in H^{\prime}$. Hemos mostrado que $\delta H \delta^{-1} \subseteq H^{\prime}$.

Para mostrar la inclusión opuesta, sea $\theta^{\prime}$ un elemento arbitrario de $H^{\prime}$, y sea $z \in E$. Entonces $\delta(z) \in E^{\prime}$, entonces $\theta^{\prime}\big(\delta(z)\big) = \delta(z)$. Entonces:

$$\big(\delta^{-1}\theta^{\prime}\delta\big)(z) = (\delta^{-1}\delta)(z) = z$$

De esta forma $\delta^{-1}\theta^{\prime}\delta \in \Gamma(E) = H$. Hemos mostrado que $\delta^{-1}H^{\prime}\delta \subseteq H$, de lo cual sigue inmediatamente que $H^{\prime} \subseteq \delta H \delta^{-1}$.

Teorema 2. (Teorema fundamental de la teoría de Galois).

Sea L una extensión de Galois finita del campo K. Entonces:

1. $[L:K] = |\mathrm{Gal(L/K)}|$

2. Para todos los subcampos E de L que contienen a K y para todo subgrupo H del Grupo de Galois $\mathrm{Gal(L/K)}$

$$\Phi\big(\Gamma(E)\big) = E \qquad \text{y} \qquad \Gamma\big(\Phi(H)\big) = H$$

3. Si E es un subcampo de L que contienen a K, entonces

$$|\Gamma(E)| = [L:E] \quad \text{y} \quad [E:K] = |\mathrm{Gal(L/K)}|/|\mathrm{Gal(L/E)}|$$

4. Un subcampo E de L que contienen a K es una extensión normal de K si y solo si $\Gamma(E)$ es un subgrupo normal de Grupo de Galois $\mathrm{Gal(L/K)}$

5. Si un subcampo E de L que contienen a K es una extensión normal de K, entonces el Grupo de Galois $\mathrm{Gal(E/K)}$ es isomorfo al grupo cociente $\mathrm{Gal(L/K)}/\Gamma(E)$.

Demostración:

1. Como sabemos, este resultado ya fue demostrado en la sección 3 de este capitulo, sin embargo es agregado aquí puesto que en la mayoría de los textos viene dado de esta forma.

2. El Teorema 8 de la sección 5, Capitulo 1, implica que L es una extensión normal de E. Por otra parte, el Teorema 10 de la sección 6, capítulo 1, nos dice que L es una extensión separable de E. Luego, L una extensión de Galois de E. A su vez, teniendo en cuenta que $\Gamma(E) = \mathrm{Gal(L/E)}$, sigue del Teorema 2, sección 3 que

$$\Phi\big(\Gamma(E)\big) = E \tag{3.9}$$

Que también se puede escribir en la forma:

$$\Phi\big(\Gamma(E)\big) = (\Phi\Gamma)(E) = E$$

Sea H un subgrupo del Grupo de Galois $\mathrm{Gal(L/K)}$. Por el Teorema 14 de la sección 1, y por (3.9) tenemos que:

$$\Gamma\big(\Phi(H)\big) = (\Gamma\Phi)(H)$$

$$\Phi\left(\Gamma\big(\Phi(H)\big)\right) = (\Phi\Gamma\Phi)(H) = \Phi(H)$$

Del mismo modo, operando en (3.9) con Γ llegamos a las relaciones:

$$(\Phi\Gamma\Phi)(H) = \Phi(H) \quad \text{y} \quad (\Gamma\Phi\Gamma)(E) = \Gamma(E) \tag{3.10}$$

Ahora, por el Teorema 1 de la sección 3, sabemos que

$$H \subseteq \Gamma\big(\Phi(H)\big)$$

Llamemos H' al grupo $\Gamma\big(\Phi(H)\big)$, entonces de las relaciones (3.10) tenemos:

$$\Phi(H) = \Phi\left(\Gamma\big(\Phi(H)\big)\right) = \Phi\big(H'\big)$$

Del Teorema 1 de la sección 2, tenemos entonces que:

$$|H| = |L\colon \Phi(H)| = \big|L\colon \Phi\big(H'\big)\big| = \big|H'\big|$$

Esto, junto con (3.10) y la finitud de Gal(L/K), nos dice que $H = H'$. Esto es:

$$H = \Gamma\big(\Phi(H)\big) \tag{3.11}$$

Luego, las funciones Γ y Φ son mutuamente inversas, esto es, bajo las condiciones del teorema, existe una biyección entre los campos intermedios de K y L y los subgrupos H del Grupo de Galois.

3. Como dijimos anteriormente, L una extensión de Galois de E. Por lo tanto, por el Corolario 4 de la sección 2, $|\Gamma(E)| = [L\colon E]$. Luego, por el Teorema de la Torre de Extensiones tenemos que:

$$[E\colon K] = [L\colon K]/[L\colon E]$$

Y según lo anterior, sigue que

$$[E\colon K] = \mathrm{Gal(L/K)}/|\Gamma(E)|$$

4. Supongamos que E es una extensión normal. Sea $\delta \in \mathrm{Gal(L/K)}$, y sea $\delta^{'}$ la restricción de δ a E. Entonces $\delta^{'}$ es un monomorfismo de E en L y además, por el Teorema 5, sección ,1 es un K −automorfismo de E. Por otro lado, dado que $\delta(E) = \delta^{'}(E) = E$, sigue, por el Teorema 1 que

$$\Gamma(E) = \Gamma\big(\delta(E)\big) = \delta\Gamma(E)\delta^{-1}$$

Entonces $\Gamma(E)$ es un subgrupo normal de $\mathrm{Gal(L/K)}$.

Por el contrario, supongamos que $\Gamma(E)$ es un subgrupo normal de $\mathrm{Gal(L/K)}$. Sea δ_1 un K −automorfismo de E en L. Por el Teorema 3 de la sección 1, este se extiende a un K −automorfismo δ de L. La normalidad de $\Gamma(E)$ dentro de $\mathrm{Gal(L/K)}$ significa que $\delta\Gamma(E)\delta^{-1} = \Gamma(E)$, y entonces por el Teorema 1,

$$\Gamma\big(\delta(E)\big) = \Gamma(E)$$

Dado que Γ es biyectivo, sigue que $\delta(E) = \delta_1(E) = E$. Entonces δ_1 es un K −automorfismo de E. Hemos mostrado entonces que cada K −automorfismo de E en L es un K −automorfismo de E. Luego, del Teorema 5 de la sección 1, sigue que E es normal.

5. Supongamos que E es normal y, como lo hicimos mas arriba, sea $\delta^{'}$ la restricción E del K −automorfismo δ de L. Hemos visto que $\delta^{'} \in \mathrm{Gal(E/K)}$. Sea $\Theta\colon \mathrm{Gal(L/K)} \to \mathrm{Gal(E/K)}$ definido por

$$\Theta(\delta) = \delta^{'}$$

Entonces Θ es un homomorfismo de grupos: para todo $\delta_1, \delta_2 \in \mathrm{Gal(L/K)}$, $\Theta(\delta_1) = \delta_1{}^{'}$ y $\Theta(\delta_2) = \delta_2{}^{'}$, y para todo $z \in E$,

$$\begin{aligned}([\Theta(\delta_1)][\Theta(\delta_2)])(z) &= \big(\delta_1{}^{'}\delta_2{}^{'}\big)(z) = \delta_1{}^{'}\big(\delta_2(z)\big) = \delta_1\big(\delta_2(z)\big) = (\delta_1\delta_2)(z) \\ &= \big(\Theta(\delta_1\delta_2)\big)(z)\end{aligned}$$

Entonces

$$[\Theta(\delta_1)][\Theta(\delta_2)] = \Theta(\delta_1\delta_2)$$

El Kernel de este homomorfismo es el conjunto de todos los $\delta \in \mathrm{Gal(L/K)}$, tale que $\delta^{'}$ es la identidad en E, y este no es otro que $\Gamma(E)$. Luego, por el Primer Teorema del Homomorfismo resulta que:

$$\mathrm{Gal(E/K)} \simeq \mathrm{Gal(L/K)} \,/\Gamma(E)$$

De este modo hemos demostrado el Teorema Fundamental de la Teoría de Galois.

Para finalizar, veamos algunos teoremas, el primero debido a Lagrange, que serán utilizados en el capítulo final.

Teorema 3. Sea K un campo de característica cero, y sea $f \in K[x]$. Sea

$$L = K(\alpha_1, \dots, \alpha_n)$$

un campo de descomposición para f sobre K. Sea M un campo que contiene a K, y sea N un campo de descomposición para f sobre M. Entonces, mediante un isomorfismo, L es un subcampo de N y $\mathrm{Gal}(N/M) \simeq \mathrm{Gal}(L/M \cap L)$.

Demostración: EL campo N es una extensión de M, y por lo tanto de K, tal que f se descompone completamente en $N[x]$. Entonces, por definición de campo de descomposición, L es, mediante un isomorfismo, un subcampo de N, y podemos escribir a N en la forma $M(\alpha_1, \dots, \alpha_n)$.

Sea $H = \mathrm{Gal}(N/M)$, y sea $\gamma \in H$. Entonces la restricción $\gamma^{'}$ de γ a L es un monomorfismo de L en N. Desde que γ fija los elementos de M, ciertamente deja fijo los elementos de K; entonces $\gamma^{'}$ lo hace también. No obstante, dado que γ transforma cada raíz de f en otra raíz de f, también debe hacerlo $\gamma^{'}$. La conclusión es que $\gamma^{'}$ es un momomorfismo de L sobre sí mismo. Desde que γ es un automorfismo de $N = M(\alpha_1, \dots, \alpha_n)$, cada raíz α_i de f es la imagen de alguna raíz de f bajo γ, y también bajo $\gamma^{'}$. Por ende $\gamma^{'}$ es sobreyectivo. De esto sigue que $\gamma^{'}$ es un automorfismo de L que deja fijo los elementos de K.

De este modo tenemos una función θ de H en el grupo $\mathrm{Gal}(L/K)$, dado por $\theta(\gamma) = \gamma'$. Esta función es biyectiva puesto que si $\delta \in H$ y $\gamma' = \delta'$, entonces γ' y δ' actuan de manera idéntica sobre las raíces $\alpha_1, \dots, \alpha_n$, y entonces $\gamma = \delta$. Tambien es un homomorfismo de grupos puesto que la restricción de $\gamma\delta$ a L es $\gamma'\delta'$. Entonces tenemos que $H \simeq \theta(H)$.

Queda por mostrar que la imagen de θ es el subgrupo $\mathrm{Gal}(L/M \cap L)$ de G. Dado que cada γ en G deja fijo los elementos de M, es claro que cada δ' deja fijo los elementos de $M \cap L$. Entonces $M \cap L \subseteq \Phi\big(\theta(H)\big)$, y por La Correspondencia de Galois

$$\theta(H) \subseteq \mathrm{Gal}(L/M \cap L) \tag{3.12}$$

Sea x un elemento de L que no pertenece a $M \cap L$. Entonces $x \notin M$. Desde que M es el campo cuyos elementos son dejados fijos por cada elemento H, existe un elemento β en H para el cual $\beta(x) \neq x$. Entonces $\big(\theta(\beta)\big)(x) \neq x$ y entonces $x \notin \Phi\big(\theta(H)\big)$. Hemos probado que $\Phi\big(\theta(H)\big) \subseteq M \cap L$. De esto sigue que

$$\mathrm{Gal}(L/M \cap L) \subseteq \theta(H) \tag{3.13}$$

De (3.12) y (3.13) sigue que

$$\mathrm{Gal}(L/M \cap L) = \theta(H) \simeq H = \mathrm{Gal}(N/M)$$

De esta manera queda demostrado el teorema.

Teorema 4. Sea K un campo de característica cero, y sea L el campo de descomposición sobre K del polinomio $x^p - 1$, donde p es primo. Entonces el Grupo de Galois $\mathrm{Gal}(L/K)$ es cíclico.

Demostración: Sea ω una raíz primitiva p −ésima de la unidad en L, y sea $\sigma \in \mathrm{Gal}(L/K)$. Entonces $L = K(\omega)$. Sabemos que $\sigma(\omega)$ también debe ser una raíz primitiva p −ésima de la unidad, entonces

$$\sigma \in \mathrm{Gal}(L/K) \text{ si y solo si } \sigma(\omega) = \omega^{k_\sigma}, \text{ donde } (k_\sigma : p) = 1 \tag{3.14}$$

Dado que $\omega^r = \omega^s$ si y solo si $r \equiv s, \mathrm{mod}(p)$, tenemos una función inyectiva de $\mathrm{Gal}(L/K)$ en $\{\bar{1}, \bar{2}, \dots, \bar{p}\} = \mathbb{Z}_p$.

Sean $\sigma, \tau \in \mathrm{Gal}(L/K)$. Entonces:

$$(\sigma\tau)(\omega) = \sigma(\omega^{k_\tau}) = (\omega^{k_\tau})^{k_\sigma} = \omega^{k_\sigma k_\tau} = (\omega^{k_\sigma})^{k_\tau} = (\tau\sigma)(\omega) \tag{3.15}$$

De esto, vemos que la función anterior es un monomorfismo. Por otra parte, de (3.14) vemos que también es sobreyectivo, luego $\mathrm{Gal}(L/K)$ es isomorfo a $\{\bar{1}, \bar{2}, \dots, \bar{p}\} = \mathbb{Z}_p$, por lo tanto $|\mathrm{Gal}(L/K)| = p$ y dado que si un grupo es de orden primo, entonces es cíclico, concluimos que $\mathrm{Gal}(L/K)$ es cíclico.

Como vimos en el teorema anterior, en ciertas circunstancias el Grupo de Galois es un grupo cíclico. Esto motiva la siguiente definición.

Definición 5. Sea L una extensión del campo K. Decimos que L una *extensión cíclica* de K si L es normal y separable y el Grupo de Galois $\mathrm{Gal}(L/K)$ es un grupo cíclico.

De acuerdo al Teorema 4, tenemos que si p es primo, entonces el campo de descomposición sobre K del polinomio $x^p - 1$ es una extensión cíclica de K.

Veamos ahora algunas cuestiones relacionadas con las extensiones cíclicas. Empecemos de este modo.

Sea L una extensión, de grado finito n, del campo K (de característica cero), y sea N la clausura normal de L. Por el Teorema 2 de la sección 2, existen exactamente n K −automorfismos distintos $\tau_1, \dots, \tau_n$ de L en N. Definamos entonces la norma y la traza de la extensión L como sigue.

Definición 6. Para cada elemento x de L, definimos la norma $N_{L/K}(x)$ y la traza $Tr_{L/K}(x)$ mediante

$$N_{L/K}(x) = \prod_{i=1}^{n} \tau_i(x), \qquad Tr_{L/K}(x) = \sum_{i=1}^{n} \tau_i(x) \tag{3.16}$$

A continuación demostraremos en siguiente teorema debido a Hilbert (1862 – 1943).

Teorema 7. Sea L una extensión cíclica del campo K, y sea τ un generador del grupo cíclico $\mathrm{Gal}(L/K)$. Si $x \in L$, entonces $N_{L/K}(x) = 1$ si y solo si existe un elemento $y \in L$ tal que $x = y/\tau(y)$, y $Tr_{L/K}(x) = 0$ si y solo si existe un elemento $z \in L$ tal que $x = z - \tau(z)$.

Demostración: Sea $[L:K] = n$, entonces $\tau^n = Id$, el automorfismo identidad. Supongamos primero que $x = y/\tau(y)$; entonces

$$N_{L/K}(x) = Id(x)\tau(x)\cdots\tau^{n-1} = \frac{y}{\tau(y)}\frac{\tau(y)}{\tau^2(y)}\cdots\frac{\tau^{n-1}(y)}{\tau^n(y)} = 1$$

Por el contrario, supongamos que $N_{L/K}(x) = 1$. Entonces

$$x^{-1} = \tau(x)\tau^2(x)\cdots\tau^{n-1}(x) \tag{3.17}$$

Por el Lema de Dedekind, el conjunto $\{Id, \tau, \tau^2, \dots, \tau^{n-1}\}$ es linealmente independiente sobre L, y entonces la función

$$Id + x\tau + x\tau(x)\tau^2 + \cdots + x\tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}$$

es no nula, lo que quiere decir que, para algún t en L, el elemento

$$y = t + x\tau(t) + x\tau(x)\tau^2(t) + \cdots + x\tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t)$$

Es distinto de cero. Aplicando al automorfismo τ tenemos

$$\tau(y) = \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots$$
$$\cdots + \tau(x)\tau^2(x)\tau^3(x)\cdots\tau^{n-1}(x)\tau^n(t) \tag{3.18}$$

Notemos también que

$$x^{-1}y = x^{-1}t + \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots$$
$$\cdots + \tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t)$$

Se puede escribir en la forma

$$x^{-1}y = \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots + \tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t)$$
$$+x^{-1}\tau^n(t) \qquad (1.4)$$

Comparando (3.18) con (3.19) y teniendo en cuenta la igualdad (3.17), resulta que $\tau(y) = x^{-1}y$, o sea $x = y/\tau(y)$ como se quería.

Análogamente se demuestra la parte que concierne a $Tr_{L/K}(x)$.

Sea K un campo de característica cero y sea $x^m - a \in K[x]$. Sea L el campo de descomposición de $f = x^m - a$ sobre K. Por el Teorema 6, seccion 6 del capítulo 1, f posee raices distintas, digamos $\alpha_1, \dots, \alpha_m$ en L, y entonces L contiene las raices diatintas

$$\alpha_1\alpha_1^{-1}, \dots, \alpha_m\alpha_1^{-1} \qquad (3.20)$$

del polinomio $x^m - 1$. Supongamos, sin perder generalidad, que $\alpha_2\alpha_1^{-1} = \omega$ es una raiz m −ésima primitiva de la unidad. Entonces, en algun orden, los elementos listados en (3.20) son los elementos $1, \omega, \dots, \omega^{m-1}$, entonces podemos renombrar las raices de $x^m - a$ en L del siguiente modo

$$\alpha_1, \omega\alpha_1, \dots, \omega^{m-1}\alpha_1 \qquad (3.21)$$

Entonces, sobre L, tenemos

$$x^m - a = (x - \alpha_1)(x - \omega\alpha_1)\cdots(x - \omega^{m-1}\alpha_1)$$

Tenemos entonces que

$$K \subseteq K(\omega) \subseteq L$$

y el campo intermedio $K(\omega)$ contiene todas las raíces de la unidad. Hemos establecido de esta forma, parte del siguiente teorema:

Teorema 8. Sea $f = x^m - a \in K[x]$, donde K es un campo de característica cero, y sea L un campo de descomposición de f sobre K. Entonces L contiene un elemento ω, una raíz primitiva m –ésima de la unidad. El Grupo de Galois $\mathrm{Gal}(L/K(\omega))$ es cíclico y su orden divide a m. El orden es igual a m si y solo si f es irreducible sobre $K(\omega)$.

Demostración: Si α es una raíz de f, entonces, sobre L,

$$f = (x - \alpha)(x - \alpha\omega) \cdots (x - \omega^{m-1}\alpha)$$

donde ω es una raíz primitiva m –ésima de la unidad. Entonces $L = K(\omega, \alpha)$, y un automorfismo σ en $\mathrm{Gal}(L/K(\omega))$ esta determinado por su acción sobre α. La imagen debe ser una raíz de f, y entonces

$$\sigma(\alpha) = \omega^{k_\sigma}\alpha$$

Para algún k_σ en $\{0,1, \dots, m-1\}$. Si τ es otro elemento de $\mathrm{Gal}(L/K(\omega))$, entonces

$$(\sigma\tau)(\alpha) = \sigma(\omega^{k_\tau}\alpha) = \omega^{k_\tau}\omega^{k_\sigma}\alpha = \omega^{k_\tau + k_\sigma}\alpha$$

Y entonces $\sigma \mapsto \bar{k}_\sigma$ es un homomorfismo sobre el grupo aditivo $\mathbb{Z}_m$ de los enteros modulo m. No obstante, $\bar{k}_\sigma = \bar{0}$ si y solo si m divide a k_σ, esto es, si y solo si $\sigma(\alpha) = \alpha$.

El Kernel del homomorfismo $\sigma \mapsto \bar{k}_\sigma$ es la identidad en $\mathrm{Gal}(L/K(\omega))$, y entonces $\mathrm{Gal}(L/K(\omega))$ es isomorfo a un subgrupo del grupo aditivo $\mathbb{Z}_m$ y dado que este último conjunto bajo la adición es cíclico y además que todo subgrupo de un grupo cíclico es cíclico, sigue que $\mathrm{Gal}(L/K(\omega))$ es un grupo cíclico.[1]

1- Véase Basic Algebra de Nathan Jacobson, Teorema 1.3, pág. 45.

Supongamos ahora que $f = x^m - a$ es irreducible sobre $K(\omega)$. Entonces por el Corolario 4 de la sección 2 y el Teorema 2 de la sección 4, capítulo 1, sigue

$$|\mathrm{Gal}(L/K(\omega))| = [L: K(\omega)] = \mathrm{Grad}(f) = m$$

Y entonces $\mathrm{Gal}(L/K(\omega)) \simeq \mathbb{Z}_m$. Por el contrario, si f no es irreducible sobre $K(\omega)$, entonces tiene un factor, que es un polinomio mónico g tal que $\mathrm{Grad}(g) < m$. Si ρ es una raíz de g en L, entonces

$$x^m - a = (x - \rho)(x - \omega\rho) \cdots (x - \omega^{m-1} \rho)$$

Y entonces $L = K(\omega, \rho)$ es un campo de descomposición para f sobre $K(\omega)$.

Entonces

$$|\mathrm{Gal}(L/K(\omega))| = [L: K(\omega)] = \mathrm{Grad}(g) < m$$

Y entonces $\mathrm{Gal}(L/K(\omega))$ es isomorfo a un subgrupo propio de $\mathbb{Z}_m$

Teorema 9. Sea K un campo de característica cero, y sea m un entero positivo, y supongamos que el polinomio $x^m - 1$ se descompone totalmente sobre K. Sea L una extensión cíclica de K tal que $[L: K] = m$. Entonces existe un elemento $a \in K$ tal que $x^m - a$ es irreducible sobre K y L es el campo de descomposición de $x^m - a$. Lo que es más, L es generado sobre K por una sola raíz de $x^m - a$.

Demostración: Bajo estas condiciones se tiene que $K = K(\omega)$. Sea τ el generador del grupo cíclico $G = \mathrm{Gal}(L/K)$. Sea ω una raíz m −ésima primitiva de la unidad en K. Ciertamente cada raíz m −ésima de la unidad queda fija por cualquier automorfismo en G. Luego $N_{L/K}(x) = \omega^m = 1$. Del Teorema 7 deducimos que existe un elemento $z \in L$ tal que $\omega = z/\tau(z)$. Por lo tanto

$$\tau(z) = \omega^{-1} z \tag{3.22}$$

y sigue que fácilmente que

$$\tau^k(z) = \omega^{-k} z \neq z, \ (k = 1,2, \dots, m-1) \tag{3.23}$$

Entonces $\Gamma[K(z)] = \{Id\}$ y por lo tanto, dado que L es una extensión cíclica (y por definición normal) podemos aplicar el Teorema Fundamental de la Teoría de Galois para obtener:

$$K(z) = \Phi(\Gamma[K(z)]) = \Phi(\{Id\}) = L$$

De (3.23) deducimos que $\tau(z^m) = [\tau(z)]^m = \omega^{-m}z^m = z^m$, e inmediatamente sigue que $\tau^k(z^m) = z^m$ para $K = 0,1,\dots,m-1$. Entonces $z^m \in \Phi(G) = K$. Denotemos a z^m por a. Entonces z es una raiz del polinomio $x^m - a$ en $K[x]$, ademas el polinomio minimal g de z sobre K es un factor de $x^m - a$. Dado que $[K(z):K] = [L:K] = m$, el polinomio minimal g debe ser, no otro sino $x^m - a$. Sigue de este modo que $x^m - a$ es irreducible sobre K. Por otra parte, las raices de $x^m - a$ son los elementos $\omega^{-k}z$, $(k = 0,1,\dots,m-1)$, todas pertenecientes a L, de ese modo L es el campo de descomposición de $x^m - a$ sobre K.

§ 5 Permutación de las raíces y el Grupo de Galois.

En esta sección mostraremos la relación entre el Grupo de Galois y las permutaciones. Supondremos en entonces que L es el campo de descomposición de un polinomio separable $f \in K[x]$. El objetico principal es interpretar el Grupo de Galois, $\mathrm{Gal}(L/K)$, en termino de las permutaciones de las raíces del polinomio f.

Sea $n =$Grad(f). Entonces en $K[x]$, podemos escribir a f en la siguiente forma:

$$f = c(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

Donde $c \neq 0$ y $\alpha_1, \cdots, \alpha_n \in L$ son distintas. Bajo estas condiciones tenemos la función:

$$\mathrm{Gal}(L/K) \to S_n$$

Definida como sigue:

Sea $\sigma \in \mathrm{Gal}(L/K)$, el Teorema 10, sección 1, implica que $\sigma(\alpha_i)$ tambien es una raíz de f, dado que α_i lo es, del mismo modo, $\sigma(\alpha_i) = \alpha_{\tau(i)}$, para $\tau(i) \in \{1, \dots, n\}$. Notemos que $\tau(i)$ queda unívocamente determinado puesto que $\alpha_1, \dots, \alpha_n$ son todas distintas. Ademas

$$\tau: \{1, \dots, n\} \to \{1, \dots, n\}$$

Es inyectiva puesto que σ tambien lo es. Esto ocurre puesto que al ser L el campo de descomposición de f, así, $L = K(\alpha_1, \dots, \alpha_n)$ y es el menor campo que contiene a $\alpha_1, \dots, \alpha_n$, luego, al ser $\sigma \in \mathrm{Gal}(L/K)$ un automorfismo, sigue lo que acabamos de decir. De esto, deducimos que τ es una permutación, i.e. $\tau \in S_n$. Esto define la función $\mathrm{Gal}(L/K) \to S_n$.

Teorema 1. La función de $\mathrm{Gal}(L/K) \to S_n$ descripta en el párrafo anterior descripta es un homomorfismo de grupos inyectivo (i.e. es un monomorfismo).

Demostración: Supongamos que $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$ corresponden a $\tau_1, \tau_2 \in S_n$, según la correspondencia anterior. Esto significa que

$$\sigma_1(\alpha_i) = \alpha_{\tau_1(i)} \quad \text{y} \quad \sigma_2(\alpha_i) = \alpha_{\tau_2(i)}$$

Entonces:

$$[\sigma_1 o \sigma_2](\alpha_i) = \sigma_1\big(\sigma_2(\alpha_i)\big) = \sigma_1\big(\alpha_{\tau_2(i)}\big) = \alpha_{\tau_1(\tau_2(i))} = \alpha_{\tau_1\tau_2(i)}$$

Esto muestra que $\sigma_1 o \sigma_2$ se corresponde con $\tau_1\tau_2$, asi que la correspondencia en cuestión es un homomorfismo de grupos. Queda por demostrar que el homomorfismo descripto es inyectivo. Esto sigue inmediatamente dado que $L = K(\alpha_1, \dots, \alpha_n)$ y además, por el Teorema 10 de la sección 1 cada σ queda unívocamente determinado por sus valores en $\alpha_1, \dots, \alpha_n$.

Notemos que el teorema anterior establece que se puede identificar al Grupo de Galois con un subgrupo del grupo simétrico. Más adelante veremos bajo que

condiciones el Grupo de Galois coincide con el grupo simétrico. Esto último será esencial en cuanto a la solubilidad de ecuaciones.

Capítulo 4

Grupos y Ecuaciones

Finalmente llegamos al último capítulo de esta presentación. En las páginas siguientes demostraremos uno de los resultados más importantes de la Teoría de la Resolución de Ecuaciones, y por que no de la Historia de la Matemática. El mismo se trata de la imposibilidad de hallar una fórmula explícita para la ecuación general de quinto grado y de grados superiores, equivalente a la fórmula resolvente de las ecuaciones de segundo, tercer y cuarto grado, que exprese sus soluciones.

§ 1 Polinomios simétricos elementales.

En esta sección veremos la relación que existe entre las raíces de un polinomio $f \in K[x]$ y sus coeficientes. Dado que K es un campo, cada elemento del mismo es inversible en K, por lo que al multiplicar por una constante adecuada, podemos hacer que el coeficiente de la potencia más alta del polinomio f sea igual a 1. Esto es, sin perder generalidad podemos trabajar con polinomios mónicos.

Empecemos a ver de qué se trata esta relación entre las raíces de un polinomio y sus coeficientes con los polinomios mónicos de tercer y cuarto grado.

Supongamos que $f = x^3 + a_1x^2 + a_2x + a_3 \in K[x]$ tiene raíces $\alpha_1, \alpha_2, \alpha_3 \in K$. Entonces

$$f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

Si expandimos esta expresión y la comparamos con los coeficientes a_1, a_2 y a_3 entonces podemos expresar los coeficientes de $f(x)$ en términos de sus raíces de la siguiente forma:

$$a_1 = -(\alpha_1 + \alpha_2 + \alpha_3)$$

$$a_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3$$

$$a_3 = -\alpha_1\alpha_2\alpha_3$$

Ahora para $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \in K[x]$ un cálculo similar muestra que si $f(x)$ tiene sus raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in F$ entonces:

$$a_1 = -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4),$$

$$a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4,$$

$$a_3 = -(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4),$$

$$a_4 = \alpha_1\alpha_2\alpha_3\alpha_4$$

Note que, salvo un signo, a_1 es la suma de las raíces, a_2 está formado por la suma de los productos de las raíces tomados de a dos y a_3 está formado por la suma de las raíces tomadas de a tres. Este patrón se generaliza en la siguiente definición.

Definición 1. Sean $x_1, x_2, \dots, x_n$ un número finito de variables sobre K. Entonces

$$\sigma_1 = x_1 + \cdots + x_n$$

$$\sigma_2 = \sum_{i<j} x_i x_j$$

$$\vdots$$

$$\sigma_r = \sum_{i_1<\cdots<i_r} x_{i_1} x_{i_2} \cdots x_{i_r}$$

$$\vdots$$

$$\sigma_n = x_1 x_2 \cdots x_n$$

Son los *polinomios simétricos elementales.* Entonces $\sigma_1, \sigma_2, \dots, \sigma_n \in K[x_1, x_2, \dots, x_n]$, esto es, $\sigma_i = \sigma_i(x_1, x_2, \dots, x_n), 1 \leq i \leq n$.

La siguiente propiedad es una de las propiedades claves de los polinomios simétricos.

Teorema 2. Sean $x_1, x_2, \dots, x_n$ un número finito de variables sobre F. Entonces, dada otra variable x, tenemos:

$$\begin{aligned}(x - x_1)(x - x_2) \cdots (x - x_n) \\ = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^r \sigma_r x^{n-r} + \cdots + (-1)^n \sigma_n \qquad (4.1)\end{aligned}$$

Demostración: La demostración se basa en multiplicar los n factores del lado izquierdo de (4.1) y comparar los coeficientes obtenidos para cada potencia de x con los con los polinomios simetricos elementales dados en la Definición 1. Por ejemplo, el término constante es obviamente el producto de todas las constantes de cada factor, esto es $(-x_1)(-x_2) \cdots (-x_n) = (-1)^n x_1 x_2 \cdots x_n = (-1)^n \sigma_n$. Similarmente es fácil ver que el coeficiente de x^{n-1} es $-x_1 - x_2 - \cdots - x_n = -\sigma_1$, puesto que para obtener la potencia $n - 1$ de x, i.e. x^{n-1}, se debe multiplicar la x de $n - 1$ factores en el lado izquierdo de (4.1) y al multiplicar esta potencia de x por el término constante del factor que falta, digamos el factor r, es decir el factor $(x - x_r)$, queda determinado un término de la forma $-x_r x^{n-1}$. Sumando todos estos términos llegamos a que el coeficiente de x^{n-1} es $-\sigma_1$ como se dijo anteriormente.

Del mismo modo, los términos que involucran a x^{n-r}, se obtiene al multiplicar esta indeterminada en exactamente $n - r$ factores en (4.1). Luego al multiplicar esta potencia por las constantes $-x_{i_1}, -x_{i_2}, \cdots, -x_{i_r}$ de los r factores restantes se obtiene un término de la forma

$$(-x_{i_1})(-x_{i_2}) \cdots (-x_{i_r}) x^{n-r} = (-1)^r x_{i_1} x_{i_2} \cdots x_{i_r} x^{n-r}$$

Luego de computar todas las posibles elecciones de las r constantes, que son un total de $\binom{n}{r}$, $-x_{i_1}, -x_{i_2}, \cdots, -x_{i_r}$ y sumar todos los términos en x^{n-r}, sigue que el coeficiente de x^{n-r} es

$$(-1)^r \sum_{i_1<\cdots<i_r} x_{i_1} \cdots x_{i_r} = (-1)^r \sigma_r.$$

Esto completa la demostración.

El Teorema 2 tiene la siguiente, y muy útil, aplicación. Suponga que un polinomio mónico $f = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n \in K[x]$ tiene sus raíces $\alpha_1, \alpha_2, \cdots, \alpha_n$ en un campo L más grande que F, esto es L es su campo de descomposición, luego f se puede escribir en la forma

$$f = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n = (x - \alpha_1) \cdots (x - \alpha_n)$$

Por otra parte, dado que la evaluación es un homomorfismo de campos,[1] podemos evaluar la identidad (4.1) en $x_1 = \alpha_1, \cdots x_n = \alpha_n$ y teniendo en cuenta que $\sigma_i = \sigma_i(x_1, x_2, \dots, x_n), 1 \leq i \leq n$ según lo visto en la Definición 1 obtenemos

$$(x - \alpha_1) \cdots (x - \alpha_n) = x^n - \sigma_1(\alpha_1, \cdots \alpha_n)x^{n-1} + \cdots$$
$$+(-1)^{n-1}\sigma_{n-1}(\alpha_1, \cdots \alpha_n)x + \cdots + (-1)^n \sigma_n(\alpha_1, \cdots \alpha_n)$$

De esta forma hemos demostrado el siguiente corolario del Teorema 2:

Corolario 3. Sea $f = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n$ un polinomio mónico de grado $n > 0$ con coeficientes en el campo K. Si f tiene sus raíces $\alpha_1, \alpha_2, \cdots, \alpha_n$ en un campo L, tal que $K \subset L$, entonces los coeficientes de f se expresan en términos de sus raíces de la siguiente forma

$$a_r = (-1)^r \sigma_r(\alpha_1, \cdots \alpha_n), \quad \text{con } r = 1, \dots, n.$$

1- Si $f \in K[x_1, \dots x_n]$ y $\alpha_1, \dots \alpha_n \in R$, siendo R un campo que contiene a K, la correspondencia definida del siguiente modo:

$$K[x_1, \dots x_n] \to R \quad \text{y} \quad f(x_1, \dots x_n) \longmapsto f(\alpha_1, \dots \alpha_n) \in R$$

caracteriza un homomorfismo y por tal motivo de lo llama Homomorfismo de Evaluación.

§ 2 Polinomios simétricos.

En la sección anterior introducimos los polinomios simétricos elementales. En esta sección daremos una definición general de polinomios simétricos. Aquí consideraremos los polinomios en varias variables $x_1, x_2, \dots, x_n$ sobre un campo K. Nuestro objetivo principal será demostrar el *Teorema Fundamental de los Polinomios Simétricos*, considerado como la piedra angular de la Teoría de Galois.

Definición 1. Un polinomio $f \in K[x_1, x_2, \dots, x_n]$ es *simétrico* si

$$f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) = f(x_1, \dots, x_n)$$

para toda permutación $\sigma \in S_n$.

Antes de pasar al enunciado y a la demostración del *Teorema Fundamental de los Polinomios Simétricos*, veamos algunas cuestiones relacionadas con los ordenamientos de monomios, que serán utilizadas mas adelante.

Según la Definición 1, el grado total del monomio $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ es la suma $\alpha_1 + \alpha_2 + \cdots + \alpha_n$ y además dijimos que el grado total, $\mathrm{Grad}(f)$, es el máximo de todos los grados de los monomios que forman el polinomio. Ahora, de lo que sabemos de los polinomios en una variable, en ciertas ocasiones es necesario ordenarlo y así por ejemplo

$$f = 5x^5 + \frac{3}{4}x^3 + x^2 - 1 \in \mathbb{Q}[x]$$

Se dice que esta ordenado en forma decreciente. Note que este tipo de ordenamiento de monomios se basa en el orden de los naturales y tiene en cuenta el grado total de cada monomio, así dado que $5 > 3$ implica que $x^5 > x^3$. De este modo, sabiendo que para $a, b \in \mathbb{N}$, con el orden habitual $>$, se cumple necesariamente alguna de las tres condiciones

$$a > b, \qquad a = b, \qquad b > a$$

Y cada una de estas implica, respectivamente, que

$$x^a > x^b, \quad x^a = x^b, \quad x^b > x^a$$

Sin embargo cuando se trabaja con polinomios en más de una variable pueden surgir algunas complicaciones al ordenar los monomios. Por ejemplo considere el polinomio

$$f = x^3y^4 + x^2y^5 + x^7 + y^7 \in \mathbb{Q}[x, y]$$

¿Cómo debemos proceder para ordenar el polinomio f en forma decreciente?

Podemos pensar en ordenarlo según el grado total de cada monomio, como con los polinomios de una variable, sin embargo como se puede ver, todos los monomios de f poseen grado total 7. En vista de esto nos damos cuanta de que cuando se trata de polinomios en más de una variable el ordenamiento de monomios y por ende el de polinomios es más complejo y hay que hallar otros tipos de ordenamiento mas elaborados que nos permitan decidir, dado un par de monomios $x_1^{\alpha_1}x_2^{\alpha_2} \cdots x_n^{\alpha_n}, x_1^{\beta_1}x_2^{\beta_2} \cdots x_n^{\beta_n}$ si

$$x_1^{\alpha_1}x_2^{\alpha_2} \cdots x_n^{\alpha_n} > x_1^{\beta_1}x_2^{\beta_2} \cdots x_n^{\beta_n},$$

$$x_1^{\alpha_1}x_2^{\alpha_2} \cdots x_n^{\alpha_n} = x_1^{\beta_1}x_2^{\beta_2} \cdots x_n^{\beta_n}, \quad \vee$$

$$x_1^{\beta_1}x_2^{\beta_2} \cdots x_n^{\beta_n} > x_1^{\alpha_1}x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

Si bien existen varios tipos de ordenamiento de monomios en varias variables,[1] aquí con el *orden lexicográfico graduado.* El cual se define de la siguiente manera.

Definición 2. (Orden lexicográfico graduado) Sean los monomios $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $x_1^{\beta_1} \cdots x_n^{\beta_n} \in K[x_1, \ldots, x_n]$, diremos que $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ es mayor que $x_1^{\beta_1} \cdots x_n^{\beta_n}$ según el orden lexicográfico graduado, denotado por

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} >_{Grlex} x_1^{\beta_1} \cdots x_n^{\beta_n}$$

1- Un estudio sobre los ordenamientos de monomios puede verse en el capítulo 2 de Ideals Varieties and Algorithms de D. Cox, J. Little y D. O´Shea, ed. 2007.

Sí

1. $\alpha_1 + \cdots + \alpha_n > \beta_1 + \cdots + \beta_n$, o sí

2. $\alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n$ y $\alpha_r > \beta_r$ para algún $0 \leq r \leq n$ y $\alpha_i = \beta_i$ para toda $0 \leq i \leq r - 1$.

Para comparar un monomio con otro, primero se computa el grado total de cada uno, y cuando estos son iguales se comparan los exponentes de la misma variable en cada monomio, siguiendo el orden $x_1 > x_2 > \cdots > x_n$, buscando el primero que difiera. Por ejemplo, en $K[x_1, x_2, x_3]$,

1. $x_1^5 x_2^3 x_3^2 >_{Grlex} x_1^4 x_2^2 x_3^1$ puesto que el grado total de $x_1^5 x_2^3 x_3^2$ es mayor que el grado total de $x_1^4 x_2^2 x_3^1$.

2. $x_1^5 x_2^3 x_3^2 >_{Grlex} x_1^5 x_2^2 x_3^3$ puesto que ambos poseen el mismo grado total, $\alpha_1 = \beta_1 = 5$ y $\alpha_2 = 3 > \beta_2 = 2$.

Una propiedad importante del orden lexicográfico graduado es que hay a lo sumo una cantidad finita de monomios $x_1^{\beta_1} \cdots x_n^{\beta_n}$ tales que

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} >_{Grlex} x_1^{\beta_1} \cdots x_n^{\beta_n} \tag{4.2}$$

Para $\alpha_1, \ldots, \alpha_n$ fijo.

De la definición del orden lexicográfico graduado y de (4.2) se sigue que

$$\alpha_1 + \cdots + \alpha_n \geq \beta_1 + \cdots + \beta_n$$

Por otra parte, dado que $N = \alpha_1 + \cdots + \alpha_n$ es fijo, y $\beta_i \geq 0$ para todo $1 \leq i \leq n$, la desigualdad

$$N = \alpha_1 + \cdots + \alpha_n \geq \beta_1 + \cdots + \beta_n \geq \beta_i \geq 0 \tag{4.3}$$

es verdadera para todo $1 \leq i \leq n$.

De esta forma vemos que hay $N + 1$ valores distintos que pueden asumir las β_i. Estos son $0, 1, 2, \ldots, N - 1, N$. Por lo tanto, hay una cantidad finita de soluciones distintas para la desigualdad (4.3) y cada una de estas determina una n −upla $\beta_1, \ldots, \beta_n$ tal que

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} >_{Grlex} x_1^{\beta_1} \cdots x_n^{\beta_n}$$

Ahora que podemos ordenar monomios, podemos definir el *monomio principal de un polinomio* como el monomio $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ de maximo grado, y *coeficiente principal* como el término del polinomio $c \cdot x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ tal que $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ es el monomio principal.

Por ejemplo, el término principal de $\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \cdots + x_{n-1}x_n$ es x_1x_2. Es fácil convencerse de esto dado que

$$\sigma_2 = \sum_{1 \le i < j \le n} x_i x_j = x_1 \sum_{1 < j \le n} x_j + \sum_{1 < i < j \le n} x_i x_j$$

y luego

$$\sigma_2 = x_1\, x_2 + x_1 \sum_{2 < j \le n} x_j + \sum_{1 < i < j \le n} x_i x_j \tag{4.4}$$

Teniendo en cuenta que todos los monomios de σ_2 poseen grado total 2, el orden lexicográfico graduado nos dice que hay que comparar los exponentes de cada variable en el orden $x_1 > x_2 > \cdots > x_n$. Ahora, es claro que $x_1\, x_2$ es mayor que cualquier monomio del tercer sumando de (4.4) dado que en estos el exponente de x_1 es cero. Con respecto a los monomios del segundo sumando de (4.4), vemos que el exponente de x_1 es igual a uno en todos ellos, del mismo modo que en $x_1\, x_2$, pero dado que en este, el exponente de x_2 es uno y en los demás cero, resulta que $x_1\, x_2$ es el término principal de σ_2 como se dijo antes. Aplicando sucesivamente el mismo argumento podemos ver que $x_1x_2 \cdots x_r$ es el término principal del r −ésimo polinomio simétrico elemental

$$\sigma_r = \sum_{i_1 < \cdots < i_r} x_{i_1} x_{i_2} \cdots x_{i_r}$$

Pasemos ahora a enunciar el *Teorema Fundamental de los Polinomios Simétricos.*

Teorema 3. (***Teorema Fundamental de los Polinomios Simétricos).*** Todo polinomio $f \in K[x_1, x_2, \dots, x_n]$ puede escribirse como un polinomio en los polinomios simétricos elementales $\sigma_1, \dots, \sigma_n$ con coeficientes en F si y solo si f es simétrico.

Demostración: Sea $f \in K[x_1, x_2, \dots, x_n]$ un polinomio simétrico no nulo con coeficiente principal

$$c \cdot x_1^{\alpha_1} \cdots x_n^{\alpha_n} \tag{4.5}$$

Decimos que

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n \tag{4.6}$$

Para probar (4.6) suponga que $\alpha_i < \alpha_{i+1}$ para algún $1 \leq i \leq n-1$. Ahora, el hecho de que f es simetrico implica que intercambiando x_i por x_{i+1}obtenemos el mismo polinomio, i.e.

$$f(x_1, \dots, x_i, x_{i+1}, \dots, x_n) = f(x_1, \dots, x_{i+1}, x_i, \dots, x_n)$$

Puesto que (4.5) es el término principal de f, sigue que

$$c \cdot x_1^{\alpha_1} \cdots x_{i+1}^{\alpha_i} x_i^{\alpha_{i+1}} \cdots x_n^{\alpha_n} \tag{4.7}$$

También es un término de f y posee el mismo grado total que (4.5). Ademas, los exponentes de las primeras $i-1$ variables son iguales, puesto que estas no fueron alteradas. No obstante, x_i tiene exponente α_{i+1} en (4.7) y exponente α_i en (4.5). Luego $\alpha_i < \alpha_{i+1}$ implica que $c \cdot x_1^{\alpha_1} \cdots x_{i+1}^{\alpha_i} x_i^{\alpha_{i+1}} \cdots x_n^{\alpha_n} >_{Grlex} c \cdot x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, pero (4.5) es el término principal de f y debe serlo también luego de permutar las variables, llegamos a una contradicción. Esto prueba (4.6).

Ahora considere

$$g = \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \cdots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n} \tag{4.8}$$

Según (4.6), los números $\alpha_i - \alpha_{i+1} \geq 0$ pata cualquier $1 \leq i \leq n-1$, luego (4.8) es un polinomio. Por otra parte, dado que $x_1 x_2 \cdots x_r$ es el término principal del r −ésimo polinomio simétrico elemental σ_r sigue que el término principal del polinomio g de (4.8) es

$$
\begin{aligned}
&x_1{}^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3}(x_1x_2x_3)^{\alpha_3-\alpha_4}\cdots(x_1\cdots x_{n-1})^{\alpha_{n-1}-\alpha_n}(x_1\cdots x_n)^{\alpha_n}\\
&\quad = x_1^{\alpha_1-\alpha_2+\alpha_2-\alpha_3+\cdots+\alpha_n}x_2^{\alpha_2-\alpha_3+\cdots+\alpha_n}\cdots x_{n-1}^{\alpha_{n-1}-\alpha_n+\alpha_n}x_n^{\alpha_n} \qquad (4.9)\\
&\quad = x_1^{\alpha_1}\cdots x_n^{\alpha_n}
\end{aligned}
$$

Esto muestra que f y cg tienen el mismo término principal y por lo tanto, de acuerdo al orden lexicográfico, $f_1 = f - cg$ tiene el termino principal estrictamente menor. Ademas, dado que f y g son simetricos, f_1 tambien lo es, por ser la suma de polinomios simétricos.

A continuación, repetimos el mismo procedimiento con f_1 en lugar de f. Puesto que f_1 es simétrico, su término principal es de la forma $c_1x_1^{\beta_1}\cdots x_n^{\beta_n}$, con $\beta_1 \geq \cdots \geq \beta_2$. Como antes, esto dará una expresión g_1 en los polinomios simétricos elementales tales que f_1 y c_1g_1 tienen el mismo término principal. De esto sigue que

$$f_2 = f_1 - c_1g_1 = f - cg - c_1g_1$$

tiene un término principal estrictamente menor que f. Continuando de esta forma, obtendremos polinomios

$$f, \qquad f_1 = f - cg, \qquad f_2 = f - cg - c_1g_1, \qquad f_3 = f - cg - c_1g_1 - c_2g_2, \ldots,$$

donde en cada etapa, el término principal es estrictamente menor de acuerdo al orden lexicográfico graduado. Este proceso terminará si encontramos algún m para el cual $f_m = 0$. Si, por el contrario, nunca encontramos $f_m = 0$, entonces la de arriba será una secuencia infinita de polinomios no nulos con términos principales estrictamente decrecientes. Pero según vimos mas arriba, existe solamente una cantidad finita de monomios estrictamente menores que el término principal de f, por lo tanto el proceso debe terminar.

Una vez encontrado el $f_m = 0$, para algún m, obtenemos

$$f = cg + c_1g_1 + c_2g_2 + \cdots + c_{m-1}g_{m-1}$$

Dado que $f_m = f - cg - c_1 g_1 - c_2 g_2 - \cdots - c_{m-1} g_{m-1} = 0$. Note que cada g_i es el producto de varias potencias de σ_j, lo cual muestra que f es un polinomio en los polinomios simétricos elementales.

Supongamos ahora que $f \in K[x_1, x_2, \dots, x_n]$ puede escribirse como un polinomio en los polinomios simétricos elementales $\sigma_1, \dots, \sigma_n$ con coeficientes en K. Dado que $\sigma_1, \dots, \sigma_n$ son simetricos, resulta que cada término de f es simétrico, por lo tanto f es simétrico. Esto completa la demostración.

La última parte de la demostración deja en evidencia que los únicos polinomios $f \in K[x_1, x_2, \dots, x_n]$ que pueden escribirse como polinomios en $\sigma_1, \dots, \sigma_n$ y coeficientes en F son solamente los polinomios simétricos. Suponga que $f \in K[x_1, x_2, \dots, x_n]$ no es simétrico, es decir que existe una permutación de las variables $x_1, x_2, \dots, x_n$, digamos, $x_{\sigma(1)}, \dots, x_{\sigma(n)}$, tal que $f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \neq f(x_1, x_2, \dots, x_n)$, y además que f puede escribirse como un polinomio en $\sigma_1, \dots, \sigma_n$ y coeficientes en K. Esto último muestra que f es simétrico, lo cual conduce a que $f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) = f(x_1, x_2, \dots, x_n)$ para cualquier permutación $x_{\sigma(1)}, \dots, x_{\sigma(n)}$ de las variables $x_1, x_2, \dots, x_n$, esto es una contradicción.

§ 3 El Grupo de Galois y el grupo simétrico S_n.

En este apartado demostraremos uno de los resultados más importantes que relaciona el Grupo de Galois y el grupo simétrico S_n. El mismo nos dará una herramienta fundamental para demostrar que la ecuación general de quinto grado no es resoluble por radicales.

Definición 1. Diremos que el polinomio

$$(x - x_1)(x - x_2) \cdots (x - x_n) =$$

$$= x^n - \sigma_1 x^{n-1} + \cdots + (-1)^r \sigma_r x^{n-r} + \cdots + (-1)^n \sigma_n$$

dado en la sección anterior es el *polinomio universal de grado* n,[1] y lo denotaremos con la letra $\bar{f}$.

Notemos que $\bar{f}$ es un polinomio con coeficientes en

$$K = F(\sigma_1, \dots, \sigma_n)$$

Puesto que las raíces de $\bar{f}$ son $x_1, \dots, x_n$, entonces

$$L = F(\sigma_1, \dots, \sigma_n)(x_1, \dots, x_n) = F(x_1, \dots, x_n)$$

es el campo de descomposición de $\bar{f}$ sobre K.

Decimos que L/K es la *extensión universal de grado* n.

Puesto que $\bar{f}$ tiene todas sus raíces distintas, el Teorema 1 de la sección 5 del capítulo 3, nos da un homomorfismo inyectivo de $\mathrm{Gal}(L/K) \to S_n$. Ahora probaremos que también es sobreyectivo. Esto es, que $\mathrm{Gal}(L/K)$ es isomorfo a S_n. Antes de pasar a la demostración formal, pensemos que cada K −automorfismo de L deja fijos los elementos de K, y teniendo en cuenta que en el campo de descomposición de $\bar{f}$ esta compuesto por el campo K, más sus n raíces $x_1, \dots, x_n$, es claro que la acción de cada K −automorfismo de L produce una permutación de los n elementos $x_1, \dots, x_n$. De esta forma, cada K −automorfismo de L puede verse como un elemento de S_n.

Teorema 2. La extensión universal de grado n, $K = F(\sigma_1, \dots, \sigma_n) \subset L = F(x_1, \dots, x_n)$ es el campo de factorización de un polinomio separable. La acción del $\mathrm{Gal}(L/K)$ sobre las raíces del polinomio universal de grado n nos da el

1- En algunos textos se llama polinomio general de grado n, y la ecuación relativa al mismo, se denomina ecuación general de grado n

isomorfismo

$$\mathrm{Gal}(L/K) \simeq S_n$$

Demostración: El hecho de que $\bar{f}$ tenga todas sus raíces distintas muestra que es separable y además que $F(x_1, \dots, x_n)$ es su campo de descomposición puesto que

$$\bar{f} = (x - x_1)(x - x_2) \cdots (x - x_n)$$

Para probar la segunda parte del teorema tengamos en cuanta la acción del grupo S_n en el anillo de polinomios $F[x_1, \dots, x_n]$ definida de la siguiente forma:

Sea $f \in F[x_1, \dots, x_n]$ y sea $\tau \in S_n$. Se define $\tau \cdot f$ como el polinomio obtenido al permutar las variables de f según τ. Podemos definir esta correspondencia como sigue:

$$\tau \cdot \big(f(x_1, \dots, x_n)\big) = f\big(x_{\tau(1)}, \dots, x_{\tau(n)}\big)$$

Esta acción posee las siguientes propiedades

$$\tau \cdot (f + g) = \tau \cdot f + \tau \cdot g$$

$$\tau \cdot (fg) = (\tau \cdot f)(\tau \cdot g)$$

$$\tau \cdot (\delta \cdot f) = (\tau \cdot \delta)f$$

las cuales se demuestran sin dificultad.

Notemos que acción de S_n sobre el anillo $F[x_1, \dots, x_n]$, transforma polinomios f de $F[x_1, \dots, x_n]$ en polinomios f' en el mismo anillo, y además, por las dos primeras propiedades dadas anteriormente, esta acción constituye un homomorfismo de $F[x_1, \dots, x_n]$ en si mismo. Por otra parte, notemos que son n variables las variables de f y juntamente, coinciden con numero de elementos del conjunto $\{1, \dots, n\}$, pero es mas, sabemos S_n es el grupo de todas las permutaciones del conjunto $\{1, \dots, n\}$, y por lo dicho anteriormente sobre las variables de f, es claro que la acción de S_n sobre $F[x_1, \dots, x_n]$ abarca cualquier permutación de las variables, esto es, dado un polinomio $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$, al aplicarle cualquier permutación de las variables para obtener el

polinomio $f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \in F[x_1, \dots, x_n]$, existe una permutación $\tau \in S_n$ tal que

$$f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) = \tau \cdot (f(x_1, \dots, x_n)) = f\left(x_{\tau(1)}, \dots, x_{\tau(n)}\right)$$

Esto muestra que la correspondencia $f \mapsto \tau \cdot f$ es un isomorfismo de anillos de

$F[x_1, \dots, x_n]$ en si mismo, y por lo tanto se extiende a un isomorfismo de su campo de fracciones,[1] en este caso el campo de las funciones racionales, denotado por $F(x_1, \dots, x_n)$. Sigue que la permutación de las variables de acuerdo a τ da u automorfismo de $L = F(x_1, \dots, x_n)$. Dado que los polinomios simetricos elementales quedan fijos bajo la acción de $\tau \in S_n$, este automorfismo es la identidad sobre $K = F(\sigma_1, \dots, \sigma_n)$, que es el campo de los coeficientes del polinomio universal.

De esta forma hemos probado que la correspondencia $f \mapsto \tau \cdot f$ es un elemento de $\mathrm{Gal}(L/K)$. Ahora, bajo el homomorfismo $\mathrm{Gal}(L/K) \to S_n$ del teorema1, sección 5 del capítulo 3, el automorfisno $f \mapsto \tau \cdot f$, obviamente se corresponde con $\tau \in S_n$. Puesto que τ es un elemento arbitrario de S_n, vemos que $\mathrm{Gal}(L/K) \to S_n$ es sobreyectivo, lo cual completa la demostración.

§ 4 Solubilidad por radicales.

Como ya dijimos, la Teoría de Galois tuvo su origen en el clásico problema de la Teoría de Ecuaciones, el cual consiste en hallar una fórmula que exprese las soluciones de una ecuación de la forma $f(x) = 0$, donde $f \in \mathbb{C}[x]$ y el grado de f, mayor o igual a 5.

Nuestro primer objetivo es formular el enunciado del problema en términos de la Teoría de Campos. Intuitivamente, la existencia de una fórmula para resolver una

1- Véase Basic Algebra de Nathan Jacobson. Teorema 2.9, pág. 114.

ecuación polinómica específica $f(x) = 0$, donde $f \in K[x]$ y K es el campo base, significa que existe una secuencia finita de pasos, en la que cada uno consiste en la aplicación de una operaciones de campo (adición, multiplicación y sus operaciones inversas) o la extracción de una raíz n −ésima que conducen a una solución de la ecuación dada. Las operaciones en la que intervienen elementos del campo base, dan como resultado elementos del mismo campo, sin embargo la extracción de raíces n −ésimas de un elemento c de F nos conduce a construir un campo de extensión $K(u)$, con $u^n \in K$, esto es $u = \sqrt[n]{c}$. Entonces, la existencia de una "fórmula" para resolver $f(x) = 0$ implicaría la existencia de una torre finita de campos

$$K = K_0 \subset K_1 \subset \cdots \subset K_n$$

tal que K_n contiene al campo de descomposición de f sobre K y para cada $i \geq 1$, $K_i = K_{i-1}(u_i)$ con ${u_i}^{n_i} \in K_{i-1}$ siendo $n_i > 0$.

Por el contrario, supongamos que existe tal torre de campos y que F_n contiene al campo de descomposición de f, en otras palabras, K_n contiene a todas las soluciones de $f(x) = 0$. Entonces

$$K_n = K(u_1, \dots, u_n)$$

y cada solución es de la forma:

$$\frac{f(u_1, \dots, u_n)}{g(u_1, \dots, u_n)}$$

con $f, g \in K[x_1, \dots, x_n]$. Entonces cada solución se puede expresar en términos de un número finito de elementos de K, un número finito de operaciones de campo y $u_1, \dots, u_n$, estos últimos obtenidos a partir del cálculo de raíces. Esta discusión nos conduce a las siguientes definiciones.

Definición 1. Una extensión L de un campo K es una *extensión por radicales* o *extensión radical* si existe una sucesión de campos

$$K = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = L$$

con $i = 1, \dots, n$, tales que existe un elemento $\gamma_i \in K_i$, donde $K_i = K_{i-1}(\gamma_i)$ y ${\gamma_i}^{m_i} \in K_{i-1}, m_i > 0$.

Notemos que haciendo $b_i = {\gamma_i}^{m_i} \in K_{i-1}$, entonces γ_i es la m_i −ésima raíz de b_i.

Esto nos conduce a escribir $\gamma_i = \sqrt[m_i]{b_i}$, y de este modo:

$$K_i = K_{i-1}\left(\sqrt[m_i]{b_i}\right)$$

con $b_i \in K_{i-1}$.

Esto muestra, en concordancia con la discusión precedente, que las extensiones radicales se obtienen mediante la adjunción sucesiva de radicales. Veamos un ejemplo. Sea la extensión $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ del campo $\mathbb{Q}$. Hagamos $\gamma_1 = \sqrt{2}$ y $\gamma_2 = \sqrt{2+\sqrt{2}}$. Entonces tenemos las extensiones:

$$\mathbb{Q} \subset \mathbb{Q}(\gamma_1) = \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})\left(\sqrt{2+\sqrt{2}}\right)$$

Puesto que ${\gamma_1}^2 = \sqrt{2}^2 = 2 \in \mathbb{Q}$ y ${\gamma_2}^2 = \left(\sqrt{2+\sqrt{2}}\right)^2 = 2+\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Y teniendo en cuenta que

$$\mathbb{Q}(\sqrt{2})\left(\sqrt{2+\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$$

La extensión $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ de $\mathbb{Q}$ es radical.

Definición 2. Sea el campo K y sea $f \in K[x]$. El polinomio f es *resoluble por radicales* si existe una extensión radical L de K y un campo de descomposición E de f sobre K tal que

$$K \subset E \subset L$$

Notemos que en la Definición 2 de ha dejado de hablar de la ecuación $f(x) = 0$ y se ha pasado a considerar solamente el polinomio f que interviene en la misma. De ahora en más adoptaremos este enfoque. Es decir, en lugar de hablar de resolver la ecuación polinomial $f(x) = 0$ nos referiremos a encontrar los ceros o las raíces del polinomio f.

De acuerdo a la Definición 2, decir que f es resoluble por radicales equivale a decir que "existe una fórmula explicita" que expresa las raíces de f en la forma descripta más arriba.

Por otra parte, veamos que la definición 2 es la formulación del clásico problema de encontrar una "fórmula" que exprese las raíces de un polinomio, que es válida para cualquier $f \in K[x]$ de grado $n > 0$, por ejemplo $n = 2$. A su vez, cualquiera que sea la definición precisa de la "fórmula", es claro de acuerdo a la discusión precedente a la Definición 1 que la existencia de tal "fórmula" implicaría que cualquier polinomio de grado $n > 0$ es resoluble por radicales. De hecho, es sabido que para $n \leq 4$ esto es cierto.[1]

Con el fin de demostrar la no existencia de tal fórmula, es suficiente mostrar que "existe un polinomio determinado que no es resoluble por radicales". En el capítulo siguiente veremos que tal polinomio existe. Pero antes de esto, veamos el siguiente teorema que da las condiciones para las cuales la clausura normal de una extensión, es una extensión radical.

Teorema 3. Sea L una extensión radical de K, y sea M la clausura normal de L. Entonces M tambien es una extensión radical de K.

Demostración: Por el Teorema 11, sección 5 del capítulo 1, $M = L_1 \vee \cdots \vee L_k$, donde las extensiones $L_1, \ldots, L_k$ son todas isomorfas a L, y por lo tanto radicales. El resultado requerido seguiría fácilmente si probamos que el compuesto de dos extensiones radicales es una extensión radical. Sean

1- Véase el capítulo 1, 2 y 3 del libro Galois´ Theory of Algebraic Equations de J. P. Tignol.

$$M_1 = K(\alpha_1, \dots, \alpha_m), \qquad M_2 = K(\beta_1, \dots, \beta_n)$$

donde

$$\alpha_i^{k_i} \in K(\alpha_1, \dots, \alpha_{i-1}) \text{ con } i = 1, \dots, m$$

$$\beta_j^{l_j} \in K\big(\beta_1, \dots, \beta_{j-1}\big) \text{ con } j = 1, \dots, n$$

Entonces $M_1 \vee M_2 = K(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$ y

$$\alpha_i^{k_i} \in K(\alpha_1, \dots, \alpha_{i-1}) \text{ con } i = 1, \dots, m$$

$$\beta_j^{l_j} \in K\big(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_{j-1}\big) \text{ con } j = 1, \dots, n$$

Entonces $M_1 \vee M_2$ es una extensión radical. Aplicando una simple inducción de este resultado, llegamos finalmente a que $M = L_1 \vee \cdots \vee L_k$ es una extensión radical.

§ 5 El resultado final.

En lo que sigue nos encargaremos de demostrar 2 teoremas claves que dan fin a la larga búsqueda de la generalización de las "formulas resolventes" para las ecuaciones de grado mayor a quinto. Aquí veremos la intima relación entre el Álgebra y la Teoría de Galois desarrollada en los capítulos anteriores y la resolución de ecuaciones. Debe tenerse en cuenta que los campos considerados a continuación poseen característica cero. Esto garantiza que sean campos separables,[1] como así también sus extensiones. Esta elección se basa en que los trabajos de Galois fueron pensados en términos del campo de los Números Complejos, el cual posee característica 0, y además, teniendo en cuenta que es en este campo en el cual se trabaja en la práctica. Por otra parte, algunos de los teoremas relativos a los campos de característica cero, no siempre son válidos en

1- Véase la sección 6 del capítulo 1 referida a extensiones separables.

caso característica finita y hay que hacerles varias modificaciones.

Teorema 1. Sea el polinomio $f \in K[x]$ y sea $\mathrm{Gal}(f)$ su Grupo de Galois. Tenemos entonces que, si $\mathrm{Gal}(f)$ es resoluble entonces f es resoluble por radicales.

Demostración: Sea L el campo de descomposición de f sobre K. Supongamos que $\mathrm{Gal}(f)$ es un grupo resoluble, y además supongamos que $|\mathrm{Gal}(L/K)| = m$. Si K no contiene una raíz m −ésima de la unidad, podemos adjuntarle una: sea E el campo de descomposición sobre K del polinomio $x^m - 1$. Ahora sea M un campo de descomposición para f sobre E. Por el Teorema 3 de la sección 4, capítulo 3, podemos considerar a M como una extensión de L, y de este modo $\mathrm{Gal}(M/E) \simeq \mathrm{Gal}(L/E \cap L)$. Ahora, puesto que $K \subseteq E \cap L \subset L$ son extensiones finitas, sigue del Teorema 12, sección 1 del capítulo 3, que $\mathrm{Gal}(L/E \cap L)$ es un subgrupo del subgrupo resoluble $\mathrm{Gal}(L/K)$, y de este modo, por el Teorema 2, sección 2 del capítulo 2, sigue que el grupo $G = \mathrm{Gal}(M/E)$ es resoluble, y por lo tanto existe una secuencia de subgrupos

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

Tal que G_{i+1}/G_i es cíclico de orden primo para $0 \leq i \leq r-1$. Ahora, por el Teorema Fundamental de la Teoría de Galois existe una secuencia correspondiente

$$E = M_r \subseteq M_{r-1} \subseteq \cdots \subseteq M_0 = M$$

de subcampos de tales que $\mathrm{Gal}(M/M_i) = G_i$, y además $\mathrm{Gal}(M_i/M_{i+1}) \simeq G_{i+1}/G_i$. Notemos que $E \subseteq M_i$ cada subcampo M_i de M, luego es el campo de descomposicion del polinomio $x^m - 1$, y por ende M_i es una extensión normal de M_{i+1}. (Teorema 8, sección 5, capítulo 1).

Sea ahora $[M_i : M_{i+1}] = d_i$ $(i = 0,1, \dots, r)$. Entonces, por el Teorema de la Torre de Extensión Generalizado y por el Corolario 4 de la sección 2, capítulo 3, tenemos que d_i divide a $[M:E] = |\mathrm{Gal}(M/E)|$, el cual a su vez divide a $|\mathrm{Gal}(L/K)| = m$. Dado que M_{i+1} contienen a E, contiene también a cada raíz

m −ésima ω de la unidad, y ciertamente contiene todas las d_i −ésimas raíces de la unidad, siendo estas potencias de ω. Por lo tanto, por el Teorema 9, sección 4 del capítulo 3, existe un elemento β_i en M_i de modo tal que $M_i = M_{i+1}(\beta_i)$, donde β_i es raíz de un polinomio irreducible $x^{d_i} - c_{i+1}$, con c_{i+1} en M_{i+1}. De este sigue que f es resoluble por radicales, y esto es lo que queríamos demostrar.

El reciproco sigue a continuación.

Teorema 2. Sea K un campo de característica cero, y sea $K \subseteq L \subseteq M$, donde M es una extensión radical. Entonces $\mathrm{Gal}(L/K)$ es un grupo resoluble.

Antes de pasar a la demostración hagamos algunas observaciones preliminares. Notemos que en el enunciado del teorema no se ha dicho nada sobre la naturaleza de la extensión L. Sin embargo, sin perder generalidad podemos suponer que la misma es una extensión normal de K. Veamos por qué. Según vimos en el capítulo 3, el campo fijo $\Phi\big(\Gamma(K)\big)$ del grupo $\mathrm{Gal}(L/K)$ es en general más grande que K: denotemoslo por K'. Por otra parte, en la demostración del Teorema Fundamental de la Taoría de Galois, vimos que:

$$\Gamma\Phi\Gamma = \Gamma \qquad \text{y} \qquad \Phi\Gamma\Phi = \Phi$$

y de este modo

$$\Phi\left(\Gamma\big(K'\big)\right) = (\Phi\Gamma\Phi\Gamma)(K) = (\Phi\Gamma)(K) = K'$$

Y por lo tanto, por el Teorema 2, sección 3 del capítulo 3, L es una extensión normal de K'. Dado que cualquier polinomio f en $K[x]$ puede considerarse como un polinomio en $K'[x]$, y desde que $\mathrm{Gal}(L/K) = \mathrm{Gal}\big(L/K'\big)$, podemos reemplazar a K por K'. Luego, para evitar el surgimiento de más notación, podemos suponer que L es una extensión normal de K.

En cuanto a la extensión radical M podemos hacer lo siguiente. Sabemos que si N es una clausura normal de M, entonces, por el Teorema 3 de la sección anterior, N es una extensión radical. Asi que, como en el caso anterior, podemos suponer que M es una extensión es normal y radical.

Demostración (del teorema 2). Si probamos que $\mathrm{Gal}(M/K)$ es resoluble, sigue del Teorema Fundamental de la Teoría de Galois y del Teorema 3, sección 2 del capítulo 2, que $\mathrm{Gal}(L/K)$ es resoluble, para $\mathrm{Gal}(M/L) \lhd \mathrm{Gal}(M/K)$, y además

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)$$

Entonces, nuestro objetivo es demostrar que $\mathrm{Gal}(M/K)$ es resoluble, donde suponemos que M es una extensión normal (y por ser K un campo de característica cero, también es separable.) y radical de K.

Sea

$$M = K(\alpha_1, \dots, \alpha_n) \tag{4.10}$$

Y supongamos que

$$\alpha_i^{p_i} \in K(\alpha_1, \dots, \alpha_{i-1}), \quad i = 1,2, \dots, n$$

Podemos suponer en efecto que p_i es primo, para todo i, con el único cambio de que deberíamos incrementar n: si por ejemplo, tenemos que $\alpha_i^{pq} \in K(\alpha_1, \dots, \alpha_n)$, podemos definir β como α_i^p, y decir que $\beta^q \in K(\alpha_1, \dots, \alpha_n)$ y $\alpha_i^p \in K(\beta, \alpha_1, \dots, \alpha_n)$.

Probaremos este resultado por inducción sobre n en (4.10).

Tenemos que $\alpha_1^{p_1} = b_1 \in K$. Para contar con suficientes raíces de la unidad, sea el campo de descomposición del polinomio $x^{p_1} - 1$ sobre M, donde ω es una p_1 −esima raíz primitiva de la unidad. Ciertamente, por el Teorema 8, sección 5 del capítulo 1, P es una extensión normal de M, y por el Teorema Fundamental de la Teoría de Galois, $\mathrm{Gal}(P/M) \lhd \mathrm{Gal}(P/K)$, y además

$$\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(P/K)/\mathrm{Gal}(P/M)$$

Según el Teorema 3, sección 2 del capitulo 2, si podemos probar que $\mathrm{Gal}(P/K)$ es resoluble, $\mathrm{Gal}(P/M)$ debe ser resoluble, al igual que $\mathrm{Gal}(P/K)/\mathrm{Gal}(P/M)$, y por el isomorfismo de arriba, ciertamente $\mathrm{Gal}(M/K)$ tambien debe ser resoluble, llegando asi al resultado deseado.

Sea M_1 el subcampo $K(\omega)$ de P. En efecto, M_1 es un campo de descomposicion de $x^{p_1} - 1$, y de este modo es una extensión normal. Por el Teorema 4, sección 4 del capítulo 3, $\mathrm{Gal}(M_1/K)$ es cíclico (y por ende resoluble). Así $\mathrm{Gal}(P/M_1) \lhd \mathrm{Gal}(P/K)$, y además

$$\mathrm{Gal}(M_1/K) \simeq \mathrm{Gal}(P/K)/\mathrm{Gal}(P/M_1)$$

Otra vez, el Teorema 3, sección 2 del capitulo 2, nos dice que si probamos que $\mathrm{Gal}(P/M_1)$ es resoluble, la solubilidad de $\mathrm{Gal}(P/K)$ sigue de inmediato.

Por lo tanto, habiendo empezado con $\mathrm{Gal}(L/K)$, hemos reducido el problema a mostrar que $\mathrm{Gal}(P/M_1)$ es resoluble. Entonces podemos escribir

$$P = M_1(\alpha_1, \dots, \alpha_n)$$

Siendo α_i los mismos que en (4.1). Denotemos por G a $\mathrm{Gal}(P/M_1)$ y sea $H = \mathrm{Gal}(P/M(\alpha_1))$, un subgrupo de G. La demostración procede mediante inducción sobre n

$$P = M(\omega) = M_1(\alpha_1, \dots, \alpha_n)$$

Ahora en $M_1[x]$,

$$x^{p_1} - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{p_1-1})$$

Y en $\big(M(\alpha_1)\big)[x]$,

$$x^{p_1} - b_1 = x^{p_1} - \alpha_1^{p_1} = (x-\alpha_1)(x-\omega\alpha_1)(x-\omega^2\alpha_1)\cdots(x-\omega^{p_1-1}\alpha_1)$$

Entonces $M(\alpha_1)$ es un campo de descomposición para $x^{p_1} - b_1$ sobre M_1. Por el Teorema 8, sección 4 del capítulo 3, $\Gamma(M(\alpha_1)) = \mathrm{Gal}(M_1(\alpha_1)/M_1)$ es cíclico. Puesto que $M_1(\alpha)$ es una extensión normal de M_1, por ser un campo de descomposición, sigue del Teorema Fundamental de la Teoría de Galois que $H \lhd G$ y que $G/H \simeq \Gamma(M(\alpha_1))$ es cíclico.

Ahora, H es el Grupo de Galois

$$\mathrm{Gal}(P/M(\alpha_1)) = \mathrm{Gal}(M_1(\alpha_1)(\alpha_2, \dots, \alpha_n)/M(\alpha_1))$$

y P es una extensión normal de $M_1(\alpha_1)$. Nuestra hipótesis inductiva nos lleva a asumir que H es resoluble. Puesto que G/H es resoluble, deducimos que G es resoluble. Y esto es lo que queríamos demostrar.

El Teorema 2 que acabamos de demostrar es fácilmente trasladable a la solubilidad de polinomios. Veamos cómo: si tenemos un polinomio $f \in K[x]$ resoluble por radicales, tenemos que su campo de descomposición L esta contenido en una extensión radical M de K, entonces $\mathrm{Gal}(L/F) = \mathrm{Gal}(f)$ es resoluble.

Del teorema 2 y del teorema 1 sigue el resultado más importante en cuanto a la solubilidad de polinomios y su Grupo de Galois correspondiente.

Teorema 3. (Galois) Un polinomio f con coeficientes en un campo K de característica cero, es resoluble por radicales si y solo si su Grupo de Galois es resoluble.

El objetivo final de este trabajo es mostrar que no existe una fórmula general que exprese las raíces del polinomio de quinto grado y de grados superiores. Esto es, que tales polinomios no son resolubles por radicales. Según lo que discutimos en la sección anterior, decir esto equivale a decir que para la ecuación general de quinto grado y de grados superiores no existe una fórmula equivalente a la fórmula resolvente de la cuadrática o de la cúbica, que permita expresar las soluciones de la misma por radicales. Si bien, en principio no es verdad que dado cualquier polinomio $f \in K[x]$ de la forma

$$f = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \tag{4.2}$$

con $a_i \in K$, no es resoluble por radicales, puesto que por ejemplo el polinomio $x^5 - a$ si lo es, la cuestión está en averiguar, teniendo en cuenta que algunos polinomios de quinto grado son resolubles, si todo polinomio de la forma (4.2) es resoluble. Como dijimos antes, basta con mostrar que existe un polinomio determinado de la forma (4.2) que no es resoluble por radicales. Efectivamente, este polinomio existe y su existencia viene dada en el siguiente corolario del Teorema 3.

Corolario 4. Sea F un campo de característica cero y sea $n \geq 5$. Entonces el polinomio universal

$$\bar{f} = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^r \sigma_r x^{n-r} + \cdots + (-1)^n \sigma_n$$

no es resoluble por radicales.

Demostración: Recordemos que $\bar{f} \in F(\sigma_1, \dots, \sigma_n)[x]$ y su campo de descomposición es

$$L = F(\sigma_1, \dots, \sigma_n)(x_1, \dots, x_n) = F(x_1, \dots, x_n)$$

Escribamos $K = F(\sigma_1, \dots, \sigma_n)$. Por el Teorema 2 de la sección 3, tenemos que $\mathrm{Gal}(L/K) = S_n$. Por otra parte, sigue la Definición 8, sección 1 del capítulo 3, que $\mathrm{Gal}(L/K) = \mathrm{Gal}(\bar{f})$. De este modo tenemos que

$$\mathrm{Gal}(\bar{f}) = S_n$$

Ahora, por el Corolario 11, sección 3 del capítulo 2, sabemos que S_n no es resoluble para $n \geq 5$. Sigue entonces que el Grupo de Galois del polinomio universal $\bar{f}$, es decir $\mathrm{Gal}(\bar{f})$ no es resoluble. Por el Teorema 3 (Teorema de Galois) sigue que el polinomio universal $\bar{f}$ no es resoluble por radicales. Queda así demostrado el resultado principal del presente trabajo.

Como caso particular del Corolario 4 tenemos el conocido Teorema de Abel (1802-1829) demostrado en el año 1824.

Teorema 5. (Abel) La ecuación general de quinto grado no es resoluble por radicales.

En su trabajo original, Abel demostró el Teorema 5 y del mismo dedujo que la ecuación general de grado superior a quinto no es resoluble por radicales.[1] Esto es debido a que si fuese posible hallar una fórmula que exprese las raíces de cualquier ecuación de grado superior al quinto, la misma debería expresar por lo menos cinco raíces. Es decir, indirectamente sería posible hallar la fórmula deseada para la ecuación de quinto grado. Por otra parte vale decir que la demostración de Niels Henrik Abel es muy distinta a la expuesta en el presente trabajo, la cual se basa en los aportes de la Teoría de Galois.

La idea de Abel consistió en considerar la expresión general de lo que él llamo las expresiones algebraicas, que según demostró en su *Mémoire sur les Équations Algébriques* de 1824 debe ser

$$y = p + p_1 R^{1/m} + p_2 R^{2/m} + \cdots + p_{m-1} R^{m-1/m} \tag{4.12}$$

A partir de esto, pensó en que si la ecuación general de quinto grado fuese resoluble por radicales, cada raíz debería poder representarse mediante una expresión de la forma (4.12). Notemos por ejemplo que en el caso de la ecuación cuadrática, la expresión que representa a sus raíces concuerda con la expresión (4.12).

Bajo esta suposición, Abel reemplazo la expresión (4.12) en la ecuación general de quinto grado y llegó a una contradicción, que lo llevo finalmente a la demostración del Teorema 5 anterior.

No obstante, aunque Abel y Galois hayan llegado por distintos caminos a la misma conclusión en cuanto a la resolución algebraica de la quintica, luego de ambos, la búsqueda de la deseada "fórmula resolvente para la ecuación general de quinto grado y de grados superiores" llegó a su fin.

2. Véase Oeuvres Complétes de Niels Henrik Abel, Vol. I y II. Edición publicada en 1839 por B. Holmboe.

Bibliografía

1. Michael L. Rosen, *Niels Hendrick Abel and Equations of fifth degree*, The Amer. Math. Monthly 102, p 495 – 505, Jun - Jul 1995.

2. David A. Cox, *Galois Theory*, Wiley – Interscience, New Jersey, 2004.

3. Ian Stewart, *Galois Theory*, 3er edición, Chapman & Hall/CRC, Boca Raton, FL. 2003.

4. John M. Howie, *Fields and GaloisTheory*, Springer Verlag, Londres, 2005.

5. J. P. Tignol, *Galois Theory of Algebraic Equations*, edición corregida por World Scientific, Singapore, 2001.

6. H. M. Edwards, *Galois Theory*, Springer Verlag, New York – Berlin – Heidelberg – Tokyo, 1984.

7. M. M. Postnikov, *Foundations of Galois Theory*, edición 1962, Dover Publications, Mineola, New York, 2004.

8. C. E. Picard, *Œuvres mathématiques d'Evariste Galois*, Gauthier – Villars et Fils, Paris, 1897.

9. B. Holmboe, *Œuvres Completes de Niels Henrik Abel Vol. I y II*, Gröndhal, Christiania, 1839.

10. I. N. Herstein, *Álgebra Abstracta*, Grupo Editorial Iberoamérica, México, 1988.

11. John B. Fraleigh, *Álgebra Abstracta, Primer Curso*, Addison – Wesley Iberoamericana, México, 1988.

12. D. Cox, J. Little, D. O´Shea, *Ideals, Varieties and Algorithms*, 3er edición, Springer, New York, 2007.

13. Nathan Jacobson, *Basic Algebra*, Vol. I, 1er edición, W. H. Freeman and Company, San Francisco,1974.

14. Hector A. Marklen, *Estructuras Algebraicas V (Teoría de Cuerpos)*, Secretaría General de la Organización de los Estados Americanos, Programa Regional de Desarrollo Científico y tecnológico, Washington D.C. 1979.

15. H. H. O´Brien, *Estructuras Algebraicas III (Grupos Finitos)*, Secretaría General de la Organización de los Estados Americanos, Programa Regional de Desarrollo Científico y tecnológico, Washington D.C. 1979.

16. Thomas W. Hungerford, Algebra, edición 1974, Springer Verlag, New York, 1980.

17. Ian Stewart, *De Aquí al Infinito*, Crítica, Barcelona, 2005.

18. I. Kleiner, *A History of Abstract Algebra*, Birkhäuser, Boston, 2007.