INTRODUCCIÓN A LA TEORíA DE GALOIS

MARTÍN MOMBELLI Y SEBASTIÁN SIMONDI

RESUMEN. Se introducen los conceptos básicos de la teoría de Galois, los resultados principales y algunas aplicaciones.

ÍNDICE

INTRODUCCIÓN

Estas notas surgen de un curso de 5 sesiones dictado en la *XV Escuela Latinoamericana de Matemática* en el mes de mayo de 2011 en la ciudad de Córdoba, Argentina.

Nuestra intención es que los participantes del curso aprendan las nociones básicas de la teoría de Galois y algunas aplicaciones. Intentamos que las notas fueran lo más autocontenidas posibles, sin embargo, dada la extensión del curso, algunos conocimientos previos de estructuras algebraicas son requeridos.

En la sección 1 recordamos ciertas nociones básicas como la definición de anillo, cuerpo, morfismos de anillos, espacios vectoriales, que luego usaremos. En la sección 2 se introduce la definición de extensión de cuerpos, se muestras los ejemplos básicos y la construcción del cuerpo de raíces de polinomios. En la sección 3 para cada extensión de cuerpos se asocia el grupo de Galois. Se estudian diversas propiedades y algunos cálculos sencillos. En la sección 4 se demuestra el principal resultado de la teoría; los cuerpos intermedios de una extensión de cuerpos están en correspondencia biyectiva con los subgrupos de Galois de la extensión. En la útlima sección se aplican los resultados anteriores para determinar cuando un polinomio dado es resoluble por radicales.

1. NOTACIÓN Y PRELIMINARES

Un *anillo* es un conjunto F munido con dos operaciones binarias, usualmente denotada como suma $+$ y multiplicación, tales que F es un grupo abeliano bajo la suma, la multiplicación es asociativa, es decir que $(ab)c = a(cb)$ para todo $a, b, c \in F$ y es distributiva con respecto a la suma, $a(b + c) = ab + ac$.

El anillo F se dice *cuerpo* si $F - \{0\}$ es un grupo abeliano bajo el producto, es decir si todo elemento no nulo posee un inverso multiplicativo. Ejemplos de cuerpos son los números racionales $\mathbb{Q}$, los números reales $\mathbb{R}$ y los números complejos $\mathbb{C}$.

Date: 25 de abril de 2011.
2010 *Mathematics Subject Classification.* 11R32, 11S20.

Si F y L son dos anillos o dos cuerpos, una función $\phi : F \to L$ es un *homomorfismo de anillo o de cuerpo* respectivamente, si para todo $a, b \in F$

$$\phi(1) = 1, \quad \phi(a+b) = \phi(a) + \phi(b) \quad \text{y} \quad \phi(ab) = \phi(a)\phi(b).$$

Un elemento no nulo $a \in F$ se dice *divisor de cero*, si existe un elemento $b \in F$ no nulo tal que $a.b = 0$ o $b.a = 0$. Un anillo que no contiene divisores de cero se llama *dominio íntegro*.

Un subconjunto S de un anillo F que es cerrado bajo las operaciones de suma y producto se llama *subanillo*. Un subanillo I se dice *ideal* si para $r \in F$ y $x \in I$ tenemos que $rx \in I$ y $xr \in I$. Sea X un subconjunto de F y $\{A_i : i \in J\}$ la familia de todos los ideales de F que contienen a X. Entonces el ideal $\cap_{i \in J} A_i$ se llama *ideal generado por* X y se denota (X) y los elementos de X se llaman generadores. Un ideal (x) generado por un sólo elemento se denomina el *ideal principal*. Un *anillo de ideales principales* es un anillo en el cual todos sus ideales son principales.

Un ideal P de un anillo F se dice *primo* si $P \neq F$ y para cada par de ideales A, B en F

$$AB \subseteq P \Longrightarrow A \subseteq P \quad \text{ó} \quad B \subseteq P.$$

Un ideal M del anillo F se dice *maximal* si $M \neq F$ y para todo ideal N tal que $M \subseteq N \subseteq F$ se tiene que $N = M$ ó $N = F$. Un resultado muy conocido cuya demostración no haremos es el siguiente:

Teorema 1.1. *Sea M un ideal en un anillo conmutativo con identidad $1_F \neq 0$. Entonces M es un ideal maximal si y sólo si el anillo cociente F/M es un cuerpo.* □

De este resultado se desprende lo siguiente:

Corolario 1.2. *Las siguientes condiciones sobre un anillo F conmutativo con identidad $1_F \neq 0$ son equivalentes*

1. *F es un cuerpo.*
2. *F no posee ideales propios.*
3. *El ideal (0) es un ideal maximal en F.*
4. *Si S es otro anillo, todo homomorfismo de anillos $F \to S$ es un monomorfismo.* □

Sea F un anillo conmutativo con identidad, un elemento $c \in F$ se dice *irreducible* si c es no inversible y además si $c = ab$ entonces a o b es inversible. Por otro lado $p \in F$ se dice *primo* si no es inversible y además si $p|ab$ entonces $p|a$ o $p|b$.

Teorema 1.3. *Sean p y c dos elementos no nulos en un dominio integral F.*

1. *El elemento p es primo si y sólo si (p) es un ideal primo no nulo.*
2. *El elemento c es irreducible si y sólo si (c) es maximal en el conjunto de todos los ideales principales propios.*
3. *Todo elemento primo de F es irreducible.*
4. *Si F es un dominio de ideales principales, entonces p es primo si y sólo si p es irreducible.* □

Un dominio íntegro F tal que todo elemento no inversible distinto de cero se puede escribir como producto de irreducibles de manera única, se llama *dominio de factorización única*.

Si F es un cuerpo definimos el conjunto de todos los polinomios de una variable con coeficientes en F como

$$F[x] = \{p(x) = a_0 + a_1 x + ... + a_n x^n : n \in \mathbb{N}_0 \text{ y } a_i \in F\}$$

Con la suma y el producto definidos de manera usual, $F[x]$ es un anillo. Como F es un cuerpo, $F[x]$ no contine divisores de cero, por lo tanto es un dominio íntegro. Más aún $F[x]$ es un *dominio euclídeo*, es decir dados dos polinomios $f(x), g(x) \in F[x]$ con $g(x) \neq 0$ existen polinomios únicos $q(x), r(x) \in F[x]$ tales que

$$f(x) = q(x)g(x) + r(x) \text{ con } r = 0 \text{ o } gr(r) < gr(g).$$

Este algoritmo de división es análogo al aprendido en la escuela secundaria para $\mathbb{R}[x]$. Como $F[x]$ es un dominio euclideano, entonces es un dominio de ideales principales y consecuentemente un dominio de factorización única.

Si $f \in F[x]$ tal que $gr(f) \geq 1$, del Teorema 1.3 se deduce que las siguientes propiedades son equivalentes

1. Si $f(x)|g(x)h(x)$ entonces $f(x)|g(x)$ o $f(x)|h(x)$.
2. $f(x)$ es un polinomio irreducible.
3. El ideal (f) es un ideal maximal.
4. El ideal (f) es un ideal primo.
5. El anillo cociente $F[x]/(f)$ es un cuerpo.

En general decidir si un polinomio $f(x) \in F[x]$ es irreducible es un problema difícil, estudiemos un criterio de irreducibilidad

Criterio de irreducibilidad de Eisenstein: Si A es un dominio de factoriazación única y F es su cuerpo cociente, si $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, con $n \geq 1$ y existe un primo $p \in A$ tal que $p \not| a_n$, $p|a_i$, con $i = 1, ..., n-1$ y $p^2 \not| a_0$, entonces $f(x)$ es irreducible en $F[x]$.

Por ejemplo sea $f(x) = 2x^5 - 6x^3 + 9x^2 - 15 \in \mathbb{Z}[x]$, entonces por el criterio de Eisenstein tomando $p = 3$ tenemos que $f(x)$ es irreducible en $\mathbb{Q}[x]$ y en $\mathbb{Z}[x]$.

Ejercicio 1. Demostrar que el polinomio $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ es irreducible sobre $\mathbb{Q}$ para todo número primo p.

Ejercicio 2. Sea $f \in \mathbb{Z}[x]$ un polinomio mónico. Si p es un número primo, denotamos por $\overline{f} \in \mathbb{Z}_p[x]$ a la imagen de f bajo la proyección canónica $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$.

(i) Demostrar que si $\overline{f}$ es irreducible en $\mathbb{Z}_p[x]$ entonces f es irreducible en $\mathbb{Z}[x]$.
(ii) Demostrar que el polinomio $x^3 - 5x + 36$ es irreducible sobre $\mathbb{Z}[x]$.
(iii) Demostrar que el polinomio $x^6 + x^3 + 1$ es irreducible sobre $\mathbb{Z}[x]$.
(iv) Demostrar que la recíproca de (i) no es cierta.

Un *espacio vectorial* V sobre un cuerpo F es un conjunto no vacío junto con dos operaciones, una suma y una operación producto externa entre el conjunto V y el cuerpo F llamado producto por escalar tales que:

1. V es un grupo abeliano con la suma.
2. El producto por escalar $\cdot : F \times V \to V$. A la imagen de (r, v) la denotaremos rv. Se satisface las siguientes propiedades para todo $v, w \in V$ y para todo $r, s \in F$:
   a) $r(v + w) = rv + rw$,
   b) $(r + s)v = rv + sv$,
   c) $s(rv) = (sr)v$,
   d) $1_F v = v$.

Dados dos espacios vectoriales V, W sobre un cuerpo F una función T de V en W es una *transformación lineal* si para todo $v, w \in V$ y $k \in F$ se satisface que $T(v+w) = T(v)+T(w)$ y $T(kv) = kT(v)$. El conjunto de todas las transformaciones lineales forman a su vez un espacio vectorial con la suma y producto por escalar usual de funciones. Denotamos por $\mathrm{Hom}_F(V, W)$ al espacio vectorial de las transformaciones F-lineales de V en W, $\mathrm{End}_F(V) = \mathrm{Hom}_F(V, V)$ y

$$\mathrm{Aut}_F(V) = \{T \in \mathrm{End}_F(V) : T \text{ es biyectiva } \}.$$

2. Extensiones de cuerpos

Un cuerpo L es una *extensión* de un cuerpo F si F es un subcuerpo de L y se denota L/F. El cuerpo L posee una estructura natural de F-espacio vectorial, este induce la siguiente definición:

Definición 2.1. La dimensión de L como F-espacio vectorial se denomina el *grado de* L/F y se denota por $[L : F]$. L se dice una *extensión finita* o *infinita* de F según si $[L : F]$ es finito o no.

Por ejemplo el cuerpo de los números complejos $\mathbb{C}$ es una extensión de grado 2 de los números reales dado que $\{1, i\}$ es una base de $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial, mientras que $\mathbb{R}$ es una extensión infinita de los números racionales $\mathbb{Q}$.

Si L es una extensión de F y A es un subconjunto de L denotamos por $F[A]$ al subanillo de L generado por F y A, es decir a la intersección de todos los subanillos de L que contienen a F y a A y denotamos $F(A)$ al subcuerpo generado por F y A, que es la intersección de todos los subcuerpos de L que contienen a F y a A. Si A es un conjunto finito, $A = \{\alpha_1, \dots, \alpha_n\}$ $F[A]$ y $F(A)$ se escriben $F[\alpha_1, \dots, \alpha_n]$ y $F(\alpha_1, \dots, \alpha_n)$ respectivamente.

Teorema 2.2. *Si L/F es una extensión y A es un subconjunto de L no vacio, entonces:*

1. $F[A] = \{f(\alpha_1, \dots, \alpha_n) : n \in \mathbb{N},\ f \in F[X_1, \dots X_n],\ \alpha_1, \dots, \alpha_n \in A\}$.
2. $$F(A) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : n \in \mathbb{N},\ f, g \in F[X_1, \dots X_n],\ \alpha_1, \dots, \alpha_n \in A, \right.$$ $$\left. g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}.$$

La demostración queda como ejercicio a desarrollar en las horas de práctico del curso.

Definición 2.3. Sea L una extensión de F. Un elemento $\alpha \in L$ se dice *algebraico* sobre F si existe un polinomio $p \in F[x]$ tal que $p(\alpha) = 0$. Si todo elemento de L es algebraico sobre F se dice que la extensión L/F es *algebraica*. Si α no es algebraico se dice *trascendente*.

Por ejemplo $i \in \mathbb{C}$ es algebraico sobre $\mathbb{R}$ y $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$. Por otro lado Hermite probó en 1873 que el número e es trascendente y Lindemann que π lo es en 1882.

Si $\alpha \in L$ es algebraico, se define a $p_{F,\alpha}$ al polinomio mónico en $F[x]$ de menor grado de todos los $p \in F[x]$ tales que $p(\alpha) = 0$. Resulta que $p_{F,\alpha}$ es el generador del ideal $Ker(ev_\alpha) \subseteq F[x]$, donde $ev_\alpha : F[x] \to L$ es la función $ev_\alpha(f) = f(\alpha)$. Si F/K es una extensión entonces $p_{K,\alpha}$ divide a $p_{F,\alpha}$.

Ejercicio 3. Sea $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Demostrar que $\sqrt[4]{2}$ es algebraico sobre $\mathbb{Q}$ y sobre $\mathbb{Q}(\sqrt{2})$. Comprobar que sobre $\mathbb{Q}$ el polinomio minimal de $\sqrt[4]{2}$ es $x^4 - 2$ pero no es minimal sobre $\mathbb{Q}(\sqrt{2})$.

Proposición 2.4. *Sea L una extensión de F y $\alpha \in L$ algebraico sobre F. Entonces*

1. *el polinomio $p_{F,\alpha}$ es irreducible.*
2. *Si $g \in F[x]$, entonces $g(\alpha) = 0$ si y sólo si $p_{F,\alpha}$ divide a g.*
3. *Si $n = gr(p_{F,\alpha})$ entonces $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ es base de $F(\alpha)$ como F-espacio vectorial. Además $F(\alpha) = F[\alpha]$.*

Demostración. (1) Como $F[x]/(p_{F,\alpha}) \simeq F[\alpha]$ que es un dominio íntegro, entonces el ideal $(p_{F,\alpha})$ es primo y así/ $p_{F,\alpha}$ es irreducible.

(2) Sea $g \in F[x]$ tal que $g(\alpha) = 0$, entonces $g \in Ker(ev_\alpha)$ pero como este ideal está generado por $p_{F,\alpha}$ entonces $p_{F,\alpha}$ divide a g. La recíproca es evidente.

(3) Como el ideal $(p_{F,\alpha})$ es maximal, el cociente $F[x]/(p_{F,\alpha}) \simeq F[\alpha]$ es un cuerpo y por lo tanto $F[\alpha] = F(\alpha)$. Si $\beta \in F(\alpha)$ entonces $\beta = g(\alpha)$ par algun $g \in F[x]$. Entonces existen polinomios $q, r \in F[x]$ tales que

$$g(x) = q(x)p_{F,\alpha}(x) + r(x),$$

donde $r = 0$ o bien $gr(r) < n$. Entonces $\beta = r(\alpha)$. Lo cual demuestra que el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es un sistema de generadores de $F(\alpha)$. Sean $a_i \in F$ tales que

$$\sum_{i_0}^{n-1} a_i \alpha^i = 0,$$

entonces $f(x) = \sum_{i_0}^{n-1} a_i\, x^i$ es divisible por $p_{F,\alpha}$ lo cual implica, ya que $gr(f) \leq n-1$, que $f = 0$. Luego $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base. □

Ejercicio 4. Sea $\zeta \neq 1$ una raíz de $x^3 - 1$. Demostrar que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.

Ejercicio 5. Demostrar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ y hallar el índice $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$.

Ejercicio 6. Demostrar que $[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}] = 8$.

Lema 2.5. *Sea L/F una extensión y K un cuerpo intermedio $K \subset F \subset L$ entonces*

1. *Si L/F es una extensión es finita entonces L es algebraico sobre F.*
2. *$[L : F] = [L : K]\,[K : F]$.*
3. *Si $\{\alpha_1, \ldots, \alpha_n\} \in L$ es un conjunto de escalares algebraicos sobre F entonces $F[\alpha_1, \ldots, \alpha_n]$ es un cuerpo y*

$$[F[\alpha_1, \ldots, \alpha_n] : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F].$$

Demostración. (1) Supongamos que $[L : F] = n$ y sea $a \in L$. El conjunto $\{1, a, a^2, \ldots, a^n\}$ es linealmente dependiente y por lo tanto existen $\lambda_i \in F$ no todos nulos tal que $\sum_{i=0}^{n} \lambda_i a^i = 0$. Si denotamos $f = \sum_{i=0}^{n} \lambda_i x^i \in F[x]$ entonces $f \neq 0$ y $f(a) = 0$ por lo tanto a es algebraico sobre F.

(2) Sea $\{a_1, \ldots, a_n\}$ una base de K como F-espacio vectorial y sea $\{b_1, \ldots, b_m\}$ una base de L como K-espacio vectorial. El conjunto $\{a_i b_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ es una base de L como F-espacio vectorial. La demostración de este hecho queda como ejercicio para el lector.

(3) Lo demostraremos por inducción en n. Asumamos que $n = 1$. Consideramos la aplicación $ev_{\alpha_1} : F[x] \to L$, $ev_{\alpha_1}(f) = f(\alpha_1)$. Como α_1 es algebraico entonces el nucleo de ev_{α_1} es un ideal no nulo de $F[x]$ que es primo. Como todo ideal primo de $F[x]$ es maximal se tiene que $F[x]/ker(ev_{\alpha_1}) \simeq F[\alpha_1]$ es un cuerpo y por lo tanto $F[\alpha_1] = F(\alpha_1)$.

Sea $K = F[\alpha_1, \ldots, \alpha_{n-1}]$. Por inducción se tiene que K es un cuerpo y $[K : F] \leq \prod_{i=1}^{n-1} [F(\alpha_i) : F]$. Como p_{K,α_n} divide a p_{F,α_n} entonces tenemos que

$$[F[\alpha_1, \ldots, \alpha_n] : K] \leq [F(\alpha_n) : F],$$

por lo tanto usando el resultado anterior se deduce que

$$[F[\alpha_1, \ldots, \alpha_n] : F] = [F[\alpha_1, \ldots, \alpha_n] : K][K : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F].$$

□

La desigualdad anterior puede ser estricta. Como los polinomios $x^4 - 18$ y $x^4 - 2$ son irreducibles sobre $\mathbb{Q}$ (demostrar) se tiene que $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4 = [\mathbb{Q}(\sqrt[4]{18}) : \mathbb{Q}]$. Demostremos que $[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}] = 8$. Para esto demostremos que $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$. Para ver esta igualdad notemos que $(\frac{\sqrt[4]{18}}{\sqrt[4]{2}})^2 = 3$, por lo tanto $\sqrt{3} \in \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18})$, es decir $\mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$ es un subcuerpo de $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18})$. Como $\sqrt[4]{18}$ es raíz del polinomio $x^2 - 3\sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})[x]$ entonces $[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}(\sqrt[4]{2})] \leq 2$. Luego

$$[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \leq 8 = [\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}].$$

Corolario 2.6. *Si L es una extensión de F entonces $\alpha \in L$ es algebraico si y sólo si $[F(\alpha) : F] < \infty$.* □

Ejercicio 7. Sea $\Bbbk$ un cuerpo. Consideremos el cuerpo de funciones racionales $\Bbbk(t)$ en una variable. Sea $\phi \in \Bbbk(t)$ tal que $\phi \notin \Bbbk$. Demostrar que $[\Bbbk(t) : \Bbbk(t)(\phi)] < \infty$.

Definición 2.7. Sea L/F una extensión y $f \in F[x]$ un polinomio.

1. Decimos que f se *factorea* sobre L si existen $a_1, \dots a_n \in L$ tales que
$$f(x) = a_1(x - a_2) \dots (x - a_n).$$
2. Se dice que L es un *cuerpo de raíces* de f si f se factorea sobre L y $L = F(\alpha_1, \dots \alpha_n)$ donde α_i son las raíces de f, éste es el menor subcuerpo de L que satisface esta propiedad.

El siguiente resultado muestra la existencia del cuerpo de raíces de un polinomio dado.

Teorema 2.8. *Si F es un cuerpo y $f(x) \in F[x]$ un polinomio de grado mayor o igual a uno, entonces existe una extensión de L de F tal que $f(x) = a(x - c_1)...(x - c_n)$ con $a \in F$ y $c_1, ..., c_n \in L$.*

Demostración. La existencia se demuestra por inducción en el grado del polinomio. Si $f(x) \in F[x]$ tiene grado 1, $L = F$ satisface el teorema. Sea $gr(f) = n$ y supongamos que el teorema es válido para todo polinomio no constante de grado menor que n. Si $f(x)$ es irreducible $F_1 = F[x]/(f(x))$ es un cuerpo que contiene a F, pues como $F[x]$ es un dominio euclideano y f es irreducible entonces el ideal $(f(x))$ es maximal, por lo tanto el anillo cociente $F[x]/(f(x))$ es un cuerpo. Si identificamos a cada $k \in F$ con su clase de equivalencia $\overline{k}$ en $F[x]/(f(x))$, tenemos que F_1 es una extensión de F. Si $c_1 = \overline{x} \in F_1$ es la clase de equivalencia que contiene al polinomio x entonces $f(\overline{x}) = \overline{f(x)} = 0$. Luego $f(x) = (x - c_1)g(x)$ en $F_1[x]$. Por hipótesis inductiva existe una extensión F_2 de F_1 tal que $g(x) = (x - c_2)...(x - c_n)$ con $c_2, ..., c_n \in F_2$. Entonces $L = F_2$. Si $f(x)$ no es irreducible, entonces $f(x) = g(x)h(x)$ con $1 \leq gr(g(x)), gr(h(x)) < n$. Por hipótesis inductiva, existe una extensión F_1 de F tal que $g(x) = a(x - c_1)...(x - c_r)$ con $c_1, ..., c_r \in F_1$. Como $F[x] \subset F_1[x]$, podemos aplicar la hipótesis inductiva en el polinomio $h(x) \in F_1[x]$. Entonces existe una extensión F_2 de F_1, y por lo tanto una extensión de F. Por lo tanto podemos tomar $L = F_2$. □

Por ejemplo, consideremos $f(x) = x^2 + x + 1$ sobre $\mathbb{Z}_2$. El polinomio f es irreducible pues $p(0) = 1 = p(1)$. Dado que $\mathbb{Z}_2$ no está contenido en $\mathbb{C}$ usaremos la construcción básica del cuerpo de raíces de f.

Como f es irreducible, entonces se puede construir una extensión $\mathbb{Z}_2(\zeta)$ de $\mathbb{Z}_2$ siguiendo el método del teorema, donde ζ es una raíz de f. Sea $\varphi : \mathbb{Z}_2[x] \to \mathbb{Z}_2[x]/(f(x))$ siendo $\zeta = \varphi(x)$. El número ζ tiene a f como polinómio minimal sobre $\mathbb{Z}_2$, luego $[\mathbb{Z}_2(\zeta), \mathbb{Z}_2] = 2$ y $\zeta^2 + \zeta + 1 = 0$, por lo que $\zeta^2 = 1 + \zeta$. El conjunto $\{1, \zeta\}$ es una base de $\mathbb{Z}_2(\zeta)$ sobre $\mathbb{Z}_2$, de modo que los elementos de $\mathbb{Z}_2(\zeta)$ son $0, 1, \zeta, 1 + \zeta$.

Las tablas de suma y producto son las siguientes:

$+$	0	1	ζ	$1+\zeta$
0	0	1	ζ	$1+\zeta$
1	1	0	$1+\zeta$	ζ
ζ	ζ	$1+\zeta$	0	1
$1+\zeta$	$1+\zeta$	ζ	1	0

$\cdot$	0	1	ζ	$1+\zeta$
0	0	0	0	0
1	0	1	ζ	$1+\zeta$
ζ	0	ζ	$\zeta+1$	1
$1+\zeta$	0	$1+\zeta$	1	ζ

En $\mathbb{Z}_2(\zeta)[x]$ el polinomio f se descompone como
$$f(x) = (x - \zeta)(x - 1 - \zeta).$$

Ejercicio 8. Sea F un cuerpo, $f \in F[x]$ un polinomio de grado n. Si L es su cuerpo de raíces entonces $[L : F] \leq n!$. Ayuda: demostrarlo por inducción en n.

Ejercicio 9. Demostrar que los polinomios $p(x) = x^2 - 2x + 2$ y $q(x) = x^2 + 1$ son irreducibles sonbre $\mathbb{Q}$ y ambos tienen a $\mathbb{Q}(i)$ como cuerpo de raíces sobre $\mathbb{Q}$.

Ejercicio 10. Construir los cuerpos de raíces de $f(x) = x^3 + 2x + 1$ y $g(x) = x^3 + x^2 + x + 2$ sobre $\mathbb{Z}_3$. Son isomorfos entre si?

Ejercicio 11. Sea $f(x) = x^3 - 2$. Encontrar el cuerpo L de raíces de f. Existe un $\zeta \in \mathbb{C}$ tal que $L = \mathbb{Q}(\zeta)$?

Teorema 2.9. *Sea $F \subseteq K \subseteq L$ una extensión de cuerpos. Si K es algebraico sobre F y L es algebraico sobre K entonces L es algebraico sobre F.*

Demostración. Sea $\alpha \in L$. Denotemos $p_{K,\alpha}(x) = a_0 + a_1 x - \cdots + a_n x^n$. Como K/F es una extensión algebraica el cuerpo $K_0 = F(a_0, \ldots, a_n)$ es una exensión finita de F. El polinomio $p_{K,\alpha}$ pertenece a $K_0[x]$ por lo tanto α es algebraico sobre K_0 y por lo tanto

$$[K_0(\alpha) : F] = [K_0(\alpha) : K_0][K_0 : F] < \infty.$$

Como $F(\alpha) \subseteq K_0(\alpha)$ tenemos que $[F(\alpha) : F] < \infty$ y así α es algebraico sobre F. □

Definición 2.10. Sea L/F una extensión. El conjunto

$$\{\alpha \in L : \alpha \text{ es algebraico sobre } L\}$$

es llamado *la clausura algebraica* de F en L.

El siguiente corolario se deja como ejercicio para el lector.

Corolario 2.11. *Sea L/F una extensión y sea K la clausura algebraica de F en L. Entonces K es un cuerpo y es la extensión algebraica más grande contenida en L.*

Ejercicio 12. Sea L/F una extensión y sea $\alpha \in L$ tal que $[F(\alpha) : F]$ es impar. Demostrar que $F(\alpha) = F(\alpha^2)$

Ejercicio 13. Sea L una extensión algebraica de F y sea $F \subseteq R \subseteq L$ un subanillo. Demostrar que R es un cuerpo.

3. El grupo de Galois de una extensión

Si L es un cuerpo los automorfismos de anillo de L forman un grupo $\mathrm{Aut}(L)$ con respecto a la composición de aplicaciones.

Definición 3.1. Si L/F es una extensión, llamaremos el *grupo de Galois* de L sobre F al subgrupo $\mathrm{Aut}_F(L)$ de $\mathrm{Aut}(L)$ formado por los F-automorfismos y lo denotamos por $\mathrm{Gal}(L/F)$. Es decir aquellos automorfismos que además son transformaciones lineales de F-espacios vectoriales.

Ejercicio 14. Demostrar que $\mathrm{Aut}(\mathbb{R}) = \{id\}$.

Por ejemplo si $F = L$ entonces $\mathrm{Gal}(L/F) = \{id\}$. Notemos que si $\sigma \in \mathrm{Aut}_F(L)$ entonces $\sigma_{|F} = id$ pues como es un homomorfismo de anillo $\sigma(1_L) = 1_L$ y si $\alpha \in F$

$$\sigma(\alpha) = \sigma(\alpha 1_L) = \alpha\sigma(1_L) = \alpha 1_L = \alpha$$

para analizar ejemplos más complejos estudiemos primero el siguiente resultado

Lema 3.2. *Sea F/L una extensión y $p \in F[x]$. Si $\alpha \in F$ es una raíz de p y $\sigma \in \mathrm{Aut}_F(L)$, entonces $\sigma(\alpha) \in F$ es también raíz de p.*

Demostración. Si $p = \sum_{i=1}^n k_i x^i$, entonces $p(\alpha) = 0$ implica

$$0 = \sigma(p(\alpha)) = \sigma\left(\sum_{i=1}^n k_i \alpha^i\right) = \sum_{i=1}^n k_i \sigma(\alpha)^i = p(\sigma(\alpha)).$$

□

Una de las principales aplicaciones de este resultado es en la situación donde α es algebraico sobre F con polinomio irreducible $p \in F[X]$ de grado n, pues cualquier $\sigma \in \mathrm{Aut}_F(F(\alpha))$ esta completamente determinado por su acción en α, pues $\{1, \alpha, ..., \alpha^{n-1}\}$ es una base de $F(\alpha)$ sobre F.

Por ejemplo $\mathbb{C} = \mathbb{R}(i)$ y $\pm i$ son raíces de $p(x) = x^2 + 1$, entonces $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ tiene orden a lo sumo dos. Es fácil verificar que la conjugación compleja ($a+ib \to a-ib$) es un $\mathbb{R}$-automorfismo de $\mathbb{C}$ que es distinto a la identidad, por lo tanto $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}_2$. De manera análoga pruebe que $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}_2$.

Ejemplo 3.3. Consideremos el polinomio $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$. El cuerpo de raíces de f es $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ y sabemos que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, es decir que

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}.$$

Nos preguntamos cual es el grupo de Galois de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

Si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ entonces σ aplicada a una raíz de $x^2 - 2$ da como resultado otra raíz de $x^2 - 2$. Lo mismo ocurre con las raíces de $x^2 - 3$. Por lo tanto $\sigma(\sqrt{2}) = \pm\sqrt{2}$ y $\sigma(\sqrt{3}) = \pm\sqrt{3}$. El valor de $\sigma(\sqrt{6})$ queda determinado por los anteriores valores. Por lo tanto $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ tiene cuatro elementos: $\{id, \sigma_1, \sigma_2, \sigma_3\}$ donde

$$\begin{aligned}
\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6},\\
\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6},\\
\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.
\end{aligned}$$

Se puede comprobar facilmente que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Ejemplo 3.4. En el anterior ejemplo teníamos que el cardinal del grupo de Galois coincidía con el índice de la extensión. Veamos un ejemplo en el cual esto no se cumple. Determinemos que grupo de Galois de la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Un automorfismo de $\mathbb{Q}(\sqrt[3]{2})$ que fije a $\mathbb{Q}$ debe aplicar $\sqrt[3]{2}$ a otra raíz del polinomio $x^3 - 2$, pero $\sqrt[3]{2}$ es la única raíz del polinomio $x^3 - 2$ en el cuerpo $\mathbb{Q}(\sqrt[3]{2})$ por lo tanto $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ es trivial. Sin embargo $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Ejercicio 15. Demostrar que si $\Bbbk$ es un cuerpo entonces $\mathrm{Gal}(\Bbbk(t)/\Bbbk) \simeq PGL_2(\Bbbk)$. Recordemos que el grupo $PGL_2(\Bbbk)$ es llamado el *grupo general lineal proyectivo* y se define como el cociente $GL_2(\Bbbk)/\{\Bbbk Id\}$.

Ayuda: Definamos $\phi : GL_2(\Bbbk) \to \mathrm{Gal}(\Bbbk(t)/\Bbbk)$ como sigue. Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ entonces

$$\phi(A)(t) = \frac{at + b}{ct + d}.$$

De esta manera queda bien definida la función $\phi(A) : \Bbbk(t) \to \Bbbk(t)$

Lema 3.5. *Si L/F es una extensión finita entonces* $|\ \mathrm{Gal}(L/F)\ | \leq [L : F]$.

Demostración. Asumamos que $m = |\ \mathrm{Gal}(L/F)\ | > [L : F] = n$.

Sea $\{\sigma_1, \ldots, \sigma_m\} = \mathrm{Gal}(L/F)$ y sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de L como F-espacio vectorial. Como $m > n$ el sistema de ecuaciones

$$\begin{cases}
\sigma_1(\alpha_1)x_1 + \cdots + \sigma_m(\alpha_1)x_m = 0\\
\sigma_1(\alpha_2)x_1 + \cdots + \sigma_m(\alpha_2)x_m = 0\\
\cdots\\
\sigma_1(\alpha_n)x_1 + \cdots + \sigma_m(\alpha_n)x_m = 0
\end{cases}$$

posee una solución no trivial, digamos $(\lambda_1, \ldots, \lambda_m) \in L^m$. Esto implica que $\sum_{i=0}^{m} \lambda_i\sigma_i = 0$ en $\mathrm{Aut}(L)$. Esto es una contradicción pues cualquier conjunto finito de elementos distintos de un grupo son linealmente independientes en el álgebra de grupo. $\square$

Si $G \subseteq \mathrm{Aut}(L)$ es un subconjunto, definimos

$$\mathcal{F}(G) = \{a \in L : \sigma(a) = a \text{ para todo } \sigma \in G\}.$$

Las siguientes propiedades son inmediatas de verificar.

Lema 3.6. 1. *$\mathcal{F}(G)$ es un subcuerpo de L.*
2. *Si $k \subseteq K \subseteq L$ entonces* $\mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/k)$.
3. *Si $G_1 \subseteq G_2 \subseteq \mathrm{Aut}(L)$ entonces $\mathcal{F}(G_2) \subseteq \mathcal{F}(G_1)$.*
4. *Si $G \subseteq \mathrm{Aut}(L)$ entonces $G \subseteq \mathrm{Gal}(L/\mathcal{F}(G))$.*
5. *Si $G \subseteq \mathrm{Aut}(L)$ entonces $\mathcal{F}(G) = \mathcal{F}(\mathrm{Gal}(L/\mathcal{F}(G)))$.*
6. *Si L/K es una extensión entonces* $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/\mathcal{F}(\mathrm{Gal}(L/K)))$.

Demostración. Las partes (1),(2),(3) y (4) son inmediatas y se dejan como ejercicio para el lector.

Sea $G \subseteq \mathrm{Aut}(L)$ un subconjunto y $F = \mathcal{F}(G) \subseteq L$. Entonces por definición $G \subseteq \mathrm{Gal}(L/F)$ por lo tanto $\mathcal{F}(\mathrm{Gal}(L/F)) \subseteq \mathcal{F}(G) = F$. Pero $F \subseteq \mathcal{F}(\mathrm{Gal}(L/F))$, luego $F = \mathcal{F}(\mathrm{Gal}(L/\mathcal{F}(G)))$ y (5) queda demostrado.

Para la parte (6) sabemos que $K \subseteq \mathcal{F}(\mathrm{Gal}(L/K)) \subseteq L$, luego sigue de la parte (2) que

$$\mathrm{Gal}(L/\mathcal{F}(\mathrm{Gal}(L/K))) \subseteq \mathrm{Gal}(L/K).$$

La parte (4) implica que $\mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/\mathcal{F}(\mathrm{Gal}(L/K)))$, lo cual finaliza la demostración. □

En conclusión, si L/F es una extensión se tiene una correspondencia:

$$\left\{\begin{array}{c}\text{Subgrupos } G \subseteq \mathrm{Gal}(L/F)\\ \text{de la forma } G = \mathrm{Gal}(L/K)\\ \text{para alguna}\\ \text{extensión } F \subseteq K \subseteq L\end{array}\right\} \begin{array}{c}\xrightarrow{\mathcal{F}(-)}\\ \xleftarrow{Gal(L/-)}\end{array} \left\{\begin{array}{c}\text{Subcuerpos de } K \subseteq L\\ \text{tales que } F \subseteq K\\ \text{y } K = \mathcal{F}(G) \text{ para algun}\\ \text{subgrupo } G \subseteq \mathrm{Aut}(L)\end{array}\right\}$$

Cabe preguntarse ahora bajo que hipótesis la correspondecia $K \longleftrightarrow \mathrm{Gal}(L/K)$ establece una biyección entre *todos* los sucuerpos de L que contienen a F y *todos* los subgrupos de $\mathrm{Gal}(L/F)$. La parte (5) del Lema anterior nos dice que una condición necesaria es que $K = \mathcal{F}(\mathrm{Gal}(L/K)$. Veremos más adelante que esta condición es también suficiente.

Proposición 3.7. *Sea L/F una extensión finita. Si $F = \mathcal{F}(G)$ para un grupo finito $G \subseteq \mathrm{Aut}(L)$, entonces $\mid G \mid = [L : F]$ y por lo tanto $G = \mathrm{Gal}(L/F)$.*

Demostración. Por el lema 3.6 parte (4) se tiene que $G \subseteq \mathrm{Gal}(L/\mathcal{F}(G))$ y por lo tanto

$$\mid G \mid \leq \mid \mathrm{Gal}(L/\mathcal{F}(G)) \mid \leq [L : \mathcal{F}(G)] \leq [L : F].$$

Asumamos que $n = \mid G \mid < [L : F]$. Sean $\alpha_1, \ldots, \alpha_{n+1} \in L$ elementos linealmente independientes sobre F y $G = \{\sigma_1, \ldots, \sigma_n\}$. Definamos la matriz

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_{n+1}) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_{n+1}) \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_{n+1}) \end{pmatrix}.$$

Las columnas de A son linealmente dependientes sobre L. Elijamos un k minimal de tal manera que las primeras k columnas de la matriz A son linealmente dependientes (permutandolas si es necesario). Por lo tanto existen escalares $c_i \in L$ tales que

$$\sum_{i=1}^{k} c_i \sigma_j(\alpha_i) = 0 \tag{3.1}$$

para todo j. La minimalidad de k implica que $c_i \neq 0$ para todo $i = 1 \dots k$, por lo que podemos asumir que $c_1 = 1$.

No todos los c_i pertenecen a F ya que, en este caso, $0 = \sum_{i=1}^{k} \sigma_j(c_i\alpha_i)$ pero esto implica que $0 = \sum_{i=1}^{k} c_i\alpha_i$ lo cual no puede ser por que $\alpha_1, \dots, \alpha_{n+1}$ son F-independientes. Tomemos $\sigma \in G$ un elemento y se lo aplicamos a la ecuación (3.1):

$$0 = \sum_{i=1}^{k} \sigma(c_i)\sigma\sigma_j(\alpha_i).$$

Como multiplicar por un elemento en un grupo permuta los elementos, obtenemos que $0 = \sum_{i=1}^{k} \sigma(c_i)\sigma_j(\alpha_i)$ para todo $\sigma \in G$. De esta útlima igualdad y (3.1) obtenemos que

$$0 = \sum_{i=2}^{k} (\sigma(c_i) - c_i)\sigma_j(\alpha_i).$$

Recordemos que elegimos $c_1 = 1$. La minimalidad de k implica que $\sigma(c_i) - c_i = 0$ para todo $i = 2 \dots k$. Como esto es cierto para todo $\sigma \in G$ entonces $c_i \in F$. Pero hemos visto que esto no puede ser por lo cual $\mid G \mid = [L : F]$. □

Ejemplo 3.8. Sea $\Bbbk$ un cuerpo y $F = \Bbbk(t_1, \dots, t_n)$ el cuerpo de funciones racionales en n variables sobre $\Bbbk$. Podemos ver al grupo simétrico $\mathbb{S}_n$ como un subgrupo de $\mathrm{Aut}(F)$ de la siguiente manera:

$$\sigma\left(\frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)}\right) = \frac{f(t_{\sigma(1)}, \dots, t_{\sigma(n)})}{g(t_{\sigma(1)}, \dots, t_{\sigma(n)})},$$

para todo $\sigma \in \mathbb{S}_n$. Sea $K = \mathcal{F}(\mathbb{S}_n)$ el *cuerpo de funciones simétricas*. Por la Proposición 3.7 tenemos que $\mathbb{S}_n = \mathrm{Gal}(F/K)$ y $[F : K] = n!$.

Sean $s_1, \dots, s_n$ las funciones simétricas elementales, es decir

$$s_1 = t_1 + \cdots + t_n, \quad s_2 = \sum_{i \neq j} t_i t_j, \quad \dots \quad s_n = t_1 \dots t_n.$$

Entonces $\Bbbk(s_1, \dots, s_n) \subseteq \mathcal{F}(\mathbb{S}_n)$. Afirmamos que $\Bbbk(s_1, \dots, s_n) = \mathcal{F}(\mathbb{S}_n)$. En efecto, sea

$$f(t) = t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n \in \Bbbk(s_1, \dots, s_n)[t].$$

Se puede verificar que $f(t) = (t - x_1) \dots (t - x_n) \in F[t]$, esto implica que el cuerpo de raíces de $f(t)$ sobre $\Bbbk(s_1, \dots, s_n)$ es F. El ejercicio 8 implica que $[F : \Bbbk(s_1, \dots, s_n)] \leq n!$ pero como $[F : K] = n!$ esto implica que necesariamente $\Bbbk(s_1, \dots, s_n) = \mathcal{F}(\mathbb{S}_n)$. En otras palabras, cualquier función simétrica puede ser escrita en terminos de las funciones simétricas elementales.

Definición 3.9. Si L/F es una extensión algebraica se dice que L es *Galois* sobre F si $F = \mathcal{F}(\mathrm{Gal}(L/F))$.

Corolario 3.10. *Sea L/F una extensión finita. Entonces L/F es una extensión Galois si y sólo si $|\mathrm{Gal}(L/F)| = [L : F]$.* □

El siguiente corolario queda como ejercicio para el lector.

Corolario 3.11. *Sea L/F una extensión y sea $\alpha \in L$ algebraico sobre F, entonces*

1. *$|\mathrm{Gal}(F(\alpha)/F)|$ es igual al número de raíces distintas de $p_{F,\alpha}$ en $F(\alpha)$.*
2. *$F(\alpha)$ es Galois sobre F si y sólo si $p_{F,\alpha}$ posee n raíces distintas, donde $n = gr(p_{F,\alpha})$.* □

Ejercicio 16. Demostrar que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es Galois.

Ejercicio 17. Sea $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ y sea F el cuerpo de raíces de f. Demostrar que $\mathrm{Gal}(F/\mathbb{Q}) = \mathbb{S}_5$.

Ejercicio 18. Sea $\Bbbk$ un cuerpo de caracteristica $p > 0$. Demostrar que $\mathrm{Gal}(\Bbbk(t)/\Bbbk(t^p)$ es trivial y que la extensión $\Bbbk(t)/\Bbbk(t^p)$ no es Galois.

4. El teorema fundamental de la teoría de Galois

Sea L/F una extensión y $\alpha \in L$. Por el Corolario 3.11 la extensión $F(\alpha)/F$ no es Galois cuando $p_{F,\alpha}$ no tiene todas las raíces en $F(\alpha)$ o $p_{F,\alpha}$ posee raíces repetidas. Estas dos situaciones son tratadas en el contexto de extensiones separables y normales.

Definición 4.1. Si L/F es una extensión, L se dice *normal* sobre F si L es el cuerpo de raíces de un conjunto de polinomios con coeficientes en F.

Definición 4.2. (a) Sea F un cuerpo. Un polinomio irreducible $f \in F[x]$ se dice *separable* sobre F si f no posee raíces repetidas en su cuerpo de raíces. Un polinomio $g \in F[x]$ se dice *separable* sobre F si todos los factores irreducibles de g son separables.

(b) Sea L/F una extensión y $\alpha \in L$. Se dice que α es *separable* sobre F si $p_{F,\alpha}$ es separable sobre F. L se dice separable sobre F si todo elemento en L es separable sobre F.

El siguiente resultado se utilizará más adelante. Para su demostración el lector puede consutlar a [M].

Teorema 4.3. *Sea L una extensión algebraica sobre F. Las siguientes afirmaciones son equivalentes:*

(i) *L es Galois sobre F.*
(ii) *L es normal y separable sobre F.*
(iii) *L es el cuerpo de raíces de un conjunto de polinomios separables sobre F.*

□

Teorema 4.4. *Sea L/F una extensión finita Galois y $G = \mathrm{Gal}(L/F)$. Existe una correspondencia biunívoca entre cuerpos intermedios de la extensión L/F y subgrupos de G. Además*

1. *Si K se corresponde al subgrupo H entonces*
$$[L : K] = |H| \quad y \quad [K : F] = [G : H].$$
2. *Si K se corresponde al subgrupo H entonces H es un subgrupo normal si y sólo si K/F es una extensión normal y en este caso* $\mathrm{Gal}(K/F) \simeq G/H$.

Demostración. Sea $F \subseteq K \subseteq L$ extensiones de cuerpos. Como L/F es Galois entonces L/F es normal y separable, lo que implica que L/K es normal y separable y por lo tanto Galois. Entonces $K = \mathcal{F}(\mathrm{Gal}(L/K))$. Es decir todo cuerpo intermedio es de la forma $\mathcal{F}(H)$ para algún subgrupo H de G.

Sea $H \subseteq G$ un subgrupo. Como H es finito entonces por la Proposición 3.7 se tiene que $H = \mathrm{Gal}(L/\mathcal{F}(H))$. Luego la corresponcencia del Lema 3.6 establece una correspondencia entre todos los subcuerpos intermedios y los subgrupos de G.

Si K se corresponde con el subgrupo H entonces por la Proposición 3.7 se tiene que $\mid H \mid = [L : K]$ además
$$[G : H] = \frac{\mid G \mid}{\mid H \mid} = \frac{[L : F]}{[L : K]} = [K : F].$$

□

Ejercicio 19. Sea F un cuerpo de caracteristica distinta a 2 y sea L un extensión de F tal que $[L : F] = 2$. Demostrar que $L = F(\alpha)$ para algun $\alpha \in L$ tal que $\alpha^2 \in F$. Demostrar que L es Galois sobre F.

Ejercicio 20. Determinar cuales de los siguientes cuerpos son extensiones Galois de $\mathbb{Q}$.

(a) $\mathbb{Q}(\omega)$ donde $\omega = e^{\frac{2\pi i}{3}}$,
(b) $\mathbb{Q}(\sqrt[4]{2})$,
(c) $\mathbb{Q}(\sqrt{5}, \sqrt{7})$.

Veamos una consecuencia del Teorema 4.4.

Teorema 4.5. *Sea F un cuerpo infinito y sea L/F una extensión. Existe un $\alpha \in L$ tal que $L = F(\alpha)$ si y sólo si la cantidad de cuerpos intermedios $F \subseteq K \subseteq L$ es finita.*

Demostración. Asumamos que existen finitos cuerpos intermedios $F \subseteq K \subseteq L$. Entonces $L = F(\alpha_1, \ldots, \alpha_n)$ para algunos $\alpha_1, \ldots, \alpha_n \in L$. Razonemos por inducción en n. Si $n = 1$ el resultado es trivial. Si denotamos $K = F(\alpha_1, \ldots, \alpha_{n-1})$, entonces como todo cuerpo intermedio entre F y K es un cuerpo intermedio de la extensión L/F por inducción $K = F(\beta)$ y así/ $L = F(\beta, \alpha_n)$. Para cada $a \in F$ denotamos el cuerpo $\Bbbk_a = F(a\beta + \alpha_n)$. Como F es infinito y los cuerpos intermedios de la extensión L/F son finitos, existen $a, b \in F$ tales que $\Bbbk_a = \Bbbk_b$. Por lo tanto

$$\beta = \frac{(a\beta + \alpha_n) - (b\beta + \alpha_n)}{a - b} \in \Bbbk_b.$$

Por lo tanto $\alpha_n = (a\beta + \alpha_n) - a\beta \in \Bbbk_a$, luego $L = \Bbbk_a$.

Recíprocamente, supongamos que $L = F(\alpha)$ y sea K un cuerpo tal que $F \subseteq K \subseteq L$. Entonces $L = K(\alpha)$. Sabemos que $p_{K,\alpha}$ divide a $p_{F,\alpha}$ en $K[x]$. Supongamos que

$$p_{K,\alpha} = a_0 + a_1 x + \cdots + x^r \in K[x].$$

Denotemos $K_0 = F(a_0, \ldots, a_{r-1}) \subseteq K$. Entonces $p_{K_0,\alpha}$ divide a $p_{K,\alpha}$. Por lo tanto

$$[L : K] = deg(p_{K,\alpha}) \geq deg(p_{K_0,\alpha}) = [L : K_0] = [L : K][K : K_0].$$

Entonces $[K : K_0] = 1$ y $K = K_0$, y por lo tanto K está determinado por $p_{K,\alpha}$. Como hay finitos divisores mónicos de $p_{F,\alpha}$ en $L[x]$ entonces existen finitas extensiones intermedias. □

Corolario 4.6. *Sea F un cuerpo infinito y sea L/F una extensión finita y separable. Entonces existe un $\alpha \in L$ tal que $L = F(\alpha)$.*

Demostración. Como la extensión L/F es finita y separable existen $\alpha_1, \ldots, \alpha_n \in L$ tales que $L = F(\alpha_1, \ldots, \alpha_n)$. Sea K el cuerpo de raíces del conjunto de polinomios $\{p_{F,\alpha_i} : 1 \leq i \leq n\}$. Como cada polinomio p_{F,α_i} es separable por el Teorema 4.3 la extensión K/F es Galois. Además $K \subseteq L$. Luego por el Teorema 4.4 los cuerpos intermedios $F \subseteq K' \subseteq K$ están en correspondencia con los subgrupos de $\mathrm{Gal}(K/F)$. Como $\mathrm{Gal}(K/F)$ es finito la cantidad de dichos cuerpos intermedios es finita. Por lo tanto los cuerpos intermedios de la extensión L/F es finita y el resultado sigue del Teorema 4.5.

□

Ejercicio 21. Sea p un número primo, $f(x) = x^n - p \in \mathbb{Q}[x]$ y L el cuerpo de raíces de f. Demostrar que para todo $n \geq 3$ el grupo $\mathrm{Gal}(L/\mathbb{Q})$ no es Abeliano.

Ejercicio 22. Sea F un cuerpo y $f \in F[x]$ un polinomio separable. Denotamos por L al cuerpo de raíces de f. Si $\alpha \in L$ es una raíz cualqueira y p es un primo que divide a $[L : F]$ demostrar que existe un subcuerpo $F \subseteq K \subseteq L$ tal que $L = K(\alpha)$ y $[L : K] = p$.

Ejercicio 23. Sea $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$ un polinomio irreducible. Demostrar que si F es el cuerpo de raíces de f y que $b > 0$ entonces $\mathrm{Gal}(F/\mathbb{Q}) = \mathbb{S}_3$.

Ejercicio 24. Sea $f(x) = x^6 - 14x^3 - 1 \in \mathbb{Q}[x]$. Sea F el cuerpo de raíces de f. Encontrar a F y calcular $\mathrm{Gal}(F/\mathbb{Q})$. Ayuda: $\alpha = \sqrt[3]{7 + 5\sqrt{2}}$ es raíz de f y $\alpha = \beta^3$ donde $\beta = 1 + \sqrt{2}$.

5. Solubilidad por radicales

Definición 5.1.

1. Una extensión L/F se dice una *extensión por radicales* si el cuerpo $L = F(a_1, \ldots, a_m)$ y existen enteros $n_1, \ldots, n_m$ tales que $a_1^{n_1} \in F$ y $a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$ para todo $i > 1$. Si $n = n_1 = \cdots = n_m$ entonces L se dice una extensión n-radical.
2. Un polinomio $f \in F[x]$ se dice *resoluble por radicales* si su cuerpo de raíces está contenido en una extensión por radicales de F.

Claramente si L es una extensión radical entonces es n-radical. Basta con tomar $n = n_1 \ldots n_m$.

Ejemplo 5.2. $\mathbb{Q}(\sqrt[4]{2})$ es una extensión 4-radical de $\mathbb{Q}$, pero también es una extensión 2-radical. Para ver esto último hay que considerar las extensiones

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{\sqrt{2}}) = \mathbb{Q}(\sqrt[4]{2}).$$

El siguiente resultado debido a Galois caracteriza aquellos polinomios que son resolubles por radicales.

Teorema 5.3. *Sea F un cuerpo de caracteristica cero y $f \in F[x]$. Si L es el cuerpo de raíces de f sobre F entonces f es resoluble por radicales si y sólo si el grupo* $\mathrm{Gal}(L/F)$ *es soluble.*

Ejercicio 25. Sea F la clausura algebraica de $\mathbb{F}_p$. Sea $L = F(x)$ y sea $f \in L[t]$ definido por $f(t) = t^p - t - x$. Llamemos a K al cuerpo de raíces de f sobre L. Demostrar que f no es resoluble por radicales sobre L y que el grupo de Galois $\mathrm{Gal}(K/L)$ es cíclico.

6. Apéndice: Grupos solubles

Un grupo G se dice soluble si existe una cadena de subgrupos

$$\{1\} \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G,$$

tal que G_i es un subgrupo normal en G_{i+1} y G_{i+1}/G_i es Abeliano.

Lema 6.1. *Sea G un grupo. Las siguientes afirmaciones se satisfacen:*

(i) *Si G es Abeliano entonces es soluble.*
(ii) *Si G es soluble entonces todo subgrupo y todo cociente de G son solubles.*
(iii) *Si $N \subseteq G$ es un subgrupo normal entonces G es soluble si y sólo si N y G/N son solubles.*

Ejemplo 6.2.

1. Los grupos $\mathbb{S}_2, \mathbb{S}_3, \mathbb{S}_4$ son solubles.
2. Los grupos $\mathbb{S}_n$ con $n \geq 5$ no son solubles.
3. Los grupos simples no Abelianos no son solubles.
4. Todo grupo finito de orden $p^a q^b$ con p, q primos es soluble (Teorema de Burnside).
5. Todo grupo de orden menor a 60 es soluble.
6. Todo grupo de orden impar es soluble (Teorema de Feit-Thompson).

Referencias

[E] H. Edwards, *Galois theory*, Graduate texts in mathematics, Springer-Verlag **101**, (1984).
[G] M. Gastaminza, *Extensiones Algebraicas y Teoría de Galois*, Notas de Curso (1), Universidad Nacional del Sur (1991).
[M] P. Morandi, *Field and Galois theory*, Graduate texts in mathematics, Springer-Verlag **167**, (1996).
[W] S. Weintraub, *Galois theory*, Universitext, Springer (2009).

Universidad Nacional de Córdoba, Universidad Nacional de Cuyo.
E-mail address: martin10090@gmail.com, sebastian.simondi@gmail.com