Teoría de cuerpos

Matemáticas en LaTeX

3 de noviembre de 2024

Índice general

Capítulo 1

Extensiones de cuerpos

1.1. Introducción

Definición 1.1. Un anillo es un conjunto no vacío R con dos operaciones internas tal que:

1. $(R, +)$ es un grupo abeliano.
2. La multiplicación es asociativa.
3. $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$ para todo $a, b, c \in R$.

Si además la multiplicación es conmutativa entonces R es un anillo conmutativo. Si R contiene un elemento neutro para la multiplicación, entonces R es un anillo unitario.

Ejemplo. $\mathbb{Z}$, $\mathbb{Z}_n$ y $\mathbb{Q}[x]$ son anillos conmutativos unitarios.

Definición 1.2. Sea R un anillo conmutativo unitario, con neutro no nulo. Un elemento $a \in R$ no nulo es un divisor de cero si existe un elemento $b \in R$ no nulo tal que $ab = 0$.
R se llama dominio de integridad si no tiene divisores de cero. Si además todo elemento no nulo es invertible, entonces R es un cuerpo.

Ejemplo. $\mathbb{Z}_n$ es un dominio de integridad si y solo si n es primo.

Ejemplo. $\mathbb{Z}$ es un dominio de integridad, pero no todo elemento de $\mathbb{Z}$ es invertible. Luego $\mathbb{Z}$ no es un cuerpo.
En $\mathbb{Q}[x]$, no todo polinomio tiene una inversa. Sin embargo, como $\mathbb{Q}[x]$ es un dominio de integridad, podemos construir su cuerpo de fracciones.

$$\mathbb{Q}(x) = \left\{ \frac{p(x)}{q(x)} : p, q \in \mathbb{Q}[x], q(x) \neq 0 \right\}$$

Este es el cuerpo más pequeño que contiene a $\mathbb{Q}[x]$.

Definición 1.3. Sea R un anillo. Un subconjunto S de R no vacío es un subanillo si es cerrado bajo las operaciones de R y S es un anillo.
Si K es un cuerpo, entonces un subconjunto F de K no vacío es un subcuerpo si, bajo las operaciones de K, F es un cuerpo. El elemento neutro de F será 1_K.
El subcuerpo más pequeño de K se llama cuerpo primal de K.

Ejemplo. El cuerpo primal de $\mathbb{R}$ o $\mathbb{C}$ es $\mathbb{Q}$.

1.2. Extensiones de cuerpos

Definición 1.4. Sean F y K cuerpos. Decimos que K es una extensión de F cuando F es un subcuerpo de K. Lo denotamos K/F. Se tiene que $(K, +, *_F)$ es un espacio vectorial sobre F.

Definición 1.5. Un espacio vectorial es un conjunto V con un cuerpo F y dos operaciones tales que:

1. $(V, +)$ es un grupo abeliano.
2. La multiplicación escalar $*_F : F \times V \to V$ satisface las siguientes propiedades:
   a) $a(v + w) = av + aw$, para todo $a \in F, v, w \in V$.
   b) $(a + b)v = av + bv$, para todo $a, b \in F, v \in V$.
   c) $(ab)v = a(bv)$, para todo $a, b \in F, v \in V$.
   d) $1_F v = v$ para todo $v \in V$.

Ejemplo. $\mathbb{C}$ es una extensión de cuerpos de $\mathbb{R}$. Como $\mathbb{C}$ es un espacio vectorial sobre $\mathbb{R}$, ha de tener una base. En efecto, los elementos 1 e i son linealmente independientes sobre $\mathbb{R}$ y constituyen una base de $\mathbb{C}$.
Por tanto, $\mathbb{C}/\mathbb{R}$ es un espacio vectorial de dimensión 2.

Definición 1.6. Sea K/F una extensión de cuerpos. El grado de K/F, denotado por $[K : F]$, es la dimensión de K como espacio vectorial sobre F.
Si el grado de K/F es finito, decimos que la extensión es finita. En caso contrario, decimos que la extensión es infinita.

Ejemplo. Consideramos de nuevo el cuerpo $\mathbb{Q}(x)$, que es el cuerpo de fracciones de $\mathbb{Q}[x]$. Este es una extensión de cuerpos de $\mathbb{Q}$.
En el espacio vectorial $\mathbb{Q}(x)$ sobre $\mathbb{Q}$, el conjunto $\{1, x, x^2, \ldots\}$ es linealmente independiente, con infinitos elementos. Por tanto, no existe una base finita, luego la extensión $\mathbb{Q}(x)/\mathbb{Q}$ es infinita.

Observación. Una extensión de cuerpos K/F tiene grado 1 si y solo si $K = F$.
Si el grado es 1, todo elemento no nulo de K es una base sobre K, en particular $1_K = 1_F$. Por tanto, $K = \{a1_F : a \in F\} = F$.

Teorema 1.1 (Teorema de la torre)**.** *Sea $F \subseteq K \subseteq L$ una sucesión de extensiones de cuerpos.*

1. *Si $[K : F] = \infty$ o $[L : K] = \infty$, entonces $[L : F] = \infty$.*
2. *Si $[K : F] < \infty$ y $[L : K] < \infty$. Entonces $[L : F] = [L : K][K : F]$.*

1.3. Elementos algebraicos y trascendentes

Definición 1.7. Sea K/F una extensión de cuerpos y $\alpha \in K$. Decimos que α es algebraico sobre F si existe un polinomio $f \in F[x]$ no constante tal que $f(\alpha) = 0$.
Si α no es algebraico sobre F, entonces decimos que es trascendente sobre F.

Ejemplo. $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, puesto que es una raíz de $x^2 - 2 \in \mathbb{Q}[x]$.

Ejemplo. Veamos que $\sqrt{2} + \sqrt{3}$ es también algebraico sobre $\mathbb{Q}$. Sea $\alpha = \sqrt{2} + \sqrt{3}$.

$$\begin{aligned}(\alpha - \sqrt{2})^2 &= 3\\ \alpha^2 - 2\sqrt{2}\alpha + 2 - 3 &= 0\\ \alpha^2 - 1 &= 2\sqrt{2}\alpha\\ \alpha^4 + 1 - 2\alpha^2 &= 8\alpha^2\\ \alpha^4 - 10\alpha^2 + 1 &= 0\end{aligned}$$

Luego $\alpha = \sqrt{2} + \sqrt{3}$ es raíz de $x^4 - 10x^2 + 1$.

Ejemplo. π es trascendente sobre $\mathbb{Q}$. Sin embargo, π es algebraico sobre $\mathbb{R}$, pues es raíz de $x-\pi \in \mathbb{R}[x]$.

Definición 1.8. Se dice que una extensión de cuerpos es algebraica cuando cada elemento en K es algebraico sobre F. De lo contrario, se dice que la extensión es trascendente.

Ejemplo. $\mathbb{R}/\mathbb{Q}$ es trascendente puesto que $\mathbb{R}$ tiene elementos transcendentes sobre $\mathbb{Q}$.
Sin embargo, $\mathbb{C}/\mathbb{R}$ es algebraico, porque todo elemento complejo $a+bi$ es raíz del polinomio:

$$(x-(a+bi))(x-(a-bi)) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$$

Observación. En una extensión de cuerpos K/F cada elemento de F es algebraico sobre F. Además, si $\alpha \in K$ es algebraico sobre F, entonces también es algebraico sobre todo cuerpo F' entre F y K.

1.4. Nociones de anillos de polinomios

Teorema 1.2 (Algoritmo de la división)**.** *Sea R un anillo unitario y $f, g \in \mathbb{R}[x]$ polinomios no nulos tales que el coeficiente líder de g sea un elemento neutro de R. Entonces existen dos únicos polinomios $q, r \in \mathbb{R}[x]$ tales que:*

$$f(x) = q(x)g(x) + r(x), \quad \text{con } r(x) = 0 \text{ o } grad(r(x)) < grad(g(x))$$

Corolario 1.3 (Algoritmo de Euclides e identidad de Bezout)**.** *Sea F un campo, $f, g \in F[x]$ polinomios no constantes y $d = MCD(f, g)$. Entonces existen polinomios $a, b \in F[x]$ tales que:*

$$d(x) = a(x)f(x) + b(x)g(x)$$

Corolario 1.4. *Todo ideal en $F[x]$ es principal, es decir, $F[x]$ es un dominio de ideales maximales.*

Corolario 1.5. *Si f es irreducible, entonces el ideal (f) es maximal en $F[x]$.*

1.5. Polinomio mínimo

Proposición 1.6. *Si $\alpha \in K$ es algebraico sobre F, entonces existe un único polinomio mónico $f \in F[x]$ tal que:*

1. *$f(\alpha) = 0$.*
2. *Si $g \in F[x]$ y $g(\alpha) = 0$, entonces f divide a g en $F[x]$.*

Definición 1.9. Dicho polinomio se llama polinomio mínimo de α sobre F.

Proposición 1.7. *Sea $\alpha \in K$ algebraico sobre F y $f \in F[x]$ un polinomio mónico no constante. Entonces las siguientes afirmaciones son equivalentes.*

1. *f es el polinomio mínimo de α sobre F.*
2. *f tiene grado mínimo entre los polinomios con raíz α.*
3. *f es irreducible y $f(\alpha) = 0$.*

Ejemplo. Trabajaremos frecuentemente con el elemento $\xi_n = e^{\frac{2\pi i}{n}}$. Es claro que $\xi_n^n = 1$, así que podemos decir que ξ_n es algebraico sobre $\mathbb{Q}$ y que su polinomio mínimo es un factor irreducible de $x^n - 1$. El polinomio mínimo de ξ_n sobre $\mathbb{Q}$ se llama polinomio ciclotómico de orden n. Si n es primo, este polinomio ciclotómico es:

$$x^{n-1} + x^{n-2} + \cdots + x + 1$$

Ejemplo. Hemos visto que $f(x) = x^4 - 10x^3 + x^2 + 1$ se anula en $\sqrt{2} + \sqrt{3}$. Si comprobamos que f es irreducible, podremos afirmar que este es el polinomio mínimo de $\sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$.

1.6. Construcción de extensiones

Definición 1.10. Sea K/F una extensión de cuerpos y X un subconjunto de K. El menor subcuerpo de K que contiene a $F \cup X$ se denota por $F(X)$ y se llama subcuerpo de K generado por X sobre F.

Definición 1.11. El subanillo más pequeño de K que contiene a $F \cup X$ se denota por $F[X]$. Siempre se tiene que $F[X] \subseteq F(X) \subseteq K$ y $F[X]$ es un dominio de integridad.

Definición 1.12. Si X es finito, $X = \{u_1, \ldots, u_n\}$, escribimos $F(X) = F(u_1, \ldots, u_n)$ y decimos que la extensión es finitamente generada sobre F.
Una extensión de cuerpos de la forma $F(u)$ se llama extensión simple.

Proposición 1.8. *Sea K/F una extensión de cuerpos, $u, u_i \in K, X \subseteq K$.*

1. $F[u] = \{f(u) : f(x) \in F[x]\}$.
2. $F[u_1, \ldots, u_n] = \{f(u_1, \ldots, u_n) : f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]\}$.
3. $F[X] = \{f(u_1, \ldots, u_n) : n \in N, u_i \in X, f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]\}$.
4. $F(u) = \left\{ \frac{f(u)}{g(u)} : f(x), g(x) \in F[x], g(x) \neq 0 \right\}$.
5. $F(u_1, \ldots, u_n) = \left\{ \frac{a}{b} : a, b \in F[u_1, \ldots, u_n], b \neq 0 \right\}$.
6. $F(X) = \left\{ \frac{a}{b} : a, b \in F[x], b \neq 0 \right\}$.

Ejemplo. Consideramos el anillo $\mathbb{Q}[\sqrt{3}]$.

$$\mathbb{Q}[\sqrt{3}] = \{f(\sqrt{3}) : f(x) \in \mathbb{Q}[x]\}$$

Sea $f(x) \in \mathbb{Q}[x]$. Entonces podemos dividir $f(x)$ por el polinomio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}$, $x^2 - 3$. De esta forma, obtenemos polinomios $q(x), r(x) \in \mathbb{Q}[x]$ únicos, con $grad(r(x)) < 2$, tales que:

$$f(x) = (x^2 - 3)q(x) + r(x)$$

Entonces, existen $a, b \in \mathbb{Q}$ tales que $r(x) = a + bx$. Evaluando en $\sqrt{3}$:

$$f(\sqrt{3}) = 0 + r(\sqrt{3})$$

Por tanto:

$$\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$$

Proposición 1.9. *Sea K/F una extensión de cuerpos. Si $\alpha \in K$ es algebraico sobre F, entonces:*

1. $F[\alpha] = F(\alpha)$.
2. $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *es una base de $F(\alpha)$ sobre F, donde n es el grado del polinomio mínimo de α sobre F.*
3. $[F(\alpha) : F] = n$.

Ejemplo. $\mathbb{Q}(\sqrt{3})$ es una extensión de cuerpos de $\mathbb{Q}$. Tiene grado 2 y una base es $\{1, \sqrt{3}\}$.

Ejemplo. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2})$.

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3})$$

Por el teorema de la torre:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

Además, una base para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$ es $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Ejemplo. $\mathbb{Q}(\pi)$ es una extensión finitamente generada sobre $\mathbb{Q}$. Sin embargo, no es una extensión finita, puesto que $\{1, \pi, \pi^2, \ldots\}$ es linealmente independiente. En caso contrario, π sería algebraico sobre $\mathbb{Q}$.

1.7. Extensiones algebraicas

Proposición 1.10. *Sea K/F una extensión finita. Entonces:*

1. *K/F es algebraica.*
2. *El grado del polinomio mínimo de $\alpha \in K$ sobre F divide a $[K : F]$.*

Observación. No toda extensión algebraica es finita. Consideramos por ejemplo:

$$\bar{\mathbb{Q}} = \{\alpha : \alpha \text{ es algebraico sobre } \mathbb{Q}\}$$

Esta es una extensión algebraica infinita de $\mathbb{Q}$.

Proposición 1.11. *Sea K/F una extensión de cuerpos. Entonces $[K : F] < \infty$ si y solo si existen $\alpha_1, \ldots, \alpha_m \in K$ algebraicos sobre F tales que $K = F(\alpha_1, \ldots, \alpha_m)$.*

Proposición 1.12. *Dada una extensión de cuerpos K/F, el siguiente subconjunto es un cuerpo intermedio de K/F:*

$$M = \{\alpha \in K : \alpha \text{ es algebraico sobre } F\}$$

Proposición 1.13. *Sea $F \subseteq K \subseteq L$ una sucesión de cuerpos. Si $\alpha \in L$ es algebraico sobre K y K es algebraico sobre F, entonces α es algebraico sobre F.*

Capítulo 2

Homomorfismos de cuerpos

2.1. Homomorfismos de anillos y cuerpos

Definición 2.1. Sean R y S anillos. Una aplicación $f : R \to S$ es un homomorfismo de anillos si para todo $a, b \in R$ se verifica:

1. $f(a + b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$

Ejemplo. Consideramos el homomorfismo de anillos:

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{3}]$$

Esta aplicación deja fijo a todo número racional y envía x a $\sqrt{3}$. Entonces, si $p(x) = a_0 + a_1x + \cdots + a_mx^m \in \mathbb{Q}[x]$:

$$\begin{aligned}\varphi(p(x)) &= \varphi(a_0 + a_1x + \cdots + a_mx^m) = \varphi(a_0) + \varphi(a_1x) + \cdots + \varphi(a_mx^m) \\ &= \varphi(a_0) + \varphi(a_1)\varphi(x) + \cdots + \varphi(a_m)\varphi(x^m) = a_0 + a_1\sqrt{3} + \cdots + a_m\sqrt{3^m} = p(\sqrt{3})\end{aligned}$$

Su núcleo es el conjunto:

$$Ker(\varphi) = \{f(x) \in \mathbb{Q}[x] : f(\sqrt{3}) = 0\} = (x^2 - 3)$$

Como φ is sobreyectiva, por el primer teorema de isomorfía tenemos que:

$$\mathbb{Q}[\sqrt{3}] \equiv \mathbb{Q}[x]/(x^2 - 3)$$

Como $x^2 - 3$ es irreducible y $\mathbb{Q}[x]$ es un dominio de ideales principales, entonces $(x^2 - 3)$ es un ideal maximal y por tanto $\mathbb{Q}[\sqrt{3}]$ es un cuerpo.

Observación. Si f es un homomorfismo de anillos, entonces $f(0) = 0$. Como siempre trabajaremos con anillos conmutativos unitarios, consideraremos homomorfismos entre anillos unitarios y añadiremos la condición $f(1_R) = 1_S$.

Definición 2.2. Sean K_1, K_2 cuerpos. Un homomorfismo de cuerpos de K_1 a K_2 es una aplicación $f : K_1 \to K_2$ tal que para todo $a, b \in R$ se verifica:

1. $f(a + b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$
3. $f(1_{K_1}) = 1_{K_2}$

Observación. Si $f : K_1 \to K_2$ es un homomorfismo de cuerpos, entonces $f(-a) = -f(a)$ para todo $a \in K_1$. Si además a es un elemento no nulo, entonces $f(a^{-1}) = f(a)^{-1}$.

Ejemplo. Consideramos el isomorfismo de anillos del ejemplo anterior.

$$\mathbb{Q}[x]/(x^2 - 3) \equiv \mathbb{Q}(\sqrt{3})$$

Observamos que es de hecho un isomorfismo de cuerpos que identifica cada clase del cociente $\mathbb{Q}[x]/(x^2 - 3)$ con un elemento de $\mathbb{Q}(\sqrt{3})$. En efecto, para cada polinomio $p(x) \in \mathbb{Q}[x]$, su clase $p(x) + (x^2 - 3)$ puede ser representada por el resto de la división de $p(x)$ por $x^2 - 3$, que será un polinomio de la forma $a + bx$, con $a, b \in \mathbb{Q}$. Entonces, el elemento correspondiente en $\mathbb{Q}(\sqrt{3})$ es $\varphi(a + bx) = a + b\sqrt{3}$.

Observación. Todo homomorfismo de cuerpos es inyectivo, es decir, todo homomorfismo de cuerpos es un monomorfismo.

2.2. F-homomorfismos

Definición 2.3. Sean K/F, K'/F extensiones de cuerpos. Un F-homomorfismo de K a K' es un homomorfismo de cuerpos $\varphi : K \to K'$ tal que $\varphi(a) = a$ para todo $a \in F$. Podemos definir análogamente los conceptos de F-endomorfismo, F-isomorfismo, F-monomorfismo y F-automorfismo.

Teorema 2.1. *Sea K/F una extensión de cuerpos, $u \in K$ trascendente sobre F. Entonces existe un F-isomorfismo entre $F(u)$ y $F(x)$.*

Ejemplo. Existe un $\mathbb{Q}$-isomorfismo entre $\mathbb{Q}(\pi)$ y $\mathbb{Q}(x)$ que identifica π con x.

Teorema 2.2. *Sea K/F una extensión de cuerpos, $\alpha \in K$ algebraico sobre F y $f(x) \in F[x]$ el polinimio mínimo de α sobre F. Entonces existe un F-isomorfismo entre $F(\alpha)$ y $F[x]/(f(x))$.*

Ejemplo. Sea p un número primo, $\zeta_p = e^{2\pi i/p}$. Entonces $\mathbb{Q}(\zeta_p)$ es isomorfo a $\mathbb{Q}[x]/(x^{p-1} + x^{p-2} + \cdots + x + 1)$. El isomorfismo fija a los números racionales e identifica ζ_p con la clase del polinomio x módulo el ideal $(x^{p-1} + x^{p-2} + \cdots + x + 1)$.

2.3. Extensiones de monomorfismos de anillos

Definición 2.4. Sea $\sigma : F_1 \to F_2$ un homomorfismo de cuerpos y

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F_1[x]$$

Denotaremos por $f^\sigma(x)$ al polinomio

$$f^\sigma(x) = \sigma(a_n) x^n + \sigma(a_{n-1}) x^{n-1} + \cdots + \sigma(a_1) x + \sigma(a_0) \in F_2[x]$$

Observación. Recordamos que todo homomorfismo de cuerpos es un monomorfismo. Los monomorfismos de cuerpos también se llaman inmersiones.

Teorema 2.3. *Sea $\sigma : F_1 \to F_2$ un isomorfismo de cuerpos. Consideramos u, v elementos trascendentes sobre F_1 y F_2, respectivamente. Entonces existe un isomorfismo $\bar{\sigma} : F_1(u) \to F_2(v)$ que extiende a σ y tal que $\bar{\sigma}(u) = v$.*

Ejemplo. Consideramos el isomorfismo identidad $1_\mathbb{Q} : \mathbb{Q} \to \mathbb{Q}$ y el elemento trascendente π. Entonces, podemos definir un isomorfismo $\bar{\sigma} : \mathbb{Q}(\pi) \to \mathbb{Q}(v)$ que deje fijos a los números racionales y envíe π a cualquier elemento v trascendente sobre $\mathbb{Q}$. Observamos que en lugar de un isomorfismo podríamos considerar una inmersión, como la inclusión $\mathbb{Q} \to \mathbb{R}$, y podríamos extenderla a una inmersión $\mathbb{Q}(\pi) \to \mathbb{R}$ que deje fijo todo elemento de $\mathbb{Q}(\pi)$. Ahora la imagen de π es algebraica sobre $\mathbb{R}$.

Proposición 2.4. *Sean K_1/F_1 y K_2/F_2 extensiones de cuerpos, $\sigma : F_1 \to F_2$ un homomorfismo de cuerpos, $\alpha \in K_1$ algebraico sobre F_1 y $f(x)$ su polinomio mínimo sobre F_1. Si $\bar{\sigma} : K_1 \to K_2$ es un homomorfismo de cuerpos que extiende a σ, entonces $\bar{\sigma}(\alpha)$ es una raíz de $f^\sigma(x) \in F_2[x]$.*

Ejemplo. Consideramos el isomorfismo $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ dado por $\tau(a+b\sqrt{2}) = a-b\sqrt{2}, a, b \in \mathbb{Q}$. Si queremos extenderlo a un automorfismo $\bar{\tau}$ de $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2})$, la imagen de $\sqrt[4]{2}$ tiene que ser una raíz de $f^{\tau}(x)$, donde $f(x) = x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$ es el polinimio mínimo de $\sqrt[4]{2}$ sobre $\mathbb{Q}(\sqrt{2})$. Como $f^{\tau}(x) = x^2 - \tau(\sqrt{2}) = x^2 - (-\sqrt{2}) = x^2 + \sqrt{2}$, tenemos que $\bar{\tau}(\sqrt[4]{2})$ tiene que ser una raíz de $x^2 + \sqrt{2}$.

Teorema 2.5. *Sea $\sigma : F_1 \to F_2$ un isomorfismo de cuerpos. Si α es algebraico sobre F_1 con polinimio mínimo $f(x) \in F_1[x]$ y β es una raíz de $f^{\sigma}(x) \in F_2[x]$, entonces existe un isomorfismo $\bar{\sigma} : F_1(\alpha) \to F_2(\beta)$ que extiende a σ y tal que $\bar{\sigma}(\alpha) = \beta$.*

Corolario 2.6. *Sean $K/F, L/F$ extensiones de cuerpos, $\alpha \in K, \beta \in L$ algebraicos sobre F. Entonces α y β son raíces del mismo polinimio irreducible $f(x) \in F[x]$ si y solo si existe un F-isomorfismo $\sigma : F(\alpha) \to F(\beta)$ tal que $\sigma(\alpha) = \beta$.*

Definición 2.5. Si α y β son raíces del mismo polinomio irreducible $f(x) \in F[x]$, decimos que son raíces conjugadas sobre F.

Observación. Dos números complejos conjugados son raíces conjugadas sobre $\mathbb{R}$. Si $a, b \in \mathbb{R}$, $a + bi$ y $a - bi$ son raíces del polinomio

$$(x - (a + bi))(x - (a - bi)) = (x - a)^2 + b^2 = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$$

Observamos que este polinomio es irreducible cuando $b \neq 0$. Además, si $a, b \in \mathbb{Q}, b \neq 0$, entonces este polinomio es irreducible en $\mathbb{Q}[x]$. Sin embargo, $a + bi$ y $a - bi$ no son raíces conjugadas sobre $\mathbb{Q}(i)$.

Corolario 2.7. *Sean F_1, F_2, K cuerpos, $\sigma : F_1 \to F_2$ una inmersión, $F_2 \subset K$. Sea α un elemento en alguna extensión de cuerpos de F_1, algebraico sobre F_1, con polinomio mínimo $f(x) \in F_1[x]$. Entonces existe una inmersión $\bar{\sigma} : F_1(\alpha) \to K$ que entiende a σ si y solo si $\bar{\sigma}(\alpha)$ es una raíz de $f^{\sigma}(x)$. En particular, si denotamos por $Emb_{\sigma}(F_1(\alpha), K)$ el conjunto de inmersiones de $F_1(\alpha)$ en K extendiendo a σ, tenemos que*

$$|Emb_{\sigma}(F_1(\alpha), K)| = \textit{número de raíces distintas de } f^{\sigma}(x) \textit{ en } K$$

Definición 2.6. Sea K/F extensión de cuerpos. El grupo de F-automorfismos de K se llama el grupo de Galois de K sobre F. Se denota por $Gal(K/F)$ o por $Gal_F(K)$.

2.4. Cuerpo primo y característica

Definición 2.7. Sea F un cuerpo y $X \subset F$, consideramos todos los subcuerpos de F que contienen a X. Esta es una familia no vacía cuya intersección es el subcuerpo de F más pequeño que contiene a X. Este se llama el subcuerpo de F generado por X. Si $X = \emptyset, 0_F, 1_F$ o $0_F, 1_F$, el subcuerpo de F más pequeño generado por X es el subcuerpo más pequeño de F. Este se llama cuerpo primo de F y se denota por $\pi(F)$.

Proposición 2.8. *Si F es un cuerpo, $\pi(F)$ es isomofo a $\mathbb{Q}$ o a $\mathbb{Z}_p$, para algún número primo p.*

Definición 2.8. Cuando $\pi(F)$ es isomorfo a $\mathbb{Q}$ decimos que la característica de F es 0. Si $\pi(F)$ es isomorfo a $\mathbb{Z}_p$, decimos que la característica de F es p.

Capítulo 3

Extensiones normales

3.1. Cuerpo stem

Definición 3.1. Sea K/F una extensión de cuerpos y $f(x) \in F[x]$ no constante. Decimos que K es un cuerpo stem de f sobre F si existe $\alpha \in K$ raíz de f tal que $K = F(\alpha)$.

Ejemplo. $\mathbb{Q}(\sqrt{2})$ es un cuerpo stem de $x^2 - 2$ sobre $\mathbb{Q}$. Contiene todas las raíces de $x^2 - 2$. Por otro lado, $\mathbb{Q}(\sqrt[3]{2})$ es un cuerpo stem de $x^3 - 2$ sobre $\mathbb{Q}$ que no contiene todas las raíces de $x^3 - 2$.

Teorema 3.1 (Existencia del cuerpo stem)**.** *Sea F un cuerpo y $f(x) \in F[x]$ de grado $n > 0$. Entonces existe una extensión simple $F(\alpha)$ de F tal que:*

1. *α es una raíz de $f(x)$.*
2. *Si $f(x)$ es irreducible en $F[x]$, entonces el cuerpo $F(\alpha)$ es único salvo F-isomorfismos.*

Ejemplo. Construyamos un cuerpo stem de $f(x) = x^4 + x^2 - x + 1$ sobre $\mathbb{Z}_5$. En primer lugar observamos que $f(x) \in \mathbb{Z}_5[x]$ es irreducible. Entonces $F = \mathbb{Z}_5[x]/(x^4 + x^2 - x + 1)$ es un cuerpo stem. Además, cualquier otro cuerpo stem de f sobre $\mathbb{Z}_5$ es $\mathbb{Z}_5$-isomorfo a F. Observamos que F tiene 5^4 elementos y que $[F : \mathbb{Z}_5] = 4$.

Ejemplo. Construyamos un cuerpo stem de $f(x) = x^5 + 3x^3 + x^2 + 2x + 2$ sobre $\mathbb{Z}_5$. Como se tiene que $f(x) = (x^2 + 2)(x^3 + x + 1)$, podemos construir dos cuerpos stem no isomorfos, cada uno con un factor irreducible: $\mathbb{Z}_5[x]/(x^2 + 2)$ y $\mathbb{Z}_5[x]/(x^3 + x + 1)$. Podemos asegurar que no son isomorfos porque son cuerpos finitos con distinto número de elementos. Tienen respectivamente 5^2 y 5^3 elementos.

Ejemplo. Consideramos el polinomio $f(x) = x^4 + 1$ sobre $\mathbb{Z}_5$. Obsservamos que es reducible: $f(x) = (x^2 + 2)(x^2 + 3)$. Podemos construir un cuerpo stem con cada factor irreducible: $\mathbb{Z}_5[x]/(x^2 + 2)$ y $\mathbb{Z}_5[x]/(x^2 + 3)$. Sin embargo, en este caso son isomorfos, aunque ningún isomorfismo envía $\alpha = x + (x^2 + 2)$ a $\beta = x + (x^2 + 3)$, puesto que son raíces de polinomios irreducibles diferentes.

Ejemplo. El polinomio $f(x) = (x^2 - 5)(x^2 - 11) \in \mathbb{Q}[x]$ tiene dos cuerpos stem no isomorfos: $\mathbb{Q}(\sqrt{5})$ y $\mathbb{Q}(\sqrt{11})$. Consideramos el polinomio $f(x) = (x^2 - 5)(x^2 - 2x - 4) \in \mathbb{Q}[x]$. Podemos construir un cuerpo stem para cada factor irreducible: $\mathbb{Q}(\sqrt{5})$ y $\mathbb{Q}(\alpha)$, donde α es una raíz de $x^2 - 2x - 4$. Sin embargo, como las raíces de este último factor son $1 \pm \sqrt{5}$, luego ambos cuerpos stem son el mismo.

3.2. Cuerpo de descomposición

Definición 3.2. Sea K/F una extensión de cuerpos y $f(x) \in F[x]$ un polinomio no constante. Decimos que $f(x)$ se descompone completamente sobre K si $f(x) = a(x - \alpha_1) \dots (x - \alpha_r)$, con $a \in F, \alpha_i \in K$.

Ejemplo. x^2-2 se descompone completamente sobre $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{R}$ y $\mathbb{C}$. No se descompone sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(i)$.

Definición 3.3. Sea F un cuerpo y $f(x)\in F[x]$ no constante. Una extensión K de F es un cuerpo de descomposición de f sobre F si:

1. $f(x)$ se descompone completamente sobre K.
2. $K=F(\alpha_1,\ldots,\alpha_r)$, con $\alpha_1,\ldots,\alpha_r$ las raíces de $f(x)$ en K.

Ejemplo. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ es cuerpo de descomposición de $(x^2-2)(x^2-3)$ sobre $\mathbb{Q}$.

Ejemplo. $\mathbb{Q}(\sqrt[4]{2},i)$ es cuerpo de descomposición de x^4-2 sobre $\mathbb{Q}$.

$$x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-i\sqrt[4]{2})(x+i\sqrt[4]{2}) \text{ y } \mathbb{Q}(\pm\sqrt[4]{2},\pm i\sqrt[4]{2})=\mathbb{Q}(\sqrt[4]{2},i)$$

Ejemplo.
1. $\mathbb{Q}(i)$ es cuerpo de descomposición de x^2+1 sobre $\mathbb{Q}$.
2. $\mathbb{C}$ es cuerpo de descomposición de x^2+1 sobre $\mathbb{R}$.
3. $\mathbb{C}$ es cuerpo de descomposición de x^2+1 sobre $\mathbb{C}$.

Teorema 3.2 (Existencia de cuerpo de descomposición)**.** *Sea $f\in F[x]$ un polinomio de grado $n>0$. Entonces existe un cuerpo de descomposición K de f sobre F.*

Teorema 3.3. *Sea $\sigma: F_1\to F_2$ un isomorfismo de cuerpos y $f(x)\in F_1[x]$ de grado $n>0$. Si K_1 es cuerpo de descomposición de $f(x)$ sobre F_1 y K_2 es cuerpo de descomposición de $f^\sigma(x)$ sobre F_2, entonces σ puede ser extendido a un isomorfismo $\bar{\sigma}: K_1\to K_2$.*

Corolario 3.4 (Unicidad del cuerpo de descomposición)**.** *Dos cuerpos de descomposición de $f(x)\in F[x]$ sobre F son F-isomorfos.*

Definición 3.4. Si S es un subconjunto de $F[x]$, una extensión de cuerpos K de F es cuerpo de descomposición de S sobre F cuando:

1. $f(x)$ se descompone completamente sobre K para cada $f(x)\in S$.
2. $K=F(X)$ con $X=\{\alpha\in K:\alpha \text{ es raíz de algún } f(x)\in S\}$.

Observación. Observamos que el cuerpo de descomposición de una familia finita de polinomios

$$f_1(x),\ldots,f_m(x)\in F[x]$$

es el mismo que el cuerpo de descomposición del producto de polinomios $f(x)=\prod_{i=1}^m f_i(x)\in F[x]$. Por tanto, la definición previa solo es interesante cuando la familia S de polinomios es infinita.

3.3. Clausura algebraica y cuerpos algebraicamente cerrados

Definición 3.5. Un cuerpo F es algebraicamente cerrado si no tiene extensiones algebraicas. Es decir, si K es una extensión algebraica de F, entonces $K=F$.

Proposición 3.5. *F es algebraicamente cerrado si y solo si todo polinomio irreducible en $F[x]$ tiene grado 1.*

Definición 3.6. Una extensión K/F es clausura algebraica de F si K es algebraico sobre F y K es algebraicamente cerrado.

Proposición 3.6. *K es clausura algebraica de F si y solo si K es cuerpo de descomposición de $F[x]$ sobre F.*

Teorema 3.7 (Existencia de clausura algebraica)**.** *Sea F un cuerpo. Entonces existe una clausura algebraica de F.*

Corolario 3.8. *Sea $S \subseteq F[x]$. Entonces existe un cuerpo de descomposición de S sobre F.*

Teorema 3.9. *Sea K/F una extensión algebraica y L un cuerpo algebraicamente cerrado. Todo homomorfismo de cuerpos $F \to L$ puede ser extendido a un homomorfismo de cuerpos $K \to L$.*

Corolario 3.10 (Unicidad de la clausura algebraica)**.** *Dos clausuras algebraicas de un cuerpo F son F-isomorfas.*

Corolario 3.11 (Unicidad del cuerpo de descomposición)**.** *Sea $S \subseteq F[x]$. Dos cuerpos de descomposición de S sobre F son F-isomorfos.*

3.4. Extensiones normales

Definición 3.7. Una extensión algebraica K/F es normal si todo polinomio irreducible $f(x) \in F[x]$ que tiene una raíz en K se descompone completamente sobre K.

Ejemplo. Observamos que $\mathbb{Q}(\sqrt[3]{2})$ no es una extensión normal de $\mathbb{Q}$.

Teorema 3.12. *Sea K cuerpo de descomposición de un polinomio $f(x) \in F[x]$ sobre F. Entonces K/F es normal.*

Observación. Si K es el cuerpo de descomposición de un conjunto $S \in F[x]$, entonces K/F es normal.

Teorema 3.13. *Sea K/F una extensión algebraica. Entonces K/F es finita y normal si y solo si K es cuerpo de descomposición sobre F de algún $f(x) \in F[x]$.*

Observación. Existe una equivalencia entre extensiones normales y cuerpos de descomposición cuando la extensión es infinita.
Sabemos que un cuerpo de descomposición de una familia de polinomios $S \subseteq F[x]$ es una extensión normal de F.
Supongamos ahhora que K/F es normal e infinita y tomamos una base $\{u_i : i \in I\}$ de K sobre F. Consideramos el conjunto:

$$S = \{f_i(x) \in F[x] : i \in I\}$$

donde cada $f_i(x) \in F[x]$ es el polinomio mínimo de α_i sobre F. Entonces K es el cuerpo de descomposición de S sobre F.

Ejemplo. Sea $S = \{\sqrt{p} : p \text{ primo en } \mathbb{Z}\}$. $\mathbb{Q}(S)$ es una extensión infinita de $\mathbb{Q}$.
Es claro que $\mathbb{Q}(S)$ es el cuerpo de descomposición de la familia de polinomios $\{x^2 - p : p \text{ primo en } \mathbb{Z}\}$. Entonces es una extensión normal de $\mathbb{Q}$, que es infinito.

Definición 3.8. Sea K/F algebraica. Una extensión L de K se llama clausura normal de K/F si:

1. L/F es normal.
2. Si $K \subseteq M \subseteq L$ y M/F es normal, entonces $M = L$.

Ejemplo. Sabemos que $\mathbb{Q}(\sqrt[3]{2})$ no es normal sobre $\mathbb{Q}$. Si adjuntamos las raíces conjugadas de $\sqrt[3]{2}$ sobre $\mathbb{Q}$, obtenemos:

$$L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$$

que es una extensión normal de $\mathbb{Q}$ porque es el cuerpo de descomposición de $x^3 - 2$.
Cualquier otra extensión de $\mathbb{Q}(\sqrt[3]{2})$ normal sobre $\mathbb{Q}$ debe contener a las raíces conjugadas de $\sqrt[3]{2}$ sobre $\mathbb{Q}$. Por tanto, L es clausura normal de $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$.

Teorema 3.14 (Existencia y unicidad de la clausura normal)**.** *Sea K/F algebraica. Entonces existe una clausura normal de K/F. De hecho, dos clausuras normales de K/F son K-isomorfas.*

Proposición 3.15. *Sea K/F algebraica y L su clausura normal. Entonces K/F es finita si y solo si L/F es finita.*

Capítulo 4

Extensiones separables

4.1. Polinomios separables

Definición 4.1. Un polinomio no constante $f(x) \in F[x]$ se llama separable si sus raíces en un cuerpo de descomposición son todas simples.

Ejemplo. Para dar un ejemplo de un polinomio no separable basta con elegir un polinomio reducible con factores repetidos, como:

$$x^2 - 2x + 1 = (x-1)^2 \in \mathbb{Q}[x]$$
$$x^4 - 4x^2 + 4 = (x^2-2)^2 \in \mathbb{Q}[x]$$

Proposición 4.1. *Sea $f \in F[x]$ un polinomio mónico y no constante. Entonces las afirmaciones siguientes son equivalentes:*

1. *f es separable.*
2. *f y su derivada f' son primos relativos en $F[x]$.*

En particular, si $f \in F[x]$ es irreducible, entonces f es separable si y solo si $f' \neq 0$.

Corolario 4.2. *Sea $f(x) \in F[x]$ un polinimio irreducible de grado $n > 0$. Si se verifica una de las siguientes condiciones, entonces $f(x)$ es separable:*

- *$char(F) = 0$.*
- *$char(F) = p$ y p no divide a n.*

4.2. Cuerpos perfectos y extensiones separables

Definición 4.2. Un cuerpo F es perfecto si todo polinomio irreducible $f(x) \in F[x]$ es separable.

Teorema 4.3. *Un cuerpo F es perfecto si y solo si se verifica una de las siguientes condiciones:*

- *$char(F) = 0$.*
- *$char(F) = p$ y para cada $a \in F$ existe $b \in F$ tal que $a = b^2$.*

Observación. Para cada cuerpo F de característica p, la aplicación

$$\varphi : F \to F$$

definida por $\varphi(a) = a^p$ para cada $a \in F$ es un endomorfismo inyectivo. Se conoce como el endomorfismo de Frobenius.

Observamos que, por el teorema previo, F es perfecto si y solo si φ es un automorfismo.
Cuando F es finito, φ es una aplicación inyectiva entre conjuntos del mismo cardinal finito, así que tiene que ser sobreyectiva. Luego todo cuerpo finito es perfecto.

Definición 4.3. Si K/F es una extensión de cuerpos y $\alpha \in K$ es algebraico sobre F, decimos que α es separable sobre F cuando su polinomio mínimo sobre F es separable.
Una extensión algebraica K/F es separable si cada elemento de K es separable sobre F. Equivalentemente, K/F es separable si cada polinomio irreducible $f(x) \in F[x]$ con una raíz en K es separable.

Proposición 4.4. *Toda extensión algebraica de un cuerpo perfecto es separable.*

Proposición 4.5. *Si toda extensión finita de un cuerpo F es separable, entonces F es perfecto.*

Ejemplo. Para dar un ejemplo de un polinomio irreducible y no separable, necesitamos un cuerpo no perfecto. Hemos visto que no puede tener característica 0 y no puede ser finito ni una extensión algebraica de un cuerpo finito. Luego F tiene que ser una extensión trascendente de su cuerpo primo. Tomaremos $F = \mathbb{Z}_p(t)$ para cierto primo p y una variable t. Por otro lado, sabemos que un polinomio irreducible de grado n, con p no dividiendo a n, es separable. Recordando además que la derivada de un polinomio irreducible no separable es el polinomio nulo, elegiremos el polinomio:

$$f(x) = x^p - t \in F[x]$$

Veamos que $f(x)$ es irreducible y no separable.
Procedemos por reducción al absurdo. Sea α una raíz de $f(x)$:

$$f(x) = (x - a)^p$$

Si $\alpha \in F$, entonces:

$$\alpha = \frac{g(t)}{h(t)}$$

con $g(t), h(t) \in \mathbb{Z}_p[t], h(t) \neq 0$. Esto implica que $h(t)^p t = g(t)^p$. Sin embargo, esto es imposible.
Por tanto, $x^p - t$ es irreducible en $F[x]$.

4.3. Inmersiones y separabilidad

Teorema 4.6. *Sea K/F una extensión finita con $[K : F] = n$ y $\sigma : F \to L$ una inmersión.*

1. *El número de inmersiones $\bar{\sigma} : K \to L$ que extienden a σ es a lo sumo n.*
2. *Si K/F no es separable, entonces el número de inmersiones $\bar{\sigma} : K \to L$ que extienden a σ es menor que n.*
3. *Si $K = F(\alpha_1, \ldots, \alpha_r)$, con $\alpha_1, \ldots, \alpha_r$ separables sobre F, entonces existe una extensión L' de L tal que el número de inmersiones $\bar{\sigma} : K \to L$ que extienden a σ es n.*
4. *Si K/F es separable, entonces existe una extensión L' de L tal que el número de inmersiones $\bar{\sigma} : K \to L$ que extienden a σ es n.*

Corolario 4.7. *Si $K = F(\alpha_1, \ldots, \alpha_r)$, con $\alpha_1, \ldots, \alpha_r$ separables sobre F, entonces K/F es separable.*

Corolario 4.8. *Sea K/F una extensión de cuerpos y*

$$K_s = \{\alpha \in K : \alpha \text{ separable sobre } F\}$$

Entonces K_s es un cuerpo intermedio de K/F. Se llama clausura separable de K/F.

4.4. Grado de separabilidad

Definición 4.4. Sea K/F una extensión finita y

$$K_s = \{\alpha \in K : \alpha \text{ separable sobre } F\}$$

El grado de separabilidad de K sobre F es el grado de $[K_s : F]$. Se denota por $[K : F]_s$.
El grado de inseparabilidad es $[K : K_s]$ y se denota por $[K : F]_i$.

Lema 4.9. *Sea K/F una extensión de cuerpos con $char(F) = p \neq 0$. Si $\alpha \in K$ es algebraico sobre F, entonces existe un entero $m > 0$ tal que α^{p^m} es separable sobre F.*

Proposición 4.10. *Sea K/F una extensión finita, L clausura algebraica de F y $\sigma : F \to L$ una inmersión. Entonces el número de inmersiones de K a L que extienden a σ es precisamente $[K : F]_s$. En particular, $[K : F]_s$ es el número de F-inmersiones de K a N, donde N es clausura normal de K/F.*

Capítulo 5

Teorema del elemento primitivo

Definición 5.1. Sea K/F una extensión de cuerpos. Si existe un elemento $\alpha \in K$ tal que $K = F(\alpha)$, decimos que K/F es simple y que α es un elemento primitivo de la extensión.

Ejemplo. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ es una extensión simple de $\mathbb{Q}$ y $\sqrt{2}+\sqrt{3}$ es un elemento primitivo.

Lema 5.1. *Sea G un grupo abeliano finito G y $a \in G$ un elemento de orden máximo m. Entonces el orden de todo elemento de G es un divisor de m.*

Lema 5.2. *Si F es un cuerpo finito, entonces el grupo multiplicativo $F^\times = \{a \in F : a \neq 0\}$ es un grupo cíclico.*

Teorema 5.3 (Teorema del elemento primitivo)**.** *Toda extensión separable finita es simple.*

Ejemplo. Por el teorema, si una extensión finita no es simple, entonces ha de ser no separable.
Sea $F = \mathbb{Z}_p(t, s)$, donde t, s son variables, α una raíz de $x^p - t$ y β una raíz de $x^p - s$. Veamos que la extensión $F(\alpha, \beta)/F$ no es simple. Para ello, observamos que $[F(\alpha) : F] = p$, pues $x^p - t$ es irreducible en $F[x]$. Con un argumento similar podemos obtener que $x^p - s$ es irreducible en $F(\alpha)[x]$, así que $[F(\alpha, \beta) : F(\alpha)] = p$. Podemos concluir que:

$$[F(\alpha, \beta) : F] = p^2$$

Si la extensión $F(\alpha, \beta)/F$ es simple, debe existir un elemento primitivo $\gamma \in F(\alpha, \beta)$ de grado p^2 sobre F. Pero podemos comprobar que todo elemento de $F(\alpha, \beta)/F$ tiene grado p.
Sea $\gamma \in F(\alpha, \beta)$. Entonces:

$$\gamma = \frac{g(\alpha, \beta)}{h(\alpha, \beta)}, \quad g, h \in F[x, y], h \neq 0$$
$$\gamma^p = \frac{\bar{g}(\alpha^p, \beta)^p}{\bar{h}(\alpha^p, \beta^p)}$$

donde los coeficientes de $\bar{(}g), \bar{h}$ son la potencia p-ésima de los coeficientes de g y h, respectivamente. Luego:

$$\gamma^p = \frac{\bar{g}(t, s)}{\bar{h}(t, s)} \in F$$

Por tanto γ es una raíz de un polinomio de la forma $x^p - a \in F[x]$, luego el grado de γ sobre F no es p^2.
Concluimos que $F(\alpha, \beta)/F$ es finita pero no es simple.

Observación. El recíproco del teorema del elemento primitivo no es cierto.

Teorema 5.4 (Steiniz)**.** *Una extensión finita K/F es simple si y solo si tiene un número finito de cuerpos intermedios.*

Proposición 5.5. *Sean K/F y L/K extensiones finitas. Entonces K/F y L/K son separables si y solo si L/F es separable.*

Capítulo 6

El teorema fundamental de la teoría de Galois

6.1. Grupo de Galois

Ejemplo.

$$Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{Id\}$$
$$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{Id, \sigma\}, \text{ donde } \sigma(\sqrt{2}) = -\sqrt{2}$$
$$Gal(\mathbb{R}/\mathbb{Q}) = \{Id\}$$
$$Gal(\mathbb{Q}(x)/\mathbb{Q}) = \{x \mapsto \frac{ax+b}{cx+d} : a, b, c, d \in \mathbb{Q}, ad - bc \neq 0\}$$

Observamos que $\mathbb{R}/\mathbb{Q}$ y $\mathbb{Q}(x)/\mathbb{Q}$ son extensiones infinitas cuyo grupos de Galois son respectivamente finito e infinito.

Lema 6.1. *Sea K/F algebraica. Entonces todo F-homomorfismo $\sigma : K \to K$ es F-automorfismo.*

Teorema 6.2. *Si K/F es una extensión finita, entonces $Gal(K/F)$ es un grupo finito.*

6.2. Subgrupos y cuerpos intermedios

Teorema 6.3. *Sea K/F una extensión de cuerpos, E un cuerpo intermedio y H un subgrupo de $G = Gal(K/F)$. Entonces:*

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

es un cuerpo intermedio de K/F y

$$Gal(K/E) = \{\sigma \in G : \sigma(\alpha) = \alpha, \text{ para todo } \alpha \in E\}$$

es un subgrupo de G.

Ejemplo. Sea G el grupo de Galois de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$. Podemos comprobar que G es un grupo de orden 4. Como sus elementos están completamente determinados por su acción en $\sqrt{2}$ y $\sqrt{3}$, podemos describirlos así:

$$\sigma_1 = Id$$
$$\sigma_2(\sqrt{2}) = \sqrt{2} \qquad \sigma_2(\sqrt{3}) = -\sqrt{3}$$
$$\sigma_3(\sqrt{2}) = -\sqrt{2} \qquad \sigma_3(\sqrt{3}) = \sqrt{3}$$
$$\sigma_4(\sqrt{2}) = -\sqrt{2} \qquad \sigma_4(\sqrt{3}) = -\sqrt{3}$$

Observamos que $\sigma_2, \sigma_3, \sigma_4$ son elementos de orden 2 en G. Luego G es isomorfo al grupo $C_2 \times C_2$.
El subgrupo de G asociado al cuerpo intermedio $\mathbb{Q}(\sqrt{3})$ es:

$$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{3}))$$

el grupo de $\mathbb{Q}(\sqrt{3})$-automorfismos de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Este es $< \sigma_3 >$.
Por otro lado, sea H el subgrupo generado por $\sigma_2 : H =< \sigma_2 >$. El correspondiente cuerpo intermedio es:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3})^H = \{\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) : \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in H\} = \{\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) : \sigma_2(\alpha) = \alpha\}$$

Obervamos que $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})^H$. Se puede demostrar que se da la igualdad considerando la acción de σ_2 en cada elemento de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, recordando que son de la forma $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$, con $a, b, c, d \in \mathbb{Q}$.

Definición 6.1. Sea K/F una extensión de cuerpos y H un subgrupo de $Gal(K/F)$. El cuerpo intermedio K^H se llama subcuerpo de K fijo por H.

6.3. Extensiones de Galois

Definición 6.2. Una extensión de Galois es una extensión de cuerpos K/F tal que $K^G = F$, donde $G = Gal(K/F)$.

Ejemplo. El grupo de Galois de $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$ es trivial. Luego todos los elementos de $\mathbb{Q}(\sqrt[3]{2})$ son fijos por todos los elementos del grupo de Galois, es decir:

$$\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}(\sqrt[3]{2})$$

y por tanto $\mathbb{Q}(\sqrt[3]{2})$ no es una extensión de Galois de $\mathbb{Q}$.

Ejemplo. Veamos si $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ es una extensión de Galois.
Su grupo de Galois G tiene dos elementos: la identidad y el elemento σ determinado por:

$$\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$$

Observamos que $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})$ es fijo por Id y σ, así que $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})^G$ y por tanto la extensión no es de Galois.

Teorema 6.4. *Sea K/F una extensión algebraica. Entonces son equivalentes:*

1. *K/F es una extensión de Galois.*
2. *K/F es normal y separable.*

6.4. El teorema fundamental

Proposición 6.5. *Sea K/F algebraico. Si K/F es de Galois y E es un cuerpo intermedio, entonces K/E es de Galois.*

Ejemplo. La extensión $\mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})/\mathbb{Q}$ es de Galois pero $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es de Galois.

Teorema 6.6. *Sea K/F una extensión finita. Entonces:*

1. *$|Gal(K/F)|$ divide a $[K : F]$.*
2. *K/F es de Galois si y solo si $|Gal(K/F)| = [K : F]$.*

Teorema 6.7. *Sea K/F una extensión finita y E un cuerpo intermedio. Si K/F es de Galois, son equivalentes:*

1. *$E = \sigma E$ para todo $\sigma \in Gal(K/F)$.*

2. *$Gal(K/E)$ es un subgrupo normal de $Gal(K/F)$.*

3. *E/F es de Galois.*

4. *E/F es una extensión normal.*

Teorema 6.8. *Sean $F \subset E \subset K$ extensiones finitas con E/F y K/F de Galois. Entonces $Gal(K/E)$ es un subgrupo normal de $Gal(K/F)$ y existe un isomorfismo de grupos:*

$$Gal(K/F)/Gal(K/E) \equiv Gal(E/F)$$

Teorema 6.9 (Teorema fundamental)**.** *Sea K/F una extensión finita de Galois. Existe una correspondencia uno a uno entre el conjunto de cuerpos intermedios de K/F y el conjunto de subgrupos del grupo de Galois $G = Gal(K/F)$. Esta correspondencia viene dada por $E \mapsto Gal(K/E)$ y satisface las siguientes condiciones:*

1. *Si $F \subseteq E \subseteq K$, entonces K/E es una extensión de Galois y su grupo de Galois $Gal(K/E)$ es un subgrupo de $G = Gal(K/F)$. Además,*

$$[K : E] = |Gal(K/E)| \text{ y } |Gal(K/F) : Gal(K/E)| = [E : F]$$

2. *E/F es de Galois si y solo si $Gal(K/E)$ es un subgrupo normal de $G = Gal(K/F)$. En este caso, $Gal(E/F)$ es isomorfo a $G/Gal(K/E)$.*

Capítulo 7

Cuerpos finitos

Proposición 7.1. *Sea F un cuerpo finito. Entonces:*

1. *La característica de F es un primo p.*
2. *F es una extensión finita de su cuerpo primo $\pi(F)$ (isomorfo a $\mathbb{Z}_p$) y*

$$|F| = p^n, \text{ donde } n = [F : \pi(F)]$$

Proposición 7.2. *Sea F un cuerpo finito con $q = p^n$ elementos. Entonces:*

1. *$\alpha^q = \alpha$ para todo $\alpha \in F$.*
2. *$x^q - x = \prod_{\alpha \in F}(x - \alpha)$.*
3. *F es un cuerpo de descomposición sobre $\pi(F)$ de $x^q - x$.*

Ejemplo.

$$x^3 - x = x(x-1)(x-2) \in \mathbb{Z}_3[x]$$

La factorización de $x^9 - x$ en factores irreducibles en $\mathbb{Z}_3[x]$ es:

$$x^9 - x = x(x-1)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2) \in \mathbb{Z}_3[x]$$

La proposición previa afirma que si F es un cuerpo finito con 9 elementos, entonces sus elementos serán las raíces de $x^9 - x$. Para expresar cada una de las raíces de $x^9 - x$ contruimos un cuerpo finito de 9 elementos como un cuerpo stem de un polinomio irreducible de grado 2 sobre $\mathbb{Z}_3[x]$. Por ejemplo, consideramos el polinomio irreducible $x^2 + 1 \in \mathbb{Z}_3[x]$. Entonces:

$$\mathbb{F} = \mathbb{Z}_3[x]/(x^2+1) \text{ es una extensión de } \mathbb{Z}_{\not 3} \text{ de grado 2.}$$

Recordamos que este cociente es isomorfo a $\mathbb{Z}_3(\alpha)$ para cada raíz α de x^2+1. Como $\{1, \alpha\}$ es una base de $\mathbb{Z}_3(\alpha)$ sobre $\mathbb{Z}$, tenemos que los 9 elementos de $F = \mathbb{Z}_3(\alpha)$ son:

$$0,\ 1,\ 2,\ \alpha,\ 1+\alpha,\ 2+\alpha,\ 2\alpha,\ 1+2\alpha,\ 2+2\alpha$$

Corolario 7.3. *Sea p primo y n un entero positivo. Entonces:*

1. *Existe un cuerpo finito con p^n elementos.*
2. *Dos cuerpos finitos con p^n elementos son isomorfos.*

Corolario 7.4. *El polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ es el producto de todos los polinomios irreducibles mónicos de $\mathbb{Z}_p[x]$ de grado d, con d divisor de n.*

Ejemplo. Descomponemos el polinomio $x^{5^2} - x$ sobre $\mathbb{Z}_5$:

$$x(x+1)(x+2)(x+3)(x+4)(x^2+2)(x^2+3)$$
$$(x^2+x+1)(x^2+x+2)(x^2+2x+3)(x^2+2x+4)$$
$$(x^2+3x+3)(x^2+3x+4)(x^2+4x+1)(x^2+4x+2)$$

7.1. Extensiones finitas de cuerpos finitos

Proposición 7.5. *Sea F un cuerpo finito con $q = p^m$ elementos y n un entero positivo. Entonces existe una extensión finita K de grado n sobre F y es única salvo F-isomorfismos.*

Corolario 7.6. *Si F es un cuerpo finito y n es un entero positivo, existe un polinomio irreducible $f \in F[x]$ de grado n.*

Teorema 7.7. *Sea F un cuerpo finito con p^m elementos y K/F una extensión finita de grado $[K : F] = n$. Entonces K/F es de Galois y su grupo de Galois es:*

$$G \equiv \mathbb{Z}/n\mathbb{Z}$$

Además, G es generado por:

$$\begin{aligned} \sigma : K &\to K \\ \alpha &\mapsto \alpha^q \end{aligned}$$

Capítulo 8

Extensiones ciclotómicas

Definición 8.1. Una extensión de cuerpos de la forma $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, con $\zeta_n = e^{2\pi i/n}$ se llama la n-ésima extensión ciclotómica.

Proposición 8.1. *$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es cuerpo de descomposición de x^n-1 sobre $\mathbb{Q}$. De hecho, es una extensión de Galois finita.*

Definición 8.2. Si θ es una raíz de $x^n - 1$ tal que $\theta^k \neq 1$ para todo $1 \leq k < n$, decimos que θ es una raíz primitiva n-ésima de la unidad.

Observación. $\zeta_n = e^{2\pi i/n}$ es una raíz primitiva n-ésima de la unidad.

Proposición 8.2. *El conjunto de raíces primitivas n-ésimas de la unidad es:*

$$\{\zeta_n^k : MCD(k, n) = 1\}$$

Teorema 8.3. *Las raíces conjugadas de ζ_n sobre $\mathbb{Q}$ son:*

$$\{\zeta_n^k : MCD(k, n) = 1\}$$

las raíces primitivas n-ésimas de la unidad.
En consecuencia, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, donde ϕ es la función de Euler.

Ejemplo. Por el teorema previo, el polinomio mímimo de ζ_{15} sobre $\mathbb{Q}$ tiene grado $\phi(15) = 8$.

$$\begin{aligned} x^{15} - 1 = ((x^5)^3 - 1) = (x^5 - 1)((x^5)^2 + (x^5) + 1) = \\ = (x - 1)(x^4 + x^3 + x^2 + x + 1)(x^{10} + x^5 + 1) \end{aligned}$$

Sabemos que $x^4 + x^3 + x^2 + x + 1$ es irreducible. Como el polinimio mímimo de ζ_{15} sobre $\mathbb{Q}$ divide a $x^{15}-1$ y tiene grado 8, debe ser un factor irreducible de $x^{10}+x^5+1$. También sabemos que x^3-1 divide a $x^15 - 1$, porque sus raíces son las raíces 3-ésimas de la unidad, luego también son raíces 15-ésimas de la unidad, aunque no sean primitivas. Entonces $x^{10} + x^5 + 1$ es múltiplo de $x^2 + x + 1$. Dividiendo por $x^2 + x + 1$, obtenemos:

$$x^{10} + x^5 + 1 = (x^2 + x + 1)(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)$$

Podemos concluir que $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ es el polinimio mínimo de ζ_{15} sobre $\mathbb{Q}$.

Definición 8.3. El polinimio mínimo de ζ_n sobre $\mathbb{Q}$ se llama n-ésimo polinomio ciclotómico.

Ejemplo. $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ es el 15-ésimo polinomio ciclotómico.
Sus raíces son $\zeta_{15}, \zeta_{15}^2, \zeta_{15}^4, \zeta_{15}^7, \zeta_{15}^8, \zeta_{15}^{11}, \zeta_{15}^{13}, \zeta_{15}^{14}$.

Observación. Si $n = p$ es primo, el p-ésimo polinomio ciclotómico es:

$$x^{p-1} + x^{p-2} + \cdots + x + 1$$

Proposición 8.4. *Sea $\Phi_n(x)$ el n-ésimo polinomio ciclotómico. Entonces:*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Teorema 8.5. *El grupo de Galois de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ es isomorfo al grupo multiplicativo de los enteros módulo n:*

$$\mathbb{Z}_n^* = \{k : 1 \leq k < n, MCD(k, n) = 1\}$$

Para cada $k \in \mathbb{Z}_n^*$, el correspondiente automorfismo en el grupo de Galois envía ζ_n a ζ_n^k.

8.1. Ciclos gaussianos

Teorema 8.6 (Gauss)**.** *Sea p un primo, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ la p-ésima extensión ciclotómica, H un subgrupo de $\mathbb{Z}_p^\times$. Entonces:*

$$\gamma_H = \sum_{a \in H} \zeta_p^a$$

es un elemento primitivo de $\mathbb{Q}(\zeta_p)^H/\mathbb{Q}$.

Ejemplo. Consideramos el subgrupo de $\mathbb{Z}_{19}^*$ generado por 8:

$$H = < 8 > = \{1, 7, 8, 11, 12, 18\}$$

Este es un ciclo. La suma:

$$\gamma_H = \zeta_{19} + \zeta_{19}^7 + \zeta_{19}^8 + \zeta_{19}^{11} + \zeta_{19}^{12} + \zeta_{19}^{18}$$

es un elemento primitivo de $\mathbb{Q}(\zeta_{19})^H$.
Los otros dos conjuntos complementarios de H en $\mathbb{Z}_{19}^*$ son también ciclos:

$$\{2, 3, 5, 14, 16, 17\},$$
$$\{4, 6, 9, 10, 13, 15\}$$

Y las correspondientes sumas:

$$\zeta_{19}^2 + \zeta_{19}^3 + \zeta_{19}^5 + \zeta_{19}^{14} + \zeta_{19}^{16} + \zeta_{19}^{17},$$
$$\zeta_{19}^4 + \zeta_{19}^6 + \zeta_{19}^9 + \zeta_{19}^{10} + \zeta_{19}^{13} + \zeta_{19}^{15}$$

son las raíces conjugadas de γ_H sobre $\mathbb{Q}$, que también generan el cuerpo intermedio $\mathbb{Q}(\zeta_{19})^H$.

Capítulo 9

Construcciones geométricas

9.1. Números construibles

Definición 9.1. Un número complejo α es construible si existe una secuencia finita de construcciones con regla y compás que empieza con 0 y 1 y acaba con α.

Proposición 9.1. *El conjunto $\mathcal{C} = \{\alpha \in \mathbb{C} : \alpha$ es construible$\}$ es un subcuerpo de $\mathbb{C}$. Además:*

1. *Sea $\alpha = a + bi \in \mathbb{C}$. Entonces $\alpha \in \mathcal{C}$ si y solo si $a, b \in \mathcal{C}$.*
2. *Si $\alpha \in \mathcal{C}$ entonces $\sqrt{\alpha} \in \mathcal{C}$.*

Teorema 9.2. *Sea α un número complejo. Entonces α es construible si y solo si existe una sucesión de cuerpos*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

tal que $\alpha \in F_n$ y $[F_i : F_{i-1}] = 2$ para todo $i = 1, \ldots, n$.

Corolario 9.3. *El cuerpo de números construibles es el subcuerpo más pequeño de $\mathbb{C}$ que es cerrado para la raíz cuadrada.*

Corolario 9.4. *Si $\alpha \in \mathbb{C}$ es un número construible, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ para algún $m \geq 0$.*

Teorema 9.5. *Sea $\alpha \in \mathbb{C}$ algebraico sobre $\mathbb{Q}$ y sea K cuerpo de descomposición del polinimio mínimo de α sobre $\mathbb{Q}$. Entonces α es construible si y solo si $[K : \mathbb{Q}]$ es una potencia de 2.*

9.2. Algunas construcciones imposibles

- Trisección del ángulo
- Duplicación del cubo
- Cuadratura del círculo

9.3. Polígonos regulares

Definición 9.2. Un primo impar p es un primo de Fermat si se puede escribir como $p = 2^{2^m} + 1$ para algún entero $m \geq 0$.

Ejemplo. Los números primos de Fermat conocidos son 3, 5, 17, 257 y 65537.

Lema 9.6. *Sea k un entero positivo. Si $p = 2^k + 1$ es un primo impar, entonces p es un primo de Fermat.*

Teorema 9.7. *Sea $n > 2$ un entero. Entonces un n-ágono regular puede ser construido por regla y compás si y solo si*

$$n = 2^s p_1 \dots p_r$$

donde $s \geq 0$ es un entero y $p_1, \dots, p_r$ son distintos primos de Fermat.

Capítulo 10

Solubilidad por radicales

10.1. Extensiones radicales y solubles

Definición 10.1. Una extensión $F \subset K$ es radical si existen cuerpos intermedios

$$F = F_0 \subset F_1 \subset \cdots \subset F_{m-1} \subset F_m = K$$

tales que para cada $i = 1, \dots m$ existe $\gamma_i \in F_i$, con $F_i = F_{i-1}(\gamma_i)$ y $\gamma_i^{m_i} \in F_{i-1}$ para algún $m_i > 0$.

Ejemplo. $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2+\sqrt{2}})$ es una extensión radical.

Ejemplo. El polinomio $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ es irreducible. Podemos comprobar que $f(x)$ tiene tres soluciones reales. Además, el discriminante de f es 49, que es un cuadrado. Se puede comprobar que el grupo de Galois de un polinimio irreducible de orden n cuyo discriminante es un cuadrado es un subgrupo del grupo alternado A_n. En este caso, podemos concluir que $Gal_{\mathbb{Q}}(f)$ es cíclico de grado 3. Por tanto, el cuerpo de descomposición es de la forma $\mathbb{Q}(\alpha)$, donde α es una raíz de f.
Si $\mathbb{Q}(\alpha)$ es radical sobre $\mathbb{Q}$, debe existir un elemento primitivo $\gamma \in \mathbb{Q}(\alpha)$ tal que $\gamma^m \in \mathbb{Q}$ para algún $m \geq 3$. Pero entonces, sus raíces conjugadas pertenecen al conjunto $\{\gamma, \gamma\zeta_m, \dots, \gamma\zeta_m^{m-1}\}$. Como ζ_m no pertenece a $\mathbb{Q}(\alpha) \subset \mathbb{R}$, esto no es posible.

Definición 10.2. Una extensión de cuerpos $F \subset K$ es solucble si existe una extensión L de K tal que L/F es radical.

Definición 10.3. Sea F un cuerpo. Si $f \in F[x]$, la ecuación $f(x) = 0$ se dice que es soluble por radicales cuando el cuerpo de descomposición de f sobre F es una extensión soluble de F.

Proposición 10.1. *Sea K/F una extensión de cuerpos y E, E' cuerpos intermedios. Denotamos por EE' al subcuerpo más pequeño de K que contiene a E y a E'. Entonces:*

1. *Si K/E y E/F son radicales, entonces K/F es radical.*
2. *Si E'/F es radical, entonces EE'/E es radical.*
3. *Si E/F y E'/F son radicales, entonces EE'/F es radical.*

Proposición 10.2. *Si K/F es una extensión radical y $\bar{K}/F$ es clausuranormal de K/F, entonces $\bar{K}/F$ es radical.*

10.2. Teorema de Galois

Lema 10.3. *Sea K/F una extensión de Galois finita de grado m y ζ una raíz primitiva m-ésima de la unidad. Entonces $K(\zeta)/F(\zeta)$ es una extensión de Galois cuyo grado divide a m.*

Lema 10.4. *Sea K/F una extensión de Galois finita con grupo de Galois cíclico de orden primo p. Si F contiene una raíz primitiva p-ésima de la unidad ζ_p, entonces existe $\alpha \in K$ tal que $K = F(\alpha)$ y $\alpha^p \in F$.*

Teorema 10.5 (Galois)**.** *Sea K/F una extensión de Galois finita con F de característica 0. Entonces son equivalentes:*

1. *K/F es soluble.*
2. *$Gal(K/F)$ es un grupo soluble.*

Corolario 10.6 (Galois)**.** *Sea F un cuerpo de característica 0 y $f \in F[x]$. Entonces $f(x) = 0$ es soluble por radicales si y solo si $Gal_F(f)$ es un grupo soluble.*

Corolario 10.7 (Teorema de Abel-Ruffini)**.** *Sea F un cuerpo de característica 0. La ecuacuón general de grado $n \geq 5$ no es soluble por radicales sobre F.*