

CHULETARIO ÁLGEBRA II

Álvaro Grande Blázquez

2025 ~ 2026

Índice

1. Repaso de teoría de cuerpos	1
1.1. Estructuras algebraicas	1
1.2. Ideales y cocientes	4
1.3. Factorización en anillos de polinomios	6
2. Extensiones de cuerpos	10
2.1. Extensiones de cuerpos y característica	10
2.2. Grado de una extensión	12
2.3. Extensiones algebraicas	13
2.4. Tres problemas clásicos	16
3. Extensiones de Galois	18
3.1. Cuerpo de descomposición y clausura algebraica	18
3.2. Extensiones normales	20
3.3. Extensiones separables	20
4. El Teorema Fundamental de la Teoría de Galois	24
4.1. Automorfismos de cuerpos	24
4.2. El Teorema Fundamental de la Teoría de Galois	29

TEMA 1. REPASO DE TEORÍA DE CUERPOS

1.1. ESTRUCTURAS ALGEBRAICAS

Definición 1.1 (Operación binaria)

Sea C un conjunto. Una **operación binaria** en C es una aplicación:

$$\begin{aligned} * : C \times C &\rightarrow C \\ (a, b) &\mapsto a * b \end{aligned}$$

Además, se impone que al operar dos elementos de C , el resultado debe estar en C .

Definición 1.2 (Grupo)

Un **grupo** $(G, *)$ es un conjunto con una operación binaria $*$ tal que:

- $*$ es asociativa: $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
- Existe elemento neutro: $\exists e \in G \mid \forall a \in G, e * a = a * e = a$
- Existe elemento inverso: $\forall a \in G \exists a^{-1} \in G \mid a * a^{-1} = a^{-1} * a = e$

El grupo es **conmutativo (abeliano)** si $\forall a, b \in G, a * b = b * a$.

Definición 1.3 (Anillo)

Un **anillo** $(A, *, \circ)$ es un conjunto A con dos operaciones binarias $*, \circ$ tales que:

- $(A, *)$ es un grupo abeliano.
- \circ es asociativa.
- Se cumplen las leyes de distributividad:
 - $(a * b) \circ c = (a \circ c) * (b \circ c)$
 - $a \circ (b * c) = (a \circ b) * (a \circ c)$

El anillo es **conmutativo** si \circ es conmutativa.

El anillo **tiene unidad** si existe un neutro para \circ .

 **Nota**

En este curso, «anillo» significará anillo conmutativo con unidad (salvo pocas excepciones)

Definición 1.4 (Cuerpo)

Un **cuerpo** $(K, *, \circ)$ es un conjunto K con al menos dos elementos y dos operaciones binarias $*, \circ$ tales que:

- $(K, *, \circ)$ es un anillo conmutativo con unidad.
- Todo elemento $a \in K$, $a \neq e$, tiene un inverso para \circ .

Definición 1.5

Sea $(A, +, \cdot)$ un anillo. Entonces:

- Un elemento $a \in A$ es un **divisor de cero** si $a \neq 0$ y existe $b \in A \setminus \{0\}$ tal que $a \cdot b = 0$.
- Un elemento $a \in A$ es una **unidad** si existe $b \in A$ tal que $a \cdot b = 1$. Decimos que $b = a^{-1}$ es su inverso.
- El anillo A es un **dominio de integridad** si $\forall a, b \in A$, $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$, es decir, no hay divisores de 0.

Lema 1.6

Todo cuerpo es un dominio de integridad.

Definición 1.7 (Anillo de polinomios)

Sea A un anillo conmutativo. El **anillo de polinomios** $A[X]$ en una variable x es el conjunto de expresiones de la forma:

$$a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0, \quad a_i \in A$$

con la suma y el producto habituales.

Definición 1.8 (Grado de un polinomio)

Si $P = a_n x^n + \dots + a_0 \in A[X]$ con $a_n \neq 0$ decimos que P tiene **grado n** y ponemos $\deg(P) = n$. Si $P = 0$, entonces $\deg(P) = -\infty$.

Proposición 1.9

Sea A un dominio de integridad. Entonces:

- $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$
- $\deg(PQ) = \deg(P) + \deg(Q)$
- $A[X]$ es un dominio de integridad.

Definición 1.10 (Polinomio mónico)

Un polinomio $a_n x^n + \dots + a_0$ de grado $n \geq 1$ es **mónico** si $a_n = 1$.

Definición 1.11 (Morfismo de anillos)

Sean A, B anillos. Un **(homo)morfismo de anillos** es una aplicación $\phi : A \rightarrow B$ tal que:

- $\phi(a_1 + a_2) = \phi(a_1) + \phi(a_2)$
- $\phi(a_1 a_2) = \phi(a_1) \phi(a_2)$
- $\phi(1_A) = 1_B$

Definición 1.12

- Un morfismo biyectivo de anillos $\phi : A \rightarrow B$ es un **isomorfismo**.
- Un morfismo de anillos $\phi : A \rightarrow A$ es un **endomorfismo**.
- Un de anillos $\phi : A \rightarrow A$ que es un isomorfismo se llama **automorfismo**.

Definición 1.13

Sea $\phi : A \rightarrow B$ un morfismo de anillos:

- Su **núcleo** es $\ker(\phi) = \{a \in A \mid \phi(a) = 0\}$.
- Su **imagen** es $\text{Im}(\phi) = \{b \in B \mid \phi^{-1}(b) \neq \emptyset\}$

Lema 1.14

Sea $\phi : A \rightarrow B$ un morfismo de anillos:

- $\ker(\phi)$ es un subanillo de A .
- $\text{Im}(\phi)$ es un subanillo de B .

Definición 1.15 (Morfismo de evaluación)

Sean $A \subset B$ anillos. Dado $b \in B$, la aplicación:

$$\phi_b : A[X] \rightarrow B \text{ tal que } (a_n x^n + \dots + a_1 x + a_0) \mapsto (a_n b^n + \dots + a_1 b + a_0)$$

es un morfismo de anillos, llamado el **morfismo de evaluación** en b .

1.2. IDEALES Y COCIENTES

Definición 1.16 (Ideal)

Sea $(A, +, \cdot)$ un anillo. Se dice que $I \subset A$ es un **ideal** si:

- $0 \in I$
- $\forall a, b \in I, a + b \in I$
- $\forall a \in A, \forall b \in I; a \cdot b \in I$

Es decir, $(I, +)$ es un subgrupo e I es absorbente para el producto.

Definición 1.17

Sean A un anillo; $a_1, \dots, a_n \in A$. El ideal generado por a_1, \dots, a_n es el menor ideal que contiene a a_1, \dots, a_n . Es decir:

$$\langle a_1, \dots, a_n \rangle = \{ \lambda_1 a_1 + \dots + \lambda_n a_n \mid \lambda_j \in A \}$$

Los elementos a_1, \dots, a_n se llaman **generadores** del ideal.

Definición 1.18

Sea A un anillo. Un ideal $I \subset A$ es:

- **Principal** si existe $a \in A$ tal que $I = \langle a \rangle$.
- **Maximal** si $I \neq A$ y no existe ningún ideal $J \subsetneq A$ tal que $I \subsetneq J \subsetneq A$.
- **Primo** si $I \neq A$ y, para todos $x, y \in I$, si $xy \in I$ entonces o bien $x \in I$ o $y \in I$.

Proposición 1.19

Sean $a, b \in \mathbb{Z}$. Supongamos que $a \neq 0$ o $b \neq 0$. Entonces:

$$\langle a, b \rangle = \langle \text{mcd}(a, b) \rangle$$

Lema 1.20

En \mathbb{Z} :

- Los **ideales maximales** son $\{\langle p \rangle \mid p \in \mathbb{Z} \text{ primo}\}$.
- Los **ideales primos** son $\{\langle 0 \rangle\} \cup \{\langle p \rangle \mid p \in \mathbb{Z} \text{ primo}\}$.

Definición 1.21 (Anillo cociente)

Sean A un anillo, I un ideal de A . Este induce una relación de equivalencia sobre A dada por:

$$a \sim b \Leftrightarrow a - b \in I, \text{ donde } \sim \text{ es reflexiva, simétrica y transitiva.}$$

Esto permite definir el **conjunto cociente** A/I (el conjunto de clases de equivalencia).

Proposición 1.22

Sean A un anillo, $I \subset A$ un ideal. El conjunto cociente A/I tiene estructura de anillo con las propiedades inducidas por las de A :

$$\forall a, b \in A, \quad \overline{a} + \overline{b} = \overline{a + b} \quad y \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

Proposición 1.23

Sean A un anillo, $I \subset A$ un ideal. Entonces:

- El ideal I es **maximal** si y solo si A/I es un **cuerpo**.
- El ideal I es **primo** si y solo si A/I es un **dominio de integridad**.

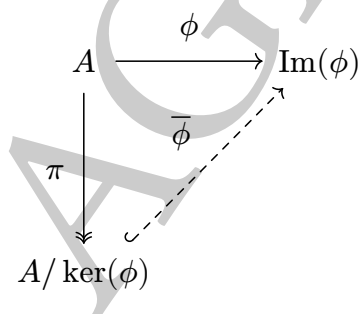
Corolario 1.24

Todo ideal maximal es primo.

Teorema 1.25 (Primer Teorema de Isomorfía)

Sean A, B dos anillos y $\phi : A \rightarrow B$ un morfismo de anillos. Entonces:

- $\ker(\phi)$ es un ideal de A .
- Existe un isomorfismo $\bar{\phi} : A/\ker(\phi) \rightarrow \text{Im}(\phi)$ tal que el siguiente diagrama conmuta:



Decimos que ϕ factoriza a través de π .

1.3. FACTORIZACIÓN EN ANILLOS DE POLINOMIOS

Teorema 1.26 (Teorema Fundamental de la Aritmética)

Todo entero mayor que 1 puede expresarse de forma única como un producto de números primos, salvo reordenación de los factores.

Definición 1.27

Sea A un dominio de integridad. Un elemento $a \in A \setminus \{0\}$ es **irreducible** si no es una unidad y, para todos $b, c \in A$, $a = bc$ implica que b o c son unidades.

Definición 1.28 (Dominio de factorización única (DFU))

Sea A un dominio de integridad. Se dice que A es un **dominio de factorización única (DFU)** si todo elemento $a \in A \setminus \{0\}$ que no sea unidad se puede expresar como un producto finito de factores irreducibles de forma única salvo producto por unidades.

Proposición 1.29

Si A es un DFU, $A[X]$ es un DFU.

Definición 1.30 (Dominio euclídeo)

Sea A un dominio de integridad. A es un **dominio euclídeo** si existe una aplicación $N : A \setminus \{0\} \rightarrow \mathbb{N}$ tal que, dados $a, b \in A$, $b \neq 0$; existen $q, r \in A$ tales que:

- $a = bq + r$
- $r = 0$ o $N(r) < N(b)$

Definición 1.31 (Dominio de ideales principales)

Un **dominio de ideales principales (DIP)** es un dominio de integridad cuyos ideales son todos principales.

Teorema 1.32

Todo dominio euclídeo es un DIP.

Teorema 1.33

Todo DIP es un DFU.

 **Importante**

Dominio euclídeo \Rightarrow DIP \Rightarrow DFU

Los recíprocos, en general, no son ciertos.

Proposición 1.34

Sea A un DIP. Un ideal $I \subset A$ es maximal si y solo si $I = \langle p \rangle$ con p irreducible.

Teorema 1.35 (Teorema Fundamental del Álgebra)

Sea $P \in \mathbb{C}[X]$ no constante. Entonces P es irreducible en $\mathbb{C}[X]$ si y solo si $\deg(P) = 1$.

Teorema 1.36

Si $P \in \mathbb{R}[X]$ es irreducible en $\mathbb{R}[X]$ entonces $\deg(P) \leq 2$.

Lema 1.37 (Lema de Gauss)

Un polinomio no constante $P = a_n x^n + \dots + a_0 \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Z}[X]$ si y solo si P es irreducible en $\mathbb{Q}[X]$ y $\text{mcd}(a_n, \dots, a_0) = 1$.

Proposición 1.38 (Criterio de reducción módulo un primo)

Sea $Q(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[X]$ y $p \in \mathbb{Z}$ primo. Sea $\overline{Q(x)} = \overline{a_n} x^n + \dots + \overline{a_0} \in \mathbb{Z}/p\mathbb{Z}[X]$. Supongamos que $\deg(Q) = \deg(\overline{Q})$. Si $\overline{Q(x)}$ es irreducible en $\mathbb{Z}/p\mathbb{Z}[X]$, entonces $Q(x)$ es irreducible en $\mathbb{Q}[X]$.

Proposición 1.39 (Criterio de Eisenstein)

Sea $Q(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[X]$. Supongamos que existe $p \in \mathbb{Z}$ primo tal que:

- $p \mid a_i$ para $0 \leq i < n$.
- $p \nmid a_n$.
- $p^2 \nmid a_0$.

Entonces $Q(x)$ es irreducible en $\mathbb{Q}[X]$.

 **Consejo: Hacer actuar automorfismo**

Sea A un dominio de integridad. Sea $\phi : A \rightarrow A$ un automorfismo de anillos. Un elemento $a \in A$ es irreducible si y solo si $\phi(a)$ es irreducible.

Proposición 1.40 (Test de las raíces racionales)

Sea:

$$P(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[X], a_0, a_n \neq 0$$

Si $\frac{r}{s} \in \mathbb{Q}$ con $\text{mcd}(r, s) = 1$ es una raíz de $P(x)$ entonces $r \mid a_0$ y $s \mid a_n$ en \mathbb{Z} .

TEMA 2. EXTENSIONES DE CUERPOS

2.1. EXTENSIONES DE CUERPOS Y CARACTERÍSTICA

Definición 2.1 (Morfismo de cuerpos)

Sean K, L dos cuerpos. Un **morfismo de cuerpos** $\phi : K \rightarrow L$ es un morfismo de anillos.

Lema 2.2

Sea K un cuerpo, A un anillo (no nulo). Sea $\phi : K \rightarrow A$ un morfismo de anillos. Entonces ϕ es inyectivo. Es decir, todo morfismo de cuerpos es inyectivo.

Definición 2.3 (Extensión de cuerpos)

Sean K, L cuerpos. Decimos que L es una **extensión** de K si existe un morfismo (inyectivo) de cuerpos $\phi : K \rightarrow L$. Denotamos la extensión mediante L/K .

En otras palabras, L/K es una extensión de cuerpos si K es, salvo isomorfismo, un subcuerpo de L ($K \subset L$ y $+, \cdot$ coinciden en K y L).

Definición 2.4 (Extensión simple)

Una extensión L/K es **simple** si existe $\alpha \in L$ tal que $L = K(\alpha)$. Decimos que α es un **elemento primitivo** de la extensión.

Teorema 2.5

Sean K un cuerpo, $p(x) \in K[X]$ un polinomio irreducible. El cuerpo $L := \frac{K[Y]}{\langle p(y) \rangle}$ es una extensión de K y el polinomio $p(x) \in L[X]$ tiene la raíz $\bar{y} \in L$.

Definición 2.6 (Característica de un cuerpo)

Un cuerpo K (o anillo) tiene **característica** n , $\text{char}(K) = n$, si n es el menor número natural tal que:

$$\underbrace{1_K + \dots + 1_K}_{n \text{ veces}} = 0$$

Si esta suma fuera siempre distinta de 0, decimos que $\text{char}(K) = 0$.

Lema 2.7

Sea K un cuerpo. Entonces $\text{char}(K) = 0$ o $\text{char}(K) = p$ un número primo.

Lema 2.8

Si $\phi : K \rightarrow L$ es un morfismo de cuerpos, entonces $\text{char}(K) = \text{char}(L)$.

Corolario 2.9

Si L/K es una extensión de cuerpos entonces $\text{char}(L) = \text{char}(K)$.

Proposición 2.9

Sea K un cuerpo.

- Si $\text{char}(K) = 0$, existe un único morfismo de cuerpos $\mathbb{Q} \rightarrow K$.
- Si $\text{char}(K) = p$, existe un único morfismo de cuerpos $\mathbb{F}_p \rightarrow K$.

Definición 2.10 (Cuerpo primo)

Un cuerpo es **primo** si no contiene subcuerpos propios. Dado un cuerpo L , su **subcuerpo primo** es el menor (para la inclusión) cuerpo $K \subset L$.

Nota

La Proposición 2.9 implica que los únicos cuerpos primos son isomorfos a \mathbb{Q} o \mathbb{F}_p , p primo. Además, $\text{Aut}(\mathbb{Q}) = \{\text{id}\}$ y $\text{Aut}(\mathbb{F}_p) = \{\text{id}\}$

Corolario 2.11

Sea K un cuerpo.

- Si $\text{char}(K) = 0$ entonces K/\mathbb{Q} es una extensión.
- Si $\text{char}(K) = p$ entonces K/\mathbb{F}_p es una extensión.

2.2. GRADO DE UNA EXTENSIÓN

Proposición 2.12

Sea L/K una extensión de cuerpos. Entonces L es un espacio vectorial sobre K .

Definición 2.13

Sea L/K una extensión de cuerpos.

- El **grado de la extensión**, $[L : K]$, es la dimensión de L como K -espacio vectorial.
- La extensión L/K es **finita** si $[L : K]$ es finito.
- La extensión L/K es **infinita** si $[L : K]$ es infinito.

Teorema 2.14

Sean K un cuerpo, $p(x) \in K[X]$ un polinomio irreducible de grado n . Sea $L = \frac{K[X]}{\langle p(x) \rangle}$. Entonces $\{\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}\}$ es una base de L como K -espacio vectorial, es decir,

$$L = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} \mid a_i \in K\}$$

En particular, $[L : K] = n$.

Corolario 2.15

Sea K un cuerpo finito. Entonces $|K| = p^n$ para $p, n \in \mathbb{N}$, p primo.

Teorema 2.16 (Ley de la torre)

Sean L/K y M/L extensiones de cuerpos. Entonces:

$$[M : K] = [M : L][L : K]$$

De hecho, si L/K y M/L son finitas y $\{x_1, x_2, \dots, x_r\}$, $\{y_1, y_2, \dots, y_s\}$ son sus bases, entonces $\{x_i y_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$ es una base de M/K .

2.3. EXTENSIONES ALGEBRAICAS

Definición 2.17

Sea L/K una extensión de cuerpos.

- $\alpha \in L$ es **algebraico** sobre K si existe un polinomio $p(x) \in K[X]$ tal que $p(\alpha) = 0$.
- $\alpha \in L$ es **trascendente** sobre K si no es algebraico sobre K .

Proposición 2.18

Sea L/K una extensión de cuerpos. Entonces son equivalentes:

- $\alpha \in L$ es trascendente sobre K
- $K[\alpha] \cong K[X]$
- $K(\alpha) \cong K(x)$

Como idea, si α es trascendente, entonces se comporta como una indeterminada.

Definición 2.19

Se dice que una extensión L/K es:

- **algebraica**, si todo $\alpha \in L$ es algebraico sobre K .
- **trascendente**, si no es algebraica (existe $\alpha \in L$ trascendente sobre K)

Definición 2.20 (Polinomio mínimo)

Si α es un elemento algebraico sobre un cuerpo K , se dice que $m_{\alpha,K}(x) \in K[X]$ es el **polinomio mínimo** de α sobre K si $m_{\alpha,K}(x)$ es el polinomio mónico de menor grado en $K[X]$ tal que $m_{\alpha,K}(\alpha) = 0$.

Lema 2.21

Sea L/K una extensión, $\alpha \in L$ algebraico sobre K . Se tiene que:

- $m_{\alpha,K}(x)$ es único
- $m_{\alpha,K}(x)$ es irreducible
- Dado $p(x) \in K[X]$, se tiene que $p(\alpha) = 0 \Leftrightarrow m_{\alpha,K}(x) \mid p(x)$
- Sea K/F una extensión, entonces α es algebraico sobre F y $m_{\alpha,F}(x) \mid m_{\alpha,K}(x)$
- Sea $p(x) \in K[X]$ mónico con $p(\alpha) = 0$. Entonces $p(x) = m_{\alpha,K}(x) \Leftrightarrow p(x)$ es irreducible en $K[X]$.

Teorema 2.22

Sean K un cuerpo, $p(x) \in K[X]$ un polinomio irreducible. Sea α una raíz de $p(x)$ en alguna extensión L de K . Entonces tenemos un isomorfismo:

$$\frac{K[Y]}{\langle p(y) \rangle} \rightarrow K[\alpha], \text{ con } a \in K \rightarrow a; \bar{y} \rightarrow \alpha$$

Corolario 2.23

- Sean K un cuerpo, α un elemento algebraico sobre K . Entonces $K(\alpha) = K[\alpha]$.
- Si $p(x) \in K[X]$ es un polinomio irreducible sobre K y α, β son dos raíces de $p(x)$, entonces:

$$K(\alpha) \cong K(\beta)$$

Corolario 2.24

Sean K un cuerpo, α un elemento algebraico sobre K . Entonces:

- $[K(\alpha) : K] = \deg(m_{\alpha, K}(x))$
- $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(m_{\alpha, K}(x))-1}\}$ es una base de la extensión $K(\alpha)/K$

Proposición 2.25

Toda extensión finita es algebraica.

Corolario 2.26

Sea L/K una extensión de cuerpos. Si $\alpha \in L$ es algebraico sobre K entonces $K(\alpha)/K$ es algebraica.

Proposición 2.27

Una extensión L/K es finita si y solo si L está generado por un número finito de elementos algebraicos sobre K .

Teorema 2.28

Si las extensiones F/K y L/F son algebraicas, entonces L/K es algebraica.

Corolario 2.29

Sea L/K una extensión de cuerpos. Sea $F = \{\alpha \in L \mid \alpha \text{ es algebraico sobre } K\}$. Entonces F es un cuerpo y F/K es una extensión algebraica.

Proposición 2.30

Una extensión de cuerpos L/K es de grado infinito si y solo si se da una de las situaciones siguientes:

- L/K es una extensión trascendente.
- L/K es una extensión algebraica que no está finitamente generada.

2.4. TRES PROBLEMAS CLÁSICOS

I) *Duplicación del cubo* \rightarrow Dado un cubo, construir otro de volumen doble.

II) *Trisección de un ángulo* \rightarrow Dado un ángulo θ , construir $\frac{\theta}{3}$.

III) *Cuadratura del círculo* \rightarrow Dado un círculo, construir un cuadrado de la misma área.

Definición 2.31 (Números constructibles)

Un **número constructible** es una longitud que puede ser construida con regla y compás (a partir de la longitud 1).

Lema 2.32

Sea K el conjunto de los números constructibles. Si a, b son constructibles ($a, b \in K$), podemos construir: $a + b$, $a - b$, ab , a/b , \sqrt{a} . Luego K es un cuerpo.

Teorema 2.33

Un número real x es constructible si y solo si pertenece a un cuerpo $L \subset \mathbb{R}$ tal que existe una cadena de subcuerpos $\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_n = L$ donde todas las extensiones L_{i+1}/L_i son de grado 2.

Corolario 2.34

Si $x \in \mathbb{R}$ es constructible, entonces $[\mathbb{Q}(x) : \mathbb{Q}] = 2^n$ para algún $n \in \mathbb{N}$.

Teorema 2.35

Ninguna de las construcciones (I), (II), (III) es posible.

AGB

TEMA 3. EXTENSIONES DE GALOIS

3.1. CUERPO DE DESCOMPOSICIÓN Y CLAUSURA ALGEBRAICA

Definición 3.1 (Cuerpo de descomposición)

Sean K un cuerpo, $p(x) \in K[X]$ con $\deg(p(x)) = n \geq 1$. Una extensión L/K es un **cuerpo de descomposición** de $p(x)$ (sobre K) si:

- $p(x)$ se descompone en factores lineales en $L[X]$ (decimos que $p(x)$ se descompone completamente en $L[X]$), es decir, se tiene que:

$$p(x) = u(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

- $p(x)$ no se descompone completamente en ningún subcuerpo propio de L que contenga a (la imagen de) K .

Definición 3.2 (K-isomorfismo)

Sean K, A, B cuerpos con $K \subset A$ y $\phi : A \rightarrow B$ un isomorfismo. Decimos que ϕ es un **K -isomorfismo** si deja fijo a K .

Proposición 3.3

Sean K un cuerpo, $p(x) \in K[X]$ un polinomio. Existe un cuerpo de descomposición L de $p(x)$ sobre K que es único salvo K -isomorfismos (la imagen de K en L vía el morfismo de la extensión).

Corolario 3.4

Sean K un cuerpo, $p(x) \in K[X]$ y L el cuerpo de descomposición de $p(x)$. Entonces:

$$[L : K] \leq n!, \quad n = \deg(p(x))$$

 **Nota**

Dado un cuerpo K , el cuerpo de descomposición es una extensión de K que contiene todas las raíces de **un** polinomio sobre K . Ahora queremos una extensión que contenga **todas** las raíces de **todos** los polinomios sobre K .

Definición 3.5 (Clausura algebraica)

Sea K un cuerpo. Una extensión algebraica \overline{K}/K es una **clausura algebraica** de K si todo polinomio $p(x) \in K[X]$ se descompone completamente sobre \overline{K} .

Podemos decir que \overline{K} contiene todos los elementos algebraicos sobre K .

Proposición 3.6

Sea K un cuerpo. Existe una clausura algebraica de K que es única salvo K -isomorfismo.

 **Importante**

Todos los «cálculos» que involucren elementos algebraicos sobre un cuerpo K pueden verse como cálculos en un cuerpo «grande», \overline{K} .

Definición 3.7 (Cuerpo algebraicamente cerrado)

Un cuerpo K es **algebraicamente cerrado** si todo polinomio con coeficientes en K tiene una raíz en K . Esto implica que todas sus raíces están en K , pues descompone completamente:

$$p(x) = (x - \alpha_1)p_1(x) = (x - \alpha_1)(x - \alpha_2)p_2(x) = \dots = (x - \alpha_1)\dots(x - \alpha_n)$$

Equivalentemente, K es **algebraicamente cerrado** si $K = \overline{K}$.

Proposición 3.8

Sean K un cuerpo, \overline{K} su clausura algebraica. Entonces \overline{K} es algebraicamente cerrado.

Teorema 3.9 (Teorema Fundamental del Álgebra)

El cuerpo \mathbb{C} es algebraicamente cerrado. En particular, $\mathbb{C} = \overline{\mathbb{R}}$

Definición 3.10 (Clausura algebraica de \mathbb{Q})

La clausura de \mathbb{Q} se define como:

$$\{a \in \mathbb{C} : a \text{ es algebraico sobre } \mathbb{Q}\}$$

A este cuerpo también se le llama **cuerpo de números algebraicos** de \mathbb{Q} , y es una extensión algebraica infinita de \mathbb{Q} .

3.2. EXTENSIONES NORMALES**Definición 3.11 (Extensión normal)**

Una extensión algebraica es **normal** si todo polinomio irreducible $p(x) \in K[X]$ que tiene una raíz en L se descompone completamente en $L[X]$.

Proposición 3.12

Una extensión L/K es normal y finita si y solo si L es un cuerpo de descomposición de un polinomio de $K[X]$.

3.3. EXTENSIONES SEPARABLES**Definición 3.13 (Raíces simples y múltiples)**

Sean K un cuerpo, $p(x) \in K[X]$ un polinomio. Sobre un cuerpo de descomposición L de $p(x)$ tenemos:

$$p(x) = (x - \alpha_1)^{m_1} (x - \alpha_2)^{m_2} \dots (x - \alpha_r)^{m_r}; \quad \alpha_i \in L, \alpha_i \neq \alpha_j, m_i \geq 1$$

Entonces α_i es una **raíz simple** si $m_i = 1$ y es **múltiple** si $m_i > 1$ (con multiplicidad m_i).

Definición 3.14 (Cosas separables)

Sea L/K una extensión algebraica.

- Un polinomio $p(x) \in K[X]$ es **separable** si no tiene raíces múltiples (en cualquier cuerpo de descomposición).
- Un elemento $\alpha \in L$ es **separable** sobre K si $m_{\alpha,K}(x)$ es separable.
- La extensión L/K es **separable** si todo $\alpha \in L$ es separable sobre K .
- Un polinomio, elemento o extensión que no es separable se dice que es **inseparable**.

Definición 3.15 (Derivada formal)

Dado un polinomio $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ en $K[X]$, su **derivada formal** es:

$$p'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \in K[X]$$

Proposición 3.16

Sean K un cuerpo, $p(x) \in K[X]$, L un cuerpo de descomposición de $p(x)$. Entonces:

- $p(x)$ tiene una raíz múltiple $\alpha \in L$ si y solo si α también es una raíz de $p'(x)$.
- $p(x)$ es separable si y solo si $\text{mcd}(p(x), p'(x)) = 1$ en $K[X]$.

Corolario 3.17

Un polinomio irreducible $p(x) \in K[X]$ es inseparable si y solo si $p'(x) \equiv 0$.

Corolario 3.18

Sea K un cuerpo de característica 0. Entonces:

- Todo polinomio irreducible en $K[X]$ es separable.
- Un polinomio en $K[X]$ es separable si y solo si es el producto de polinomios irreducibles distintos.

i Nota

En característica $p > 0$, sí hay anulaciones al derivar:

$$(x^{pm})' = pmx^{pm-1} = 0$$

Y esto puede ocurrir también para polinomios irreducibles.

Proposición 3.19 (Endomorfismo de Frobenius)

Sea K un cuerpo con $\text{char}(K) = p > 0$. La aplicación $\varphi : K \rightarrow K$ con $a \rightarrow a^p$ es un morfismo de cuerpos, llamado el **endomorfismo de Frobenius**.

El endomorfismo de Frobenius es inyectivo (es un morfismo de cuerpos). Es interesante la situación en la que también es sobreyectivo (luego automorfismo).

Definición 3.20 (Cuerpo perfecto)

Un cuerpo K es **perfecto** si $\text{char}(K) = 0$ o bien $\text{char}(K) = p$ y $K = K^p$, es decir, que todo elemento de K es una potencia p -ésima (o admite una raíz p -ésima).

Lema 3.21

Todo cuerpo finito es perfecto.

Teorema 3.22

Sea K un cuerpo perfecto.

- Todo polinomio irreducible en $K[X]$ es separable.
- Un polinomio en $K[X]$ es separable si y solo si es el producto de polinomios irreducibles distintos.

Teorema 3.23 (Existencia y unicidad de cuerpos finitos)

Para $n \in \mathbb{N}$, $n \geq 1$ y p primo, existe un cuerpo con p^n elementos que es único salvo \mathbb{F}_p -isomorfismo.

Teorema 3.24 (Teorema del elemento primitivo)

Si L/K es una extensión separable finita, entonces es simple (es decir, $\exists \alpha \in L : L = K(\alpha)$).

AGB

TEMA 4. EL TEOREMA FUNDAMENTAL DE LA TEORÍA DE GALOIS

4.1. AUTOMORFISMOS DE CUERPOS

Definición 4.1 (Morfismo de cuerpos)

Sean K un cuerpo, F/K y L/K dos extensiones. Un **morfismo de cuerpos** $\varphi : F \rightarrow L$ es un K -morfismo (o morfismo de extensiones) si $\varphi|_K = \text{id}_K$ ($\varphi(a) = a$ para $a \in K$).

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & L \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi|_K = \text{id}_K} & K \end{array}$$

Proposición 4.2

Sean F, L cuerpos, $\varphi : F \rightarrow L$ un morfismo de cuerpos, $K \subset F$ el subcuerpo primo de F . Entonces:

- K es también el subcuerpo primo de L (salvo isomorfismo).
- φ es un K -morfismo.

Lema 4.3

Sean K un cuerpo, F/K y L/K extensiones, $\sigma : F \rightarrow L$ un K -morfismo. Sea $\alpha \in F$ algebraico sobre K y $p(x) \in K[X]$ un polinomio del que α es raíz. Entonces $\sigma(\alpha) \in L$ es raíz de $p(x)$.

$$p(x) \in K[X] \rightarrow \begin{cases} p(x) \in F[X] \rightarrow p(\alpha) = 0 \text{ en } F \\ p(x) \in L[X] \rightarrow p(\sigma(\alpha)) = 0 \text{ en } L \end{cases}$$

Lema 4.4

Sean K un cuerpo, F/K y L/K extensiones, \mathcal{B} una base de F como K -espacio vectorial. Sea $\sigma : F \rightarrow K$ un morfismo de K -espacios vectoriales. Entonces σ es un K -morfismo de cuerpos si y solo si $\sigma(\alpha\alpha') = \sigma(\alpha)\sigma(\alpha')$ para todos $\alpha, \alpha' \in \mathcal{B}$.



Importante

Los K -morfismos de cuerpos están determinados por las imágenes de los elementos de una base si estas son compatibles con el producto.

Proposición 4.5

- Si $[K(\alpha) : K] = n$, L contiene a un cuerpo de descomposición de $m_{\alpha, K}(x)$ sobre K y $m_{\alpha, K}(x)$ es separable, entonces hay $n = \deg(m_{\alpha, K}(x))$ K -morfismos $K(\alpha) \rightarrow L$ distintos.
- Buscando morfismos de la forma $K(\alpha_1, \alpha_2, \dots, \alpha_r) \rightarrow L$. Si $m_{\alpha_i, K(\alpha_1, \alpha_2, \dots, \alpha_{i-1})}(x)$ tiene la misma expresión que $m_{\alpha_i, K}(x)$ para $2 \leq i \leq r$, entonces todas las combinaciones de raíces de $m_{\alpha_j, K}(x)$ son imágenes válidas de α_j en un K -morfismo de cuerpos. Es decir, hemos encontrado una **condición suficiente**.

Definición 4.6 (Grupo de automorfismos)

Sea K un cuerpo. Entonces:

- Un isomorfismo $\sigma : K \rightarrow K$ se llama un **automorfismo** de K .
- El conjunto de automorfismos de K se denota $\mathbf{Aut}(K)$.
- Si L/K es una extensión, el conjunto de K -automorfismos de L se denota $\mathbf{Aut}(L/K)$.

Lema 4.7

Sea L/K una extensión algebraica. Entonces todo K -endomorfismo de L es un K -auto-morfismo.

Lema 4.8

Sean K un cuerpo, L/K una extensión. Entonces $(\text{Aut}(L), \circ, \text{id}_L)$ es un grupo y $(\text{Aut}(L/K), \circ, \text{id}_L)$ es un subgrupo.

Definición 4.9 (Cuerpo fijo)

Sean $K, L/K$ una extensión, H un subgrupo de $\text{Aut}(L/K)$. El conjunto

$$L^H = \{a \in L : \forall h \in H \ h(a) = a\}$$

es un subcuerpo de L , llamado el **cuerpo fijo** de H .

! Importante

Tenemos dos correspondencias:

- Subcuerpos de $L \rightarrow$ Subgrupos de $\text{Aut}(L) \rightarrow K \rightarrow \text{Aut}(L/K)$.
- Subgrupos de $\text{Aut}(L) \rightarrow$ Subcuerpos de $L \rightarrow H \rightarrow L^H$.

La siguiente proposición nos dice que revierten las inclusiones.

Proposición 4.10

Sean K un cuerpo, L/K una extensión.

- Si $K_1 \subseteq K_2 \subseteq L$ son dos subcuerpos de L , entonces $\text{Aut}(L/K_2) \leq \text{Aut}(L/K_1)$.
- Si $H_1 \leq H_2 \leq \text{Aut}(L/K)$ son dos subgrupos de $\text{Aut}(L/K)$, entonces $K \subseteq L^{H_2} \subseteq L^{H_1}$.

i Nota

Nos gustaría que la correspondencia entre subgrupos de $\text{Aut}(L/K)$ y subcuerpos de L que contienen a K fuese perfecta. Necesitamos $\text{Aut}(L/K)$ sea lo más grande posible. Para ello buscamos que L/K sea **normal** y **separable**.

Lema 4.11

Sea L/K una extensión. Sean $\sigma_1, \sigma_2, \sigma_r \in \text{Aut}(L/K)$ automorfismos distintos. Entonces son linealmente independientes sobre L . Es decir, si $\lambda_1, \dots, \lambda_r \in L$ no son todos nulos, entonces:

$$\begin{aligned} \lambda_1 \sigma_1 + \lambda_2 \sigma_2 + \dots + \lambda_r \sigma_r : L &\rightarrow L \\ a &\rightarrow \lambda_1 \sigma_1(a) + \lambda_2 \sigma_2(a) + \dots + \lambda_r \sigma_r(a) \end{aligned}$$

no es el morfismo de grupos nulo $L \rightarrow L$; $a \rightarrow 0$.

Proposición 4.12

Sean L/K una extensión y H un subgrupo finito de $\text{Aut}(L/K)$. Entonces:

$$[L : L^H] = |H| \quad \text{y} \quad [L^H : K] = \frac{[L : K]}{|H|}$$

Corolario 4.13

Sea L/K una extensión finita. Entonces

$$|\text{Aut}(L/K)| \leq [L : K]$$

y $|\text{Aut}(L/K)| = [L : K]$ si y solo si $K = L^{\text{Aut}(L/K)}$.



Importante

- Ya hemos visto que, si L/K es una extensión y $p(x) \in K[X]$ es irreducible, todo K -automorfismo de L debe permutar las raíces de $p(x)$ en L .
- No es cierto que para toda permutación haya un K -automorfismo que la efectúe, pero sí que, fijadas dos raíces de $p(x)$ en L , hay un K -automorfismo que lleva una en la otra.

Proposición 4.14

Sean L/K una extensión normal y finita, M_1/K y M_2/K dos subextensiones. Si $\psi : M_1 \rightarrow M_2$ es un K -isomorfismo, entonces existe $\sigma \in \text{Aut}(L/K)$ tal que $\sigma|_{M_1} = \psi$.

Corolario 4.15

Sea K/L una extensión normal y finita. Si $p(x) \in K[X]$ es un polinomio irreducible y $\alpha, \beta \in L$ son raíces de $p(x)$, entonces existe $\sigma \in \text{Aut}(L/K)$ con $\sigma(\alpha) = \beta$.

Corolario 4.16

Sea L/K una extensión normal, finita y separable. Entonces

$$|\text{Aut}(L/K)| = [L : K]$$

Definición 4.17 (Extensiones y grupos de Galois)

- Se dice que una extensión L/K es **de Galois** si es normal, finita y separable.
- Si L/K es una extensión de Galois, llamamos a $\text{Aut}(L/K)$ el **grupo de Galois** de L/K y lo denotamos $\text{Gal}(L/K)$.

Definición 4.18 (Polinomios ciclotómicos)

Sea p primo. Definimos el **polinomio ciclotómico** de orden p como:

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1 \in \mathbb{Q}[X]$$

Además, $\phi_p(x)$ es irreducible.

Definición 4.19 (Extensión ciclotómica)

La **extensión ciclotómica p -ésima** es el cuerpo de descomposición de $\phi_p(x)$, es decir, sean las raíces de $\phi_p(x) := e^{\frac{2\pi i}{p}} = \zeta_p^i$, $i = 1, \dots, p-1$, entonces podemos poner

$$\mathbb{Q}(\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}) = \mathbb{Q}(\zeta_p)$$

Lema 4.20

La extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es de Galois.

i Nota

Si L es el cuerpo de descomposición de un polinomio $p(x) \in K[X]$ (irreducible o no) de grado n , entonces (salvo isomorfismo) $\text{Aut}(L/K) \leq S_n$, con S_n el grupo de permutaciones de n elementos

Si $\alpha_1, \dots, \alpha_n \in L$ son las raíces de $p(x)$ en L , entonces un elemento de $\text{Aut}(L/K)$ las permuta. Esta asociación **no** es sobreyectiva en general.

Si $p(x) = f(x)g(x)$ en $K[X]$, entonces $\text{Aut}(L/K) \leq S_m \times S_r$.

4.2. EL TEOREMA FUNDAMENTAL DE LA TEORÍA DE GALOIS**Teorema 4.21 (Caracterizaciones de extensiones de Galois)**

Sea L/K una extensión finita de cuerpos. Entonces son equivalentes:

- L/K es una extensión de Galois (finita, normal y separable)
- $[L : K] = |\text{Aut}(L/K)|$
- $K = L^{\text{Aut}(L/K)}$

Proposición 4.22

Sean K un cuerpo, $G \leq \text{Aut}(K)$ un subgrupo finito de automorfismos. Entonces $\text{Aut}(K/K^G) = G$ y se deduce que K/K^G es una extensión de Galois, con grupo de Galois G . Es decir, no hay ningún automorfismo de K que fije K^G y no esté en G .

Corolario 4.23

Sea K un cuerpo, $G_1 \neq G_2$ dos subgrupos finitos de $\text{Aut}(K)$. Entonces $K^{G_1} \neq K^{G_2}$.

Teorema 4.24 (Teorema Fundamental de la Teoría de Galois)

Sea L/K una extensión de Galois. Hay una biyección:

$$\begin{aligned} \{\text{subcuerpos } F \text{ de } L \text{ que contienen a } K\} &\rightarrow \{\text{subgrupos de } H \text{ de } \text{Aut}(L/K)\} \\ F &\rightarrow \text{Aut}(L/F) \\ L^H &\rightarrow H \end{aligned}$$

Bajo esta correspondencia:

- Se revierten las inclusiones: $L^{H_1} \subseteq L^{H_2} \Leftrightarrow H_2 \leq H_1$
- $[L : L^H] = |H|$ y $[L^H : K] = |\text{Aut}(L/K) : H|$
- L/F es siempre una extensión de Galois, con grupo de Galois $\text{Aut}(L/F)$
- F/K es una extensión de Galois si y solo si $\text{Aut}(L/F)$ es un subgrupo normal de $\text{Aut}(L/K)$. En ese caso,

$$\text{Aut}(F/K) \cong \frac{\text{Aut}(L/K)}{\text{Aut}(L/F)}$$

- Sean cuerpos $K \subseteq F_1, F_2 \subseteq L$, $H_1 = \text{Aut}(L/F_1)$, $H_2 = \text{Aut}(L/F_2)$. Entonces $F_1 \cap F_2$ corresponde a $\langle H_1, H_2 \rangle$ (grupo generado por H_1 y H_2) y $F_1 F_2$ (menor cuerpo que contiene a F_1 y F_2) corresponde a $H_1 \cap H_2$.

Es decir, los retículos de subcuerpos de L que contienen a K y de subgrupos de G son duales (el diagrama de uno es el otro «dado la vuelta»).

Definición 4.25 (Retículo)

Un **retículo** es un conjunto parcialmente ordenado tal que para cada par de elementos, existen:

- Su supremo: menor elemento mayor que ambos (*join*)
- Su ínfimo: mayor elemento menor que ambos (*meet*)

ACGB