Universidad de Murcia

Grado en Matemáticas

Ecuaciones Algebraicas

Notas de Clase

Laura Fernández Sánchez

Curso 2025 – 2026

Índice general

Capítulo 1

Extensiones Algebraicas

1.1. Extensiones de Cuerpos

Recordemos de la teoría general de anillos que un cuerpo es un anillo conmutativo con la suma y el producto, donde todo elemento no nulo tiene inverso multiplicativo.

Definición 1.1.1: Extensión de un cuerpo (Def. 1.1)

Sea K un cuerpo. Una **extensión** de K es un cuerpo L que contiene a K como subcuerpo. En tal caso, decimos que L/K (o simplemente $K \subseteq L$) es una extensión de cuerpos.

Observación 1.1.1: Estructura de Espacio Vectorial y Grado de la Extensión

Toda extensión L/K dota a L de una estructura natural de **espacio vectorial sobre** K, que denotaremos como L_K.

- La "suma de vectores.[es] simplemente la suma habitual de elementos en L.
- El "producto por escalar.[es] el producto de un elemento de K por un elemento de L dentro del cuerpo L.

Como todo espacio vectorial, L_K posee una base (llamada base de la extensión). A la dimensión de este espacio vectorial la llamaremos **grado de la extensión** y la denotaremos por $[L : K]$:

$$[L : K] = \dim_K(L)$$

Decimos que L/K es una **extensión finita** si su grado es finito ($[L : K] < \infty$).

Observación 1.1.2: Consideraciones de Cardinalidad

Si L/K es una extensión finita de grado n, entonces como espacios vectoriales se tiene el isomorfismo $L_K \simeq K^n$. Esto implica que la cardinalidad de los cuerpos cumple $|L| = |K|^n$.

- Si K es un cuerpo finito de orden q, entonces L será un cuerpo finito de orden q^n.
- Si K es un cuerpo infinito, entonces L tendrá exactamente el mismo cardinal (infinito) que K.

Ejemplos Fundamentales de Extensiones (Ej. 1.2)

Ejemplo 1.1.1: Extensión Trivial

Si L/K es una extensión de cuerpos, entonces $[L : K] = 1$ si y solo si $K = L$.
Justificación: Si $[L : K] = 1$, esto significa que $\dim_K(L) = 1$. Cualquier elemento no nulo de L forma una base. En particular, el elemento $1 \in K$ es una base válida. Por tanto, $L = \langle 1 \rangle_K = \{k \cdot 1 \mid k \in K\} = K$. Y trivialmente, si $K = L$, la dimensión sobre sí mismo es 1.

Ejemplo 1.1.2: Los Complejos sobre los Reales

$\mathbb{C}/\mathbb{R}$ es una extensión finita de grado exactamente 2.
Justificación: Todo número complejo $z \in \mathbb{C}$ se escribe de forma única como $z = a \cdot 1 + b \cdot i$, con $a, b \in \mathbb{R}$. El conjunto $\{1, i\}$ es un sistema generador y sus elementos son linealmente independientes sobre $\mathbb{R}$. Por tanto, es una base y $[\mathbb{C} : \mathbb{R}] = 2$.

Ejemplo 1.1.3: Extensiones de Grado Infinito

Las extensiones $\mathbb{R}/\mathbb{Q}$ y $\mathbb{C}/\mathbb{Q}$ son extensiones de grado infinito.
Justificación (por cardinalidad): Sabemos que $\mathbb{Q}$ es un conjunto numerable. Si la extensión $\mathbb{R}/\mathbb{Q}$ fuera finita de grado n, entonces $\mathbb{R}$ sería isomorfo a $\mathbb{Q}^n$. El producto cartesiano finito de conjuntos numerables ($\mathbb{Q}^n$) sigue siendo numerable. Sin embargo, $\mathbb{R}$ es no numerable. Por reducción al absurdo, el grado no puede ser finito.

Ejemplo 1.1.4: Extensiones Cuadráticas Racionales

Para cualquier $n \in \mathbb{Q}$, consideramos la extensión $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$, donde $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}$.

- **Caso 1:** Si n es un cuadrado perfecto en $\mathbb{Q}$ (ej. $n = 9$), entonces $\sqrt{n} \in \mathbb{Q}$. En este caso $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}$ y el grado de la extensión es 1.
- **Caso 2:** Si n no es un cuadrado perfecto, entonces $\{1, \sqrt{n}\}$ forma una base. ¿Por qué son linealmente independientes? Si existieran $a, b \in \mathbb{Q}$ tales que $a \cdot 1 + b \cdot \sqrt{n} = 0$, y supusiéramos que $b \neq 0$, tendríamos $\sqrt{n} = \frac{-a}{b}$. Pero $\frac{-a}{b} \in \mathbb{Q}$, lo cual es una contradicción porque habíamos supuesto que $\sqrt{n} \notin \mathbb{Q}$. Por tanto $b = 0$, lo que fuerza a que $a = 0$. Son independientes y el grado de la extensión es $[\mathbb{Q}(\sqrt{n}) : \mathbb{Q}] = 2$.

Ejemplo 1.1.5: Cuerpos de Fracciones Polinómicas

El cuerpo de fracciones racionales $K(X)$ (formado por los cocientes $\frac{P(X)}{Q(X)}$) del anillo de polinomios $K[X]$ es una extensión de K de grado infinito. (Basta observar que el conjunto infinito $\{1, X, X^2, X^3, \dots\}$ es linealmente independiente sobre K).

Morfismos, Torres y Grupos de Galois

Definición 1.1.2: Torres y Multiplicatividad

Una **torre de extensiones** es una cadena de subcuerpos: $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$. Cada paso K_{i+1}/K_i se llama subextensión.
Una clase $\mathcal{C}$ de extensiones se dice **multiplicativa** (o transitiva) si para cada torre $K_1 \subseteq K_2 \subseteq K_3$, se cumple que:

$$K_3/K_1 \in \mathcal{C} \iff K_2/K_1 \in \mathcal{C} \text{ y } K_3/K_2 \in \mathcal{C}$$

Definición 1.1.3: Homomorfismos de Extensiones

Si L_1 y L_2 son extensiones de K, un **homomorfismo de extensiones** (o K-homomorfismo) de L_1/K en L_2/K es un homomorfismo de cuerpos $f : L_1 \to L_2$ que deja fijos los elementos del cuerpo base, es decir, $f(a) = a$ para todo $a \in K$. Esto equivale a decir que f es una aplicación lineal entre espacios vectoriales sobre K.

Definición 1.1.4: Clasificación de Morfismos y Grupo de Galois

- **Endomorfismo:** Un K-homomorfismo de L/K en sí misma ($L \to L$).
- **Isomorfismo (K-isomorfismo):** Un K-homomorfismo que además es biyectivo.
- **Automorfismo (K-automorfismo):** Un isomorfismo de una extensión L/K en sí misma.

El **Grupo de Galois** de una extensión L/K, denotado como $\mathrm{Gal}(L/K)$, es el conjunto de todos los K-automorfismos de L, dotado de la operación de composición de funciones.

Definición 1.1.5: Subextensiones y Admisibilidad

- Una **subextensión** de L/K es un cuerpo intermedio M tal que $K \subseteq M \subseteq L$.
- Dos extensiones L_1/K y L_2/K se dicen **admisibles** si existe un cuerpo mayor L que las contiene simultáneamente ($L_1 \subseteq L$ y $L_2 \subseteq L$).

Observación 1.1.3: Inyectividad universal de los homomorfismos de cuerpos

Todos los homomorfismos entre cuerpos son inyectivos. *Demostración:* El núcleo de un homomorfismo de anillos $f : K \to L$ es siempre un ideal de K. Pero los únicos ideales de un cuerpo son $\{0\}$ y el propio cuerpo. Como un homomorfismo de cuerpos por definición cumple $f(1) = 1 \neq 0$, el núcleo no puede ser todo K. Por exclusión, $\ker(f) = \{0\}$, lo que garantiza que la aplicación es estrictamente inyectiva.
Consecuencia fundamental: Si existe un homomorfismo $f : K \to L$, la imagen $f(K)$ es un subcuerpo de L idéntico a K. A efectos prácticos, abusaremos de la notación e identificaremos K con su imagen $f(K)$, considerando siempre que el cuerpo de partida es un subcuerpo del cuerpo de llegada ($K \subseteq L$).

Proposición 1.1.1: Propiedades Estructurales Básicas (Prop. 1.3)

1. Sean L_1 y L_2 extensiones de K. Si existe un K-homomorfismo $f : L_1 \to L_2$, entonces sus grados cumplen:
$$[L_1 : K] \leq [L_2 : K]$$
2. Todo endomorfismo de una extensión **finita** es automáticamente un automorfismo.
3. **Propiedad Multiplicativa del Grado:** Sea $K \subseteq E \subseteq L$ una torre de cuerpos. Si la extensión base y la extensión superior son finitas, entonces la extensión total es finita y se cumple:
$$[L : K] = [L : E] \cdot [E : K]$$
Además, si B es una base de E_K y B' es una base de L_E, entonces el producto de bases:
$$A = \{b \cdot b' \mid b \in B, b' \in B'\}$$
es una base exacta de L_K.

Demostración de la Proposición 1.3. **1) Desigualdad de grados para homomorfismos:** Sea $f : L_1 \to L_2$ el K-homomorfismo en cuestión. Como L_1 y L_2 son cuerpos, sabemos que todo homomorfismo entre cuerpos es estrictamente inyectivo. Por tanto, f establece un isomorfismo entre L_1 y su imagen, es decir, $L_1 \simeq f(L_1)$.

Viendo a $f(L_1)$ como un subespacio vectorial de L_2 sobre el cuerpo base K, la inyectividad garantiza que la dimensión se conserva:

$$\dim_K(L_1) = \dim_K(f(L_1))$$

Como la dimensión de un subespacio nunca puede exceder la dimensión del espacio total ($f(L_1) \subseteq L_2$), se sigue que:
$$\dim_K(f(L_1)) \leq \dim_K(L_2) \implies [L_1 : K] \leq [L_2 : K]$$

2) Todo endomorfismo de una extensión finita es un automorfismo: Sea $\sigma : L \to L$ un endomorfismo y sea $[L : K] = n < \infty$. De nuevo, por ser un homomorfismo de cuerpos, σ es inyectivo.

Recordemos el **Teorema de las Dimensiones** (o Teorema del Rango-Nulidad) que vimos en Álgebra Lineal. Para cualquier aplicación lineal $T : V \to V$:

$$\dim(\ker(T)) + \dim(\mathrm{Im}(T)) = \dim(V)$$

Aplicando esto a nuestro K-endomorfismo σ (que es una aplicación K-lineal del espacio L_K en sí mismo): Como σ es inyectivo, su núcleo es trivial, $\ker(\sigma) = \{0\}$, luego $\dim_K(\ker(\sigma)) = 0$. Sustituyendo en la fórmula:

$$0 + \dim_K(\mathrm{Im}(\sigma)) = n \implies \dim_K(\mathrm{Im}(\sigma)) = n$$

Dado que la imagen de σ tiene la misma dimensión que el espacio total L y está contenida en él ($\mathrm{Im}(\sigma) \subseteq L$), deducimos que $\mathrm{Im}(\sigma) = L$. Por tanto, σ es suprayectiva. Al ser inyectiva y suprayectiva, es biyectiva, lo que la convierte por definición en un **automorfismo**.

3) Propiedad multiplicativa del grado: Sea $K \subseteq E \subseteq L$. Supongamos que $B = \{u_1, \dots, u_m\}$ es una base de E como K-espacio vectorial ($m = [E : K]$) y que $C = \{v_1, \dots, v_n\}$ es una base de L como E-espacio vectorial ($n = [L : E]$). Queremos demostrar que el conjunto producto $A = \{u_i \cdot v_j \mid i = 1 \dots m, j = 1 \dots n\}$ es una base de L_K.

Paso A: A es un Sistema Generador. Sea $x \in L$ un elemento cualquiera. Como C es base de L sobre E, podemos escribir x como combinación lineal con coeficientes en E:

$$x = \sum_{j=1}^{n} \lambda_j \cdot v_j \quad \text{con } \lambda_j \in E$$

Ahora, como B es base de E sobre K, cada coeficiente $\lambda_j \in E$ se puede escribir a su vez como combinación lineal con coeficientes en K:

$$\lambda_j = \sum_{i=1}^{m} a_{ij} \cdot u_i \quad \text{con } a_{ij} \in K$$

Sustituyendo λ_j en la primera ecuación:

$$x = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} \cdot u_i \right) \cdot v_j = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} \cdot (u_i \cdot v_j)$$

Esto demuestra que cualquier $x \in L$ se puede expresar como combinación lineal de los elementos de A con coeficientes en K.

Paso B: A es Linealmente Independiente. Supongamos que una combinación lineal de los elementos de A se anula:

$$\sum_{j=1}^{n} \sum_{i=1}^{m} k_{ij} \cdot (u_i \cdot v_j) = 0 \quad \text{con } k_{ij} \in K$$

Queremos ver que $k_{ij} = 0$ para todo i, j. "Deshacemos"la suma agrupando respecto a v_j:

$$\sum_{j=1}^{n} \underbrace{\left(\sum_{i=1}^{m} k_{ij} \cdot u_i \right)}_{C_j} \cdot v_j = 0$$

Llamemos $C_j = \sum_{i=1}^{m} k_{ij} u_i$. Como $u_i \in E$ y $k_{ij} \in K$, está claro que $C_j \in E$. Nuestra ecuación se convierte en $\sum_{j=1}^{n} C_j \cdot v_j = 0$. Como los v_j forman una base de L sobre el cuerpo E, son linealmente independientes sobre E, lo que fuerza a que todos los coeficientes sean cero: $C_j = 0$ para todo j. Es decir:

$$\sum_{i=1}^{m} k_{ij} \cdot u_i = 0 \quad \forall j$$

Pero los u_i forman una base de E sobre K, por lo que son linealmente independientes sobre K. Esto fuerza a que los coeficientes internos también sean cero: $k_{ij} = 0$ para todo i. Como $k_{ij} = 0$ para todo i, j, el conjunto A es linealmente independiente.

Al ser un sistema generador y linealmente independiente, A es una base de L_K. Como el cardinal de A es $m \cdot n$, concluimos que:

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

$\square$

1.2. Operaciones con Extensiones: Compuesto y Adjunción

Definición 1.2.1: (4) El Cuerpo Compuesto L_1L_2

Si L_1 y L_2 son dos subcuerpos admisibles (es decir, ambos contenidos dentro de un cuerpo mayor L), se define su **cuerpo compuesto** L_1L_2 como el menor subcuerpo de L que contiene tanto a L_1 como a L_2.

Observación 1.2.1: Construcción rigurosa del cuerpo compuesto

El problema lógico: La simple unión conjuntista $L_1 \cup L_2$ casi nunca es un cuerpo. Si tomamos $a \in L_1$ y $b \in L_2$, para que sea un cuerpo debe contener su suma $a + b$ y su producto $a \cdot b$. Pero si $a \notin L_2$ y $b \notin L_1$, esos resultados caen fuera de la unión.
La Construcción (Paso a Paso):

1. *La estructura de Anillo (Numeradores):* Para capturar todos los productos y sumas posibles, consideramos el conjunto de todas las combinaciones lineales finitas de productos cruzados:

$$R = \left\{ \sum_{k=1}^{n} a_k b_k \;\middle|\; a_k \in L_1, b_k \in L_2 \right\}$$

   Este conjunto R es un anillo. Es cerrado bajo suma y multiplicación, pero no necesariamente tiene inversos.

2. *La estructura de Cuerpo (Divisiones):* El cuerpo compuesto L_1L_2 debe contener los inversos de todos los elementos no nulos de ese anillo R. Por tanto, sus elementos tienen necesariamente la forma de fracciones:

$$L_1L_2 = \left\{ \frac{x}{y} \;\middle|\; x, y \in R, y \neq 0 \right\}$$

   Sustituyendo la forma explícita de x e y, llegamos a la expresión general:

$$L_1L_2 = \left\{ \frac{a_1b_1 + \cdots + a_nb_n}{a'_1b'_1 + \cdots + a'_mb'_m} \;\middle|\; a_i, a'_i \in L_1;\ b_i, b'_i \in L_2;\ \text{den.} \neq 0 \right\}$$

Nota para la intuición: Si la extensión es algebraica y finita (como suele ocurrir en Teoría de Galois), muchas veces el anillo R ya es un cuerpo por sí mismo (gracias a las propiedades de los elementos algebraicos), y no hace falta efectuar la división. Sin embargo, la definición general con fracciones cubre rigurosamente todos los casos, incluyendo extensiones trascendentes.

Definición 1.2.2: (5) Adjunción de un conjunto S a un cuerpo K

Sea K un cuerpo base y $S \subset L$ un conjunto de elementos .$^{\text{ex}}$traños.$^{\text{en}}$ una extensión mayor. Queremos "pegarle"(adjuntar) esos elementos a K. Es fundamental distinguir entre el **Anillo generado** $K[S]$ y el **Cuerpo generado** $K(S)$.

Observación 1.2.2: A. El Menor Subanillo $K[S]$

¿Qué elementos debe tener obligatoriamente cualquier anillo que contenga a K y a S?

1. Debe tener productos de elementos de S entre sí (potencias $s^2, s_1 s_2$, etc.).
2. Debe tener productos de escalares de K por esos elementos.
3. Debe tener sumas de todo lo anterior.

Esto describe exactamente la evaluación de un polinomio. Cualquier elemento de este anillo generado tiene la forma de un polinomio evaluado en los elementos de S:

$$y = p(s_1, s_2, \dots, s_n) \quad \text{donde } p \in K[X_1, \dots, X_n] \text{ y } s_i \in S$$

Detalle Lógico Importante: Aunque el conjunto S sea infinito, cualquier cálculo concreto (polinomio) solo puede usar una **cantidad finita** de elementos de S a la vez. Por eso la definición indica "donde n es un número natural arbitrario"; la estructura algebraica siempre opera de forma finitaria.

Observación 1.2.3: B. El Menor Subcuerpo $K(S)$

Un anillo de polinomios (como $K[S]$) no suele ser un cuerpo (por ejemplo, el propio anillo $K[X]$ carece de inversos multiplicativos para X). Para obtener el cuerpo generado, es imperativo añadir los inversos.
Por tanto, el cuerpo generado $K(S)$ se construye formalmente como el **cuerpo de fracciones del anillo** $K[S]$. Sus elementos son funciones racionales (cocientes de polinomios) evaluadas en combinaciones finitas de los elementos de S:

$$z = \frac{p(s_1, \dots, s_n)}{q(s_1, \dots, s_n)} \quad \text{donde } p, q \in K[X_1, \dots, X_n],\ s_i \in S \text{ y } q(s_1, \dots, s_n) \neq 0$$

Observación 1.2.4: Intersección de cuerpos

Recordemos que la intersección de cuerpos es siempre un cuerpo. Entonces, la intersección de cualquier familia de subcuerpos de L es también un subcuerpo de L.
Dado un conjunto $S \subset L$, el cuerpo generado $K(S)$ se define como el menor subcuerpo de L que contiene tanto a K como a S. Así pues, podemos ver a $K(S)$ como la intersección de todos los subcuerpos de L que contienen a $K \cup S$.
Además, si tenemos dos conjuntos $S_1, S_2 \subset L$, se cumple que al generar sucesivamente es lo mismo que generar con la unión:

$$K(S_1)K(S_2) = K(S_1 \cup S_2)$$

Definición 1.2.3: Compuesto de una familia de subextensiones

Si L_1/K y L_2/K son dos subextensiones de L, entonces su cuerpo compuesto L_1L_2 es la intersección de todos los subcuerpos de L que contienen a $L_1 \cup L_2$.
Este concepto se puede generalizar de forma natural a una familia arbitraria de subextensiones $\mathcal{C}$. El compuesto de $\mathcal{C}$ es el menor subcuerpo de L que contiene a todos los elementos de $\mathcal{C}$, y coincide con $K(\bigcup_{E\in\mathcal{C}} E)$.
Si $\mathcal{C} = \{L_1/K, \ldots, L_n/K\}$, el compuesto se denota $L_1 \ldots L_n = K(L_1 \cup \cdots \cup L_n)$ y está formado explícitamente por todos los elementos de la forma:

$$\frac{\sum_{i=1}^{m} a_{1i} \cdots a_{ni}}{\sum_{i=1}^{m} b_{1i} \cdots b_{ni}}$$

con m arbitrario, $a_{ji}, b_{ji} \in L_j$ y el denominador distinto de cero.

Definición 1.2.4: Extensiones Simples y Finitamente Generadas

- Diremos que L/K es una **extensión finitamente generada** si existe un número finito de elementos $\alpha_1, \ldots, \alpha_n \in L$ tales que $L = K(\alpha_1, \ldots, \alpha_n)$.
- Diremos que L/K es **simple** si $L = K(\alpha)$ para un único elemento $\alpha \in L$. En este caso, diremos que α es un **elemento primitivo** de la extensión.

Observación 1.2.5:

$K[S]$: El Anillo generado (Corchetes = Polinomios) Cuando usamos corchetes, estamos generando el menor **anillo** que contiene a K y a S. Las operaciones permitidas son suma, resta y multiplicación. **NO división**.

- *Forma:* Polinomios evaluados en los elementos de S.
- *Ejemplo:* En $\mathbb{Z}[\sqrt{2}]$ podemos tener $1+\sqrt{2}$ o $(\sqrt{2})^2 = 2$, pero no podemos tener $1/\sqrt{2}$ porque en un anillo no se garantiza la existencia de inversos.

$K(S)$**: El Cuerpo generado (Paréntesis = Fracciones)** Cuando usamos paréntesis, estamos generando el menor **cuerpo** que contiene a K y a S. Operaciones permitidas: Suma, resta, multiplicación y **división** (por no nulos).

- *Forma:* Cocientes de polinomios (fracciones racionales) evaluados en S. Es el Çuerpo de Fracciones"del anillo $K[S]$.
- Se tiene siempre la inclusión: $K[S] \subseteq K(S)$.

¿Cuándo son iguales $K[S]$ y $K(S)$?
Aquí está la clave para entender por qué en Teoría de Galois a menudo se operan como si fueran idénticos:

- **Si S es trascendente** (como una variable X): $K[X] \neq K(X)$. El inverso de X (que es $1/X$) vive en el cuerpo $K(X)$ pero no en el anillo $K[X]$.
- **Si S es algebraico** (ej. $\alpha = \sqrt{2}$): ¡Sorpresa! $K[\alpha] = K(\alpha)$. Si un elemento satisface una ecuación polinómica, esto permite racionalizarçualquier fracción. Por ejemplo, en $\mathbb{Q}(\sqrt{2})$, el inverso $1/\sqrt{2}$ se puede reescribir como $\frac{\sqrt{2}}{2} = 0 + \frac{1}{2}\sqrt{2}$. Al poder escribir el inverso como una combinación lineal (un polinomio), el anillo absorbe al cuerpo.

Concepto	**Definición Formal**	**Ejemplo Clave**
Finitamente Generada	Existe un conjunto finito $S = \{\alpha_1, \dots, \alpha_n\}$ tal que $L = K(\alpha_1, \dots, \alpha_n)$.	$K(X)$ (generada solo por el elemento X).
Extensión Finita	El grado $[L : K]$ es un número finito n (dimensión vectorial finita).	$\mathbb{Q}(\sqrt{2})$ (grado 2).

La trampa: $K(X)$ está generada por 1 solo elemento (X), así que es finitamente generada. PERO, su base como espacio vectorial es $\{1, X, X^2, \dots\}$, por lo que su grado es infinito.

Conclusión: Toda extensión finita es finitamente generada, pero **NO toda extensión finitamente generada es finita**. (Solo lo son si sus generadores son algebraicos).

Lema 1.2.1: Lema 1.4

Sea L/K una extensión. Si $\alpha \in L$ es una raíz de un polinomio irreducible $p \in K[X]$ de grado n, entonces:

1. $K[\alpha] = K(\alpha)$.
2. Para cualquier $q \in K[X]$, se tiene $q(\alpha) = 0 \iff p \mid q$ en $K[X]$.
3. El conjunto $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ es una base de $K(\alpha)$ como espacio vectorial sobre K. En particular, $[K(\alpha) : K] = n$.

Demostración. **Demostración de (1) y (2):** Consideramos la aplicación de evaluación $\delta_\alpha : K[X] \to L$ definida por $q(X) \mapsto q(\alpha)$. Es un homomorfismo de anillos.

El núcleo de este homomorfismo es:

$$\ker(\delta_\alpha) = \{g(X) \in K[X] \mid g(\alpha) = 0\}$$

Como K es un cuerpo, $K[X]$ es un Dominio de Ideales Principales (DIP), por lo que todo ideal está generado por un único polinomio. Luego $\ker(\delta_\alpha) = (I)$ para algún polinomio I.

Como $\delta_\alpha(1) = 1 \neq 0$, el núcleo no es todo el anillo, por lo que (I) es un ideal propio ($\subsetneq K[X]$). Por hipótesis, α es raíz de p, luego $p(\alpha) = 0$. Esto implica que $p \in \ker(\delta_\alpha)$, es decir, el ideal generado por p está contenido en el núcleo: $(p) \subseteq \ker(\delta_\alpha)$.

Ahora bien, p es un polinomio irreducible. En un DIP, las nociones de elemento irreducible y primo coinciden, y todo ideal primo no nulo es maximal. Por tanto, (p) es un ideal **maximal**. Como tenemos la cadena de ideales $(p) \subseteq \ker(\delta_\alpha) \subsetneq K[X]$ y (p) no puede estar contenido estrictamente en otro ideal propio, forzosamente:

$$\ker(\delta_\alpha) = (p)$$

Esto demuestra el **apartado (2)** directamente: $q(\alpha) = 0 \iff q \in \ker(\delta_\alpha) \iff q \in (p) \iff p \mid q$.

Aplicando el Primer Teorema de Isomorfía de anillos:

$$\frac{K[X]}{\ker(\delta_\alpha)} \simeq \mathrm{Im}(\delta_\alpha)$$

Sustituyendo el núcleo y la imagen (que es precisamente el anillo generado $K[\alpha]$):

$$\frac{K[X]}{(p)} \simeq K[\alpha]$$

Dado que (p) es maximal, el cociente $K[X]/(p)$ es un cuerpo. Por isomorfismo, $K[\alpha]$ también es un **cuerpo**.

Por definición, $K(\alpha)$ es el *menor* cuerpo que contiene a K y a α. Como $K[\alpha]$ ya es un cuerpo que contiene a ambos, se debe cumplir $K(\alpha) \subseteq K[\alpha]$. Como la inclusión contraria $K[\alpha] \subseteq K(\alpha)$ es trivial, concluimos que $K[\alpha] = K(\alpha)$. Esto demuestra el **apartado (1)**.

Demostración de (3): Sea $\beta \in K(\alpha)$. Por el apartado anterior, sabemos que $K(\alpha) = K[\alpha]$, por lo que β puede expresarse como $\beta = f(\alpha)$ para algún polinomio $f \in K[X]$.

Dado que $K[X]$ es un dominio euclídeo, realizamos la división euclídea de f entre p:

$$f(X) = p(X)q(X) + r(X) \quad \text{con } \mathrm{gr}(r) < \mathrm{gr}(p) = n$$

Evaluamos esta expresión en α:

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

Como $p(\alpha) = 0$, nos queda simplemente $\beta = r(\alpha)$. Como el grado de r es estrictamente menor que n, podemos escribir $r(X) = r_0 + r_1X + \cdots + r_{n-1}X^{n-1}$. Al sustituir obtenemos $\beta = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}$, lo que prueba que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es un **sistema generador** de $K(\alpha)$ sobre K.

Veamos ahora que son **linealmente independientes**. Supongamos una combinación lineal nula: $\sum_{i=0}^{n-1} a_i\alpha^i = 0$ con $a_i \in K$. Definimos el polinomio $a(X) = \sum_{i=0}^{n-1} a_iX^i$. Claramente, $a(\alpha) = 0$. Por el apartado (2), esto implica que el polinomio $a(X)$ es múltiplo de $p(X)$. Sin embargo, por construcción, $\mathrm{gr}(a) \leq n - 1 < n = \mathrm{gr}(p)$. El único polinomio múltiplo de $p(X)$ cuyo grado es estrictamente menor que el del propio $p(X)$ es el **polinomio cero**. Por tanto, $a(X) = 0$, lo que fuerza a que $a_i = 0$ para todo i.

Al ser un sistema generador y linealmente independiente, conforman una base, por lo que $\dim_K(K(\alpha)) = n$. □

1.3. Adjunción de Raíces y Teorema de Kronecker

Teorema 1.3.1: Teorema de Kronecker

Si K es un cuerpo y $p \in K[X] \setminus K$ es un polinomio no constante, entonces existe una extensión L de K que contiene al menos una raíz de p.

Demostración. Como $p \notin K$, sabemos que $p \neq 0$ y p no es invertible. Dado que $K[X]$ es un Dominio de Factorización Única (DFU), p es divisible por algún factor irreducible $q \in K[X]$. Es evidente que cualquier raíz de q será automáticamente una raíz de p (pues $p = q \cdot c$). Por tanto, sin pérdida de generalidad, podemos suponer desde el principio que p es **irreducible**.

Al ser p irreducible en el DFU $K[X]$, el ideal generado por él, (p), es un ideal maximal. Definimos el anillo cociente:

$$L := \frac{K[X]}{(p)}$$

Como (p) es maximal, L es un **cuerpo**.

¿Es L una extensión de K? Sí, porque la aplicación natural $K \to K[X]/(p)$ dada por $k \mapsto k + (p)$ es un homomorfismo de cuerpos, y por tanto, inyectivo. Esto nos permite identificar a K con un subcuerpo de L.

Solo falta ver que L contiene una raíz de p. Definimos el elemento $\alpha \in L$ como la clase de equivalencia de la indeterminada X:

$$\alpha = X + (p)$$

Evaluamos el polinomio p (cuyos coeficientes están en K) en este elemento α:

$$p(\alpha) = p(X + (p)) = p(X) + (p)$$

Pero $p(X) \in (p)$, por lo que la clase $p(X) + (p)$ es exactamente la clase del cero en el cociente.

$$p(\alpha) = (p) \equiv 0_L \quad \text{(la clase nula)}$$

Hemos construido un cuerpo L donde α es raíz de p. □

Definición 1.3.1: Polinomio completamente factorizable

Sea $p \in K[X] \setminus K$. Diremos que p es **completamente factorizable** en K si se puede expresar como un producto de polinomios de grado 1 en $K[X]$, es decir:

$$p(X) = a(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n) \quad \text{con } a, \alpha_i \in K$$

En tal caso, las raíces de p son exactamente $\alpha_1, \ldots, \alpha_n$.

Ejemplo 1.3.1: E

l polinomio $X^3 - 1$ factoriza como $(X-1)(X^2+X+1)$. Esta expresión no es completamente factorizable ni en $\mathbb{Q}$ ni en $\mathbb{R}$. Sin embargo, sobre $\mathbb{C}$, es completamente factorizable:

$$X^3 - 1 = (X - 1)\left(X - \frac{-1 + \sqrt{-3}}{2}\right)\left(X - \frac{-1 - \sqrt{-3}}{2}\right)$$

Corolario 1.3.1: Factorización total

Si K es un cuerpo y $p \in K[X] \setminus K$, entonces p es completamente factorizable en alguna extensión de K.

Demostración. Procedemos por inducción sobre el grado de p. Si $\mathrm{gr}(p) = 1$, el polinomio ya está factorizado en el propio K y no hay nada que demostrar.

Por el Teorema de Kronecker, existe una extensión E/K que contiene al menos una raíz de p, digamos α. Por el Teorema del Resto, en el anillo $E[X]$, podemos factorizar p como:

$$p(X) = (X - \alpha)q(X) \quad \text{con } q \in E[X]$$

Como $\operatorname{gr}(q) = \operatorname{gr}(p) - 1$, podemos aplicar la hipótesis de inducción a q: existe una extensión L/E donde q es completamente factorizable. Al ser $p = (X - \alpha)q$ y q descomponer totalmente en L, p también descompone totalmente en L. Dado que L es extensión de E y E es extensión de K, L es una extensión de K. □

1.4. Torres Radicales y Resolubilidad

Definición 1.4.1: Torre Radical y Extensión Radical (Def. 1.7)

Una **torre radical** es una torre de cuerpos $E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$ tal que, para cada $i \geq 1$, existen un entero $n_i \geq 1$ y un elemento $\alpha_i \in E_i$ que cumplen:

$$E_i = E_{i-1}(\alpha_i) \quad \text{y} \quad \alpha_i^{n_i} \in E_{i-1}$$

Diremos que una extensión L/K es **radical** si existe una torre radical $K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = L$.
Una ecuación polinómica $P(X) = 0$ se dice que es **resoluble por radicales** en K si existe una extensión radical L/K tal que P es completamente factorizable en L.

Observación 1.4.1: La analogía de la Torre Radical (.El Edificio")

La definición nos dice que un cuerpo se construye añadiendo raíces de elementos que ya teníamos, paso a paso. Es como un edificio en construcción:

- **Piso 0 (E_0):** Los cimientos. Es nuestro cuerpo base (por ejemplo, $\mathbb{Q}$).
- **El paso radical ($E_i = E_{i-1}(\alpha_i)$):** El piso actual se construye tomando un número $\beta \in E_{i-1}$ que ya existía en el piso de abajo, y añadiendo formalmente su raíz n-ésima $\alpha_i = \sqrt[n_i]{\beta}$.

Ejemplo de Raíces Anidadas: Queremos un cuerpo que contenga a $\sqrt{3 + \sqrt{2}}$. No podemos añadirlo de golpe partiendo de $\mathbb{Q}$.

1. Piso 0: $E_0 = \mathbb{Q}$.
2. Piso 1: Añadimos $\alpha_1 = \sqrt{2}$. Como $\alpha_1^2 = 2 \in E_0$, definimos $E_1 = \mathbb{Q}(\sqrt{2})$.
3. Piso 2: Ahora que tenemos $\sqrt{2}$, consideramos $\beta = 3 + \sqrt{2} \in E_1$. Tomamos $\alpha_2 = \sqrt{\beta}$. Como $\alpha_2^2 \in E_1$, definimos $E_2 = E_1(\alpha_2) = \mathbb{Q}(\sqrt{3 + \sqrt{2}})$.

Esta es la conexión profunda con la Teoría de Galois: la fórmula cuadrática es una torre de altura 1. Las fórmulas de Cardano para el grado 3 requieren torres más altas. Si las soluciones de una ecuación no caben en *ninguna* torre de este tipo (Abel-Ruffini para grado ≥ 5), la ecuación no tiene fórmula resolutiva.

Observación 1.4.2: Notación de homomorfismos de cuerpos y su acción sobre polinomios

Si $\sigma : K \to E$ es un homomorfismo de cuerpos, este induce de forma natural un homomorfismo entre anillos de polinomios $\sigma : K[X] \to E[X]$ simplemente aplicando σ a los coeficientes: $\sigma(a_n X^n + \cdots + a_0) = \sigma(a_n)X^n + \cdots + \sigma(a_0)$.

Lema 1.4.1: Invarianza y Permutación de Raíces (Lema 1.8)

Sean $\sigma : E \to L$ un homomorfismo de cuerpos y $p \in E[X]$.

1. Si α es una raíz de p en E, entonces $\sigma(\alpha)$ es una raíz del polinomio imagen $\sigma(p)$ en L.
2. Si E/K y L/K son extensiones de un cuerpo base K, $p \in K[X]$, y σ es un K-**homomorfismo**, entonces σ se restringe a una aplicación **inyectiva** del conjunto de las raíces de p en E al conjunto de las raíces de p en L.
3. En particular, si $E = L$ (es decir, $\sigma \in \mathrm{Gal}(L/K)$ es un K-automorfismo), entonces esta restricción es una **permutación** (aplicación biyectiva) del conjunto de las raíces de p en L.

Demostración. **Demostración de (a):** Sea $p(X) = p_0 + p_1 X + \cdots + p_n X^n$ con $p_i \in E$. Evaluamos el polinomio transformado $\sigma(p)$ en el elemento transformado $\sigma(\alpha)$:

$$\begin{aligned}(\sigma(p))(\sigma(\alpha)) &= \sigma(p_0) + \sigma(p_1)\sigma(\alpha) + \cdots + \sigma(p_n)\sigma(\alpha)^n \\ &= \sigma(p_0 + p_1\alpha + \cdots + p_n\alpha^n) \quad \text{(por ser } \sigma \text{ homomorfismo)} \\ &= \sigma(p(\alpha))\end{aligned}$$

Como por hipótesis α es raíz, $p(\alpha) = 0$. Y como todo homomorfismo lleva el cero al cero, $\sigma(0) = 0$. Por tanto, $\sigma(\alpha)$ es raíz de $\sigma(p)$.

Demostración de (b) [La Restricción a las Raíces]: El escenario es fundamental: $p \in K[X]$ (los coeficientes están en K) y σ es un K-homomorfismo. ¿Qué significa ser K-homomorfismo? Que fija los elementos de K, es decir, $\sigma(k) = k$ para todo $k \in K$.

Al aplicar σ al polinomio p, como sus coeficientes están en K, estos no cambian:

$$\sigma(p) = \sigma(a_n)X^n + \cdots + \sigma(a_0) = a_n X^n + \cdots + a_0 = p$$

El polinomio es invariante ($\sigma(p) = p$).

Sean R_E y R_L los conjuntos de raíces de p en E y L, respectivamente. Si $\alpha \in R_E$, por el apartado (a), $\sigma(\alpha)$ es raíz de $\sigma(p)$. Pero como $\sigma(p) = p$, resulta que $\sigma(\alpha)$ es raíz de p en L. Es decir, $\sigma(\alpha) \in R_L$.

Así, σ mapea $R_E \to R_L$. ¿Es inyectiva? Sí, es "gratis". Todo homomorfismo de cuerpos es inyectivo en todo su dominio E. Si es inyectivo en un conjunto grande, su restricción a un subconjunto (R_E) también lo es trivialmente.

Demostración de (c) [La Permutación]: Ahora $E = L$, luego σ es un automorfismo de L que fija K. Sea S el conjunto de las raíces de p en L. Por el apartado (b), la restricción de σ nos da una función inyectiva $f : S \to S$.

El argumento de finitud: Un polinomio no nulo de grado n tiene a lo sumo n raíces. Por tanto, el conjunto S es **finito**.

Por teoría básica de conjuntos, toda aplicación inyectiva de un conjunto finito en sí mismo es forzosamente sobreyectiva (y por tanto, biyectiva). *(Intuición: Si tienes 3 sillas y 3 personas que cambian de asiento, y cada persona se sienta en una silla distinta —inyectividad—, es imposible que quede alguna silla vacía —sobreyectividad—).*

Como la aplicación es una biyección del conjunto finito de raíces S en sí mismo, constituye por definición una **permutación** de las raíces de p. □

Lema 1.4.2: Lema de Extensión (Lema 1.9)

Sea $\sigma : K_1 \to K_2$ un homomorfismo de cuerpos y sea $p \in K_1[X]$ un polinomio irreducible. Sean L_1/K_1 y L_2/K_2 dos extensiones de cuerpos y sean $\alpha_1 \in L_1$ y $\alpha_2 \in L_2$ con α_1 una raíz de p.
Entonces, existe un homomorfismo $\hat{\sigma} : K_1(\alpha_1) \to K_2(\alpha_2)$ tal que $\hat{\sigma}|_{K_1} = \sigma$ y $\hat{\sigma}(\alpha_1) = \alpha_2$ **si y solo si** α_2 es una raíz del polinomio imagen $\sigma(p)$.
En tal caso, sólo hay un homomorfismo $\hat{\sigma}$ que satisfaga la condición indicada y, si además σ es un isomorfismo, entonces también $\hat{\sigma}$ es un isomorfismo.

Demostración. ($\Longrightarrow$) Supongamos que existe $\hat{\sigma}$ en las condiciones dadas. Queremos ver que α_2 es raíz de $\sigma(p)$. Como por hipótesis α_1 es raíz de $p \in K_1[X]$, se tiene $p(\alpha_1) = 0$. Aplicando el homomorfismo $\hat{\sigma}$, obtenemos $\hat{\sigma}(p(\alpha_1)) = \hat{\sigma}(0) = 0$. Por el Lema de invarianza de raíces (Lema 1.8), sabemos que aplicar $\hat{\sigma}$ a la evaluación de un polinomio es equivalente a evaluar el polinomio transformado en la raíz transformada:

$$0 = \hat{\sigma}(p(\alpha_1)) = \hat{\sigma}(p)(\hat{\sigma}(\alpha_1))$$

Como $\hat{\sigma}$ extiende a σ sobre K_1, se tiene $\hat{\sigma}(p) = \sigma(p)$. Además, $\hat{\sigma}(\alpha_1) = \alpha_2$. Sustituyendo, obtenemos $0 = \sigma(p)(\alpha_2)$, lo que prueba que α_2 es raíz de $\sigma(p)$.

($\Longleftarrow$) Supongamos que α_2 es raíz de $\sigma(p)$. Vamos a construir $\hat{\sigma}$. Consideramos los homomorfismos de evaluación:

$$\begin{aligned} \delta_{\alpha_1} &: K_1[X] \longrightarrow K_1(\alpha_1), \quad f(X) \mapsto f(\alpha_1) \\ \delta_{\alpha_2} &: K_2[X] \longrightarrow K_2(\alpha_2), \quad g(X) \mapsto g(\alpha_2) \end{aligned}$$

Sabemos (por el Lema 1.4) que, como p es irreducible y α_1 es raíz, el núcleo es $\ker(\delta_{\alpha_1}) = (p)$ y la imagen es $K_1[\alpha_1] = K_1(\alpha_1)$. Esto nos permite definir la aplicación natural:

$$\hat{\sigma} : K_1(\alpha_1) \longrightarrow K_2(\alpha_2)$$

$$\hat{\sigma}(f(\alpha_1)) := \sigma(f)(\alpha_2) \quad \text{para cualquier } f \in K_1[X]$$

1. ¿Está bien definida? (¿Imágenes iguales?) Supongamos que $f(\alpha_1) = g(\alpha_1)$. Entonces $(f - g)(\alpha_1) = 0$, lo que implica que $f - g \in \ker(\delta_{\alpha_1}) = (p)$. Es decir, $f - g = p \cdot h$ para algún $h \in K_1[X]$. Aplicando el homomorfismo inducido por σ:

$$\sigma(f - g) = \sigma(p \cdot h) = \sigma(p)\sigma(h)$$

Evaluamos en α_2:

$$\sigma(f-g)(\alpha_2) = \sigma(p)(\alpha_2)\cdot\sigma(h)(\alpha_2)$$

Como α_2 es raíz de $\sigma(p)$ por hipótesis, el término de la derecha es 0. Luego $\sigma(f-g)(\alpha_2) = 0 \implies \sigma(f)(\alpha_2) - \sigma(g)(\alpha_2) = 0 \implies \sigma(f)(\alpha_2) = \sigma(g)(\alpha_2)$. La aplicación está perfectamente definida, independientemente del representante elegido.

2. ¿Es homomorfismo de cuerpos? Sí, hereda trivialmente las propiedades de los polinomios. Para la suma:

$$\begin{aligned}\hat{\sigma}(f(\alpha_1)+g(\alpha_1)) &= \hat{\sigma}((f+g)(\alpha_1)) = \sigma(f+g)(\alpha_2)\\ &= (\sigma(f)+\sigma(g))(\alpha_2) = \sigma(f)(\alpha_2)+\sigma(g)(\alpha_2)\\ &= \hat{\sigma}(f(\alpha_1))+\hat{\sigma}(g(\alpha_1))\end{aligned}$$

El producto es análogo. Además, verifica las condiciones exigidas: $\hat{\sigma}|_{K_1} = \sigma$ (aplicado a polinomios constantes) y $\hat{\sigma}(\alpha_1) = \hat{\sigma}(X(\alpha_1)) = \sigma(X)(\alpha_2) = \alpha_2$.

3. Unicidad: Supongamos que $\tau : K_1(\alpha_1) \to K_2(\alpha_2)$ es otro homomorfismo con $\tau|_{K_1} = \sigma$ y $\tau(\alpha_1) = \alpha_2$. Cualquier elemento $\beta \in K_1(\alpha_1)$ se escribe como $f(\alpha_1) = f_0 + f_1\alpha_1 + \cdots + f_n\alpha_1^n$ con $f_i \in K_1$.

$$\begin{aligned}\tau(\beta) = \tau(f(\alpha_1)) &= \tau(f_0)+\tau(f_1)\tau(\alpha_1)+\cdots+\tau(f_n)\tau(\alpha_1)^n\\ &= \sigma(f_0)+\sigma(f_1)\alpha_2+\cdots+\sigma(f_n)\alpha_2^n\\ &= \sigma(f)(\alpha_2) = \hat{\sigma}(f(\alpha_1)) = \hat{\sigma}(\beta)\end{aligned}$$

Luego $\tau = \hat{\sigma}$.

4. Es Isomorfismo: Por último, si σ es un isomorfismo, sabemos que $\hat{\sigma}$ es inyectivo (todo homomorfismo de cuerpos lo es). Para la suprayectividad, notemos que $\mathrm{Im}(\hat{\sigma})$ es un subcuerpo de $K_2(\alpha_2)$ que contiene a $\sigma(K_1) = K_2$ y contiene a $\hat{\sigma}(\alpha_1) = \alpha_2$. Como $K_2(\alpha_2)$ es el menor cuerpo que contiene a K_2 y α_2, forzosamente $\mathrm{Im}(\hat{\sigma}) = K_2(\alpha_2)$. Por tanto, $\hat{\sigma}$ es suprayectivo y constituye un isomorfismo. □

Proposición 1.4.1: Isomorfismo de raíces conjugadas

Sea $p \in K[X]$ un polinomio irreducible y sean α, β raíces de p en dos extensiones de K. Entonces, existe un único K-isomorfismo $f : K(\alpha) \xrightarrow{\simeq} K(\beta)$ tal que $f(\alpha) = \beta$.

Demostración. Basta tomar la identidad $\sigma = \mathrm{id}_K$ en el Lema anterior, definiendo $K_1 = K_2 = K$. Como $\sigma(p) = p$, la condición de que β sea raíz de $\sigma(p)$ se cumple trivialmente. El Lema nos garantiza entonces el isomorfismo deseado. □

Observación 1.4.3: Nota: No es superfluo que sea irreducible

La hipótesis de irreducibilidad de p es vital. Si tomamos $p(X) = X(X^2+1) \in \mathbb{Q}[X]$ (que es reducible), tiene como raíces $\alpha = 0$ y $\beta = i$. Los cuerpos generados son $\mathbb{Q}(0) = \mathbb{Q}$ y $\mathbb{Q}(i)$. Evidentemente $\mathbb{Q} \not\simeq \mathbb{Q}(i)$ ya que tienen distinto grado sobre $\mathbb{Q}$ (1 y 2, respectivamente).
Conclusión general: Dado $p \in K[X]$ irreducible, la extensión de K obtenida al adjuntar *cualquier* raíz α de p es esencialmente idéntica al cuerpo cociente genérico $K[X]/(p)$, independientemente del cuerpo "grande"donde hayamos encontrado dicha raíz.

1.5. Extensiones Algebraicas

Definición 1.5.1: Elemento Algebraico y Extensión Algebraica (Def. 1.11)

Dada una extensión L/K y un elemento $\alpha \in L$:

- Se dice que α es **algebraico** sobre K si existe algún polinomio no nulo $p \in K[X]$ tal que $p(\alpha) = 0$.
- En caso contrario, diremos que α es **transcendente** sobre K.

Diremos que la extensión total L/K es una **extensión algebraica** si *todo* elemento $\alpha \in L$ es algebraico sobre K. En caso contrario, diremos que la extensión es transcendente.

Ejemplo 1.5.1: E

n la extensión $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$, el elemento $\sqrt{n}$ es algebraico, ya que es raíz del polinomio $X^2 - n \in \mathbb{Q}[X]$.

Proposición 1.5.1: Caracterización de elementos algebraicos (Prop. 1.12)

Si L/K es una extensión de cuerpos y $\alpha \in L$, entonces las siguientes condiciones son equivalentes:

1. α es algebraico sobre K.
2. El homomorfismo de evaluación $\delta_\alpha : K[X] \to L$ (dado por $p \mapsto p(\alpha)$) **no** es inyectivo.
3. $K[\alpha] = K(\alpha)$.
4. El anillo $K[\alpha]$ es un subcuerpo de L.
5. $K(\alpha)/K$ es una extensión finita (de dimensión vectorial finita).

(La demostración seguirá el esquema de implicaciones lógicas: (1) $\iff$ (2) $\implies$ (3) $\implies$ (4) $\implies$ (2)*, y comprobando la finitud por otro lado).*

Capítulo 2

Cuerpos de Descomposición

2.1. Cuerpos Algebraicamente Cerrados

Recordemos del tema anterior que una extensión de cuerpos es finita si y solo si es una extensión algebraica y finitamente generada. Una consecuencia fundamental del Teorema de Kronecker nos permite caracterizar de múltiples formas aquellos cuerpos en los que todo polinomio tiene solución.

Proposición 2.1.1: Caracterización de Cuerpos Algebraicamente Cerrados (Prop. 2.1)

Las siguientes condiciones son lógicamente equivalentes para un cuerpo K:

1. Todo polinomio no constante con coeficientes en K tiene al menos una raíz en K (esta es la definición estándar de que K es algebraicamente cerrado).

2. Los polinomios irreducibles del anillo $K[X]$ son exactamente los polinomios de grado 1.

3. Todo polinomio no constante de $K[X]$ es completamente factorizable sobre K (se descompone unívocamente en un producto de factores lineales).

4. K contiene un subcuerpo K_0 tal que la extensión K/K_0 es algebraica y todo polinomio de $K_0[X]$ es completamente factorizable en $K[X]$.

5. Si L/K es una extensión algebraica, entonces forzosamente $L = K$ (es decir, K no posee extensiones algebraicas propias).

6. Si L/K es una extensión finita, entonces $L = K$ (es decir, K no posee extensiones finitas propias).

Demostración. Acometemos la demostración mediante un ciclo cerrado de implicaciones lógicas:

(1) $\implies$ (2): Es una consecuencia inmediata. Si existiera un polinomio irreducible de grado $n \geq 2$, por la condición (1) este tendría al menos una raíz $\alpha \in K$. Pero si tiene una raíz en K, por el Teorema del Resto el polinomio sería divisible por $(X - \alpha)$, lo cual contradice frontalmente su irreducibilidad. Por tanto, los únicos irreducibles son los de grado 1.

(2) $\implies$ (3): Como K es un cuerpo, sabemos que el anillo de polinomios $K[X]$ es un Dominio de Factorización Única (DFU). Esto garantiza que cualquier polinomio se descompone de forma única en producto de polinomios irreducibles. Aplicando (2), todos estos factores irreducibles tienen grado 1. Esto significa exactamente que el polinomio original es completamente factorizable.

(3) $\implies$ (4): Es una implicación trivial. Basta con tomar $K_0 = K$. La extensión K/K es trivialmente algebraica (todo elemento es raíz de su polinomio $X - a$) y, por (3), todo polinomio en $K_0[X]$ descompone completamente.

(4) $\implies$ (5): Supongamos que existe un subcuerpo $K_0 \subseteq K$ que cumple la hipótesis (4) y sea L/K una extensión algebraica cualquiera. Como, por hipótesis, la extensión base K/K_0 también es algebraica, la transitividad de las extensiones algebraicas nos asegura que la torre completa L/K_0 es una extensión algebraica.

Sea $\alpha \in L$ un elemento arbitrario. Consideramos su polinomio mínimo sobre el cuerpo base pequeño: $p = \mathrm{Min}_{K_0}(\alpha)$. Por la condición (4), este polinomio se descompone linealmente en $K[X]$, es decir, todas sus raíces residen en K:

$$p(X) = a_0(X - \alpha_1)\cdots(X - \alpha_n) \quad \text{con } \alpha_i \in K$$

Evaluando el polinomio en α, obtenemos:

$$0 = p(\alpha) = a_0(\alpha - \alpha_1)\dots(\alpha - \alpha_n)$$

Al estar trabajando en un dominio de integridad (un cuerpo carece de divisores de cero), forzosamente $\alpha - \alpha_i = 0$ para algún i. Es decir, $\alpha = \alpha_i$. Como sabíamos que $\alpha_i \in K$, deducimos inmediatamente que $\alpha \in K$. Al ser α un elemento arbitrario de L, tenemos que $L \subseteq K$, y por consiguiente $L = K$.

(5) $\implies$ (6): Esta implicación es directa, puesto que toda extensión finita es, por definición, una extensión algebraica.

(6) $\implies$ (1): Supongamos que se verifica (6) y tomemos un polinomio no constante arbitrario $p \in K[X] \setminus K$. Por el Teorema de Kronecker, sabemos que existe una extensión $K(\alpha)/K$ donde α es una raíz de p. Como α es raíz de un polinomio con coeficientes sobre K, α es un elemento algebraico sobre K. Esto implica que la extensión simple $K(\alpha)/K$ es de grado finito. Aplicando ahora nuestra hipótesis (6) a esta extensión finita, concluimos que $K(\alpha) = K$, lo que exige que la raíz α pertenezca a K. $\square$

Ejemplo 2.1.1: Ejemplos de Cuerpos NO Algebraicamente Cerrados

- Los cuerpos $\mathbb{Q}$ y $\mathbb{R}$ no son algebraicamente cerrados, ya que el polinomio $X^2 + 1 \in \mathbb{R}[X]$ carece de raíces en ambos.
- El cuerpo finito $\mathbb{Z}_2$ tampoco lo es. El polinomio $X^2 + X + 1 \in \mathbb{Z}_2[X]$ no se anula ni al evaluar en 0 ni en 1 (de hecho, sus raíces en su cuerpo de descomposición serían complejas de la forma $\frac{-1\pm\sqrt{3}i}{2}$).
- **Ningún cuerpo finito es algebraicamente cerrado.** A modo de demostración para $p \geq 3$ (Ejemplo 2.4): el polinomio $X^{p-1} + 1$ jamás tiene raíces en $\mathbb{Z}_p$. Si tuviese una raíz $\alpha \in \mathbb{Z}_p$, al ser $\alpha \neq 0$ (el cero no lo anula), por el Pequeño Teorema de Fermat se cumpliría invariablemente que $\alpha^{p-1} \equiv 1 \pmod{p}$. Sustituyendo esto en la ecuación del polinomio, tendríamos $1 + 1 \equiv 0 \pmod{p}$, lo que implicaría que p

divide a 2. Esto fuerza a que $p = 2$, contradiciendo nuestra premisa original de que $p \geq 3$.

Teorema 2.1.1: Teorema Fundamental del Álgebra (Teorema 2.2)

El cuerpo de los números complejos $\mathbb{C}$ es algebraicamente cerrado.

(Nota: La demostración analítica de este teorema, basada en la compacidad de los discos en el plano complejo y el principio del módulo mínimo, se omite en este desarrollo puramente algebraico).

2.2. Clausura Algebraica

Una vez establecido empíricamente que no todos los cuerpos son algebraicamente cerrados, surge una de las preguntas fundamentales de la Teoría de Cuerpos: dado un cuerpo cualquiera K, ¿existe siempre un cuerpo algebraicamente cerrado que lo contenga y actúe como su ünuniverso de soluciones¿

Proposición 2.2.1: La clausura relativa hereda la completitud (Prop. 2.3)

Sea L/K una extensión con L algebraicamente cerrado y sea C la clausura algebraica de K en L (es decir, el conjunto de todos los elementos de L que son algebraicos sobre K). Entonces la extensión C/K es algebraica y el cuerpo C es algebraicamente cerrado.

Demostración. Que C/K es una extensión algebraica es una tautología derivada de la propia definición constructiva de C (como vimos en el Corolario 1.17).

Para demostrar que el subcuerpo C es algebraicamente cerrado, tomemos un polinomio no constante $p \in C[X] \setminus C$. Dado que $C \subseteq L$, podemos visualizar p como un polinomio en $L[X]$. Como el cuerpo L es, por hipótesis inicial, algebraicamente cerrado, el polinomio p posee garantizada al menos una raíz $\alpha \in L$.

Al ser α raíz de un polinomio cuyos coeficientes están en C, podemos afirmar con total rigor que α es algebraico sobre C. Por tanto, la extensión simple $C(\alpha)/C$ es una extensión algebraica.

Se nos presenta entonces una torre de extensiones: $K \subseteq C \subseteq C(\alpha)$. Sabemos que $C(\alpha)/C$ es algebraica y que C/K es algebraica. Invocando la propiedad de transitividad (multiplicatividad) de las extensiones algebraicas, la extensión global $C(\alpha)/K$ es también una extensión algebraica.

Esta transitividad implica inexorablemente que todos los elementos del cuerpo $C(\alpha)$ son algebraicos sobre el cuerpo base K. En particular, nuestro elemento α es algebraico sobre K. Pero recordemos que el cuerpo C se definió precisamente como el conjunto máximo de *todos* los elementos de L que son algebraicos sobre K. Por consiguiente, $\alpha \in C$.

Acabamos de demostrar que cualquier polinomio con coeficientes en C tiene una raíz que también pertenece a C. Luego C es algebraicamente cerrado. $\square$

Definición 2.2.1: Clausura Algebraica Absoluta

Una **clausura algebraica** de un cuerpo K es una extensión de K que cumple simultáneamente dos condiciones: es una extensión algebraica y, además, es un cuerpo algebraicamente cerrado.

Observación 2.2.1: Cuidado con la nomenclatura (!)

Es imperativo en el estudio del álgebra distinguir con precisión entre dos conceptos sutilmente diferentes pero a menudo confundidos:

- **Una clausura algebraica de** K: Es una estructura matemática absoluta. Es una extensión que es a la vez algebraica y algebraicamente cerrada.

- **La clausura algebraica de** K **en** L: Es un concepto puramente relativo a una extensión previamente dada L/K. Se define simplemente como el mayor subcuerpo de L formado por elementos algebraicos sobre K. *No tiene por qué ser algebraicamente cerrado* (a menos que el propio universo L del que partimos lo sea, como ha demostrado de forma brillante la Proposición 2.3).

Teorema 2.2.1: Existencia de la Clausura Algebraica (Teorema 2.5)

Todo cuerpo K posee una clausura algebraica.

Teorema 2.2.2: Teorema de Extensión de Homomorfismos (Teorema 2.6)

Sean K y L cuerpos, con L algebraicamente cerrado, y sea $\sigma : K \to L$ un homomorfismo de cuerpos. Si F/K es una extensión algebraica, entonces existe otro homomorfismo de cuerpos $\tau : F \to L$ que extiende a σ (es decir, $\tau|_K = \sigma$).

Demostración. Utilizaremos el **Lema de Zorn**, el cual establece que si un conjunto parcialmente ordenado $(S, \leq)$ es inductivo (toda cadena tiene una cota superior en S), entonces posee al menos un elemento maximal.

Paso 1: Definición del conjunto parcialmente ordenado. Consideremos el conjunto de todas las extensiones parciales de σ. Definimos:

$$\Omega = \{(E, \tau) \mid K \subseteq E \subseteq F \text{ subextensión, y } \tau : E \to L \text{ homomorfismo que extiende a } \sigma\}$$

El conjunto Ω es no vacío ya que, trivialmente, $(K, \sigma) \in \Omega$.

Dotamos a Ω de un orden parcial $\leq$ definido por la relación de "ser extensión de":

$$(E_1, \tau_1) \leq (E_2, \tau_2) \iff E_1 \subseteq E_2 \quad \text{y} \quad \tau_2|_{E_1} = \tau_1$$

Es fácil comprobar que $\leq$ es una relación de orden (reflexiva, antisimétrica y transitiva).

Paso 2: Comprobación de que Ω es inductivo. Sea $\{(E_i, \tau_i)\}_{i \in I}$ una cadena (un subconjunto totalmente ordenado) en Ω. Fabricaremos una cota superior para esta cadena.

Definimos el cuerpo unión $E = \bigcup_{i \in I} E_i$.

- *¿Es E un cuerpo?* Sí. Sean $\alpha, \beta \in E$. Por definición de unión, existen índices $i, j \in I$ tales que $\alpha \in E_i$ y $\beta \in E_j$. Al ser una cadena, podemos suponer sin pérdida de generalidad que

$E_i \subseteq E_j$. Por tanto, $\alpha, \beta \in E_j$. Como E_j es un cuerpo, $\alpha + \beta \in E_j \subseteq E$, $\alpha \cdot \beta \in E_j \subseteq E$, y los inversos también residen en $E_j \subseteq E$. Luego E es un subcuerpo de F.

Definimos ahora la aplicación $\tau : E \to L$. Si $\alpha \in E$, existe algún E_i tal que $\alpha \in E_i$; definimos $\tau(\alpha) = \tau_i(\alpha)$.

- *¿Está bien definida?* Supongamos que α también pertenece a otro E_j. Como es una cadena, supongamos $E_i \subseteq E_j$. Por la relación de orden, $\tau_j|_{E_i} = \tau_i$, lo que implica que $\tau_j(\alpha) = \tau_i(\alpha)$. La definición es consistente.
- *¿Es homomorfismo?* Claramente sí, hereda la linealidad y multiplicatividad de los τ_i al operar siempre en un E_i lo suficientemente grande que contenga a los operandos.

Por construcción, τ extiende a σ (ya que cada τ_i lo hace) y (E, τ) es una cota superior de la cadena. Por tanto, Ω es inductivo.

Paso 3: Aplicación del Lema de Zorn y maximalidad. Por el Lema de Zorn, Ω posee un elemento maximal, al que llamaremos (E, τ). Por pertenecer a Ω, sabemos que $E \subseteq F$.

¿Se tiene que $E = F$? Lo demostraremos por reducción al absurdo. Supongamos que $E \subsetneq F$. Entonces existe un elemento $\alpha \in F \setminus E$. Tenemos la torre de cuerpos: $K \subseteq E \subsetneq E(\alpha) \subseteq F$.

Como la extensión global F/K es algebraica, el elemento α es algebraico sobre K, y por consiguiente, también es algebraico sobre E. Consideremos su polinomio mínimo $p = \mathrm{Min}_E(\alpha) \in E[X]$. (Es un polinomio irreducible tal que $p(\alpha) = 0$).

Aplicamos el homomorfismo τ a los coeficientes de p para obtener un nuevo polinomio $\tau(p) \in \tau(E)[X] \subseteq L[X]$. Como el cuerpo de llegada L es, por hipótesis, **algebraicamente cerrado**, el polinomio $\tau(p)$ tiene obligatoriamente al menos una raíz $\beta \in L$.

Aquí entra en juego el **Lema de Extensión (Lema 1.9)**. Como p es irreducible sobre E y β es raíz de $\tau(p)$ en L, existe un homomorfismo $\tau' : E(\alpha) \to L$ tal que:

1. $\tau'|_E = \tau$ (extiende a τ).
2. $\tau'(\alpha) = \beta$ (envía la raíz α a la raíz β).

Pero esto significa que el par $(E(\alpha), \tau')$ pertenece a Ω y, además, $(E, \tau) \leq (E(\alpha), \tau')$ con $E \subsetneq E(\alpha)$. Esto contradice flagrantemente que (E, τ) era un elemento maximal de Ω.

La suposición de que $E \subsetneq F$ debe ser falsa. Concluimos entonces que $E = F$, y por tanto, el homomorfismo maximal τ está definido sobre todo F y extiende a σ, completando la demostración. $\square$

Observación 2.2.2: Aclaración intuitiva del Teorema

Intuitivamente, este teorema nos dice que si tenemos un homomorfismo hacia un cuerpo algebraicamente cerrado (L), y el cuerpo de partida crece de manera exclusivamente ALGEBRAICA (pasando de K a F), el homomorfismo también puede crecer (extenderse) para cubrir este nuevo dominio sin romperse, gracias a que el cuerpo de llegada tiene espacio de sobra (raíces) para acomodar a los nuevos elementos.

El primer corolario importante de este teorema muestra que la clausura algebraica de un cuerpo es única salvo isomorfismos. Gracias a esto, a partir de ahora podemos usar el artículo definido y hablar de *LA* clausura algebraica de un cuerpo, en lugar de *ϋna"* clausura.

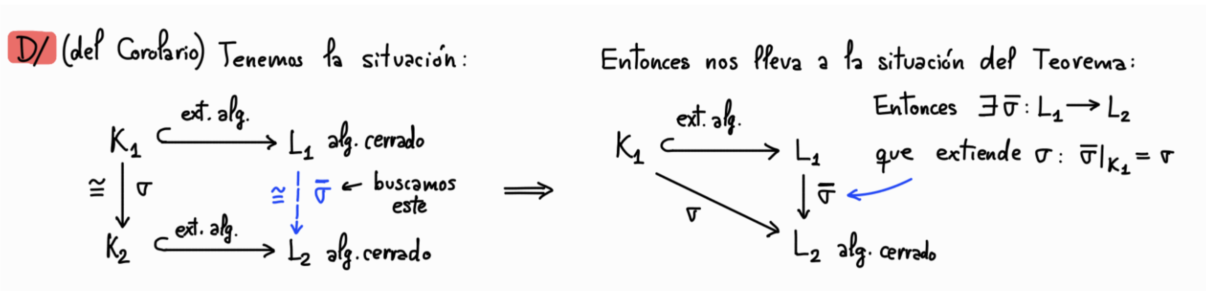
Corolario 2.2.1: Unicidad de la clausura algebraica (Corolario 2.7)

La clausura algebraica de un cuerpo es única salvo isomorfismos.
Formalmente: Si $\sigma : K_1 \to K_2$ es un isomorfismo de cuerpos y L_1, L_2 son clausuras algebraicas de K_1 y K_2 respectivamente, entonces existe un isomorfismo global $\overline{\sigma} : L_1 \to L_2$ que extiende a σ (es decir, $\overline{\sigma}|_{K_1} = \sigma$).

Observación 2.2.3: Estrategia general para la unicidad

La forma habitual de demostrar la unicidad es: si se tiene un cuerpo con dos clausuras, encontrar un isomorfismo entre ellas. Este Corolario 2.7 es una forma de generalizarlo, encontrando un isomorfismo entre las clausuras de dos cuerpos que ya son isomorfos previamente ($\sigma : K_1 \xrightarrow{\cong} K_2$).

Continuación de la demostración del Corolario 2.7. Tenemos la siguiente situación inicial con dos cuerpos isomorfos y sus respectivas clausuras algebraicas:



Esto nos lleva exactamente a la hipótesis del **Teorema 2.6** (Teorema de Extensión). Si consideramos $\sigma : K_1 \to L_2$ (componiendo con la inclusión $K_2 \hookrightarrow L_2$), como L_1/K_1 es algebraica y L_2 es algebraicamente cerrado, el teorema garantiza que:

$$\exists \overline{\sigma} : L_1 \longrightarrow L_2 \quad \text{que extiende a } \sigma \text{ (es decir, } \overline{\sigma}|_{K_1} = \sigma)$$

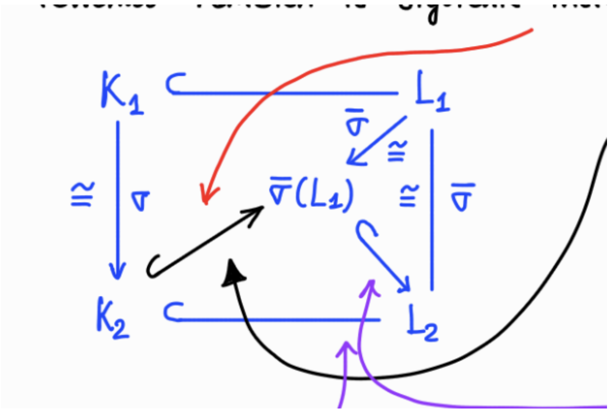
Faltaría ver que este $\overline{\sigma}$ es, de hecho, un isomorfismo. Como todo homomorfismo entre cuerpos es inyectivo, solo necesitamos demostrar la **suprayectividad**, es decir, que $\overline{\sigma}(L_1) = L_2$.

Al ser $\overline{\sigma}$ inyectivo, establece un isomorfismo entre L_1 y su imagen: $L_1 \cong \overline{\sigma}(L_1)$. Como L_1 es algebraicamente cerrado y esta propiedad se conserva por isomorfismos, deducimos que $\overline{\sigma}(L_1)$ **es algebraicamente cerrado**.

Veamos ahora la inclusión del cuerpo base. Sabemos que $K_2 \hookrightarrow L_2$. Dado un elemento cualquiera $\alpha \in K_2$, como $\sigma : K_1 \to K_2$ es isomorfismo (y por tanto biyectiva), existe $\sigma^{-1}(\alpha) \in K_1 \subseteq L_1$. Al aplicar $\overline{\sigma}$ a este elemento, y recordando que $\overline{\sigma}$ coincide con σ sobre K_1:

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

Como $\sigma^{-1}(\alpha) \in L_1$, su imagen α pertenece a $\overline{\sigma}(L_1)$. Esto demuestra que $K_2 \subseteq \overline{\sigma}(L_1)$.



Utilizando la definición, como L_2 es una extensión algebraica de K_2, y $K_2 \subseteq \overline{\sigma}(L_1) \subseteq L_2$, la extensión $L_2/\overline{\sigma}(L_1)$ también es algebraica. Pero hemos demostrado que $\overline{\sigma}(L_1)$ es algebraicamente cerrado, y los cuerpos algebraicamente cerrados no tienen extensiones algebraicas propias (Prop. 2.1 (5)). Por consiguiente, forzosamente $\overline{\sigma}(L_1) = L_2$.

Al ser suprayectiva e inyectiva, $\overline{\sigma}$ es el isomorfismo buscado. □ □

Observación 2.2.4: Unicidad absoluta

De aquí deducimos que LA clausura algebraica de un cuerpo K es única salvo isomorfismos simplemente tomando en este corolario $K_1 = K_2 = K$ y $\sigma = \mathrm{id}_K$.

2.3. Cuerpos de Descomposición (CD) y Extensiones Normales

Definición 2.3.1: Cuerpo de Descomposición

Sean K un cuerpo y $\mathcal{P}$ un conjunto de polinomios no constantes de $K[X]$ (es decir, $\mathcal{P} \subseteq K[X] \setminus K$).
Se llama **cuerpo de descomposición (CD)** de $\mathcal{P}$ sobre K a un cuerpo de la forma $K(S)$, donde:

$$S = \{\text{todas las raíces de todos los polinomios de } \mathcal{P} \text{ en una clausura algebraica de } K\}$$

Observemos que siempre se cumple la torre: $K \subseteq K(S) \subseteq \overline{K}$. Se tendrá la igualdad $K(S) = \overline{K}$ cuando la familia $\mathcal{P}$ contenga a todos los polinomios de $K[X]$.

Observación 2.3.1: Aclaración intuitiva

Claramente, todos los polinomios de $\mathcal{P}$ tendrán sus raíces en la clausura algebraica $\overline{K}$ (pues es el universo donde todo factoriza). El cuerpo de descomposición busca tener *todas* las raíces necesarias para factorizar $\mathcal{P}$, pero construyendo el cuerpo más pequeño posible, "sin que sobre mucho". Lo habitual en la práctica es aplicarlo a un único polinomio $p \in K[X]$.

Proposición 2.3.1: Isomorfismo de Cuerpos de Descomposición (Prop. 2.9)

Sea $\sigma : K_1 \longrightarrow K_2$ un isomorfismo de cuerpos. Sean $\mathcal{P}_1 \subseteq K_1[X] \setminus K_1$ una familia de polinomios y $\mathcal{P}_2 = \{\sigma(p) : p \in \mathcal{P}_1\}$ la familia imagen en $K_2[X]$.
Si L_1 es un cuerpo de descomposición de $\mathcal{P}_1$ sobre K_1, y L_2 es un cuerpo de descomposición de $\mathcal{P}_2$ sobre K_2, entonces existe un isomorfismo $\overline{\sigma} : L_1 \longrightarrow L_2$ que extiende a σ.

Demostración. Sean $\overline{K_1}$ y $\overline{K_2}$ las clausuras algebraicas de K_1 y K_2 respectivamente. Por definición de cuerpo de descomposición, podemos escribir $L_i = K_i(S_i)$ dentro de $\overline{K_i}$ para $i = 1, 2$, donde S_i es el conjunto de las raíces de los polinomios de $\mathcal{P}_i$.

Estrategia de la demostración: "Subir al cielo para bajar a la tierra" El problema es que construir un isomorfismo directamente entre L_1 y L_2 .ª ciegas.ᵉˢ difícil. La estrategia matemática estándar aquí es:

1. **Subir:** Irnos a las Clausuras Algebraicas ($\overline{K_1}$ y $\overline{K_2}$), que son cuerpos enormes donde sabemos que todas las raíces existen.
2. **Conectar:** Usar el Teorema anterior (Corolario 2.7) para conectar esas dos clausuras mediante un isomorfismo global.
3. **Restringir:** Demostrar que, al restringir la acción de ese isomorfismo a las raíces que nos interesan (S_1), caemos exactamente en las raíces del otro lado (S_2), conectando así L_1 con L_2.

Paso 1 y 2 (Subir y Conectar): Por el Corolario 2.7, sabemos que existe un isomorfismo $\overline{\sigma} : \overline{K_1} \longrightarrow \overline{K_2}$ que extiende a σ.

Paso 3 (Restringir): Tomemos una raíz cualquiera $s \in S_1$. Por definición, existe un polinomio $p \in \mathcal{P}_1$ tal que $p(s) = 0$. Aplicando el **Lema 1.8** (que asegura que los homomorfismos envían raíces de p a raíces de $\sigma(p)$), deducimos que $\overline{\sigma}(s)$ será raíz del polinomio imagen $\overline{\sigma}(p) = \sigma(p)$. Como $\sigma(p) \in \mathcal{P}_2$, cualquier raíz suya pertenece a S_2. Por tanto, $\overline{\sigma}(s) \in S_2$. Esto demuestra la inclusión: $\overline{\sigma}(S_1) \subseteq S_2$.

Con un razonamiento completamente análogo (usando el isomorfismo inverso σ^{-1} y subiendo desde $\overline{K_2}$ hasta $\overline{K_1}$), obtenemos que $\overline{\sigma}^{-1}(S_2) \subseteq S_1$. La doble inclusión nos garantiza que las raíces se biyectan perfectamente: $\overline{\sigma}(S_1) = S_2$.

Finalmente, evaluamos la imagen del cuerpo de descomposición L_1:

$$\overline{\sigma}(L_1) = \overline{\sigma}(K_1(S_1)) = \overline{\sigma}(K_1)(\overline{\sigma}(S_1))$$

Como $\overline{\sigma}$ extiende a σ, $\overline{\sigma}(K_1) = K_2$. Y como acabamos de probar, $\overline{\sigma}(S_1) = S_2$. Sustituyendo:

$$\overline{\sigma}(L_1) = K_2(S_2) = L_2$$

Al restringir el isomorfismo global $\overline{\sigma}$ al subcuerpo L_1, obtenemos una aplicación suprayectiva sobre L_2. Al ser la restricción de un isomorfismo, conserva la inyectividad. Por tanto, hemos hallado una aplicación biyectiva que es isomorfismo de cuerpos entre L_1 y L_2 y que extiende a σ. □

Corolario 2.3.1: Unicidad del cuerpo de descomposición

Si $\mathcal{P} \subseteq K[X] \setminus K$, todos los cuerpos de descomposición de $\mathcal{P}$ sobre un mismo cuerpo base K son K-isomorfos entre sí.

Demostración. Basta con aplicar la Proposición 2.9 tomando $K_1 = K_2 = K$ y como isomorfismo base la identidad $\sigma = \mathrm{id}_K$. El isomorfismo resultante entre los cuerpos de descomposición fijará los elementos de K, siendo por tanto un K-isomorfismo. $\square$

Observación 2.3.2: El artículo definido en el Cuerpo de Descomposición

A partir de ahora, gracias al teorema de unicidad salvo isomorfismos, hablaremos de **EL** cuerpo de descomposición (y no *un* cuerpo de descomposición).
Además, el cuerpo de descomposición realmente solo tendrá sentido para un único polinomio o para un conjunto infinito de ellos. ¿Por qué?

1. Si $\mathcal{P} = \{p\}$, hablamos simplemente del C.D. "del polinomio p".
2. Si tenemos un conjunto finito de polinomios $\mathcal{P} = \{p_1, p_2, \ldots, p_r\}$, podemos tomar su producto $p = p_1 \cdot p_2 \cdots p_r$. El conjunto de las raíces de todos los p_i es exactamente el conjunto de las raíces del polinomio producto p.

Luego, la familia finita $\mathcal{P}$ tiene exactamente el mismo cuerpo de descomposición que el polinomio único p.

Ejemplos de Cuerpos de Descomposición

Vamos a calcular los cuerpos de descomposición de varios polinomios sobre $\mathbb{Q}$. Recordemos que si un cuerpo contiene a un elemento (como $\sqrt{2}$), por clausura de las operaciones de cuerpo, también contiene a su opuesto ($-\sqrt{2}$).

Ejemplo 2.3.1: Cálculo de Cuerpos de Descomposición sobre $\mathbb{Q}$

1. **Polinomios cuadráticos puros:**
   - El C.D. de $X^2 - 2$ es $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$.
   - El C.D. de $X^2 + 1$ es $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$.
   - El C.D. de $X^2 + 4$ es $\mathbb{Q}(\sqrt{-4}, -\sqrt{-4}) = \mathbb{Q}(2i, -2i)$. Como $\frac{1}{2} \in \mathbb{Q}$, el cuerpo absorbe las constantes racionales: $\mathbb{Q}(2i) = \mathbb{Q}(i)$.
   - De manera general, el C.D. de $X^2 - q$ (con $q \in \mathbb{Q}$) es $\mathbb{Q}(\sqrt{q})$.
2. **El polinomio $X^3 - 1$:** Factoriza como $X^3 - 1 = (X-1)(X^2+X+1)$. Las raíces son 1 y las complejas $\omega, \overline{\omega} = \frac{-1\pm\sqrt{-3}}{2} = \frac{-1\pm\sqrt{3}i}{2}$. El C.D. será $\mathbb{Q}(1, \omega, \overline{\omega})$. Como $1 \in \mathbb{Q}$ y $\overline{\omega} = \omega^{-1} = \omega^2$, basta con adjuntar ω. El C.D. es $\mathbb{Q}(\omega) = \{a + b\omega \mid a, b \in \mathbb{Q}\}$.
3. **El polinomio $X^3 - 2$:** Sus tres raíces en $\mathbb{C}$ son $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, y $\sqrt[3]{2}\omega^2$. El C.D. será $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$. Notemos que adjuntando la raíz real y ω, generamos todas las demás multiplicando. Además, $\omega = \frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}$, por lo que ω pertenece al cuerpo. Por

tanto, el C.D. se simplifica a $\mathbb{Q}(\sqrt[3]{2}, \omega)$. De forma análoga, para cualquier $a \in \mathbb{Q}$, el C.D. de $X^3 - a$ es $\mathbb{Q}(\sqrt[3]{a}, \omega)$.

4. **El polinomio general $X^n - 1$:** Las raíces son $\xi_n^k = e^{\frac{2\pi i k}{n}}$ para $k = 0, \dots, n-1$. Las que tienen orden multiplicativo exacto n se llaman raíces primitivas. El C.D. es $\mathbb{Q}(1, \xi_n, \xi_n^2, \dots, \xi_n^{n-1}) = \mathbb{Q}(\xi_n)$. (Las demás son simplemente potencias del generador).

5. **El binomio $X^n - a$ ($a \in \mathbb{Q}$):** Las raíces son de la forma $\sqrt[n]{a} \cdot \xi_n^k$. El C.D. requiere tanto la raíz real principal como las raíces de la unidad que rotan.esa magnitud en el plano complejo. El C.D. es $\mathbb{Q}(\sqrt[n]{a}, \xi_n)$.

6. **El polinomio $X^6 - 1$:** Hay 6 raíces, pero no hace falta cogerlas todas; con adjuntar una primitiva es suficiente. Tomamos $\xi_6 = e^{\frac{2\pi i}{6}} = \frac{1}{2} + \frac{\sqrt{3}}{2} i$. El C.D. es $\mathbb{Q}(\xi_6) = \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\sqrt{-3})$. El grado de la extensión es $[\mathbb{Q}(\xi_6) : \mathbb{Q}] = 2$. (Nota: $X^6 - 1 = (X^3 - 1)(X^3 + 1) = (X - 1)(X^2 + X + 1)(X + 1)(X^2 - X + 1)$).

7. **Cálculo del grado para $X^6 - 2$:** Las raíces son $\sqrt[6]{2}\xi_6^k$. Por el caso general visto antes, el C.D. es $\mathbb{Q}(\sqrt[6]{2}, \xi_6)$. Para calcular el grado $[\mathbb{Q}(\sqrt[6]{2}, \xi_6) : \mathbb{Q}]$, consideramos la torre de extensiones: El grado inferior es 6 porque el polinomio mínimo de $\sqrt[6]{2}$ sobre $\mathbb{Q}$ es $X^6 - 2$, el cual es irreducible por el Criterio de Eisenstein (con el primo $p = 2$). El grado superior m es como mucho 2, porque ξ_6 es raíz de $X^2 - X + 1$ (cuyos coeficientes están trivialmente en $\mathbb{Q}(\sqrt[6]{2})$). ¿Podría ser $m = 1$? Si $m = 1$, entonces $\xi_6 \in \mathbb{Q}(\sqrt[6]{2})$. Pero $\mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{R}$ (es un cuerpo puramente real), mientras que $\xi_6 \in \mathbb{C} \setminus \mathbb{R}$. Por tanto, $\xi_6 \notin \mathbb{Q}(\sqrt[6]{2})$. Esto fuerza a que $m = 2$. El grado total de la extensión es:
$$[\mathbb{Q}(\sqrt[6]{2}, \xi_6) : \mathbb{Q}] = 6 \cdot 2 = 12$$

2.4. Extensiones Normales

Definición 2.4.1: Extensión Normal

Una extensión de cuerpos L/K se dice que es **normal** si satisface cualquiera de las condiciones equivalentes del siguiente teorema.

Teorema 2.4.1: Caracterización de Extensiones Normales (Teorema 2.11)

Las siguientes afirmaciones son lógicamente equivalentes para una extensión L/K:

1. L es el cuerpo de descomposición sobre K de una familia de polinomios no constantes con coeficientes en K.

2. L/K es algebraica y, para toda clausura algebraica F de L y todo K-homomorfismo $\sigma : L \longrightarrow F$, se verifica que $\sigma(L) = L$ (es decir, σ es un endomorfismo de L, $\sigma \in \mathrm{Gal}(L/K)$).

3. L/K es algebraica y existe *una* clausura algebraica F de L tal que todo K-homomorfismo $\sigma : L \longrightarrow F$ cumple que $\sigma(L) \subseteq L$.

4. L/K es algebraica y, para todo $\alpha \in L$, su polinomio mínimo $\mathrm{Min}_K(\alpha)$ factoriza completamente en L.

5. L/K es algebraica y todo polinomio irreducible de $K[X]$ que tenga *al menos una* raíz en L, factoriza completamente en L (es decir, "si tenemos una raíz, las tenemos todas").

Demostración. Demostramos las equivalencias mediante un ciclo de implicaciones lógicas:

(1) $\implies$ (2): Supongamos que L es el C.D. de una familia $\mathcal{P} \subseteq K[X] \setminus K$. Sea F la clausura algebraica de L y $\sigma : L \longrightarrow F$ un K-homomorfismo de cuerpos. Por definición de C.D., $L = K(S)$, siendo $S = \{\text{Raíces de los polinomios de } \mathcal{P}\}$. Si tomamos un elemento $\alpha \in S$, α es raíz de un cierto polinomio $p \in \mathcal{P}$. Por el Lema 1.8 (invarianza de raíces bajo homomorfismos), $\sigma(\alpha)$ es raíz del polinomio transformado $\sigma(p)$. Pero σ es un K-homomorfismo (fija los elementos de K), y como p tiene coeficientes en K, resulta que $\sigma(p) = p$. Por tanto, $\sigma(\alpha)$ sigue siendo raíz de p, lo que implica que $\sigma(\alpha) \in S$. Esto demuestra que σ envía el conjunto generador S dentro de sí mismo: $\sigma(S) \subseteq S$. Como los homomorfismos son inyectivos y preservan la estructura algebraica:

$$\sigma(L) = \sigma(K(S)) = K(\sigma(S)) \subseteq K(S) = L$$

(De hecho, como S es invariante y la aplicación es inyectiva sobre las raíces de cada polinomio que son conjuntos finitos, permuta las raíces, obligando a que $\sigma(S) = S$ y por tanto $\sigma(L) = L$). Que la extensión es algebraica es obvio, pues $L = K(S)$ está generada por raíces de polinomios.

(2) $\implies$ (3): Es una implicación lógica trivial. Si la propiedad (2) se cumple para *toda* clausura algebraica y garantiza la igualdad $\sigma(L) = L$, entonces en particular existe *alguna* clausura algebraica donde se cumple la inclusión $\sigma(L) \subseteq L$.

(3) $\implies$ (4): Objetivo: Queremos demostrar que L/K es algebraica y que, para todo $\alpha \in L$, el polinomio $p = \mathrm{Min}_K(\alpha)$ factoriza completamente en L.

Como $K \subseteq L \subseteq F$, podemos considerar p como un polinomio en $F[X]$. Dado que F es una clausura algebraica y por tanto algebraicamente cerrado, el polinomio p factoriza completamente en F (por la Proposición 2.1):

$$p(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) \quad \text{con } \alpha_i \in F$$

A cada raíz α_i vamos a aplicarle la **Proposición 2.10**:

> *Proposición 2.10:* Sea $p \in K[X]$ irreducible (el polinomio mínimo lo es por construcción) y sean α, β raíces de p en dos extensiones de K (pueden no ser las mismas extensiones de K). Entonces, existe un único K-isomorfismo $f : K(\alpha) \xrightarrow{\simeq} K(\beta)$ tal que $f(\alpha) = \beta$.

Aplicando este resultado, deducimos que $K(\alpha) \simeq K(\alpha_i)$ para todo $i \in \{1, \dots, n\}$. Es decir, existe un K-isomorfismo $\tau_i : K(\alpha) \to K(\alpha_i)$ que cumple $\tau_i(\alpha) = \alpha_i$. Como $\alpha_i \in F$, deducimos que el cuerpo generado $K(\alpha_i)$ está contenido en F. Esto nos permite definir el siguiente homomorfismo bien compuesto hacia F: A continuación, aplicamos la siguiente proposición conocida:

> *Teorema 2.6:* Si $\sigma : K \to L$ es un homomorfismo de cuerpos con L algebraicamente cerrado y F/K una extensión algebraica, entonces existe otro homomorfismo de cuerpos $\tau : F \to L$ que extiende a σ.

Adaptación a nuestro contexto: Tomamos como homomorfismo base a $\tau : K(\alpha) \to F$. Sabemos que la extensión $L/K(\alpha)$ es algebraica porque $K \subseteq K(\alpha) \subseteq L$ y la extensión global L/K es algebraica por hipótesis. Como F es algebraicamente cerrado, el teorema nos garantiza que existe una extensión del homomorfismo a todo L. Es decir, $\exists \overline{\tau} : L \to F$ que extiende a τ. (Para simplificar la notación, la llamaremos simplemente τ).

Evaluamos el elemento α bajo este homomorfismo:

$$\tau(\alpha) = (i \circ \tau_i)(\alpha) = i(\tau_i(\alpha)) = i(\alpha_i) = \alpha_i$$

Ahora bien, por la hipótesis (3), todo K-homomorfismo de L en su clausura F cumple que $\tau(L) = L$. (Basta con que $\tau(L) \subseteq L$). Como $\alpha \in L$, su imagen debe pertenecer a L:

$$\alpha \in L \implies \tau(\alpha) \in L \implies \alpha_i \in L$$

Aplicando este mismo razonamiento sistemáticamente a todos los índices $i \in \{1, \dots, n\}$, concluimos que $\alpha_i \in L \ \ \forall i$. Por consiguiente, el polinomio $p = \mathrm{Min}_K(\alpha)$ factoriza completamente dentro de L.

(4) $\implies$ (5): Es inmediato. Sea $p \in K[X]$ un polinomio irreducible que tiene una raíz $\alpha \in L$. Al ser irreducible y mónico (salvo constante multiplicativa), p coincide con $\mathrm{Min}_K(\alpha)$. Por la hipótesis (4), $\mathrm{Min}_K(\alpha)$ factoriza completamente en L. Luego p factoriza completamente en L.

(5) $\implies$ (1): Si asumimos (5), afirmamos que L es el cuerpo de descomposición sobre K de la familia de polinomios irreducibles que tienen raíces en L. Formalmente:

$$\mathcal{P} = \{\mathrm{Min}_K(\alpha) \mid \alpha \in L\}$$

Como cada $\alpha \in L$ aporta su polinomio mínimo, todas las raíces necesarias para generar L están contempladas, y por hipótesis (5), todos estos polinomios factorizan completamente sin necesidad de "salir"de L. □

Ejemplos de Extensiones Normales

Ejemplo 2.4.1: Extensiones cuadráticas simples

Cualquier extensión de la forma $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ es normal, ya que es el cuerpo de descomposición del polinomio $X^2 - q$.

Ejemplo 2.4.2: ¡TODA extensión de grado 2 es normal!

Si L/K es una extensión de grado 2 (con $\operatorname{car}(K) \neq 2$), siempre es normal y su grupo de Galois tiene exactamente orden 2.
Desarrollo riguroso: Sea $\alpha \in L \setminus K$. Entonces la extensión generada es $L = K(\alpha)$. Al ser el grado de la extensión 2, el polinomio mínimo $p = \operatorname{Min}_K(\alpha)$ tiene obligatoriamente grado 2. Pongamos $p(X) = X^2 + aX + b$. Como la característica no es 2, podemos çompletar el cuadrado.ªlgebraicamente:

$$p(X) = \left(X + \frac{a}{2}\right)^2 + b - \frac{a^2}{4}$$

Definimos un nuevo generador $\beta = \alpha + \frac{a}{2}$ y una constante $c = \frac{a^2}{4} - b \in K$. El polinomio mínimo de β es $q(X) = X^2 - c$, y se cumple que $L = K(\alpha) = K(\beta) = K(\sqrt{c})$.
Como las raíces de $q(X)$ son $\pm\beta$, vemos que al contener una raíz (β), la otra raíz $(-\beta)$ es simplemente el elemento opuesto y, por axiomas de cuerpo, también pertenece a L. Por tanto, $\operatorname{Min}_K(\beta)$ (y en consecuencia $\operatorname{Min}_K(\alpha)$) es completamente factorizable en L. Como el cuerpo L se construye precisamente al añadir todas las raíces de este polinomio, L es el cuerpo de descomposición de $\operatorname{Min}_K(\alpha)$ sobre K. Por el Teorema 2.11(1), la extensión L/K es normal.
El Grupo de Galois: Cualquier K-automorfismo $\sigma \in \operatorname{Gal}(L/K)$ debe enviar β a otra raíz de su polinomio mínimo. Las únicas opciones teóricas son $\sigma(\beta) = \beta$ (la identidad) y $\sigma(\beta) = -\beta$ (la conjugación). Para garantizar que existen exactamente dos automorfismos, debemos ver que ambas opciones generan automorfismos distintos y bien definidos:

- Son distintos: como $\operatorname{car}(K) \neq 2$ y $\beta \notin K \implies \beta \neq 0$, se cumple que $2\beta \neq 0 \implies \beta \neq -\beta$.
- Son válidos: Al ser $X^2 - c$ irreducible y tener raíces simples (es separable al ser característica $\neq 2$), la teoría elemental asegura que, por cada raíz en el cuerpo de descomposición, existe un automorfismo que envía el generador a dicha raíz.

En particular, $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ tiene orden 2 y está formado exclusivamente por la aplicación identidad y la conjugación compleja.

Ejemplo 2.4.3:

Consideremos la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. El polinomio mínimo del generador es $\operatorname{Min}_{\mathbb{Q}}(\sqrt[3]{2}) = X^3 - 2$. Sus raíces en $\mathbb{C}$ son $\alpha, \alpha\xi_3, \alpha\xi_3^2$ (donde $\alpha = \sqrt[3]{2}$ es real).
Sin embargo, en el cuerpo $L = \mathbb{Q}(\sqrt[3]{2})$ solamente está la raíz real α. Las otras dos raíces son complejas y no pertenecen a L. Como el polinomio irreducible $\operatorname{Min}_{\mathbb{Q}}(\alpha)$ tiene una raíz en L pero no factoriza completamente en L, la extensión no es normal.

Corolario 2.4.1: Corolario 2.12

Una extensión finitamente generada es normal si y solo si es el cuerpo de descomposición de un polinomio de $K[X]$.

Demostración del Corolario 2.12. $\Longleftarrow$: Es la propia definición geométrica (por la equivalencia (1) del Teorema Anterior).

$\Longrightarrow$: Supongamos que L/K es una extensión normal y finitamente generada. Al ser finitamente generada, podemos escribir $L = K(\alpha_1, \ldots, \alpha_n)$ con $\alpha_i \in L$ para todo $i = 1, \ldots, n$.

Al ser L/K normal, la caracterización (4) del Teorema Anterior nos garantiza que cada polinomio mínimo $p_i(X) = \mathrm{Min}_K(\alpha_i)$ factoriza completamente en L (es decir, todas las raíces de cada $p_i(X)$ están dentro de L).

Definimos el polinomio producto $P(X) = \prod_{i=1}^{n} p_i(X)$. ¿Es L el cuerpo de descomposición de este polinomio $P(X)$? Sea E el cuerpo de descomposición de $P(X)$. Vamos a demostrar la doble inclusión para ver que $L = E$.

- $\subseteq$: Como E es el cuerpo de descomposición, contiene a todas las raíces de $P(X)$. En particular, contiene a todos los generadores $\alpha_i \in E$. Además, $K \subseteq E$. Como $L = K(\alpha_1, \ldots, \alpha_n)$ es el menor cuerpo que contiene a K y a los α_i, se deduce que $L \subseteq E$.
- $\supseteq$: Por otra parte, hemos visto que todas las raíces de $P(X)$ (que son la unión de las raíces de los p_i) viven en L. El cuerpo de descomposición E está generado precisamente por esas raíces: $E = K(\text{raíces de } P)$. Como $K \subseteq L$ y las raíces están en L, el cuerpo generado E está contenido en L, es decir $E \subseteq L$.

Por la doble inclusión, concluimos que $E = L$, como queríamos demostrar. $\square$

Corolario 2.4.2: Corolario 2.13

Si L es una clausura algebraica de K, entonces la extensión L/K es normal.

Demostración: Trivial aplicando la equivalencia (3) del Teorema de normalidad y tomando $L = F$.

Ejemplo 2.4.4: Falta de transitividad de la normalidad

Consideremos $L = \mathbb{Q}(\sqrt[4]{2})$. El polinomio mínimo es $\mathrm{Min}_{\mathbb{Q}}(\sqrt[4]{2}) = X^4 - 2$, cuyas 4 raíces son $\pm\sqrt[4]{2}$ y $\pm i\sqrt[4]{2}$. Entonces L solo contiene 2 de las 4 raíces (las reales). Por lo que $L/\mathbb{Q}$ **no** es normal.
Sin embargo, podemos construir la siguiente torre de cuerpos:

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

Ambas subextensiones (la superior $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ y la inferior $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$) son extensiones de grado 2 y, por tanto, son normales. Esto demuestra de forma constructiva que **la clase de extensiones normales no es multiplicativa (no es transitiva)**.

Proposición 2.4.1: Propiedades de las extensiones normales (Prop. 2.15)

1. Sea $K \subseteq E \subseteq L$ una torre de cuerpos. Si L/K es normal, entonces la subextensión superior L/E es normal.

2. Sea $\{E_i/K\}_{i\in I}$ una familia de extensiones admisibles. Si cada E_i/K es normal, entonces la intersección $(\bigcap_{i\in I} E_i)/K$ y el compuesto $(\prod_{i\in I} E_i)/K$ son normales.

3. **Levantamientos:** La clase de extensiones normales es cerrada para levantamientos. Es decir, si E/K es normal y admisible con F/K, entonces el cuerpo compuesto EF/F es normal.

Demostración. **(1)** Obvio por definición, ya que si los polinomios factorizan completamente sobre K, también lo hacen sobre E.

(2) Para la intersección: Sea $p \in K[X]$ un polinomio irreducible con una raíz en $\bigcap E_i$. Entonces p tiene una raíz en cada E_i. Como cada E_i/K es normal (Teorema 2.11(5)), p factoriza completamente en cada E_i. Al tener todas sus raíces en todos los E_i, tiene todas sus raíces en la intersección $\bigcap E_i$. Luego la intersección es normal. Para el producto: Si $E_i = K(S_i)$ es el C.D. de $\mathcal{P}_i$, entonces $\prod E_i = K(\bigcup S_i)$ es el C.D. de $\bigcup \mathcal{P}_i$, que la hace normal.

(3) Supongamos que E/K es normal. Por la caracterización (1), E es el cuerpo de descomposición de un cierto conjunto $\mathcal{P} \subseteq K[X] \setminus K$. Podemos escribir $E = K(S)$ donde S es el conjunto de raíces de $\mathcal{P}$. Consideremos el cuerpo compuesto EF. Por propiedades del cuerpo generado:

$$EF = F(E) = F(K(S)) = F(S)$$

Como $K \subseteq F$, la familia de polinomios cumple que $\mathcal{P} \subseteq F[X] \setminus F$. Entonces $EF = F(S)$ es exactamente el cuerpo de descomposición de la familia $\mathcal{P}$ sobre el cuerpo base F. Por la caracterización (1), la extensión EF/F es normal. □

2.5. Clausura Normal

Intuitivamente: Tenemos una extensión L/K que no es normal (le faltan raíces). Queremos encontrar el cuerpo "más ajustado posible"(N) que contenga a L y que sí sea normal. A ese cuerpo lo llamamos clausura normal.

Teorema 2.5.1: Existencia de la Clausura Normal (Teorema 2.16)

Sea L/K una extensión algebraica. Entonces:

1. Existe una extensión N/L que verifica:

   a) N/K es normal.

   b) Si E es una subextensión de N/L y E/K es normal, entonces $E = N$.

   (Es decir, N/K es la extensión normal más pequeña que extiende a L). En tal caso, se dice que N/K es **una clausura normal** de L/K.

2. Todas las clausuras normales de L/K son L-isomorfas.

3. Si la extensión inicial L/K es finita, entonces su clausura normal N/K también es finita.

Ejemplo 2.5.1: Construcción intuitiva de la clausura normal

Veamos un ejemplo antes de demostrar el teorema general. Vimos anteriormente que la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no era normal porque al polinomio mínimo $X^3 - 2$ le faltaban sus otras dos raíces complejas.
Para que sea normal, tenemos que "meterle lo que le falta". Las raíces que faltan son $\sqrt[3]{2}\xi_3$ y $\sqrt[3]{2}\xi_3^2$. Al adjuntar la raíz primitiva de la unidad, la clausura normal resultante será exactamente el cuerpo de descomposición: $\mathbb{Q}(\sqrt[3]{2}, \xi_3)$.

Demostración del Teorema 2.16. **Demostración de (1): Existencia y minimidad.** Sea $\overline{L}$ una clausura algebraica de L. Definimos el siguiente conjunto de subextensiones:

$$\Omega = \{E \mid L \subseteq E \subseteq \overline{L} \text{ tal que } E/K \text{ es una extensión normal}\}$$

¿Está este conjunto vacío? No. Como $\overline{L}$ es algebraicamente cerrado, por el Corolario 2.13 sabemos que la extensión $\overline{L}/K$ es normal. Por tanto, $\overline{L} \in \Omega$, lo que implica que $\Omega \neq \emptyset$.

Si tomamos la intersección de todos los cuerpos de esta familia:

$$N := \bigcap_{E \in \Omega} E$$

se tiene trivialmente que $L \subseteq N \subseteq \overline{L}$.

Comprobemos las dos condiciones exigidas:

1. Por la Proposición 2.15, la intersección arbitraria de extensiones normales vuelve a ser una extensión normal. Por tanto, N/K es normal.

2. Si E es una subextensión de N/L que es normal sobre K, entonces $E \in \Omega$. Por la propia definición de la intersección, N está contenido en todos los elementos de Ω, luego $N \subseteq E$. Como por hipótesis de subextensión $E \subseteq N$, forzosamente $N = E$.

Con esto queda demostrada la existencia. De esta demostración nos quedamos con la idea clave de que la clausura normal se obtiene *intersecando* todas las subextensiones de la clausura algebraica que son normales sobre K.

Demostración de (2) y (3): Unicidad e finitud. Supongamos que tenemos dos clausuras normales N_1/K y N_2/K de L. Queremos ver que son L-isomorfas.

Sea B una base de L visto como espacio vectorial sobre K. Para cada elemento básico $\alpha \in B$, construimos su polinomio mínimo $p_\alpha = \mathrm{Min}_K(\alpha)$. Definimos la familia de polinomios $\mathcal{P} = \{p_\alpha \mid \alpha \in B\}$.

Llamemos $R_{1,\alpha}$ al conjunto de raíces de p_α que residen en N_1, y $R_{2,\alpha}$ a las que residen en N_2. Como N_1/K y N_2/K son extensiones normales por definición, cada polinomio p_α (al tener una raíz $\alpha \in L \subseteq N_i$) es completamente factorizable sobre N_1 y sobre N_2.

Además, la clausura normal N_1 ha de contener a L (que contiene a la base B) y ser normal. Para ser normal, debe contener obligatoriamente *todas* las raíces de los polinomios mínimos de sus elementos. Por minimalidad, no puede contener elementos .$^{\text{ex}}$tra". Por tanto, N_1 y N_2 son exactamente los cuerpos de descomposición de la familia de polinomios $\mathcal{P}$ sobre K.

Formalmente, se tiene:

$$N_1 = K\left(\bigcup_{\alpha\in B} R_{1,\alpha}\right) \quad \text{y} \quad N_2 = K\left(\bigcup_{\alpha\in B} R_{2,\alpha}\right)$$

Dado que $K \subseteq L$, podemos reescribir estos cuerpos añadiendo la base L:

$$N_1 = L\left(\bigcup_{\alpha\in B} R_{1,\alpha}\right) \quad \text{y} \quad N_2 = L\left(\bigcup_{\alpha\in B} R_{2,\alpha}\right)$$

Esto demuestra que N_1 y N_2 son cuerpos de descomposición de la **misma familia de polinomios** $\mathcal{P}$, pero vistos como extensiones sobre el cuerpo base L. Aplicando la Proposición 2.9 (Unicidad del cuerpo de descomposición), garantizamos la existencia de un L-isomorfismo entre ellos:

$$\sigma : N_1 \longrightarrow N_2$$

Lo que prueba la parte (2).

Finalmente, para la parte (3): Si la extensión inicial L/K es finita, entonces la base B tiene un número finito de elementos. Esto implica que la familia de polinomios $\mathcal{P}$ es finita, y por ende, el conjunto total de raíces que debemos adjuntar es finito. Como acabamos de ver que N_i es el cuerpo de descomposición de estos polinomios sobre L, la extensión N_i/K está generada por un número finito de elementos algebraicos. Por el Corolario 1.15 (toda extensión finita generada por elementos algebraicos es finita), deducimos que $\frac{N_i}{K}$ es finita. $\square$

Capítulo 3

Extensiones Ciclotómicas

3.1. Extensiones Ciclotómicas

Definición 3.1.1: Extensión ciclotómica (Def. 3.4)

Sea K un cuerpo y n un entero positivo. Se llama **n-ésima extensión ciclotómica** de K al cuerpo de descomposición del polinomio $X^n - 1$ sobre K.
Como el conjunto de las raíces n-ésimas de la unidad forma un grupo cíclico, la n-ésima extensión ciclotómica de K es $K(\xi)$, donde ξ es un generador del grupo de raíces n-ésimas de la unidad.

Definición 3.1.2: Polinomio ciclotómico

Supongamos que $\operatorname{car}(K) = p \nmid n$ y sean $\xi_1, \xi_2, \dots, \xi_{\varphi(n)}$ las raíces n-ésimas primitivas de la unidad en un cuerpo de descomposición. Llamamos **n-ésimo polinomio ciclotómico** a:

$$\Phi_n = (X - \xi_1) \cdots (X - \xi_{\varphi(n)})$$

(Más adelante veremos que si consideramos cuerpos de característica p, entonces $\Phi_n \in \mathbb{Z}_p[X]$).

Observación 3.1.1: Aclaración sobre raíces de la unidad

Para el polinomio $X^n - 1$:

- α es **raíz n-ésima** si $\alpha^n = 1$.
- α es **raíz n-ésima primitiva** si su orden multiplicativo es exactamente n, es decir $|\alpha| = |\langle \alpha \rangle| = n$. Esto equivale a decir que $\alpha^n = 1$, pero $\alpha^k \neq 1$ para todo $k = 1, \dots, n-1$.

Observación 3.1.2: Recordatorio de Grupos y Anillos

- El **subcuerpo primo** de un cuerpo K es el menor cuerpo contenido en él.
- Se tiene que el cuerpo primo de $K \cong \mathbb{Q}$ si $\operatorname{car}(K) = 0$, y es isomorfo a $\mathbb{Z}_p$ si $\operatorname{car}(K) = p$.

- El **anillo primo** de K es isomorfo a $\mathbb{Z}$ si $\operatorname{car}(K) = 0$, o igual al cuerpo primo si la característica es distinta de cero.
- En cualquier caso, el anillo primo es siempre un Dominio de Factorización Única (DFU).

3.2. Polinomios sobre un DFU

Definición 3.2.1: Polinomio Primitivo y Contenido

Sea D un Dominio de Factorización Única (DFU) y K su cuerpo de fracciones. Sea $P \in K[X] \setminus \{0\}$.

- Un polinomio $Q \in D[X]$ es un **polinomio primitivo** si sus coeficientes son coprimos entre sí.
- Llamaremos **contenido** de P a un elemento $a \in K$ tal que $P = aP_1$ con $P_1 \in D[X]$ primitivo.
- Lo denotamos por $C(P)$. Este valor siempre existe: como $P \in K[X]$, podemos multiplicar por un denominador común $d \in D \setminus \{0\}$ tal que $dP \in D[X]$. Si extraemos el máximo común divisor de los coeficientes, $a = \operatorname{mcd}(\text{coeficientes de } dP)$, entonces $P_1 = \frac{d}{a}P$ es un polinomio primitivo, y podemos escribir $P = \frac{a}{d}P_1$. Por tanto, $\frac{a}{d} \in C(P)$.

Observación 3.2.1: Unicidad del contenido

El concepto de contenido de un polinomio es único salvo producto por unidades de D ($D^\times$). En efecto, si $a, b \in C(P)$, entonces $P = aP_1 = bP_2$ con $P_1, P_2 \in D[X]$ primitivos. Escribiendo $a = \frac{a_1}{a_2}$ y $b = \frac{b_1}{b_2}$, tenemos $\frac{a_1}{a_2}P_1 = \frac{b_1}{b_2}P_2$, lo que equivale a $a_1 b_2 P_1 = a_2 b_1 P_2$. Como D es un dominio y los polinomios son primitivos, al igualar los máximos comunes divisores de los coeficientes a ambos lados, obtenemos que $a_1 b_2$ y $a_2 b_1$ son elementos asociados en D. Por tanto, existe una unidad $u \in D^\times$ tal que $b = au$.

Lema 3.2.1: Lema de Gauss

Si K es el cuerpo de fracciones de un DFU D, y $P, Q \in K[X] \setminus \{0\}$, entonces:

$$C(P \cdot Q) = C(P) \cdot C(Q)$$

En particular, el producto de dos polinomios primitivos es primitivo (salvo unidad).

Demostración. Podemos escribir $P = aP_1$ y $Q = bQ_1$ con P_1, Q_1 primitivos y $a \in C(P)$, $b \in C(Q)$. Está claro que $P \cdot Q = ab(P_1 Q_1)$. Bastará con demostrar que el producto $P_1 Q_1$ es primitivo, ya que eso implicaría automáticamente que $ab \in C(PQ)$.

Procedemos por reducción al absurdo. Supongamos que $P_1 Q_1$ no es primitivo. Entonces existe un elemento primo $p \in D$ que divide a todos los coeficientes de $P_1 Q_1$. Sean $P_1 = a_0 + a_1 X + \cdots + a_n X^n$ y $Q_1 = b_0 + b_1 X + \cdots + b_m X^m$. Como P_1 y Q_1 son primitivos, $\operatorname{mcd}(a_i) = 1$ y $\operatorname{mcd}(b_j) = 1$. Por lo tanto, p no puede dividir a todos sus coeficientes. Elijamos i como el menor índice tal que $p \nmid a_i$, y j como el menor índice tal que $p \nmid b_j$.

Analicemos el coeficiente de grado $i+j$ en el polinomio producto P_1Q_1, que viene dado por la suma $\sum_{k+l=i+j} a_k b_l$:

$$\cdots + a_{i-1}b_{j+1} + a_i b_j + a_{i+1}b_{j-1} + \ldots$$

Por nuestra elección minimal de i y j, el primo p divide a todos los sumandos anteriores a $a_i b_j$ (porque $p \mid a_k$ para $k < i$) y a todos los sumandos posteriores (porque $p \mid b_l$ para $l < j$). Sin embargo, $p \nmid a_i$ y $p \nmid b_j$, y como p es primo, $p \nmid a_i b_j$. Por tanto, p no puede dividir a la suma total, lo que es una flagrante contradicción con la suposición de que p dividía a todos los coeficientes de P_1Q_1. □

Lema 3.2.2: Lema 3.6

Sea D un DFU, K su cuerpo de fracciones y $P \in D[X]$, $Q \in K[X]$ polinomios mónicos. Si Q divide a P en el anillo $K[X]$, entonces $Q \in D[X]$ y Q divide a P en $D[X]$.

Demostración. Dado que Q divide a P en $K[X]$, existe un polinomio $R \in K[X]$ tal que $P = Q \cdot R$. Como P es mónico y está en $D[X]$, sus coeficientes son coprimos (el coeficiente principal es 1, que solo es divisible por unidades). Por tanto, P es primitivo y $C(P) = 1$. Además, como P y Q son mónicos, necesariamente R debe ser también un polinomio mónico.

Aplicamos el Lema de Gauss a la igualdad $P = Q \cdot R$:

$$1 = C(P) = C(Q \cdot R) = C(Q) \cdot C(R)$$

Por la definición de contenido, existen polinomios primitivos $Q^*, R^* \in D[X]$ tales que $Q = C(Q)Q^*$ y $R = C(R)R^*$. Fijémonos en los coeficientes principales. Sea $u \in D$ el coeficiente principal de Q^*. Al ser Q mónico, su coeficiente principal es 1, por lo que $1 = C(Q) \cdot u$, lo que implica que $C(Q) = u^{-1}$. Análogamente, si $v \in D$ es el coeficiente principal de R^*, tenemos $1 = C(R) \cdot v$, por lo que $C(R) = v^{-1}$.

Sustituyendo esto en la ecuación de los contenidos:

$$1 = C(Q) \cdot C(R) = u^{-1} \cdot v^{-1} \implies uv = 1$$

Esta relación nos indica que tanto u como v son unidades en D ($u, v \in D^\times$).

Por lo tanto, $C(Q) = u^{-1} \in D$. Esto significa que $Q = u^{-1}Q^*$ es el producto de un elemento de D por un polinomio de $D[X]$, lo que garantiza que $Q \in D[X]$. Del mismo modo, $R = v^{-1}R^* \in D[X]$. Al tener $P = Q \cdot R$ con $Q, R \in D[X]$, concluimos que Q divide a P dentro de $D[X]$. □

Proposición 3.2.1: Propiedades de los polinomios ciclotómicos (Prop. 3.7)

En característica $p \geq 0$ (siempre que $p \nmid n$), se verifican las siguientes propiedades:

1. $\mathrm{gr}(\Phi_n) = \varphi(n) = |\mathbb{Z}_n^*|$.
2. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
3. $\Phi_n \in \mathbb{Z}_p[X]$.
4. Si K es el cuerpo de fracciones de $\mathbb{Z}_p$ y ξ es una raíz de la unidad en una extensión de K, entonces $\mathrm{Min}_K(\xi) \in \mathbb{Z}_p[X]$.

(Nota notacional: Si $p = 0$, entendemos que el anillo primo es $\mathbb{Z}_0 = \mathbb{Z}$ y su cuerpo de fracciones es $K = \mathbb{Q}$).

Demostración. **Demostración de 1): Grado del polinomio ciclotómico**

Consideremos el polinomio $f(X) = X^n - 1$ sobre el cuerpo K. Su derivada formal es $f'(X) = nX^{n-1}$. Como por hipótesis la característica p no divide a n ($p \nmid n$), tenemos que $n \neq 0$ en K, por lo que $f'(X)$ solo se anula en $X = 0$. Dado que 0 no es raíz de $X^n - 1$, el polinomio y su derivada son coprimos ($\mathrm{mcd}(f, f') = 1$). Esto garantiza que $X^n - 1$ tiene exactamente n raíces distintas en su cuerpo de descomposición.

El conjunto de estas n raíces forma un grupo multiplicativo, denotado por G. Todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico, por lo que $G \cong (\mathbb{Z}_n, +)$. Por la teoría elemental de grupos cíclicos, el número de generadores de un grupo cíclico de orden n es exactamente $\varphi(n)$ (la función indicatriz de Euler, que cuenta los números coprimos con n). Dado que el n-ésimo polinomio ciclotómico $\Phi_n(X)$ se define como el producto de los factores $(X - \xi_i)$ donde ξ_i son precisamente estos generadores (las raíces n-ésimas primitivas), concluimos irremediablemente que su grado es el número de factores, es decir, $\mathrm{gr}(\Phi_n) = \varphi(n)$.

Demostración de 2): Factorización de $X^n - 1$

Como hemos establecido, el grupo G de las n raíces de $X^n - 1$ es un grupo cíclico de orden n. El polinomio descompone linealmente en su cuerpo de escisión como:

$$X^n - 1 = \prod_{z \in G} (X - z)$$

Por el Teorema de Lagrange, el orden de cualquier elemento $z \in G$ debe ser un divisor exacto de n. Clasifiquemos los elementos de G atendiendo a su orden multiplicativo exacto. Para cada divisor $d \mid n$, definimos el conjunto:

$$G_d = \{z \in G \mid \mathrm{orden}(z) = d\}$$

Es fundamental observar que un elemento tiene orden d en G si y solo si es una raíz d-ésima primitiva de la unidad. Por tanto, el producto de los factores lineales asociados a G_d construye exactamente el d-ésimo polinomio ciclotómico:

$$\prod_{z \in G_d} (X - z) = \Phi_d(X)$$

Dado que todo elemento de G tiene un único orden, la familia de subconjuntos $\{G_d\}_{d|n}$ constituye una partición disjunta del grupo G (es decir, $G = \bigsqcup_{d|n} G_d$). Reordenando los factores del producto original según esta partición geométrica, obtenemos:

$$X^n - 1 = \prod_{d|n} \left(\prod_{z \in G_d} (X - z) \right) = \prod_{d|n} \Phi_d(X)$$

Demostración de 3): Pertenencia a $\mathbb{Z}_p[X]$

Dividiremos esta demostración en dos fases lógicas. Primero demostraremos que $\Phi_n \in K[X]$ (donde K es el cuerpo de fracciones de $\mathbb{Z}_p$) razonando por inducción fuerte sobre n.

- **Caso base ($n = 1$):** $\Phi_1(X) = X - 1$. Como los coeficientes 1 y -1 pertenecen a cualquier cuerpo primo, trivialmente $\Phi_1 \in K[X]$.
- **Paso inductivo:** Supongamos que la proposición es cierta para todo entero $d < n$. Esto es, para todo divisor d de n estrictamente menor que n, se cumple que $\Phi_d \in K[X]$. Despejando el término $d = n$ del producto obtenido en el apartado anterior, tenemos:

  $$X^n - 1 = \left(\prod_{\substack{d|n \\ d<n}} \Phi_d(X) \right) \cdot \Phi_n(X)$$

  Definamos $G(X) = \prod_{d|n, d<n} \Phi_d(X)$. Por la hipótesis de inducción, al ser un producto de polinomios en $K[X]$, el propio $G(X)$ pertenece a $K[X]$. Además, como cada Φ_d es mónico por definición, $G(X)$ también es un polinomio mónico.

  Realizamos la división euclídea de $X^n - 1$ entre $G(X)$ dentro del anillo $K[X]$. El algoritmo de la división nos garantiza que existen únicos polinomios $C(X), R(X) \in K[X]$ tales que:

  $$X^n - 1 = G(X)C(X) + R(X) \quad \text{con } \operatorname{gr}(R) < \operatorname{gr}(G)$$

  Sin embargo, operando en el cuerpo de descomposición (un cuerpo más grande), sabemos que la división es exacta y el cociente es $\Phi_n(X)$. Por la unicidad del algoritmo de división, el cociente y el resto deben ser los mismos independientemente de si operamos en K o en su extensión. Por tanto, el resto $R(X)$ es obligatoriamente el polinomio nulo y el cociente $C(X) = \Phi_n(X)$ debe tener sus coeficientes en K. Concluimos que $\Phi_n \in K[X]$.

A continuación, fortalecemos el resultado para demostrar que realmente caen en $\mathbb{Z}_p[X]$, dependiendo de la característica:

- **Si $p > 0$:** El cuerpo primo K es exactamente $\mathbb{Z}_p$. Al no haber denominadores, el anillo y su cuerpo de fracciones coinciden. Hemos probado que $\Phi_n \in K[X] = \mathbb{Z}_p[X]$.
- **Si $p = 0$:** El anillo es $\mathbb{Z}_0 = \mathbb{Z}$ y su cuerpo de fracciones es $K = \mathbb{Q}$. Hasta ahora sabemos que $\Phi_n \in \mathbb{Q}[X]$. Consideremos la igualdad $X^n - 1 = G(X) \cdot \Phi_n(X)$. Sabemos que $X^n - 1 \in \mathbb{Z}[X]$. Además, tanto $G(X)$ como $\Phi_n(X)$ son polinomios mónicos con coeficientes en $\mathbb{Q}$. Aplicamos el **Lema 3.6** (corolario del Lema de Gauss): si un polinomio mónico en $\mathbb{Q}[X]$ divide a un polinomio en $\mathbb{Z}[X]$, entonces el divisor pertenece necesariamente a $\mathbb{Z}[X]$. Dado que $\Phi_n(X)$ divide a $X^n - 1$ en $\mathbb{Q}[X]$, deducimos que $\Phi_n(X) \in \mathbb{Z}[X]$.

Demostración de 4): El polinomio mínimo sobre el cuerpo de fracciones

Sea ξ una raíz de la unidad (de algún orden m) y $f(X) = \mathrm{Min}_K(\xi)$. Por la propia definición axiomática del polinomio mínimo, sus coeficientes siempre residen en el cuerpo base, luego $f(X) \in K[X]$.

Como ξ es raíz de la unidad de orden m, es raíz del polinomio $X^m - 1$. Por las propiedades del polinomio mínimo, si un elemento es raíz de un polinomio sobre K, su polinomio mínimo debe dividirlo. Por lo tanto, $f(X)$ divide a $X^m - 1$ en $K[X]$.

Replicamos la dicotomía según la característica del cuerpo:

- **Si** $p > 0$**:** De nuevo, $K = \mathbb{Z}_p$, luego $f(X) \in \mathbb{Z}_p[X]$ de forma trivial.
- **Si** $p = 0$**:** $K = \mathbb{Q}$. Tenemos que $f(X) \in \mathbb{Q}[X]$ y $f(X)$ es un polinomio mónico que divide a $X^m - 1$ (el cual pertenece a $\mathbb{Z}[X]$). Apelando nuevamente al **Lema 3.6**, como $f(X)$ es un divisor mónico racional de un polinomio entero, se sigue forzosamente que $f(X)$ tiene coeficientes exclusivamente enteros. Por tanto, $\mathrm{Min}_{\mathbb{Q}}(\xi) \in \mathbb{Z}[X]$.

□

Observación 3.2.2: Independencia de la característica

Observemos que la expresión polinómica de Φ_n **no depende de la característica** del cuerpo (siempre que la característica no divida a n). Sin embargo, que el polinomio Φ_n sea o no irreducible **sí que depende** fuertemente de la característica del cuerpo base.

Observación 3.2.3: Cálculo recursivo de Polinomios Ciclotómicos

La expresión obtenida en la demostración anterior nos proporciona un método iterativo y recursivo directo para calcular Φ_n:

$$X^n - 1 = \Phi_n(X) \cdot \prod_{d|n, d\neq n} \Phi_d(X) \implies \Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d\neq n} \Phi_d(X)}$$

Ejemplos de cálculo directo:

- $\Phi_1(X) = X - 1$
- $\Phi_2(X) = \frac{X^2-1}{\Phi_1(X)} = \frac{(X+1)(X-1)}{X-1} = X + 1$
- $\Phi_3(X) = \frac{X^3-1}{\Phi_1(X)} = \frac{X^3-1}{X-1} = X^2 + X + 1$
- $\Phi_4(X) = \frac{X^4-1}{\Phi_1(X)\cdot\Phi_2(X)} = \frac{(X^2+1)(X^2-1)}{(X-1)(X+1)} = X^2 + 1$

En general, si q es un número primo (distinto de la característica), sus únicos divisores son 1 y q, por lo que:

$$\Phi_q(X) = \frac{X^q - 1}{\Phi_1(X)} = \frac{X^q - 1}{X - 1} = X^{q-1} + X^{q-2} + \cdots + X + 1$$

Por ejemplo: $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$.

Teorema 3.2.1: Irreducibilidad en $\mathbb{Q}$ (Teorema 3.9)

Los polinomios ciclotómicos $\Phi_n \in \mathbb{Z}[X]$ en característica 0 son siempre **irreducibles** sobre $\mathbb{Q}$.

Demostración del Teorema 3.9. **Fase 1: Planteamiento inicial** Fijemos una raíz n-ésima primitiva de la unidad, a la que llamaremos ξ. Sea $f = \mathrm{Min}_{\mathbb{Q}}(\xi)$ su polinomio mínimo sobre los racionales y denotemos $\Phi = \Phi_n$ al n-ésimo polinomio ciclotómico.

Sabemos que Φ es un polinomio mónico cuyas raíces son *todas* las raíces primitivas de la unidad:

$$\Phi(X) = (X - \xi_1)(X - \xi_2)\dots(X - \xi_{\varphi(n)})$$

Como f es el polinomio mínimo de ξ, y ξ es raíz de Φ, se sigue obligatoriamente que f debe dividir a Φ en $\mathbb{Q}[X]$.

Para que $\Phi = f$ (y con ello Φ sea irreducible por definición), siendo ambos polinomios mónicos, es suficiente con demostrar que f contiene *todas* las raíces de Φ. Con esto, tendrían las mismas raíces, serían polinomios asociados y, por ser mónicos, serían iguales.

Las raíces primitivas n-ésimas son de la forma ξ^r con $\mathrm{mcd}(r, n) = 1$. Por lo tanto, nuestro objetivo se reduce a demostrar la siguiente afirmación: *Si ξ es raíz de f, entonces cualquier ξ^r con $\mathrm{mcd}(r, n) = 1$ también es raíz de f.*

Fase 2: El paso primo (Lema clave por reducción al absurdo) Vamos a demostrar primero el caso en el que $r = p$ es un número primo tal que $p \nmid n$. Lo haremos por reducción al absurdo. Supongamos que ξ^p **no** es raíz de f.

Sean $g = \mathrm{Min}_{\mathbb{Q}}(\xi^p)$ y $g_1(X) = g(X^p)$. Como ξ es raíz de g_1 (pues $g_1(\xi) = g(\xi^p) = 0$), el polinomio mínimo f divide automáticamente a g_1 en $\mathbb{Q}[X]$.

Por la Proposición 3.7, el polinomio mínimo de cualquier raíz de la unidad tiene coeficientes enteros. Por tanto, $f \in \mathbb{Z}[X]$ y $g \in \mathbb{Z}[X]$, de donde también se deduce que $g_1 \in \mathbb{Z}[X]$. En resumen: tenemos que $\mathbb{Z}$ es un DFU, $\mathbb{Q}$ su cuerpo de fracciones, $f, g_1 \in \mathbb{Z}[X]$ son mónicos, y f divide a g_1 en $\mathbb{Q}[X]$. Aplicando el **Lema 3.6** (consecuencia del Lema de Gauss), deducimos que f divide a g_1 en $\mathbb{Z}[X]$. Es decir, existe un $h \in \mathbb{Z}[X]$ tal que:

$$g_1(X) = f(X) \cdot h(X)$$

Fase 3: Descenso al cuerpo finito $\mathbb{Z}_p$ Vamos a "trasladar"los coeficientes de los polinomios a $\mathbb{Z}_p$. Para ello, consideramos la proyección canónica $\pi : \mathbb{Z} \to \mathbb{Z}_p$ y la extendemos al anillo de polinomios $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$ reduciendo sus coeficientes módulo p. Denotaremos con una barra ($\overline{f}$) a la imagen de un polinomio bajo esta aplicación.

Recordemos dos propiedades fundamentales en un cuerpo de característica p:

1. El binomio de Newton: $(a + b)^p = a^p + b^p$.
2. El Pequeño Teorema de Fermat: $a^p \equiv a \pmod{p}$, lo que implica que $\overline{a}^p = \overline{a}$ en $\mathbb{Z}_p$.

Juntando estos dos resultados, si $\overline{g}(X) = a_0 + a_1X + \dots + a_mX^m$, tenemos:

$$(\overline{g}(X))^p = (a_0 + a_1X + \dots + a_mX^m)^p = a_0^p + a_1^pX^p + \dots + a_m^pX^{mp}$$

Como $a_i^p = a_i$ en $\mathbb{Z}_p$, esto es exactamente igual a:

$$= a_0 + a_1 X^p + \cdots + a_m (X^p)^m = \overline{g}(X^p) = \overline{g_1}(X)$$

Proyectando la igualdad $g_1 = f \cdot h$ a $\mathbb{Z}_p[X]$, obtenemos:

$$(\overline{g}(X))^p = \overline{g_1}(X) = \overline{f}(X) \cdot \overline{h}(X)$$

Fase 4: La contradicción de la raíz múltiple Sea $q(X) \in \mathbb{Z}_p[X]$ un factor irreducible de $\overline{f}(X)$. Como $q \mid \overline{f}$, la igualdad anterior implica que $q \mid (\overline{g})^p$. Al ser q irreducible, esto fuerza a que $q \mid \overline{g}$. Por tanto, $\overline{f}$ y $\overline{g}$ comparten un factor irreducible q en $\mathbb{Z}_p[X]$.

Retomemos nuestra hipótesis de absurdo: habíamos supuesto que ξ^p no era raíz de f. Si ξ^p no es raíz de f, entonces f y g (siendo ambos polinomios irreducibles y mónicos distintos en $\mathbb{Q}[X]$) son **coprimos**. Además, ξ es raíz primitiva (raíz de Φ_n) y ξ^p también es raíz primitiva (pues $p \nmid n \implies \mathrm{mcd}(p, n) = 1$). Esto significa que tanto f como g dividen a Φ_n, y por ser coprimos, su producto divide a Φ_n:

$$f \cdot g \mid \Phi_n(X) \implies f \cdot g \mid X^n - 1 \quad \text{en } \mathbb{Z}[X]$$

Proyectando esta divisibilidad a $\mathbb{Z}_p[X]$, tenemos que $\overline{f} \cdot \overline{g} \mid X^n - 1$. Como q divide tanto a $\overline{f}$ como a $\overline{g}$, deducimos que:

$$q^2 \mid X^n - 1 \quad \text{en } \mathbb{Z}_p[X]$$

Esto significa que el polinomio $X^n - 1$ tiene una **raíz múltiple** en alguna extensión del cuerpo $\mathbb{Z}_p$. Sin embargo, ya demostramos anteriormente que si la característica p no divide a n ($p \nmid n$), la derivada de $X^n - 1$ es $nX^{n-1} \neq 0$, por lo que $X^n - 1$ **no tiene raíces múltiples**.

¡Hemos llegado a una contradicción! La suposición de que ξ^p no era raíz de f es falsa. Por tanto, ξ^p es raíz de f.

Fase 5: Paso al caso general (Inducción) Queremos ver que para cualquier r con $\mathrm{mcd}(r, n) = 1$, ξ^r es raíz de f. Podemos factorizar r en producto de números primos: $r = p_1 p_2 \ldots p_k$ (donde algunos p_i pueden repetirse, pero ninguno divide a n). Razonamos por inducción sobre el número de factores primos k:

- **Caso base ($k = 1$):** Es exactamente el paso primo que acabamos de demostrar.
- **Paso inductivo:** Supongamos que el resultado es cierto para $k - 1$ factores. Sea $\eta = \xi^{p_1 \cdots p_{k-1}}$. Por hipótesis de inducción, η es raíz de f. Como f es irreducible y η es raíz, f debe ser el polinomio mínimo de η, es decir, $f = \mathrm{Min}_{\mathbb{Q}}(\eta)$. Ahora aplicamos el caso base (el paso primo) al elemento η y al primo p_k: si η es raíz de su polinomio mínimo f, entonces η^{p_k} también es raíz de f. Pero $\eta^{p_k} = (\xi^{p_1 \cdots p_{k-1}})^{p_k} = \xi^r$.

Por lo tanto, ξ^r es raíz de f para todo r coprimo con n.

Conclusión: El polinomio mínimo f contiene a todas las raíces de Φ_n. Dado que ambos son mónicos y $f \mid \Phi_n$, concluimos irrevocablemente que $f = \Phi_n$. Como el polinomio mínimo es irreducible por definición, Φ_n es irreducible en $\mathbb{Q}[X]$. □

Corolario 3.2.1: Corolario 3.10

Si ξ es una raíz n-ésima primitiva de la unidad en característica 0, entonces:

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \text{gr}(\text{Min}_{\mathbb{Q}}(\xi)) = \text{gr}(\Phi_n) = \varphi(n)$$

Observación 3.2.4: Nota: El Teorema 3.9 y la característica p

El Teorema 3.9 (que afirma que los polinomios ciclotómicos son irreducibles) **no funciona si la característica es distinta de 0** (es decir, la hipótesis de característica 0 no es superflua).
Por ejemplo, consideremos el cuerpo finito $\mathbb{F}_8$. Sabemos que $[\mathbb{F}_8 : \mathbb{F}_2] = 3$. El grupo multiplicativo de este cuerpo es $\mathbb{F}_8^* = \langle \xi_7 \rangle$, donde ξ_7 es un generador y, por tanto, una raíz 7-ésima primitiva de la unidad.
Como $\xi_7 \in \mathbb{F}_8$, el grado de su polinomio mínimo sobre $\mathbb{F}_2$ debe dividir al grado de la extensión, que es 3 (de hecho, es exactamente 3). Sin embargo, el grado del polinomio ciclotómico $\Phi_7(X)$ es $\varphi(7) = 6$. Como el grado del polinomio mínimo (3) no coincide con $\varphi(7)$, deducimos que el polinomio mínimo no es Φ_7, lo que implica inequívocamente que $\Phi_7(X)$ **no es irreducible sobre** $\mathbb{F}_2$ (se descompone en factores).

Ejemplos Adicionales del Tema 3 (Extensiones Ciclotómicas)

Ejemplo 3.2.1: Cálculo del 6º polinomio ciclotómico

Queremos calcular $\Phi_6(X)$ usando la fórmula recursiva $X^n - 1 = \prod_{d|n} \Phi_d(X)$. Los divisores de 6 son 1, 2, 3 y 6. Por tanto:

$$X^6 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \cdot \Phi_6(X)$$

Ya conocemos los anteriores (calculados previamente):

- $\Phi_1(X) = X - 1$
- $\Phi_2(X) = X + 1$
- $\Phi_3(X) = X^2 + X + 1$

Notemos que $\Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) = (X^2 - 1)(X^2 + X + 1) = X^4 + X^3 - X - 1$. También podemos ser más astutos y observar que $\Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) = (X^3 - 1)(X + 1)$. Pero aún más fácil, sabemos que $X^6 - 1 = (X^3 - 1)(X^3 + 1)$. Como $\Phi_1\Phi_3 = X^3 - 1$, deducimos que:

$$X^3 + 1 = \Phi_2(X) \cdot \Phi_6(X) \implies \Phi_6(X) = \frac{X^3 + 1}{X + 1} = X^2 - X + 1$$

Ejemplo 3.2.2: Grados de extensiones ciclotómicas sobre $\mathbb{Q}$

Sea ξ una raíz 8-ésima primitiva de la unidad (por ejemplo, $\xi = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$). ¿Cuál es el grado de la extensión $\mathbb{Q}(\xi)/\mathbb{Q}$?

Por el Corolario 3.10, como estamos en característica 0, el grado es exactamente $\varphi(8)$. Dado que $8 = 2^3$, calculamos la función de Euler:

$$\varphi(8) = 8\left(1 - \frac{1}{2}\right) = 4$$

Por tanto, $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$. El polinomio mínimo de ξ será $\Phi_8(X)$. Como los divisores de 8 son 1, 2, 4, 8:

$$\Phi_8(X) = \frac{X^8 - 1}{\Phi_1\Phi_2\Phi_4} = \frac{X^8 - 1}{X^4 - 1} = X^4 + 1$$

Este polinomio es irreducible en $\mathbb{Q}[X]$.

Ejemplo 3.2.3: Descomposición de un polinomio ciclotómico en característica p

Vamos a desarrollar con detalle la **Nota** teórica anterior sobre $\mathbb{F}_2$. El polinomio ciclotómico $\Phi_7(X)$ en $\mathbb{Z}[X]$ es:

$$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

Sobre $\mathbb{Q}$, este polinomio es irreducible (Teorema 3.9). Sin embargo, si lo vemos como un polinomio con coeficientes en $\mathbb{F}_2$ (reduciendo módulo 2), se factoriza.
En $\mathbb{F}_2[X]$, se comprueba que:

$$(X^3 + X + 1)(X^3 + X^2 + 1) = X^6 + X^5 + X^4 + 2X^3 + X^2 + X + 1$$

Como $2 = 0$ en $\mathbb{F}_2$, el término $2X^3$ desaparece, y obtenemos exactamente $\Phi_7(X)$.
Esto demuestra empíricamente que:

$$\Phi_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1) \quad \text{en } \mathbb{F}_2[X]$$

Las raíces primitivas 7-ésimas se reparten: 3 de ellas son raíces del primer factor, y las otras 3 son raíces del segundo. El polinomio mínimo de cualquiera de ellas tiene grado 3, no $\varphi(7) = 6$.

Capítulo 4

Extensiones separables

4.1. Grado de separabilidad

Definición 4.1.1: Grado de separabilidad

Sea E/K una extensión algebraica y L un *cuerpo algebraicamente cerrado* Definimos el conjunto S_σ^E de extensiones de σ a un homomorfismo $E \to L$ como:

$$S_\sigma^E = \{\tau : E \longrightarrow L \text{ homomorfismo de cuerpos } \mid \tau|_K = \sigma\}$$

donde $\sigma : K \longrightarrow L$ es un homomorfismo de cuerpos fijado. Se llama **grado de separabilidad** de E sobre K (o de la extensión E/K) al cardinal $|S_\sigma^E|$. Denotaremos este grado de separabilidad por $[E : K]_s$.

Para que esta sea una buena definición matemática, el cardinal obtenido no debe depender de la elección del cuerpo L ni del homomorfismo inicial σ.

Proposición 4.1.1: Buena definición de $[E : K]_s$

Sea E/K una extensión algebraica. Entonces, el cardinal del conjunto de extensiones S_σ^E es el mismo para todos los homomorfismos de cuerpos $\sigma : K \to L$, asumiendo que L es un cuerpo algebraicamente cerrado.

Demostración. La demostración procede en cuatro fases lógicas.

Fase 1: Reducción del codominio a la clausura algebraica relativa. Nuestro objetivo inicial es demostrar que podemos restringir el cuerpo de llegada L a un subcuerpo más manejable sin alterar el conjunto S_σ^E.

Sea $\tau \in S_\sigma^E$ una extensión cualquiera. Tomemos un elemento arbitrario $\alpha \in E$. Como, por hipótesis, la extensión E/K es algebraica, existe un polinomio $P \in K[X]$ tal que $P(\alpha) = 0$. Al aplicar el homomorfismo τ a esta igualdad, obtenemos que $\tau(\alpha)$ es raíz del polinomio $\tau(P)$ que se obtiene aplicando τ a los coeficientes de P. Dado que los coeficientes de P pertenecen a K, y $\tau|_K = \sigma$, se sigue que $\tau(P) = \sigma(P) \in \sigma(K)[X]$.

Como esto es cierto para todo $\alpha \in E$, deducimos que la imagen completa $\tau(E)$ es algebraica sobre $\tau(K) = \sigma(K)$. Por la Proposición 2.3, la clausura algebraica de un cuerpo dentro de un cuerpo algebraicamente cerrado es, en sí misma, un cuerpo algebraicamente cerrado. Por tanto, podemos asumir a partir de ahora, sin pérdida de generalidad, que L es exactamente la clausura algebraica de $\sigma(K)$.

Fase 2: Consideración de un segundo homomorfismo y construcción del puente base. Para demostrar que el cardinal es independiente de σ y de L, supongamos la existencia de otro homomorfismo de cuerpos $\sigma' : K \to L'$, donde L' es otro cuerpo algebraicamente cerrado. Análogamente, asumimos que L' es la clausura algebraica de $\sigma'(K)$. Consideremos ahora la aplicación $\rho : \sigma(K) \to \sigma'(K)$ definida mediante la composición $\rho = \sigma' \circ \sigma^{-1}$.

Fase 3: Extensión del isomorfismo a las clausuras algebraicas. Aplicamos la Proposición 2.7 (Teorema de extensión de isomorfismos). Dado que L y L' son las clausuras algebraicas de $\sigma(K)$ y $\sigma'(K)$ respectivamente, existe un isomorfismo global $\lambda : L \to L'$ tal que $\lambda|_{\sigma(K)} = \rho$. Es decir, $\forall k \in K$, $\lambda(\sigma(k)) = \sigma'(k)$ (1).

Fase 4: Construcción de la biyección entre los conjuntos de extensiones. Procedemos a demostrar que $|S_\sigma^E| = |S_{\sigma'}^E|$ estableciendo una biyección explícita. Definimos la aplicación:

$$\Phi : S_\sigma^E \longrightarrow S_{\sigma'}^E, \quad \tau \mapsto \lambda \circ \tau$$

Buena definición de Φ*:* Debemos verificar que la imagen de τ reside efectivamente en $S_{\sigma'}^E$. Es decir, que $\lambda \circ \tau$ extiende a σ'. Sea $k \in K$. Evaluamos la composición:

$$(\lambda \circ \tau)(k) = \lambda(\tau(k))$$

Dado que $\tau \in S_\sigma^E$, sabemos que $\tau(k) = \sigma(k)$:

$$= \lambda(\sigma(k))$$

Aplicando la propiedad de extensión de λ demostrada en (1):

$$= \sigma'(k)$$

Por tanto, $\lambda \circ \tau$ es una extensión de σ', lo que confirma que está bien definida.

Biyectividad de Φ*:* Dado que λ es un isomorfismo de cuerpos, admite una aplicación inversa $\lambda^{-1} : L' \to L$. Esto nos permite definir la aplicación inversa de Φ:

$$\Psi : S_{\sigma'}^E \longrightarrow S_\sigma^E, \quad \tau' \mapsto \lambda^{-1} \circ \tau'$$

Un razonamiento análogo al anterior demuestra que Ψ está bien definida.

Habiendo establecido una biyección entre S_σ^E y $S_{\sigma'}^E$, concluimos innegablemente que ambos conjuntos tienen el mismo cardinal:

$$|S_\sigma^E| = |S_{\sigma'}^E|$$

Esto finaliza la demostración y nos permite definir unívocamente el grado de separabilidad $[E : K]_s$. □

Observación 4.1.1: NOTA: ¿Qué definición estamos usando de clausura?

La respuesta corta y directa es: En el contexto de esta demostración, son exactamente la misma cosa. Empieza siendo la primera interpretación que mencionas, y gracias a un teorema, se convierte automáticamente en la segunda. Vamos a desenredar esto con todo el rigor formal que requiere:

1. La Interpretación .A"(Clausura algebraica RELATIVA) Tu primera interpretación (.el conjunto de los elementos que son algebraicos sobre el cuerpo") es lo que formalmente se llama la clausura algebraica de un cuerpo F dentro de una extensión mayor L. Definición: Dado $F \subseteq L$, definimos $\Omega = \{x \in L \mid x \text{ es algebraico sobre } F\}$. *Problema de esta definición:* En general, este conjunto Ω no tiene por qué ser algebraicamente cerrado. (Por ejemplo, la clausura algebraica de $\mathbb{Q}$ en $\mathbb{R}$ son los reales algebraicos, pero a ese conjunto le falta la raíz de $X^2 + 1$, por lo que no es algebraicamente cerrado).

2. La Interpretación "B"(Clausura algebraica ABSOLUTA) Tu segunda interpretación (üna extensión algebraica del cuerpo que es algebraicamente cerrada") es la definición axiomática de lo que es una Çlausura Algebraicaçon mayúsculas (suele denotarse como $\overline{F}$). Es un cuerpo que cumple simultáneamente dos cosas:

1. Es extensión algebraica de la base.
2. Es algebraicamente cerrado.

La Magia de la Proposición 2.3 (El puente entre A y B) Aquí es donde los apuntes hacen la conexión magistral. Fíjate cómo procede la demostración paso a paso:

- **Construye usando A:** El texto dice está incluido en la clausura algebraica de $\sigma(K)$ en L. Aquí está usando tu primera interpretación pura y dura. Agarra el saco gigante L y filtra solo los elementos algebraicos sobre $\sigma(K)$. Llamemos a ese subconjunto Ω.
- **Aplica el Teorema (Prop 2.3):** El texto recuerda que nuestro L original de partida ya era, por hipótesis, algebraicamente cerrado. La Proposición 2.3 afirma que si el universo L es algebraicamente cerrado, entonces el subconjunto relativo Ω hereda esa propiedad y también es algebraicamente cerrado.
- **Llega a "B":** Como Ω es una extensión algebraica de $\sigma(K)$ (por construcción) y además es algebraicamente cerrado (por la Prop 2.3), entonces cumple perfectamente la definición de tu segunda interpretación.

Cálculo de $[K(\alpha) : K]_s$ para α algebraico sobre K

Ejemplo 4.1.1: Ejemplo 4.3: Grado de separabilidad de una extensión simple

Sea α algebraico sobre K. Sabemos que $[K(\alpha) : K] = \text{gr}(\text{Min}_K(\alpha))$, pero buscamos calcular específicamente su grado de separabilidad $[K(\alpha) : K]_s$.

Recordemos que, por definición, $[K(\alpha) : K]_s$ es el cardinal del conjunto de extensiones $S_\sigma^{K(\alpha)}$, el cual depende a priori de la elección de un cuerpo algebraicamente cerrado L y de un homomorfismo base $\sigma : K \to L$.

Fase 1: Elección del marco de trabajo óptimo. Como el grado de separabilidad es independiente del homomorfismo σ y de L (Proposición 4.2), tomamos los más "fáciles":

- $L = \overline{K}$ (la clausura algebraica absoluta de K).
- $\sigma =$ inclusión natural de K en $\overline{K}$.

Fase 2: Simplificación del conjunto de extensiones. Bajo estas elecciones, el conjunto queda:

$$S_\sigma^{K(\alpha)} = \{\tau : K(\alpha) \to \overline{K} \mid \tau \text{ es homomorfismo y } \tau|_K = \sigma\}$$

Como σ es la inclusión, la condición $\tau|_K = \sigma$ significa que $\tau(k) = k$ para todo $k \in K$, es decir, τ es un K-homomorfismo. Entonces, $[K(\alpha) : K]_s$ es simplemente el número de K-homomorfismos de $K(\alpha)$ a $\overline{K}$.

Fase 3: Restricción sobre la imagen del generador α. Sea $p(X) = \text{Min}_K(\alpha) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$ con $c_i \in K$. Sabemos que $p(\alpha) = 0$. Si tomamos $\tau \in S_\sigma^{K(\alpha)}$ y lo aplicamos a esta ecuación, usando que τ deja fijos los coeficientes $c_i \in K$, obtenemos:

$$(\tau(\alpha))^n + c_{n-1}(\tau(\alpha))^{n-1} + \cdots + c_0 = \tau(0) = 0$$

Esto equivale a $p(\tau(\alpha)) = 0$, lo que demuestra que $\tau(\alpha)$ está forzada a ser una raíz de $\text{Min}_K(\alpha)$ en $\overline{K}$.

Fase 4: Biyección mediante el Lema de Extensión. Por el Lema de Extensión (1.9), todo K-homomorfismo de $K(\alpha)$ en $\overline{K}$ queda unívocamente determinado por la imagen del generador α. Recíprocamente, si $\beta \in \overline{K}$ es cualquier raíz de $\text{Min}_K(\alpha)$, existe un isomorfismo $K(\alpha) \simeq K(\beta)$ que envía $\alpha \mapsto \beta$.

Por tanto, hemos establecido una biyección entre los K-homomorfismos y las raíces distintas de $\text{Min}_K(\alpha)$ en $\overline{K}$. Concluimos formalmente que:

$$[K(\alpha) : K]_s = \text{Número de raíces distintas de } \text{Min}_K(\alpha) \text{ en } \overline{K}$$

Proposición 4.1.2: Propiedad multiplicativa del grado de separabilidad (Prop 4.4)

Si $K \subseteq E \subseteq F$ es una torre de cuerpos, entonces:

$$[F : K]_s = [F : E]_s \cdot [E : K]_s$$

Demostración. Sea L un cuerpo algebraicamente cerrado y $\sigma : K \to L$ un homomorfismo. Consideremos los conjuntos de extensiones y sus cardinales respectivos:

- $|S_\sigma^E| = [E : K]_s$
- $|S_\sigma^F| = [F : K]_s$

Para cada homomorfismo $\tau \in S_\sigma^E$ (es decir, $\tau : E \to L$ con $\tau|_K = \sigma$), definimos el conjunto de sus extensiones a F:

$$S_\tau^F = \{\rho : F \to L \text{ homomorfismo} \mid \rho|_E = \tau\}$$

Por definición de separabilidad en la extensión F/E, el cardinal de este conjunto es $|S_\tau^F| = [F : E]_s$.

Si tomamos un $\rho \in \bigcup_{\tau \in S_\sigma^E} S_\tau^F$, existe un $\tau \in S_\sigma^E$ tal que $\rho|_E = \tau$. Como $\tau|_K = \sigma$, se cumple que $\rho|_K = (\rho|_E)|_K = \tau|_K = \sigma$. Por tanto, $\rho \in S_\sigma^F$. Esto prueba que $\bigcup_\tau S_\tau^F \subseteq S_\sigma^F$.

Recíprocamente, si tomamos cualquier $\rho \in S_\sigma^F$, podemos definir $\tau = \rho|_E$. Claramente $\tau|_K = \rho|_K = \sigma$, por lo que $\tau \in S_\sigma^E$. Y por definición, $\rho \in S_\tau^F$. Esto demuestra la igualdad de los conjuntos:

$$S_\sigma^F = \bigcup_{\tau \in S_\sigma^E} S_\tau^F$$

¿Es esta unión disjunta? Supongamos que un mismo homomorfismo ρ pertenece a la intersección $S_{\tau_1}^F \cap S_{\tau_2}^F$ para ciertos $\tau_1, \tau_2 \in S_\sigma^E$. Entonces, por definición, $\rho|_E = \tau_1$ y también $\rho|_E = \tau_2$. Esto implica trivialmente que $\tau_1 = \tau_2$. Por lo tanto, los conjuntos S_τ^F son disjuntos dos a dos cuando los τ son distintos.

Al ser una unión disjunta de conjuntos, el cardinal total es la suma de los cardinales de las partes:

$$|S_\sigma^F| = \sum_{\tau \in S_\sigma^E} |S_\tau^F|$$

Sustituyendo los cardinales que establecimos al inicio:

$$[F : K]_s = \sum_{\tau \in S_\sigma^E} [F : E]_s = |S_\sigma^E| \cdot [F : E]_s = [E : K]_s \cdot [F : E]_s$$

Lo que concluye la demostración. □

4.2. Homomorfismo de Frobenius y Multiplicidad de Raíces

Lema 4.2.1: Homomorfismo de Frobenius (Lema 4.5)

Sea K un cuerpo con característica $\mathrm{car}(K) = p > 0$. Entonces la aplicación $\varphi : K \longrightarrow K$ dada por $\varphi(x) = x^p$ es un homomorfismo de cuerpos, llamado **homomorfismo de Frobenius**.
Además, si K es algebraico sobre su cuerpo primo (por ejemplo, si K es un cuerpo finito), entonces φ es un automorfismo de K, conocido como el **Automorfismo de Frobenius**.

Demostración. Veamos primero que φ es un homomorfismo de cuerpos. Claramente $\varphi(1) = 1^p = 1$ y preserva el producto: $\varphi(ab) = (ab)^p = a^p b^p$. Para la suma, utilizamos el desarrollo del binomio de Newton:

$$(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$$

Como $\mathrm{car}(K) = p$, todos los coeficientes binomiales $\binom{p}{i}$ para $0 < i < p$ son múltiplos de p y, por tanto, se anulan en K. Así, la suma se reduce a los términos extremos: $\varphi(a + b) = (a + b)^p = a^p + b^p = \varphi(a) + \varphi(b)$. Al ser un homomorfismo entre cuerpos, φ es siempre inyectivo.

Para demostrar que es un automorfismo, solo falta ver que es suprayectivo (es decir, que todo elemento de K tiene una raíz p-ésima en K). Aquí utilizamos la hipótesis de que K es una extensión algebraica sobre su cuerpo primo, que en característica p es isomorfo a $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

Primero observamos que φ deja fijos a los elementos de $\mathbb{F}_p$. En efecto, por el Pequeño Teorema de Fermat, para todo $a \in \mathbb{F}_p$ se cumple $a^p \equiv a \pmod{p}$, lo que implica $a^p = a$. Por tanto, φ es un $\mathbb{F}_p$-homomorfismo y, dado que $\varphi(K) \subseteq K$, es un $\mathbb{F}_p$-endomorfismo de la extensión $K/\mathbb{F}_p$.

Dado que $K/\mathbb{F}_p$ es una extensión algebraica, y recordando que todo endomorfismo de una extensión algebraica es un automorfismo (ver Proposición auxiliar abajo), concluimos que φ es suprayectivo. Luego φ es un automorfismo. □

Proposición 4.2.1: Todo endomorfismo algebraico es automorfismo

Si E/K es una extensión algebraica y $\sigma : E \to E$ es un K-endomorfismo, entonces σ es un automorfismo.

Demostración. Como σ es un homomorfismo de cuerpos, es trivialmente inyectivo. Veamos que es suprayectivo. Sea $\alpha \in E$ un elemento cualquiera y consideremos su polinomio mínimo $p = \mathrm{Min}_K(\alpha)$ con $\mathrm{gr}(p) = n$. Por las propiedades elementales (Lema 1.8), cualquier K-homomorfismo permuta las raíces de un polinomio irreducible. Por tanto, la restricción de σ al conjunto (finito) de las raíces de p en E es una aplicación inyectiva de un conjunto finito en sí mismo, lo que fuerza a que sea biyectiva. Al ser biyectiva sobre las raíces, α debe ser forzosamente la imagen de alguna otra raíz bajo σ. Esto demuestra que σ es suprayectivo. □

Lema 4.2.2: Uniformidad de la multiplicidad (Lema 4.6)

Sea $f \in K[X]$ un polinomio irreducible:

1. Todas las raíces de f (en su cuerpo de descomposición) tienen exactamente la misma multiplicidad.
2. Si $\mathrm{car}(K) = 0$, entonces todas las raíces de f son simples.
3. Si $\mathrm{car}(K) = p > 0$, la multiplicidad de las raíces de f es una potencia de p. De hecho, es p^n si n es el mayor entero no negativo tal que $f(X) = g(X^{p^n})$ para algún polinomio $g \in K[X]$.

Demostración.

Observación 4.2.1: Preámbulo fundamental sobre derivadas:

Un polinomio $f \in K[X]$ tiene raíces múltiples si y solo si comparte raíces con su derivada f', es decir, si $\mathrm{mcd}(f, f') \neq 1$. Como f es irreducible por hipótesis, sus únicos divisores son 1 y él mismo. Por tanto, si tiene raíces múltiples, $\mathrm{mcd}(f, f') = f$, lo que significa que f divide a f'. Sin embargo, el grado de la derivada siempre es estrictamente menor: $\mathrm{gr}(f') < \mathrm{gr}(f)$. La única forma de que un polinomio divida a otro de grado menor es que el segundo sea el polinomio nulo. En conclusión: f tiene raíces múltiples $\iff f' = 0$.

Demostración de (1): Sean $\alpha_1, \ldots, \alpha_r$ las raíces distintas de f y m_i la multiplicidad de cada α_i. Podemos suponer sin pérdida de generalidad que f es mónico. En el cuerpo de descomposición factoriza como:

$$f(X) = (X - \alpha_1)^{m_1} \ldots (X - \alpha_r)^{m_r}$$

Por el Lema de Extensión, para cualquier par de raíces α_i, α_j, existe un K-homomorfismo $\sigma : K(\alpha_i) \to K(\alpha_j)$ tal que $\sigma(\alpha_i) = \alpha_j$. Como f tiene coeficientes en K, el homomorfismo deja invariante al polinomio: $\sigma(f) = f$. Pero al aplicar σ a la factorización lineal, obtenemos:

$$\sigma(f) = (X - \sigma(\alpha_1))^{m_1} \ldots (X - \sigma(\alpha_r))^{m_r}$$

Al sustituir $\sigma(\alpha_i) = \alpha_j$, vemos que el factor $(X - \alpha_j)$ ahora aparece con el exponente m_i. Por el Teorema de Factorización Única, los exponentes deben coincidir obligatoriamente, concluyendo que $m_i = m_j$.

(2): Queremos demostrar que $\text{car}(K) = 0 \implies f$ no tiene raíces múltiples.

Si $f(X) = X^n + \cdots + a_1X + a_0$, $n \geq 1$, $f'(X) = nX^{n-1} + \cdots + a_1$, como $\text{car}(K) = 0$, $nX^{n-1} \neq 0$

$$\implies f' \neq 0 \xrightarrow[\text{Preámbulo}]{} f \text{ tiene raíces simples}$$

(3): Sabemos que si $\text{car}(K) = p \neq 0$, un polinomio $f \in K[X]$ cumple $f' = 0 \iff$ los exponentes no nulos de f son múltiplos de p.

O sea, que si $f' = 0$, podemos .$^{\text{ex}}$traerüna potencia de p y escribir $f(X) = f_1(X^p)$

Si este nuevo polinomio cumple $f_1' = 0$, podemos seguir sacando .$^{\text{o}}$tra p" $f_1(X) = f_2(X^p)$

Por tanto, $f(X) = f_2(X^{p^2})$.

Al ser $\text{gr}(f) < \infty$, no podremos extraer potencias de p infinitamente. Sea $n \in \mathbb{Z}^+$ el mayor entero positivo (no-neg.) tal que $f(X) = g(X^{p^n})$ para algún $g \in K[X]$.

Observemos que $\text{gr}(f) = p^n \cdot \text{gr}(g) \implies p^n \leq \text{gr}(f) < \infty$

Se cumple que $\underline{g \text{ es irreducible}}$ (si no lo fuera, $g(X) = a(X)b(X) \implies g(X^{p^n}) = a(X^{p^n}) \cdot b(X^{p^n}) = f(X)$ **(!!)**)

Y también $g' \neq 0$ (pq si $g' = 0 \implies g(X) = h(X^p) \implies f(X) = h(X^{p^{n+1}})$ y esto no puede ocurrir pq habíamos elegido el $\underline{\text{mayor}}$ $n \in \mathbb{Z}^+$ que cumple esto)

Por tanto, como $g' \neq 0$ y g es irreducible $\implies$ sus raíces son simples.

Por otra parte, consideramos $\alpha_1, \alpha_2, \ldots, \alpha_k$ las distintas raíces de f en su cuerpo de descomposición. Se cumple $f(\alpha_i) = g(\alpha_i^{p^n}) = 0 \implies \alpha_i^{p^n}$ es raíz de g (vamos a demostrar que son justamente k)

Tendremos k raíces distintas también del polinomio g pq si $\alpha_1 \neq \alpha_2 \implies \alpha_1^{p^n} \neq \alpha_2^{p^n}$ ya que, por el Lema Anterior, el homomorfismo de Frobenius es una aplicación inyectiva. Veamos que estas son las únicas raíces de g.

Por reducción al absurdo, supongamos que g tuviera otras raíces adicionales $\beta_1, \ldots, \beta_l$

Como g no tiene raíces múltiples, $g(X) = (X - \alpha_1^{p^n}) \ldots (X - \alpha_k^{p^n})(X - \beta_1) \ldots (X - \beta_l)$

$\rightsquigarrow f(X) = (X^{p^n} - \alpha_1^{p^n}) \ldots (X^{p^n} - \alpha_k^{p^n})(X^{p^n} - \beta_1) \ldots (X^{p^n} - \beta_l)$

Fijemos un $(X^{p^n} - \beta_i)$. SPG supongamos que $i = 1$

El polinomio $(X^{p^n} - \beta_1)$ tiene una raíz (al menos) en el cuerpo de descomposición;

Si γ es la raíz en cuestión, se cumple $\gamma^{p^n} = \beta_1 \implies f(\gamma) = 0$.

O sea, γ es raíz de $f \implies \gamma = \alpha_i$ para algún $i \rightsquigarrow \alpha_i^{p^n} = \beta_1$ **(!!)**

Habíamos asumido que $\alpha_i^{p^n} \neq \beta_i \ \forall i$

Por tanto, $g(X) = (X - \alpha_1^{p^n}) \ldots (X - \alpha_k^{p^n}) \rightsquigarrow f(X) = (X^{p^n} - \alpha_1^{p^n}) \ldots (X^{p^n} - \alpha_k^{p^n})$

$$f(X) = (X-\alpha_1)^{p^n}\dots(X-\alpha_k)^{p^n} \implies \alpha_i \text{ tienen multiplicidad } p^n \ \forall i \in \{1,\dots,k\}$$

□

4.3. Grados de separabilidad e inseparabilidad

Definición 4.3.1: Grados de un polinomio irreducible (Def. 4.7)

Sea $f \in K[X]$ un polinomio irreducible. Se definen los siguientes grados asociados al polinomio:

- **Grado de separabilidad** ($\mathrm{gr}_s(f)$): Es el número exacto de raíces distintas que tiene el polinomio f en su cuerpo de descomposición.
- **Grado de inseparabilidad** ($\mathrm{gr}_i(f)$): Es la multiplicidad de cualquiera de sus raíces. (Recordemos por el Lema 4.6 que, al ser irreducible, todas las raíces de f tienen exactamente la misma multiplicidad).

Dado que el grado total del polinomio cuenta todas las raíces con su multiplicidad, se cumple trivialmente la relación:

$$\mathrm{gr}(f) = \mathrm{gr}_s(f)\cdot \mathrm{gr}_i(f)$$

Proposición 4.3.1: Proposición 4.8

Si α es un elemento algebraico sobre K, entonces el grado de separabilidad de la extensión simple generada por α coincide con el grado de separabilidad de su polinomio mínimo:

$$[K(\alpha):K]_s = \mathrm{gr}_s(\mathrm{Min}_K(\alpha))$$

(Esta proposición es una consecuencia directa del Ejemplo 4.3, donde establecimos la biyección entre los K-homomorfismos y las raíces distintas del polinomio mínimo en la clausura algebraica).

Proposición 4.3.2: Proposición 4.9

Si E/K es una extensión finita, entonces el grado de separabilidad $[E:K]_s$ divide al grado total de la extensión $[E:K]$.

Demostración. Razonamos por inducción sobre el grado de la extensión $n = [E:K]$.

Caso base ($n = 1$): Si $[E:K] = 1$, entonces trivialmente $E = K$. Como ya vimos, la definición del grado de separabilidad $[E:K]_s$ no depende del homomorfismo σ ni del cuerpo algebraicamente cerrado L. Tomamos las elecciones más sencillas: $L = \overline{K}$ y $\sigma = \mathrm{id}_K$. El conjunto de extensiones es:

$$S^E_\sigma = \{\tau : K \to \overline{K} \mid \tau \text{ es } K\text{-homomorfismo y } \tau|_K = \mathrm{id}_K\}$$

La única aplicación de K en sí mismo que deja fijo a K es la propia identidad ($\tau(x) = x \implies \tau = \mathrm{id}$). Por lo tanto, $|S^E_\sigma| = 1$, lo que implica que $[K:K]_s = 1$. Evidentemente, 1 divide a 1.

Paso inductivo ($n > 1$): Supongamos que la proposición es cierta para cualquier extensión cuyo grado sea estrictamente menor que n. Como $n > 1$, los cuerpos no son iguales ($K \subsetneq E$). Por tanto, podemos tomar un elemento $\alpha \in E \setminus K$. Esto nos permite construir la siguiente torre de cuerpos intermedia:

Por la fórmula de los grados en torres de cuerpos (Corolario 1.12), tenemos:

$$[E : K] = [E : K(\alpha)] \cdot [K(\alpha) : K]$$

Como $\alpha \notin K$, sabemos que $[K(\alpha) : K] > 1$. En consecuencia, el grado del tramo superior debe ser estrictamente menor que el total: $[E : K(\alpha)] < n$.

Por la **hipótesis de inducción**, sabemos que $[E : K(\alpha)]_s$ divide a $[E : K(\alpha)]$. Esto significa que existe un entero $k \geq 1$ tal que:

$$[E : K(\alpha)] = k \cdot [E : K(\alpha)]_s \quad \text{— (Ec. 1)}$$

Por otro lado, consideremos el tramo inferior $K(\alpha)/K$. Sea $p = \mathrm{Min}_K(\alpha)$. Dado que es una extensión finita y α es algebraico, sabemos que el grado de la extensión coincide con el grado del polinomio mínimo:

$$[K(\alpha) : K] = \mathrm{gr}(p)$$

Utilizando la Definición 4.7 y la Proposición 4.8, podemos descomponer este grado:

$$[K(\alpha) : K] = \mathrm{gr}(p) = \mathrm{gr}_s(p) \cdot \mathrm{gr}_i(p) = [K(\alpha) : K]_s \cdot \mathrm{gr}_i(p) \quad \text{— (Ec. 2)}$$

Ahora, sustituimos (Ec. 1) y (Ec. 2) en la fórmula general de los grados de la torre:

$$[E : K] = \underbrace{(k \cdot [E : K(\alpha)]_s)}_{[E:K(\alpha)]} \cdot \underbrace{([K(\alpha) : K]_s \cdot \mathrm{gr}_i(p))}_{[K(\alpha):K]}$$

Reordenando los factores obtenemos:

$$[E : K] = k \cdot \mathrm{gr}_i(p) \cdot \Big([E : K(\alpha)]_s \cdot [K(\alpha) : K]_s\Big)$$

Por la Proposición 4.4 (Propiedad multiplicativa del grado de separabilidad), el término entre paréntesis es exactamente el grado de separabilidad total $[E : K]_s$. Sustituyendo esto, llegamos a:

$$[E : K] = \Big(k \cdot \mathrm{gr}_i(p)\Big) \cdot [E : K]_s$$

Dado que tanto k como $\mathrm{gr}_i(p)$ son enteros, hemos demostrado que $[E : K]_s$ divide a $[E : K]$, completando así la inducción. □

Definición 4.3.2: Grado de inseparabilidad de una extensión

Como consecuencia directa de la Proposición 4.9, para cualquier extensión finita E/K, se define el **grado de inseparabilidad** (denotado como $[E : K]_i$) como el cociente exacto entre el grado de la extensión y su grado de separabilidad:

$$[E : K]_i = \frac{[E : K]}{[E : K]_s}$$

Equivalentemente, se cumple siempre la factorización global: $[E : K] = [E : K]_s \cdot [E : K]_i$.

4.3.1. Tipos de separabilidad

La noción de separabilidad se puede aplicar a polinomios, a elementos individuales y a extensiones completas. Las definiciones formales son las siguientes:

Definición 4.3.3: Separabilidad (Def. 4.10)

1. **Polinomio separable:** Un polinomio $f \in K[X]$ es separable si no tiene raíces múltiples en su cuerpo de descomposición (ni en ninguna otra extensión de K). Analíticamente, esto equivale a afirmar que el polinomio es coprimo con su derivada formal: $\mathrm{mcd}(f, f') = 1$.

2. **Elemento separable:** Un elemento α perteneciente a una extensión de K es separable sobre K si cumple dos condiciones:

   - Es algebraico sobre K.
   - Su polinomio mínimo $\mathrm{Min}_K(\alpha)$ es un polinomio separable.

   Nota analítica: Decir que α es separable equivale a decir que su extensión simple es totalmente separable: $[K(\alpha) : K]_s = [K(\alpha) : K]$, o lo que es lo mismo, su grado de inseparabilidad es trivial ($[K(\alpha) : K]_i = 1$).

3. **Extensión separable:** Una extensión L/K es separable si *todos* los elementos de L son separables sobre K. (Como consecuencia inmediata de la definición anterior, toda extensión separable debe ser, por fuerza, una extensión algebraica).

4. **Extensión puramente inseparable:** Una extensión L/K es puramente inseparable si los únicos elementos de L que son separables sobre K son precisamente los elementos que ya pertenecen al cuerpo base K.

Observación 4.3.1:

Si $\mathrm{car}(K) = 0$, entonces toda extensión de K es separable.
Como vimos anteriormente, en característica cero la derivada de un polinomio irreducible nunca es nula, por lo que los polinomios irreducibles no pueden tener raíces múltiples. Por consiguiente, todo elemento algebraico sobre un cuerpo de característica cero es automáticamente separable.

Teorema 4.3.1: Equivalencias de separabilidad (Teorema 4.12)

Las siguientes afirmaciones son equivalentes para una extensión finita L/K:

1. L/K es separable.
2. $[L : K] = [L : K]_s$.
3. $[L : K]_i = 1$.

Demostración. **(2) $\iff$ (3):** Es obvio por la propia definición del grado de inseparabilidad: $[L : K]_i = \frac{[L:K]}{[L:K]_s}$. Que este cociente sea 1 equivale a que el numerador y el denominador sean iguales.

(2) $\implies$ (1): Supongamos que $[L:K]=[L:K]_s$. Queremos ver que todo elemento de L es separable sobre K. Sea $\alpha \in L$ un elemento arbitrario y denotemos $E=K(\alpha)$. Consideramos la torre de cuerpos $K \subseteq E \subseteq L$. Por la fórmula de grados y la propiedad multiplicativa del grado de separabilidad (Prop. 4.9), se tiene:

$$[L:E]\cdot[E:K]=[L:K]=[L:K]_s=[L:E]_s\cdot[E:K]_s$$

Sabemos que el grado de separabilidad siempre divide al grado de la extensión, es decir, $[L:E]_s \leq [L:E]$ y $[E:K]_s \leq [E:K]$. Para que el producto de los grados de separabilidad sea igual al producto de los grados totales, es algebraicamente necesario que las igualdades se den factor a factor. Por tanto, se deduce forzosamente que:

$$[E:K]=[E:K]_s$$

Sustituyendo E, obtenemos $[K(\alpha):K]=[K(\alpha):K]_s$. Esto significa que α es separable sobre K. Como α era arbitrario, concluimos que L/K es una extensión separable.

(1) $\implies$ (2): Supongamos que L/K es separable. Razonamos por inducción sobre $n=[L:K]$.

- **Caso base ($n=1$):** Si $[L:K]=1$, entonces $L=K$ y trivialmente $[K:K]=1=[K:K]_s$.
- **Paso inductivo:** Supongamos que $n>1$ y que la hipótesis de inducción se cumple para extensiones de grado estrictamente menor. Sea $\alpha \in L \setminus K$. Dado cualquier otro elemento $\beta \in L$, su polinomio mínimo sobre $K(\alpha)$, es decir $\mathrm{Min}_{K(\alpha)}(\beta)$, divide a su polinomio mínimo sobre K, $\mathrm{Min}_K(\beta)$, en el anillo $K(\alpha)[X]$. Como L/K es separable, β es separable sobre K, luego $\mathrm{Min}_K(\beta)$ no tiene raíces múltiples. Al ser un divisor, $\mathrm{Min}_{K(\alpha)}(\beta)$ tampoco tiene raíces múltiples, lo que implica que β es separable sobre $K(\alpha)$. Como esto vale para cualquier $\beta \in L$, la extensión $L/K(\alpha)$ es separable.

  Además, por la fórmula de la torre: $[L:K]=[L:K(\alpha)]\cdot[K(\alpha):K]$. Como $\alpha \notin K$, $[K(\alpha):K]>1$, lo que implica que $[L:K(\alpha)]<n$. Podemos aplicar la hipótesis de inducción a la extensión $L/K(\alpha)$, obteniendo que $[L:K(\alpha)]=[L:K(\alpha)]_s$. Por otra parte, como $\alpha \in L$ y L/K es separable, α es separable sobre K, por lo que $[K(\alpha):K]=[K(\alpha):K]_s$.

  Multiplicando ambas igualdades:

  $$[L:K]=[L:K(\alpha)]\cdot[K(\alpha):K]=[L:K(\alpha)]_s\cdot[K(\alpha):K]_s=[L:K]_s$$

  Lo que completa la inducción.

□

Corolario 4.3.1: Multiplicatividad de la clase de extensiones separables (Corolario 4.13)

Sea $K \subseteq E \subseteq L$ una torre de cuerpos. La extensión L/K es separable si y solo si las extensiones E/K y L/E son separables.

Demostración. **($\implies$) Supongamos que L/K es separable:** Claramente E/K es separable, porque todo elemento de E pertenece a L, y por hipótesis todos los elementos de L son separables sobre K. Falta ver que L/E es separable. Si tomamos $\alpha \in L$, sabemos que $\mathrm{Min}_E(\alpha)$ divide a $\mathrm{Min}_K(\alpha)$. Como α es separable sobre K, $\mathrm{Min}_K(\alpha)$ no tiene raíces múltiples. En consecuencia, su divisor $\mathrm{Min}_E(\alpha)$ tampoco tiene raíces múltiples. Por tanto, α es separable sobre E, lo que demuestra que L/E es separable.

($\Longleftarrow$) Supongamos que L/E y E/K son separables: Queremos demostrar que L/K es separable. Sea $\alpha \in L$. Como L/E es separable, α es algebraico sobre E. Sea $p = \mathrm{Min}_E(\alpha)$. Al ser separable, p no tiene raíces múltiples, es decir, $\mathrm{gr}(p) = \mathrm{gr}_s(p)$.

(La sutileza inmensa): El Teorema 4.12 requiere que la extensión sea **finita** para poder relacionar la separabilidad con la igualdad de grados. Como no sabemos si la torre $L/E/K$ es infinita, tenemos que construir un andamio finito a medida para α.

Sean A los coeficientes del polinomio p, y definamos el cuerpo intermedio $F = K(A)$. Entonces construimos la subtorre $K \subseteq F \subseteq F(\alpha) \subseteq L$.

Dado que $F \subseteq E$, el polinomio $p \in F[X]$ sigue siendo irreducible sobre F (porque lo era sobre un cuerpo más grande E). Por tanto, $p = \mathrm{Min}_F(\alpha)$. Como p no tiene raíces múltiples, α es separable sobre F, lo que implica que $[F(\alpha) : F] = [F(\alpha) : F]_s$.

Por otro lado, la extensión F/K es **finita** (porque hemos adjuntado un número finito de elementos, los coeficientes de p, que son algebraicos sobre K). Como $F \subseteq E$ y E/K es separable, F/K es una extensión finita y separable. Aplicando el Teorema 4.12, sabemos que $[F : K] = [F : K]_s$.

Usando la propiedad multiplicativa de los grados totales y de los grados de separabilidad:

$$[F(\alpha) : K] = [F(\alpha) : F] \cdot [F : K] = [F(\alpha) : F]_s \cdot [F : K]_s = [F(\alpha) : K]_s$$

Como $[F(\alpha) : K] = [F(\alpha) : K]_s$, deducimos que la extensión $F(\alpha)/K$ es separable. En particular, $\alpha \in F(\alpha)$ es separable sobre K. Al ser α un elemento cualquiera de L, concluimos que toda la extensión L/K es separable. □

Corolario 4.3.2: Corolario 4.14

Si $L = K(A)$ y todos los elementos del conjunto A son separables sobre K, entonces la extensión L/K es separable.

Demostración. Sea $\alpha \in L = K(A)$ un elemento cualquiera. Por la definición de cuerpo generado, α puede expresarse utilizando un número finito de elementos de A. Es decir, $\exists B \subseteq A$ con B finito, tal que $\alpha \in K(B)$. Podemos suponer que $B = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$, donde cada α_i es separable sobre K.

Consideremos la torre de cuerpos sucesivos:

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \dots, \alpha_k) = K(B)$$

Como α_1 es separable sobre K, $K(\alpha_1)/K$ es separable. Para el siguiente paso, α_2 es separable sobre K, luego su polinomio mínimo sobre $K(\alpha_1)$ divide a su polinomio mínimo sobre K, por lo que α_2 también es separable sobre $K(\alpha_1)$. Esto hace que $K(\alpha_1, \alpha_2)/K(\alpha_1)$ sea separable.

Aplicando el Corolario 4.13 reiteradamente (inducción sobre k), deducimos que toda la extensión $K(B)/K$ es separable. Como $\alpha \in K(B)$, α es separable sobre K. Al ser α un elemento arbitrario de L, la extensión completa L/K es separable.

Observación 4.3.2: Conclusión del paso inductivo final

Para formalizar el paso inductivo final, observemos que α_n es separable sobre el cuerpo intermedio $K(\alpha_1, \ldots, \alpha_{n-1})$. Esto se justifica porque el polinomio mínimo sobre la extensión, $\mathrm{Min}_{K(\alpha_1,\ldots,\alpha_{n-1})}(\alpha_n)$, divide al polinomio mínimo sobre el cuerpo base, $\mathrm{Min}_K(\alpha_n)$. Como α_n es separable sobre K, sabemos que $\mathrm{Min}_K(\alpha_n)$ no tiene raíces múltiples. En consecuencia, su divisor tampoco las tiene, haciendo que α_n sea separable sobre $K(\alpha_1, \ldots, \alpha_{n-1})$. Razonando por inducción y usando que la separabilidad es multiplicativa, llegamos a que $E = K(\alpha_1, \ldots, \alpha_n)$ es una extensión separable sobre K. □

□

Corolario 4.3.3: Clausura separable (Corolario 4.15)

Sea L/K una extensión de cuerpos. El conjunto:

$$A = \{\alpha \in L \mid \alpha \text{ es separable sobre } K\}$$

es un subcuerpo de L que contiene a K. A este subcuerpo A se le llama la **clausura separable** de K en L.

Demostración. Denotemos por A a dicho conjunto. Por definición, todo elemento de A es separable sobre K. Si aplicamos el Corolario 4.14 tomando a A como el conjunto generador, deducimos que la extensión generada $K(A)/K$ es una extensión separable. Dado que toda la extensión es separable, cualquier elemento que pertenezca a $K(A)$ es separable sobre K. Esto implica, por la propia definición del conjunto A, que $K(A) \subseteq A$. Por otro lado, la inclusión contraria $A \subseteq K(A)$ es obvia (todo conjunto está trivialmente contenido en el cuerpo que genera). Por tanto, concluimos que $A = K(A)$. Al coincidir con un cuerpo generado, A es indiscutiblemente un subcuerpo de L. □

Corolario 4.3.4: Levantamiento de extensiones (Corolario 4.16)

La clase de extensiones separables es cerrada para levantamientos.

Demostración. Sean E y L dos extensiones sobre un mismo cuerpo base K. El "levantamiento"de E a L se define como el cuerpo compuesto EL. La situación se ilustra en el siguiente diagrama: Supongamos que la extensión base E/K es separable. Queremos demostrar que el levantamiento EL/L también es separable.

Dado que E/K es separable, todo elemento $\alpha \in E$ es separable sobre K. Consideremos el polinomio mínimo de este elemento sobre L, es decir, $\mathrm{Min}_L(\alpha)$, y su polinomio mínimo sobre K, $\mathrm{Min}_K(\alpha)$. Como $K \subseteq L$, se cumple que $\mathrm{Min}_L(\alpha)$ divide a $\mathrm{Min}_K(\alpha)$ en el anillo de polinomios $L[X]$. Al ser α separable sobre K, sabemos que $\mathrm{Min}_K(\alpha)$ no tiene raíces múltiples. En consecuencia, su divisor $\mathrm{Min}_L(\alpha)$ tampoco puede tener raíces múltiples, lo que demuestra inequívocamente que α es separable sobre L.

Hemos probado que todos los elementos de E son separables sobre L. Recordemos que el cuerpo compuesto EL es exactamente el cuerpo generado $L(E)$. Como está generado por un conjunto de elementos (E) que son todos separables sobre L, el Corolario 4.14 nos garantiza que la extensión generada $\frac{L(E)}{L} = \frac{EL}{L}$ es separable. □

Corolario 4.3.5: Grado de la clausura separable (Corolario 4.18)

Si L/K es una extensión finita y S es la clausura separable de K en L (es decir, el subcuerpo de los elementos separables), entonces se cumple la igualdad:

$$[L : K]_s = [S : K]$$

Capítulo 5

Extensiones de Galois

5.1. La correspondencia de Galois

Definición 5.1.1: Homomorfismos de extensiones

Dadas $K \subseteq L_1, L_2$ extensiones.
Si L_1 y L_2 son dos extensiones de K, entonces un **homomorfismo** de L_1/K en L_2/K (también llamado K-homomorfismo) es un homomorfismo de cuerpos $f : L_1 \to L_2$ tal que $f(a) = a$ para todo $a \in K$.
Un **endomorfismo** de una extensión L/K es un homomorfismo de L/K en sí misma. Un **isomorfismo** de extensiones (o K-isomorfismo) es un homomorfismo de extensiones que es isomorfismo de cuerpos y un **automorfismo** de extensiones (o K-automorfismo) es un isomorfismo de una extensión de K en sí misma.

Definición 5.1.2: Grupo de Galois

El **grupo de Galois** de L/K es el conjunto de K-automorfismos de L/K con la composición de aplicaciones.
Lo denotamos por $\mathrm{Gal}(L/K)$.

Definición 5.1.3: Subextensión

Una **subextensión** de L/K es un cuerpo M tal que $K \subseteq M \subseteq L$.
Recordemos que $\mathrm{Sub}(L/K)$ denota el conjunto de las subextensiones de L/K.

Definición 5.1.4: Extensiones admisibles

Dos extensiones L_1/K y L_2/K son **admisibles** si existe un cuerpo L tal que $L_1 \subseteq L$ y $L_2 \subseteq L$.

Observación 5.1.1: Convenios y propiedades básicas

En todo momento supondremos $1 \neq 0 \implies$ Todos los homomorfismos entre cuerpos son inyectivos. Además, los K-homomorfismos son homomorfismos de K-espacios vectoriales. De esta forma siempre que exista un homomorfismo de cuerpos $f : K \to L$, el cuerpo L contiene un subcuerpo isomorfo a K, la imagen $f(K)$ de f. Por otro lado K admite una

extensión isomorfa a L, a saber el conjunto $K \cup (L \setminus f(K))$, en el que se define el producto de la forma obvia.
Abusaremos a menudo de la notación y cada vez que tengamos un homomorfismo de cuerpos $f : K \to L$, simplemente consideraremos K como subcuerpo de L, identificando los elementos de K y $f(K)$, a través de f.
De aquí tenemos que, si $f : K \to L$ es un homomorfismo de cuerpos:

Observación 5.1.2:

1. $f(K) \simeq K$ (como cuerpos). A veces simplemente escribiremos K para referirnos a $f(K)$.
2. Por convenio, K es subcuerpo de L identificando K con $f(K)$.

Lema 5.1.1: Propiedades de los homomorfismos sobre raíces

1. Sean $\sigma : E \to L$ un homomorfismo de cuerpos y $p \in E[X]$. Si α es una raíz de p en E, entonces $\sigma(\alpha)$ es una raíz de $\sigma(p)$.
   - *Nota:* Esto asegura que la propiedad de ser algebraicamente cerrado es invariante bajo isomorfismos.
2. Si E/K y L/K son extensiones de un cuerpo K, $p \in K[X]$ y σ es un K-homomorfismo, entonces σ se restringe a una aplicación inyectiva del conjunto de las raíces de p en E al conjunto de las raíces de p en L.
3. En particular, si $E = L$ (es decir, si $\sigma \in \mathrm{Gal}(L/K)$), entonces esta restricción de σ es una permutación del conjunto de las raíces de p en L.

Ejemplo 5.1.1: Algunas extensiones con grupo trivial

Claramente $\mathrm{Gal}(K/K) = 1$, pero no son éstas las únicas extensiones con grupo de Galois trivial.
Por ejemplo, si a es un número racional positivo que no es el cubo de un número racional, entonces $p = X^3 - a$ es irreducible en $\mathbb{Q}[X]$. Las raíces de p son $\alpha = \sqrt[3]{a}$, $\omega\alpha$ y $\omega^2\alpha$, donde ω es una raíz tercera primitiva de la unidad. Como ω no es un número real, la única raíz de p que pertenece a $\mathbb{Q}(\alpha)$ es α y por tanto $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = 1$ (¿por qué?).

Observación 5.1.3: Justificación del Ejemplo 1

Cualquier K-automorfismo $\sigma \in \mathrm{Gal}(K(\alpha)/K)$ está completamente determinado por la imagen del generador de la extensión, es decir, por $\sigma(\alpha)$.
Además, los homomorfismos de cuerpos preservan las raíces de los polinomios con coeficientes en el cuerpo base. Como α es raíz de $p \in K[X]$, su imagen $\sigma(\alpha)$ debe ser obligatoriamente otra raíz de p.
Por tanto, las únicas opciones teóricas son $\sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}$. Sin embargo, σ es un endomorfismo de $K(\alpha)$, lo que exige que $\sigma(\alpha) \in K(\alpha)$. Dado que $a > 0$ es racional, podemos considerar $K(\alpha) \subset \mathbb{R}$. Como $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \notin \mathbb{R}$, se sigue que $\omega\alpha \notin \mathbb{R}$ y $\omega^2\alpha \notin \mathbb{R}$, por lo que ninguna de estas dos raíces pertenece a $K(\alpha)$. La única asignación bien definida y posible es $\sigma(\alpha) = \alpha$, lo que implica que σ es la aplicación identidad.

Ejemplo 5.1.2: Extensiones de grado 2

Si L/K es una extensión de grado 2 y $\mathrm{car}(K) \neq 2$, entonces $|\,\mathrm{Gal}(L/K)| = 2$.
¿Por qué ocurre esto? Si $\alpha \in L \setminus K$, entonces $L = K(\alpha)$ y por tanto $p = \mathrm{Min}_K(\alpha)$ tiene grado 2. Pongamos $p = X^2 + aX + b = \left(X + \frac{a}{2}\right)^2 + b - \frac{a^2}{4}$
Para simplificar el estudio de la extensión, realizamos un cambio de variable para eliminar el término en X:

$$p(X) = X^2 + aX + b = \left(X + \frac{a}{2}\right)^2 + \underbrace{b - \frac{a^2}{4}}_{-c}$$

Definimos un nuevo generador $\beta = \alpha + \frac{a}{2}$. Como $\frac{a}{2} \in K$, se tiene que $K(\alpha) = K(\beta)$. El polinomio mínimo de β es ahora mucho más sencillo: $q(X) = X^2 - c$. Sus raíces son simplemente $\pm\beta$.
¿Por qué el grupo de Galois tiene orden 2? Cualquier K-automorfismo σ debe enviar una raíz de $q(X)$ a otra raíz de $q(X)$.

- **Opción 1:** $\sigma(\beta) = \beta$. Esto define la aplicación identidad id_L.
- **Opción 2:** $\sigma(\beta) = -\beta$. Esto define un automorfismo no trivial (análogo a la conjugación compleja).

Observación 5.1.4: Justificación del Ejemplo 2

Para asegurar que efectivamente tiene *exactamente* dos elementos, debemos garantizar que las dos opciones teóricas ($\sigma(\beta) = \beta$ y $\sigma(\beta) = -\beta$) generan automorfismos distintos y bien definidos.
Primero, comprobamos que son distintos: como $\mathrm{car}(K) \neq 2$, se cumple que $2\beta \neq 0$ (ya que $\beta \notin K \implies \beta \neq 0$), por lo que $\beta \neq -\beta$. Segundo, comprobamos que ambas opciones dan lugar a automorfismos válidos: L es el cuerpo de escisión del polinomio $X^2 - c$ sobre K. Al ser irreducible y tener raíces simples (es separable por ser de característica distinta de 2), la teoría elemental de extensiones asegura que por cada raíz en el cuerpo de escisión existe un K-automorfismo que envía el generador a dicha raíz. Por consiguiente, existe el automorfismo identidad ($\beta \mapsto \beta$) y un automorfismo no trivial ($\beta \mapsto -\beta$), formando un grupo de Galois de orden 2.

Ejemplo 5.1.3: Automorfismos en extensiones de $\mathbb{R}$

Como un automorfismo de $\mathbb{R}$ ha de ser una aplicación creciente (¿por qué?), necesariamente $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = 1$ y por tanto $\mathrm{Gal}(\mathbb{R}/K) = 1$ para todo subcuerpo K de $\mathbb{R}$ (¿por qué?). De hecho, el único automorfismo de $\mathbb{R}$ es la identidad (¿por qué?).

Observación 5.1.5: Justificación del Ejemplo 3

Vamos a responder a las tres preguntas secuencialmente:

1. **¿Por qué ha de ser creciente?** Sea $\sigma \in \mathrm{Aut}(\mathbb{R})$. Todo número real positivo $x > 0$ admite una raíz cuadrada real, es decir, $x = (\sqrt{x})^2$. Al aplicar σ, obtenemos $\sigma(x) = \sigma((\sqrt{x})^2) = (\sigma(\sqrt{x}))^2$. Un cuadrado en $\mathbb{R}$ es siempre positivo o cero. Como σ es un automorfismo (y por tanto inyectivo, enviando $0 \mapsto 0$), para $x > 0$ se tiene estrictamente que $\sigma(x) > 0$. Si tomamos $a < b$, entonces $b - a > 0$. Por la propiedad

anterior, $\sigma(b-a) > 0$, y por linealidad $\sigma(b) - \sigma(a) > 0$, lo que implica $\sigma(a) < \sigma(b)$. Por lo tanto, σ preserva el orden estrictamente.

2. **¿Por qué el único automorfismo es la identidad?** Sabemos que todo automorfismo fija el cuerpo primo; por tanto, $\sigma(q) = q$ para todo $q \in \mathbb{Q}$. Sea $x \in \mathbb{R}$ un número irracional. Por la densidad de $\mathbb{Q}$ en $\mathbb{R}$, podemos acotarlo entre dos sucesiones de racionales tales que $q_1 < x < q_2$. Dado que σ es creciente (como demostramos arriba), preserva estas desigualdades: $\sigma(q_1) < \sigma(x) < \sigma(q_2)$. Como σ fija los racionales, esto se traduce en $q_1 < \sigma(x) < q_2$. Al tomar el límite cuando q_1 y q_2 tienden a x, por el Teorema del Sandwich (o encaje de intervalos), obtenemos forzosamente que $\sigma(x) = x$. Por tanto, σ es la identidad en todo $\mathbb{R}$.

3. **¿Por qué** $\mathrm{Gal}(\mathbb{R}/K) = 1$**?** El grupo $\mathrm{Gal}(\mathbb{R}/K)$ está formado por los automorfismos de $\mathbb{R}$ que fijan K. Pero acabamos de demostrar que el único automorfismo general de $\mathbb{R}$ (es decir, el único elemento de $\mathrm{Aut}(\mathbb{R})$) es la identidad. Por tanto, exijamos que fije K o que fije $\mathbb{Q}$, el único candidato posible sigue siendo la aplicación identidad.

Ejemplo 5.1.4:

Sean $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Entonces $\sigma(\sqrt{2}) = \pm\sqrt{2}$ y $\sigma(\sqrt{3}) = \pm\sqrt{3}$ y por tanto $\mathrm{Gal}(K/\mathbb{Q})$ tiene a lo sumo 4 elementos. De hecho $\mathrm{Gal}(K/\mathbb{Q})$ tiene exactamente cuatro elementos. En efecto, en el Ejemplo (2) hemos visto que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ tiene 2 elementos. Por otro lado $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Por tanto, $K/\mathbb{Q}(\sqrt{2})$ es una extensión separable (¿por qué?) de grado 2, con lo que cada uno de los dos elementos de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ tiene dos extensiones a un homomorfismo de K en una clausura algebraica de K que, como además $K/\mathbb{Q}$ es normal (¿por qué?), estas dos extensiones son elementos de $\mathrm{Gal}(K/\mathbb{Q})$. Por tanto $\mathrm{Gal}(K/\mathbb{Q})$ tiene cuatro elementos: $\sigma_{++}, \sigma_{+-}, \sigma_{-+}, \sigma_{--}$ dados por $\sigma_{ab}(\sqrt{2}) = a\sqrt{2}$ y $\sigma_{ab}(\sqrt{3}) = b\sqrt{3}$.

Observación 5.1.6: Justificación del Ejemplo 4

1. **¿Por qué** $K/\mathbb{Q}(\sqrt{2})$ **es separable?** Esta extensión se obtiene adjuntando $\sqrt{3}$, cuyo polinomio mínimo sobre $\mathbb{Q}(\sqrt{2})$ es divisor de $X^2 - 3$. Estamos trabajando sobre una extensión de $\mathbb{Q}$, lo que significa que el cuerpo base tiene característica cero. Todo polinomio irreducible sobre un cuerpo de característica cero es separable (sus derivadas formales nunca son nulas), por lo que toda extensión algebraica en característica cero es automáticamente separable.

2. **¿Por qué** $K/\mathbb{Q}$ **es normal?** Una extensión finita es normal si y solo si es el cuerpo de escisión de algún polinomio sobre el cuerpo base. En este caso, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ contiene todas las raíces del polinomio $f(X) = (X^2-2)(X^2-3) \in \mathbb{Q}[X]$, y de hecho es generado por ellas. Al ser cuerpo de escisión, la extensión es normal.

Ejemplo 5.1.5:

Sea ξ una raíz n-ésima primitiva de la unidad y sea $L = K(\xi)/K$ una extensión ciclotómica. Si $\sigma \in \mathrm{Gal}(L/K)$, entonces $\sigma(\xi) = \xi^i$ para algún entero i coprimo con n, y σ está completamente determinada por el resto de i módulo n. Por tanto, tenemos una aplicación $\psi : \mathrm{Gal}(L/K) \to \mathbb{Z}_n^*$ que asocia $\sigma \in \mathrm{Gal}(L/K)$ con la única clase en $\mathbb{Z}_n^*$ que contiene a

i (con $\sigma(\xi) = \xi^i$). Entonces ψ es un homomorfismo inyectivo de grupos (comprobarlo) y por tanto $\mathrm{Gal}(L/K)$ es isomorfo a un subgrupo de $\mathbb{Z}_n^*$. En particular, el grupo de Galois de toda extensión ciclotómica es abeliano. Si además $K = \mathbb{Q}$, entonces $\mathrm{Min}_{\mathbb{Q}}(\xi) = \Phi_n$, el n-ésimo polinomio ciclotómico (Teorema 3.9). Por tanto, para cada i coprimo con n existe un elemento $\sigma \in \mathrm{Gal}(L = \mathbb{Q}(\xi)/\mathbb{Q})$ con $\sigma(\xi) = \xi^i$. En otras palabras, $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ es isomorfo a $\mathbb{Z}_n^*$ y un isomorfismo $\tau : \mathbb{Z}_n^* \to \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ viene dado asociando $i \in \mathbb{Z}_n^*$ con el único automorfismo τ_i de $\mathbb{Q}(\xi)$ tal que $\tau_i(\xi) = \xi^i$.

Observación 5.1.7: Justificación del Ejemplo 5

Comprobación de que ψ es un homomorfismo inyectivo:
Primero, veamos que respeta la operación del grupo (la composición). Sean $\sigma, \tau \in \mathrm{Gal}(L/K)$. Supongamos que $\psi(\sigma) = [i]$ y $\psi(\tau) = [j]$, lo que significa por definición que $\sigma(\xi) = \xi^i$ y $\tau(\xi) = \xi^j$. Calculemos la imagen de ξ bajo la composición $\sigma \circ \tau$:

$$(\sigma \circ \tau)(\xi) = \sigma(\tau(\xi)) = \sigma(\xi^j)$$

Como σ es un homomorfismo de cuerpos, preserva los exponentes:

$$\sigma(\xi^j) = (\sigma(\xi))^j = (\xi^i)^j = \xi^{ij}$$

Esto nos dice que el automorfismo composición $\sigma \circ \tau$ eleva ξ a la potencia ij. Por tanto, $\psi(\sigma \circ \tau) = [ij] = [i][j] = \psi(\sigma)\psi(\tau)$ en el grupo multiplicativo $\mathbb{Z}_n^*$. Esto demuestra que ψ es un homomorfismo.
Segundo, evaluemos la inyectividad estudiando el núcleo. Supongamos que $\sigma \in \ker(\psi)$. Esto significa que $\psi(\sigma)$ es el elemento neutro de $\mathbb{Z}_n^*$, es decir, la clase $[1]$. Entonces, $\sigma(\xi) = \xi^1 = \xi$. Dado que el cuerpo $L = K(\xi)$ está generado en su totalidad por ξ y los elementos de K (los cuales todo automorfismo de Galois deja fijos por definición), si un automorfismo deja fijo al generador ξ, obligatoriamente deja fijo a todo elemento de L. Luego $\sigma = \mathrm{id}_L$. Al ser su núcleo trivial, ψ es inyectiva.

Observación 5.1.8: Isomorfismos de grupos de Galois

Obsérvese que si $\phi : L \to L^*$ es un K-isomorfismo, entonces la aplicación $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L^*/K)$ dada por $\sigma \mapsto \phi\sigma\phi^{-1}$ es un isomorfismo.

Si L/K es una extensión algebraica y $\overline{L}$ una clausura algebraica de L, entonces podemos ver cada elemento de $\mathrm{Gal}(L/K)$ como un elemento de $S_1^L = \{\sigma : L \to \overline{L} \mid \sigma|_K = 1_K\}$. Por tanto de la Proposición 4.9 deducimos:

Proposición 5.1.1:

Si L/K es una extensión finita entonces $|\mathrm{Gal}(L/K)| \leq [L : K]_s \leq [L : K]$.

Si G es un grupo, entonces vamos a denotar por $\mathrm{Sub}(G)$ al conjunto de todos los subgrupos de G y si H es un subgrupo de G, entonces $\mathrm{Sub}(G/H)$ es el conjunto de los subgrupos de G que contienen a H. En realidad esta última notación es ambigua pues si N es un subgrupo normal de G, entonces $\mathrm{Sub}(G/N)$ tiene dos significados: el conjunto de los subgrupos de G que contienen a N y el conjunto de los subgrupos del cociente G/N. El Teorema de la Correspondencia (Teorema 5.4 de GyA) nos muestra que esta ambigüedad no es muy grave.

Definición 5.1.5: Homomorfismo y anti-homomorfismo de conjuntos ordenados

Consideramos $\mathrm{Sub}(L/K)$ y $\mathrm{Sub}(G/H)$ como conjuntos ordenados por la inclusión. Una aplicación $f:(A,\leq)\to(B,\leq)$ entre conjuntos ordenados se dice que es un **homomorfismo de conjuntos ordenados** si conserva el orden, es decir, si para cada $x,y\in A$ tales que $x\leq y$ se verifica que $f(x)\leq f(y)$ y se dice que es un **anti-homomorfismo de conjuntos ordenados** si $f(x)\geq f(y)$ para todo $x,y\in A$ con $x\leq y$.

Definición 5.1.6: Correspondencia de Galois

El par formado por las siguientes aplicaciones se llama **correspondencia de Galois de la extensión** L/K. Si L/K es una extensión de cuerpos entonces tenemos dos aplicaciones:

$$\begin{aligned}(-)^\circ = \mathrm{Gal}(L/-)\colon\ \mathrm{Sub}(L/K) &\longrightarrow \mathrm{Sub}(\mathrm{Gal}(L/K))\\ (-)^\circ = L^{(-)}\colon\ \mathrm{Sub}(\mathrm{Gal}(L/K)) &\longrightarrow \mathrm{Sub}(L/K)\end{aligned}$$

La aplicación que va para la derecha asocia $F\in\mathrm{Sub}(L/K)$ con

$$F^\circ=\mathrm{Gal}(L/F)=\{\sigma\in\mathrm{Gal}(L/K)\mid\sigma(x)=x\text{ para todo }x\in F\}$$

y la que va para la izquierda asocia $H\in\mathrm{Sub}(\mathrm{Gal}(L/K))$ con

$$H^\circ=L^H=\{a\in L\mid\sigma(a)=a\text{ para todo }\sigma\in H\}.$$

Veamos algunas propiedades de la correspondencia de Galois.

Recordemos que tanto la unidad de un anillo, como el neutro de un grupo o el subgrupo trivial del grupo lo denotamos siempre como 1. En la siguiente proposición 1 siempre denota el subgrupo trivial de $\mathrm{Gal}(L/K)$.

Proposición 5.1.2: Propiedades de la correspondencia de Galois

Sea L/K una extensión de cuerpos y sea $G=\mathrm{Gal}(L/K)$. La correspondencia de Galois $(-)^\circ:\mathrm{Sub}(L/K)\rightleftharpoons\mathrm{Sub}(G)$ satisface las siguientes propiedades, donde X e Y son ambos subextensiones de L/K o ambos subgrupos de G:

1. $L^\circ=1$, $K^\circ=G$ y $1^\circ=L$.
2. $(-)^\circ=\mathrm{Gal}(L/-)$ y $(-)^\circ=L^{(-)}$ son antihomomorfismos de conjuntos ordenados, es decir, si $X\subseteq Y$ entonces $Y^\circ\subseteq X^\circ$.
3. $X\subseteq X^{\circ\circ}$ y $X^\circ=X^{\circ\circ\circ}$.
4. Las dos aplicaciones que forman la correspondencia de Galois se restringen a un anti-isomorfismo de conjuntos ordenados entre sus dos imágenes.

Demostración. Vamos a demostrar las propiedades paso a paso, recordando las definiciones explícitas de los operadores: si E es un subcuerpo, $E^\circ=\mathrm{Gal}(L/E)=\{\sigma\in G\mid\sigma(x)=x\text{ para todo }x\in E\}$; y si H es un subgrupo, $H^\circ=L^H=\{x\in L\mid\sigma(x)=x\text{ para todo }\sigma\in H\}$.

(1) Casos triviales:

- $L^\circ=\mathrm{Gal}(L/L)$. El único automorfismo de L que deja fijo todo elemento de L es la identidad. Por tanto, $L^\circ = \{1\} = 1$.

- $K^\circ = \mathrm{Gal}(L/K)$. Por definición, este es el grupo de Galois total G.
- $1^\circ = L^{\{1\}}$. El conjunto de elementos de L fijados por el automorfismo identidad es todo L.

(2) Antihomomorfismos (Inversión del orden):

- *Para subcuerpos:* Supongamos que $E_1 \subseteq E_2$. Sea $\sigma \in E_2^\circ = \mathrm{Gal}(L/E_2)$. Por definición, σ deja fijos todos los elementos de E_2. Como $E_1 \subseteq E_2$, σ deja fijos todos los elementos de E_1. Esto implica que $\sigma \in \mathrm{Gal}(L/E_1) = E_1^\circ$. Por tanto, $E_2^\circ \subseteq E_1^\circ$.
- *Para subgrupos:* Supongamos que $H_1 \subseteq H_2$. Sea $x \in H_2^\circ = L^{H_2}$. Por definición, x es fijado por todo automorfismo de H_2. Como $H_1 \subseteq H_2$, x es fijado por todo automorfismo de H_1. Luego $x \in L^{H_1} = H_1^\circ$. Por tanto, $H_2^\circ \subseteq H_1^\circ$.

(3) Clausura y reflexividad: Vamos a probar primero que $X \subseteq X^{\circ\circ}$.

- *Si $X = E$ es un subcuerpo:* Sea $x \in E$. Para cualquier automorfismo $\sigma \in E^\circ = \mathrm{Gal}(L/E)$, se cumple por definición que $\sigma(x) = x$. Esto significa que x está en el cuerpo fijo de E°, es decir, $x \in (E^\circ)^\circ = E^{\circ\circ}$. Por tanto, $E \subseteq E^{\circ\circ}$.
- *Si $X = H$ es un subgrupo:* Sea $\sigma \in H$. Para cualquier elemento $x \in H^\circ = L^H$, se cumple por definición que $\sigma(x) = x$. Esto significa que σ deja fijo todo el cuerpo H°, luego $\sigma \in \mathrm{Gal}(L/H^\circ) = (H^\circ)^\circ = H^{\circ\circ}$. Por tanto, $H \subseteq H^{\circ\circ}$.

Ahora probaremos que $X^\circ = X^{\circ\circ\circ}$.

- Sustituyendo X por X° en la inclusión que acabamos de demostrar ($X \subseteq X^{\circ\circ}$), obtenemos inmediatamente que $X^\circ \subseteq (X^\circ)^{\circ\circ} = X^{\circ\circ\circ}$.
- Por otro lado, tomemos la inclusión original $X \subseteq X^{\circ\circ}$. Si aplicamos a ambos lados el operador $(-)^\circ$, por la propiedad (2) de inversión del orden, la inclusión se da la vuelta: $(X^{\circ\circ})^\circ \subseteq X^\circ$, es decir, $X^{\circ\circ\circ} \subseteq X^\circ$.
- Al tener la doble inclusión, concluimos que $X^\circ = X^{\circ\circ\circ}$.

(4) Anti-isomorfismo de las imágenes: Llamemos .elementos cerrados.ª aquellos subcuerpos o subgrupos que pertenecen a las imágenes de la correspondencia de Galois (es decir, aquellos de la forma $Y = X^\circ$).

Si tomamos un elemento cerrado $Y = X^\circ$ y le aplicamos dos veces el operador de Galois, obtenemos $Y^{\circ\circ} = (X^\circ)^{\circ\circ} = X^{\circ\circ\circ}$. Por la propiedad (3), sabemos que $X^{\circ\circ\circ} = X^\circ$, con lo que deducimos que $Y^{\circ\circ} = Y$.

Esto demuestra que si restringimos las aplicaciones $(-)^\circ$ a sus respectivas imágenes, componerlas da la identidad (son biyecciones mutuamente inversas). Como además sabemos por (2) que invierten el orden, deducimos que establecen un anti-isomorfismo perfecto de conjuntos ordenados entre los subcuerpos cerrados y los subgrupos cerrados. □

Definición 5.1.7:

Los elementos de las imágenes de las dos aplicaciones de la correspondencia de Galois se dice que son respectivamente subextensiones cerradas en L/K y subgrupos cerrados en $\mathrm{Gal}(L/K)$.

Observación 5.1.9:

Obsérvese que de la propiedad (3) de la Proposición 5.3 se tiene que X es cerrado si y solo si $X = X^{\circ\circ}$

Corolario 5.1.1:

Las aplicaciones de la correspondencia de Galois de una extensión de cuerpos L/K se restringen a un anti-isomorfismo de conjuntos ordenados entre las subextensiones cerradas en L/K y los subgrupos cerrados en $\mathrm{Gal}(L/K)$.

Observación 5.1.10:

Por la Proposición 5.3, L, 1 y $\mathrm{Gal}(L/K)$ son cerrados en L/K, pero K no tiene por qué serlo. Por ejemplo, si $L \neq K$ y $\mathrm{Gal}(L/K) = 1$ (ver Ejemplos 5.1) entonces $K^{\circ\circ} = 1^\circ = L \neq K$.

Proposición 5.1.3: Respecto a los grados de las extensiones y los índices de los subgrupos

Sea L/K una extensión de cuerpos.

1. Si $E_1 \subseteq E_2$ son subextensiones de L/K con E_2/E_1 finita entonces $[E_1^\circ : E_2^\circ] \leq [E_2 : E_1]$.
2. Si $H_1 \leq H_2$ son subgrupos de $\mathrm{Gal}(L/K)$ con $[H_2 : H_1] < \infty$, entonces $[H_1^\circ : H_2^\circ] \leq [H_2 : H_1]$.

Demostración. (1) Razonamos por inducción sobre $n = [E_2 : E_1]$ con el caso $n = 1$ obvio. Supongamos pues que $n > 1$ y la hipótesis de inducción. Sean $\alpha \in E_2 \setminus E_1$, $p = \mathrm{Min}_{E_1}(\alpha)$ y $s = \mathrm{gr}(p)$. Entonces $s = [E_1(\alpha) : E_1]$ y $[E_2 : E_1(\alpha)] < n$. Si $s < n$, entonces por la hipótesis de inducción tenemos:

$$[E_1^\circ : E_2^\circ] = [E_1^\circ : E_1(\alpha)^\circ][E_1(\alpha)^\circ : E_2^\circ] \leq [E_1(\alpha) : E_1][E_2 : E_1(\alpha)] = [E_2 : E_1].$$

En caso contrario, $E_2 = E_1(\alpha)$. Sean R el conjunto de raíces de p y $\phi : E_1^\circ/E_2^\circ \to R$ la aplicación dada por $\phi(\sigma E_2^\circ) = \sigma(\alpha)$. Es fácil ver que esta aplicación está bien definida y es inyectiva. Por tanto $[E_1^\circ : E_2^\circ] \leq |R| \leq \mathrm{gr}(p) = [E_2 : E_1]$.

(2) Pongamos $[H_2 : H_1] = n$, $H_2/H_1 = \{\tau_1 H_1, \dots, \tau_n H_1\}$ con $\tau_1 = 1$ y razonemos por reducción al absurdo, es decir, supondremos que $[H_1^\circ : H_2^\circ] > n$. Entonces existen $\alpha_1, \dots, \alpha_n, \alpha_{n+1} \in H_1^\circ$ linealmente independientes sobre H_2°. Consideremos la matriz:

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \tau_1(\alpha_2) & \dots & \tau_1(\alpha_{n+1}) \\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \dots & \tau_2(\alpha_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n(\alpha_1) & \tau_n(\alpha_2) & \dots & \tau_n(\alpha_{n+1}) \end{pmatrix}$$

y sea r el rango de A. Reordenamos los α_i para que las primeras r columnas sean linealmente independientes. Entonces la columna $r+1$ es combinación lineal de las r primeras (obsérvese que $r \le n < n+1 =$ número de columnas de A) y por tanto existe $a = (a_1, \dots, a_r, 1, 0, \dots, 0)^T \in (L)^{n+1}$ tal que $Aa = 0$. Como $\tau_1 = 1$ tenemos:

$$\alpha_1 a_1 + \cdots + \alpha_r a_r + \alpha_{r+1} = 0$$

y, como los α_i son linealmente independientes sobre H_2°, existe $1 \le i \le r$ tal que $a_i \notin H_2^\circ$. Reordenando $a_1, \dots, a_r$ podemos suponer que $a_1 \notin H_2^\circ$, es decir $\sigma(a_1) \neq a_1$ para algún $\sigma \in H_2$. La aplicación $H_2/H_1 \to H_2/H_1$ dada por $\tau H_1 \mapsto \sigma\tau H_1$ es inyectiva pues si $\sigma\sigma_1 H_1 = \sigma\sigma_2 H_1$ entonces $\sigma_2^{-1}\sigma_1 = (\sigma\sigma_2)^{-1}(\sigma\sigma_1) \in H_1$, luego $\sigma_1 H_1 = \sigma_2 H_1$. Por tanto existe una permutación $\rho \in S_n$ tal que $\sigma^{-1}\tau_i = \tau_{\rho(i)}$ para todo $i = 1, \dots, n$, con lo que la matriz:

$$B = \begin{pmatrix} \sigma^{-1}\tau_1(\alpha_1) & \sigma^{-1}\tau_1(\alpha_2) & \dots & \sigma^{-1}\tau_1(\alpha_{n+1}) \\ \sigma^{-1}\tau_2(\alpha_1) & \sigma^{-1}\tau_2(\alpha_2) & \dots & \sigma^{-1}\tau_2(\alpha_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{-1}\tau_n(\alpha_1) & \sigma^{-1}\tau_n(\alpha_2) & \dots & \sigma^{-1}\tau_n(\alpha_{n+1}) \end{pmatrix}$$

se obtiene permutando las filas de la matriz A. Eso implica que $Ba = 0$ y por tanto $A\sigma(a) = 0$. Luego $A(a - \sigma(a)) = 0$ y:

$$a - \sigma(a) = \begin{pmatrix} a_1 - \sigma(a_1) \\ \vdots \\ a_r - \sigma(a_r) \\ 1 - 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 - \sigma(a_1) \\ \vdots \\ a_r - \sigma(a_r) \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

con $a_1 - \sigma(a_1) \neq 0$. Eso implica que las primeras r columnas de A son linealmente dependientes en contra de la elección, lo que proporciona la contradicción deseada. □

Corolario 5.1.2:

Sea L/K una extensión de cuerpos.

1. Si $K \subseteq E_1 \subseteq E_2 \subseteq L$ es una torre de cuerpos, con $[E_2 : E_1] < \infty$ y E_1 cerrado en L/K entonces E_2 es cerrado en L/K y $[E_1^\circ : E_2^\circ] = [E_2 : E_1]$.
2. Si $H_1 \le H_2 \le \mathrm{Gal}(L/K)$ son subgrupos de $\mathrm{Gal}(L/K)$ con $[H_2 : H_1] < \infty$ y H_1 cerrado en L/K entonces H_2 es cerrado en L/K y $[H_1^\circ : H_2^\circ] = [H_2 : H_1]$.

Demostración. (1) Aplicando el primer apartado de la Proposición 5.5 a $E_1 \le E_2$ obtenemos que $[E_1^\circ : E_2^\circ] \le [E_2 : E_1]$ y aplicando el segundo apartado a $E_2^\circ \subseteq E_1^\circ$ obtenemos $[E_2^{\circ\circ} : E_1^{\circ\circ}] \le [E_1^\circ : E_2^\circ]$. Como E_1 es cerrado tenemos que $[E_2^{\circ\circ} : E_1] = [E_2^{\circ\circ} : E_1^{\circ\circ}] \le [E_2 : E_1]$ y como $E_2 \subseteq E_2^{\circ\circ}$ concluimos que $E_2 = E_2^{\circ\circ}$, es decir $E_2^{\circ\circ}$ es cerrado.

(2) Es completamente análoga. □

Como consecuencia del segundo apartado del Corolario 5.6 y el primero de la Proposición 5.3 se tiene el siguiente corolario:

Corolario 5.1.3:

Todo subgrupo finito de $\mathrm{Gal}(L/K)$ es cerrado en L/K.

5.2. Extensiones de Galois

Definición 5.2.1: Extensión de Galois

Una extensión de Galois es una extensión de cuerpos que es normal y separable.

Observación 5.2.1:

Obsérvese que toda extensión de Galois es algebraica (por ser separable).

La siguiente proposición es consecuencia inmediata de que la clase de extensiones normales es cerrada para levantamientos y de que la clase de extensiones separables también lo es.

Proposición 5.2.1:

La clase de extensiones de Galois es cerrada para levantamientos.

El siguiente teorema caracteriza las extensiones de Galois.

Teorema 5.2.1: Condiciones equivalentes para una extensión de Galois

Las siguientes condiciones son equivalentes para una extensión de cuerpos L/K con $G = \mathrm{Gal}(L/K)$:

1. L/K es una extensión de Galois.
2. L/E es una extensión de Galois para todo $E \in \mathrm{Sub}(L/K)$.
3. L/K es algebraica y toda subextensión de L/K es cerrada.
4. L/K es algebraica y K es una subextensión cerrada de L/K.
5. L/K es algebraica y $G^\circ = K$, o sea, si $\alpha \in L$ satisface $\sigma(\alpha) = \alpha$ para todo $\sigma \in G$ entonces $\alpha \in K$.
6. L/K es algebraica y para todo $\alpha \in L \setminus K$ existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\alpha) \neq \alpha$.

Demostración. (1) $\Longrightarrow$ (2) es consecuencia de la Proposición 5.9.

(2) $\Longrightarrow$ (3). Supongamos que L/K satisface (2) y sea $E \in \mathrm{Sub}(L/K)$. De la Proposición 5.3 se tiene que $E \subseteq E^{\circ\circ}$ y tenemos que demostrar que se verifica la igualdad, o lo que es lo mismo, tenemos que demostrar que si $\alpha \in L \setminus E$ entonces existe $\sigma \in \mathrm{Gal}(L/E)$ tal que $\sigma(\alpha) \neq \alpha$. Sea $\alpha \in L \setminus E$ y sea $p = \mathrm{Min}_E(\alpha)$. Este polinomio tiene una raíz en L y, como L/E es normal, p es completamente factorizable en L. Como además L/E es separable y $\alpha \notin E$, existe $\beta \in L$, con $\alpha \neq \beta$, tal que β también es raíz de p. De la Proposición 1.10 se deduce que existe un E-isomorfismo $\sigma : E(\alpha) \to E(\beta)$. Sea $\overline{L}$ una clausura algebraica de L. Como L/E es algebraica (y por tanto también lo es $L/E(\alpha)$), σ se extiende a un homomorfismo de L en $\overline{L}$ que también

denotaremos por σ, y como L/E es normal, $\sigma(L) \subseteq L$, con lo que $\sigma \in \mathrm{Gal}(L/E)$. Deducimos que $\alpha \neq \beta = \sigma(\alpha)$.

(3) $\implies$ (4), (4) $\implies$ (5), y que (5) y (6) son equivalentes, está claro.

(5) $\implies$ (1). Supongamos que L/K verifica (5). Sea $\alpha \in L$; sean $p = \mathrm{Min}_K(\alpha)$ y $n = \mathrm{gr}(p)$. Tenemos que demostrar que p factoriza completamente en L (para demostrar que L/K es normal) y que p no tiene raíces múltiples (para mostrar que L/K es separable). Esto equivale a demostrar que p tiene n raíces (distintas) en L. Sea $R = \{\alpha = \alpha_1, \dots, \alpha_r\}$ el conjunto de las (distintas) raíces de p en L y sea $q = (X - \alpha_1) \cdots (X - \alpha_r)$. Si $\sigma \in \mathrm{Gal}(L/K)$, entonces $\sigma(\alpha_i)$ es una raíz de p en L, lo que implica que σ induce una permutación de R y por tanto $\sigma(q) = q$, es decir $\sigma(a) = a$ para cada uno de los coeficientes a de q. Como estamos suponiendo que L/K satisface la propiedad (5), concluimos que cada uno de estos coeficientes pertenece a K, es decir $q \in K[X]$. Como $r = \mathrm{gr}(q) \leq n = \mathrm{gr}(p)$ y p tiene grado mínimo entre los polinomios de $K[X]$ que tienen a α como raíz deducimos que $p = q$ y por tanto $r = n$. □

La siguiente proposición muestra criterios para decidir si una extensión es de Galois para el caso de extensiones finitas.

Proposición 5.2.2: Criterios para una extensión de Galois finita

Las siguientes condiciones son equivalentes para una extensión finita L/K:

1. L/K es una extensión de Galois.
2. $[L : K] = |\,\mathrm{Gal}(L/K)|$.
3. $[L : E] = |\,\mathrm{Gal}(L/E)|$ para todo $E \in \mathrm{Sub}(L/K)$.

Demostración. Sea $\overline{L}$ una clausura algebraica. Podemos ver cada elemento de $\mathrm{Gal}(L/K)$ como un K-homomorfismo de L en $\overline{L}$. De esta manera, si σ denota la inclusión de K en L tenemos que $\mathrm{Gal}(L/K) \subseteq S_\sigma^L$. Combinando esto con la Proposición 5.2 tenemos que:

$$|\,\mathrm{Gal}(L/K)| \leq [L : K]_s \leq [L : K]$$

Por el Teorema 4.12, la segunda desigualdad es una igualdad si y solo si L/K es separable. La primera desigualdad es una igualdad si y solo si todo K-homomorfismo de L a $\overline{L}$ cumple $\tau(L) \subseteq L$ si y solo si L/K es normal. Esto demuestra que (1) y (2) son equivalentes.

Combinando la equivalencia entre (1) y (2) y el Teorema 5.10 se deduce de forma inmediata que (1) y (3) son equivalentes. □

Teorema 5.2.2: Teorema Fundamental de la Teoría de Galois

Sea L/K una extensión de Galois finita y sea $G = \text{Gal}(L/K)$. Entonces se verifican las siguientes propiedades:

1. La correspondencia de Galois es un anti-isomorfismo de conjuntos ordenados entre $\text{Sub}(L/K)$ y $\text{Sub}(G)$.

2. Si X e Y están ambos en $\text{Sub}(L/K)$ o en $\text{Sub}(G)$ y $X \subseteq Y$ entonces $[X^\circ : Y^\circ] = [Y : X]$. En particular:

   (a) Si $E \in \text{Sub}(L/K)$ entonces $[L : E] = |E^\circ|$ y $[E : K] = [G : E^\circ]$.

   (a) Si $H \in \text{Sub}(G)$ entonces $|H| = [L : H^\circ]$ y $[G : H] = [H^\circ : K]$.

Demostración. (1) A la vista de la Proposición 5.3 y el Teorema 5.10, para demostrar (1) sólo falta demostrar que todo subgrupo H de G es cerrado, pero eso es consecuencia inmediata del Corolario 5.7.

(2) Es consecuencia de la Proposición 5.6. □

Si $K \subseteq E \subseteq L$ es una torre de cuerpos y $\sigma \in \text{Gal}(L/K)$, entonces $\text{Res}_E^L(\sigma)$ denota la restricción de σ a E. En principio $\text{Res}_E^L(\sigma)$ es un K-homomorfismo de E en L, pero si E/K es normal entonces $\sigma \in \text{Gal}(E/K)$. Eso es lo que pasa en las condiciones de la siguiente proposición y está claro que en tal caso $\text{Res}_E^L : \text{Gal}(L/K) \to \text{Gal}(E/K)$ es un homomorfismo de grupos.

Proposición 5.2.3: Condiciones equivalentes para una extensión de Galois

Sea L/K una extensión finita de Galois. Si $E \in \text{Sub}(L/K)$ entonces las siguientes condiciones son equivalentes:

(1) E/K es de Galois.

(1) E/K es normal.

(1) $\sigma(E) \subseteq E$ para todo $\sigma \in \text{Gal}(L/K)$.

(1) $\text{Gal}(L/E)$ es normal en $\text{Gal}(L/K)$.

Además, si estas condiciones se satisfacen, entonces la aplicación de restricción

$$\text{Res}_E^L : \text{Gal}(L/K) \to \text{Gal}(E/K), \quad \sigma \mapsto \sigma|_E$$

es suprayectiva y como su núcleo es $\text{Gal}(L/E)$, se tiene que

$$\text{Gal}(E/K) \simeq \frac{\text{Gal}(L/K)}{\text{Gal}(L/E)}$$

Demostración. La equivalencia entre (1) y (2) es consecuencia inmediata de que la clase de extensiones separables es multiplicativa (Proposición 4.13).

(2) $\implies$ (3). Supongamos que E/K es normal y sean $\alpha \in E$ y $\sigma \in \text{Gal}(L/K)$. Entonces $p = \text{Min}_K(\alpha)$ es completamente factorizable en E, o sea $p = (X-\alpha_1)\cdots(X-\alpha_n)$ con $\alpha_1, \dots, \alpha_n \in E$. Entonces $\sigma(\alpha)$ es raíz de p y por tanto $\sigma(\alpha) = \alpha_i \in E$, para algún i. Esto prueba que $\sigma(E) \subseteq E$.

(3) $\implies$ (4). Supongamos que se verifica (3) y sean $\sigma \in \mathrm{Gal}(L/K)$ y $\tau \in \mathrm{Gal}(L/E)$. Entonces $\sigma(E) \subseteq E$ y por tanto $\tau(\sigma(\alpha)) = \sigma(\alpha)$, es decir $\sigma^{-1}\tau\sigma(\alpha) = \alpha$, para todo $\alpha \in E$. Esto prueba que $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$ para todo $\sigma \in \mathrm{Gal}(L/K)$ y todo $\tau \in \mathrm{Gal}(L/E)$, es decir $\mathrm{Gal}(L/E)$ es normal en $\mathrm{Gal}(L/K)$.

(4) $\implies$ (2). Supongamos que $\mathrm{Gal}(L/E)$ es normal en $\mathrm{Gal}(L/K)$. Sea $\rho : E \to \overline{L}$ un K-homomorfismo. Como L/E es algebraica, ρ se extiende a un K-homomorfismo $\sigma : L \to \overline{L}$. Como L/K es normal, $\sigma(L) = L$ (Teorema 2.11), y por tanto podemos considerar σ como un elemento de $\mathrm{Gal}(L/K)$. Por hipótesis, $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$ para todo $\tau \in \mathrm{Gal}(L/E)$, con lo que $\tau\sigma(\alpha) = \sigma(\alpha)$, para todo $\tau \in \mathrm{Gal}(L/E)$ y todo $\alpha \in E$. Esto muestra que $\rho(\alpha) = \sigma(\alpha) \in \mathrm{Gal}(L/E)^\circ = E^{\circ\circ} = E$65]. Como L/E es algebraica, $\overline{L}$ es una clausura algebraica de E con lo que hemos comprobado que E/K satisface las condiciones del Teorema 2.11, es decir E/K es normal65].

Supongamos ahora que las condiciones (1)-(4) se verifican. Entonces la aplicación de restricción

$$f = \mathrm{Res}^L_E : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K), \quad \sigma \mapsto \sigma|_E$$

es un homomorfismo de grupos cuyo núcleo es $\mathrm{Gal}(L/E)$. Aplicando el Primer Teorema de Isomorfía y que todas las extensiones L/K, E/K y L/E son de Galois deducimos que

$$|\,\mathrm{Im}\, f| = \frac{|\,\mathrm{Gal}(L/K)|}{|\,\mathrm{Gal}(L/E)|} = \frac{[L:K]}{[L:E]} = [E:K] = |\,\mathrm{Gal}(E/K)|,$$

lo que implica que f es suprayectiva y $\mathrm{Gal}(E/K) \simeq \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/E)}$. □

En el siguiente Teorema volvemos a encontrar una versión diferente de homomorfismo de restricción.

Teorema 5.2.3: Teorema de las Irracionalidades Accesorias de Lagrange

Sean L/K y E/K dos extensiones admisibles y supongamos que la primera es finita y de Galois. Entonces LE/E y $L/L\cap E$ son extensiones de Galois finitas y el homomorfismo de restricción

$$\mathrm{Res}^{LE}_L : \mathrm{Gal}(LE/E) \to \mathrm{Gal}(L/L\cap E)$$

es un isomorfismo de grupos.

Demostración. Como L/K es de Galois, del Teorema 5.10 se deduce que $L/L\cap E$ también es de Galois y de la Proposición 5.9 que lo es LE/E. Que la primera es finita es obvio y que lo sea la segunda es consecuencia de la Proposición 1.18.

Sea $f = \mathrm{Res}^{LE}_L$7. Que f es inyectiva es obvio ya que un elemento del núcleo es un automorfismo σ de LE que verifica $\sigma(x) = x$ para todo $x \in L$ y todo $x \in E$7.

Para ver que f es suprayectiva ponemos $H = \mathrm{Im}\, f \subseteq \mathrm{Gal}(L/L\cap E)$. Entonces $L\cap E = (L\cap E)^{\circ\circ} = \mathrm{Gal}(L/L\cap E)^\circ \subseteq H^\circ$. Sea $\alpha \in H^\circ$. Entonces para todo $\sigma \in \mathrm{Gal}(LE/E)$ se verifica $\sigma(\alpha) = f(\sigma)(\alpha) = \alpha$, pues $f(\sigma) \in H$. Esto demuestra que $\alpha \in \mathrm{Gal}(LE/E)^\circ = E^{\circ\circ} = E$, pues LE/E es de Galois. Como esto se verifica para cada $\alpha \in H^\circ$ y $H^\circ \subseteq L$ deducimos que $H^\circ \subseteq L\cap E = (L\cap E)^{\circ\circ}$. Por tanto, $H^\circ = (L\cap E)^{\circ\circ}$. Como $L/L\cap E$ es de Galois, concluimos que $\mathrm{Im}\, f = H = (L\cap E)^{\circ\circ\circ} = \mathrm{Gal}(L/L\cap E)$, o sea f es suprayectiva. □

5.2.1. Ejemplo tocho

Vamos a calcular los subcuerpos del cuerpo de escisión F del polinomio $X^5 - p$, donde p es un número primo, y cuáles son normales sobre $\mathbb{Q}$.

Los subcuerpos de F son precisamente las subextensiones de $F/\mathbb{Q}$. Por el Teorema Fundamental de la Teoría de Galois (Teorema 5.12) dichos cuerpos están en correspondencia biunívoca con los subgrupos de $G = \mathrm{Gal}(F/\mathbb{Q})$ y los normales son los que corresponden con subgrupos normales de G. Sea $\alpha = \sqrt[5]{p}$.

Entonces $F = \mathbb{Q}(\alpha, \zeta_5)$. Además, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ y $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \varphi(5) = 4$. Por tanto $[F : \mathbb{Q}]$ es al menos 20. Por otro lado $[F : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ y por tanto $[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 20$. Luego $|G| = [F : \mathbb{Q}] = 20$. Además G contiene a $\mathrm{Gal}(F/\mathbb{Q}(\alpha))$ y a $\mathrm{Gal}(F/\mathbb{Q}(\zeta_5))$ que serán dos subgrupos de órdenes 4 y 5 respectivamente.

Por el Teorema de las Irracionalidades Accesorias (Teorema 5.14), $\mathrm{Res}^F_{\mathbb{Q}(\zeta_5)} : \mathrm{Gal}(F/\mathbb{Q}(\alpha)) \to \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ es un isomorfismo8. Usando el isomorfismo entre $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ y $\mathbb{Z}_5^*$ (Problema (3.15)) deducimos que $\mathrm{Gal}(F/\mathbb{Q}(\alpha)) = \langle\tau\rangle$ con $\tau(\zeta_5) = \zeta_5^2$. Por otro lado tenemos otro elemento $\sigma \in \mathrm{Gal}(F/\mathbb{Q}(\zeta_5))$ con $\sigma(\alpha) = \zeta_5\alpha$ y claramente $\mathrm{Gal}(F/\mathbb{Q}(\zeta_5)) = \langle\sigma\rangle$.

Por otro lado, como $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ es de Galois pero $\mathbb{Q}(\alpha)/\mathbb{Q}$ no lo es, deducimos que $\langle\sigma\rangle$ es normal en G pero $\langle\tau\rangle$ no es normal en G. Por tanto $\tau\sigma\tau^{-1} = \sigma^i$ para algún $i \in \{2, 3, 4\}$. De hecho $i = 2$ pues $\tau\sigma\tau^{-1}(\alpha) = \tau\sigma(\alpha) = \tau(\zeta_5\alpha) = \zeta_5^2\alpha = \sigma^2(\alpha)$. Por tanto, todos los elementos de G tienen una única forma $\sigma^i\tau^j$ con $0 \leq i \leq 4$ y $0 \leq j \leq 3$.

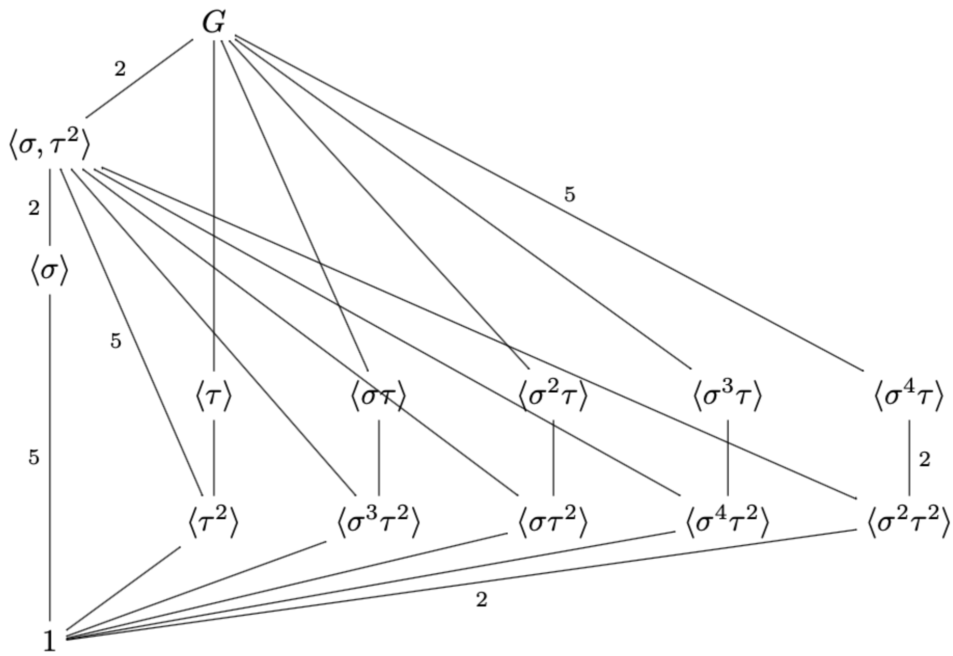
Vamos a calcular los subgrupos cíclicos. Ya tenemos tres: 1, $\langle\sigma\rangle$ y $\langle\tau\rangle$, que tienen orden 1, 5 y 4, respectivamente. Todos los elementos de la forma σ^i generan $\langle\sigma\rangle$ y τ y τ^{-1} generan $\langle\tau\rangle$. Otro subgrupo cíclico más será $\langle\tau^2\rangle$. Este último tiene orden 2. Solo nos falta calcular los subgrupos cíclicos generados por los elementos de la forma $\sigma^i\tau^j$ con $1 \leq i \leq 4$ y $1 \leq j \leq 3$.

Comenzamos con los de la forma $\sigma^i\tau^2$. De la igualdad $\tau\sigma = \sigma^2\tau$ observamos que $\tau^2\sigma = \sigma^4\tau^2 = \sigma^{-1}\tau^2$. Por tanto, para cada i tenemos que $(\sigma^i\tau^2)^2 = 1$. O sea, cada $\sigma^i\tau^2$ tiene orden 2 . Esto nos proporciona cinco subgrupos de orden 2, uno de los cuales es $\langle\tau^2\rangle$.

Por otro lado $(\sigma^i\tau)^2 = \sigma^{3i}\tau^2$, que tiene orden 296. Por tanto, $\langle\sigma^i\tau\rangle$ tiene orden 4 y su único subgrupo de orden 2 es $\langle\sigma^{3i}\tau^2\rangle$96. Como estos últimos son distintos para los cinco valores distintos de i, obtenemos de esta forma cinco subgrupos cíclicos de orden 4, uno de los cuales es $\langle\tau\rangle$. Cada uno de estos subgrupos tiene dos elementos de orden 49. Más concretamente $\langle\sigma^i\tau\rangle$ también está generado por $(\sigma^i\tau)^3 = \sigma^i\tau\sigma^{3i}\tau^2 = \sigma^{2i}\tau^3$9. Por tanto, ya tenemos todos los subgrupos cíclicos:

- De orden 1: 1.
- De orden 2: $\langle\sigma^i\tau^2\rangle$ con $0 \leq i \leq 4$.
- De orden 4: $\langle\sigma^i\tau\rangle$ con $0 \leq i \leq 4$.
- De orden 5: $\langle\sigma\rangle$.

Calculamos ahora los grupos generados por dos elementos g y h. Por supuesto, si uno de ellos está en el subgrupo generado por el otro lo que obtendremos es uno de los grupos cíclicos, con lo que suponemos que $g \notin \langle h\rangle$ y $h \notin \langle g\rangle$.



Supongamos primero que uno de los dos tiene orden 5. Por ejemplo, supongamos que $|g| = 5$ y por tanto h tiene orden 2 ó 4. Si h tiene orden 4 entonces $\langle g, h\rangle = G$. Sin embargo si h tiene orden 2 entonces $\langle g, h\rangle = \langle \sigma, \tau^2\rangle$ y como $\tau^2\sigma = \sigma^{-1}\tau^2$ tenemos que $\langle \sigma, \tau^2\rangle$ tiene orden 10.

En los demás casos g y h tienen orden 2 ó 4 y vamos a ver que siempre $\langle g, h\rangle = G$. Si $|g| = |h| = 4$ entonces podemos suponer que $g = \sigma^i\tau$ y $h = \sigma^j\tau$ con $i \neq j$. Por tanto, $\langle g, h\rangle$ contiene a $gh^{-1} = \sigma^{i-j}$. Como este elemento genera a $\langle\sigma\rangle$, tenemos que $\langle g, h\rangle = \langle \sigma, \tau\rangle = G$. El mismo argumento muestra que si g y h tienen orden 2 y son distintos, entonces generan G. Finalmente si uno tiene orden 2 y el otro 4, por ejemplo h, entonces $\langle g, h\rangle$ contiene a $\langle g, h^2\rangle$ con g y h^2 distintos de orden 2 y de nuevo obtenemos que $\langle g, h\rangle = G$.

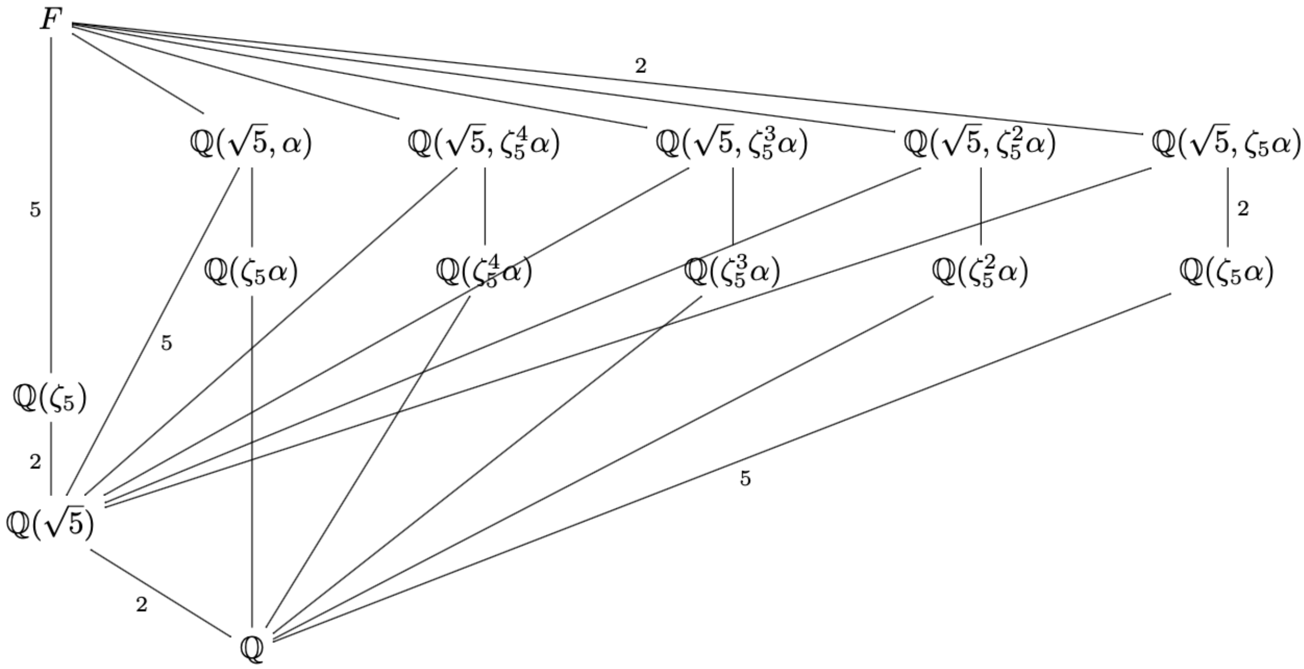
El retículo de subgrupos que obtenemos es el siguiente:

Dando la vuelta al diagrama obtenemos las inclusiones entre los subcuerpos de F. Pero antes de hacerlo vamos a calcular los cuerpos.

Claramente $G^\circ = \mathbb{Q}$, $1^\circ = F$, $\langle\sigma\rangle^\circ = \mathbb{Q}(\zeta_5)$, $\langle\tau\rangle^\circ = \mathbb{Q}(\alpha)$. Cada uno de los $\langle\sigma^i\tau\rangle^\circ$ tiene que tener grado 5 sobre $\mathbb{Q}$ y serán los únicos subcuerpos de grado 5 sobre $\mathbb{Q}$, que necesariamente son $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\zeta_5\alpha)$, $\mathbb{Q}(\zeta_5^2\alpha)$, $\mathbb{Q}(\zeta_5^3\alpha)$ y $\mathbb{Q}(\zeta_5^4\alpha)$. Observamos que $\sigma^i\tau(\zeta_5^{-i}\alpha) = \sigma^i(\zeta_5^{-2i}\alpha) = \zeta_5^{-i}\alpha$. Por tanto $\langle\sigma^i\tau\rangle^\circ = \mathbb{Q}(\zeta_5^{-i}\alpha)$.

Por otro lado $\langle\sigma, \tau^2\rangle$ es el único subgrupo que tiene grado 2 sobre $\mathbb{Q}$, cuyo cuerpo fijo además está contenido en $\langle\sigma\rangle^\circ = \mathbb{Q}(\zeta_5)$. Observando que $\beta = \zeta_5 + \zeta_5^{-1} = 2\cos(2\pi/5) \in \mathbb{R}$, tenemos que $\mathbb{Q}(\beta)$ está contenido en $\mathbb{Q}(\zeta_5)$. Además, como $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$ tenemos que $\beta^2 = \zeta_5^2 + \zeta_5^{-2} + 2 = -\beta + 1$, con lo que β es raíz de $X^2 + X - 1$, de donde $\beta = \frac{-1+\sqrt{5}}{2}$ y por tanto $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{5})$.

Por tanto $\langle\sigma, \tau^2\rangle^\circ = \mathbb{Q}(\sqrt{5})$. Ahora observamos que $\langle\sigma^{3i}\tau^2\rangle = \langle\sigma, \tau^2\rangle \cap \langle\sigma^i\tau\rangle$. Como la correspondencia de Galois es un anti-isomorfismo de retículos deducimos que $\langle\sigma^{3i}\tau^2\rangle^\circ = \langle\sigma, \tau^2\rangle^\circ\langle\sigma^i\tau\rangle^\circ =$



$\mathbb{Q}(\sqrt{5}, \zeta_5^{-i}\alpha)$.

Por tanto el retículo de subcuerpos es el siguiente:

Obsérvese que los únicos subgrupos normales de G son 1, $\langle\sigma\rangle$, $\langle\sigma, \tau^2\rangle$ y G. Por tanto, los únicos subcuerpos de F que son normales sobre $\mathbb{Q}$ son $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\zeta_5)$ y F.