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:

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

□

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 .[ex]traños.[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_1s_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:

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

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:

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

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 $\mathcal{C} = \{L_1/K, \dots, L_n/K\}$, el compuesto se denota $L_1 \dots L_n = K(L_1 \cup \dots \cup L_n)$ 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 $\alpha_1, \dots, \alpha_n \in L$ tales que $L = K(\alpha_1, \dots, \alpha_n)$.
- 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 $\text{gr}(p) = 1$, 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 $\text{gr}(q) = \text{gr}(p) - 1$, 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: $\sigma(a_nX^n + \cdots + a_0) = \sigma(a_n)X^n + \cdots + \sigma(a_0)$.

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 $p(X) = p_0+p_1X+\cdots+p_nX^n$ 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:

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

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:

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

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).*

Continuación de la demostración de la Proposición 1.12.

- **(b) $\Rightarrow$ (a):** Se tiene porque $\ker(S_\alpha) \neq (0)$, luego el homomorfismo de evaluación no es inyectivo.
- **(c) $\Rightarrow$ (d):** Obvio.
- **(a) $\Rightarrow$ (c):** Si α es algebraico sobre K, existe $f \in K[X] \setminus \{0\}$ tal que $f(\alpha) = 0$. Esto implica que α es raíz de algún factor p_i irreducible (ya que $K[X]$ es un Dominio de Factorización Única y $f = p_1 \cdots p_k$).

  Aplicando el Primer Teorema de Isomorfía al homomorfismo de evaluación, obtenemos:

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

  Como (p_i) es un ideal maximal (por ser p_i irreducible), el cociente es un cuerpo. Por lo tanto, $K[\alpha]$ es un cuerpo, lo que implica que $K(\alpha) = K[\alpha]$ y que la extensión es finita.

- **(e) ⇒ (b):** Supongamos por reducción al absurdo que $\ker(S_\alpha) = (0)$ (es decir, el homomorfismo es inyectivo). Entonces $K[X] \simeq K[\alpha]$. Como $K[X]$ es un espacio vectorial de dimensión infinita sobre K, $K[\alpha]$ también lo sería, lo cual contradice la hipótesis de que la extensión es de dimensión finita.

□

El Polinomio Mínimo

Sea L/K una extensión y $\alpha \in L$ un elemento algebraico sobre K. Consideramos el homomorfismo de evaluación $S_\alpha : K[X] \to L$. Se cumple que su núcleo $I = \ker(S_\alpha)$ es un ideal primo porque:

$$\frac{K[X]}{I} \simeq K[\alpha] \subseteq L$$

y al estar contenido en un cuerpo, es un dominio de integridad. De hecho, al ser $K[X]$ un Dominio de Ideales Principales (por el algoritmo de la división), el ideal está generado por un único elemento, $I = (p)$.

De todos los generadores posibles de este ideal, hay uno solo que es mónico. Si $\ker(S_\alpha) = (f(X))$ donde $f(X) = f_n X^n + \ldots$, al ser K un cuerpo y el núcleo un ideal, podemos multiplicar por el inverso del coeficiente principal $\frac{1}{f_n}$ para obtener un polinomio mónico que genera el mismo ideal.

Definición 1.5.2: Polinomio Mínimo

Llamaremos polinomio mínimo al único polinomio irreducible y mónico de α sobre K que lo anula. Lo denotaremos como $\mathrm{Min}_K(\alpha)$.

Del Teorema de Extensión Simple deducimos lo siguiente:

Lema 1.5.1: Lema 1.13

Si α es algebraico sobre K, entonces:

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

Y si este grado es n, entonces el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ constituye una base de $K(\alpha)$ como espacio vectorial sobre K.

Observación 1.5.1: Recordatorio: Criterio de Eisenstein

Sea $p \in \mathbb{Z}[X]$ tal que $p(X) = a_0 + a_1 X + \cdots + a_n X^n$ y sea q un número primo. Si se cumple que:

- $q \nmid a_n$ (el primo no divide al coeficiente principal)
- $q \mid a_i$ para $i = 0, \ldots, n-1$ (el primo divide a los demás coeficientes)
- $q^2 \nmid a_0$ (el cuadrado del primo no divide al término independiente)

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

Ejemplo 1.5.2: Ejemplos 1.14

1. **Polinomios mínimos básicos:** $\mathrm{Min}_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$, mientras que $\mathrm{Min}_{\mathbb{R}}(\sqrt{2}) = X - \sqrt{2}$. Por otro lado, $\mathrm{Min}_{\mathbb{Q}}(i) = \mathrm{Min}_{\mathbb{R}}(i) = X^2 + 1$. Más generalmente, si $q \in \mathbb{Q}$ y $\sqrt{q} \notin \mathbb{Q}$, entonces $\mathrm{Min}_{\mathbb{Q}}(\sqrt{q}) = X^2 - q$.

2. Si $\alpha = \sqrt{5 + \sqrt{5}}$, entonces $\alpha^2 - 5 = \sqrt{5}$. Elevando al cuadrado de nuevo obtenemos $5 = (\alpha^2 - 5)^2 = \alpha^4 - 10\alpha^2 + 25$, es decir, α es una raíz del polinomio $X^4 - 10X^2 + 20$. Aplicando el Criterio de Eisenstein a este polinomio para el primo $q = 5$, deducimos que es irreducible sobre $\mathbb{Q}$ y, por tanto, $\mathrm{Min}_{\mathbb{Q}}(\alpha) = X^4 - 10X^2 + 20$.

3. **Trascendencia de variables:** El cuerpo de fracciones de $K[X]$ es $K(X)$ y la extensión $K(X)/K$ es de grado infinito, pues las potencias de X ($\{1, X, X^2, \dots\}$) son linealmente independientes sobre K. Por tanto, X es trascendente sobre K.

4. **Trascendencia de constantes famosas:** Decidir si un número real o complejo es algebraico sobre el cuerpo de los números racionales es un problema normalmente muy difícil. El carácter trascendente de π sobre $\mathbb{Q}$ fue demostrado por Lindemann en 1882. También es trascendente la base e del logaritmo neperiano, lo que fue demostrado por Hermite en 1873.

Corolario 1.5.1: Equivalencias de Extensiones Finitas (Corolario de Prop. 1.12)

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

1. L/K es finita.
2. L/K es algebraica y finitamente generada.
3. Existen $\alpha_1, \dots, \alpha_n \in L$ algebraicos sobre K tales que $L = K(\alpha_1, \dots, \alpha_n)$.

Demostración. **(2) ⇒ (3):** Obvio, por la propia definición.

(1) ⇒ (2): Si L/K es finita, entonces $[L : K] < \infty$. Entonces, para todo $\alpha \in L$, se tiene la torre $K \subseteq K(\alpha) \subseteq L$, lo que implica que $[K(\alpha) : K] \leq [L : K] < \infty$. Al ser una extensión simple finita, α es algebraico, por lo que la extensión total L/K es algebraica. Además, como el grado es finito (sea $[L : K] = n$), existe una base $\{u_1, \dots, u_n\}$, por lo que $L = K(u_1, \dots, u_n)$, siendo finitamente generada.

(3) ⇒ (1): Para deducir que la extensión es finita, vamos a construir una torre de cuerpos que empiece en K y acabe en L, para usar la propiedad multiplicativa del grado:

$$
\begin{aligned}
F_0 &= K \\
F_1 &= K(\alpha_1) \\
F_2 &= K(\alpha_1, \alpha_2) = F_1(\alpha_2) \\
&\vdots \\
F_i &= K(\alpha_1, \dots, \alpha_i) = F_{i-1}(\alpha_i) \\
&\vdots \\
F_n &= K(\alpha_1, \dots, \alpha_n) = L
\end{aligned}
$$

Vamos a probar que cada grado $[F_i : F_{i-1}]$ es finito. Como cada $F_i = F_{i-1}(\alpha_i)$, para saber su grado basta ver si α_i es algebraico sobre F_{i-1}. Esto se cumple por hipótesis: como $K \subseteq F_{i-1}$ y α_i es algebraico sobre K, también lo es sobre F_{i-1} (el polinomio mínimo de α_i sobre K pertenece a $K[X]$ y, por tanto, a $F_{i-1}[X]$). Luego cada salto $[F_i : F_{i-1}]$ es finito. Por la multiplicatividad de los grados en torres de cuerpos, el grado total $[L : K]$ es finito. □

Proposición 1.5.2: La clase de extensiones algebraicas es multiplicativa (Prop. 1.16)

Sea $K_1 \subseteq K_2 \subseteq K_3$ una torre de extensiones. Se cumple que:

$$K_3/K_1 \text{ es algebraica} \iff K_2/K_1 \text{ y } K_3/K_2 \text{ son algebraicas}$$

Demostración. **(⇒)** Es obvio. Las raíces de K_3 sobre K_1 se mantienen en el cuerpo y son automáticamente raíces sobre K_2.

(⇐) Sea $\alpha \in K_3$. Como K_3/K_2 es algebraica, α es raíz de algún polinomio no nulo en $K_2[X]$. Es decir, existe $p(X) = p_0 + p_1X + \cdots + p_nX^n \in K_2[X] \setminus \{0\}$ tal que $p(\alpha) = 0$.

Como $p_0, p_1, \ldots, p_n \in K_2$ y la extensión base K_2/K_1 es algebraica, todos estos coeficientes son algebraicos sobre K_1. Sea $F = K_1(p_0, p_1, \ldots, p_n)$. Por el corolario anterior, la extensión F/K_1 es finita.

Sabemos que α es algebraico sobre F (puesto que $p(X) \in F[X]$), lo que implica que la extensión simple $F(\alpha)/F$ es finita.

Como F/K_1 y $F(\alpha)/F$ son extensiones finitas, y la clase de extensiones finitas es multiplicativa, se sigue que la extensión global $F(\alpha)/K_1$ es finita. Al ser finita, es algebraica, y como $\alpha \in F(\alpha)$, concluimos que α es algebraico sobre K_1. □

Corolario 1.5.2: Clausura algebraica de K en L

Si L/K es una extensión de cuerpos, entonces el conjunto C de los elementos de L que son algebraicos sobre K es un subcuerpo de L que contiene a K, llamado **clausura algebraica de K en L**.
En concreto, si $S \subseteq L$ está formado por elementos algebraicos sobre K, entonces la extensión $K(S)/K$ es algebraica.

Demostración. Para cualesquiera $\alpha, \beta \in C$, sabemos que la extensión generada $K(\alpha, \beta)/K$ es finita y, por tanto, algebraica. Esto implica que cualquier combinación de estos elementos mediante las operaciones del cuerpo (como $\alpha + \beta$, $\alpha \cdot \beta$, etc.) produce elementos que también son algebraicos sobre K. Por lo tanto, estos elementos pertenecen a C, demostrando que C es un cuerpo. □

Definición 1.5.3: Clase cerrada para levantamientos

Decimos que una clase $\mathcal{C}$ de extensiones de cuerpos es **cerrada para levantamientos** si, para cada par de extensiones admisibles L_1/K y L_2/K, se cumple que:

$$L_1/K \in \mathcal{C} \implies L_1L_2/L_2 \in \mathcal{C}$$

Proposición 1.5.3: Levantamiento de las clases fundamentales

Cada una de las clases de extensiones finitas, algebraicas, finitamente generadas y simples son cerradas para levantamientos.

Demostración. Analizamos cada caso asumiendo que $L_1/K \in \mathcal{C}$ y levantamos al cuerpo compuesto L_1L_2:

- **Finitamente generadas o simples:** Si L_1/K es finitamente generada o simple, entonces $L_1 = K(\alpha_1, \ldots, \alpha_n)$ con $\alpha_i \in L_1$. El compuesto es $L_1L_2 = L_2(L_1) = L_2(\alpha_1, \ldots, \alpha_n)$. Como está generado por una cantidad finita de elementos, la extensión L_1L_2/L_2 es finitamente generada.
- **Algebraicas:** Si L_1/K es algebraica, todo elemento de L_1 es algebraico sobre K. Como $K \subseteq L_2$, también es algebraico sobre L_2 (trivialmente). Por el corolario anterior, el conjunto de elementos algebraicos sobre L_2 es un cuerpo. Este cuerpo contiene a L_1 y a L_2, por lo que contiene a su compuesto L_1L_2. Por tanto, la extensión L_1L_2/L_2 es algebraica.
- **Finitas:** Si L_1/K es finita, equivale a ser algebraica y finitamente generada. Por los dos apartados anteriores, el levantamiento L_1L_2/L_2 será simultáneamente algebraico y finitamente generado. Aplicando el Corolario 1.15, deducimos que L_1L_2/L_2 es una extensión finita.

□

Proposición 1.5.4: Automorfismos en extensiones algebraicas

Sea L/K una extensión algebraica y sea σ un K-endomorfismo de L. Entonces σ es un automorfismo.

Demostración. Como σ es un homomorfismo de cuerpos, sabemos que es inyectivo. Solo necesitamos demostrar que es suprayectivo.

Sea $\alpha \in L$. Como la extensión es algebraica, α tiene un polinomio mínimo $p = \mathrm{Min}_K(\alpha)$ de grado $\mathrm{gr}(p) = n$. Por el Lema 1.8 (invarianza de raíces), el endomorfismo σ induce una permutación sobre el conjunto finito de las raíces de p que residen en L.

Al ser una permutación de un conjunto finito, la restricción de σ a estas raíces es biyectiva y, en particular, suprayectiva. Por lo tanto, el elemento α (que es una de las raíces) debe tener una preimagen bajo σ.

Como todo elemento $\alpha \in L$ tiene preimagen, la aplicación σ es suprayectiva. Siendo inyectiva y suprayectiva, concluimos que σ es un automorfismo. □

Capítulo 2

Cuerpos de Descomposición

Capítulo 3

Extensiones Ciclotómicas

Capítulo 4

Extensiones separables

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 $\text{car}(K) \neq 2$, entonces $|\text{Gal}(L/K)| = 2$.
¿Por qué ocurre esto? Si $\alpha \in L \setminus K$, entonces $L = K(\alpha)$ y por tanto $p = \text{Min}_K(\alpha)$ 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 $\text{car}(K) \neq 2$, 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 $\text{Gal}(\mathbb{R}/\mathbb{Q}) = 1$ y por tanto $\text{Gal}(\mathbb{R}/K) = 1$ 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 $\sigma \in \text{Aut}(\mathbb{R})$. 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 $|\mathrm{Gal}(L/K)| \leq [L : K]_s \leq [L : K]$.

Recordemos que $\mathrm{Sub}(L/K)$ denota el conjunto de todas las subextensiones de 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.

Como $(\mathrm{Gal}(L/K))$ es un grupo, $\mathrm{Sub}(\mathrm{Gal}(L/K))$ es el conjunto de los subgrupos de $\mathrm{Gal}(L/K)$ y $\mathrm{Sub}(\mathrm{Gal}(L/K)/H)$ es el conjunto de los subgrupos de $\mathrm{Gal}(L/K)$ que contienen a H.

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:

$$(-)^\circ := \mathrm{Gal}(L/-)\colon\ \mathrm{Sub}(L/K) \longrightarrow \mathrm{Sub}(\mathrm{Gal}(L/K))$$
$$(-)^\circ := L^{(-)}\colon\ \mathrm{Sub}(\mathrm{Gal}(L/K)) \longrightarrow \mathrm{Sub}(L/K)$$

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, $L^\circ = \{1\} = 1$.
- $K^\circ = \mathrm{Gal}(L/K) = G$. Por definición, este es el grupo de Galois total G.
- $1^\circ = L^{\{1\}} = \{\alpha \in L : 1(\alpha) = \alpha\} = L$. 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: El operador de clausura

Se tiene que un elemento X (ya sea un cuerpo intermedio o un subgrupo) es cerrado si y solo si $X = X^{\circ\circ}$.
Llamamos a $X^{\circ\circ}$ la **clausura** de X porque la doble aplicación de la correspondencia cumple las propiedades axiomáticas de un operador de clausura:

- **Extensivo:** $X \subseteq X^{\circ\circ}$. Para un cuerpo M, $M \subseteq L^{\mathrm{Gal}(L/M)}$, lo que significa que el cuerpo fijo por los automorfismos que fijan M es, al menos, tan grande como M.
- **Idempotente:** $(X^{\circ\circ})^{\circ\circ} = X^{\circ\circ}$. Una vez cerrado, el conjunto no crece más mediante aplicaciones sucesivas.
- **Monótono:** Si $A \subseteq B$, entonces $A^{\circ\circ} \subseteq B^{\circ\circ}$.

Corolario 5.1.1: Anti-isomorfismo de conjuntos ordenados

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: Cuerpos y grupos siempre cerrados (Obs. 5.1.10)

Por las propiedades de la correspondencia, los elementos extremos L, 1 (el subgrupo identidad) y $\mathrm{Gal}(L/K)$ son siempre cerrados en L/K.
Sin embargo, el cuerpo base K **no tiene por qué ser cerrado**. Por ejemplo, si $L \neq K$ pero $\mathrm{Gal}(L/K) = 1$ (como ocurre en extensiones no normales o puramente inseparables), entonces la clausura de K es:

$$K^{\circ\circ} = (K^{\circ})^{\circ} = 1^{\circ} = L \neq K$$

En este caso, K no es un elemento cerrado de la correspondencia.

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) Demostración de** $[E_1^{\circ} : E_2^{\circ}] \leq [E_2 : E_1]$

Procedemos por inducción sobre el grado de la extensión $n = [E_2 : E_1]$.

Caso base ($n = 1$): Si $[E_2 : E_1] = 1$, entonces $E_2 = E_1$. Por definición, sus grupos de automorfismos asociados son idénticos: $E_1^\circ = E_2^\circ$. En consecuencia, el índice del subgrupo es $[E_1^\circ : E_2^\circ] = 1$, cumpliéndose la igualdad trivialmente.

Paso inductivo: Supongamos que el resultado es válido para cualquier extensión de grado menor que n. Consideramos un elemento $\alpha \in E_2 \setminus E_1$ y el cuerpo intermedio $E_1(\alpha)$.

Si $E_1(\alpha) \subsetneq E_2$, podemos descomponer la extensión en una torre: $E_1 \subseteq E_1(\alpha) \subseteq E_2$. Por la propiedad multiplicativa de los grados:

$$[E_2 : E_1] = [E_2 : E_1(\alpha)] \cdot [E_1(\alpha) : E_1]$$

Como ambos factores son estrictamente menores que n, aplicamos la hipótesis de inducción a cada uno. Usando la propiedad de los índices de subgrupos en una torre:

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

Caso de la extensión simple ($E_2 = E_1(\alpha)$): Sea $p = \mathrm{Min}_{E_1}(\alpha)$ el polinomio mínimo de α sobre E_1, con grado $s = \mathrm{gr}(p) = [E_2 : E_1]$. Definimos R como el conjunto de raíces de p contenidas en L.

Consideramos la aplicación entre el conjunto de clases laterales y las raíces:

$$\psi : E_1^\circ / E_2^\circ \longrightarrow R, \quad \psi(\sigma E_2^\circ) = \sigma(\alpha)$$

- **Buena definición:** Supongamos que $\sigma E_2^\circ = \tau E_2^\circ$. Esto implica que $\tau^{-1}\sigma \in E_2^\circ$. Por definición, el grupo $E_2^\circ = \mathrm{Gal}(L/E_2)$ fija todos los elementos de E_2. Como $\alpha \in E_2$, se tiene que $\tau^{-1}\sigma(\alpha) = \alpha$, lo que implica $\sigma(\alpha) = \tau(\alpha)$. Además, como $\sigma \in E_1^\circ$ fija E_1 y α es raíz de $p \in E_1[X]$, $\sigma(\alpha)$ es obligatoriamente otra raíz de p en L, por lo que la imagen está en R.
- **Inyectividad:** Supongamos que $\psi(\sigma E_2^\circ) = \psi(\tau E_2^\circ)$, es decir, $\sigma(\alpha) = \tau(\alpha)$. Multiplicando por la izquierda por el inverso, tenemos $\tau^{-1}\sigma(\alpha) = \alpha$. Dado que $\tau^{-1}\sigma$ ya fijaba E_1 (por ser composición de elementos de E_1°), ahora también fija al generador α. Por tanto, fija a todo el cuerpo $E_1(\alpha) = E_2$, lo que significa que $\tau^{-1}\sigma \in E_2^\circ$. Esto demuestra que $\sigma E_2^\circ = \tau E_2^\circ$.

Al ser ψ una aplicación inyectiva, el cardinal del dominio no puede superar al del codominio:

$$[E_1^\circ : E_2^\circ] \leq |R| \leq \mathrm{gr}(p) = [E_2 : E_1]$$

donde la última desigualdad se debe a que un polinomio de grado s tiene a lo sumo s raíces.

2) Demostración de $[H_1^\circ : H_2^\circ] \leq [H_2 : H_1]$
Aclaración previa sobre los representantes τ_i: Por hipótesis, el índice del subgrupo es finito y vale $[H_2 : H_1] = n$. En la teoría de grupos, el índice nos dice exactamente en cuántos "trozos"(clases laterales) podemos dividir el grupo grande (H_2) usando el subgrupo pequeño (H_1). Por tanto, el grupo H_2 se particiona en n clases laterales por la izquierda. Los elementos $\tau_1, \tau_2, \ldots, \tau_n \in H_2$ son los **representantes** elegidos para cada una de esas clases, de modo que $H_2/H_1 = \{\tau_1 H_1, \ldots, \tau_n H_1\}$. Como el propio subgrupo H_1 es una de estas clases laterales, resulta muy conveniente elegir el elemento neutro (la identidad de Galois) como su representante, por lo que fijamos $\tau_1 = 1$.

Desarrollo formal por reducción al absurdo:

Nuestro objetivo es demostrar que $[H_1^\circ : H_2^\circ] \leq n$. Supongamos lo contrario, es decir, que $[H_1^\circ : H_2^\circ] > n$. Recordemos que H_1° y H_2° son subcuerpos de L denominados **cuerpos fijos** por la acción de los subgrupos $H_1, H_2 \leq \mathrm{Gal}(L/K)$.

Formalmente, se definen como los conjuntos de elementos de L que permanecen invariantes ante la acción de cada uno de los automorfismos del subgrupo correspondiente:

$$H_1^\circ = \{a \in L \mid \sigma(a) = a, \quad \forall \sigma \in H_1\}$$
$$H_2^\circ = \{a \in L \mid \sigma(a) = a, \quad \forall \sigma \in H_2\}$$

Donde cada $\sigma \in \mathrm{Gal}(L/K)$ es un K-automorfismo del cuerpo L. Por las propiedades de la correspondencia de Galois, estos conjuntos siempre tienen estructura de cuerpo.

Si la dimensión del espacio vectorial H_1° sobre el cuerpo base H_2° es estrictamente mayor que n, significa que podemos encontrar al menos $n+1$ elementos en H_1° que sean linealmente independientes sobre H_2° (aquí H_2° funciona como el cuerpo donde cogemos los escalares). Llamemos a estos elementos $\alpha_1, \ldots, \alpha_n, \alpha_{n+1} \in H_1^\circ$.

Evaluemos todos nuestros representantes τ_i en cada uno de estos elementos y formemos la siguiente matriz A de tamaño $n \times (n+1)$ con coeficientes en L:

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

Cualquier sistema de ecuaciones lineales homogéneo con más incógnitas (columnas $= n+1$) que ecuaciones (filas $= n$) tiene siempre soluciones no triviales. Por tanto, el núcleo de esta matriz contiene vectores distintos de cero.

El argumento de minimidad (Truco de Artin): Sea r el rango por columnas de A. Evidentemente $r \leq n < n+1$. Reordenando los elementos α_i si fuera necesario, podemos suponer sin pérdida de generalidad que las primeras r columnas de A son linealmente independientes y que la columna $r+1$ es una combinación lineal exacta de estas r primeras columnas.

Esto nos garantiza que existe un vector solución $a \in L^{n+1}$ no nulo con una estructura muy específica:

$$a = (a_1, \ldots, a_r, 1, 0, \ldots, 0)^T$$

donde el 1 está en la posición $r+1$. Se cumple que $Aa = 0$.

Análisis de los coeficientes de la solución: Fijémonos en la primera fila del sistema $Aa = 0$. Al ser $\tau_1 = 1$ (la identidad), la primera fila de la matriz es simplemente $(\alpha_1, \alpha_2, \ldots, \alpha_{n+1})$. Multiplicando por el vector a, obtenemos:

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

Si todos los coeficientes $a_1, \ldots, a_r$ pertenecieran al cuerpo base H_2°, tendríamos una combinación lineal nula de elementos α_i sobre el cuerpo H_2°. Pero habíamos elegido los α_i precisamente para que fueran linealmente independientes sobre H_2°, lo cual haría esto imposible. Concluimos que al

menos uno de los coeficientes no pertenece a H_2°. Reordenando de nuevo si hace falta, supongamos que $a_1 \notin H_2^\circ$.

¿Qué significa que $a_1 \notin H_2^\circ$? Por la definición de cuerpo fijo, significa que existe algún automorfismo $\sigma \in H_2$ que "mueve.ª a_1, es decir, $\sigma(a_1) \neq a_1$.

La acción del automorfismo σ sobre el sistema: Tomemos la ecuación vectorial completa $Aa = 0$ y apliquémosle el automorfismo σ a todo el sistema. Dado que $\sigma(0) = 0$, obtenemos $\sigma(A)\sigma(a) = 0$.

Vamos a ver qué forma tiene la matriz transformada $\sigma(A)$. Su elemento genérico en la fila i y columna j es $\sigma(\tau_i(\alpha_j))$. Notemos que, al ser $\sigma \in H_2$, el conjunto de clases laterales por la izquierda $\{\sigma\tau_1 H_1, \ldots, \sigma\tau_n H_1\}$ es exactamente el mismo conjunto original de clases laterales (solo se han permutado). Por tanto, para cada índice i, existe un único índice $k = \rho(i)$ y un elemento $h_i \in H_1$ tales que:

$$\sigma\tau_i = \tau_{\rho(i)} h_i$$

Ahora evaluamos esto en α_j. Recordemos que $\alpha_j \in H_1^\circ$, lo que significa que es invariante (se queda fijo) ante cualquier elemento de H_1, incluyendo h_i. Por tanto $h_i(\alpha_j) = \alpha_j$. Sustituyendo:

$$\sigma(\tau_i(\alpha_j)) = \tau_{\rho(i)}(h_i(\alpha_j)) = \tau_{\rho(i)}(\alpha_j)$$

Esto demuestra un hecho crucial: la matriz $\sigma(A)$ es exactamente la misma matriz A, pero con las **filas permutadas** según la permutación ρ. Un sistema de ecuaciones no cambia sus soluciones por cambiar el orden de las filas, lo que implica directamente que:

$$A\sigma(a) = 0$$

La contradicción final: Tenemos ahora dos soluciones distintas para el sistema matricial original:

- $a = (a_1, \ldots, a_r, 1, 0, \ldots, 0)^T$
- $\sigma(a) = (\sigma(a_1), \ldots, \sigma(a_r), \sigma(1), 0, \ldots, 0)^T = (\sigma(a_1), \ldots, \sigma(a_r), 1, 0, \ldots, 0)^T$

(Dado que σ es un automorfismo de cuerpos, $\sigma(1) = 1$ y $\sigma(0) = 0$).

Como el sistema es lineal, la resta de dos soluciones es otra solución. Restamos ambos vectores:

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

Observemos este nuevo vector solución. Es distinto del vector nulo porque habíamos garantizado que $\sigma(a_1) \neq a_1$, luego su primera componente $a_1 - \sigma(a_1) \neq 0$. Sin embargo, tiene un cero en la

posición $r+1$. Esto significa que acabamos de encontrar una combinación lineal nula utilizando **únicamente** las primeras r columnas de la matriz A (sin necesitar la columna $r+1$).

Pero esto es una contradicción flagrante, porque habíamos elegido r precisamente de forma que las primeras r columnas de A fueran **linealmente independientes**.

Esta contradicción proviene de nuestra suposición inicial de que $[H_1^\circ : H_2^\circ] > n$. Por lo tanto, dicha suposición debe ser falsa, quedando demostrado que $[H_1^\circ : H_2^\circ] \leq n = [H_2 : H_1]$. □

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 $H_1 \leq H_2 \leq \mathrm{Gal}(L/K)$ 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) Demostración para subextensiones:**

Queremos probar que si E_1 es cerrado ($E_1 = E_1^{\circ\circ}$) y la extensión es finita, entonces E_2 también es cerrado y se da la igualdad de grados.

- **Paso 1: Aplicación de la Proposición 5.5 (parte 1).** Consideramos la inclusión de subextensiones $E_1 \subseteq E_2$. Por la proposición demostrada anteriormente, sabemos que el índice del subgrupo asociado no supera al grado de la extensión:
$$[E_1^\circ : E_2^\circ] \leq [E_2 : E_1] \tag{I}$$
- **Paso 2: Aplicación de la Proposición 5.5 (parte 2).** Ahora aplicamos la segunda parte de la proposición a los subgrupos $H_1 = E_2^\circ$ y $H_2 = E_1^\circ$. Notemos que al ser $E_1 \subseteq E_2$, se invierte el orden en los grupos: $E_2^\circ \subseteq E_1^\circ$. La proposición nos dice que el grado de la extensión de los cuerpos fijos no supera al índice de los grupos:
$$[E_2^{\circ\circ} : E_1^{\circ\circ}] \leq [E_1^\circ : E_2^\circ] \tag{II}$$
- **Paso 3: Uso de la hipótesis de clausura.** Como E_1 es cerrado en L/K por hipótesis, se cumple que $E_1 = E_1^{\circ\circ}$. Sustituyendo esto en la desigualdad (II) y encadenándola con la (I), obtenemos:
$$[E_2^{\circ\circ} : E_1] \leq [E_1^\circ : E_2^\circ] \leq [E_2 : E_1] \tag{III}$$
- **Paso 4: Conclusión por inclusión y dimensiones.** Sabemos que para cualquier subextensión se cumple la inclusión $E_2 \subseteq E_2^{\circ\circ}$. En una torre de cuerpos $E_1 \subseteq E_2 \subseteq E_2^{\circ\circ}$, si el grado total $[E_2^{\circ\circ} : E_1]$ es menor o igual al grado intermedio $[E_2 : E_1]$, la única posibilidad lógica es que los cuerpos sean idénticos:
$$E_2 = E_2^{\circ\circ}$$
Esto demuestra que E_2 es **cerrado**. Al ser idénticos, sus grados son iguales, lo que fuerza a que todas las desigualdades en (III) se conviertan en igualdades, probando que $[E_1^\circ : E_2^\circ] = [E_2 : E_1]$.

(2) Demostración para subgrupos:

El razonamiento es totalmente simétrico al anterior, intercambiando los roles de cuerpos y grupos.

- Por la Proposición 5.5 (parte 2) aplicada a $H_1 \leq H_2$, tenemos que $[H_1^\circ : H_2^\circ] \leq [H_2 : H_1]$.
- Aplicando la parte 1 de la misma proposición a los cuerpos $E_1 = H_2^\circ$ y $E_2 = H_1^\circ$ (recordando que $H_2^\circ \subseteq H_1^\circ$), obtenemos $[H_2^{\circ\circ} : H_1^{\circ\circ}] \leq [H_1^\circ : H_2^\circ]$.
- Como H_1 es cerrado, $H_1 = H_1^{\circ\circ}$. Combinando las desigualdades:
$$[H_2^{\circ\circ} : H_1] \leq [H_1^\circ : H_2^\circ] \leq [H_2 : H_1]$$
- Dada la inclusión natural $H_2 \subseteq H_2^{\circ\circ}$, y que el índice de la clausura no puede superar al del grupo original respecto al mismo subgrupo cerrado H_1, concluimos que $H_2 = H_2^{\circ\circ}$.
- Por tanto, H_2 es **cerrado** y se verifica la igualdad de índices $[H_1^\circ : H_2^\circ] = [H_2 : H_1]$.

□

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: Cierre de subgrupos finitos

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

Demostración. Sea H un subgrupo finito de $\mathrm{Gal}(L/K)$. Para demostrar que es cerrado, aplicaremos los resultados de cierre obtenidos anteriormente:

- Consideramos el subgrupo trivial $H_1 = \{1\}$.
- Sabemos que el subgrupo trivial $\{1\}$ es siempre un subgrupo **cerrado** en $\mathrm{Gal}(L/K)$. Esto se debe a que su cuerpo fijo es todo el cuerpo superior, $\{1\}^\circ = L$, y el grupo de automorfismos que fijan L es únicamente la identidad, $L^\circ = \{1\}$.
- Por hipótesis, H es un subgrupo finito, lo que implica que el índice del subgrupo trivial dentro de H es finito: $[H : \{1\}] = |H| < \infty$.
- Aplicamos ahora el segundo apartado del corolario anterior, el cual establece que si $H_1 \leq H$ es una inclusión de subgrupos donde el subgrupo menor (H_1) es cerrado y el índice $[H : H_1]$ es finito, entonces el subgrupo mayor (H) es obligatoriamente cerrado.

Por lo tanto, al ser $\{1\}$ cerrado y $[H : \{1\}]$ finito, concluimos que H 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. Vamos a demostrar la equivalencia formando un ciclo de implicaciones lógicas y demostrando las equivalencias directas cuando sea conveniente.

(1) $\implies$ (2): Toda subextensión es de Galois.
Recordemos la definición de una clase de extensiones cerrada para levantamientos: si una extensión L_1/K pertenece a una clase $\mathcal{C}$, y tenemos otra extensión admisible L_2/K, entonces la extensión "levantada"hacia el cuerpo compuesto, L_1L_2/L_2, también pertenece a la clase $\mathcal{C}$.

Sabemos que la clase de las extensiones de Galois es cerrada para levantamientos (al igual que lo son las extensiones finitas, algebraicas, finitamente generadas y simples).

Para nuestro caso, definimos nuestras extensiones admisibles sobre el cuerpo base K:

- Sea $L_1 = L$. Por la hipótesis (1), sabemos que L/K es una extensión de Galois, luego $L_1/K \in \mathcal{C}$.
- Sea $L_2 = E$, donde E es un cuerpo intermedio ($K \subseteq E \subseteq L$). Esta es la extensión hacia la que queremos levantar.

Calculamos el cuerpo compuesto L_1L_2:

$$L_1L_2 = L \cdot E$$

Como E es un subcuerpo de L (es decir, $E \subseteq L$), el menor cuerpo que contiene a ambos es simplemente el cuerpo más grande. Por tanto, el cuerpo compuesto es $L_1L_2 = L$.

Aplicando la definición de la propiedad de cierre bajo levantamientos:

$$L_1/K \text{ es de Galois} \implies L_1L_2/L_2 \text{ es de Galois}$$

Sustituyendo nuestros cuerpos concretos en la implicación, obtenemos:

$$L/K \text{ es de Galois} \implies L/E \text{ es de Galois}$$

Lo cual demuestra de forma directa y estructural que, para todo cuerpo intermedio $E \in \mathrm{Sub}(L/K)$, la subextensión L/E es de Galois.

(2) $\implies$ (3): Toda subextensión es cerrada.
Supongamos que L/E es una extensión de Galois para cualquier cuerpo intermedio E. Queremos demostrar que E es una subextensión cerrada, es decir, que $E = E^{\circ\circ}$.

Por las propiedades de la correspondencia de Galois, siempre se tiene la inclusión trivial $E \subseteq E^{\circ\circ}$. Para demostrar la igualdad, probaremos la inclusión contraria viendo que si un elemento α no está en E, tampoco puede estar en $E^{\circ\circ}$. Recordemos que $E^{\circ\circ}$ es el cuerpo fijo del grupo $\mathrm{Gal}(L/E)$. Por tanto, demostrar que $\alpha \notin E^{\circ\circ}$ equivale a encontrar al menos un automorfismo $\sigma \in \mathrm{Gal}(L/E)$ que "mueva.ª α (es decir, $\sigma(\alpha) \neq \alpha$).

Sea $\alpha \in L \setminus E$ y sea $p = \mathrm{Min}_E(\alpha)$.

- Como L/E es normal por hipótesis, p factoriza completamente en L, es decir, todas sus raíces están en L.
- Como L/E es separable y $\alpha \notin E$ (luego el grado de p es estrictamente mayor que 1), p no tiene raíces múltiples.

Por consiguiente, existe obligatoriamente otra raíz $\beta \in L$ del mismo polinomio p, con $\beta \neq \alpha$.

Por la Proposición 1.10 (isomorfismo de raíces conjugadas), sabemos que existe un E-isomorfismo $\tau : E(\alpha) \xrightarrow{\simeq} E(\beta)$ tal que $\tau(\alpha) = \beta$. Sea $\overline{L}$ la clausura algebraica de L. Como la extensión $L/E(\alpha)$ es algebraica, el Teorema de Extensión de Homomorfismos garantiza que podemos extender τ a un homomorfismo global $\sigma : L \to \overline{L}$.

Pero, al ser L/E una extensión normal, cualquier E-homomorfismo de L en su clausura algebraica cumple que $\sigma(L) = L$. Esto convierte a σ en un E-automorfismo de L, es decir, $\sigma \in \mathrm{Gal}(L/E)$. Evaluando en nuestro elemento: $\sigma(\alpha) = \beta \neq \alpha$. Hemos encontrado el automorfismo que mueve a α, luego $\alpha \notin E^{\circ\circ}$. Esto prueba que $E^{\circ\circ} \subseteq E$ y, por tanto, $E = E^{\circ\circ}$.

(3) $\implies$ (4): El cuerpo base es cerrado.
Si toda subextensión de L/K es cerrada, en particular el propio cuerpo base K es una subextensión (la más pequeña posible). Por lo tanto, K es cerrado. (La extensión es algebraica por hipótesis heredada).

(4) $\implies$ (5): Igualdad del cuerpo fijo.
Asumimos que K es cerrado, lo que por definición significa que $K = K^{\circ\circ}$. Desplegando la notación de la correspondencia de Galois:

- K° es el grupo de automorfismos que fijan K. Esto es, por definición, todo el grupo de Galois: $K^\circ = \mathrm{Gal}(L/K) = G$.
- Aplicando el segundo círculo, $K^{\circ\circ} = (K^\circ)^\circ = G^\circ$.

Sustituyendo en la hipótesis, obtenemos directamente $K = G^\circ$. Esto significa exactamente que el conjunto de elementos de L que quedan fijos por todos los elementos de G es exactamente K.

(5) $\iff$ (6): Equivalencia lógica del cuerpo fijo.
Esta equivalencia es un mero parafraseo de la definición de cuerpo fijo.

- (5) $\implies$ (6): Si $G^\circ = K$, significa que si un elemento está en L pero no en K ($\alpha \in L \setminus K$), entonces no puede pertenecer al cuerpo fijo G°. Al no estar en el cuerpo fijo, debe existir al menos un automorfismo en el grupo G que no lo deje fijo, es decir, $\exists \sigma \in G$ tal que $\sigma(\alpha) \neq \alpha$.
- (6) $\implies$ (5): Si para todo $\alpha \notin K$ existe un automorfismo que lo mueve, entonces ningún elemento fuera de K puede pertenecer al cuerpo fijo G°. Por otro lado, todos los elementos de K quedan fijos por definición de los K-automorfismos de G. Por tanto, el cuerpo fijo es exactamente K ($G^\circ = K$).

(5) $\implies$ (1): Caracterización de Galois.
Esta es la implicación fundamental. Supongamos que $G^\circ = K$. Queremos demostrar que L/K es de Galois, es decir, que es simultáneamente normal y separable. Para ello, tomamos un elemento arbitrario $\alpha \in L$, sea $p = \mathrm{Min}_K(\alpha)$ su polinomio mínimo, con $n = \mathrm{gr}(p)$. Debemos demostrar que p factoriza completamente en L (normalidad) y que todas sus raíces son simples (separabilidad).

Definimos $R = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ como el conjunto de las **distintas** raíces de p que residen dentro de L. (Sabemos que $r \geq 1$ porque al menos el propio α está en R).

Construimos el polinomio $q(X)$ usando exclusivamente estas raíces distintas:

$$q(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_r)$$

Por construcción, $q(X)$ es un polinomio de $L[X]$ que no tiene raíces múltiples y cuyo grado es r.

Consideremos la acción de cualquier automorfismo $\sigma \in G = \mathrm{Gal}(L/K)$ sobre el polinomio $q(X)$. Como $p \in K[X]$, sus coeficientes están fijos por σ, por lo que $\sigma(p) = p$. Esto implica que σ envía raíces de p en raíces de p. Dado que $\sigma(L) = L$, σ induce una permutación sobre el conjunto finito R.

Si aplicamos σ a los coeficientes de $q(X)$, lo que estamos haciendo es aplicar σ a sus raíces:

$$\sigma(q(X)) = (X - \sigma(\alpha_1))(X - \sigma(\alpha_2)) \cdots (X - \sigma(\alpha_r))$$

Como σ simplemente permuta los elementos de R, los factores son exactamente los mismos pero en distinto orden. Por tanto, $\sigma(q(X)) = q(X)$.

Esto significa que todos y cada uno de los coeficientes del polinomio $q(X)$ quedan fijos por **todos** los automorfismos $\sigma \in G$. Por la hipótesis (5), el conjunto de elementos de L que quedan fijos por todo el grupo de Galois es exactamente el cuerpo base K. Por consiguiente, los coeficientes de $q(X)$ pertenecen a K, lo que implica que $q \in K[X]$.

Recapitulemos: tenemos un polinomio $q \in K[X]$ que tiene a α como raíz (pues $\alpha \in R$). Por la propia definición de polinomio mínimo, el mínimo $p(X)$ debe dividir a cualquier otro polinomio en $K[X]$ que anule a α. Por tanto, p divide a q.

Sin embargo, analizamos los grados:

$$\mathrm{gr}(q) = r \quad \text{y} \quad \mathrm{gr}(p) = n$$

Como R contiene, a lo sumo, a todas las raíces de p, es obvio que $r \leq n$. El único modo en que un polinomio p de grado n pueda dividir a un polinomio q de grado $r \leq n$ (siendo ambos mónicos) es que sean el mismo polinomio.

Concluimos que $p(X) = q(X)$ y $r = n$. Esta igualdad nos da automáticamente las dos propiedades que buscábamos:

- *Normalidad:* Como $p = q$ y q se construyó multiplicando factores $(X - \alpha_i)$ con $\alpha_i \in L$, p descompone completamente en L.
- *Separabilidad:* Como q se construyó tomando raíces distintas (sin repeticiones), p no tiene raíces múltiples.

Dado que esto es cierto para todo $\alpha \in L$, la extensión L/K es de Galois. □

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. $[L : K] = |\operatorname{Gal}(L/K)|$.
3. $[L : E] = |\operatorname{Gal}(L/E)|$ para todo $E \in \operatorname{Sub}(L/K)$.

Demostración. Vamos a demostrar en primer lugar la equivalencia entre (1) y (2) analizando la cadena de desigualdades fundamentales que relaciona el orden del grupo de Galois, el grado de separabilidad y el grado de la extensión.

Demostración de (1) $\iff$ (2):

Sea $\overline{L}$ una clausura algebraica de L. Recordemos que el grupo de Galois, $\operatorname{Gal}(L/K)$, está formado por todos los K-automorfismos de L. Todo automorfismo $\tau \in \operatorname{Gal}(L/K)$ puede verse de forma natural como un K-homomorfismo (o inmersión) del cuerpo L en su clausura algebraica $\overline{L}$, con la particularidad de que su imagen es exactamente L ($\tau(L) = L$).

Sea S_K^L el conjunto de todos los K-homomorfismos de L en $\overline{L}$. (En la notación original, si σ es la inclusión de K en $\overline{L}$, este conjunto se denota como S_σ^L). Como todo elemento de $\operatorname{Gal}(L/K)$ es una de estas inmersiones, tenemos la inclusión de conjuntos:

$$\operatorname{Gal}(L/K) \subseteq S_K^L$$

Lo que implica que el número de automorfismos es menor o igual al número total de inmersiones:

$$|\operatorname{Gal}(L/K)| \leq |S_K^L|$$

Por teoría de cuerpos (Proposición 5.2), el número total de K-homomorfismos de L en $\overline{L}$ se define como el **grado de separabilidad** de la extensión, denotado como $[L:K]_s$. A su vez, es un resultado conocido que el grado de separabilidad nunca supera al grado total de la extensión $[L:K]$.

Juntando todo esto, obtenemos la cadena de desigualdades fundamental:

$$|\operatorname{Gal}(L/K)| \leq [L:K]_s \leq [L:K] \qquad (*)$$

Analicemos cuándo estas dos desigualdades se convierten en igualdades estrictas:

- **La segunda desigualdad ($[L:K]_s \leq [L:K]$):** El Teorema 4.12 nos garantiza que el número de inmersiones coincide con el grado de la extensión si y solo si todos los elementos de L tienen polinomios mínimos con raíces simples. Es decir, esta desigualdad es una igualdad **si y solo si L/K es una extensión separable**.
- **La primera desigualdad ($|\operatorname{Gal}(L/K)| \leq [L:K]_s$):** Para que el número de K-automorfismos sea exactamente igual al número de K-inmersiones en $\overline{L}$, toda inmersión $\tau : L \to \overline{L}$ debe ser, en realidad, un automorfismo de L. Esto significa que para cualquier $\tau \in S_K^L$, se debe cumplir que $\tau(L) = L$ (o de forma equivalente, $\tau(L) \subseteq L$). Como vimos en el Teorema 2.11 (Condiciones equivalentes de normalidad), que todo K-homomorfismo en la clausura algebraica deje invariante a L es cierto **si y solo si L/K es una extensión normal**.

En conclusión, para que los extremos de la cadena (*) sean iguales, es decir, para que $|\operatorname{Gal}(L/K)| = [L:K]$, es necesario y suficiente que se den ambas igualdades intermedias. Esto ocurre si y solo si la extensión L/K es simultáneamente normal y separable. Por definición, esto significa que L/K es una extensión de Galois. Así queda probada la equivalencia (1) $\iff$ (2).

Demostración de (1) $\iff$ (3):

Esta equivalencia es ahora una consecuencia rápida de la equivalencia anterior y de las propiedades hereditarias de las extensiones de Galois.

- **(1) $\implies$ (3):** Supongamos que L/K es de Galois y sea E cualquier subextensión ($K \subseteq E \subseteq L$). Por el Teorema 5.10 (demostrado previamente usando levantamientos o el análisis de subextensiones cerradas), sabemos que si L/K es de Galois, entonces L/E también es una extensión de Galois. Aplicando la equivalencia recién demostrada (1 $\iff$ 2) pero a la extensión L/E, deducimos directamente que $[L:E] = |\operatorname{Gal}(L/E)|$. Como E era arbitrario, se cumple (3).
- **(3) $\implies$ (1):** Si asumimos que $[L:E] = |\operatorname{Gal}(L/E)|$ para absolutamente toda subextensión $E \in \operatorname{Sub}(L/K)$, esta propiedad debe cumplirse en particular para la subextensión trivial $E = K$. Sustituyendo E por K, obtenemos $[L:K] = |\operatorname{Gal}(L/K)|$, que es exactamente la condición (2). Y como hemos demostrado exhaustivamente que (2) $\implies$ (1), concluimos que L/K es una extensión de Galois.

□

Teorema 5.2.2: Teorema Fundamental de la Teoría de Galois

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

1. La correspondencia de Galois es un **anti-isomorfismo de conjuntos ordenados** (una biyección que invierte el orden) entre $\mathrm{Sub}(L/K)$ (el conjunto de cuerpos intermedios) y $\mathrm{Sub}(G)$ (el conjunto de subgrupos de G).
2. Si X e Y están ambos en $\mathrm{Sub}(L/K)$ o en $\mathrm{Sub}(G)$ y se cumple que $X \subseteq Y$, entonces se invierten los índices/grados:

   $$[X^\circ : Y^\circ] = [Y : X]$$

   En particular, evaluando en los extremos se obtienen las siguientes igualdades:

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

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

Demostración. **Demostración de (1): El Anti-isomorfismo.**

Para demostrar que las aplicaciones de la correspondencia de Galois ($E \mapsto E^\circ$ y $H \mapsto H^\circ$) conforman una biyección perfecta entre los cuerpos intermedios y los subgrupos, necesitamos probar que son funciones inversas mutuas. Es decir, debemos garantizar que todo elemento coincide con su clausura: $E = E^{\circ\circ}$ para todo cuerpo intermedio y $H = H^{\circ\circ}$ para todo subgrupo.

- *Para los cuerpos intermedios:* Por hipótesis, L/K es una extensión de Galois. Como vimos en las condiciones equivalentes (Teorema 5.10), que una extensión sea de Galois implica que absolutamente **toda subextensión** $E \in \mathrm{Sub}(L/K)$ **es cerrada**. Por tanto, $E = E^{\circ\circ}$ siempre se cumple.
- *Para los subgrupos:* Al ser L/K una extensión finita (y de Galois), su grupo de Galois $G = \mathrm{Gal}(L/K)$ es un grupo finito (de orden igual a $[L : K]$). En consecuencia, cualquier subgrupo $H \in \mathrm{Sub}(G)$ es obligatoriamente un subgrupo finito. Por el Corolario 5.7, todo subgrupo finito del grupo de Galois es cerrado. Por tanto, $H = H^{\circ\circ}$ siempre se cumple.

Dado que todos los elementos de ambos conjuntos son cerrados, las aplicaciones restringen a una biyección exacta. Como ya sabíamos por la Proposición 5.3 que el operador $^\circ$ invierte las inclusiones (es antítono), esta biyección constituye un anti-isomorfismo de conjuntos ordenados.

Demostración de (2): Fórmulas de índices y grados.

La igualdad general $[X^\circ : Y^\circ] = [Y : X]$ es consecuencia directa de la Proposición 5.6 (y su corolario). Dicha proposición establecía que si el elemento más pequeño (X) es cerrado, entonces los grados coinciden. Como acabamos de demostrar en el apartado (1) que **todos** los elementos son cerrados, la igualdad es universalmente válida para cualquier par $X \subseteq Y$.

Vamos a deducir las fórmulas particulares (a) y (b) sustituyendo los casos extremos:

Demostración de (a) - Para un cuerpo intermedio E:

- Tomamos $X = E$ e $Y = L$. Aplicamos la fórmula general:

$$[E^\circ : L^\circ] = [L : E]$$

  Sabemos que el grupo de automorfismos que fijan todo L es únicamente la identidad, luego $L^\circ = \{1\}$. Sustituyendo: $[E^\circ : \{1\}] = [L : E]$. Como el índice respecto al subgrupo trivial es el orden del grupo, concluimos que $|E^\circ| = [L : E]$.

- Tomamos $X = K$ e $Y = E$. Aplicamos la fórmula general:

$$[K^\circ : E^\circ] = [E : K]$$

  Sabemos que el grupo de automorfismos que fijan el cuerpo base K es el grupo de Galois completo, luego $K^\circ = G$. Sustituyendo directamente obtenemos $[G : E^\circ] = [E : K]$.

Demostración de (b) - Para un subgrupo H:

- Tomamos $X = \{1\}$ e $Y = H$. Aplicamos la fórmula general:

$$[\{1\}^\circ : H^\circ] = [H : \{1\}]$$

  El cuerpo fijado por la identidad es todo el cuerpo superior, por lo que $\{1\}^\circ = L$. El índice $[H : \{1\}]$ es simplemente el orden del grupo $|H|$. Sustituyendo, obtenemos $[L : H^\circ] = |H|$.

- Tomamos $X = H$ e $Y = G$. Aplicamos la fórmula general:

$$[H^\circ : G^\circ] = [G : H]$$

  El cuerpo fijado por todo el grupo de Galois es (por ser extensión de Galois) el cuerpo base K, luego $G^\circ = K$. Sustituyendo directamente obtenemos $[H^\circ : K] = [G : H]$.

Estas deducciones completan la demostración de la estructura numérica de la correspondencia de Galois. □

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

(1) E/K es de Galois.

(1) E/K es normal.

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

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

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

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

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

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

Demostración. Vamos a desglosar el ciclo de implicaciones y la demostración del isomorfismo final paso a paso. Recordemos que por hipótesis global, L/K es una extensión de Galois (finita, normal y separable).

(1) $\iff$ (2): La separabilidad se hereda (es gratis).
Recordemos que una extensión es de Galois si y solo si es normal y separable. Como L/K es separable por hipótesis, y la separabilidad es una propiedad que se hereda a las subextensiones (Proposición 4.13), la extensión intermedia E/K es automáticamente separable. Por tanto, para que E/K sea de Galois, la única condición que le falta cumplir es ser normal. Esto hace que las afirmaciones (1) y (2) sean estrictamente equivalentes.

(2) $\implies$ (3): La normalidad encierra a las raíces conjugadas.
Supongamos que E/K es normal. Tomemos un elemento cualquiera $\alpha \in E$ y un automorfismo cualquiera $\sigma \in \mathrm{Gal}(L/K)$. Nuestro objetivo es demostrar que $\sigma(\alpha)$ se queda dentro de E.

Sea $p = \mathrm{Min}_K(\alpha)$ su polinomio mínimo sobre K. Como $\alpha \in E$ y E/K es normal, este polinomio factoriza completamente dentro de E. Es decir, todas sus raíces $\alpha_1, \alpha_2, \ldots, \alpha_n$ pertenecen a E.

Ahora, apliquemos el automorfismo σ a α. Como σ es un K-automorfismo, deja fijos los coeficientes de p (que están en K), lo que implica por el Lema de Invarianza que σ envía raíces de p a raíces de p. Por consiguiente, $\sigma(\alpha)$ debe ser obligatoriamente una de esas raíces α_i. Y como ya sabíamos que todas las $\alpha_i \in E$, concluimos que $\sigma(\alpha) \in E$. Como esto vale para todo $\alpha \in E$, hemos demostrado que $\sigma(E) \subseteq E$.

(3) $\implies$ (4): El subgrupo de Galois es normal.
Supongamos que $\sigma(E) \subseteq E$ para todo $\sigma \in \mathrm{Gal}(L/K)$. Queremos ver que el subgrupo $H = \mathrm{Gal}(L/E)$ es un subgrupo normal del grupo total $G = \mathrm{Gal}(L/K)$.

Por la definición de subgrupo normal en teoría de grupos, debemos demostrar que para cualquier

$\sigma \in G$ y cualquier $\tau \in H$, el elemento conjugado $\sigma^{-1}\tau\sigma$ pertenece a H. ¿Qué significa pertenecer a $H = \mathrm{Gal}(L/E)$? Significa ser un automorfismo de L que deja fijo a todo elemento de E.

Tomemos un elemento cualquiera $\alpha \in E$ y evaluemos la composición:

- Primero actúa σ: Por la hipótesis (3), sabemos que $\sigma(\alpha) \in E$. Llamemos $y = \sigma(\alpha)$, con $y \in E$.
- Luego actúa τ: Al ser $\tau \in \mathrm{Gal}(L/E)$, deja fijos todos los elementos de E. Como $y \in E$, entonces $\tau(y) = y$. Sustituyendo de vuelta: $\tau(\sigma(\alpha)) = \sigma(\alpha)$.
- Finalmente actúa σ^{-1}: Aplicamos σ^{-1} a ambos lados de la igualdad anterior:

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

Hemos demostrado que el automorfismo conjugado $\sigma^{-1}\tau\sigma$ deja fijo el elemento α. Como esto es válido para todo $\alpha \in E$, el conjugado pertenece a $\mathrm{Gal}(L/E)$, probando que es un subgrupo normal.

(4) $\implies$ (2): El truco del cuerpo fijo.
Supongamos que $\mathrm{Gal}(L/E)$ es un subgrupo normal de $\mathrm{Gal}(L/K)$. Queremos ver que E/K es normal. Usaremos el criterio de que todo K-homomorfismo $\rho : E \to \overline{L}$ debe cumplir $\rho(E) \subseteq E$.

- *Paso 1: Extender el homomorfismo.* Como L/E es una extensión algebraica, el Teorema de Extensión nos permite prolongar ρ a un K-homomorfismo global $\sigma : L \to \overline{L}$.
- *Paso 2: σ es un automorfismo.* Como la extensión total L/K es normal por hipótesis, cualquier K-homomorfismo de L cumple $\sigma(L) = L$. Esto nos asegura que $\sigma \in \mathrm{Gal}(L/K)$.
- *Paso 3: Bajar a E.* Sea $\alpha \in E$. Queremos probar que $\rho(\alpha) = \sigma(\alpha) \in E$. Sabemos que la subextensión L/E es de Galois (por ser L/K de Galois), luego por el Teorema Fundamental, E es exactamente el cuerpo fijo de su grupo de Galois: $E = \mathrm{Gal}(L/E)^\circ$. Para probar que $\sigma(\alpha) \in E$, basta con ver que es invariante bajo cualquier $\tau \in \mathrm{Gal}(L/E)$.

  Evaluemos $\tau(\sigma(\alpha))$. Esto es equivalente a $\sigma(\sigma^{-1}\tau\sigma(\alpha))$. Por hipótesis, $\mathrm{Gal}(L/E)$ es normal, luego el conjugado $\sigma^{-1}\tau\sigma$ es algún elemento $\tau' \in \mathrm{Gal}(L/E)$. Como $\alpha \in E$ y τ' fija E, tenemos que $\tau'(\alpha) = \alpha$. Sustituyendo: $\tau(\sigma(\alpha)) = \sigma(\tau'(\alpha)) = \sigma(\alpha)$.

  Como $\sigma(\alpha)$ queda fijo ante todo $\tau \in \mathrm{Gal}(L/E)$, obligatoriamente $\sigma(\alpha) \in \mathrm{Gal}(L/E)^\circ = E$.

Esto demuestra que todo $\rho(E) \subseteq E$, por lo que E/K es normal.

Demostración de la aplicación de Restricción y el Isomorfismo:
Supongamos ahora que se verifican las condiciones. Definimos la aplicación de restricción:

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

- *Buena definición:* La aplicación tiene sentido porque por la condición (3), $\sigma(E) \subseteq E$. Al ser σ una inyección lineal en un espacio de dimensión finita sobre K, forzosamente $\sigma(E) = E$. Luego la restricción de σ a E es efectivamente un K-automorfismo de E, es decir, pertenece a $\mathrm{Gal}(E/K)$.

- *Es homomorfismo:* La restricción de una composición es la composición de las restricciones.
- *El Núcleo:* ¿Qué elementos $\sigma \in \mathrm{Gal}(L/K)$ van a parar al elemento neutro de $\mathrm{Gal}(E/K)$ (que es la identidad id_E)? Exactamente aquellos que cumplen $\sigma|_E = \mathrm{id}_E$, es decir, los que dejan fijos todos los elementos de E. Por definición, este conjunto es $\mathrm{Gal}(L/E)$. Por tanto, $\mathrm{Ker}(f) = \mathrm{Gal}(L/E)$.

Aplicamos el **Primer Teorema de Isomorfía** de grupos:

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Ker}(f)} \simeq \mathrm{Im}(f) \subseteq \mathrm{Gal}(E/K)$$

Para ver que la imagen es todo $\mathrm{Gal}(E/K)$ (es decir, que f es suprayectiva), comparamos las cardinalidades. Como las tres extensiones implicadas (L/K, L/E y E/K) son de Galois, el orden de sus grupos de Galois coincide exactamente con el grado de sus extensiones.

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

Por la propiedad multiplicativa del grado en la torre $K \subseteq E \subseteq L$, sabemos que $[L:K] = [L:E][E:K]$, luego la fracción se simplifica a:

$$|\operatorname{Im} f| = [E:K]$$

Y como E/K es de Galois, $[E:K] = |\operatorname{Gal}(E/K)|$.

Al tener la imagen el mismo tamaño finito que el codominio, la aplicación f es suprayectiva, y el isomorfismo queda establecido:

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

□

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

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

es un isomorfismo de grupos.

Demostración. Vamos a dividir la demostración en cuatro bloques lógicos para garantizar el rigor en cada afirmación.

Paso 1: Naturaleza de las extensiones (Finitud y propiedad de Galois)

- *La extensión $L/(L \cap E)$:* Como L/K es de Galois por hipótesis, sabemos por el Teorema 5.10 (propiedad hereditaria) que cualquier subextensión superior es de Galois. Al ser $L \cap E$ un cuerpo intermedio ($K \subseteq L \cap E \subseteq L$), la extensión $L/(L \cap E)$ hereda automáticamente la finitud y la propiedad de Galois.
- *La extensión LE/E:* Por hipótesis, L/K es finita y de Galois. Esto significa que L es el cuerpo de descomposición de un cierto polinomio separable $p \in K[X]$. Al considerar el cuerpo compuesto LE, podemos ver este mismo polinomio p como un elemento de $E[X]$ (ya que $K \subseteq E$). El cuerpo LE se forma adjuntando a E las raíces de p, por lo que LE es exactamente el cuerpo de descomposición de p sobre E. Al ser un polinomio separable, LE/E es una extensión normal y separable, es decir, de Galois. Su finitud se deduce de la Proposición 1.18 (el grado del compuesto no supera el producto de los grados).

Paso 2: Buena definición de la aplicación de restricción
Definimos la aplicación $f = \mathrm{Res}_L^{LE}$, que toma un automorfismo $\sigma \in \mathrm{Gal}(LE/E)$ y lo restringe al cuerpo L, denotándolo $\sigma|_L$. ¿Por qué $\sigma|_L \in \mathrm{Gal}(L/L \cap E)$?

- Como L/K es normal, sabemos que cualquier K-homomorfismo del cuerpo compuesto que se aplique sobre L debe cumplir que la imagen de L es L. Como σ fija E (y por ende fija $K \subseteq E$), σ es un K-homomorfismo, luego $\sigma(L) = L$. Esto hace que $\sigma|_L$ sea un automorfismo bien definido de L.
- Además, como $\sigma \in \mathrm{Gal}(LE/E)$, σ deja fijos **todos** los elementos de E. En particular, dejará fijos los elementos de la intersección $L \cap E$. Por tanto, $\sigma|_L$ es un automorfismo de L que fija $L \cap E$, lo que demuestra que $\sigma|_L \in \mathrm{Gal}(L/L \cap E)$.

Paso 3: Inyectividad de f
Para demostrar que f es un homomorfismo inyectivo, basta con calcular su núcleo ($\mathrm{Ker}(f)$) y ver que solo contiene al elemento neutro (la identidad id_{LE}).

Supongamos que $\sigma \in \mathrm{Ker}(f)$. Por definición, esto significa que $f(\sigma) = \sigma|_L = \mathrm{id}_L$. Es decir, $\sigma(x) = x$ para todo $x \in L$. Pero recordemos de dónde viene σ: es un elemento de $\mathrm{Gal}(LE/E)$, por lo que, por definición, también fija todo elemento de E.

El cuerpo compuesto LE está generado por las sumas, productos y cocientes de elementos de L y de E. Si σ deja fijos todos los elementos de L y todos los elementos de E, obligatoriamente deja fijos todos los elementos generados por ellos. Por tanto, $\sigma(x) = x$ para todo $x \in LE$, lo que implica que $\sigma = \mathrm{id}_{LE}$. Como $\mathrm{Ker}(f) = \{\mathrm{id}_{LE}\}$, la aplicación es inyectiva.

Paso 4: Suprayectividad de f (El argumento del cuerpo fijo)
Este es el paso más brillante de la demostración. Denotemos la imagen de nuestra aplicación como $H = \mathrm{Im}\, f \subseteq \mathrm{Gal}(L/L \cap E)$. Queremos demostrar que H es todo el grupo, lo cual haremos utilizando la correspondencia de Galois y demostrando que el cuerpo fijo de H es exactamente $L \cap E$.

Denotemos el cuerpo fijo de H (dentro de L) como $H^\circ = \{\alpha \in L \mid \tau(\alpha) = \alpha, \forall \tau \in H\}$.

- *Inclusión trivial ($L \cap E \subseteq H^\circ$):* Como H es un subgrupo de $\mathrm{Gal}(L/L \cap E)$, todos los automorfismos de H fijan por definición a $L \cap E$. Por tanto, $L \cap E$ está contenido en el cuerpo fijo de H.

- *Inclusión profunda ($H^\circ \subseteq L \cap E$):* Sea α un elemento cualquiera del cuerpo fijo, $\alpha \in H^\circ$. Para cualquier automorfismo $\sigma \in \mathrm{Gal}(LE/E)$, su imagen $f(\sigma)$ pertenece a H. Por estar α en el cuerpo fijo de H, sabemos que:

  $$f(\sigma)(\alpha) = \alpha$$

  Pero por la propia definición de la restricción, $f(\sigma)(\alpha)$ es simplemente $\sigma(\alpha)$. Por tanto:

  $$\sigma(\alpha) = \alpha \quad \forall \sigma \in \mathrm{Gal}(LE/E)$$

  Esta última afirmación significa que α es un elemento de LE que queda invariante bajo **todo** automorfismo de $\mathrm{Gal}(LE/E)$. Como sabemos que la extensión LE/E es de Galois, el único cuerpo fijo de su grupo de Galois es el cuerpo base E. Es decir, $\mathrm{Gal}(LE/E)^\circ = E$. Concluimos que $\alpha \in E$.

  Pero, al principio, habíamos tomado $\alpha \in H^\circ \subseteq L$, lo que significa que α también pertenece a L. Si $\alpha \in E$ y $\alpha \in L$, entonces irremediablemente $\alpha \in L \cap E$. Como esto se cumple para todo $\alpha \in H^\circ$, deducimos que $H^\circ \subseteq L \cap E$.

Por la doble inclusión, hemos demostrado que el cuerpo fijo del subgrupo imagen es exactamente la intersección: $H^\circ = L \cap E$.

Finalmente, invocamos el Teorema Fundamental de la Teoría de Galois sobre la extensión $L/(L \cap E)$. Como todo subgrupo es cerrado, podemos recuperar el subgrupo original aplicando la clausura:

$$H = H^{\circ\circ} = (L \cap E)^\circ = \mathrm{Gal}(L/L \cap E)$$

Esto demuestra de forma concluyente que la imagen H cubre todo el grupo codominio, haciendo que la aplicación f sea suprayectiva y, en definitiva, un isomorfismo. □

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.

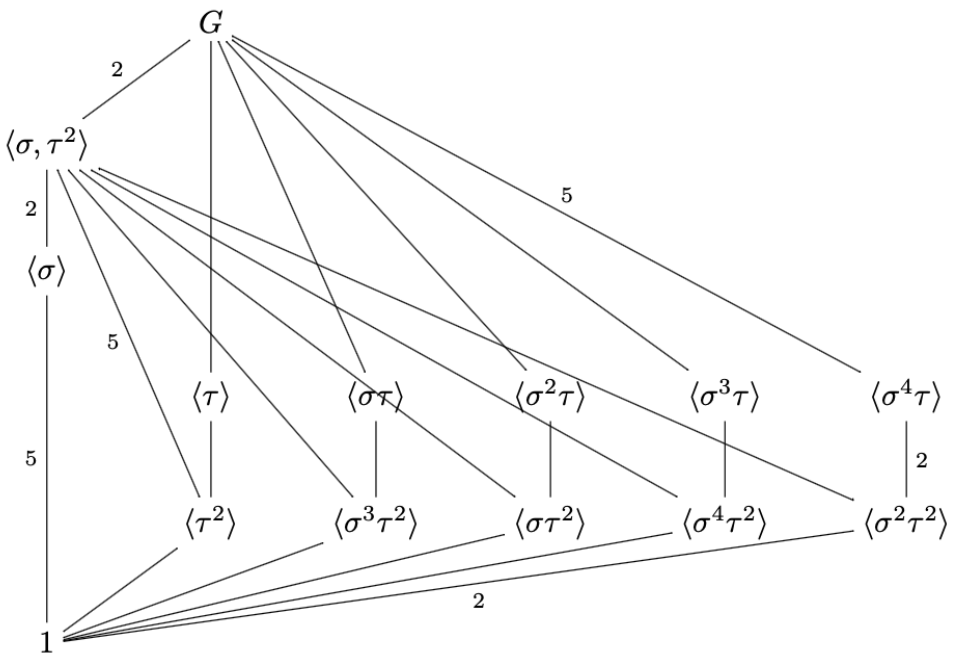
En los demás casos g y h tienen orden 2 ó 4 y vamos a ver que siempre $\langle g, h\rangle = G$. Si $|g| = |h| = 4$ entonces podemos suponer que $g = \sigma^i\tau$ y $h = \sigma^j\tau$ con $i \neq j$. Por tanto, $\langle g, h\rangle$ contiene a $gh^{-1} = \sigma^{i-j}$. Como este elemento genera a $\langle\sigma\rangle$, 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

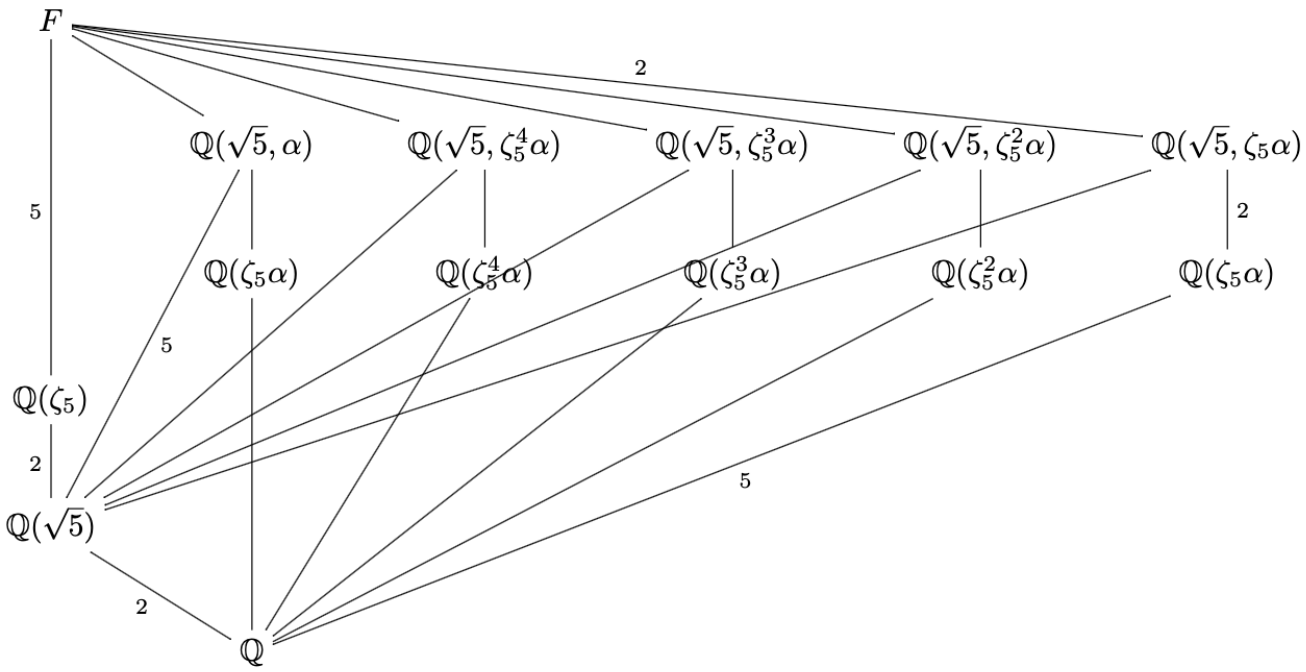


que $\mathbb{Q}(\beta)$ está contenido en $\mathbb{Q}(\zeta_5)$. Además, como $1+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_5^4=0$ tenemos que $\beta^2=\zeta_5^2+\zeta_5^{-2}+2=-\beta+1$, con lo que β es raíz de X^2+X-1, de donde $\beta=\frac{-1+\sqrt{5}}{2}$ y por tanto $\mathbb{Q}(\beta)=\mathbb{Q}(\sqrt{5})$.

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.


F
2
$\mathbb{Q}(\sqrt{5},\alpha)$
$\mathbb{Q}(\sqrt{5},\zeta_5^4\alpha)$
$\mathbb{Q}(\sqrt{5},\zeta_5^3\alpha)$
$\mathbb{Q}(\sqrt{5},\zeta_5^2\alpha)$
$\mathbb{Q}(\sqrt{5},\zeta_5\alpha)$
5
2
$\mathbb{Q}(\zeta_5\alpha)$
$\mathbb{Q}(\zeta_5^4\alpha)$
$\mathbb{Q}(\zeta_5^3\alpha)$
$\mathbb{Q}(\zeta_5^2\alpha)$
$\mathbb{Q}(\zeta_5\alpha)$
5
$\mathbb{Q}(\zeta_5)$
2
5
$\mathbb{Q}(\sqrt{5})$
2
$\mathbb{Q}$