Ecuaciones Algebraicas

Bibliografía:

- Alberto del Valle Robles. *Apuntes de Clase, Tercer Curso del Grado en Matemáticas (Cuarto Curso del Programa Conjunto Matemáticas+Informática): Ecuaciones Algebraicas* (2021). Departamento de Matemáticas, Universidad de Murcia.

Se indican con este formato los resultados que proceden de los ejercicios.

Capítulo 1

Polinomios

Trabajaremos solo con anillos conmutativos.

1.1. Propiedad universal

GyA

Primer teorema de isomorfía: Dado un homomorfismo de anillos [...] $f : A \to B$, existe un único isomorfismo [...] $\tilde{f} : A/\ker f \to \mathrm{Im} f$ tal que $i \circ \tilde{f} \circ p = f$, donde $i : \mathrm{Im} f \to B$ es la inclusión y $p : A \to A/\ker f$ es la proyección. En particular,

$$A/\ker f \cong \mathrm{Im} f.$$

[...] **Propiedad universal del anillo de polinomios (PUAP):** Sean A un anillo y $u : A \to A[X]$ el homomorfismo inclusión [...] para cada homomorfismo de anillos [...] $f : A \to B$ y $b \in B$, el único homomorfismo $\tilde{f} : A[X] \to B$ tal que $\tilde{f}(X) = b$ y $\tilde{f} \circ u = f$ es

$$\tilde{f}\left(\sum_n p_n X^n\right) := \sum_n f(p_n) b^n.$$

[...]

1. Si A es un subanillo de B y $b \in B$, el **homomorfismo** [...] **de evaluación** en b es $S_b : A[X] \to B$ dado por

$$S_b(p) := p(b) := \sum_n p_n b^n,$$

y su imagen es el subanillo generado por $A \cup \{b\}$, llamado $A[b]$.

Por ejemplo, $\mathbb{C} = \mathbb{R}[i]$. Entonces b es **trascendente** sobre A si $\ker(S_b) = 0$, es decir, si b solo es raíz del polinomio nulo, y en otro caso b es **algebraico** y llamamos **ideal de las relaciones algebraicas** de b sobre A a $\ker(S_b) \neq 0$.

Así:

1. $A[b] \cong A[X]/\ker(S_b)$.
2. Si b es trascendente, $S_b : A[X] \to A[b]$ es un isomorfismo.
3. Todo $a \in A$ es algebraico sobre A.
4. π y e son trascendentes sobre $\mathbb{Q}$.
5. $\mathbb{R}[i] = \mathbb{C}$.

GyA

Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo $\hat{f} : A[X] \to B[X]$ dado por

$$\hat{f}(p) = \sum_n f(p_n)X^n$$

1.2. Raíces

GyA

Todo DIP [(dominio de ideales principales)] es un DFU. [...] Dado un dominio $D \neq 0$, una función $\delta : D \setminus \{0\} \to \mathbb{N}$ es **euclídea** si cumple:

1. $\forall a, b \in D \setminus \{0\}, (a \mid b \implies \delta(a) \leq \delta(b))$.
2. $\forall a \in D, b \in D \setminus \{0\}, \exists q, r \in D : (a = bq + r \wedge (r = 0 \vee \delta(r) < \delta(b)))$.

Un **dominio euclídeo** es uno que admite una función euclídea. [...] Todo dominio euclídeo es DIP.

[...] Sean $f, g \in A[X]$, si el coeficiente principal de g es invertible en A, existen dos únicos polinomios $q, r \in A[X]$, llamados respectivamente **cociente** y **resto** de la **división** de f entre g, tales que $f = gq + r$ y $\text{gr}(r) < \text{gr}(g)$, y [$f$ y g son el **dividendo** y el **divisor**][...]. En particular, el grado es una función euclídea.

Teorema del resto: Dados $f \in A[X]$ y $a \in A$, el resto de f entre $X - a$ es $f(a)$.

[...] **Teorema de Ruffini**, [...] f es divisible por $X - a$ si y solo si $f(a) = 0$ [...].

Para $f \in A[X] \setminus \{0\}$ y $a \in A$, existe $m \coloneqq \text{máx}\{k \in \mathbb{N} \mid (X - a)^k \mid f\}$. Llamamos a m **multiplicidad** de a en f, y a es raíz de f si y solo si $m \geq 1$. [...] a es una **raíz simple** de f si $m = 1$ y [...] es una **raíz** [...][**múltiple**] si $m > 1$.

La multiplicidad de a en f es el único natural m tal que $f = (X - a)^m g$ para algún $g \in A[X]$ del que a no es raíz.

Si D es un dominio, $f \in D[X] \setminus \{0\}$, [...] la suma de las multiplicidades de las raíces de f, y el número de raíces, no son superiores a $\text{gr}(f)$.

En particular, si $g \in D[X]$ tiene infinitas raíces en D entonces $g = 0$. Esto no tiene por qué cumplirse si D no en un dominio.

GyA

Dado un anillo [...] A, definimos la **derivada** de $P \coloneqq \sum_k a_k X^k \in A[X]$ como $P' \coloneqq [...] \coloneqq \sum_{k\geq 1} k a_k X^{k-1}$, y escribimos $P^{(0)} \coloneqq P$ y $P^{(n+1)} \coloneqq P^{(n)\prime}$.

GyA

Dados $a, b \in A$ y $P, Q \in A[X]$:

1. $(aP + bQ)' = aP' + bQ'$.
2. $(PQ)' = P'Q + PQ'$.
3. $(P^n)' = nP^{n-1}P'$.

Dados un dominio D de característica 0, $P \in D[X] \setminus \{0\}$ y $a \in D$, la multiplicidad de a en P es el menor $m \in \mathbb{N}_0$ con $P^{(m)}(a) \neq 0$.

Si A es un anillo, $a \in A$ es raíz múltiple de $p \in A[X]$ si y solo si $p(a) = p'(a) = 0$.

GyA

Si [...] $a = \text{mcd}S$ [...] llamamos **identidad de Bézout** a una expresión de la forma $a = a_1 s_1 + \cdots + a_n s_n$ con $a_1, \ldots, a_n \in A$ y $s_1, \ldots, s_n \in S$, que existe [...].
[...] Si $1 \in (S)$, $\text{mcd}S = 1$.
[...] $A[X]$ es un dominio euclídeo si y solo si es un DIP, si y solo si A es un cuerpo.

Llamamos car$A$ a la característica del anillo A. Sean $K \subseteq L$ cuerpos y $f \in K[X]$:

1. Si $\text{mcd}\{f, f'\} = 1$, entonces f no tiene raíces múltiples en K.
2. Si f es irreducible en $K[X]$ con una raíz en L, entonces f tiene raíces múltiples en L si y solo si $f' = 0$.
3. Si car$K = 0$ y f es irreducible en $K[X]$, entonces f no tiene raíces múltiples en L.
4. Si $p \coloneqq \text{car}K \neq 0$, $f' = 0$ si y solo si $f \in K[X^p]$. En particular, si f es irreducible en $K[X]$ con alguna raíz en L, f tiene raíces múltiples en L si y solo si $f \in K[X^p]$.

1.3. Divisibilidad

Si $p \in A[X]$ está formado por subsecuencias proporcionales, es decir, si viene dado por

$$(0, \ldots, 0, \alpha_1 a_0, \ldots, \alpha_1 a_k, 0, \ldots, 0, \alpha_2 a_0, \ldots, \alpha_2 a_k, 0, \ldots, 0, \alpha_t a_0, \ldots, \alpha_t a_k, 0, \ldots),$$

donde $\alpha_1, \ldots, \alpha_t, a_0, \ldots a_k \in A$ con $a_0, a_k \neq 0$, sea n_i la posición de $\alpha_i a_0$ para cada i, entonces $p = (a_0 + a_1 X + \cdots + a_k X^k)(\alpha_1 X^{n_1} + \cdots + \alpha_t X^{n_t})$.

GyA

Sean D un dominio y $p \in D$ [...] p es irreducible en D si y solo si lo es en $D[X]$.

[...] Como **teorema**, D es un DFU si y solo si lo es $D[X]$.

[...] Si D es un DFU [...][para $p \in D[X]$], $c(p) \coloneqq \{x \mid x = \mathrm{mcd}_{k\geq 0} p_k\}$, y [...] si $c(p) = aD^*$, a es el **contenido** de p ($a = c(p)$). [...] p es **primitivo** si $c(p) = 1$, esto es, si [...]$\mathrm{mcd}_k p_k = 1$. [...] Dado $f \in D[X] \setminus D$ primitivo, f es irreducible en $D[X]$ si y sólo si lo es en $K[X]$[,siendo K el cuerpo de fracciones de D][...].

[...] Sean K un cuerpo y $f \in K[X]$:

1. Si $\mathrm{gr}(f) = 1$, f es irreducible en $K[X]$. [...]

3. Si $\mathrm{gr}(f) \in \{2, 3\}$, f es irreducible en $K[X]$ si y solo si no tiene raíces en K.

Si D es un DFU con cuerpo de fracciones K, $f \coloneqq \sum_k a_k X^k \in D[X]$ y $n \coloneqq \mathrm{gr}(f)$, todas las raíces de f en K son de la forma $\frac{r}{s}$ con $r \mid a_0$ y $s \mid a_n$.

Criterio de reducción: [...] Si $p \in \mathbb{Z}$ es primo, $f \coloneqq \sum_k a_k X^k \in \mathbb{Z}[X]$ es primitivo, $n \coloneqq \mathrm{gr}(f)$, $p \nmid a_n$ y f es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Z}[X]$.

Criterio de Eisenstein: Sean D un DFU, $f \coloneqq \sum_k a_k X^k \in D[X]$ primitivo y $n \coloneqq \mathrm{gr} f$, si existe un irreducible $p \in D$ tal que $\forall k \in \{0, \ldots, n-1\}, p \mid a_k$ y $p^2 \nmid a_0$, entonces f es irreducible en $D[X]$.

La irreducibilidad se conserva por automorfismos de dominios, por lo que si D es un dominio, $a \in D^*$ y $b \in D$, $f \in D[X]$ es irreducible si y solo si lo es $f(aX+b)$. En $\mathbb{Z}[X]$, $f \coloneqq X^6 + X^3 + 1$ es irreducible, pues $f(X+1) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$ y, como este es irreducible por Eisenstein con $p = 3$, f es irreducible.

Si $p \in \mathbb{Z}$ es primo, $f(X) \coloneqq \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$ es irreducible en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$.

Un polinomio $p \in K[X]$ de grado n es **recíproco** si para $i \in \{0, \ldots, n\}$ es $p_i = p_{n-i}$. Si K es un cuerpo y n es par, las raíces no nulas de $p(X)$ son los ceros de $f(x) \coloneqq p(x)/x^{n/2} : K^* \to K$, que será de la forma

$$f(x) = p_0 x^k + \cdots + p_{k-1} x + p_k + p_{k-1} x^{-1} + \cdots + p_0 x^{-k},$$

donde $k \coloneqq n/2$. Haciendo el cambio de variable $y \coloneqq x + x^{-1}$ nos queda una función polinómica de grado k y hemos reducido el grado a la mitad. Para hacer el cambio, calculamos $y^2, y^3, \ldots, y^k$, sustituimos $p_0(x^k + x^{-k})$ por $p_0 y^k$ más un polinomio de grado menor, hacemos lo propio con el grado $k - 1$, etc.

Para $n, m \in \mathbb{Z}^+$, $\mathrm{mcd}\{X^n - 1, X^m - 1\} = X^{\mathrm{mcd}\{n,m\}} - 1$.

1.4. Factorización en $\mathbb{C}[X]$ y $\mathbb{R}[X]$

FVC

Teorema fundamental del álgebra: $\mathbb{C}$ es algebraicamente cerrado, esto es, todo polinomio complejo de grado n es la forma $p(x) = \alpha \prod_{k=1}^{n} (x - a_k)$ con $\alpha, a_1, \ldots, a_n \in \mathbb{C}$.

Si $\alpha \in \mathbb{C}$ es raíz de $f \in \mathbb{R}[X]$, entonces $\overline{\alpha}$ también lo es, y ambas tienen la misma multiplicidad.

Los irreducibles de $\mathbb{R}[X]$ son los de grado 1 y los de grado 2 sin raíces reales. Además, todo polinomio en $\mathbb{R}[X]$ se puede expresar de forma única (salvo orden) como

$$a\prod_{i=1}^{r}(X-c_i)^{k_i}\prod_{i=1}^{s}(X^2-2\mathrm{Re}\alpha_i X+|\alpha_i|^2)^{m_i}$$

con $r, s \in \mathbb{N}$, $a, c_1, \ldots, c_r \in \mathbb{R}$, $\alpha_1, \ldots, \alpha_s \in \mathbb{C} \setminus \mathbb{R}$ y $k_1, \ldots, k_r, m_1, \ldots, m_s \in \mathbb{N}^*$.

Las raíces de $X^n - r \in \mathbb{R}[X]$ en $\mathbb{C}$ son las raíces n-ésimas de r de la forma $\sqrt[n]{r}\omega^k$ con $\omega = e^{2\pi i/n}$.

Dado $f \coloneqq Y^3 + 3pY + 2q \in \mathbb{C}[X]$, si $\omega \coloneqq e^{2\pi i/3}$, existe $k \in \{0, 1, 2\}$ tal que, si

$$r := \sqrt[3]{-q+\sqrt{q^2+p^3}}, \qquad s := \omega^k\sqrt[3]{-q-\sqrt{q^2+p^3}},$$

las raíces de f son $r + s$, $r\omega + s\omega^2$ y $r\omega^2 + s\omega$.

Si $f \coloneqq aX^3 + bX^2 + cX + d \in \mathbb{C}[X]$, podemos obtener las raíces de $f(X)$ obteniendo las de $(\frac{1}{a}f)(X - \frac{b}{3a})$, que será de la forma $X^3 + 3pX + 2q$.

1.5. Polinomios en varias variables

GyA

PUAP en n indeterminadas: Sean A un anillo conmutativo, $n \in \mathbb{N}^*$ y $u : A \to A[X_1, \ldots, X_n]$ la inclusión:

1. Dados un homomorfismo de anillos $f : A \to B$ y $b_1, \ldots, b_n \in B$, existe un único homomorfismo de anillos $\tilde{f} : A[X_1, \ldots, X_n] \to B$ tal que $\tilde{f} \circ u = f$ y $\tilde{f}(X_k) = b_k$ para $k \in \{1, \ldots, n\}$.

$$\left[\tilde{f}\left(\sum_{i\in\mathbb{N}^n} p_i X_1^{i_1}\cdots X_n^{i_n}\right) = \sum_{i\in\mathbb{N}^n} f(p_i)b_1^{i_1}\cdots b_n^{i_n}.\right]$$

[...]Dados dos anillos conmutativos $A \subseteq B$ y $b_1, \ldots, b_n \in B$, el **homomorfismo de** [...][**evaluación**] $S : A[X_1, \ldots, X_n] \to B$ viene dado por

$$p(b_1, \ldots, b_n) \coloneqq S(p) \coloneqq \sum_{i\in\mathbb{N}^n} p_i b_1^{i_1}\cdots b_n^{i_n}$$

[y $S(p)$ es la **evaluación** o **valor** de f en $b \coloneqq (b_1, \ldots, b_n)$]. [La imagen de S] es el subanillo de B generado por $A \cup \{b_1, \ldots, b_n\}$ [o **engendrado por** $b_1, \ldots, b_n$ **sobre** A], $A[b_1, \ldots, b_n]$ [...].

Entonces $b_1, \ldots, b_n \in B$ son **algebraicamente independientes** sobre A si $\ker S = 0$, y son **algebraicamente dependientes** en otro caso, es decir, si b es cero de un polinomio no nulo, en cuyo caso $\ker S$ es el **ideal de las relaciones algebraicas** de $b_1, \ldots, b_n$ sobre A.

$$A[b_1, \ldots, b_n] \cong \frac{A[X_1, \ldots, X_n]}{\ker S},$$

y en particular, si $b_1, \dots, b_n$ son algebraicamente independientes, $A[b_1, \dots, b_n] \cong A[X_1, \dots, X_n]$.

Por ejemplo, $b_1 := 1/\pi$ y $b_2 := 1 + \sqrt{\pi}$ son algebraicamente dependientes

Si B es un dominio, llamamos $A(b_1, \dots, b_n)$ al cuerpo de fracciones de $A[b_1, \dots, b_n]$, que en general no está contenido en B, pero sí en su cuerpo de fracciones K, y de hecho es el menor subcuerpo de K que contiene a $A \cup \{b_1, \dots, b_n\}$.

GyA

2. Sean A un anillo y σ una permutación de $\mathbb{N}_n$ con inversa $\tau := \sigma^{-1}$, tomando $B = A[X_1, \dots, X_n]$ y $b_k = X_{\sigma(k)}$ en el punto anterior obtenemos un automorfismo $\hat{\sigma}$ en $A[X_1, \dots, X_n]$ con inversa $\hat{\tau}$ que permuta las indeterminadas. [Llamamos $f^\sigma := \hat{\sigma}(f)$.]

3. $$A[X_1, \dots, X_n, Y_1, \dots, Y_m] \cong A[X_1, \dots, X_n][Y_1, \dots, Y_m] \cong A[Y_1, \dots, Y_m][X_1, \dots, X_n],$$

   por lo que en la práctica no distinguimos entre estos anillos.

4. Todo homomorfismo de anillos [...] $f : A \to B$ induce un homomorfismo $\hat{f} : A[X_1, \dots, X_n] \to B[X_1, \dots, X_n]$ dado por $\hat{f}(p) := \sum_{i \in \mathbb{N}^n} f(p_i) X_1^{i_1} \cdots X_n^{i_n}$.

Llamamos **grado** de un monomio $aX_1^{i_1} \cdots X_n^{i_n}$ a $i_1 + \cdots + i_n$, y grado de $p \in A[X_1, \dots, X_n] \setminus 0$, $\operatorname{gr}(p)$, al mayor de los grados de los monomios no nulos en la expresión por monomios de p. Entonces $\operatorname{gr}(p+q) \leq \max\{\operatorname{gr}(p), \operatorname{gr}(q)\}$ y $\operatorname{gr}(pq) \leq \operatorname{gr}(p) + \operatorname{gr}(q)$.

Un polinomio es **homogéneo** de grado n si es suma de monomios de grado n. Todo polinomio se escribe de modo único como suma de polinomios homogéneos de distintos grados, [las **componentes homogéneas** del polinomio.]

1.6. Polinomios simétricos

Un $f \in A[X_1, \dots, X_n]$ es **simétrico** si $f^\sigma = f$ para todo $\sigma \in \mathcal{S}_n$, si y solo si todas sus componentes homogéneas son simétricas.

Sea $F \in A[X_1, \dots, X_n][T]$ dado por

$$F := (T - X_1) \cdots (T - X_n) =: \sum_{k=0}^{n} (-1)^k s_k(X_1, \dots, X_n) T^{n-k},$$

llamamos **polinomios simétricos elementales** en las indeterminadas $X_1, \dots, X_n$ a los $s_k \in A[X_1, \dots, X_n]$, dados por

$$s_k(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \dots < i_k \leq n} \prod_{j=1}^{k} X_{i_j}$$

que son simétricos. En particular $s_0 = 1$, $s_1 = X_1 + \cdots + X_n$ y $s_n = X_1 \cdots X_n$. Si $\tilde{s}_1, \dots, \tilde{s}_{n-1}$ son los polinomios simétricos elementales en las variables $X_1, \dots, X_{n-1}$, entonces, para $i \in \{1, \dots, n-1\}$,

$$\tilde{s}_i(X_1, \dots, X_{n-1}) = s_i(X_1, \dots, X_{n-1}, 0).$$

Sean A un subanillo de B, $f \in A[X]$ y $\alpha_1, \ldots, \alpha_n \in B[X]$ con $f = (X - \alpha_1) \cdots (X - \alpha_n)$, entonces, para $k \in \{1, \ldots, n\}$, $s_k = (-1)^k f_k$.

Teorema fundamental de los polinomios simétricos: Sea $S[X_1, \ldots, X_n]$ el subanillo de los polinomios simétricos de $A[X_1, \ldots, X_n]$, el homomorfismo de evaluación $\varphi : A[X_1, \ldots, X_n] \to S[X_1, \ldots, X_n]$ con $\varphi(X_i) = s_i$ es un isomorfismo, es decir, todo polinomio simétrico se escribe de forma única como expresión polinómica en los polinomios simétricos elementales.

El **orden lexicográfico** en $\mathbb{N}^n$ es el buen orden dado por $(i_1, \ldots, i_n) < (j_1, \ldots, j_n)$ si y solo si existe k con $i_k \neq j_k$ y, para el menor de esos k, $i_k < j_k$. Sea

$$f = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \cdots X_n^{i_n},$$

llamamos **término superior** de f al término $a_i X_1^{i_1} \cdots X_n^{i_n}$ con $a_i \neq 0$ y máximo i en orden lexicográfico. Para cada k, el término superior de s_k es $X_1 X_2 \cdots X_k$.

Si D es un dominio y $f_1, \ldots, f_r \in D[X_1, \ldots, X_n]$, el término superior de $f_1 \cdots f_r$ es el producto de los términos superiores de los factores.

Si f es simétrico con término superior $aX_1^{i_1} \cdots X_n^{i_n}$, entonces $i_1 \geq i_2 \geq \cdots \geq i_n$.

Entrada: Dominio $(D, +, \cdot)$ y polinomio $f \in D[X_1, \ldots, X_n]$ simétrico.
Salida: Polinomio $g \in D[X_1, \ldots, X_n]$ con $g(s_1, \ldots, s_n) = f$.
$g \leftarrow 0$;
mientras $f \neq 0$ **hacer**
  Obtener el término superior $M = aX_1^{i_1} \cdots X_n^{i_n}$ de f;
  $p \leftarrow aX_1^{i_1 - i_2} X_2^{i_2 - i_3} \cdots X_{n-1}^{i_{n-1} - i_n} X_n^{i_n}$;
  $f \leftarrow f - p(s_1, \ldots, s_n)$;
  $g \leftarrow g + p$;
fin

Algoritmo 1: Descomposición de un polinomio simétrico en un dominio como expresión polinómica de polinomios simétricos elementales.

El algoritmo 1 permite descomponer un polinomio simétrico en un dominio como expresión polinómica de polinomios simétricos elementales.

Si $f \in D[X_1, \ldots, X_n]$ es un polinomio homogéneo con término superior $aX_1^{i_1} \cdots X_n^{i_n}$, la expresión será una D-combinación lineal de polinomios del tipo $s_1^{j_1 - j_2} s_2^{j_2 - j_3} \cdots$ con $j_1 + \cdots + j_n = i_1 + \cdots + i_n$ y $(j_1, \ldots, j_n) \leq (i_1, \ldots, i_n)$, donde el coeficiente correspondiente a $(i_1, \ldots, i_n)$ será a y, para casos sencillos, podemos determinar el resto dando valores «fáciles» a las indeterminadas y resolviendo las ecuaciones lineales en los coeficientes obtenidas.

Si D es un dominio, $f/g \in D(X_1, \ldots, X_n)$ es una **función racional simétrica** si $f^\sigma/g^\sigma = f/g$ para todo $\sigma \in \mathcal{S}_n$. Esto está bien definido, pues $f/g = p/q \implies fq = gp \implies f^\sigma q^\sigma = g^\sigma p^\sigma \implies f^\sigma/g^\sigma = p^\sigma/q^\sigma$. Si $f, g \in D[X_1, \ldots, X_n]$ son simétricos con $g \neq 0$ entonces f/g es simétrica, pero el recíproco no se cumple, pues $X^2Y/(X^2 + XY)$ es una función racional simétrica pero el numerador y el denominador no lo son. El conjunto de funciones racionales simétricas en $D(X_1, \ldots, X_n)$ es precisamente $D(s_1, \ldots, s_n)$.

Capítulo 2

Extensiones de cuerpos

Si K es un cuerpo y $A \neq 0$ es un anillo, todo homomorfismo de anillos $h : K \to A$ es un isomorfismo $K \to h(K)$. En efecto, $\ker h \subseteq K$ es un ideal y los únicos ideales de K son 0 y K, pero como $A \neq 0$, $1 \notin \ker h$, luego $\ker h = 0$, h es inyectivo y $h : K \to h(K)$ es biyectivo.

Una **extensión** (**de cuerpos**) es un par de cuerpos (K, L) con K subcuerpo de L, que representamos como $K \subseteq L$, L/K o, si $K \neq L$, como $K \subsetneq L$.

Algunas extensiones son $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{R} \subseteq \mathbb{C}$ y, para todo cuerpo K, $K \subseteq K(X)$, donde $K(X)$ es el cuerpo de fracciones de $K[X]$. Otras son $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{m}]$ para $m \in \mathbb{Z}$ no cuadrado de entero, incluyendo $\mathbb{Q}[i]$.

Dados $c, d \in \mathbb{Z}$ no cuadrados, $\mathbb{Q}(\sqrt{c}) = \mathbb{Q}(\sqrt{d})$ si y sólo si cd es un cuadrado en $\mathbb{Z}$.

GyA

Llamamos **subanillo primo** de A a $\mathbb{Z}1 \coloneqq \{n1_A\}_{n\in\mathbb{Z}}$, el menor subanillo de A.

[...] Sea K un cuerpo no trivial, existe un subcuerpo K' de K llamado **subcuerpo primo** de K contenido en cualquier subcuerpo de K, y este es isomorfo a $\mathbb{Z}_p$ si la característica de K es un entero primo p o a $\mathbb{Q}$ en caso contrario. **Demostración:** Si la característica es un primo p, el subanillo primo de K, isomorfo a $\mathbb{Z}_p$, es un cuerpo y contiene a cualquier subanillo de K [...]. En otro caso [...] la característica es 0, por lo que $f : \mathbb{Z} \to K$ dado por $f(n) \coloneqq n1$ es un homomorfismo inyectivo y la propiedad universal [de los cuerpos de fracciones] nos da un homomorfismo $\tilde{f} : Q(\mathbb{Z}) = \mathbb{Q} \to K$ dado por $f(\frac{n}{m}) = f(n)f(m)^{-1}$. Es claro entonces que $K' \coloneqq \tilde{f}(\mathbb{Q})$ es isomorfo a $\mathbb{Q}$, y queda ver que está contenido en cualquier subcuerpo de K. Dado un tal F, para $m \in \mathbb{Z}$, $f(m) = m1 \in F$, y para $n \in \mathbb{Z} \setminus \{0\}$, $f(n) \neq 0$ y $f(n)^{-1} \in F$, luego $\tilde{f}(\frac{m}{n}) = f(m)f(n)^{-1} \in F$, y en resumen $\tilde{f}(\mathbb{Q}) \subseteq F$.

2.1. Grado de una extensión

Si $K \subseteq L$ es una extensión de cuerpos, L es un K-espacio vectorial con la suma y el producto por escalares dados por la suma y el producto en L, y K es un subespacio de L. Llamamos

grado de $K \subseteq L$ a $[L : K] \coloneqq \dim_K L$. $K \subseteq L$ es **finita** o **infinita** según lo sea $[L : K]$. Entonces:

1. $[L : K] = 1 \iff L = K$.

   $\Longrightarrow$] Si hubiera $\alpha \in L \setminus K$, como $\alpha \notin K = \text{span}\{1\}$, α y 1 son linealmente independientes y $\text{span}\{1, \alpha\} \subseteq L$, luego $[L : K] \geq 2\#$.

2. $[\mathbb{C} : \mathbb{R}] = 2$.

   Tomando la base $(1, i)$.

3. Para $m \in \mathbb{Z}$ no cuadrado, $[\mathbb{Q}[\sqrt{m}] : \mathbb{Q}] = 2$.

   Tomando la base $(1, \sqrt{m})$.

4. $\mathbb{Q} \subseteq \mathbb{R}$ es infinita.

   Si fuera $[\mathbb{R} : \mathbb{Q}] =: n < +\infty$, habría un isomorfismo de espacios vectoriales $\mathbb{R} \cong \mathbb{Q}^n$ y $\mathbb{R}$ sería numerable.$\#$

5. $K \subseteq K(X)$ es infinita.

   $\{X^n\}_{n\in\mathbb{N}}$ es infinito y linealmente independiente sobre K.

Dadas dos extensiones $K \subseteq L$ y $L \subseteq M$, $[M : K] = [M : L][L : K]$, y en particular, si $K \subseteq L$ y $L \subseteq M$ son finitas, $[M : L], [L : K] \mid [M : K]$. **Demostración:** Sean $(u_i)_{i\in I}$ una base de M sobre L y $(v_j)_{j\in J}$ una de L sobre K, todo $\alpha \in M$ se expresa de forma única como $\alpha =: \sum_{i\in I} a_i u_i$ con los $a_i \in L$, y cada a_i se expresa de forma única como $a_i =: \sum_{j\in J} c_{ij} v_j$ con los $c_{ij} \in K$, luego $\alpha = \sum_{(i,j)\in I\times J} c_{ij} u_i v_j$. Pero agrupando, esta descomposición es única, luego $(u_i v_j)_{(i,j)\in I\times J}$ es base de M sobre K y $[M : K] = |I \times J| = |I||J| = [M : L][L : K]$.

Así, si $K \subseteq L$ tiene grado finito y primo, no hay ningún cuerpo intermedio entre ellos.

2.2. Extensiones generadas y admisibles

Dado un conjunto $\mathcal{C}$, la unión $\bigcup \mathcal{C}$ es una **unión dirigida** si para $A, B \in \mathcal{C}$ existe $C \in \mathcal{C}$ con $A, B \subseteq C$.

Dados una extensión de cuerpos $K \subseteq L$ y un $S \subseteq L$, llamamos $K[S]$ al conjunto de expresiones polinómicas de elementos de S con coeficientes en K, es decir, la unión dirigida $\bigcup_{\{\alpha_1,\ldots,\alpha_k\}\subseteq S} K[\alpha_1, \ldots, \alpha_k]$, que es el menor subanillo de L que contiene a $K \cup S$, la intersección de todos ellos. $K[S]$ es un dominio.

Llamamos $K(S)$ al cuerpo de fracciones de $K[S]$, que es la unión dirigida

$$\bigcup_{\{\alpha_1,\ldots,\alpha_k\}\subseteq S} K(\alpha_1, \ldots, \alpha_k)$$

y el menor subcuerpo de L que contiene a $K \cup S$, es decir, la intersección de todos ellos. Claramente $K(S) = K[S]$ si y solo si $K[S]$ es un cuerpo.

Dos extensiones $K \subseteq E_1$ y $K \subseteq E_2$ son **admisibles** si E_1 y E_2 son subcuerpos de un mismo cuerpo L, y entonces $E_1 \cap E_2$ es un cuerpo. Llamamos **compuesto** de E_1 y E_2 a $K(E_1 \cup E_2) = E_1(E_2) = E_2(E_1)$, de modo que tenemos las extensiones

$$K \subseteq E_1 \cap E_2 \subseteq E_1, E_2 \subseteq E_1E_2 \subseteq L.$$

2.3. Grupos de Galois

Dadas las extensiones $K \subseteq L$ y $K \subseteq L'$, un K**-encaje** o K**-homomorfismo** es un homomorfismo de anillos $\sigma : L \to L'$ con $\sigma|_K = 1_K$. Entonces σ es K-lineal e inyectivo. En efecto, sean $r \in K$ y $\alpha, \beta \in L$, $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ y $\sigma(r\alpha) = \sigma(r)\sigma(\alpha) = r\sigma(\alpha)$, y σ es inyectivo como todo homomorfismo que parte de un cuerpo. Si además σ es suprayectivo, es un K**-isomorfismo** y $K \subseteq L$ y $K \subseteq L'$ son extensiones K**-isomorfas**.

> Dado un homomorfismo de cuerpos $f : K \to L$, K y L tienen un mismo subcuerpo primo P ($\mathbb{Q}$ o $\mathbb{Z}_p$) y f es un P-encaje.

Si $K \subseteq L$ y $K \subseteq L'$ son extensiones finitas y $\sigma : L \to L'$ es un K-encaje, entonces

$$[L : K] \mid [L' : K],$$

con igualdad si y solo si σ es un K-isomorfismo. En efecto, $K = \sigma(K) \subseteq \sigma(L) \subseteq L'$ y se tiene $[\sigma(L) : K] \mid [L' : K]$ con igualdad si y solo si $[L' : \sigma(L)] = 1$, si y solo si $L' = \sigma(L)$, y $[L : K] = [\sigma(L) : K]$ porque $\sigma : L \to \sigma(L)$ es un isomorfismo de espacios vectoriales.

Dos extensiones finitas $K \subseteq L$ y $K \subseteq L'$ de igual grado no son necesariamente K-isomorfas. Por ejemplo, $[\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, pero si hubiese un $\mathbb{Q}$-isomorfismo $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$ sería $\sigma(i) \in \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ y $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1\#$.

Los K-encajes llevan raíces de $f \in K[X]$ a raíces de f, pues dados un K-encaje $\sigma : L \to L'$ y una raíz $\alpha \in L$ de f,

$$f(\sigma(\alpha)) = \textstyle\sum_i f_i \sigma(\alpha)^i = \sum_i \sigma(f_i)\sigma(\alpha)^i = \sigma\left(\sum_i f_i \alpha^i\right) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Un K**-automorfismo** de una extensión $K \subseteq L$ es un K-isomorfismo $L \to L$. El conjunto de todos los K-automorfismos en L es un grupo con la composición de aplicaciones y con elemento neutro 1_L, llamado **grupo de Galois** de L sobre K o de la extensión $K \subseteq L$, y denotado $\mathrm{Gal}(L/K)$ o $\mathrm{Aut}_K(L)$.

Ejemplos:

1. $\mathrm{Gal}(K/K) = \{1_L\}$.
2. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1_L, (z \mapsto \overline{z})\} \cong C_2$.

   Sea $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, como $(1, i)$ es base de $\mathbb{C}$ sobre $\mathbb{R}$ y $\sigma(1) = 1$, basta ver cómo actúa $\sigma(i)$, pero $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$ y por tanto $\sigma(i) \in \{\pm i\}$, de modo que o bien $\sigma(i) = i$ y $\sigma = 1_L$ o $\sigma(i) = -i$ y σ es la conjugación. Finalmente, el único grupo de 2 elementos es C_2 y por tanto $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2$.

Extensiones K-isomorfas de K tienen grupos de Galois isomorfos. En efecto, sea $\sigma : L \to L'$ un K-isomorfismo, $\hat{\sigma} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K)$ dada por $\hat{\sigma}(f) \coloneqq \sigma \circ f \circ \sigma^{-1}$ es un isomorfismo de grupos, dado que $\hat{\sigma}(1_L) = \sigma \circ \sigma^{-1} = 1_{L'}$ y $\hat{\sigma}(f)\hat{\sigma}(g) = \sigma \circ f \circ \sigma^{-1} \circ \sigma \circ g \circ \sigma^{-1} = \hat{\sigma}(fg)$.

GyA
Si D es un DIP y $a \in D \setminus (D^* \cup \{0\})$, a es irreducible si y solo si (a) es un ideal maximal, si y solo si $\frac{A}{(a)}$ es un cuerpo, si y solo si $\frac{A}{(a)}$ es un dominio.

2.4. Extensiones algebraicas

Teorema de Kronecker: Sean K un cuerpo y $f \in K[X] \setminus K$, existe una extensión L de K en la que f tiene una raíz. Si g es un factor irreducible de f, la extensión podría ser $K[X]/(g)$ y una raíz es $X + (g)$.[1] **Demostración:** Como $K[X]$ es un DFU y $f \notin K$, f tiene un factor irreducible g y las raíces de g lo serán de f. Al ser g irreducible en el DIP $K[X]$, $L \coloneqq K[X]/(g)$ es un cuerpo. Como la inclusión $i : K \to K[X]$ y la proyección $[\cdot] : K[X] \to L$ son homomorfismos y $[\cdot] \circ i$ es inyectivo por ser K un cuerpo, podemos identificar $a \in K$ con $[i(a)] \in L$, de modo que $K \subseteq L$ y, usando la evaluación $S_\alpha : K[X] \to L$ y que $[\cdot]$ es un homomorfismo,

$$S_\alpha(g) = g(\alpha) = g([X]) = \sum_i g_i [X]^i = \left[\sum_i g_i X^i\right] = [g] = [0].$$

Por inducción, dados un cuerpo K y $f \in K[X] \setminus K$, existe una extensión L de K en la que f tiene todas sus raíces.

Sean $K \subseteq L$ una extensión y $\alpha \in L$:

1. Si α es algebraico sobre K, también lo es sobre cualquier cuerpo entre K y L.

   Un $f \in K[X] \setminus 0$ con $f(\alpha) = 0$ también está en el cuerpo intermedio.

2. α es trascendente sobre K si y solo si $\{\alpha^n\}_{n\in\mathbb{N}}$ es linealmente independiente sobre K.

3. Para $m \in \mathbb{Q}^{\geq 0}$, $\pm\sqrt{m} \in \mathbb{R}$ son algebraicos sobre $\mathbb{Q}$.

4. Si $n \in \mathbb{N}^*$ y $\omega \coloneqq e^{2\pi i/n} \in \mathbb{C}$, $\omega, \omega^2, \ldots, \omega^n$ son algebraicos sobre $\mathbb{Q}$.

   Son raíces de $X^n - 1 \in \mathbb{Q}[X]$.

Una extensión $K \subseteq L$ es **algebraica** si todo elemento de L es algebraico sobre K, y es **trascendente** en otro caso.

1. Toda extensión finita es algebraica. En particular $\mathbb{R} \subseteq \mathbb{C}$ es algebraica.

   Sea $K \subseteq L$ finita, si hubiera un $\alpha \in L$ trascendente, $\{\alpha^n\}_{n\in\mathbb{N}}$ sería linealmente independiente y la extensión sería infinita.#

2. $K \subseteq K(X)$ es trascendente.

   $\{X^n\}_{n\in\mathbb{N}}$ es linealmente independiente sobre K, luego X es trascendente.

3. $\mathbb{Q} \subseteq \mathbb{R}$ es trascendente.

   π es trascendente.

[1] Para esto se usa el transporte de estructuras. Sea $\varphi : K \to (L_0 \coloneqq K[X]/(g))$ el homomorfismo $\varphi(a) \coloneqq a + (g)$, definimos $L \coloneqq K \amalg (L_0 \setminus \varphi(K))$ y las operaciones en L $a + b \coloneqq \psi^{-1}(\psi(a) + \psi(b))$ y $ab \coloneqq (\psi(a)\psi(b))$, donde $\psi : L \to L_0$ viene dado por $\psi(a) \coloneqq \varphi(a)$ para $a \in K$ y $\psi(a) \coloneqq a$ para $a \in L_0 \setminus \varphi(K)$. Esto nos da una «copia» de L_0 que es una extensión de K.

$K \subseteq L$ es algebraica si y sólo si todo subanillo A intermedio entre K y L es un cuerpo, si y sólo si para todo cuerpo intermedio E, todo K-endomorfismo en E es un automorfismo.

2.5. Extensiones simples

Una extensión $K \subseteq L$ es **simple** si existe $\alpha \in L$ con $L = K(\alpha)$. La extensión dada por el teorema de Kronecker es simple. En efecto, sean $f \in K[X] \setminus K$, $L = K[X]/I$ el cuerpo dado por el teorema de Kronecker para f y $\alpha \coloneqq [X] = X + I \in L$ la raíz, para $[p] \in L$ es $p(\alpha) = p([X]) = \sum_i p_i [X]^i = \left[\sum_i p_i X^i\right] = [p]$, luego $L = K[\alpha]$ y, como L es un cuerpo, $K[\alpha] = K(\alpha)$.

Dados una extensión $K \subseteq L$ y un $\alpha \in L$ trascendente, entonces $K(\alpha) \cong K(X)$, y en particular $K \subseteq K(\alpha)$ es infinita, pues como $K[X] \cong K[\alpha]$, sus cuerpos de fracciones también son isomorfos.

Sean $K \subseteq L$ una extensión y $\alpha \in L$ algebraico:

1. α es raíz de un único polinomio mónico e irreducible en $f \in K[X]$, el **polinomio irreducible de α sobre K**, $\mathrm{Irr}(\alpha, K)$.

   $S_\alpha : K[X] \to K[\alpha]$ tiene núcleo no nulo, y como $K[X]$ es un DIP, existe $f \in K[X] \setminus 0$ con $\ker(S_\alpha) = (f)$, que podemos tomar mónico. Como $K[X]/(f) \cong K[\alpha]$ es un dominio siendo $K[X]$ un DIP, f es irreducible. Si $g \in K[X]$ es un irreducible mónico con raíz α, como $g \in \ker(S_\alpha) = (f)$, $f \mid g$. Como ambos son irreducibles, son asociados, pero al ser ambos mónicos deben ser iguales.

2. $K[\alpha]$ es un cuerpo.

   Como $K[X]$ es DIP, $K[X]/(f)$ es un cuerpo si es un dominio, y lo es.

3. $\forall g \in K[X], (g(\alpha) = 0 \iff f \mid g)$.

   $g(\alpha) = 0 \iff g \in \ker(S_\alpha) = (f) \iff f \mid g$.

4. Sea $n \coloneqq \mathrm{gr} f$, $[K(\alpha) : K] = n$ y $(\alpha^i)_{i=0}^{n-1}$ es base de $K(\alpha)$ sobre K.

   Si $(\alpha^i)_{i=0}^{n-1}$ no fuera linealmente independiente, existiría $(a_0, \ldots, a_{n-1}) \neq 0$ con

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

   pero entonces $g \coloneqq \sum_{i=0}^{n-1} a_i X^i \in K[X] \setminus 0$ tendría a α como raíz y por tanto $f \mid g$, lo que contradice que $\mathrm{gr} g < \mathrm{gr} f \#$. Para ver que $(\alpha^i)_{i=0}^{n-1}$ es un conjunto generador, los elementos de $K[\alpha]$ son de la forma $h(\alpha)$ para $h \in K[X]$, y dividiendo h entre f con resto tenemos $h = fq + r$ para ciertos $q, r \in K[X]$ con $\mathrm{gr} r < \mathrm{gr} f = n$, luego $h(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = \sum_{i=0}^{n-1} r_i \alpha^i$.

Ejemplos:

1. Para $z \in \mathbb{C}$,

   $$\mathrm{Irr}(z, \mathbb{R}) = \begin{cases} X - z, & z \in \mathbb{R}; \\ X^2 - 2\mathrm{Re} z X + |z|^2, & z \notin \mathbb{R}. \end{cases}$$

2. Si $m \in \mathbb{Q}$ no es un cuadrado de racional, $\mathrm{Irr}(\sqrt{m}, \mathbb{Q}) = X^2 - m$.

3. Si $f \in K[X]$ es irreducible de grado al menos 2, f no tiene raíces en ninguna extensión finita L de K con $[L:K]$ coprimo con $\mathrm{gr}f$.

4. Sean $X^n - a \in K[X]$ irreducible, β una raíz de $X^n - a$ en una extensión de K y $m \mid n$, $[K(\beta^m):K] = n/m$.

Sea $K \subseteq L$ una extensión, un $\alpha \in L$ es algebraico sobre K si y solo si $K \subseteq K(\alpha)$ es finita, si y solo si $K[\alpha]$ es un cuerpo.

Sean $p, q \in \mathbb{N}$ primos, $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p}]$ y $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{q}]$ son admisibles y

$$\mathbb{Q}[\sqrt{p}]\mathbb{Q}[\sqrt{q}] = \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}\}_{a,b,c,d\in\mathbb{Q}} = \mathbb{Q}(\sqrt{p} + \sqrt{q}).$$

Demostración: Para $p = q$ esto es obvio, por lo que supondremos $p \neq q$. Sean $F_p \coloneqq \mathbb{Q}[\sqrt{p}]$ y $F_q \coloneqq \mathbb{Q}[\sqrt{q}]$, F_p y F_q son admisibles por ser ambos subcuerpos de $\mathbb{R}$. Claramente $S \coloneqq \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}\}_{a,b,c,d\in\mathbb{Q}} \subseteq F_pF_q$. Sea ahora $\alpha \coloneqq \sqrt{p} + \sqrt{q} \in S$,

$$\alpha^2 = p + q + 2\sqrt{pq} \implies \alpha^2 - (p+q) = 2\sqrt{pq} \implies$$
$$\implies \alpha^4 - 2(p+q)\alpha^2 + 2(p+q)^2 = 4pq \implies \alpha^4 - 2(p+q)\alpha^2 + 2(p-q)^2 = 0,$$

luego α es raíz del polinomio $X^4 - 2(p+q)X^2 + 2(p-q)^2 \in \mathbb{Q}[X]$ y por tanto es algebraico, con lo que $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. S es un anillo, pues es cerrado para restas y productos y contiene al 1, y como además $\mathbb{Q} \cup \{\alpha\} \subseteq S$, $\mathbb{Q}[\alpha] \subseteq S$. Finalmente, como

$$\frac{1}{\alpha} = \frac{1}{\sqrt{p} + \sqrt{q}} \frac{\sqrt{p} - \sqrt{q}}{\sqrt{p} - \sqrt{q}} = \frac{\sqrt{p} - \sqrt{q}}{p - q} \in \mathbb{Q}(\alpha),$$

$\sqrt{p} - \sqrt{q} \in \mathbb{Q}(\alpha)$ y por tanto $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(\alpha)$, con lo que $F_p, F_q \subseteq \mathbb{Q}(\alpha)$ y $F_pF_q \subseteq \mathbb{Q}(\alpha)$. Con esto $S \subseteq F_pF_q \subseteq \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha] \subseteq S$, lo que prueba la igualdad.

Sean K un cuerpo y $f \in K[X] \setminus 0$ con raíz α en alguna extensión de K, $[K(\alpha):K] \leq \mathrm{gr}f$, con igualdad si y solo si f es irreducible sobre K.

Sean K un cuerpo, $f \in K[X]$ irreducible en $K[X]$ con una raíz α, $\sigma : K \to K'$ un isomorfismo de cuerpos y $f' \coloneqq \sigma(f)$ con una raíz α', σ se extiende a un isomorfismo $\hat{\sigma} : K(\alpha) \to K'(\alpha')$ con $\hat{\sigma}(\alpha) = \alpha'$. **Demostración:** Sea r el coeficiente principal de f, entonces $f = r\mathrm{Irr}(\alpha, K)$ y por tanto $f' = \sigma(r)\mathrm{Irr}(\alpha', K')$. Como $K(\alpha) = K[\alpha]$ por ser $K[\alpha]$ un cuerpo, sus elementos son de la forma $g(\alpha)$ con $g \in K[X]$. Sea $\hat{\sigma}(g(\alpha)) \coloneqq \sigma(g)(\alpha')$, $\hat{\sigma}$ está bien definido, pues si $g(\alpha) = h(\alpha)$ entonces $(g-h)(\alpha) = 0$ y por tanto $f \mid r^{-1}f = \mathrm{Irr}(\alpha, k) \mid g - h$, luego $f' = \sigma(f) \mid \sigma(g-h)$ y, como $f'(\alpha') = 0$, $\sigma(g)(\alpha') - \sigma(h)(\alpha') = \sigma(g-h)(\alpha') = 0$. Entonces para $r \in K$ es $\hat{\sigma}(r) = \sigma(r)$ y $\hat{\sigma}(\alpha) = \sigma(X)(\alpha') = \alpha'$, y $\hat{\sigma}$ es un homomorfismo. Es biyectivo porque $\hat{\sigma}^{-1}$ se construye de forma análoga a partir de σ^{-1}.

Sea $K \subseteq L$ una extensión, $\alpha, \beta \in L$ algebraicos sobre K son **K-conjugados** si son raíces de un mismo irreducible sobre K, si y solo si $\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$, si y solo si existe un K-isomorfismo $\sigma : K(\alpha) \to K(\beta)$ con $\sigma(\alpha) = \beta$, si y solo si existe un K-encaje $\sigma : K(\alpha) \to K(\beta)$ con $\sigma(\alpha) = \beta$, y entonces $\mathrm{Gal}(K(\alpha)/K) \cong \mathrm{Gal}(K(\beta)/K)$ como grupos.

$1 \implies 2]$ Sea f dicho irreducible con coeficiente principal r, $r^{-1}f = \mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$.

$2 \implies 1]$ Obvio.

$1 \implies 3]$ El automorfismo identidad en K se extiende a un isomorfismo $\sigma : K(\alpha) \to K(\beta)$ con $\sigma(\alpha) = \beta$. Entonces $K(\alpha) \cong K(\beta)$ y $\mathrm{Gal}(K(\alpha)/K) \cong \mathrm{Gal}(K(\beta)/K)$.

$3 \implies 4]$ Obvio.

$4 \implies 2]$ Sea $f \coloneqq \mathrm{Irr}(\alpha, K)$, al ser α raíz de f, también lo es $\sigma(\alpha) = \beta$.

Sean $f \in K[X]$ irreducible de grado n y α una raíz de f, si f tiene m raíces en $K(\alpha)$:

1. $|\mathrm{Gal}(K(\alpha)/K)| = m$.

   Un K-automorfismo σ en $K(\alpha)$ queda determinado por $\sigma(\alpha)$, que sabemos que debe ser raíz de f. Además, si β es otra raíz de f en $K(\alpha)$, existe un K-isomorfismo $\sigma : K(\alpha) \to K(\beta)$ con $\sigma(\alpha) = \beta$, pero el K-isomorfismo implica que $[K(\alpha) : K] = [K(\beta) : K]$ y, como $K(\beta) \subseteq K(\alpha)$, $[K(\alpha) : K(\beta)] = 1$ y $K(\beta) = K(\alpha)$, luego este $\sigma \in \mathrm{Gal}(K(\alpha)/K)$. Por tanto hay biyección entre $\mathrm{Gal}(K(\alpha)/K)$ y las m raíces de f en $K(\alpha)$.

2. Para toda raíz β de f, f tiene m raíces en $K(\beta)$.

   Al ser α y β raíces de un mismo irreducible, $\mathrm{Gal}(K(\alpha)/K) \cong \mathrm{Gal}(K(\beta)/K)$, luego $|\mathrm{Gal}(K(\beta)/K)| = m$ y el resultado se obtiene del punto anterior.

3. Si f no tiene raíces múltiples (por ejemplo, si $\mathrm{car}K = 0$), entonces $m \mid n$.

   Las n raíces se reparten en extensiones $K(\alpha)$ de m elementos, y si una raíz α estuviera en una extensión $K(\beta)$ siendo β otra raíz de f, entonces $K(\beta) \subseteq K(\alpha)$ con $[K(\beta) : K] = [K(\alpha) : K]$, luego $K(\alpha) = K(\beta)$ y ninguna raíz está en dos extensiones distintas.

2.6. Algunos grupos de Galois

$$\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = 1.$$

Demostración: Sea $\sigma : \mathbb{R} \to \mathbb{R}$ un $\mathbb{Q}$-automorfismo, y queremos ver que entonces $\sigma = 1_{\mathbb{R}}$. Para $r, s \in \mathbb{R}$, si $r < s$, existe $a \in \mathbb{R}^*$ con $s - r = a^2$, y como $a \neq 0$, $\sigma(a) \neq 0$ y $\sigma(s) - \sigma(r) = \sigma(a^2) = \sigma(a)^2 > 0$, con lo que $\sigma(r) < \sigma(s)$. Entonces σ conserva el orden, luego para $t \in \mathbb{R}$, si $\sigma(t) < t$, sea $q \in \mathbb{Q}$ con $\sigma(t) < q < t$, entonces $\sigma(t) < q = \sigma(q) < \sigma(t)\#$, y si $\sigma(t) > t$, sea $q \in \mathbb{Q}$ con $t < q < \sigma(t)$, entonces $\sigma(t) < \sigma(q) = q < \sigma(t)\#$, por lo que $\sigma(t) = t$.

GyA

[Si G es un grupo,] llamamos **orden** de G al cardinal del conjunto. Algunos grupos:

1. Si A es un anillo, [...] $(A^*, \cdot)$ es su **grupo de unidades** [...]

3. Dada una familia $(G_i)_{i \in I}$ de grupos, $\prod_{i \in I} G_i$ [...] con el producto componente a componente.

4. Llamamos **grupo cíclico** de orden $n \in \mathbb{N}^*$ a $C_n \coloneqq \{1, a, a^2, \ldots, a^{n-1}\}$ con [...] $a^i a^j \coloneqq a^{[i+j]_n}$ [...].

5. Si $n \in \mathbb{N}^*$, llamamos **grupo diédrico** de orden $2n$ a

$$D_n := \{1, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$$

con la operación $(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) := a^{[i_1+(-1)^{j_1}i_2]_n}b^{[j_1+j_2]_2}$.

[...] **Teorema de Lagrange:** Si G es un grupo finito y $H \leq G$, $|G| = |H|[G : H]$.

[...] Permutaciones entre conjuntos finitos, S_n con $n \in \mathbb{N}$[, con la composición]. [...] Llamamos **grupo alternado** [...] a $A_n := \ker \operatorname{sgn}$, el subgrupo de S_n de las permutaciones pares.

El **grupo de Klein** es $C_2 \times C_2$. Para todo grupo finito G, $\operatorname{Exp} G \mid |G|$, y en particular, para $g \in G$, $g^{|G|} = 1$. Dado un cuerpo $K \neq 0$, todo subgrupo finito de $(K^*, \cdot)$ es cíclico. En particular, si p es primo, $\mathbb{Z}_p^*$ es cíclico.

Sean $p \in \mathbb{Z}^+$ primo y $\xi := e^{2\pi i/p}$, $\operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong C_{p-1}$. **Demostración:** $\operatorname{Irr}(\xi, \mathbb{Q}) = X^{p-1} + \cdots + X^2 + X + 1$ tiene $p-1$ raíces, los ξ^k para $k \in \{1, \dots, p-1\}$, que están en $\mathbb{Q}(\xi)$, luego $\operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ tiene $p-1$ elementos $\{\sigma_k\}_{k=1}^{p-1}$ donde $\sigma_k(\xi) := \xi^k$. Además, la biyección $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\} \to \operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ dada por $k \mapsto \sigma_k$ es un isomorfismo, pues $1 \mapsto 1_{\mathbb{Q}(\xi)}$ y, para $j, k \in \mathbb{Z}_p^*$, $(\sigma_j\sigma_k)(\xi) = \sigma_j(\xi^k) = \sigma_j(\xi)^k = \xi^{jk} = \sigma_{jk}(\xi)$, luego $\operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong \mathbb{Z}_p^* \cong C_{p-1}$.

2.7. Extensiones finitamente generadas

Una extensión $K \subseteq L$ es **finitamente generada** si existen $\alpha_1, \dots, \alpha_n \in L$ con $L = K(\alpha_1, \dots, \alpha_n)$. $K \subseteq L$ es finita si y solo si es finitamente generada y algebraica, si y solo si existen $\alpha_1, \dots, \alpha_n \in L$ algebraicos sobre K tales que $L = K(\alpha_1, \dots, \alpha_n)$.

$1 \implies 2]$ Toda extensión finita es algebraica, y dada una base $(\alpha_1, \dots, \alpha_n)$ de L sobre K, $L = K(\alpha_1, \dots, \alpha_n)$.

$2 \implies 3]$ Obvio.

$3 \implies 1]$ Para $n = 1$, $[L : K] = \operatorname{grIrr}(\alpha_1, K) < +\infty$. Para $n > 1$, supuesto esto probado para $1, \dots, n-1$, $K \subseteq K(\alpha_1)$ es finita y, como $\alpha_2, \dots, \alpha_n$ son algebraicos sobre $K(\alpha_1)$, $K(\alpha_1) \subseteq K(\alpha_1)(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_n) = L$ es finita, y $[L : K] = [L : K(\alpha_1)][K(\alpha_1) : K]$ es finito.

Dada una extensión algebraica $K \subseteq L$ y $\alpha_1, \dots, \alpha_n \in L$, $K(\alpha_1, \dots, \alpha_n) = K[\alpha_1, \dots, \alpha_n]$.

Sean $K \subseteq L$ una extensión y $S \subseteq L$ un subconjunto cuyos elementos son algebraicos sobre K, entonces $K \subseteq K(S)$ es una extensión algebraica, pues para $\alpha \in K(S)$, $\alpha \in K(\alpha_1, \dots, \alpha_k)$ para ciertos $\alpha_1, \dots, \alpha_k \in S$, que son algebraicos, y por lo anterior $K \subseteq K(\alpha_1, \dots, \alpha_k)$ es algebraica y por tanto α es algebraico.

La **clausura algebraica** de una extensión $K \subseteq L$ o de K en L es

$$\overline{K}_L := \{\alpha \in L \mid \alpha \text{ es algebraico sobre } K\}.$$

Es un cuerpo, pues para $\alpha, \beta \in \overline{K}_L$, $K(\alpha, \beta)$ es una extensión algebraica de K que contiene a 1, $\alpha - \beta$, $\alpha\beta$ y, si $\beta \neq 0$, a $\alpha\beta^{-1}$, y que al ser algebraica está contenida en $\overline{K}_L$. Así, $\overline{K}_L$ es el mayor cuerpo intermedio de $K \subseteq L$ algebraico sobre K.

Para todo cuerpo K, $\overline{K}_{K(X)} = K$.

Un **cuerpo de números algebraicos** es un cuerpo L entre $\mathbb{Q}$ y $\mathbb{C}$ tal que $\mathbb{Q} \subseteq L$ es finita. Llamamos **cuerpo de los números algebraicos** a $\mathcal{A} \coloneqq \overline{\mathbb{Q}}_{\mathbb{C}}$, y **números algebraicos** a los elementos de $\mathcal{A}$, de modo que para todo cuerpo de números algebraicos L, $L \subseteq \mathcal{A}$.

$\mathbb{Q} \subseteq \mathcal{A}$ es algebraica pero no finita, pues para un primo p, $\mathcal{A}$ contiene a $\mathbb{Q}(\xi_p)$ para $\xi_p \coloneqq e^{2\pi i/p}$, pero $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$, luego $[\mathcal{A} : \mathbb{Q}] \geq p - 1$ para todo primo p y por tanto $[\mathcal{A} : \mathbb{Q}]$ es infinito.

2.8. Propiedades de extensiones

Una **torre de extensiones** es una secuencia de extensiones de cuerpos de la forma $(K_{i-1} \subseteq K_i)_{i=1}^n$, escrita como $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$, y cada extensión de la secuencia es una **subextensión** de $K_0 \subseteq K_n$.

Una propiedad de extensiones es **multiplicativa en torres** si para cada torre de extensiones $K \subseteq L \subseteq M$, $K \subseteq M$ cumple la propiedad si y solo si la cumplen $K \subseteq L$ y $L \subseteq M$. Son multiplicativas en torres:

1. Ser finita.

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

2. Ser algebraica.

   $\Longrightarrow$] $K \subseteq L$ es algebraica porque, para $\alpha \in L$, $\alpha \in M$ y α es algebraico sobre K, y $L \subseteq M$ lo es porque, para $\alpha \in M$, α es algebraico sobre K y por tanto sobre L.

   $\Longleftarrow$] Para $\alpha \in M$, existe $f \coloneqq \sum_{i=0}^n a_i X^i \in L[X]$ que tiene a α como raíz. Pero cada $a_i \in L$ es algebraico sobre K, luego $K \subseteq L' \coloneqq K(a_0, \ldots, a_{n-1})$ es finita, y como α es algebraico sobre L' por ser raíz de $f \in L'[X]$, $L' \subseteq L'(\alpha)$ es finita, de modo que $K \subseteq L'(\alpha)$ es algebraica y α es algebraico sobre K.

Una propiedad relativa a extensiones es **estable por levantamientos** si, dadas dos extensiones admisibles $K \subseteq L$ y $K \subseteq M$, si $K \subseteq M$ cumple la propiedad, $L \subseteq LM$ también.

Son estables por levantamientos:

1. Ser algebraica.

   Si $K \subseteq M$ es algebraica, los $\alpha \in M$ son algebraicos sobre L al serlo sobre K, por lo que $L \subseteq L(M) = LM$ es algebraica.

2. Ser finitamente generada.

   Sean $\alpha_1, \ldots, \alpha_n \in M$ tales que $M = K(\alpha_1, \ldots, \alpha_n)$,

   $$LM = LK(\alpha_1, \ldots, \alpha_n) = L(\alpha_1, \ldots, \alpha_m),$$

   pues $LK(\alpha_1, \ldots, \alpha_n)$ es el menor cuerpo que contiene a $L \cup K \cup \{\alpha_1, \ldots, \alpha_n\} = L \cup \{\alpha_1, \ldots, \alpha_n\}$.

3. Ser finita.

   Equivale a ser algebraica y finitamente generada.

Dadas dos extensiones admisibles $K \subseteq L$ y $K \subseteq M$:

1. $[LM : K]$ es finito si y sólo si lo son $[L : K]$ y $[M : K]$, en cuyo caso $[L : K], [M : K] \mid [LM : K]$ y $[LM : K] \leq [L : K][M : K]$.
2. Si L y M son extensiones algebraicas de K, también lo es LM.
3. Si $[LM : K] = [L : K][M : K]$, entonces $L \cap M = K$. El recíproco no se cumple.
4. Si $[L : K] \leq 2$ y $L \cap M = K$, entonces $[LM : K] = [L : K][M : K]$.

Capítulo 3

Cuerpos de descomposición

Sea $K \subseteq L$ una extensión de cuerpos, $f \in K[X]$ de grado $n \geq 0$ se **descompone** o **factoriza completamente** en L si existen $c \in K$ y $\alpha_1, \ldots, \alpha_n \in L$ con

$$f(X) = c\prod_{i=1}^{n}(X - \alpha_i).$$

Sean K un cuerpo y $\mathcal{P} \subseteq K[X] \setminus 0$, un **cuerpo de descomposición** de $\mathcal{P}$ sobre K es una extensión L de K en la que todos los polinomios de $\mathcal{P}$ se descomponen completamente y sus raíces generan L. Un cuerpo de descomposición de $f \in K[X] \setminus 0$ sobre K es uno de $\{f\}$ sobre K.

Sean $K \subseteq L$ una extensión de cuerpos, $f \in K[X] \setminus 0$ de grado n y $\mathcal{P} \subseteq K[X] \setminus 0$:

1. f se descompone completamente sobre L si y solo si lo hace el polinomio mónico f/f_n.
2. Si $n \in \{0, 1\}$, K es cuerpo de descomposición de f sobre K.
3. Sean $f_1, \ldots, f_n \in K[X] \setminus 0$, L es un cuerpo de descomposición de $\{f_1, \ldots, f_n\}$ sobre K si y solo si lo es de $f_1 \cdots f_n$ sobre K.
4. Si L es un cuerpo de descomposición sobre K, $K \subseteq L$ es algebraica.
5. Si L es un cuerpo de descomposición sobre K, también lo es de $\mathcal{P}$ sobre cualquier cuerpo intermedio entre K y L.
6. Si cada $f \in \mathcal{P}$ se descompone completamente en L, sea $S \subseteq L$ el conjunto de raíces de los elementos de $\mathcal{P}$, $K(S)$ es un cuerpo de descomposición de $\mathcal{P}$ sobre K.

Así, para obtener el cuerpo de descomposición de $\mathcal{P}$ sobre K, basta considerar los polinomios mónicos correspondientes a los polinomios de $\mathcal{P}$ de grado al menos 2, u opcionalmente del producto de todos ellos si hay un número finito de ellos, luego hay que encontrar una extensión de K en que estos polinomios tengan todas sus raíces y quedarnos con el subcuerpo generado sobre K por las raíces.

Un cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\xi)$, con $\xi \coloneqq e^{2\pi i/n}$, que también es el cuerpo de descomposición de $X^{n-1} + \cdots + X + 1$ y de $\mathrm{Irr}(\xi, \mathbb{Q})$.

3.1. Cuerpos de descomposición de conjuntos finitos

Si K es un cuerpo y $f \in K[X] \setminus 0$ tiene grado n, existe un cuerpo de descomposición L de f sobre K y $[L:K] \mid n!$. **Demostración:** Para $n = 0$, $f \in K$ y $L = K$, luego $[L:K] = 1 = 0!$. Sea $n > 0$ y supongamos esto probado para $\operatorname{gr} f < n$. Por el teorema de Kronecker existe una extensión L de K en la que f tiene todas sus raíces, y podemos suponer $L = K(\alpha_1, \ldots, \alpha_n)$, siendo $\alpha_1, \ldots, \alpha_n$ las raíces, posiblemente repetidas, de f. Si f es irreducible, $\frac{f}{f_n} = \operatorname{Irr}(\alpha_1, K)$ y $[K(\alpha_1):K] = n$, y como

$$[L : K(\alpha_1)] = [K(\alpha_1)(\alpha_2, \ldots, \alpha_n) : K(\alpha_1)] \mid (n-1)!$$

por hipótesis de inducción, entonces $[L:K] = [L:K(\alpha_1)][K(\alpha_1):K] \mid n!$. Si no es irreducible, sean $g, h \in K[X] \setminus K$ con $f = gh$ y $m \coloneqq \operatorname{gr} g$, podemos suponer que $\alpha_1, \ldots, \alpha_m$ son las raíces de g y $\alpha_{m+1}, \ldots, \alpha_n$ son las de h, y como por hipótesis de inducción,

$$[L : K(\alpha_1, \ldots, \alpha_m)] = [K(\alpha_1, \ldots, \alpha_m)(\alpha_{m+1}, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_m)] \mid (n-m)!$$

y $[K(\alpha_1, \ldots, \alpha_m) : K] \mid m!$, $[L:K] \mid m!(n-m)!$, pero $\binom{n}{m} = \frac{n!}{m!(n-m)!} \in \mathbb{Z}$, luego $[L:K] \mid m!(n-m)! \mid n!$.

Esta cota no es mejorable; por ejemplo, las raíces de $X^3 - 2$ en $\mathbb{C}$ son α, $\alpha\omega$ y $\alpha\omega^2$ con $\alpha \coloneqq \sqrt[3]{2}$ y $\omega \coloneqq e^{2\pi i/3}$, luego un cuerpo de descomposición es $\mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$, y como $\omega = \frac{1}{2}\alpha^2(\alpha\omega)$, esto es lo mismo que $\mathbb{Q}(\alpha, \omega)$, pero como $\operatorname{Irr}(\alpha, \mathbb{Q}) = X^3 - 2$ e $\operatorname{Irr}(\omega, \mathbb{Q}(\alpha)) = X^2 + X + 1$, $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}] = [\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = 2 \cdot 3 = 6$.

> Si $K \subseteq L$ es una extensión de grado 2, L es el cuerpo de descomposición sobre K de un polinomio de $K[X]$. Sean $K \subseteq L$ y $K \subseteq M$ son extensiones admisibles:
>
> 1. Si L es un cuerpo de descomposición de $f \in K[X]$ sobre K, LM es un cuerpo de descomposición de f sobre M.
> 2. Si L y M son cuerpos de descomposición respectivos de $f, g \in K[X]$ sobre K, LM es un cuerpo de descomposición de fg sobre K.

3.2. Grupo de Galois de un polinomio

Dados un cuerpo K y un $f \in K[X]$ con cuerpo de descomposición L sobre K, el **grupo de Galois** de f es $G_f \coloneqq \operatorname{Gal}(L/K)$. Sean $\alpha_1, \ldots, \alpha_n \in L$ las raíces distintas de f, cada $\sigma \in G_f$ lleva raíces a raíces y por tanto $\sigma|_{\{\alpha_1,\ldots,\alpha_n\}} : \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha_1, \ldots, \alpha_n\}$ es inyectiva por serlo σ y por tanto biyectiva. Sea $\varphi : G_f \to \mathcal{S}_n$ dada por $\varphi(\sigma)(i) = j \iff \sigma(\alpha_i) = \alpha_j$, φ es un homomorfismo inyectivo y por tanto $G_f \cong \operatorname{Im}\varphi \leq \mathcal{S}_n$.

Para el polinomio ciclotómico Φ_p con p primo, sea $\xi \coloneqq e^{2\pi i/p}$,

$$G_{\Phi_p} = \operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}.$$

3.3. Clausura algebraica

Un cuerpo K es **algebraicamente cerrado** si todo $f \in K[X] \setminus K$ tiene una raíz en K, si y sólo si todo irreducible de $K[X]$ es de grado 1, si y sólo si todo $f \in K[X] \setminus 0$ se descompone

completamente en K, si y sólo si existe un subcuerpo K_0 de K tal que $K_0 \subseteq K$ es algebraica y todo $f \in K_0[X] \setminus 0$ se descompone completamente en K, si y sólo si K no admite extensiones algebraicas propias.

$1 \implies 2]$ Todo $f \in K[X]$ con $\mathrm{gr} f \geq 2$ tiene una raíz y por tanto no es irreducible.

$2 \implies 3]$ $K[X]$ es un DFU.

$3 \implies 4]$ Tomamos $K_0 = K$.

$4 \implies 5]$ Sea $K \subseteq L$ una extensión algebraica y queremos ver que $K = L$. Como $K_0 \subseteq K \subseteq L$ son algebraicas, $K_0 \subseteq L$ también, luego para $\alpha \in L$ existe $\mathrm{Irr}(\alpha, K_0)$ y se descompone completamente en K, con lo que $\alpha \in K$ y $L \subseteq K$.

$5 \implies 1]$ Para $f \in K[X] \setminus K$, por el teorema de Kronecker existe una extensión algebraica L de K en la que f tiene una raíz α, pero esta no puede ser propia, luego $L = K$ y $\alpha \in K$.

Así:

1. Ningún cuerpo finito es algebraicamente cerrado.

   Sea K un cuerpo finito, si hubiera una cantidad finita de irreducibles mónicos en $K[X]$, su producto más 1 sería un irreducible distinto a todos ellos#, luego en $K[X]$ hay infinitos irreducibles mónicos y por tanto los hay de grado mayor que 1.

2. Ser algebraicamente cerrado se conserva por isomorfismos.

   Los anillos de polinomios también son isomorfos y ser irreducible se conserva.

Una **clausura algebraica** de un cuerpo K es una extensión $K \subseteq L$ algebraica con L algebraicamente cerrado. Si $K \subseteq L$ es una extensión con L algebraicamente cerrado, $\overline{K}_L$ es una clausura algebraica de K. En efecto, $K \subseteq \overline{K}_L$ es algebraica y, para $f \in \overline{K}_L[X] \setminus \overline{K}_L$, f tiene una raíz α en L, de modo que α es algebraico sobre $\overline{K}_L$ y, como $K \subseteq \overline{K}_L \subseteq \overline{K}_L(\alpha)$ son extensiones algebraicas, $K \subseteq \overline{K}_L(\alpha)$ también y por tanto $\overline{K}_L(\alpha) \subseteq \overline{K}_L$ y $\alpha \in \overline{K}_L$, luego $\overline{K}_L$ es algebraicamente cerrado.

Así, $\mathbb{C}$ es una clausura algebraica de $\mathbb{R}$ y, por lo anterior, el cuerpo $\mathcal{A}$ de los números algebraicos es una clausura algebraica de $\mathbb{Q}$.

Como **teorema**, todo cuerpo tiene una clausura algebraica. Si K es un cuerpo y $\mathcal{P} \subseteq K[X] \setminus 0$, toda clausura algebraica $\overline{K}$ de K contiene un único cuerpo de descomposición de $\mathcal{P}$, $K(\{\alpha \in \overline{K} \mid \exists f \in \mathcal{P} : f(\alpha) = 0\})$, por lo que existe un cuerpo de descomposición de $\mathcal{P}$ sobre K.

Como **teorema**, si $K \subseteq L$ es una extensión algebraica, todo homomorfismo de cuerpos $\sigma : K \to M$ con M algebraicamente cerrado se extiende a un homomorfismo $\overline{\sigma} : L \to M$.

Dada una extensión $K \subseteq M$, M es una clausura algebraica de K si y sólo si $K \subseteq M$ es algebraica y toda extensión algebraica $K \subseteq L$ admite un K-homomorfismo $\sigma : L \to M$.

$\implies]$ Por lo anterior, como M es algebraicamente cerrado, la inclusión $i : K \hookrightarrow M$ se extiende a un homomorfismo $\overline{\imath} : L \to M$, que es un K-homomorfismo.

$\impliedby]$ Sea $\overline{K}$ una clausura algebraica de K, existe un K-homomorfismo $\sigma : \overline{K} \to M$, luego $\sigma(\overline{K})$ es algebraicamente cerrado por ser isomorfo a $\overline{K}$ y, como $\sigma(\overline{K}) \subseteq M$ es algebraica y $\sigma(\overline{K})$ no admite extensiones algebraicas propias, $\sigma(\overline{K}) = M$.

3.4. Unicidad

Sean $\sigma : K \to K'$ un isomorfismo de cuerpos y M y M' clausuras algebraicas respectivas de K y K', entonces σ se extiende a un isomorfismo $\overline{\sigma} : M \to M'$, pues si $u : K' \hookrightarrow M'$ es la inclusión, $u \circ \sigma : K \to M'$ se extiende a un homomorfismo $\overline{\sigma} : M \to M'$. En particular dos clausuras algebraicas de K son K-isomorfas, tomando $\sigma = 1_K$.

Sean $\sigma : K \to K'$ un isomorfismo de cuerpos, L un cuerpo de descomposición de $\mathcal{P} \subseteq K[X] \setminus 0$ sobre K y L' uno de $\mathcal{P}' \coloneqq \sigma(\mathcal{P})$ sobre K, entonces σ se extiende a un isomorfismo $\overline{\sigma} : L \to L'$, y en particular dos cuerpos de descomposición de $\mathcal{P}$ sobre K son K-isomorfos.

Dada una extensión de cuerpos $K \subseteq L$, L es la clausura algebraica de K si y sólo si es el cuerpo de descomposición sobre K de $K[X] \setminus 0$, si y sólo si es el cuerpo de descomposición sobre K de todos los irreducibles de $K[X]$.

3.5. Cuerpos finitos

Dado un anillo A de característica prima p, $h : A \to A$ dado por $h(a) \coloneqq a^p$ es un homomorfismo de anillos, el **homomorfismo de Frobenius**, pues conserva el 1, $h(ab) = (ab)^p = a^p b^p$ y $h(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^p b^{p-k} = a^p + b^p$, usando que, para $k \in \{1, \dots, p-1\}$, $\binom{p}{k} = \frac{p!}{(p-k)!k!} = 0$ al ser un cociente de un múltiplo de p entre algo que no es múltiplo de p. En particular $h^n = (a \mapsto a^{p^n})$ es un homomorfismo.

Como **teorema**:

1. Si K es un cuerpo finito, existen $p, n \in \mathbb{Z}^+$ con p primo tales que $\mathrm{car}K = p$, $|K| = p^n$ y K es un cuerpo de descomposición sobre $\mathbb{Z}_p$ de $X^{p^n} - X$.

   Como K es finito, $\mathrm{car}K \neq 0$ y $\mathrm{car}K = p$ para cierto primo p. Entonces K es una extensión finita de su subcuerpo primo $\mathbb{Z}_p$ y, tomando $n \coloneqq [K : \mathbb{Z}_p]$, $|K| = p^n$. El grupo multiplicativo K^* tiene $p^n - 1$ elementos, pero para $g \in K^*$, $g^{|K^*|} = g^{p^n - 1} = 1$ y g es raíz de $X^{p^n-1} - 1$ y por tanto de $f \coloneqq X^{p^n} - X$, del que también es raíz 0. Como f tiene a lo sumo $p^n = |K|$ raíces, K está formado por las raíces de f y por tanto está generado por estas.

2. Para cada $p, n \in \mathbb{Z}^+$ con p primo, sea $\overline{\mathbb{Z}_p}$ la clausura algebraica de $\mathbb{Z}_p$, el cuerpo de descomposición sobre $\mathbb{Z}_p$ de $X^{p^n} - X$ tiene p^n elementos y viene dado por $\mathbb{F}_{p^n} \coloneqq \{\alpha \in \overline{\mathbb{Z}_p} \mid \alpha^{p^n} = \alpha\}$.

   Sea $S \coloneqq \{\alpha \in \overline{\mathbb{Z}_p} \mid \alpha^{p^n} = \alpha\}$ el conjunto de raíces de $f \coloneqq X^{p^n} - X$ en $\mathbb{Z}_p$, el cuerpo de descomposición es $\mathbb{F}_{p^n} = \mathbb{Z}_p(S)$, pero S es un cuerpo, pues $1 \in S$ y, para $\alpha, \beta \in S$, por el homomorfismo de Frobenius, $(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ y $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$. Además, $(1) = \mathbb{Z}_p \subseteq S$ y $\mathbb{Z}_p(S) = S$, u como $\mathrm{mcd}\{f, f'\} = \mathrm{mcd}\{X^{p^n} - X, -1\} = 1$, f no tiene raíces múltiples y $|\mathbb{F}_{p^n}| = |S| = p^n$.

3. Para $p, n \in \mathbb{Z}^+$ con p primo, todo cuerpo finito de tamaño p^n es isomorfo a $\mathbb{F}_{p^n}$.

Con esto:

1. Vistos como subcuerpos de $\overline{\mathbb{Z}_p}$, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$.

   $\Longrightarrow$] $\mathbb{Z}_p \subseteq \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, luego $m = [\mathbb{F}_{p^m} : \mathbb{Z}_p] \mid [\mathbb{F}_{p^n} : \mathbb{Z}_p] = n$.

$\Longleftarrow$] Sea $t \coloneqq \frac{n}{m}$, para α con $\alpha = \alpha^{p^m}$ es $\alpha = \alpha^{p^{mt}} = \alpha^{p^n}$. En efecto, para $t = 1$ esto es trivial, y para $t > 1$, supuesto esto probado para $t-1$, $\alpha^{p^{mt}} = \alpha^{p^{m(t-1)+m}} = \alpha^{p^{m(t-1)}p^m} = (\alpha^{p^{m(t-1)}})^{p^m} = \alpha^{p^m} = \alpha$.

2. $X^{p^n} - X$ es el producto de todos los irreducibles mónicos de $\mathbb{Z}_p[X]$ cuyo grado divide a n.

   Como $F \coloneqq X^{p^n} - X$ no tiene raíces múltiples, no tiene factores repetidos y es pues el producto de todos los irreducibles mónicos que lo dividen, y queremos ver que, para un irreducible mónico $f \in \mathbb{Z}_p[X]$ de grado m, $f \mid F$ si y solo si $m \mid n$. Sea entonces una raíz $\alpha \in \overline{\mathbb{Z}_p}$ de f, $f = \mathrm{Irr}(\alpha, \mathbb{Z}_p)$ y $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = m$, luego $|\mathbb{Z}_p(\alpha)| = p^m$ y por tanto $\mathbb{Z}_p(\alpha) \cong \mathbb{F}_{p^m}$. Entonces, por la caracterización de $\mathrm{Irr}(\alpha, f)$, $f \mid F$ si y solo si α es raíz de F, si y solo si $\alpha^{p^n} = \alpha$, si y solo si $\alpha \in \mathbb{F}_{p^n}$, si y solo si $\mathbb{F}_{p^m} \cong \mathbb{Z}_p(\alpha) \subseteq \mathbb{F}_{p^n}$, si y solo si $m \mid n$.

3. Dada una extensión de cuerpos finitos $K \subseteq L$ de grado m, existe $\alpha \in L$ tal que $L = K(\alpha)$, $\mathrm{Irr}(\alpha, K)$ tiene m raíces distintas en L y $|\mathrm{Gal}(L/K)| = m$.

   Como L es finito, L^* es cíclico y existe $\alpha \in L^*$ con $L^* = \langle\alpha\rangle$, pero entonces $L = L^* \cup \{0\} = K(\alpha)$. Como los elementos de L son las raíces de $f \coloneqq X^{p^n} - X$, α es raíz de f, con lo que $\mathrm{Irr}(\alpha, K) \mid f$ y las m raíces de $\mathrm{Irr}(\alpha, K)$ lo son de f y están en m. Además estas raíces son distintas ya que f no tiene raíces múltiples, y como $\mathrm{Irr}(\alpha, K)$ tiene m raíces en $L = K(\alpha)$, $|\mathrm{Gal}(K(\alpha)/K)| = m$.

4. Si K es finito, en $K[X]$ existen polinomios irreducibles de cualquier grado $m \geq 1$.

   Sean $K =: \mathbb{F}_{p^n}$ y $L \coloneqq \mathbb{F}_{p^{nm}}$, entonces $K \subseteq L$ y, por lo anterior, existe $\alpha \in L$ tal que $\mathrm{Irr}(\alpha, K)$ tiene m raíces distintas en L y es un irreducible de grado m en $K[X]$.

Si p es primo:

1. Todo α algebraico sobre $\mathbb{Z}_p$ cumple $\mathrm{Irr}(\alpha, \mathbb{Z}_p) = \mathrm{Irr}(\alpha^p, \mathbb{Z}_p)$.
2. La función $h : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ dada por $h(x) \coloneqq x^p$ es biyectiva.
3. La suma de todos los elementos de un cuerpo finito con más de dos elementos es 0.
4. Si L es el cuerpo de descomposición sobre $\mathbb{Z}_p$ de un $f \in \mathbb{Z}_p[X]$ que se factoriza en irreducibles como $f =: f_1 \cdots f_r$, sea $[L : \mathbb{Z}_p] = \mathrm{mcm}\{\mathrm{gr} f_1, \ldots, \mathrm{gr} f_r\}$.

Si $p = 2k+1$ es un primo impar, llamamos **restos cuadráticos** módulo p a los cuadrados no nulos en $\mathbb{Z}_p$, $1^2, 2^2, \ldots, k^2$. Entonces $\prod_{i=1}^k i^2 = (-1)^{k+1}$ y, si $p \neq 3$, $\sum_{i=1}^k i^k = 0$.

1. $\mathbb{F}_4 = \{a\alpha + b\}_{a,b \in \mathbb{Z}_2}$ se obtiene al añadir a $\mathbb{Z}_2$ una raíz α del irreducible $X^2 + X + 1 \in \mathbb{Z}_2[X]$. $\mathbb{F}_4^* = \langle\alpha\rangle = \langle\alpha + 1\rangle$.
2. $\mathbb{F}_8 = \{a\beta^2 + b\beta + c\}_{a,b,c \in \mathbb{Z}_2}$ se obtiene al añadir a $\mathbb{Z}_2$ una raíz β del irreducible $X^3 + X + 1 \in \mathbb{Z}_2[X]$. $\mathbb{F}_8^* = \langle x\rangle$ para $x \in \mathbb{F}_8^* \setminus \{1\}$.
3. $\mathbb{F}_9 = \{a\gamma + b\}_{a,b \in \mathbb{Z}_3}$ se obtiene al añadir a $\mathbb{Z}_3$ una raíz γ del irreducible $X^2 + 1 \in \mathbb{Z}_3[X]$. $\mathbb{F}_9^* = \langle\gamma + 1\rangle$.

Capítulo 4

Raíces de la unidad

Sean K un cuerpo y $n \geq 2$, un $\xi \in K$ es una **raíz n-ésima de la unidad** o **de uno** si $\xi^n = 1$, y llamamos

$$\mathcal{U}_n(K) := \{\xi \in K \mid \xi^n = 1\} = \{\xi \in K \mid o_{K^*}(\xi) \mid n\}.$$

En efecto, el orden de ξ en K^* es el menor $m > 0$ con $\xi^m = n$, luego si $m \mid n$ entonces $\xi^n = (\xi^m)^{n/m} = 1^{n/m} = 1$ y si $\xi^n = 1$, sean q y r el cociente y resto de n/m, entonces $1 = \xi^{mq+r} = (\xi^m)^q \xi^r = \xi^r$, pero como $r < m$ debe ser $r = 0$ y $mq = n$.

$\mathcal{U}_n(K)$ es un subgrupo cíclico de K^*, pues contiene al 1, es cerrado por productos ($\xi^n = 1 \wedge \mu^n = 1 \implies (\xi\mu)^n = \xi^n\mu^n = 1$) y, como K^* es cíclico, todos sus subgrupos también. Una raíz n-ésima es **primitiva** si $o_{K^*}(\xi) = n$.

Propiedades: Si K es un cuerpo y $n \geq 2$:

1. Toda raíz n-ésima de uno es raíz tn-ésima de uno para $t \geq 1$.
2. 1 no es raíz n-ésima primitiva.
3. Si $\mathrm{car} K \neq 2$, -1 es raíz cuadrada primitiva de uno.
4. $\xi \in K$ es raíz n-ésima primitiva de uno si y sólo si $|\mathcal{U}_n(K)| = n$ y $\mathcal{U}_n(K) = \langle\xi\rangle$.
5. K contiene alguna raíz n-ésima primitiva de uno si y sólo si $|\mathcal{U}_n(K)| = n$.
6. Si K es finito, contiene alguna raíz n-ésima primitiva de uno si y sólo si $n \mid |K| - 1$.

Ejemplos:

1. $\mathcal{U}_n(\mathbb{C}) = \langle e^{2\pi i/n}\rangle$.
2. $$\mathcal{U}_n(\mathbb{R}) = \begin{cases} \{\pm 1\}, & n \text{ es par;} \\ \{1\}, & n \text{ es impar.} \end{cases}$$
3. Ni $\mathbb{R}$ ni ningún subcuerpo suyo contienen raíces n-ésimas primitivas para $n \geq 3$.

4. $\mathbb{F}_4$ tiene 2 raíces cúbicas primitivas; $\mathbb{F}_8$ tiene 6 raíces séptimas primitivas, y $\mathbb{F}_9$ tiene 4 raíces octavas primitivas y 2 raíces cuartas primitivas.

5. Si $\mathrm{car}K = p \neq 0$, la única raíz p-ésima es 1.

6. Una extensión finita de $\mathbb{Q}$ tiene solo un número finito de raíces de uno.

Dados un cuerpo K y $n \geq 2$, existe una extensión L de K que contiene raíces n-ésimas primitivas de la unidad si y sólo si $\mathrm{car}K \nmid n$.

$\Longrightarrow$] Sea L un cuerpo de descomposición sobre K de $X^n - 1$, como $f' = nX^{n-1}$ y $n \neq 0$ al ser $\mathrm{car}K \nmid n$, la única raíz de f' es 0 y por tanto f no tiene raíces múltiples, luego tiene n raíces raíces distintas y $|\mathcal{U}_n(L)| = n$.

$\Longleftarrow$] Probamos el contrarrecíproco. Si $p \coloneqq \mathrm{car}K \mid n$, existe $t \in \mathbb{N}$ con $n = tp$ y $X^n - 1 = X^{tp} - 1^p = (X^t - 1)^p$ por el homomorfismo de Frobenius, luego $X^n - 1$ tiene a lo sumo $t = n/p < n$ raíces y por tanto no tiene raíces n-ésimas de uno primitivas.

GyA

Si [G es un grupo,] a[$\in G$] tiene orden finito y $n > 0$,

$$|a^n| = \frac{|a|}{\mathrm{mcd}\{|a|, n\}}.$$

CyN

Definimos la **función ϕ de Euler** como $\phi : \mathbb{N} \to \mathbb{N}$ tal que $\phi(m) = |\{x \in \mathbb{N} | 1 \leq x \leq m \wedge \mathrm{mcd}(x, m) = 1\}| = |\mathbb{Z}_m^*|$. [...] Si p es primo, $\phi(p^n) = p^{n-1}(p-1)$. [...] Si p es primo, $\phi(p^n) = p^{n-1}(p-1)$.

Si un cuerpo K tiene una raíz n-ésima primitiva de uno ξ:

1. K tiene exactamente n raíces n-ésimas de uno, $\xi, \xi^2, \ldots, \xi^n = 1$, y $\phi(n)$ de ellas son primitivas. En particular $X^n - 1$ se descompone completamente en $K[X]$.

2. Para cada $d \mid n$ natural hay una raíz d-ésima primitiva en K, $\xi^{n/d}$.

Si K es finito, esto se cumple para $n = |K| - 1$, y si $K \subseteq \mathbb{C}$, se aplica cuando $e^{2\pi i/n} \in K$.

4.1. Polinomios ciclotómicos

Sean P un cuerpo primo ($\mathbb{Q}$ o $\mathbb{Z}_p$), $n \geq 2$ con $\mathrm{car}P \nmid n$ y L el cuerpo de descomposición sobre P de $X^n - 1$, que contiene $\phi(n)$ raíces n-ésimas primitivas de uno $\xi_1, \ldots, \xi_n$, llamamos **n-ésimo polinomio ciclotómico en característica car$P$** a

$$\Phi_n(X) \coloneqq (X - \xi_1) \cdots (X - \xi_r) \in L[X].$$

Si $\mathrm{car}K \nmid n$, $X^n - 1 = \prod_{0<d|n} \Phi_d(X)$, con el convenio de que $\Phi_1(X) = X - 1$.

Si P es un cuerpo primo:

1. Si $q \neq \mathrm{car}P$ es primo, $\Phi_q(X) = X^{q-1} + \cdots + X + 1$.
2. Si $n \geq 3$ es impar, $\Phi_{2n}(X) = \Phi_n(-X)$.
3. Si p es primo y $k \geq 1$, entonces $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$.
4. Si $n = p_1^{r_1} \cdots p_s^{r_s}$ con los p_i primos distintos, $\Phi_n(X) = \Phi_{p_1 \cdots p_s}(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$.
5. Si p es primo y no divide a n entonces $\Phi_{pn}(X)\Phi_n(X) = \Phi_n(X^p)$.
6. $\Phi_n \in P[X]$.

4.2. Extensiones ciclotómicas

Una extensión $K \subseteq F$ es una **ciclotómica de orden** n o F es el n-ésimo **cuerpo ciclotómico** sobre K si F es el cuerpo de descomposición de $X^n - 1$ sobre K, y F también es el cuerpo ciclotómico sobre cualquier K' entre K y F. Cada cuerpo tiene una extensión ciclotómica de cada orden, única salvo isomorfismos. Ejemplos:

1. $\mathbb{Q} \subseteq \mathbb{Q}(e^{2\pi i/n})$ es una extensión ciclotómica de orden n.
2. $\mathbb{Z}_p \subseteq \mathbb{F}_{p^n}$ es ciclotómica de orden $p^n - 1$.
3. La extensión ciclotómica de orden n sobre $\mathbb{Z}_p$ con $p \nmid n$ es $\mathbb{F}_{p^m}$, con $m := o_{\mathbb{Z}_n^*}(p)$.

Dado un cuerpo K con $p := \mathrm{car}K \neq 0$ y $m \in \mathbb{Z}^+$ con $p \nmid m$, para $r \in \mathbb{N}$, las extensiones ciclotómicas de órdenes m y $p^r m$ coinciden. En efecto, por el homomorfismo de Frobenius, $(\xi^m - 1)^{p^r} = \xi^{p^r m} - 1$, luego ξ es raíz de $X^{p^r m} - 1$ si y sólo si lo es de $X^m - 1$.

Como **teorema**, si $\mathrm{car}K \nmid n$ y F es una extensión ciclotómica de orden n sobre K:

1. $F = K(\xi)$, siendo ξ una raíz n-ésima primitiva de uno.

   Como $\mathrm{car}F = \mathrm{car}K \nmid n$, existe una extensión M de F con una raíz n-ésima primitiva ξ, luego $\xi \in F$, $K(\xi) \subseteq F$ y, como el resto de raíces de $X^n - 1$ son potencias de ξ, $F \subseteq K(\xi)$.

2. $\mathrm{Gal}(F/K)$ tiene tamaño $[F : K]$ y es isomorfo a un subgrupo de $\mathbb{Z}_n^*$.

   $|\mathrm{Gal}(K(\xi)/K)| = [K(\xi) : K]$ porque el resto de raíces de $X^n - 1$ y por tanto de $\mathrm{Irr}(\xi, K)$ están en $K(\xi)$. Cada $\sigma \in \mathrm{Gal}(F/K)$ lleva ξ a una raíz ξ^j de $X^n - 1$ que debe tener el mismo orden que ξ por ser σ inyectiva, luego $\sigma(\xi) = \xi^j$ para cierto j coprimo con n. Entonces $f : \mathrm{Gal}(F/K) \to \mathbb{Z}_n^*$ dada por $f(\sigma) = j \iff \sigma(\xi) = \xi^j$, f está bien definida, es inyectiva y es un homomorfismo, ya que $f(1) = 1$ y, llamando $\sigma_j \in \mathrm{Gal}(F/K)$ al elemento con $\sigma_j(\xi) = \xi^j$, $f(\sigma_j\sigma_k) = f(\sigma_{jk}) = jk = f(\sigma_j)f(\sigma_k)$.

3. Si n es primo, $\mathrm{Gal}(F/K)$ es un cíclico.

   $\mathbb{Z}_n^*$ es cíclico y por tanto sus subgrupos también.

En general los polinomios ciclotómicos no son irreducibles en el cuerpo primo, pues por ejemplo en $\mathbb{Z}_7$ las raíces terceras primitivas son 2 y 4 y $\Phi_3(X) = (X-2)(X-4)$. Sin embargo, como **teorema**, si ξ es una raíz n-ésima primitiva de uno en $\mathbb{C}$, $\Phi_n(X) = \mathrm{Irr}(\xi, \mathbb{Q})$, luego si $\xi \coloneqq e^{2\pi i/n}$, $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$ y $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong \mathbb{Z}_n^*$. Si $n, m \in \mathbb{Z}^+$ son coprimos y, para $r \in \mathbb{Z}^+$, $\xi_r \in \mathbb{C}$ es cualquier raíz r-ésima primitiva de uno, entonces $\mathbb{Q}(\xi_n, \xi_m) = \mathbb{Q}(\xi_{nm})$ y $\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}$.

Capítulo 5

Extensiones normales y separables

5.1. Extensiones normales

Una extensión $K \subseteq L$ es **normal**, o L **es normal sobre** K, si es algebraica y todo irreducible de $K[X]$ con una raíz en L tiene todas sus raíces en L. Basta considerar los irreducibles mónicos de grado al menos 3, pues los de grado 1 tienen su raíz en K y, si $f = X^2 + aX + b$ tiene raíces α_1 y α_2, $\alpha_1 + \alpha_2 = -a$ y, si $\alpha_1 \in L$, $\alpha_2 = -\alpha_1 - a \in L$.

Ejemplos:

1. $K \subseteq \overline{K}$ es normal.
2. $K \subseteq K$ es normal.

   Los irreducibles en K con una raíz en K son de grado 1.
3. Si $[L : K] = 2$, $K \subseteq L$ es normal.

   Los irreducibles en K con una raíz $\alpha \in L$ tienen grado $\mathrm{grIrr}(\alpha, K) \leq 2$.

Si $K \subseteq L$ es algebraica, todo K-encaje $\sigma : L \to L$ es un K-automorfismo. **Demostración:** Para $\alpha \in L$, sean $f \coloneqq \mathrm{Irr}(\alpha, K)$ y $R \coloneqq \{\alpha_1 \coloneqq \alpha, \ldots, \alpha_m\}$ el conjunto de las raíces de f en L, entonces $f = \mathrm{Irr}(\alpha_i, K)$ para cada i y, como σ lleva raíces a raíces, $\sigma(R) \subseteq R$, pero σ es inyectiva, luego $\sigma|_R : R \to R$ es biyectiva y $\alpha \in R = \sigma(R) \subseteq \sigma(L)$.

Como **teorema**, una extensión algebraica $K \subseteq L$ es normal si y sólo si L es el cuerpo de descomposición sobre K de un cierto $\mathcal{P} \subseteq K[X] \setminus 0$, si y sólo si para cada clausura algebraica $\overline{L}$ de L y todo K-encaje $\sigma : L \to \overline{L}$ es $\sigma(L) = L$, si y sólo si existe una clausura algebraica $\overline{L}$ de L para la que todo K-encaje $\sigma : L \to \overline{L}$ cumple $\sigma(L) = L$.

$1 \implies 2]$ Sean $\mathcal{P} \coloneqq \{f_\alpha \coloneqq \mathrm{Irr}(\alpha, K)\}_{\alpha \in L} \subseteq K[X] \setminus 0$ y S el conjunto de todas las raíces de los polinomios de $\mathcal{P}$ en una clausura $\overline{L}$ de L, cada $\alpha \in L$ está en S por ser raíz de f_α y cada $\beta \in S$ está en L ya que es raíz de un irreducible $f_\alpha \in K[X]$ que ya tiene una raíz α en L y por tanto las tiene todas, luego $L = S$ es el cuerpo de descomposición de $\mathcal{P}$ sobre K.

$2 \implies 3]$ Para $f \in \mathcal{P}$ y $\alpha \in L$ raíz de f, como los K-encajes llevan raíces a raíces, $\sigma(\alpha)$ es raíz de f y está en L, y como L está generado por las raíces de los $f \in \mathcal{P}$, $\sigma(L) \subseteq L$, luego por la proposición anterior σ es un K-automorfismo y $\sigma(L) = L$.

$3 \implies 4]$ Por la existencia de clausura algebraica.

$4 \implies 1]$ Sean $f \in K[X]$ irreducible con una raíz $\alpha \in L$ y $\beta \in \overline{L}$ otra raíz de f, existe un K-isomorfismo $\sigma' : K(\alpha) \to K(\beta)$ con $\sigma'(\alpha) = \beta$, pero como $K(\beta) \subseteq L$, podemos ver $\sigma' : K(\alpha) \to \overline{L}$ y, como $K(\alpha) \subseteq L$ es algebraica por serlo $K \subseteq L$, σ' se extiende a un K-homomorfismo $\sigma : L \to \overline{L}$, pero por hipótesis $\sigma(L) = L$, luego $\beta = \sigma'(\alpha) = \sigma(\alpha) \in L$.

Una extensión finita $K \subseteq L$ es normal si y sólo si L es el cuerpo de descomposición sobre K de un polinomio de $K[X]$.

$\implies]$ Si $L = K(\alpha_1, \ldots, \alpha_n)$, sean $f_\alpha \coloneqq \mathrm{Irr}(\alpha, K)$ para $\alpha \in L$ y S el conjunto de las raíces de $f_{\alpha_1}, \ldots, f_{\alpha_n}$, cada $\beta \in S$ está en L por ser raíz de un $f_{\alpha_i} \in K[X]$ teniendo f_{α_i} una raíz en L y siendo $K \subseteq L$ normal, luego $S \subseteq L$ y $K(S) \subseteq L$, pero $\{\alpha_1, \ldots, \alpha_n\} \subseteq S$ y por tanto $L = K(\alpha_1, \ldots, \alpha_n) \subseteq K(S)$, luego $L = K(S)$ es el cuerpo de descomposición sobre K de $\{f_{\alpha_1}, \ldots, f_{\alpha_n}\}$ y por tanto de $f_{\alpha_1} \cdots f_{\alpha_n}$.

$\impliedby]$ Por el teorema.

Dada una torre $K \subseteq E \subseteq L$:

1. Si $K \subseteq L$ es normal, $E \subseteq L$ también.

   Si L es cuerpo de descomposición de un $\mathcal{P} \subseteq K[X] \setminus 0$ sobre K, también lo es sobre E.

2. Que $K \subseteq L$ sea normal no implica que $K \subseteq E$ lo sea.

   $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ es normal por ser el cuerpo de descomposición de $X^3 - 2$, pero $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ no lo es ya que solo una raíz del irreducible $X^3 - 2$ está en $\mathbb{Q}(\sqrt[3]{2})$.

3. Que $K \subseteq E$ y $E \subseteq L$ sean normales no implica que $K \subseteq L$ lo sea.

   $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ son normales por tener grado 2, pero $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ no lo es ya que dos de las raíces del irreducible $X^4 - 2$ no están en $\mathbb{Q}(\sqrt[4]{2})$.

> Si $K \subseteq L$ es normal, $K \subseteq E$ lo es si y sólo si E es **estable** en $K \subseteq L$, es decir, si $\forall \sigma \in \mathrm{Gal}(L/K), \sigma(E) = E$. Una extensión $K \subseteq L$ es normal si y sólo si existe una extensión $L \subseteq N$ con $K \subseteq N$ normal y tal que todo K-encaje de L en N es un K-automorfismo de L.

Sean $K \subseteq L$ y $K \subseteq M$ extensiones admisibles, si L es el cuerpo de descomposición sobre K de un $\mathcal{P} \subseteq K[X] \setminus 0$ entonces LM es el cuerpo de descomposición sobre M de $\mathcal{P}$. En efecto, sean S el conjunto de raíces de los polinomios de $\mathcal{P}$ en L, como $L = K(S)$, $LM = ML = MK(S) = M(S)$. Ser normal es estable por levantamientos, pues lo es ser algebraica y ser cuerpo de descomposición de un $\mathcal{P}$.

Si $K \subseteq L$ y $K \subseteq M$ son normales y admisibles, $K \subseteq LM$ es normal. En efecto, L es el cuerpo de descomposición sobre K de un $\mathcal{P} \subseteq K[X] \setminus 0$ y M el de un $\mathcal{Q} \subseteq K[X] \setminus 0$, luego si S el conjunto de las raíces de polinomios de $\mathcal{P}$ y T es el de las raíces de polinomios de Q, $LM = K(S)K(T) = K(S \cup T)$ es el cuerpo de descomposición sobre K de $\mathcal{P} \cup \mathcal{Q}$ y por tanto es normal.

5.2. Clausura normal

Si $\{L_i\}_{i\in I}$ es una familia de extensiones admisibles de K y cada $K \subseteq L_i$ es normal, también lo es $K \subseteq \bigcap_{i\in I} L_i$. En efecto, si $f \in K[X]$ es irreducible con una raíz en $\bigcap_{i\in I} L_i$, entonces tiene todas sus raíces en todos los L_i y por tanto en $\bigcap_{i\in I} L_i$.

Sean $K \subseteq L$ algebraica y $\overline{L}$ una clausura normal de L, la **clausura normal** de $K \subseteq L$ en $\overline{L}$ es la menor extensión normal de K entre L y $\overline{L}$, y viene dada por

$$N := \bigcap\{E \text{ intermedio en } L \subseteq \overline{L} \mid K \subseteq E \text{ normal}\}.$$

Como **teorema**:

1. Sean $S \subseteq L$ con $L = K(S)$ y $\mathcal{P} := \{\mathrm{Irr}(\alpha, K)\}_{\alpha\in S}$, entonces N es el único cuerpo de descomposición de $\mathcal{P}$ sobre K en $\overline{L}$.

   Sea R el conjunto de raíces en $\overline{L}$ de los polinomios de $\mathcal{P}$, queremos ver que $N = K(R)$. Como $S \subseteq R \subseteq L$, $L = K(S) \subseteq K(R) \subseteq \overline{L}$ y $K \subseteq K(R)$ es normal, se tiene $N \subseteq K(R)$, y como $K \subseteq N$ es normal y cada $\alpha \in L \subseteq N$, todas las raíces de los $\mathrm{Irr}(\alpha, K)$ están en N y por tanto $R \subseteq N$ y $K(R) \subseteq N$.

2. $K \subseteq L$ es finita si y sólo si lo es $K \subseteq N$.

   $\Longrightarrow$] Sea $L =: K(\alpha_1, \ldots, \alpha_n)$ y $S := \{\alpha_1, \ldots, \alpha_n\}$, el conjunto R de raíces de los polinomios $\mathrm{Irr}(\alpha, K)$ con $\alpha \in S$ es finito y, por el punto anterior, $N = K(R)$, luego $K \subseteq N$ es algebraica y finitamente generada y por tanto finita.

   $\Longleftarrow$] $K \subseteq L \subseteq N$.

3. Dos clausuras normales de $K \subseteq L$ en distintas clausuras algebraicas de L son L-isomorfas.

   $L = K(L)$, N es un cuerpo de descomposición de $\{\mathrm{Irr}(\alpha, K)\}_{\alpha\in L}$ sobre K y por tanto sobre L y todos los cuerpos tales son L-isomorfos.

4. Si $K \subseteq L$ es finita, existen $E_1, \ldots, E_r \subseteq \overline{L}$ K-isomorfos a L con $N = E_1 \cdots E_r$.

   Sean $L =: K(\alpha_1, \ldots, \alpha_n)$ y $R = \{\beta_1, \ldots, \beta_r\}$ el conjunto de raíces de los $f_i := \mathrm{Irr}(\alpha_i, K)$ en $\overline{L}$, cada β_j es conjugado con un α_i, luego existe un K-isomorfismo $\sigma_j : K(\alpha_i) \to K(\beta_j)$ con $\sigma_j(\alpha_i) = \beta_j$. Como N es el cuerpo de descomposición de $\{f_1, \ldots, f_n\}$ sobre K, lo es sobre $K(\alpha_i)$ y sobre $K(\beta_j)$, luego σ_j se extiende a un K-automorfismo $\overline{\sigma}_j : N \to N$, con lo que $E_j := \overline{\sigma}_j(L)$ es un subcuerpo de N K-isomorfo a L con $\beta_j = \sigma_j(\alpha_i) = \overline{\sigma}_j(\alpha_i) \in \overline{\sigma}_j(L) = E_j$ y por tanto $N = K(\beta_1, \ldots, \beta_r) = K(\beta_1) \cdots K(\beta_r) \subseteq E_1 \cdots E_r \subseteq N$.

5.3. Extensiones separables

Sea K un cuerpo, $f \in K[X]$ es **separable** si no tiene raíces múltiples en un cuerpo de descomposición de f sobre K. Dada una extensión L de K, $\alpha \in L$ es **separable** sobre K si es algebraico sobre K e $\mathrm{Irr}(\alpha, K)$ es separable. Entonces $K \subseteq L$ es **separable** si cada $\alpha \in L$ es separable sobre K. K es **perfecto** si todo irreducible en $K[X]$ es separable, si y sólo si toda extensión algebraica de K es separable sobre K.

Dado un cuerpo K y un $f \in K[X]$ irreducible:

1. Si $\text{car}K = 0$, f es separable.

   Sea L el cuerpo de descomposición, como $\text{car}K = 0$ y f es irreducible en $K[X]$, f no tiene raíces múltiples en L.

2. Si $p \coloneqq \text{car}K \neq 0$ y $f \in K[X]$ es irreducible, f es no separable si y sólo si $f \in K[X^p]$.

   Para $K \subseteq L$, como f es irreducible en $K[X]$ con alguna raíz en L, f tiene raíces múltiples en L si y solo si $f \in K[X^p]$.

3. Si K es de característica 0, finito o algebraicamente cerrado, K es perfecto.

   Si $\text{car}K = 0$ ya lo hemos visto. Si K es finito y $f \in K[X]$ es irreducible, existe una raíz α de f en un cierto $K(\alpha)$, que es finito y por tanto está formado por las raíces de $X^{|K(\alpha)|} - X$, que no tiene raíces múltiples, pero como $f = \text{Irr}(\alpha, K)$, $f \mid X^{|K(\alpha)|} \mid X$ y f no tiene raíces múltiples. Si K es algebraicamente cerrado, los únicos irreducibles son de la forma $X - a$ y no tienen raíces múltiples.

4. Si $p \coloneqq \text{car}K \neq 0$, K es perfecto si y sólo si todo $a \in K$ tiene una raíz p-ésima en K.

5. Una extensión algebraica de un cuerpo perfecto es perfecta.

Además:

1. No todos los polinomios irreducibles son separables.

   Sean $K \coloneqq \mathbb{Z}_p(T)$ y $f(X) \coloneqq X^p - T \in K[X]$, f es irreducible por Eisenstein al ser T irreducible en $\mathbb{Z}_p[T]$, pero si α es una raíz de f en una extensión de K, entonces $\alpha^p = T$ y, en $K(\alpha)[X]$, $f(X) = X^p - \alpha^p = (X - \alpha)^p$, con lo que α es raíz múltiple.

2. Si $K \subseteq L$ y $K \subseteq F$ son admisibles y $\alpha \in L$ es separable sobre K, lo es sobre F.

   Sean $f \coloneqq \text{Irr}(\alpha, K)$ y $g \coloneqq \text{Irr}(\alpha, F)$, como α es raíz de $f \in F[X]$, $g \mid f$, y como f no tiene raíces múltiples, tampoco las tiene g.

3. Dada la torre $K \subseteq F \subseteq L$, si $K \subseteq L$ es separable, también lo son $K \subseteq F$ y $F \subseteq L$.

   Todo $\alpha \in L$ es separable sobre K y, por lo anterior, sobre F, luego $F \subseteq L$ es separable. Todo $\alpha \in F$ está en L y por tanto es separable sobre K, luego $K \subseteq F$ es separable.

Si $K \subseteq L$ es una extensión normal, separable y finita, $|\text{Gal}(L/K)| = [L : K]$. Si el cuerpo K es perfecto, para $f \in K[X] \setminus K$, G_f es el grupo de Galois de una extensión normal, separable y finita. Dada una extensión $K \subseteq L$ y $S \subseteq L$ con $L = K(S)$, si todo elemento de S es separable sobre K, $K \subseteq L$ es separable.

Como **teorema**, la separabilidad es multiplicativa en torres y estable por levantamientos, y si $K \subseteq L$ es una extensión separable y N es una clausura normal de $K \subseteq L$, entonces $K \subseteq N$ es separable.

Capítulo 6

Teoría de Galois

$$\mathrm{Gal}(K(X)/K) = \left\{ \sigma \,\middle|\, \exists a,b,c,d \in K \mid \left(ad - bc \neq 0 \wedge \sigma(X) = \frac{aX+b}{cX+d} \right) \right\}.$$

6.1. Conexión de Galois

Sean $K \subseteq L$ una extensión de cuerpos, $G \coloneqq \mathrm{Gal}(L/K)$, $\mathcal{F}$ el conjunto de cuerpos intermedios de $K \subseteq L$ y $\mathcal{H}$ el conjunto de subgrupos de G, llamamos **correspondencia** o **conexión de Galois** asociada a $K \subseteq L$ al par $(f : \mathcal{F} \to \mathcal{H}, g : \mathcal{H} \to \mathcal{F})$ dado por

$$f(F) \coloneqq F' \coloneqq \{\sigma \in G \mid \forall \alpha \in F, \sigma(\alpha) = \alpha\} = \mathrm{Gal}(L/F),$$
$$g(H) \coloneqq H' \coloneqq \{\alpha \in L \mid \forall \sigma \in H, \sigma(\alpha) = \alpha\} = \bigcap_{\sigma \in H} \mathrm{Fix}\sigma.$$

En particular, para $\beta \in L$, $K(\beta)' = \{\sigma \in G \mid \sigma(\beta) = \beta\}$, y para $\tau \in G$, $\langle \tau \rangle' = \mathrm{Fix}\tau$.

Propiedades: Sean $K \subseteq L$, $G \coloneqq \mathrm{Gal}(L/K)$, F, F_1, F_2 cuerpos intermedios de $K \subseteq L$ y H, H_1, H_2 subcuerpos de G:

1. $L' = \{1_G\}$, $\{1_G\}' = L$ y $K' = G$, pero en general no es $G' = K$.

   $L' = \mathrm{Gal}(L/L) = 1$, $1' = \mathrm{Fix}1_G = L$ y $K' = \mathrm{Gal}(L/K) = G$, pero si la extensión es $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$, como $\sqrt[3]{2}$ es la única raíz de $X^3 - 2$ en $\mathbb{Q}(\sqrt[3]{2})$, debe ser $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ para todo $\sigma \in G$ y por tanto $G = 1$, y $G' = 1' = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$.

2. $F_1 \subseteq F_2 \implies F_2' \subseteq F_1'$.

3. $H_1 \subseteq H_2 \implies H_2' \subseteq H_1'$.

4. $F \subseteq F''$.

5. $H \subseteq H''$.

6. $F' = F'''$.

   $F' \subseteq (F')''$, y como $F \subseteq F''$, $(F'')' \subseteq F'$.

7. $H' = H'''$.

Sea $K \subseteq L$ una extensión con retículo de cuerpos intermedios $\mathcal{F}$ y $G \coloneqq \mathrm{Gal}(L/K)$ con retículo de subgrupos $\mathcal{H}$, un $F \in \mathcal{F}$ es **cerrado** si $F = F''$, si y sólo si existe $H \in \mathcal{H}$ con $F = H'$, y un $H \in \mathcal{H}$ es **cerrado** si $H = H''$, si y sólo si existe $F \in \mathcal{F}$ con $H = F'$. Así, la conexión de Galois induce biyecciones inversas una de la otra, que invierten las inclusiones, entre el conjunto de cuerpos cerrados en $\mathcal{F}$ y el de subgrupos cerrados en $\mathcal{H}$.

GyA

Dados $H \leq G$, definimos la relación de equivalencia en G

$$a \equiv_i b \bmod H :\iff a^{-1}b \in H;$$

la clase de equivalencia de $a \in G$, llamada **clase lateral módulo H por la izquierda**, es $aH = \{ah\}_{h \in H}$, y llamamos $G/H \coloneqq G/(\equiv_i \bmod H)$. [...] Llamamos **índice** de H en G a $[G : H] \coloneqq |G/H|$.

[...] Si G es un grupo finito y $H \leq G$, $|G| = |H|[G : H]$. [...]

Un subgrupo $N \leq G$ es **normal** si [...] $\forall x \in G, Nx = xN$, [...] escribimos $N \trianglelefteq G$, y si además es propio, escribimos $N \triangleleft G$.

Si $H \leq J \leq G$ son grupos, G/H es un grupo si y sólo si $H \trianglelefteq G$, y $[G : J][J : H] = [G : H]$.
Sean $K \subseteq L$ una extensión con grupo de Galois G:

1. Dada una torre $K \subseteq E \subseteq F \subseteq L$, si $[F : E]$ es finito, $[E' : F'] \leq [F : E]$.

   Hacemos inducción sobre $n \coloneqq [F : E]$. Si $n = 1$, $E = F$ y es trivial. Si $n > 1$, sea $\alpha \in F \setminus E$, entonces $1 < s \coloneqq [E(\alpha) : E] \leq [F : E] = n$, luego $[F : E(\alpha)] = n/s < n$. Si $s < n$, por la hipótesis de inducción, $[E' : F'] = [E' : E(\alpha)'][E(\alpha)' : F'] \leq s \cdot \frac{n}{s} = n$.

   En otro caso, $[F : E(\alpha)] = 1$ y $F = E(\alpha)$, luego $f \coloneqq \mathrm{Irr}(\alpha, E)$ tiene grado n. Sea R el conjunto de raíces de f en L, como cada $\sigma \in E'$ fija los elementos de E y lleva α a un elemento de R, podemos definir $f : E'/F' \to R$ como $f(\sigma F') \coloneqq \sigma(\alpha)$, y esto está bien definido y es inyectivo ya que

   $$\sigma F' = \tau F' \iff \tau^{-1}\sigma \in F' = E(\alpha)' \iff (\tau^{-1}\sigma)(\alpha) = \alpha \iff \sigma(\alpha) = \tau(\alpha),$$

   por ser τ y σ biyectivos, luego $[E' : F'] \leq |R| \leq n = [F : E]$.

2. Si $H \subseteq J$ son subgrupos de G y $[J : H]$ es finito, $[H' : J'] \leq [J : H]$.

Como **teorema**, sean $K \subseteq E \subseteq F \subseteq L$ una torre de extensiones, $G \coloneqq \mathrm{Gal}(L/K)$ y $H \subseteq J$ subgrupos de G:

1. Si E es cerrado y $[F : E]$ es finito, entonces F es cerrado y $[E' : F'] = [F : E]$.

   $[F : E] \geq [E' : F'] \geq [F'' : E''] = [F'' : E] = [F'' : F][F : E] \geq [F : E]$, lo que da la igualdad, y como entonces $[F'' : F] = 1$, $F = F''$ es cerrado.

2. Si H es cerrado y $[J : H]$ es finito, J es cerrado y $[H' : J'] = [J : H]$.

   Análogo.

3. Todo subgrupo finito de G es cerrado.

   Sea J tal subgrupo, como 1 es cerrado $[J : 1]$ es finito, J es cerrado.

6.2. Extensiones de Galois

Una extensión $K \subseteq L$ con grupo de Galois G es **de Galois** si K es cerrado, es decir, si $K = G'$, si y sólo si $G' \subseteq K$, si y sólo si $\forall \alpha \in L, (\forall \sigma \in G, \sigma(\alpha) = \alpha \implies \alpha \in K)$, si y sólo si $\forall \alpha \in L \setminus K, \exists \sigma \in G : \sigma(\alpha) \neq \alpha$. Si $G = \langle \tau \rangle$, $K \subseteq L$ es de Galois si y sólo si $\forall \alpha \in L, (\tau(\alpha) = \alpha \implies \alpha \in K)$, si y sólo si $\forall \alpha \in L \setminus K, \tau(\alpha) \neq \alpha$.

Ejemplos:

1. Las extensiones propias $K \subsetneq L$ con $\mathrm{Gal}(L/K)$ trivial no son de Galois.

   $\mathrm{Gal}(L/K)' = 1' = L \neq K$.

2. $\mathbb{R} \subseteq \mathbb{C}$ es de Galois.

   Si σ es la conjugación, $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle \sigma \rangle$, pero $\sigma(\alpha) = \alpha \implies \alpha \in \mathbb{R}$.

Sea $K \subseteq L$ una extensión y F un cuerpo intermedio cerrado, $F \subseteq L$ es de Galois, pues $F = F'' = \mathrm{Gal}(L/F)'$. En particular $\mathrm{Gal}(L/K)' \subseteq L$ es de Galois, pues $\mathrm{Gal}(L/K)' = \mathrm{Gal}(L/K)'''$.

Como **teorema**, una extensión es algebraica y de Galois si y sólo si es normal y separable.

$\implies$] Sea $K \subseteq L$ la extensión, queremos ver que si un irreducible mónico $f \in K[X]$ tiene una raíz $\alpha \in L$ entonces tiene $n \coloneqq \mathrm{gr} f$ raíces distintas en L. Sean entonces $\alpha = \alpha_1, \ldots, \alpha_r$ las raíces distintas de f en L con $r \leq n$ y $g \coloneqq (X - \alpha_1) \cdots (X - \alpha_r) \in L[X]$, cada $\sigma \in G \coloneqq \mathrm{Gal}(L/K)$ permuta las raíces de f y por tanto $\sigma(g) = g$, luego los coeficientes de g quedan fijos y están en $G' = K$. Por tanto $g \in K[X]$, $f \mid g$ y $n = \mathrm{gr} f \leq \mathrm{gr} g = r$.

$\impliedby$] Como es normal es algebraica, y hay que ver que, para $\alpha \in L \setminus K$, existe $\sigma \in \mathrm{Gal}(L/K)$ con $\sigma(\alpha) \neq \alpha$. Sea $f \coloneqq \mathrm{Irr}(\alpha, K)$, como $\alpha \notin K$, $n \coloneqq \mathrm{gr} f > 1$, pero por la hipótesis, f tiene n raíces distintas en L y en particular tiene una raíz $\beta \neq \alpha$, luego hay un K-isomorfismo $\sigma : K(\alpha) \to K(\beta)$ con $\sigma(\alpha) = \beta$. Como $K \subseteq L$ es normal, L es el cuerpo de descomposición de cierto $\mathcal{P} \subseteq K[X] \setminus 0$ sobre K y por tanto sobre $K(\alpha)$ y $K(\beta)$, por lo que se extiende a un K-automorfismo $\overline{\sigma} : L \to L$ con $\sigma(\alpha) = \beta \neq \alpha$.

Así:

1. «Ser una extensión algebraica de Galois» es estable por levantamientos.
2. Si K es perfecto, $K \subseteq L$ es algebraica y de Galois si y sólo si es normal, y es finita y de Galois si y sólo si L es el cuerpo de descomposición sobre K de un polinomio de $K[X]$.
3. Toda extensión ciclotómica $K \subseteq F$ con $\mathrm{car} K \nmid [F : K]$ es finita y de Galois.
4. Si $K \subseteq L$ es separable con clausura normal N, $K \subseteq N$ es de Galois.

6.3. Teoremas fundamentales

Primer Teorema Fundamental de la Teoría de Galois: Si $K \subseteq L$ es finita y de Galois con grupo de Galois G:

1. $|G| = [L : K]$.

   Como $K \subseteq L$ es finita y K es cerrado, $[L : K] = [K' : L'] = [G : 1] = |G|$.

2. Todos los cuerpos intermedios entre K y L y todos los subgrupos de G son cerrados.

   Sea F un cuerpo intermedio, $K \subseteq F$ es finita por serlo $K \subseteq L$ y K es cerrado, luego F es cerrado. Si $H \leq G$, $[H : 1]$ es finito por serlo $[G : 1]$, luego H es cerrado.

3. Si $X \subseteq Y$ son cuerpos intermedios o subgrupos, $[X' : Y'] = [Y : X]$.

   Por lo anterior, X es cerrado e $[Y : X]$ es finito.

4. La correspondencia de Galois establece biyecciones inversas una de la otra, que invierten las inclusiones, entre el conjunto de cuerpos intermedios de $K \subseteq L$ y el de subgrupos de G.

   Estas se dan entre los cerrados, pero ahora todos son cerrados.

Una extensión finita $K \subseteq L$ es de Galois si y sólo si $|\mathrm{Gal}(L/K)| = [L : K]$.

$\Longrightarrow$] Por el teorema.

$\Longleftarrow$] Sean $G \coloneqq \mathrm{Gal}(L/K)$ y $K_0 \coloneqq G'$, $K_0 \subseteq L$ es finita por serlo $K \subseteq L$, y es de Galois con $\mathrm{Gal}(L/K_0) = K_0' = G$, luego por el teorema es $|G| = [L : K_0]$, pero $|G| = [L : K] = [L : K_0][K_0 : K]$, luego $[K_0 : K] = 1$ y $K = K_0$.

Sean $K \subseteq L_1$ y $K \subseteq L_2$ extensiones finitas y de Galois admisibles, $K \subseteq L_1L_2$ es finita y de Galois y $\varphi : \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ dado por $\varphi(\sigma) \coloneqq (\sigma|_{L_1}, \sigma|_{L_2})$ es un homomorfismo inyectivo de grupos, que es biyectivo si $L_1 \cap L_2 = K$.

Si $K \subseteq L$ tiene grado 2 y $\mathrm{car}K \neq 2$, $\mathrm{Gal}(L/K) \cong C_2$.