Tema 8.-. Extensiones algebraicas. Cuerpos de descomposición. Elemento primitivo.

8.1. Extensiones algebraicas. Grado.

Si k es un subcuerpo de K, diremos que K es una *extensión* de k, que notaremos $K|k$.

Si $K|k$ es una extensión y $E \subset K$ es un subconjunto, escribiremos $k(E)$ para el menor subcuerpo de K que contiene a k y a E. En el caso de un conjunto finito $E = \{\alpha_1, \ldots, \alpha_m\}$, también escribiremos $k(\alpha_1, \ldots, \alpha_m)$ para indicar $k(E)$. En particular, se tiene que $k(\alpha, \beta) = k(\alpha)(\beta)$.

Si $K|k$ es una extensión entonces K es un $k-$espacio vectorial, cuya dimensión se llama *grado* de la extensión y se denota por $[K : k]$. La extensión $K|k$ se dice *finita*, si el grado lo es.

Podemos hacer lo análogo para anillos: si $A \subset A'$ son anillos y $E \subset A'$ es un subconjunto, escribiremos $A[E]$ para el menor subanillo de A' que contiene a A y a E. En particular, si E se reduce a una indeterminada $E = \{X\}$, se obtiene así el clásico anillo de polinomios $A[X]$.

Lema 8.1.1.– Sea $\{u_i\}_{i\in I} \subset L$ conjunto linealmente independiente sobre K, $\{v_j\}_{j\in J} \subset K$ conjunto linealmente sobre k. Entonces $\{u_i v_j\}_{i\in I, j\in J} \subset L$ es un conjunto linealmente independiente sobre k.

Demostración. Consideremos una combinación lineal finita $\sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij} u_i v_j = 0$, con $\alpha_{ij} \in k$. Entonces

$$0 = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} v_j \right) u_i$$

implica, por la independencia lineal de $\{u_i\}$ sobre K, que

$$0 = \sum_{j=1}^{n} \alpha_{ij} v_j.$$

Entonces cada $\alpha_{ij} = 0$ por la independencia lineal de $\{v_j\}$ sobre k. □

Proposición 8.1.2.– Si $L|K$ y $K|k$ son extensiones se tiene que

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

Se sobrentiende que esta igualdad quiere decir que las extensiones dadas son ambas finitas si y sólo si $L|k$ es finita.

Demostración. Si $[L : K] = r$ y $[K : k] = s$ son finitas, con bases respectivas $\{u_1, \ldots, u_r\}, \{v_1, \ldots, v_s\}$, consideremos $a \in L$. Entonces

$$a = \sum_{i=1}^{r} \beta_i u_i, \text{ con } \beta_i \in K.$$

Para cada $i = 1, \ldots, r$, podemos expresar

$$\beta_i = \sum_{j=1}^{s} \alpha_{ij} v_j, \text{ con } \alpha_{ij} \in k.$$

Entonces

$$a = \sum_{i=1}^{r} \sum_{j=1}^{s} \alpha_{ij} u_i v_j$$

por lo que $\{u_i v_j : i = 1, \ldots, r, j = 1, \ldots, s\}$ es un sistema generador de L sobre k. Por el lema anterior, es base y $[L : k] = rs = [L : K][K : k]$. De igual forma, si $[L : K]$ o $[K : k]$ fuera infinito, también lo sería $[L : k]$. □

Corolario 8.1.3.– Si $K_1|K_2|\ldots|K_n$ son extensiones, entonces

$$[K_1 : K_n] = [K_1 : K_2] \cdots [K_{n-1} : K_n]$$

Definición 8.1.4.– Sea $K|k$ una extensión, diremos que un elemento $\alpha \in K$ es *algebraico* sobre k si existe un polinomio $f(X) \in k[X]$ no nulo tal que $f(\alpha) = 0$. A un polinomio mónico de $k[X]$, de grado mínimo entre los que se anulan en α, se le llama *polinomio mínimo* de α sobre k.

Lema 8.1.5.– Sea α algebraico sobre k y $f(X) \in k[X]$ su polinomio mínimo. Entonces

1. Si $g(X) \in k[X]$ es un polinomio tal que $g(\alpha) = 0$ entonces $f(X)$ divide a $g(X)$.
2. $f(X)$ es único e irreducible.

Nota 8.1.6.– Si $f(X) \in k[X]$ es un polinomio mónico e irreducible que se anula en un elemento α, es su polinomio mínimo sobre k.

Proposición 8.1.7.– Sea una extensión $K|k$, $\alpha \in K$ algebraico sobre k, $f(X)$ su polinomio mínimo sobre k, de grado n. Se verifica que:

1. $k[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in k\}$.
2. $k(\alpha)$ es isomorfo a $k[X]/\langle f(X)\rangle$.
3. $k[\alpha] = k(\alpha)$.
4. $[k(\alpha) : k] = n$.

Demostración. Sea $E_0 = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in k\}$. Claramente es un anillo que contiene a k y α. Además, si E_1 es un anillo que contiene a k y α, también contiene todas las potencias $\alpha^i, i = 1, \ldots, n-1$ y contiene entonces a E_0. Por tanto, $E_0 = k[\alpha]$.

Como $f(X)$ es irreducible, el anillo $k[X]/\langle f(X)\rangle$ es un cuerpo. Consideremos el homomorfismo de anillos $\Phi : k[X]/\langle f(X)\rangle \to k[\alpha]$ definido por $\Phi(g(X) + \langle f(X)\rangle) =$

$g(\alpha)$. Es inmediato comprobar que Φ está bien definido y es sobreyectivo. Si $\Phi(g(X) + \langle f(X)\rangle) = 0$ entonces $g(\alpha) = 0$, y por ser $f(X)$ el polinomio mínimo, $f(X)$ divide a $g(X)$. De aquí, Φ es inyectiva, por lo que $k[\alpha]$ es cuerpo. Tenemos entonces que $k(\alpha) = k[\alpha]$.

Los elementos $\{1, \alpha, \ldots, \alpha^{n-1}\}$ son linealmente independientes sobre k, pues n es el grado del polinomio mínimo. Y son un sistema generador por la forma de $k[\alpha]$. Por tanto, $[k[\alpha] : k] = n$. □

Ejemplo 8.1.8.–

1. $\mathbb{Q}[\sqrt{2}]$ es una extensión de grado 2 sobre $\mathbb{Q}$.
2. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es una extensión de grado 4 sobre $\mathbb{Q}$.

El problema básico del Álgebra consiste en resolver ecuaciones polinómicas. En las siguientes líneas veremos que siempre se pueden resolver las ecuaciones "agrandando" convenientemente el cuerpo base.

8.2. Cuerpos de descomposición.

Definición 8.2.1.– Sea $K|k$ una extensión y $f(X) \in k[X]$ no constante. Diremos que K es un *cuerpo de descomposición* de f sobre k si existen $\alpha_1, \ldots, \alpha_n \in K$ tales que

1. $K = k(\alpha_1, \ldots, \alpha_n)$.
2. $f(X) = a \prod_{i=1}^{n} (X - \alpha_i), a \in k$.

Lema 8.2.2.– (*Kronecker*) Dado un polinomio $f(X) \in k[X]$ no constante, existe una extensión de $K|k$ (en el sentido de que K contiene a un cuerpo isomorfo a k), que contiene una raíz de f.

Demostración. Por inducción sobre el grado de $f(X)$. Si $f(X) = f_1(X) \cdots f_r(X)$ con $f_i(X) \in k[X]$ irreducible, entonces basta tomar $K = k[X]/\langle f_1(X)\rangle$. □

Teorema 8.2.3.– Si $f(X) \in k[X]$ entonces existe un cuerpo de descomposición para $f(X)$.

Demostración. Podemos factorizar $f(X) = f_1(X) \cdots f_r(X)$, con $f_i(X) \in k[X]$ irreducibles y grado$(f_i(X) \geq 1$. Si grado$(f_i(X)) = 1$ para todo $i = 1, \ldots, r$, entonces k es el cuerpo de descomposición. Si, por ejemplo, grado$(p_1(X)) > 1$, entonces existe una extensión $K_1|k$ tal que $f_1(X)$ tiene una raíz en K_1. Entonces $f_1(X) = (X - \alpha_1)g_1(X) \in K_1[X]$, y grado$(g_1(X))$ = grado$(f_1(X)) - 1$. Por inducción sobre los grados de los $f_i(X)$ garantizamos la existencia de un cuerpo de descomposición de $g_1(X)f_2(X) \cdots f_r(X)$. Si las raíces de este polinomio son $\alpha_2, \ldots, \alpha_n \in L$, entonces $k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ es un cuerpo de descomposición para $f(X)$. □

NOTA 8.2.4.– Sea $\sigma : k \to k'$ un isomorfismo entre cuerpos. Es muy fácil extender este isomorfismo a uno entre los anillos de polinomios $k[X]$ y $k'[X]$, que seguiremos llamando σ, de modo que el siguiente diagrama es conmutativo

$$\begin{array}{ccc} k[X] & \overset{\sigma}{\dashrightarrow} & k'[X] \\ \uparrow & \sharp & \uparrow \\ k & \xrightarrow{\sigma} & k' \end{array}$$

Concretamente, si $f(X) \in k[X]$, $f = a_0 + a_1X + \ldots + a_nX^n$, $\sigma(f) = \sigma(a_0) + \sigma(a_1)X + \ldots + \sigma(a_n)X^n$. Además, como σ es isomorfismo, conserva el carácter irreducible de los polinomios.

LEMA 8.2.5.– Sea $\sigma : k \to k'$ un isomorfismo, $f(X) \in k[X]$ irreducible, $g = \sigma(f) \in k'[X]$ (ver nota previa). Si α es una raíz de f y β una raíz de g existe un isomorfismo $\tau : k(\alpha) \to k'(\beta)$ tal que $\tau(\alpha) = \beta$ y que extiende a σ, es decir que el siguiente diagrama conmuta

$$\begin{array}{ccc} k(\alpha) & \overset{\tau}{\dashrightarrow} & k'(\beta) \\ \uparrow & \sharp & \uparrow \\ k & \xrightarrow{\sigma} & k' \end{array}$$

Demostración. Existen isomorfismos

$$\Phi_1 : k[X]/\langle f(X)\rangle \to k(\alpha), \Phi_2 : k'[X]/\langle g(X)\rangle \to k'(\beta)$$

tales que $\Phi_1|_k = id, \Phi_2|_{k'} = id$. Si tomamos el homomorfismo $\sigma_1 : k[X]/\langle f(X)\rangle \to k'[X]/\langle g(X)\rangle$ inducido por σ, vemos que es un isomorfismo y basta considerar $\tau = \Phi_2\sigma_1\Phi_1^{-1}$.

□

Como consecuencia se obtiene que las raíces de un polinomio irreducible son indistinguibles, en el sentido del siguiente corolario.

COROLARIO 8.2.6.– Si α y β son raíces de un polinomio irreducible $f \in k[X]$, existe un isomorfismo σ entre $k(\alpha)$ y $k(\beta)$, que deja invariante los elementos de k y $\sigma(\alpha) = \beta$.

LEMA 8.2.7.– Sea $\sigma : k \to k'$ un isomorfismo, $f(X) \in k[X]$ no constante, $g = \sigma(f) \in k'[X]$ (ver nota previa). Sean $K|k$ y $K'|k'$ cuerpos de descomposición de f y g respectivamente. Existe un isomorfismo $\tau : K \to K'$ tal que $\tau_{|k} = \sigma$, que lleva raíces de f en raíces de g.

Demostración. Sean $\alpha_1, \ldots, \alpha_n \in K$ raíces de $f(X)$ con

$$f(X) = a_0(X - \alpha_1)\cdots(X - \alpha_n) \in K[X].$$

Si cada $\alpha_i \in k$, entonces $K = k$ y en

$$g(X) = \sigma(f(X)) = \sigma(a)(X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_n)) \in K'[X]$$

ocurre lo mismo, luego $K' = k'$. En este caso, $\tau = \sigma$ nos vale.

Supongamos que hemos probado el resultado para todos los polinomios que tienen menos de m raíces ($m \geq 1$) fuera de k. El caso $m = 0$ ya lo hemos tratado. Supongamos que $f(X)$ tiene m raíces fuera de k. Descomponemos $f(X)$ en factores irreducibles

$$f(X) = p_1(X) \cdots p_r(X) \in K[X]$$

y podemos suponer, por ejemplo, que grado$(p_1(X)) > 1$. Si $q_j(X) = \sigma(p_j(X))$ entonces $q_j(X)$ es irreducible en $k'[X]$ y

$$g(X) = q_1(X) \cdots q_r(X).$$

Sea α una raíz de $p_1(X)$. Entonces $k \subset k(\alpha) \subset K$. De igual forma, si β es raíz de $q_1(X)$ tenemos $k' \subset k'(\beta) \subset K'$. Sabemos que existe un isomorfismo

$$\tau_1 : k(\alpha) \to k'(\beta) \text{ tal que } \tau_1(a) = \sigma(a) \text{ si } a \in k.$$

Entonces $f(X) \in k(\alpha)[X]$ es un polinomio que tiene menos de $m - 1$ raíces fuera de $k(\alpha)$, y su cuerpo de descomposición es K. Aplicamos inducción a $\tau_1 : k(\alpha) \to k'(\beta)$ y tenemos el resultado. □

Corolario 8.2.8.– Si $f(X) \in k[X]$ tiene dos cuerpos de descomposición $K_1|k, K_2|k$ entonces existe un isomorfismo $\tau : K_1 \to K_2$ tal que $\tau_{|k} = id$.

Demostración. Basta tomar $id : k \to k$ en el teorema anterior. □

8.3. Elemento primitivo.

Sea k un cuerpo que contiene a $\mathbb{Q}$, el cuerpo de los números racionales. Lema 8.3.1.– Si $f(X) \in k[X]$ es irreducible, entonces no tiene raíces múltiples en ninguna extensión de k.

Demostración. Podemos suponer $f(X)$ mónico. Supongamos que α es raíz múltiple de $f(X)$. Entonces α también es raíz de su derivada. Como $f(X)$ es irreducible, es polinomio mínimo de α sobre k. Entonces $f(X)$ divide a $f'(X)$. Como la derivada tiene grado estrictamente menor, solamente puede ocurrir que $f'(X) = 0$, pues $f'(X) = nX^{n-1} + \ldots$ y $n \neq 0$ en k. □

Teorema 8.3.2.– Si K es una extensión finita de k entonces existe $\alpha \in K$ tal que $K = k(\alpha)$, esto es, la extensión es simple. Decimos que α es un elemento primitivo de la extensión.

Demostración. Existe $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ tales que $K = k(\alpha_1, \ldots, \alpha_n)$. Veremos en primer lugar que existe $\lambda_2 \in K$ tal que $k(\alpha_1, \alpha_2) = k(\alpha_1 + \lambda_2\alpha_2)$. Entonces, por inducción, tendremos que $K = k(\alpha_1 + \lambda_2\alpha_2 + \ldots + \lambda_n\alpha_n)$.

Sean $f_1(X), f_2(X) \in k[X]$ los polinomios mínimos de α_1, α_2 respectivamente. Existe una extensión K' de k tal que $f_2(X)$ se descompone en factores lineales

$$f_2(X) = (X - \beta_1) \ldots (X - \beta_r)$$

en K' y $\beta_i \neq \beta_j$ para $i \neq j$, por el lema anterior. Tomemos $\alpha_2 = \beta_1$.

Consideremos el conjunto finito

$$\mathcal{S} = \{\frac{b_1 - \alpha_1}{\alpha_2 - b_2} : b_1, b_2 \in K', f_1(b_1) = 0, f_2(b_2) = 0, b_2 \neq \alpha_2\}.$$

Observemos que cada f_i tiene un número finito de raíces en K'. Como $\mathbb{Q} \subset k$, podemos elegir $\lambda \in k - \mathcal{S}$. Sea $\alpha = \alpha_1 + \lambda\alpha_2 \in k(\alpha_1, \alpha_2)$. Vamos a probar que $k(\alpha) = k(\alpha_1, \alpha_2)$, para lo que basta ver que $\alpha_2 \in k(\alpha)$.

Consideremos el polinomio

$$h(X) = f_1(\alpha - \lambda X) \in k(\alpha)[X].$$

Tenemos que $h(\alpha_2) = f_1(\alpha_1) = 0$, luego $X - \alpha_2$ divide a $h(X)$ en K'. Sea ahora b_2 raíz de $f_2(X)$ en K', $b_2 \neq \alpha_2$. Entonces $h(b_2) \neq 0$ pues, en otro caso,

$$0 = h(b_2) = f_1(\alpha - \lambda b_2)$$

y $b_1 = \alpha - \lambda b_2 = \alpha_1 + \lambda(\alpha_2 - b_2)$ sería raíz de $f_1(X)$, con lo que

$$\lambda = \frac{b_1 - \alpha_1}{\alpha_2 - b_2}, b_2 \neq \alpha_2,$$

contra la elección de λ.

Por tanto, $h(X)$ no comparte con $f_2(X)$ ninguna raíz en K', salvo α_2. Sea $g(X) = \text{mcd}(h(X), f_2(X))$ en $k(\alpha)[X]$, que podemos tomar mónico. El polinomio $g(X)$ no puede ser 1, porque $h(X)$ y $f_2(X)$ tienen una raíz común.

En $k(\alpha)[X]$ $g(X)$ divide a $f_2(X)$. Por la factorización de $f_2(X)$ tendremos que

$$g(X) = (X - \beta_{i_1}) \cdots (X - \beta_{i_s}), i_k \neq i_l.$$

Pero $f_2(X)$ y $h(X)$ no comparten más raíz que α_2, por lo que $g(X)$ tiene que ser igual a $X - \alpha_2$. Como $g(X) \in k(\alpha)[X]$ tenemos que $\alpha_2 \in k(\alpha)$, como queríamos probar. $\square$