Tema 3.- Cuerpos de descomposición. Clausura algebraica.

3.1 Cuerpos de descomposición.

DEFINICIÓN 3.1.1.– Dados k un cuerpo y L una extensión de K, diremos que $f \in k[X]$ *factoriza sobre* L si $f = \lambda(X-\alpha_1)\cdots(X-\alpha_n)$ con $\lambda \in k,\ \alpha_i \in L$. Si además no existe un subcuerpo propio L' de L conteniendo k tal que f factorice sobre L', diremos que L es un *cuerpo de descomposición para f (sobre k).*

PROPOSICIÓN 3.1.2.– Supongamos que $L : k$ es una extensión tal que $f \in k[X]$ factoriza sobre L

$$f = \lambda(X-\alpha_1)\cdots(X-\alpha_n)$$

con $\lambda \in k,\ \alpha_i \in L$. Entonces $k(\alpha_1,\dots,\alpha_n)$ es un cuerpo de descomposición para f. En particular, un cuerpo de descomposición es una extensión finita.

Recordemos que una extensión $L : k$ es *simple* si $L = k(\alpha)$ para algún $\alpha \in L$.

PROPOSICIÓN 3.1.3.– Sea $f \in k[X]$ irreducible de grado n. Existe una extensión simple de grado n, $k(\alpha) : k$ de grado n y $f(\alpha) = 0$.

PROPOSICIÓN 3.1.4.– Existe un cuerpo de descomposición L para $f \in k[X]$ con $[L : k] \leq n$.

`La idea de prueba (Milne 2.4., pág. 13) es tomar para` $f \in k[X]$ `el cuerpo` $k_1 = k[X]/g_1(X) = k[\alpha_1],\ \alpha_1 = X + (g_1)$ `donde` g_1 `es un factor irreducible de` f. `Se continúa con` $f_1 = f/(X-\alpha_1) \in k_1[X]$.

EJEMPLO 3.1.5.– Sea $f(X) = aX^2 + bX^2 + c \in \mathbb{Q}[X]$. El cuerpo $\mathbb{Q}[\sqrt{b^2-4ac}]$ es un cuerpo de descomposición para f.

EJEMPLO 3.1.6.– Sea $f = (X^p-1)/(X-1) \in k[X]$ con k un cuerpo cualquiera. Todo cuerpo generado por una raíz de f es un cuerpo de descomposición de f.

EJEMPLO 3.1.7.– Sea $f(X) = X^p - X - a \in \mathbb{F}_p[X]$. Todo cuerpo generado por una raíz de f es un cuerpo de descomposición de f.

Los resultados que siguen son necesarios para probar la unicidad del cuerpo de descomposición:

PROPOSICIÓN 3.1.8.– Sea $k(\alpha)$ una extensión simple de un cuerpo k, Ω y $\varphi_0 : k \longrightarrow \Omega$ un homomorfismo en otro cuerpo Ω.

1. Si α es trascendente sobre k, la aplicación $\varphi \mapsto \varphi(\alpha)$ define una biyección entre los conjuntos

   $$\{\text{extensiones de } \varphi_0,\ \varphi : k(\alpha) \longrightarrow \Omega\} \leftrightarrow \{\text{elem. de } \Omega \text{ trasc. sobre } \varphi_0(k)\}.$$

2. Si α es algebraico sobre k con polinomio mínimo $f(X)$, la aplicación $\varphi \mapsto \varphi(\alpha)$ define una biyección entre los conjuntos

   $$\{\text{extensiones de } \varphi_0,\ \varphi : k(\alpha) \longrightarrow \Omega\} \leftrightarrow \{\text{raíces distintas en } \ \Omega \text{ de } \varphi_0(f)(X)\}.$$

Corolario 3.1.9.– Sean $k(\alpha) : k, k'(\alpha') : k'$ dos extensiones simples con α, α' algebraicos. Sea $i : k \longrightarrow k'$ un isomorfismo. Entonces existe un isomorfismo $j : k(\alpha) \longrightarrow k'(\alpha')$ tal que $j(\alpha) = \alpha'$ y $j|_k = i$ si y sólo si $i(m_\alpha) = m_{\alpha'}$.

Proposición 3.1.10.– Sea $f \in k[X]$, E un cuerpo de descomposición para f y $\Omega \subset k$ otro cuerpo donde f factoriza.

1. Existe al menos un k-homomorfismo $\varphi : E \longrightarrow \Omega$.

2. El número de k-homomorfismos de $E \to \Omega$ es $\leq [E : k]$ y se tiene la igualdad si f tiene $grad(f)$ raíces distintas.

3. Si Ω es otro cuerpo de descomposición, entonces todos los k-homomorfismos son isomorfismos. En particular dos cuerpos de descomposición son k-isomorfos.

Nota: El recíproco de la primera parte es también cierto: si existe el k-homomorfismo f factoriza en Ω.

Una consecuencia interesante de la proposición anterior es la siguiente:
Corolario 3.1.11.– Sea $f \in k[X]$ irreducible, $\Sigma : k$ un cuerpo de descomposición y α, β raíces de f en Σ. Existe un automorfismo σ de Σ tal que $\sigma(\alpha) = \beta$ y k queda fijo.

3.2 Clausura algebraica.

Definición 3.2.1.– Un cuerpo L es *algebraicamente cerrado* si todo polinomio $f \in L[X]$ se descompone sobre L.

Definición 3.2.2.– Una extensión $L : k$ es una *clausura algebraica* si es algebraica y L es algebraicamente cerrado.

Nótese que $\mathbb{C} : \mathbb{Q}$ no es una clausura algebraica. En la siguiente proposición se dan dos caracterizaciones:
Proposición 3.2.3.– Supongamos que $L : k$ es una extensión. Son equivalentes:

1. $L : k$ es una clausura algebraica.

2. $L : k$ es algebraica y todo polinomio irreducible en $k[X]$ factoriza sobre L.

3. $L : k$ es algebraica y si $L' : L$ es algebraica entonces $L = L'$.

Corolario 3.2.4.– Sea $L : k$ una extensión con L algebraicamente cerrado. Sea

$$L_\alpha = \{\alpha \in L \mid \alpha \text{ algebraico sobre } k\}.$$

L_α es una clausura algebraica de k.

Teorema 3.2.5.– Todo cuerpo tiene una clausura algebraica.

`Proponemos la prueba que usa el Lema de Zorn. Milne 2.12., pág. 16.`

Concluimos este capítulo con un resultado sobre la unicidad de la clausura algebraica.

Teorema 3.2.6.– Sea Ω una clausura algebraica de k y E una extensión algebraica de k. Existe un k-homomorfismo de E en Ω. Si E es también una clausura algebraica, entonces cualquier k-homomorfismo es un isomorfismo.