Unicidad de campos de descomposición

Facultad de Ciencias UNAM

Introducción

En esta sección veremos que cualesquiera dos campos de descomposición de un polinomio fijo son isomorfos. Esto nos permite hablar de "*el* campo de descomposición de $f(x)$ sobre F" en vez de "*un* campo de descomposición de $f(x)$ sobre F".

Unicidad de los campos de descomposición

Teorema 1

Supongamos que F, F' son campos, que $\phi : F \to F'$ es un isomorfismo de campos, que $\Phi : F[x] \to F'[x]$ es el isomorfismo entre anillos de polinomios inducido por ϕ, que $f(x) \in F[x]$, y que $f'(x) := \Phi(f(x))$.

Si E es un campo de descomposición de $f(x)$ sobre F y E' es un campo de descomposición de $f'(x)$ sobre F', entonces existe un isomorfismo $\sigma : E \to E'$ que extiende a ϕ.

En otras palabras, tenemos el siguiente diagrama conmutativo donde las flechas horizontales son isomorfismos y las flechas verticales son inclusiones.

$$\begin{tikzcd} E \arrow[r, "\sigma"] & E' \\ F \arrow[u, hook] \arrow[r, "\phi"] & F' \arrow[u, hook] \end{tikzcd}$$

Demostración. Supongamos que E es un campo de descomposición de $f(x)$ sobre F y que E' es un campo de descomposición de $f'(x)$ sobre F'. Procedemos por inducción sobre el grado del polinomio.

Paso base. Si $\deg f(x) = 1$, entonces (como ya vimos anteriormente) $E = F$. Por otro lado, $\deg f(x) = 1$ también implica $\deg f'(x) = 1$, de donde también tenemos $E' = F'$. Por lo tanto, $\sigma = \phi$ obviamente cumple lo deseado.

Paso inductivo. Sea $n > 1$. La hipótesis inductiva es la siguiente:

> *Supongamos que A, A' son campos, que $\psi : A \to A'$ es un isomorfismo de campos, que $\Psi : A[x] \to A'[x]$ es el isomorfismo entre anillos de polinomios inducido por ψ, que $a(x) \in A[x]$, y que $a'(x) \coloneqq \Psi(a(x))$. Si $\deg a(x) \leq n-1$, B es un campo de descomposición de $a(x)$ sobre A, y B' es un campo de descomposición de $a'(x)$ sobre A', entonces existe un isomorfismo $\theta : B \to B'$ que extiende a ψ.*

Ahora si, supongamos que $f(x) \in F[x]$ y $n = \deg f(x)$.

Recordemos que $F[x]$ es un DFU[1] y como $f(x)$ no es invertible[2], entonces podemos factorizar a $f(x)$ en irreducibles.

Caso 1. Todos los factores irreducibles de $f(x)$ tienen grado 1.

Claramente, en este caso $E = F$. Mas aun, como los isomorfismos preservan las factorizaciones en irreducibles (c.f. proposición 1.20.8) en este caso también tenemos que todos los factores irreducibles de $f'(x)$ tienen grado 1 y en particular $E' = F$. Por lo tanto (como $E = F$ y $E' = F'$), $\sigma = \phi$ cumple lo deseado.

Caso 2. No todos los factores irreducibles de $f(x)$ tienen grado 1.

Entonces debe existir un factor irreducible de $f(x)$ con grado ≥ 2, llamémoslo $p(x)$ y también denotemos $p'(x) = \Phi(p(x))$. De nuevo, como los isomorfismos preservan las factorizaciones en irreducibles $p'(x)$ es un factor irreducible de $f'(x)$ con grado ≥ 2.

---

[1] Pues F es campo.

[2] Pues $\deg f(x) = n > 1$.

Ahora bien, supongamos que α es una raíz de $p(x)$ y α' es una raíz de $p'(x)$. Recordemos que en el teorema 2.5.4 vimos que las hipótesis

- $\phi : F \to F'$ es un isomorfismo,
- $p(x) \in F[x]$ es irreducible en $F[x]$,
- $p'(x) \coloneqq \Phi(p(x))$,
- α es raíz de $p(x) \in F[x]$, y
- α' es raíz de $p'(x) \in F'[x]$

implican que existe un isomorfismo $\xi : F(\alpha) \to F'(\alpha')$ que extiende a ϕ. En otras palabras, tenemos el siguiente diagrama conmutativo donde las flechas horizontales son isomorfismos y las flechas verticales son inclusiones.

$$
\begin{tikzcd}
F(\alpha) \arrow[r, "\xi"] & F'(\alpha') \\
F \arrow[u, hook] \arrow[r, "\phi"] & F' \arrow[u, hook]
\end{tikzcd}
\tag{1}
$$

Por otro lado, como α es una raíz de $f(x)$ en $F(\alpha)$, y α' es una raíz de $f'(x)$ en $F'(\alpha')$, entonces $(x-\alpha)$ divide a $f(x)$ en $F(\alpha)[x]$ y $(x-\alpha')$ divide a $f'(x)$ en $F'(\alpha')[x]$. Equivalentemente, existen $g(x) \in F(\alpha)[x]$ y $g'(x) \in F'(\alpha')[x]$ tales que

$$f(x) = (x-\alpha)g(x) \quad \text{y} \quad f'(x) = (x-\alpha')g'(x).$$

Como $\deg f(x) = n = \deg f'(x)$ y $\deg(x-\alpha) = 1 = \deg(x-\alpha')$, las ecuaciones anteriores implican que $\deg g(x) = n-1$ y $\deg g'(x) = n-1$.

Ya casi estamos en condiciones de ocupar la hipótesis de inducción. Para esto, veamos que E es un campo de descomposición de $g(x)$ sobre $F(\alpha)$ y que E' es un campo de descomposición de $g'(x)$ sobre $F'(\alpha')$.

Antes que nada, notemos que esto tiene sentido porque $F(\alpha) \subset E$; en efecto, $F \subset E$ y $\alpha \in E$ (pues α también es raíz de $f(x)$). Analogamente, $F'(\alpha') \subset E'$. Ahora si, verifiquemos las dos condiciones de campo de descomposición. Empecemos con $E/F(\alpha)$.

1. *$g(x)$ se descompone en $E/F(\alpha)$:*

   Como E es campo de descomposición de $f(x)$ sobre F, entonces

   $$f(x) = c \cdot (x - \alpha)(x - \alpha_1) \cdots (x - \alpha_n) \tag{2}$$

   con $c \in F$ y $\alpha_1, \ldots, \alpha_n \in F$ (recordemos que α es raíz de $p(x)$ y por lo tanto también de $f(x)$). Por otro lado, recordemos que

   $$f(x) = (x - \alpha)g(x) \tag{3}$$

   Usando (2), (3), y el hecho de que $F[x]$ es un DFU, obtenemos que

   $$g(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

2. *No existe L campo tal que $F(\alpha) \subset L \subsetneq E$ y $g(x)$ se descompone en $L/F(\alpha)$:*

   Supongamos lo contrario. Como $f(x) = (x - \alpha)g(x)$, esto implicaría que $f(x)$ se descompone en L. El lector podrá fácilmente verificar que esto contradice el hecho de que E es campo de descomposición de $f(x)$ sobre F (específicamente, se contradice la segunda condición de la definición de campo de descomposición).

Por lo tanto, E es campo de descomposición de $g(x)$ sobre $F(\alpha)$ y análogamente, E' es un campo de descomposición de $f'(x)$ sobre $F'(\alpha')$.

Ahora si, estamos en condiciones de aplicar la hipótesis de inducción. Recordemos que esta dice lo siguiente:

> *Supongamos que A, A' son campos, que $\psi : A \to A'$ es un isomorfismo de campos, que $\Psi : A[x] \to A'[x]$ es el isomorfismo entre anillos de polinomios inducido por ψ, que $a(x) \in A[x]$, y que $a'(x) \coloneqq \Psi(a(x))$. Si $\deg a(x) \leq n-1$, B es un campo de descomposición de $a(x)$ sobre A, y B' es un campo de descomposición de $a'(x)$ sobre A', entonces existe un isomorfismo $\theta : B \to B'$ que extiende a ψ.*

Entonces por hipótesis de inducción[3], existe un isomorfismo $\theta : E \to E'$ que extiende a $\xi : F(\alpha) \to F'(\alpha')$. En otras palabras, tenemos el siguiente diagrama conmutativo donde las flechas horizontales son isomorfismos y las flechas verticales son inclusiones.

$$\begin{tikzcd} E \arrow[r, "\theta"] & E' \\ F(\alpha) \arrow[u, hook] \arrow[r, "\xi"] & F'(\alpha)' \arrow[u, hook] \end{tikzcd} \tag{4}$$

[3]Con $A = F(\alpha)$, $A' = F'(\alpha')$, $\psi = \xi$, $a(x) = g(x)$, $a'(x) = g'(x)$, $B = E$, y $B' = E'$.

Por supuesto, definiendo $\sigma := \theta$ y juntando los diagramas (1) y (4) obtenemos lo deseado. Específicamente, tenemos el siguiente diagrama conmutativo donde las flechas horizontales son isomorfismos y las flechas verticales son inclusiones.

$$\begin{tikzcd} E \arrow[r, "\sigma"] & E' \\ F(\alpha) \arrow[r, "\xi"] \arrow[u, hook] & F'(\alpha)' \arrow[u, hook] \\ F \arrow[r, "\phi"] \arrow[u, hook] & F' \arrow[u, hook] \end{tikzcd}$$

$\square$

Repitiendo lo que dijimos en la introducción, notemos que este teorema nos permite decir "*el* campo de descomposición de $f(x)$ sobre F" en vez de "*un* campo de descomposición de $f(x)$ sobre F". De ahora en adelante, (cuando sea conveniente) adoptamos esta convención.

El grado de el campo de descomposición es menor o igual al factorial del grado del polinomio

Corolario 2

Supongamos que F es un campo, que $f(x) \in F[x]$, y que $n = \deg f(x) \geq 1$. Si K es el campo de descomposición de $f(x)$ sobre F, entonces

$$[K : F] \leq \deg f(x)!$$

Demostración. Por la proposición 2.9.1 sabemos que existe una extensión E de F en donde $f(x)$ se descompone en E/F. En particular, E contiene todas las raíces de $f(x)$, llamémoslas $\alpha_1, \ldots, \alpha_n \in E$.

Mas aun, por la proposición 2.9.2 ya sabemos que $F(\alpha_1, \ldots, \alpha_n) \subset E$ es un campo de descomposición de $f(x)$ sobre F y por el teorema anterior, $F(\alpha_1, \ldots, \alpha_n) \cong K$.

Antes de continuar, recordemos que en el corolario 2.6.4 vimos que para toda extensión de campos E/L y toda $\beta \in E$ algebraica sobre L tenemos que

$$[L(\beta) : L] \leq \deg p(x) \text{ para todo } p(x) \in L[x] \text{ con } p(\beta) = 0. \tag{5}$$

Ahora si, sigamos con la demostración. Primero notemos que

$$\begin{aligned}[K : F] &= [F(\alpha_1, \dots, \alpha_n) : F] \\ &= \Big[\big(F(\alpha_1, \dots, \alpha_{n-1})\big)(\alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})\Big] \cdot \\ &\qquad \Big[\big(F(\alpha_1, \dots, \alpha_{n-2})\big)(\alpha_{n-1}) : F(\alpha_1, \dots, \alpha_{n-2})\Big] \cdots \\ &\qquad\quad \Big[\big(F(\alpha_1)\big)(\alpha_2) : F(\alpha_1)\Big] \cdot [F(\alpha_1) : F].\end{aligned} \tag{6}$$

Por otro lado, notemos que por (5) tenemos que

$$[F(\alpha_1) : F] \leq \deg f(x) = n.$$

Por otro lado, como α_1 es una raíz de $f(x)$ en $F(\alpha_1)$, entonces (por el recordatorio 1)

$$f(x) = (x - \alpha_1)g_1(x)$$

para algún polinomio $g_1(x) \in F(\alpha_1)(x)$. Mas aun, la ecuación anterior claramente implica que $\deg g(x) = n - 1$ y que α_2 es raíz de $g(x)$. Entonces por (5) tenemos que

$$\Big[\big(F(\alpha_1)\big)(\alpha_2) : F(\alpha_1)\Big] \leq \deg g_1(x) = n - 1.$$

Continuando de esta manera y sustituyendo cada una de estas desigualdades en (6), obtenemos lo deseado. $\square$

El campo de descomposición de un producto es el producto de los campos de descomposición

Lema 3

Supongamos que F es un campo, que $f(x), g(x) \in F[x]$, y que K es el campo de descomposición de $f(x)g(x)$. Entonces K contiene a un campo de descomposición de $f(x)$ sobre F y a un campo de descomposición de $g(x)$ sobre F. Si los denotamos por K_1 y K_2 respectivamente, entonces $K_1K_2 = K$.

Demostración. Usando la definición de producto de subcampos, el lector podrá fácilmente verificar que $f(x)g(x)$ se descompone en K_1K_2/K. Pero como (i) K_1K_2 esta contenido en K y (ii) K es campo de descomposición de $f(x)g(x)$, entonces $K_1K_2 = K$. □