F-Isomorfismos

Recordemos que todo morfismo de anillos $F \longrightarrow R$ con F campo, es inyectivo ya que F no tiene ideales propios distintos de cero.

Def: Decimos que dos extensiones de campos $F_1 \subseteq E_1$ y $F_2 \subseteq E_2$ son isomorfas si hay un isomorfismo $\theta : E_1 \to E_2$ tal que $\theta(F_1) = F_2$.

Es claro que E_2 es algebraica, simple o tiene grado finito sobre F_2 si y solo si E_1 es algebraica, simple o tiene grado finito sobre F_1. De hecho, si las extensiones son isomorfas $[E_2 : F_2] = [E_1 : F_1]$.

Ahora supongamos que tenemos un isomorfismo $\varphi : F_1 \to F_2$. y extensiones $E_1 \supseteq F_1$ y $E_2 \supseteq F_2$. Queremos un isomorfismo

$$
\begin{tikzcd}
E_1 \arrow[r, "\theta", "\cong"'] \arrow[d, dash] & E_2 \arrow[d, dash] \\
F_1 \arrow[r, "\theta|", "\cong"'] & F_2
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
E_1 \arrow[r, dashed, "\theta"] \arrow[d, dash] & E_2 \arrow[d, dash] \\
F_1 \arrow[r, "\varphi", "\cong"'] & F_2
\end{tikzcd}
$$

$\theta : E_1 \to E_2$ que además $\theta(a) = \varphi(a)$ $\forall a \in F_1$

En tal caso de que exista θ, decimos que las extensiones son isomorfas respecto a φ.

Un caso particular que usaremos es cuando $\varphi = Id_F$, es decir, dadas dos extensiones de un campo F, $F \leq E_1$ y $F \leq E_2$ queremos encontrar un isomorfismo $\theta: E_1 \to E_2$ que fije a F

$$\begin{tikzcd}
E_1 \arrow[rr, dashed, "\theta"] \arrow[dr, no head] & & E_2 \arrow[dl, no head] \\
& F &
\end{tikzcd}$$

$\theta(a) = a \quad \forall a \in F$

$\theta: {}_F E_1 \to {}_F E_2$ es una transformacion lineal.

En este caso decimos que θ es un <u>F-isomorfismo</u> y que las extensiones son <u>F-isomorfas</u>

Notemos que si $\varphi: F_1 \to F_2$ es un isomorfismo, entonces φ induce un isomorfismo de anillos $\hat{\varphi}: F_1[x] \to F_2[x]$, donde $\hat{\varphi}(f)$ es aplicar φ a los coeficientes de $f(x)$. (

(Usualmente vamos a suprimir los parentesis en $\hat{\varphi}(f)$ y escribiremos $\hat{\varphi}f$)

Lema: Sean $F_1 \subseteq E_1$ y $F_2 \subseteq E_2$ extensiones de campos y sea $\varphi: F_1 \to F_2$ un isomorfismo. Sea $\alpha_i \in E_i$ y $f_i \in F_i[x]$ con $f_i(\alpha_i) = 0$. Supongamo que $\hat{\varphi}f_1 = f_2$ y que $f_1(x)$ es irreducible en $F_1[x]$. Entonces φ se extiende a un isomorfismo $\theta: F_1[\alpha_1] \to F_2[\alpha_2]$ tal que $\theta(\alpha_1) = \alpha_2$.

Dem:

Cada elemento de $F_1[\alpha_1]$ es de la forma $g(\alpha_1)$ para algún $g(x) \in F_1[x]$. Como $g(x) \in F_1[x]$, $\hat{\varphi}g \in F_2[x]$. Definimos $\theta: F_1[\alpha_1] \longrightarrow F_2[\alpha_2]$ como $g(\alpha_1) = \hat{\varphi}g(\alpha_2)$.

Tenemos que ver que θ esta bien definida, es decir, si $h(x) \in F_1[X]$ es otro polinomio tal que $h(\alpha_1) = g(\alpha_1)$, entonces $\hat{\varphi}h(\alpha_2) = \hat{\varphi}g(\alpha_2)$.

Si $h(\alpha_1) = g(\alpha_1)$, entonces $(h-g)(\alpha_1) = 0$.

Como $f_1(\alpha_1) = 0$ y f_1 es irreducible, $f_1 \mid h-g$. Aplicando $\hat{\varphi}$, se tiene que $\hat{\varphi}f_1 = f_2 \mid \hat{\varphi}h - \hat{\varphi}g$. Por lo tanto $(\hat{\varphi}h - \hat{\varphi}g)(\alpha_2)$ i.e., $\hat{\varphi}h(\alpha_2) = \hat{\varphi}g(\alpha_2)$. $\therefore$ θ está bien definida

Es facil ver que θ es un morfismo de anillos y que ademas es supreyectiva ya que $\hat{\varphi}: F_1[X] \longrightarrow F_2[X]$ es sobre. Si $h(\alpha_2) \in F[\alpha_2]$ con $h \in F_2[x]$, existe un $g \in F_1[X]$ tal que $\hat{\varphi} g = h$. $\therefore$ $\theta(g(\alpha_1)) = h(\alpha_2)$. $\therefore$ θ es un isomorfismo.

Sea $a \in F_1$. Al elemento a lo puedo ver como $g(\alpha_1) \in F_1[\alpha_1]$ con $g(X) = a$. Así

$$\theta(a) = \theta(g(\alpha_1)) = \hat{\varphi} g(\alpha_2) = \varphi(a)$$

Tenemos $\alpha_1 = g(\alpha_1) \in F[\alpha_1]$ con $g(x) = x$.

Entonces

$$\theta(\alpha_1) = \theta(g(\alpha_1)) = \hat{\varphi} g(\alpha_2) = \alpha_2$$

Cor. Sean $F\subseteq E_1$ y $F\subseteq E_2$ extensiones de campos y $f\in F[x]$ irreducible. Sup. que $\alpha_i\in E_i$ es tal que $f(\alpha_i)=0$. Entonces $F[\alpha_1]$ y $F[\alpha_2]$ son F-isomorfas via un isomorfismo que lleva a α_1 en α_2.

Ejemplo: Considere los números $\sqrt[4]{2}, i\sqrt[4]{2}\in\mathbb{C}$. Estos numeros son raices del polinomio $x^4-2\in\mathbb{Q}[x]$ que es irreducible sobre $\mathbb{Q}$. Por lo tanto las extensiones $\mathbb{Q}[\sqrt[4]{2}] \xrightarrow{\cong} \mathbb{Q}[i\sqrt[4]{2}]$ son isomorfas

$$\begin{tikzcd}
\mathbb{Q}[\sqrt[4]{2}] \arrow[rr, "\cong"] & & \mathbb{Q}[i\sqrt[4]{2}] \\
& \mathbb{Q} \arrow[ul, dash, "4"] \arrow[ur, dash, "4"'] &
\end{tikzcd}$$

Def: Un polinomio $f(x)\in F[x]$ se dice que **se escinde** si cada divisor irreducible de f tiene grado 1. (En particular los polinomios constantes son separables). En otras palabras, $f(x)$ es separable si tiene la forma

$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ con a y $\alpha_i \in F$.

Notemos que a es el coeficiente de grado de $f(x)$ y $n = gr(f)$.

Por ejemplo: El polinomio $X^4 - 1 \in \mathbb{Q}[x]$ no se escinde.

$$(X^4-1) = ((X^2)^2 - 1) = (X^2-1)(X^2+1)$$
$$= (X+1)(X-1)(X^2+1) \in \mathbb{Q}[x].$$

Sin embargo $X^4 - 1 \in \mathbb{C}[x]$ sí se escinde, ya que

$$X^4 - 1 = (X+1)(X-1)(X-i)(X+i) \text{ sobre } \mathbb{C}$$

Todo polinomio se escinde sobre $\mathbb{C}$.

Lema: Sea $f(x) \in F[X]$ irreducible. Entonces existe un campo $E \supseteq F$ tal q que f tiene una raiz en E.

Dem:

Sabemos que si encontramos una extension $E \supseteq F$ y $\alpha \in E$ con $f(\alpha)=0$ entonces $F[\alpha] \cong F[x]/\langle f \rangle$. Como el polinomio $f(x)$ es irreducible y $F[X]$ es un DIP, $\langle f(x) \rangle$ es maximo, Por lo tanto, $F[X]/\langle f(x) \rangle$ es un campo. Para cada polinomio $g \in F[X]$ denotamos $\overline{g}$ a su imagen en $F[x]/\langle f(x) \rangle$. Tenemos el morfismo

$$F \hookrightarrow F[X] \twoheadrightarrow \frac{F[X]}{\langle f(x) \rangle}$$

el cual es inyectivo. Así podemos identificar a F con su imagen en $F[x]/\langle f(x)\rangle$

Por lo tanto tenemos una extension

$F \subseteq F[x]/\langle f(x)\rangle$. Sea $\alpha = \overline{x} \in F[x]/\langle f(x)\rangle$

Entonces $f(\alpha) = f(\overline{x}) = \overline{f(x)} = 0 \in F[x]/\langle f(x)\rangle$

$\therefore$ α es raiz de $f(x) \in F[x]$.

Ejemplo: Consideremos el polinomio $x^2+1 \in \mathbb{R}[x]$. Este polinomio es irreducible. Por el lema anterior x^2+1 tiene una raiz en $\dfrac{\mathbb{R}[x]}{\langle x^2+1\rangle}$.

A saber, $i = x + \langle x^2+1\rangle$. Notemos que

$$i^2 = (x+\langle x^2+1\rangle)(x+\langle x^2+1\rangle) = x^2 + \langle x^2+1\rangle$$

$$= -1 + \langle x^2+1\rangle = -1$$

$$\begin{array}{c} \mathbb{C} \\ |\,2 \\ \mathbb{R} \end{array}$$

$\therefore$ es una raiz cuadrada de -1.

$$\mathbb{R}[x]/\langle x^2+1\rangle = \mathbb{R}[i] = \{\, a+bi \;/\; a,b \in \mathbb{R} \,\} = \mathbb{C}$$