Lema 0.1.
Dada cualquier extensión de cuerpos $\frac{F}{K}$, el conjunto

$$M = \{\alpha \in F : \alpha \text{ es algebraico sobre } K\}$$

es un subcuerpo de F que contiene a K. Además la extensión $\frac{M}{K}$ es algebraica.

Demostración. Veamos que M es cerrado para sumas y productos. En efecto, si $\alpha, \beta \in M$ entonces $\frac{K(\alpha,\beta)}{K}$ es una extensión finita ya que es de generación finita por generadores algebraicos. Como es una extensión finita, tiene que ser algebraica.

Entonces todo elemento de $K(\alpha, \beta)$ es algebraico sobre K y claramente $\alpha + \beta, \alpha\beta \in K(\alpha, \beta)$, luego son algebraicos sobre K.

Por otro lado, es claro que $K \subseteq M$ ya que si $\alpha \in K$ entonces ciertamente, α es raíz del polinomio $X - \alpha$. En particular, $1, -1 \in M$ y por tanto, se tiene que M es un subanillo. Nos falta comprobar que también es cerrado para inversos de los elementos no nulos.

Sea $\alpha \neq 0$ algebraico, entonces α es raíz de algún polinomio con coeficientes en K. Sea este $p = \sum_{i=0}^{n} a_i X^i$ entonces es claro que $\sum_{i=0}^{n} a_{n-i} X^i$, si evaluamos en $\frac{1}{\alpha}$ y multiplicamos por α^n es claro que $\frac{1}{\alpha}$ es raíz de este polinomio. En resumen $\frac{1}{\alpha} \in M$.

Por tanto, M es un cuerpo que contiene a K. Claramente, la extensión $\frac{M}{K}$ es algebraica ya que todos los elementos de α son raíces de algún polinomio con coeficientes en K. □

Lema 0.2.
Sea $\frac{F}{K}$ una extensión de cuerpos, $p \in K[x]$ y $z \in F$ tal que $p(z) = 0$. Si $\sigma : F \to F$ es un endomorfismo de anillos tal que $\sigma|_K = Id|_K$ entonces $\sigma(z)$ es raíz de p.

Demostración. Sea $p(X) = \sum a_i X^i$ entonces $p(\sigma(z)) = \sum a_i \sigma(z)^i$ y ya que σ fija los elementos de K lo anterior es igual a $\sigma(p(z))$ como $p(z) = 0$ por hipótesis, se tiene que $p(\sigma(z)) = 0$. □

Ejercicio 0.1: Se considera F_1 (resp. F_2) el subcuerpo de $\mathbb{R}$ (resp. $\mathbb{C}$) de todos los elementos algebraicos sobre $\mathbb{Q}$. Probar que $\frac{F_i}{\mathbb{Q}}$ es una extensión algebraica y que $[F_2 : F_1] = 2$.

Demostración. Basta tomar $F = \mathbb{R}, \mathbb{C}$ y $K = \mathbb{Q}$ en el lema 0.1

Por otro lado, se tiene la siguiente cadena de cuerpos $\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \mathbb{C}$. Vamos a ver que de hecho $F_2 = F_1[i] \cong \frac{F_1[X]}{<X^2+1>}$ de donde la dimensión es claramente dos, esto es, $[F_2 : F_1] = 2$.

$F_1[i] \subseteq) F_2$ Claramente, $1, i \in F_2$ ya que son números complejos y son raíces de los polinomios $X - 1, X^2 - 1 \in \mathbb{Q}[X]$. También se verifica que $F_1 \subseteq F_2$. Como F_2 es un cuerpo, cualquier combinación lineal de sus elementos $\alpha + \beta i$ con $\alpha, \beta \in F_1$ está en F_2. Esto completa la inclusión.

$F_2 \subseteq F_1[i])$ Sea $\alpha + \beta i \in F_2$ raíces de cierto polinomio $p \in \mathbb{Q}[X]$ y queremos ver que $\alpha, \beta \in F_1$. Por el lema 0.2, ya que $\sigma(\alpha + i\beta) = \alpha - i\beta$ es un endomorfismo por cálculo directo, se tiene que la raíz conjugada $\alpha - i\beta$ también es raíz de $p \in \mathbb{Q}[X]$. En consecuencia como claramente $\frac{1}{2}, \frac{1}{2i} \in F_2$ y F_2 es cuerpo y como $\alpha = \frac{\alpha+i\beta}{2} + \frac{\alpha-i\beta}{2} \wedge \beta = \frac{\alpha+i\beta}{2i} - \frac{\alpha-i\beta}{2i}$ se tiene que $\alpha, \beta \in F_2$ y como $\alpha, \beta \in \mathbb{R}$ se verifica claramente que $\alpha, \beta \in F_1$, como se quería. □

Ejercicio 0.2: Calcular:

- $Irr(\sqrt{2}, \mathbb{F}_3)$
- $Irr(\sqrt[4]{2}, \mathbb{F}_3)$
- $Irr(\sqrt{2} + \sqrt[4]{2}, \mathbb{F}_3)$
- $Irr(\sqrt{2} + \sqrt[4]{2}, \mathbb{Q})$

Para determinar los valores α que corresponden a cada una de las expresiones ambiguas $\sqrt[n]{}$ nos vamos a ir a un cuerpo extensión. Uno natural es $\mathbb{F}_9 \cong \frac{\mathbb{F}_3[X]}{<x^2+2x+2>} \cong \mathbb{F}_3[\sqrt{2}]$.

1. Por definición si $\alpha = \sqrt{2}$ entonces $\alpha^2 - 2 = 0$ y por tanto, α será un número algebraico sobre $\mathbb{F}_3$ que anula al polinomio $p(X) = X^2 - 2$. Este polinomio es irreducible y mónico sobre $\mathbb{F}_3$ ya que no tiene raíces en $\mathbb{F}_3$. Como α es una raíz suya deducimos que $Irr(\alpha, \mathbb{F}_3) = X^2 - 2$.

Obsérvese que en el cuerpo extensión estas raíces son $\alpha = \sqrt{2}, -\sqrt{2}$.

2.Por definición si $\alpha = \sqrt[4]{2}$ entonces $\alpha^4 - 2 = 0$ y por tanto, α será un número algebraico sobre $\mathbb{F}_3$ que anula al polinomio $p(X) = X^4 - 2$. Este polinomio no es irreducible sobre F_3. Veámoslo.

Como p no tiene raíces sobre $\mathbb{F}_3$, no tiene factores de grado 1 ni de grado 3. Luego sólo puede tener factores de grado 2. Los irreducibles de grado 2 en $\mathbb{F}_3[X]$ son $X^2 + 1, X^2 + X + 2, X^2 + 2X + 2$ y realizando la división euclídea se tiene que $p(X) = (X^2 + X + 2)(X^2 + 2X + 2)$. Por ser α una raíz del polinomio p será una raíz del polinomio $X^2 + X + 2$ o $X^2 + 2X + 2$ que como son mónicos e irreducibles son candidatos a ser $Irr(\alpha, \mathbb{F}_3)$.

Las raíces $\alpha = 2 + \sqrt{2}, 2 - \sqrt{2}$ tienen $Irr(\alpha, \mathbb{F}_3) = X^2 + 2X + 2$ y las raíces $\alpha = 1 + 2\sqrt{2}, 1 - 2\sqrt{2}$ tienen $Irr(\alpha, \mathbb{F}_3) = X^2 + X + 2$.

3. Primero obtenemos un polinomio que se anule en α mediante cálculo directo:

$$\alpha = \sqrt{2} + \sqrt[4]{2}$$

$$(\alpha - \sqrt{2})^2 = \sqrt{2}$$

$$(\alpha^2 + 2)^2 = ((2\alpha + 1)\sqrt{2})^2$$

$$\alpha^4 - 4\alpha^2 - 8\alpha + 2 = 0$$

$$\alpha^4 - \alpha^2 + \alpha + 2 = 0$$

$$(\alpha - 1)^2(\alpha^2 + 2\alpha^2 + 2)$$

La raíz $\alpha = 1$ tiene $Irr(\alpha, \mathbb{F}_3) = X - 1$ y las raíces $\alpha = 2 + \sqrt{2}, 2 + 2\sqrt{2}$ tienen $Irr(\alpha, \mathbb{F}_3) = X^2 + 2X + 2$.

Nos damos cuenta que esto no puede contener a todas los sumandos de las raíces halladas en los apartados 1 y 2. La razón es que en el primer paso hemos asumido implícitamente que $\sqrt{2} = (\sqrt[4]{2})^2$. Pero también podríamos elegir $\sqrt{2} = -(\sqrt[4]{2})^2$. Los cálculos en este caso son los siguientes:

$$\alpha = \sqrt{2} + \sqrt[4]{2}$$

$$(\alpha - \sqrt{2})^2 = -\sqrt{2}$$

$$(\alpha^2 + 2)^2 = ((2\alpha - 1)\sqrt{2})^2$$

$$\alpha^4 - 4\alpha^2 + 8\alpha + 2 = 0$$
$$\alpha^4 - \alpha^2 - \alpha + 2 = 0$$
$$(\alpha - 2)^2(\alpha^2 + \alpha + 2)$$

Por tanto, si $\alpha = 2$ obtengo que $Irr(\alpha, \mathbb{F}_3) = X - 2$ y si $\alpha = 1 + \sqrt{2}, 1 - \sqrt{2}$ tienen $Irr(\alpha, \mathbb{F}_3) = X^2 + X + 2$.

4. Repitiendo el proceso anterior, llegamos al polinomio

$$\alpha^4 - 4\alpha^2 - 8\alpha + 2 = 0$$

Esto nos da como candidato a polinomio mínimo $p(X) = X^4 - 4X^2 - 8X + 2$.

Sabemos que estudiar la irreducibilidad de un polinomio primitivo en $\mathbb{Z}$ es equivalente a estudiarla en $\mathbb{Q}$. Entonces en nuestro caso basta aplicar el criterio de Eisenstein con un primo $p = 2$ para obtener que es irreducible.

Dado que p es irreducible, mónico y α debe ser raíz de p deducimos que

$$Irr(\sqrt{2} + \sqrt[4]{2}, \mathbb{Q}) = X^4 - 4X^2 - 8X + 2$$