

1.1. Sean $p, q \in \mathbb{Z}$ primos relativamente primos.

$F = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Demuestra que:

① $[F : \mathbb{Q}] = 4$ y $\{\sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ es una \mathbb{Q} -base de F .

→ Aplicando el teorema de Lagrange sabemos que

$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = [F : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})][\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 4.$$

(p y q son primos relativos).

Sabemos que $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$. Vemos que

$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$, es decir, necesitamos que $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.

Suponemos que $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$. Por lo que existen $a, b \in \mathbb{Q}$

tales que $\sqrt{q} = a + b\sqrt{p}$, luego $q = a^2 + b^2 \cdot p + 2ab\sqrt{p}$.

Analizemos la igualdad:

$$\text{) } a = b = 0 \Rightarrow q = a^2 \quad (q \in \mathbb{Z}, a \in \mathbb{Q}) \quad !!$$

$$\text{) } a = 0 \Rightarrow q = b^2 \cdot p, \text{ luego, } q \mid p = (bp)^2 \quad !!$$

$$\text{) } \text{En otro caso tenemos } \sqrt{p} = \frac{q - a^2 - bp}{2ab} \in \mathbb{Q} \quad !!$$

Es decir, en todos los casos tenemos contradicción, luego

$\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. y $[F : \mathbb{Q}] = 4$.

→ Vemos que $\{\sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ es una \mathbb{Q} -base de F .

Una base de $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ es $\{\sqrt{p}\}$ ($\text{Ind}(\sqrt{p}, \mathbb{Q}) = x^2 - p$)

Por otro lado, $\sqrt{q} \notin \mathbb{Q}(\sqrt{p}) \Rightarrow \text{Ind}(\sqrt{q}, \mathbb{Q}(\sqrt{p})) = x^2 - q$ y

$\{\sqrt{q}\}$ es una base de $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}(\sqrt{p})$.

Usando la igualdad de Lagrange, tenemos que

$\{\sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ es una \mathbb{Q} -base de F

$$\textcircled{2} \quad \text{Im}(\sqrt{p} + \sqrt{q}) = x^4 - (p+q)x^2 + (p-q)^2$$

→ Llamo $\alpha = \sqrt{p} + \sqrt{q} \Rightarrow \alpha^2 = p + q + 2\sqrt{p}\sqrt{q} \Rightarrow$
 $\alpha^2 - (p+q) = 2\sqrt{p}\sqrt{q} \Rightarrow (\alpha^2 - (p+q))^2 = 4pq \Rightarrow$
 $\alpha^4 + (p+q)^2 - 2\alpha^2(p+q) = 4pq \Rightarrow$
 $\alpha^4 - 2\alpha^2(p+q) + (p-q)^2 = 0.$ Vemos que α es
raíz de $r = x^4 - 2(p+q)x^2 + (p-q)^2.$

El polinomio $\text{Im}(\sqrt{p} + \sqrt{q}, \mathbb{Q})$ es un divisor de $r.$

Por el apartado $\textcircled{1}$, tenemos que $[f : \mathbb{Q}] = 4,$
haciendo uso del apartado $\textcircled{3}$, tenemos que
 $\text{Im}(\sqrt{p} + \sqrt{q}, \mathbb{Q}) = x^4 - 2(p+q)x^2 + (p-q)^2.$

$$\textcircled{3} \quad F = \mathbb{Q}(\sqrt{p} + \sqrt{q}).$$

\supset Veremos ambas inclusiones.

Es claro que $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

Veremos que $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \supseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Basta probar que $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

$$\begin{aligned} \Rightarrow \sqrt{p} &= \frac{(p-q)\sqrt{p} + p\sqrt{q} - p\sqrt{q}}{(p-q)} = \\ &= \frac{p(\sqrt{p} + \sqrt{q}) - (q\sqrt{p} + p\sqrt{q})}{p-q} \in \mathbb{Q}(\sqrt{p} + \sqrt{q}). \end{aligned}$$

$$\begin{aligned} \Rightarrow \sqrt{q} &= \frac{(q-p)\sqrt{q} + q\sqrt{p} - q\sqrt{p}}{(q-p)} = \\ &= \frac{q(\sqrt{p} + \sqrt{q}) - (q\sqrt{p} + p\sqrt{q})}{(q-p)} \in \mathbb{Q}(\sqrt{p} + \sqrt{q}) \end{aligned}$$

□

$$\textcircled{4} \quad \mathbb{Q}(\sqrt{p}) \neq \mathbb{Q}(\sqrt{q}).$$

\supset Suponemos que no es cierto y llegaremos a contradicción.

Por el apartado $\textcircled{1}$, $\{\sqrt{p}\}$ es una base de $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ y

$\{\sqrt{q}\}$ es una base de $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}(\sqrt{p})$

Suponemos que $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{q}) \Rightarrow$ una base de $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ sea $\{\sqrt{q}\}$.

Por la igualdad de rangos usada en el apartado $\textcircled{1}$,

tenemos que $\{\sqrt{q}\}$ ~~y~~ sea una \mathbb{Q} -base de F ,

lo que contradice el propio apartado $\textcircled{1}$.

$$\Rightarrow \mathbb{Q}(\sqrt{p}) \neq \mathbb{Q}(\sqrt{q}).$$

1.2. Sea K un cuerpo con características $\neq \infty$.

Si $F = K(\sqrt{D_1}, \sqrt{D_2})$ con $D_1, D_2 \in K$ tienen la propiedad de que D_1, D_2 y D_1, D_2 no son cuadrados en K .

Demuestra que F/K es una extensión de Galois con grupo de Galois isomórfico al grupo de Klein.

Demuestra que cualquier extensión de Galois con grupo de Galois isomórfico al de Klein es del tipo descrito.

→ Vamos que F/K es una extensión de Galois.

Tenemos que $\sqrt{D_1}, \sqrt{D_2} \notin K$, ya que D_1, D_2, D_1, D_2 no son cuadrados en K . Tenemos que $\text{Irr}(\sqrt{D_1}, K) = x^2 - D_1$
 $\text{Irr}(\sqrt{D_2}, K) = x^2 - D_2$.

$\Rightarrow F = K(\sqrt{D_1}, \sqrt{D_2})$ es el cuerpo de descomposición de $(x^2 - D_1)(x^2 - D_2)$. $\Rightarrow F/K$ es normal.

Las raíces de $x^2 - D_1$ son $\sqrt{D_1}$ y $-\sqrt{D_1} \Rightarrow x^2 - D_1$ no tiene raíces múltiples.

Las raíces de $x^2 - D_2$ son $\sqrt{D_2}$ y $-\sqrt{D_2} \Rightarrow x^2 - D_2$ no tiene raíces múltiples.

$\Rightarrow F/K$ es separable $\Rightarrow F/K$ es de Galois.

□

Veamos que $\text{Gal}(F/k) \cong \text{Klein}$.

Consideremos la torre $k \subseteq K(\sqrt{D_1}) \subseteq K(\sqrt{D_1}, \sqrt{D_2})$

$$[F:k] = 4$$

$$\begin{array}{ccc} & K(\sqrt{D_1}, \sqrt{D_2}) & \\ 2/ & & \backslash 2 \\ k(\sqrt{D_1}) & & K(\sqrt{D_2}) \\ \backslash 2 & & /2 \\ & k & \end{array}$$

$$\begin{array}{ccc} & K^* = \text{Gal}(F/k) & \\ 2/ & & \backslash 2 \\ K(\sqrt{D_1})^* & & K(\sqrt{D_2})^* \\ \backslash 2 & & /2 \\ & <1> & \end{array}$$

Tenemos que $\text{Gal}(F/k)$ es un grupo de orden 4 y tiene dos subgrupos de orden 2, luego llegamos a $\text{Gal}(F/k) \cong \text{Klein}$.

Veamos el recíproco.

Supongamos que $\text{Gal}(F/k) \cong \text{Klein}$, entonces dicho grupo sera de la forma $\text{Gal}(F/k) = \langle a, b; a^2 = 1 = b^2 \rangle$.

Su retículo de subgrupos viene dado por

$$\begin{array}{ccc} \text{Gal}(F/k) & & F \\ \langle a \rangle & \langle b \rangle & \langle a \rangle^* \quad \langle b \rangle^* \\ \langle a \rangle & \langle ab \rangle & \langle a \rangle^* \quad \langle ab \rangle^* \\ \langle a \rangle & \langle b \rangle & \langle a \rangle^* \quad \langle b \rangle^* \\ & & \langle ab \rangle^* \end{array}$$

y obtenemos la torre $K \subset \langle a \rangle^* \subset F \Rightarrow \langle a \rangle^*$ es una extensión de grado 2 y de Galois $\Rightarrow \langle a \rangle^* = k(\alpha_1)$

donde α_1 es algebraico sobre k de grado 2 \Rightarrow
 α_1 es raiz de $x^2 + a_1x + b_1$ ($a_1, b_1 \in k$).

$$\text{Es decir, } \alpha_1 = \frac{-\alpha_1 + \sqrt{\alpha_1^2 - 4b_1}}{2}.$$

$$\Rightarrow K(\alpha_1) = K\left(-\frac{\alpha_1 + \sqrt{\alpha_1^2 - 4b_1}}{2}\right) = K(\sqrt{\alpha_1^2 - 4b_1})$$

$\sqrt{\alpha_1^2 - 4b_1} \notin K$ ya que $x^2 + \alpha_1 x + b_1$ es irreducible \Rightarrow $\alpha_1^2 - 4b_1$ no puede ser cuadrado en K .

Con un razonamiento análogo para α_2 , tenemos que

$$K(\alpha_2) = K(\sqrt{\alpha_2^2 - 4b_2}) \quad (\alpha_2, b_2 \in K)$$

Llamando $D_1 = \alpha_1^2 - 4b_1$ y $D_2 = \alpha_2^2 - 4b_2$ de modo que

$$\begin{aligned} & K(\sqrt{D_1}) \subseteq F \\ & K(\sqrt{D_2}) \subseteq F \end{aligned} \quad \Rightarrow K(\sqrt{D_1}, \sqrt{D_2}) \subseteq F$$

ya que $\text{In}(\sqrt{D_2}, K(\sqrt{D_1})) = x^2 + \alpha_2 x + b_2$

$$\text{Entonces } \underbrace{K \subseteq K(\sqrt{D_1}) \subseteq K(\sqrt{D_1}, \sqrt{D_2}) \subseteq F}_{\varphi}$$

$$\text{Por lo que } [K(\sqrt{D_1}, \sqrt{D_2}) : F] = 1 \Rightarrow F = K(\sqrt{D_1}, \sqrt{D_2})$$

□