$\boxed{5.1}$ 1) Veamos que $[K(\alpha):K] = [K(\beta):K]$.

Por ser α y β raíces de un polinomio irreducible $p(x) \in K[x]$, tenemos que $Irr(\alpha, K) = Irr(\beta, K)$. Usando el lema 3.1.1, sabemos que existirá un isomorfismo $\eta: K(\alpha) \longrightarrow K(\beta)$ con $\eta(\alpha) = \beta$. De este modo tenemos que $K(\alpha)$ y $K(\beta)$ son isomorfos y se tiene $[K(\alpha):K] = [K(\beta):K]$.

2) Prueba que $K(\alpha)/K \cong K(\beta)/K$.

Por el mismo razonamiento que hemos hecho en 5.1.1. se tiene que $K(\alpha) \cong K(\beta) \Rightarrow$ se tiene la igualdad que nos piden.

3) E cuerpo de descomposición de $p(x)$ sobre K tal que $\alpha, \beta \in E$. ¿Existe siempre un automorfismo $\sigma: E/K \longrightarrow E/K$ tal que $\sigma(\alpha) = \beta$?

Por ser α y β raíces de un polinomio irreducible $p(x) \in K[x]$, tenemos que $Irr(\alpha, K) = Irr(\beta, K)$. Usando el lema 3.1.1, sabemos que existirá un isomorfismo $\varphi: K(\alpha) \to \overline{K}$ sobre K con $\varphi(\alpha) = \beta$.

Scanned by CamScanner

Haciendo uso del lema 5.4, podremos extender a un automorfismo $\tilde{\sigma}$ $\overline{K}/K \longrightarrow \overline{K}/K$ llevando alfa en β. Quedándonos con la restricción en E, tendremos que sí es cierto.

4) ¿Existe siempre $\sigma: E/K \longrightarrow E/K$ tal que $\sigma(\alpha)=\beta$ y $\sigma(\beta)=\sigma$, dejando las demás raíces fijas?

Veremos que también es cierto.
Por el mismo razonamiento que en 5.1.3 tenemos un isomorfismo $\varphi: K(\alpha) \longrightarrow \overline{K}$ sobre K con $\varphi(\alpha)=\beta$.
Sabemos que los automorfismos llevan raíces en raíces, luego podemos llevar β en α, dejando el resto fijos.

5) ¿Existe $\sigma: E/K \longrightarrow E/K$, $\sigma \neq id$, tal que $\sigma(\alpha)=\alpha$?

No tiene porqué ser cierto. Veamos un contraejemplo:
Si α y β son las únicas raíces, como $\sigma(\alpha)=\alpha$ y tenemos que llevar raíces a raíces tendría que ser $\sigma(\beta)=\beta$, lo que nos da la identidad.

$\boxed{5.2}$ Sean α, β raíces de polinomio illeducible $p(x) \in K[x]$, tal que $\alpha^n \in K$. Probar que β también lo cumple.

Por ser α raíz de $p(x) \in K[x]$ illeducible y $\alpha^n \in K$, se tiene α es raíz de $g(x) = x^n - \alpha^n \in K[x]$ $\Rightarrow p(x) \mid g(x)$, y puedo tomar $q(x) \in K[x]$ de modo que $g(x) = p(x) \cdot q(x)$.

Evaluando en β nos queda $g(\beta) = p(\beta) q(\beta) = 0$, por ser β raíz de $p(x)$. Luego tenemos $g(\beta) = 0$.

Es decir, $\beta^n - \alpha^n = 0 \Rightarrow \beta^n = \alpha^n \in K$.

$\boxed{5.3}$ Sea K cuerpo de característica p, $a \in K$. Probar que si $x^p - a$ no tiene raíces en K, entonces $x^p - a$ es illeducible sobre K.

Vamos a hacer uso del tema 13, extensiones ciclotómicas.

Las raíces del polinomio $\tilde{p}(x) = x^n - a$ son todas distintas $\Leftrightarrow$ $\tilde{p}$ es primo con su derivada ($D\tilde{p} = nx^{n-1}$).

Esto ocurre si y sólo si la característica de K no divide a n. En nuestro caso $car(K) = p \neq 0$, si $n = mp^r$, con $p \nmid m \Rightarrow x^n - a = (x^m - 1)^{p^r}$ y existirían únicamente m raíces n-ésimas distintas de multiplicidad p^r. En nuestro caso $m=1$ y $n=1$, luego tenemos $x^p - a = (x-a)^p$. $\Rightarrow$ sus raices es la a de multiplicidad p, luego si no tiene raiz es irreducible.

$\boxed{5.4}$ Sean $a, b, d \in \mathbb{Z}$. d y $a^2 - db^2$ libres de cuadrados.

Determinar el grupo de Galois de la extensión $\mathbb{Q}(\sqrt{a+b\sqrt{d}})/\mathbb{Q}$.

Veamos el irreducible:

$\alpha = \sqrt{a+b\sqrt{d}} \Rightarrow \alpha^2 = a + b\sqrt{d} \Rightarrow (\alpha^2 - a)^2 = b^2 d \Rightarrow$

$\alpha^4 - 2\alpha^2 a + a^2 = b^2 d \Rightarrow$

$\mathrm{Irr}(\alpha, \mathbb{Q}) = x^4 - 2a x^2 + (a^2 - b^2 d)$

$[\mathbb{Q}(\sqrt{a+b\sqrt{d}}) : \mathbb{Q}] = 4.$

Veamos las raices:

$$\alpha^2 = \frac{2a \pm \sqrt{4a^2 - 4a^2 + 4b^2 d}}{2} = a \pm b\sqrt{d}$$

$\alpha_1 = \sqrt{a + b\sqrt{d}}$

$\alpha_2 = \sqrt{a - b\sqrt{d}}$

$\alpha_3 = -\sqrt{a + b\sqrt{d}}$

$\alpha_4 = -\sqrt{a - b\sqrt{d}}$

Entonces podemos considerar:

$\sigma_1 : \sqrt{a+b\sqrt{d}} \longrightarrow \sqrt{a+b\sqrt{d}}$

$\sigma_2 : \sqrt{a+b\sqrt{d}} \longrightarrow -\sqrt{a+b\sqrt{d}}$

$\sigma_3 : \sqrt{a+b\sqrt{d}} \longrightarrow \sqrt{a-b\sqrt{d}}$

$\sigma_4 : \sqrt{a+b\sqrt{d}} \longrightarrow -\sqrt{a-b\sqrt{d}}$

$\mathrm{Gal}(\mathbb{Q}(\sqrt{a+b\sqrt{d}})/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}.$

$\boxed{5.1}$ K cuerpo.

$p(x) \in K[x]$ polinomio de grado n

$p(x) = p_1(x) \cdots p_t(x)$, con $p_i(x) \in K[x]$ polinomio irreducible de grado d_i y $p_i(x) \neq p_j(x)$ si $i \neq j$.

Da una cota, que se alcance, del grado de la extensión $K(p(x))/K$.

Considero F_i como el cuerpo de descomposición de p_i. Como p_i es irreducible, tenemos que $[F_i : K] = d_i$ ya que $F_i = K(\alpha_{i1}, \ldots, \alpha_{id})$ y $gr(p_i) = d_i$.

Ahora considero la torre

$K(p(x)) \subset K(\alpha_{11}, \ldots, \alpha_{1d_1}, \ldots, \alpha_{1t}, \ldots, \alpha_{d_t t})$

$[K(p(x)) : K] \leq [K(\alpha_{11}, \ldots, \alpha_{d_t t}) : K]$.

construimos las torres

$$K \subset \underbrace{K(\alpha_{11}, \ldots, \alpha_{d_1 1})}_{d_1} \subset \cdots \subset \underbrace{K(\alpha_{11}, \ldots, \alpha_{d_1 1}, \ldots, \alpha_{1t}, \ldots, \alpha_{d_t t})}_{d_t}$$

$\Rightarrow$ tendremos como cota $[K(p(x)) : K] \leq d_1 \cdots d_t$.

$\boxed{6.2}$ K cuerpo. $p(x) \in K[x]$ polinomio irreducible de grado n. Prueba que si el grado del $K(p(x))/K$ es igual a $n!$ $\Rightarrow$ $p(x)$ es irreducible.

Sean $\alpha_1, .., \alpha_n$ las raices del polinomio $p(x)$, vamos a considerar la torre de extensiones

$$\begin{array}{c}
K(\alpha_1, .., \alpha_n) \\
\Big| \; 1 \\
K(\alpha_1, .., \alpha_{n-1}) \\
\vdots \; 2 \\
\vdots \\
K(\alpha_1, \alpha_2, \alpha_3) \\
\Big| \; n-2 \\
K(\alpha_1, \alpha_2) \\
\Big| \; n-1 \\
K(\alpha_1) \\
\Big| \; n \\
K
\end{array}$$

Por ser el grado de la extension $n!$, solo queda una opcion para los grados de las subextensiones que será $n, n-1, n-2, n-3 \dots$ como vemos en la representación.

Por esto ninguna extension es trivial, esto nos lleva a que cada raiz que añado no estaba en la extension anterior $\Rightarrow$ ninguna raiz estaba en K y ninguna raiz es multiple $\Rightarrow$ $p(x)$ es irreducible.

$\boxed{7.1}$ Dado $K \subseteq F \subseteq E$.

1) Si E/K es normal $\Rightarrow$ F/K no necesariamente es normal. Justifica este hecho.

Para justificar este hecho, usaremos el ejemplo que nos dan para demostrar que no se cumple.

$$\begin{array}{c} E = \mathbb{Q}(\omega, \sqrt[3]{2}) \\ | \\ F = \mathbb{Q}(\sqrt[3]{2}) \\ | \\ K = \mathbb{Q} \end{array}$$

E/K es normal por ser el cuerpo de descomposición del polinomio $p(x) = x^3 - 2 \in \mathbb{Q}[x]$.

Para ver que F/K no es normal usamos el teorema 5.2. Para que dicha extensión sea normal necesitamos que todo polinomio irreducible $p(x) \in K[x]$ con una raíz en F descomponga en F.

Tomo $p(x) = x^3 - 2$. Es irreducible en $\mathbb{Q}$ y tiene una raíz en $\mathbb{Q}(\sqrt[3]{2})$ pero no descompone en $\mathbb{Q}(\sqrt[3]{2})$ $\Rightarrow$ la extensión no es normal.

2) Si las extensiones E/F y F/K son normales no siempre E/K es normal.

En este caso tenemos el ejemplo siguiente:

$$\begin{array}{c} E = \mathbb{Q}(\sqrt{\sqrt{2}}) \\ | \\ F = \mathbb{Q}(\sqrt{2}) \\ | \\ K = \mathbb{Q} \end{array}$$

Igual que en el caso anterior tenemos que buscar los polinomios que nos permiten obtener la normalidad. Para la extensión F/K tomo $p(x) = x^2 - 2$ y para la extensión E/F tomo $g(x) = x^2 - \sqrt{2}$.

Sin embargo E/K no es normal. Para verlo hago uso del teorema 5.2, considerando el polinomio $p(x) = x^4 - 2$, el polinomio irreducible de $\sqrt{\sqrt{2}}$, con raíces $\pm\sqrt{\sqrt{\pm 2}}$.

Scanned by CamScanner

$\boxed{9.2}$ K un cuerpo. Si $K(\alpha)/K$, $K(\beta)/K$ son extensiones de Galois abelianas, entonces $K(\alpha+\beta)/K$ es una extension de Galois abeliana.

$$\begin{tikzcd}[column sep=small] & K(\alpha,\beta) \arrow[dl, dash] \arrow[dr, dash] & \\ K(\alpha) \arrow[d, dash] & & K(\beta) \arrow[d, dash] \\ K \arrow[rr, equal] & & K \end{tikzcd}$$

Sabemos que $K(\alpha,\beta)$ es de Galois sobre K. Además su correspondiente grupo de Galois es un subgrupo de $Gal(K(\alpha)/K) \times Gal(K(\beta)/K)$. Como estos dos son abelianos, se tiene que $K(\alpha,\beta)/K$ es abeliano.

Nos piden trabajar sobre $K(\alpha+\beta)/K$, pero esto lo podemos ver en una torre de extensiones como

$$\begin{tikzcd}[column sep=small] K(a,b) \supseteq K(a+cb) \quad \forall c \in \mathbb{R} \arrow[d, dash] & \\ K(a+b) \arrow[d, dash] \arrow[dr, dash] & \\ K(a) & K(b) \end{tikzcd}$$

y cualquier extensión intermedia de Galois debe de ser abeliana $\Rightarrow K(\alpha+\beta)/K$ es una extension de Galois abeliana.

$\boxed{10.1}$ Determinar el grupo de Galois del polinomio

$p(x) = x^4 - 3x^2 + 4 \in \mathbb{Q}[x]$.

Se trata de un polinomio irreducible. $\Rightarrow$ el grupo de $p(x)$ será un subgrupo transitivo de S_4. tomo una raiz α_1 de $p(x)$ y lo estudio en la extension $K(\alpha_1)$. Dicho polinomio se escribe de la forma $p(x) = (x-\alpha_1)p_1(x)p_2(x)p_3(x)$ y $\sqrt{dis(p)} \in K \Rightarrow Gal(p/K) = V$. Hemos hecho uso de Mathematica para ver que todas estas igualdades y pertenencias son ciertas.

$\boxed{10.2}$ Determinar el grupo de Galois de

$p(x) = x^5 - 2x^3 - x^2 + 2$

En este caso el polinomio no es irreducible, considero como raiz $\alpha = -\sqrt{2} \Rightarrow p(x) = (x-\alpha)\, q_1(x)$ donde $q_1(x)$ tendrá grado 4. Aplicando el algoritmo visto en clase tenemos $Gal(p/K) \simeq C_2 \times C_2$.

$\boxed{10.3}$ Determinar el grupo de Galois de

$p(x) = x^5 - 4x + 12$.

$p(x)$ es irreducible. Nos vamos al caso 3 del algoritmo trabajado en clase y tenemos $Gal(p/K) \simeq S_5$.