

Ejercicios.pdf



crgs_



Algebra lii



4º Doble Grado en Ingeniería Informática y Matemáticas



Escuela Técnica Superior de Ingenierías Informática y de
Telecomunicación
Universidad de Granada



[Accede al documento original](#)

antes



**Descarga sin publi
con 1 coin**



Después

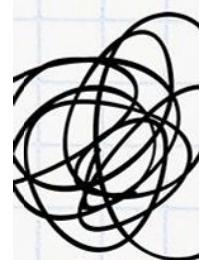


Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato
→ Planes pro: más coins

pierdo
espacio



Necesito
concentración

ali ali ooooh
esto con 1 coin me
lo quito yo...

wuolah
XXXXXX

Ejercicios Apuntes

• Tema 1

EJERCICIO 1. Demostrar que el cardinal de un cuerpo finito es de la forma p^n , donde p es un entero primo y n es un entero positivo. ¿Qué interpretación tienen p y n ?

Sea K un cuerpo finito, sup $p = \text{car}(K) > 0 \Rightarrow$ subcuerpo primo $\cong \mathbb{Z}_p \leq K$. Sup $[K : \mathbb{Z}_p] = n < \infty$
como $\mathbb{Z}_p \leq K$, K es un \mathbb{Z}_p -espacio vectorial $\Rightarrow |K| = |\mathbb{Z}_p|^n = p^n$

EJERCICIO 2. Dada una extensión de cuerpos $F \leq K$ y subconjuntos $S, T \subseteq K$, razonar que $F(S \cup T) = F(S)(T)$.

$$F \leq K, S, T \subseteq K \Rightarrow F(S \cup T) = F(S)(T)$$

$$\cap F(S \cup T) \subseteq F(S)(T)$$

$F(S \cup T)$ es el menor subcuerpo que contiene a $F \cup S \cup T$ y $F, S, T \subseteq F(S)(T) \Rightarrow F(S \cup T) \subseteq F(S)(T)$

$$\cap F(S)(T) \subseteq F(S \cup T)$$

$F(S) \subseteq F(S \cup T)$ pues $F(S)$ es el menor subcuerpo que contiene a $F \cup S \subseteq F(S \cup T)$

$F(S)(T)$ es el menor subcuerpo que contiene a $F(S) \cup T$. Como $F(S), T \subseteq F(S)(T) \Rightarrow F(S) \cup T \subseteq F(S)(T)$

EJERCICIO 3. Sea $F \leq K$ una extensión de cuerpos y $\alpha \in K$ de grado 2 sobre F . Demostrar que $F(\alpha)$ es un cuerpo de descomposición de $\text{Irr}(\alpha, F)$.

$$F \leq K, \deg_K(\alpha) = 2 \Rightarrow F(\alpha) \text{ es cdd de } \text{Irr}(\alpha, F)$$

$$\text{Como } [K : F] = 2 \Rightarrow \deg(\text{Irr}(\alpha, F)) = 2. \text{ Como } \alpha \text{ es raíz de } f(x) = (x-\alpha)(x-\bar{\alpha}) \Rightarrow F(\alpha, \bar{\alpha}) \text{ es cdd de } f$$

$$\text{Vemos que } F(\alpha, \bar{\alpha}) = F(\alpha), \text{ siendo que } \bar{\alpha} \notin F(\alpha)$$

$$\text{Como } \alpha \notin F(\alpha) \Rightarrow \alpha \notin F \Rightarrow \alpha \notin F(\alpha) \Rightarrow \alpha^2 \alpha = \alpha^3 \in F(\alpha) \Rightarrow \alpha^3 \in F(\alpha)$$

EJERCICIO 4. Calcular $\text{Irr}(\omega, \mathbb{Q}(\sqrt[3]{2}))$, para $\omega = e^{i2\pi/3}$.

$$\begin{aligned} x^3 - 1 &\text{ no es irreducible pues } 1 \in \mathbb{Q}(\sqrt[3]{2}) \text{ es raíz} \Rightarrow \frac{x^3 - 1}{x^3 + x^2} \mid \frac{x-1}{x^2 + x + 1} \Rightarrow x^2 + x + 1 = (x^2 + x + 1)(x-1) \\ &\text{Como } x^3 - 1 = x^2 + x + 1 \text{ tiene } 3 \text{ raíces} \\ &\text{son complejas y no están en } \mathbb{Q}(\sqrt[3]{2}) \end{aligned}$$

EJERCICIO 5. Sea p un número primo y $\omega \neq 1$ una raíz p -ésima compleja de la unidad. Calcular $\text{Irr}(\omega, \mathbb{Q})$.

wuolah

EJERCICIO 6. Calcular $\text{Irr}(\sqrt{2} + i, \mathbb{Q})$.

Sea $\alpha = \sqrt{2} + i$, veamos que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$. Por un lado, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, i)$

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

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

$$\alpha^2 - 2\sqrt{2}\alpha + 3 = 0 \Rightarrow \alpha^2 + 3 = 2\sqrt{2}\alpha \Rightarrow \sqrt{2} = \frac{\alpha^2 + 3}{2\alpha} \in \mathbb{Q}(\alpha)$$

$$i = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$$

$$\Rightarrow \mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$$

Por el lema de la Torre, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4 \Rightarrow z = \frac{(\alpha^2 + 3)^2}{4\alpha^2}$

$\underbrace{\mathbb{Q}(\sqrt{2})(i)}$

$\underbrace{x+1}_{x^2-2}$ es irred

por Eisenstein para $p=2$

es irred

porque todas

sus raíces

son complejas y no

están en $\mathbb{Q}(\sqrt{2})$

$$8\alpha^2 = \alpha^4 + 6\alpha^2 + 9$$

$$\alpha^4 - 2\alpha^2 + 9 = 0$$

el os raíz de $g(x) = x^4 - 2x^2 + 9 \Rightarrow g(x)$ es múltiplo del $\text{Irr}(\alpha, \mathbb{Q})$ y como ambos tienen grado 4 son iguales

EJERCICIO 7. Calcular $\text{Irr}(\sqrt{2} + i\sqrt{3}, \mathbb{Q})$.

Sea $\alpha = \sqrt{2} + i\sqrt{3}$, veamos que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$. Por un lado, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, i\sqrt{3})$

$$(\alpha - \sqrt{2})^2 = -3$$

$$\alpha^2 - 2\sqrt{2}\alpha + 5 = 0 \Rightarrow \alpha^2 + 5 = 2\sqrt{2}\alpha \Rightarrow \sqrt{2} = \frac{\alpha^2 + 5}{2\alpha} \in \mathbb{Q}(\alpha)$$

$$i\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$$

$$\Rightarrow \mathbb{Q}(\sqrt{2}, i\sqrt{3}) \subseteq \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$$

Por el lema de la Torre, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4 \Rightarrow z = \frac{\alpha^4 + 10\alpha^2 + 25}{4\alpha^2}$

$\underbrace{\mathbb{Q}(\sqrt{2})}_{x+3}$

$\underbrace{x-2}_{x^2+2}$ es irred

por Eisenstein para $p=2$

es irred

porque todas

sus raíces

son complejas y no

están en $\mathbb{Q}(\sqrt{2})$

$$8\alpha^2 = \alpha^4 + 10\alpha^2 + 25$$

$$\alpha^4 + 2\alpha^2 + 25$$

el os raíz de $g(x) = x^4 + 2x^2 + 25 \Rightarrow g(x)$ es múltiplo del $\text{Irr}(\alpha, \mathbb{Q})$ y como ambos tienen grado 4 son iguales

EJERCICIO 8. Calcular un cuerpo de descomposición de $X^4 + 16 \in \mathbb{Q}[X]$ y su grado sobre \mathbb{Q} .

$$x^4 + 16 = 0$$

$$x^4 = -16 \Rightarrow x = \sqrt[4]{-16} = \sqrt[4]{-1} \cdot \sqrt[4]{16} = 2\sqrt[4]{-1}$$

$$\text{fórmula de } \sqrt[n]{-1} \rightarrow e^{i\frac{\pi+2k\pi}{n}} = \cos\left(\frac{\pi+2k\pi}{n}\right) + i\sin\left(\frac{\pi+2k\pi}{n}\right) \Rightarrow 4\sqrt[4]{-1} \cdot \left(1+i\right)\sqrt[4]{2}, \left(-1+i\right)\sqrt[4]{2}, \left(-1-i\right)\sqrt[4]{2}, \left(1-i\right)\sqrt[4]{2}$$

$$\mathbb{Q}(\left(1+i\right)\sqrt[4]{2}, \left(-1+i\right)\sqrt[4]{2}, \left(-1-i\right)\sqrt[4]{2}, \left(1-i\right)\sqrt[4]{2}) = \mathbb{Q}(\sqrt{2+i\sqrt{2}}, \sqrt{2-i\sqrt{2}}) = \mathbb{Q}(\sqrt{2}, i)$$

como $x^4 + 16$ es irreducible sobre $\mathbb{Q} \Rightarrow [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$

$\underbrace{x+1}_{x^2+1}$ es irred

porque todas

sus raíces

no están en

$\mathbb{Q}(\sqrt{2})$

$\underbrace{x-2}_{x^2+2}$ es irred en \mathbb{Q}

por Eisenstein para $p=2$

EJERCICIO 9. Calcular $\text{Irr}(\sqrt{2} + \sqrt[3]{2}, \mathbb{Q})$.

Sea $\alpha = \sqrt{2} + \sqrt[3]{2}$, veamos que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Por un lado, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

$$(\alpha - \sqrt{2})^3 = 2$$

$$\alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} = 2$$

$$\alpha^3 + 6\alpha - 2 = 3\sqrt[3]{2}\sqrt{2} + 2\sqrt{2} \Rightarrow \sqrt{2} = \frac{\alpha^3 + 6\alpha - 2}{3\sqrt[3]{2} + 2} \in \mathbb{Q}(\alpha)$$

$$\sqrt[3]{2} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$$

$$\Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$$

Por el Teorema de la Torre, $[\mathbb{Q}(G_1):\mathbb{Q}] = [\mathbb{Q}(G_1):\mathbb{Q}(F_1)] \cdot [\mathbb{Q}(F_1):\mathbb{Q}] \leq 6 \rightarrow [\mathbb{Q}(G_1):\mathbb{Q}]$ es múltiplo de 2.

$x^3 - 2$ no
sabemos si
es irracional

Σ_2 es irreduzibel
aus $p=2$

$$[\mathbb{Q}(\zeta_3):\mathbb{Q}] = [\mathbb{Q}(\zeta_3):\mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] \leq 6 \Rightarrow [\mathbb{Q}(\zeta_3):\mathbb{Q}] \text{ es múltiplo de } 3$$

$$\begin{array}{l} x^2 - 2 \text{ es} \\ \text{sobremodo si} \\ \text{es irred} \end{array}$$

-2 es irreduzibel einstein
para $p=2$

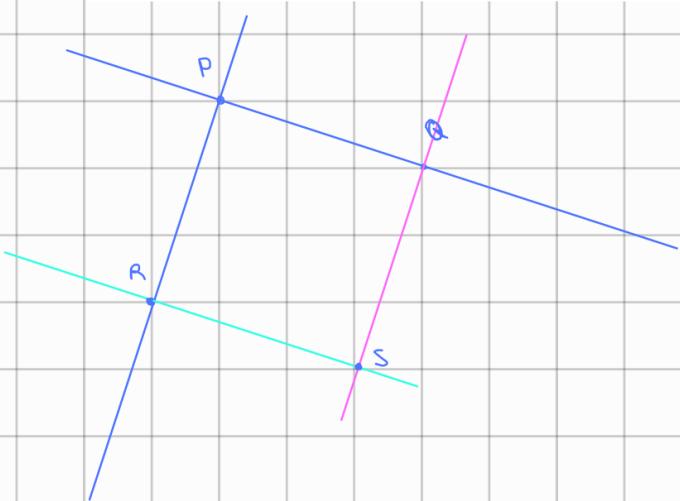
$$\Rightarrow [Q(\omega) : Q] = 6$$

$$\frac{(\sqrt{2})^2}{(3a^2+2)^2} = \frac{(a^3+6a^2-2)^2}{(3a^2+2)^2} \Rightarrow 2(a^4 + 12a^2 + 4) = a^6 + 12a^4 - 4a^3 + 36a^2 - 24a + 4$$

$$a^6 - 6a^4 - 4a^3 + 12a^2 - 24a - 4$$

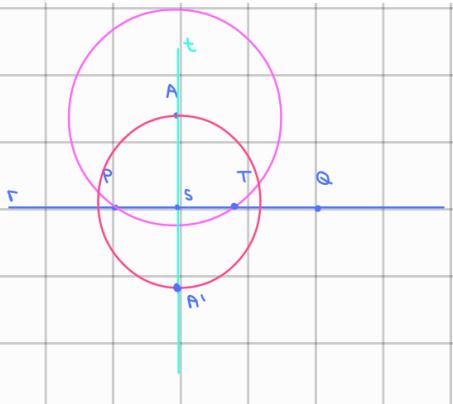
2 es raíz de $f(x) = x^6 - 6x^4 - 4x^3 +$, $f(x)$ es múltiplo del Ir(x , Q) y como ambos tienen grado 6 son iguales

EJERCICIO 10. Construir a partir de tres puntos no colineales, usando regla y compás, el cuarto punto que completa un paralelogramo.



- 1º Trazo las rectas PQ y PR
2º Perpendicular a PQ que pasa por Q
3º Perpendicular a PR que pasa por R
4º " a RS " " " Q
5º " " QS " " " R

EJERCICIO 11. Dados dos puntos que determinan una recta r y un punto A con contenido en ella, construir, usando regla y compás, el simétrico de A con respecto de r .



- 1º Perpendicular a \overline{PA} que pase por A (t)
 - 2º Circunferencia centrada en S y radio SA
 - 3º Intersección de la circunferencia con t es A'

EJERCICIO 12. Sea F un subcuerpo de \mathbb{R} . Los puntos $(x, y) \in F \times F$ se llaman F -puntos del plano. Una F -recta es aquella determinada por dos F -puntos. Demostrar que la intersección de dos F -rectas, de ser no vacía, es un F -punto.

Sean $r = ax + b$ y $s = cx + d$ dos F-rectas. Sean $x_1, x_2 \in F$ ($x_1 \neq x_2$), el sistema $\begin{cases} r = ax_1 + b \\ s = cx_1 + d \end{cases}$ tiene solución en $F \Rightarrow a \neq c$

Análogamente para $s \Rightarrow c, d, E, F$

$$\text{se } \alpha x + b = cx + d \Rightarrow \alpha x - cx = d - b \Leftrightarrow x = \frac{d-b}{\alpha-c}$$

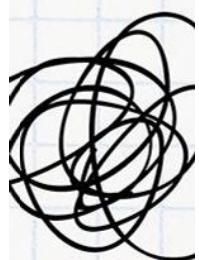
$\text{sum } 113 + x \quad g \# s \rightarrow \text{sum } x + 113 \rightarrow \text{sum } 113 + x \quad \text{for } x = 1 \dots a - c$

Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato
→ Planes pro: más coins

pierdo
espacio



Necesito
concentración

ali ali ooooh
esto con 1 coin me
lo quito yo...

wuolah

EJERCICIO 13. Con la notación del Ejercicio 12. Una F -circunferencia es aquella que tiene como centro un F -punto y pasa por otro F -punto. Demostrar que la intersección de una F -recta y una F -circunferencia, de ser no vacía, consiste en uno o dos $F(\sqrt{c})$ -puntos para cierto $c \in F$ positivo. Deducir que dos F -circunferencias se intersecan, de hacerlo, en $F(\sqrt{c})$ -puntos, para $c \in F$ positivo adecuado.

Tomemos una circunferencia genérica $(x-a)^2 + (y-b)^2 = r^2$ en una F -circunferencia con centro en (a,b) un F -punto. Supongamos que pasa por otro F -punto $(c,d) \Rightarrow (c-a)^2 + (d-b)^2 = r^2 \Rightarrow r^2 \in F$.

Tomemos una recta $r = qx + p$ con $q, p \in F$.

Al intersectar la recta y la circunferencia $\Rightarrow (x-a)^2 + (qx+p-b)^2 = r^2$

$$x^2 - 2ax + a^2 + q^2x^2 + 2qx(x-p) + (p-b)^2 = r^2$$

$$\underbrace{x^2(1+q^2)}_U + x(2q(p-b) - 2a) + \underbrace{(a^2 + (p-b)^2 - r^2)}_W = 0$$

$$x = \frac{-v \pm \sqrt{v^2 - 4uw}}{2w} \Rightarrow \text{también } r^2 = \sqrt{v^2 - 4uw}$$

Si la recta es tangente a la circunferencia sólo intersecará en un punto, si no en dos.

$$\text{son dos } F\text{-circunferencias} \Rightarrow (x-a)^2 + (y-b)^2 = r^2$$

$$(z-c)^2 + (t-d)^2 = s^2$$

EJERCICIO 14. Sean $\tau : F \rightarrow E$ y $\rho : E \rightarrow E$ homomorfismos de cuerpos. Demostrar que ρ es $\tau(F)$ -lineal si, y sólo si, $\rho\tau = \tau$.

$$F \xrightarrow{\tau} E \xrightarrow{\rho} E \quad \tau, \rho \text{ homomorfismos}$$

\Leftarrow Sup que $\rho\tau = \tau$, sea $a \in F$ arbitrario $\Rightarrow \rho(\tau(a)) = \tau(a) \Rightarrow \rho|_{\tau(F)} = \text{Id}_{\tau(F)} \Rightarrow \rho$ es $\tau(F)$ -lineal

\Rightarrow Sup que ρ es $\tau(F)$ -lineal \Rightarrow si $a \in F$, $\rho(\tau(a)) = \rho(\tau(a)) \cdot \text{Id}_E = \tau(a) \rho(\text{Id}_E) = \tau(a) \Rightarrow \rho$ es $\tau(E)$ -lineal $\Rightarrow \rho\tau = \tau$
de ser ρ lineal

EJERCICIO 15. Sea F es un cuerpo de característica positiva p . Demostrar que, si $a, b \in F$, entonces $(a-b)^q = a^q - b^q$ para todo $q = p^n$ con n natural no nulo.

$$F \text{ cuerpo con } \text{car}(F) = p > 0. \text{ Si } a, b \in F \Rightarrow (a-b)^q = a^q - b^q \quad \forall q = p^n \text{ con } n \in \mathbb{N} \setminus \{0\}$$

Por inducción: para $n=1$, $(a-b)^p = \sum_{i=0}^p \binom{p}{i} a^i (-b)^{p-i}$ cuando $p \mid \binom{p}{i}$ visto ip $\Rightarrow (a-b)^p = a^p - b^p$

Supuesto para $n \Rightarrow (a-b)^{p^n} = a^{p^n} - b^{p^n}$

Probamos para $n+1$

$$(a-b)^{p^{n+1}} = ((a-b)^{p^n})^{p} = (a^{p^n} - b^{p^n})^p = a^{p^{n+1}} - b^{p^{n+1}}$$

EJERCICIO 16. Demostrar que, si Π denota el subcuerpo primo de K , entonces $\text{Aut}_{\Pi}(K) = \text{Aut}(K)$.

EJERCICIO 15. Demostrar que, si π es el subcuerpo primo de un cuerpo K , entonces el único homomorfismo de cuerpos $\pi \rightarrow K$ es la inclusión.

wuolah

Ex 17 y 18 están repetidos

EJERCICIO 19. Sea $F \leq K$ una extensión de cuerpos de grado 2. Mostrar que, si la característica de F es distinta de dos, existe $\beta \in K$ tal que $\beta^2 \in F$ y $K = F(\beta)$.

$$[K:F]=2 \quad \Rightarrow \exists \beta \in K : \beta^2 \in F \quad y \quad K = F(\beta)$$
$$\text{car}(F) \neq 2$$

como $[K:F]=2$, $\exists \alpha \in K \setminus F : \text{irr}(\alpha, F) = f(x)$ tiene grado 2 $\Rightarrow f(x) = x^2 + ax + b$ con $f(a) = 0$

$$f(x) = x^2 + ax + \frac{a^2}{4} + b - \frac{a^2}{4} = \left(x + \frac{a}{2}\right)^2 + b - \frac{a^2}{4}$$

$$\text{Sea } \beta = \alpha + \frac{a}{2} \Rightarrow f(\beta) = \left(\alpha + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} = 0 \Rightarrow \beta^2 = \left(\alpha + \frac{a}{2}\right)^2 = \frac{a^2}{4} - b \in F \quad \text{porque } a, b \in F$$

Claramente $\beta \in K \setminus F$ y $K = F(\alpha) = F(\beta)$

Ex 20-22 están repetidos

EJERCICIO 23. Razonar cuáles de los siguientes números complejos son algebraicos sobre \mathbb{Q} , suponiendo conocido que e y π son trascendentales:

$$\sqrt[5]{4}, (1 + \sqrt[5]{4})(1 - \sqrt[5]{16})^{-1}, \pi^2, e^2 - i, i\sqrt{i} + \sqrt{2}, \sqrt{1 - \sqrt[3]{2}}, \sqrt{\pi}, \sqrt{2}(\sqrt[3]{2} + \sqrt[5]{2})^{-1}.$$

$\sqrt[5]{4}$ es raíz de $x^5 - 4 \Rightarrow$ es algebraico

$(1 + \sqrt[5]{4})$ es raíz de $(x - 1)^5 - 4 \Rightarrow$ es algebraico

$(1 - \sqrt[5]{16})^{-1}$ es algebraico $\Leftrightarrow \underbrace{1 - \sqrt[5]{16}}_0$ lo es
es raíz de $(x - 1)^5 + 16 \Rightarrow$ es algebraico

π^2 sup que es algebraico $\Rightarrow \exists f(x) : f(\pi^2) = 0$ con $\deg f < \infty$, tomando $g(x) = f(x^2)$ $\Rightarrow g(\pi) = f(\pi^2) = 0 \Rightarrow \pi$ es algebraico!!!
 $\Rightarrow \pi^2$ es trascendente

$e^2 - i$ si fuera algebraico, $\exists f(x) : f(e^2 - i) = 0$, $\deg f < \infty$, tomando $g(x) = f(x^2 - i)$ $\Rightarrow g(e) = f(e^2 - i) = 0 \Rightarrow e$ es algebraico!!!
 $\Rightarrow e^2 - i$ trascendente $\underset{e \in \mathbb{C} \setminus \mathbb{Q}}{\Leftrightarrow} (e^2 - i \text{ algebraico en } \mathbb{Q} \Leftrightarrow e \text{ alg en } \mathbb{Q}(i))$

$i\sqrt{i} + \sqrt{2}$ alg en $\mathbb{Q} \Leftrightarrow$ es alg en $\mathbb{Q}(\sqrt{2}) \Leftrightarrow \underbrace{i\sqrt{i}}_{\text{es alg en } \mathbb{Q}(\sqrt{2})} \in \mathbb{Q}(\sqrt{2}) \Rightarrow$ es algebraico
es raíz de $x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$

$\sqrt{1 - \sqrt[3]{2}}$ es raíz de $(x^2 - 1)^3 + 2 \Rightarrow$ es algebraico

$$1 - \sqrt[3]{2} = \omega^2$$

$$\sqrt[3]{2} = \omega^2 - 1$$

$$-2 = (\omega^2 - 1)^3$$

$\sqrt{\pi}$ si fuera algebraico $\Rightarrow [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] < \infty$
como π es trascendente y $\pi \notin \mathbb{Q}(\sqrt{\pi}) \Rightarrow [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ no puede ser finita $\Rightarrow \sqrt{\pi}$ es trascendente

$[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] < \infty$ pero $\pi \in \mathbb{Q}(\sqrt{\pi})$ y π es trascendente $\Rightarrow [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ no puede ser finita!!! $\Rightarrow \sqrt{\pi}$ trascendente

$$\sqrt{2}(\sqrt[3]{2} + \sqrt[5]{2})^{-1}$$

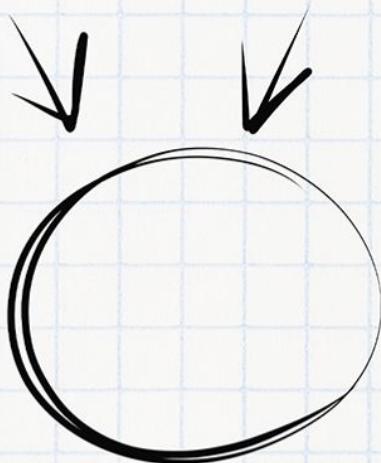
$$\frac{\sqrt[11]{2}}{2\sqrt[5]{2}} = \frac{\sqrt[6]{2^5}}{\sqrt[6]{2^2}} = \frac{\sqrt[6]{2^5}}{2} \quad \text{alg} \Leftrightarrow \underbrace{\sqrt[6]{2^5}}_{\text{raíz de } x^6 - 2} \text{ es alg} \Rightarrow \text{es algebraico}$$

Imagínate aprobando el examen

Necesitas tiempo y concentración

Planes	PLAN TURBO	PLAN PRO	PLAN PRO+
diamond Descargas sin publi al mes	10 🟡	40 🟡	80 🟡
clock Elimina el video entre descargas	✓	✓	✓
folder Descarga carpetas	✗	✓	✓
download Descarga archivos grandes	✗	✓	✓
circle Visualiza apuntes online sin publi	✗	✓	✓
glasses Elimina toda la publi web	✗	✗	✓
€ Precios	Anual <input type="checkbox"/>	0,99 € / mes	3,99 € / mes
			7,99 € / mes

Ahora que puedes conseguirlo,
¿Qué nota vas a sacar?



WUOLAH

EJERCICIO 24. Sea $F \leq K$ una extensión de cuerpos, $\alpha \in K$ y n natural no nulo. Demostrar que α es algebraico sobre F si, y sólo si, α^n es algebraico sobre F .

$$\begin{array}{l} F \leq K \\ \alpha \in K \\ n \in \mathbb{N} \end{array} \left\{ \begin{array}{l} \alpha \text{ alg sobre } F \Leftrightarrow \alpha^n \text{ es alg sobre } F \end{array} \right.$$

$$\Rightarrow \sup_{\alpha \text{ alg sobre } F} [\mathbb{F}(\alpha) : F] < \infty . \text{ Como } \alpha^n \in \mathbb{F}(\alpha) \Rightarrow \alpha^n \text{ pertenece a una extensión finita} \Rightarrow \alpha^n \text{ alg}$$

$$\Leftarrow \sup_{\alpha^n \text{ alg sobre } F} [\mathbb{F}(\alpha^n) : F] < \infty . \text{ Tomamos } p(x) = x^2 - \alpha^n \in \mathbb{F}(\alpha^n)[x] \Rightarrow p(\alpha) = 0 \Rightarrow [\mathbb{F}(\alpha, \alpha^n) : F] \leq n \Rightarrow [\mathbb{F}(\alpha^n) : F] < \infty \Rightarrow \alpha \text{ alg}$$

EJERCICIO 25. Sea $F \leq K$ una extensión de cuerpos, $\alpha \in K$ y $\beta = 1 + \alpha^2 + \alpha^5$. Demostrar que α es algebraico sobre F si, y sólo si, β es algebraico sobre F .

$$\begin{array}{l} F \leq K \\ \alpha \in K \\ \beta = 1 + \alpha^2 + \alpha^5 \end{array} \left\{ \begin{array}{l} \alpha \text{ alg sobre } F \Leftrightarrow \beta \text{ alg sobre } F \end{array} \right.$$

$$\Rightarrow \sup_{\alpha \text{ alg sobre } F} [\mathbb{F}(\alpha) : F] < \infty . \text{ Como } p \in \mathbb{F}(\alpha) \Rightarrow \beta \text{ pertenece a una extensión finita} \Rightarrow \beta \text{ es alg}$$

$$\Leftarrow \sup_{\beta \text{ alg sobre } F} [\mathbb{F}(\beta) : F] < \infty . \text{ Tomamos } p(x) = x^2 + x^5 - (\beta - 1) \Rightarrow p(\beta) = \alpha^2 + \alpha^5 - (1 + \alpha^2 + \alpha^5 - 1) = 0 \Rightarrow [\mathbb{F}(\alpha, \beta) : F] = \underbrace{[\mathbb{F}(\alpha, \beta) : \mathbb{F}(\beta)]}_{\leq 5} [\mathbb{F}(\beta) : F] < \infty \Rightarrow \alpha \text{ alg sobre } F$$

EJERCICIO 26. Calcular $\text{Irr}(\alpha, \mathbb{Q})$ para los siguientes valores de α :

$$3 + \sqrt{2}, \sqrt{3} - \sqrt[4]{3}, \sqrt[3]{2} + \sqrt[3]{4}.$$

$$\alpha = 3 + \sqrt{2} \quad \text{Claramente } \alpha \text{ es raíz de } g(x) = x^2 - 6x + 7 \text{ y este es irreducible en } \mathbb{Q} \text{ porque no tiene raíces}$$

$$(\alpha - 3)^2 = 2$$

$$\alpha^2 - 6\alpha + 9 = 2$$

$$\alpha^2 - 6\alpha + 7$$

$$\alpha = \sqrt{3} - \sqrt[4]{3} \quad \sqrt{3} \in \mathbb{Q}(\sqrt[4]{3}) \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[4]{3}) \Rightarrow \alpha - \sqrt{3} = -\sqrt[4]{3}$$

$$(\alpha - \sqrt{3})^2 = \sqrt{3}$$

$$\alpha^2 - 2\alpha\sqrt{3} + 3 = \sqrt{3}$$

$$\alpha^2 + 3 = \sqrt{3} + 2\alpha\sqrt{3}$$

$$\sqrt{3} = \frac{\alpha^2 + 3}{1 + 2\alpha} \Rightarrow 3 = \frac{(\alpha^2 + 3)^2}{(1 + 2\alpha)^2} \Rightarrow 3(1 + 4\alpha + 4\alpha^2) = \alpha^2 + 6\alpha + 9$$

$$3 + 12\alpha + 12\alpha^2 = \alpha^2 + 6\alpha + 9$$

$$\alpha^2 - 6\alpha - 12\alpha + 6$$

$$\alpha \text{ es raíz de } g(x) = x^4 - 6x^2 - 12x + 6 = \text{Irr}(\alpha, \mathbb{Q})$$

$$\alpha = \sqrt[3]{2} + \sqrt[3]{4} \quad \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2}) \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}) \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 = \deg(\text{Irr}(\alpha, \mathbb{Q}))$$

$$\alpha^3 = (\sqrt[3]{2} + \sqrt[3]{4})^3 = (\sqrt[3]{2} + \sqrt[3]{2}\sqrt[3]{2})^3 = (\sqrt[3]{2}(1 + \sqrt[3]{2}))^3 = 2(1 + \sqrt[3]{2})^3 = 2(1 + 2\sqrt[3]{2} + \sqrt[3]{4})(1 + \sqrt[3]{2}) = 2(1 + 2\sqrt[3]{2} + \sqrt[3]{4} + \sqrt[3]{2} + \sqrt[3]{4} + 2)$$

$$\alpha^3 = 2(1 + 3\sqrt[3]{2} + 3\sqrt[3]{4} + 2) = 2(3\alpha + 2) = 6\alpha + 6 \Rightarrow \alpha^3 - 6\alpha - 6 = 0 \Rightarrow \text{Irr}(\alpha, \mathbb{Q}) = x^3 - 6x - 6$$

EJERCICIO 29. Pongamos $\mathbb{F}_4 = \mathbb{F}_2(a)$ con $a^2 + a + 1 = 0$. Comprobar que \mathbb{F}_{16} puede presentarse como $\mathbb{F}_{16} = \mathbb{F}_2(b)$ donde $b^4 + b + 1 = 0$. Determinar todos los homomorfismos de cuerpos $\mathbb{F}_4 \rightarrow \mathbb{F}_{16}$ en función de a y b .

$$\mathbb{F}_4 = \mathbb{F}_2(a) \text{ con } a^2 + a + 1 = 0.$$

$$\mathbb{F}_{16} = \mathbb{F}_2(b) \text{ con } b^4 + b + 1 = 0$$

Veremos si $f(x) = x^4 + x + 1$ es irreducible \Rightarrow no tiene raíces simples mas $f(0) = 1$ y $f(1) = 1$
si descompone será como producto de dos factores de grado 2. Los trinomios irreducibles de grado 2 en \mathbb{F}_2 es $x^2 + x + 1$

Como $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f(x) \Rightarrow f(x)$ es irreducible $\Rightarrow \frac{\mathbb{F}_2[x]}{\langle x^4 + x + 1 \rangle}$ es un cuerpo de 16 elementos

Tomando $b = x + \langle f \rangle$ y se tiene $\mathbb{F}_{16} = \mathbb{F}_2(b)$ con $b^4 + b + 1 = 0$

Veremos todos los homomorfismos de $\mathbb{F}_4 \rightarrow \mathbb{F}_{16}$ en función de a y b

$$\begin{array}{ccc} & \sigma = i & \\ \text{Por el lema de extensión:} & \mathbb{F}_2 \xrightarrow{\sigma} \mathbb{F}_4 = \mathbb{F}_2(a) & \text{Irreducibles en } \mathbb{F}_2[x] \\ & \downarrow \eta & \text{Hay que buscar las raíces de } x^2 + x + 1 \text{ en } \mathbb{F}_2(b) \\ & \mathbb{F}_{16} = \mathbb{F}_2(b) & \end{array}$$

Veremos si $\mathbb{F}_{16}^\times = \langle b \rangle$ órdenes posibles de b : $\frac{1}{3} \rightarrow \text{no}$, $\frac{5}{5} \rightarrow \text{no}$, $\frac{15}{15} \rightarrow \text{si}$

Veremos si b^5 es raíz $\Rightarrow b^5 + b^3 + 1 = b^5(b+1) + b^3 + 1 = b^3 + b^2 + b^3 + 1 = b^2 + 1 \neq 0$

Veremos si b^5 es raíz $\Rightarrow b^{10} + b^5 + 1 = (b^5)^2 + b^5 \cdots (b+1)^2 + b^5 + 1 = (b^5 + 1)^2 + b(b+1)^2 + 1 = b+1 + b^2 + b^3 + b + 1 = 0$

$$1 \not\rightarrow b \not\rightarrow b^2 \not\rightarrow b^5 \not\rightarrow b^3 \not\rightarrow b^7 \not\rightarrow b^9 \not\rightarrow b^{11} \not\rightarrow b^{13} \not\rightarrow b^{14}$$

↑
10

$\Rightarrow b^5$ y b^{10} son las raíces de $x^2 + x + 1$

$$b^5 = b(b+1) = b^2 + b$$

$$b^{10} = (b^5)^2 = (b^2 + b)^2 = b^4 + b^2 = b^2 + b + 1$$

Luego hay dos homomorfismos

$$\begin{array}{ccc} \mathbb{F}_4 & \xrightarrow{\sigma} & \mathbb{F}_{16} \\ a \mapsto b^5 & & \\ a \mapsto b^{10} & & \end{array}$$

EJERCICIO 30. Demostrar que, si F es un cuerpo, entonces cualquier subgrupo finito de F^\times es cíclico. Deducimos que, en particular, \mathbb{F}_q^\times es un grupo cíclico de orden $q - 1$. (Pista: usar la descomposición cíclica de un grupo finito abeliano).

$$|\mathbb{F}_q| = q, |\mathbb{F}_q^\times| = q-1$$

Como \mathbb{F}_q^\times es el grupo multiplicativo de \mathbb{F}_q^\times , sabremos que es abeliano. Su descomposición cíclica es:

$$\mathbb{F}_q^\times \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \dots \oplus \mathbb{Z}_{d_t}, d_1, \dots, d_t > 1 \text{ y } d_i | d_{i+1} \quad \forall i = 1, \dots, t-1 \quad \text{y} \quad q-1 = d_1 \cdots d_t$$

Hacé \mathbb{F}_q^\times , orden d_i divide a algún d_j . Sea $p(x) = x^{d_j} - 1$, tenemos que $p(x) = 0 \Leftrightarrow x^{d_j} \in \mathbb{F}_q^\times \Rightarrow q-1 \leq d_j$

Como $q-1 = d_1 \cdots d_t \Rightarrow d_t \leq q-1 \Rightarrow \boxed{d_t = q-1} \Rightarrow \mathbb{F}_q^\times \cong \mathbb{Z}_{q-1} \Rightarrow \mathbb{F}_q^\times$ es cíclico

EJERCICIO 31. Demostrar los anillos $\mathbb{Z}[i]/\langle 3 \rangle$ y $\mathbb{F}_3[X]/\langle X^2 + X + 2 \rangle$ son isomorfos, sin necesidad de dar un isomorfismo concreto. ¿Serías capaz de darlo? ¿Y de calcularlos todos?

Por un lado $x^2 + x + 2$ es irred en \mathbb{F}_3 pues no tiene raíces simples ($f(0) = 2, f(1) = 1, f(2) = 2 \Rightarrow \# \mathbb{F}_3[x] = 3^2 = 9$)

Veremos que 3 es irred en $\mathbb{Z}[i]$. Supongamos $3 = zw$ con $z, w \in \mathbb{Z}[i] \Rightarrow N(z) = z\bar{z} \Rightarrow N(z) = 9 \neq 1$
(que no lo es)

$\Rightarrow 3$ es irred en $\mathbb{Z}[i] \Rightarrow \frac{\mathbb{Z}[i]}{\langle 3 \rangle}$ es un cuerpo

$$9 = N(z)N(w) = |z|^2|w|^2 \Rightarrow |z|^2 = 3 \Rightarrow a^2 + b^2 = 3$$

$\begin{matrix} z = a+bi \\ a, b \in \mathbb{Z} \end{matrix}$

Veamos que $\frac{\mathbb{Z}[i]}{\langle 3 \rangle}$ tiene 9 elementos. Sea $\alpha = 9 \cdot 3 + r$ con $N(r) < N(3) = 9$

Veamos todos los elementos de $\mathbb{Z}[i]/\langle 3 \rangle$ con norma < 9 $\Rightarrow 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i, 0 \Rightarrow$ son 9

Como el cuerpo de cardinal $9 = 3^2$ es único salvo isomorfismos $\Rightarrow \mathbb{Z}[i]/\langle 3 \rangle \cong \frac{\mathbb{F}_3[x]}{\langle x^2 + x + 2 \rangle}$

$$\text{Vemos } K = \frac{\mathbb{F}_3[x]}{\langle x^2 + x + 2 \rangle} = \mathbb{F}_3[\alpha] \text{ con } \alpha^2 + \alpha + 2 = 0$$

$$\text{llamó } U = \frac{\mathbb{Z}[i]}{\langle 3 \rangle}, \text{ con } \omega = \alpha$$



hay que calcular las raíces de $x^2 + x + 2$ en \mathbb{F}_3
teorema 2

$$\mathbb{F}_3 = \{0 + \langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$$

Raíces

Probaremos que todas cuadras da 0 en la ecuación

las raíces son $1+i$ y $1+2i$

$$\eta_1: \alpha \mapsto 1+i + \langle 3 \rangle$$

$$\eta_2: \alpha \mapsto 1+2i + \langle 3 \rangle$$

$$(1+i)^2 + (1+i) + 2 = -1+2i+i+(1+i)+2 = 3i+3 = 0$$

$$(1+2i)^2 + (1+2i) + 2 = 1+4i-4 + 1+2i+2 = 6i = 0$$

EJERCICIO 32. Realizar las siguientes tareas:

1. Probar que $\sqrt{3} \in \mathbb{Q}(\sqrt{1+2\sqrt{3}})$.
2. Calcular $\text{Irr}(\sqrt{1+2\sqrt{3}}, \mathbb{Q}(\sqrt{3}))$.
3. Describir todos los homomorfismos de cuerpos de $\mathbb{Q}(\sqrt{1+2\sqrt{3}})$ en \mathbb{C} .
4. Calcular $\text{Irr}(\sqrt{1+2\sqrt{3}}, \mathbb{Q})$ y sus raíces en \mathbb{C} .

$$1) \alpha = \sqrt{1+2\sqrt{3}}$$

$$\alpha^2 = 1+2\sqrt{3} \Rightarrow \alpha^2 - 1 = 2\sqrt{3} \Rightarrow \sqrt{3} = \frac{\alpha^2 - 1}{2} \in \mathbb{Q}(\alpha)$$

$$2) \text{Irr}(\alpha, \mathbb{Q}(\sqrt{3}))$$

sea $\varphi_{\alpha} = x^2 - (\alpha + 2\sqrt{3})$, claramente α es raíz de φ_{α} . Veamos que es irred en $\mathbb{Q}(\sqrt{3})$.

$\varphi_{\alpha}(0) = 0 \Leftrightarrow x^2 = \alpha + 2\sqrt{3} \Rightarrow x = \pm\sqrt{\alpha} \Rightarrow$ las únicas raíces son $\pm\sqrt{\alpha}$ y $\not\in \mathbb{Q}(\sqrt{3})$

Luego, $\text{Irr}(\alpha, \mathbb{Q}(\sqrt{3})) = x^2 - (\alpha + 2\sqrt{3})$

$$3) \mathbb{Q}(\sqrt{3}) \xrightarrow{\sigma} \mathbb{C}$$

$$\text{Irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3 \text{ y sus raíces son } \pm\sqrt{3} \Rightarrow \text{hay 2 ramas}$$

$$\begin{aligned} \sigma_1(\sqrt{3}) &= \sqrt{3} & \Rightarrow \sigma_1 = (-1)^{\frac{j}{2}} \\ \sigma_2(\sqrt{3}) &= -\sqrt{3} & j = 0, 1 \end{aligned}$$

$$4) \mathbb{Q}(\alpha) \xrightarrow{i} \mathbb{C}$$

$$\text{Irr}(\alpha, \mathbb{Q}(\sqrt{3})) = x^2 - (\alpha + 2\sqrt{3}) \text{ y sus raíces son } \pm\sqrt{\alpha} \text{ por cada ramo de } \alpha \text{ habrá 2 ramas:}$$

$$\eta_{11}(\alpha) = \sqrt{\alpha + 2\sqrt{3}} = \alpha \quad \eta_{21}(\alpha) = \sqrt{\alpha - 2\sqrt{3}}$$

$$\eta_{12}(\alpha) = -\sqrt{\alpha + 2\sqrt{3}} = -\alpha \quad \eta_{22}(\alpha) = -\sqrt{\alpha - 2\sqrt{3}}$$

$$5) \text{Irr}(\alpha, \mathbb{Q}), \text{raíces en } \mathbb{C}$$

$$\begin{aligned} [\mathbb{Q}(\alpha) : \mathbb{Q}] &= [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4 = \deg(\text{Irr}(\alpha, \mathbb{Q})) \\ &\text{irred por el} \\ &\text{apartado 2} \end{aligned}$$

$$\sqrt{3} = \frac{\alpha^2 - 1}{2} \Rightarrow \alpha = \frac{(\alpha^2 - 1)^2}{4}$$

$$\alpha = \alpha^4 - 2\alpha^2 + 1$$

$$\text{Irr}(\alpha, \mathbb{Q}) = x^4 - 2x^2 - 11. \text{ Sus raíces coinciden con las imágenes de los homomorfismos anteriores: } \alpha, -\alpha, \sqrt{1+2\sqrt{3}}, -\sqrt{1+2\sqrt{3}}$$

Ejercicio 18. Dados dos puntos distintos, dividir el segmento que determinan en tres partes iguales usando regla y compás.

Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato
→ Planes pro: más coins

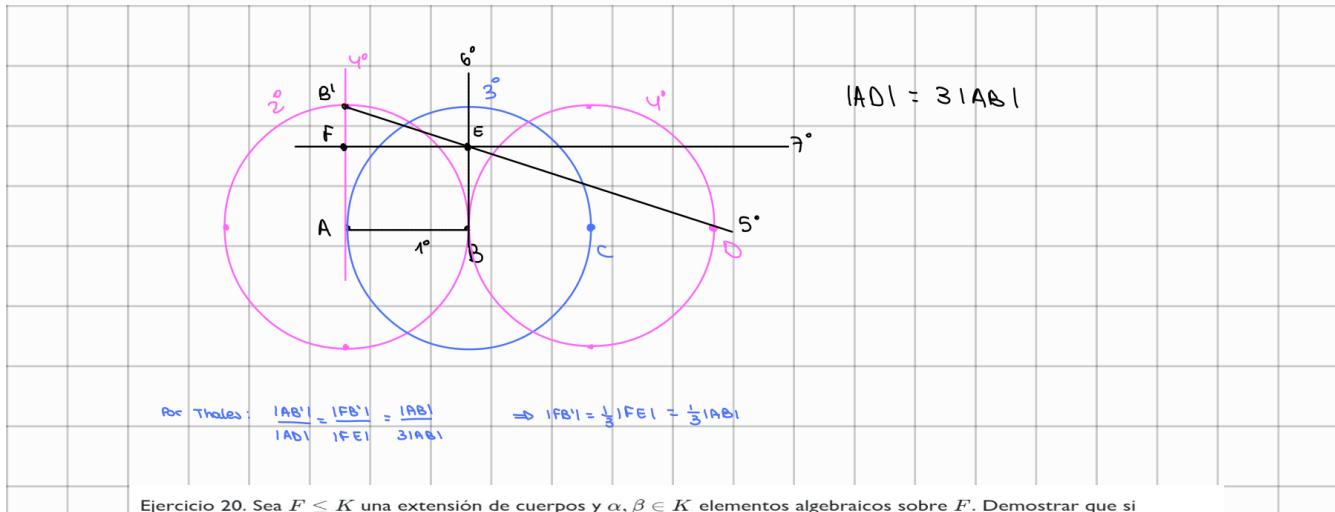
pierdo
espacio



Necesito
concentración

ali ali ooooh
esto con 1 coin me
lo quito yo...

wuolah



Ejercicio 20. Sea $F \leq K$ una extensión de cuerpos y $\alpha, \beta \in K$ elementos algebraicos sobre F . Demostrar que si $\text{Irr}(\alpha, F) = \text{Irr}(\beta, F)$, entonces existe un isomorfismo de cuerpos F -lineal $F(\alpha) \cong F(\beta)$.

EJERCICIO 10. Calcular $f(X) = \text{Irr}(1 + \sqrt[3]{2}, \mathbb{Q})$. Calcular las raíces complejas de $f(X)$ y un cuerpo de descomposición suyo.

$$\begin{aligned} \alpha &= 1 + \sqrt[3]{2} \\ \alpha - 1 &= \sqrt[3]{2} \\ (\alpha - 1)^3 &= 2 \Rightarrow \text{Irr}(1 + \sqrt[3]{2}, \mathbb{Q}) = (X - \alpha)^3 - 2 = X^3 - 3X^2 + 3X - 3 \quad (\text{es irreducible porque no tiene raíces}) \\ f'(x) &= -2x^2 + 6x - 10 \end{aligned}$$

Calculando las raíces: α es raíz y faltan otras dos raíces complejas (ω_0 y su conjugado)

$$\begin{aligned} &\frac{x^3 - 3x^2 + 3x - 3}{x^2 + 2x^2} \mid x - \alpha \\ &x^2 + 2x^2 \quad x^2 + (2\alpha - 3)x + (\alpha^2 - 3\alpha + 3) \\ &(2\alpha - 3)x^2 + 2x - 3 \\ &-(2\alpha - 3)x^2 - (2\alpha - 3)\alpha x \\ &\alpha^2 x - 2\alpha x + 3x - 3 \\ &\alpha^2 x^2 - 3\alpha x^2 + 3x - 3 \\ &-(\alpha^2 - 3\alpha + 3)x + (\alpha^2 - 3\alpha + 3)\alpha \\ &\alpha^2 - 3\alpha^2 + 3\alpha - 3 \\ &0 \quad (\text{porque } \alpha \text{ es raíz de } f) \end{aligned}$$

$$f(x) = (x - \alpha)(x^2 + (2\alpha - 3)x + (\alpha^2 - 3\alpha + 3))$$

ec. de 2º grado

$$x = \frac{-c \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-2\alpha + \sqrt{\alpha^2 - 6\alpha + 9 - 4\alpha^2 + 12\alpha - 12}}{2} = \frac{-2 + 3 \pm \sqrt{\alpha^2 - 6\alpha + 9 - 4\alpha^2 + 12\alpha - 12}}{2} = \frac{-2 + 3 \pm \sqrt{-3\alpha^2 + 6\alpha - 3}}{2} = \frac{-2 + 3 \pm \sqrt{-3(\alpha^2 - 2\alpha + 1)}}{2} = \frac{-2 + 3 \pm i\sqrt{3(\alpha^2 - 2\alpha + 1)}}{2}$$

El cuerpo de descomposición de f sería $\mathbb{Q}(\alpha, \omega_0, \bar{\omega}_0) = \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(1 + \sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$

EJERCICIO 17. Sea $\sigma : F \rightarrow E$ un homomorfismo de cuerpos tal que la extensión $\sigma(F) \leq E$ es finita. Demostrar que existe un polinomio $f \in F[X]$ y un homomorfismo de cuerpos $\tau : E \rightarrow K$ tal que $\tau\sigma : F \rightarrow K$ es cuerpo de descomposición de f .

•1 Tema 2

EJERCICIO 33. Supongamos que hemos expresado

$$\mathbb{F}_{16} = \{0, a, a^2, \dots, a^{15}\}.$$

Expresar, usando potencias de a , todos los subcuerpos de \mathbb{F}_{16} .

$$16 = 2^4 \Rightarrow \text{divisores de } 4 \quad | \quad \begin{array}{l} \text{el subcuerpo primo } \mathbb{F}_2 \\ | \quad 2 \quad \text{el total } \mathbb{F}_{16} \\ | \quad 4 \end{array}$$

$\mathbb{F}_4 \Rightarrow \mathbb{F}_4^\times \text{ es cíclico de orden } 3 \Rightarrow \mathbb{F}_4^\times = \langle a^5 \rangle \Rightarrow \mathbb{F}_4 = \{0, a^5, a^{10}, 1\}$

EJERCICIO 34. Generalizar la descripción de los subcuerpos de cualquier \mathbb{F}_q según la pauta descrita en el Ejercicio 33.

$$\mathbb{F}_q \text{ con } q = p^n \Rightarrow \text{Tomo los divisores de } n \text{ y hay un subcuerpo por cada divisor de orden } p^d$$

Hay dos subcuerpos triviales que son el subcuerpo primo \mathbb{F}_p y el total \mathbb{F}_q .

Para el resto de subcuerpos de la forma \mathbb{F}_{p^d} , sabemos que $\mathbb{F}_{p^d}^\times$ es cíclico de orden $p^d - 1$. Buscamos el generador del grupo cíclico que sea a^{p^d-1} .

EJERCICIO 35. Sea $F \leq K$ una extensión de Galois de grado 3^n . Demostrar que, para cada $1 \leq i \leq n$, existe una subextensión $F \leq E \leq K$ tal que $[E : F] = 3^i$.

$$[K:F] = 3^n \Rightarrow \forall i \in \{1, \dots, n\} \quad [E:F] = 3^i$$

Como $F \leq K$ es Galois $\Rightarrow E \leq K$ es Galois. Por el Thm Sylow

Como $[K:F] = 3^n = \# \text{Aut}_F(K) \Rightarrow \text{Aut}_F(K)$ es un p -grupo \Rightarrow \exists subgrupo G_i de $\text{Aut}_F(K)$ / $\# G_i = 3^i$

Por la convención, viendo $1, \dots, n$ tomo $E_i = K^{G_i}$, $[E_i : F] = 3^i$

EJERCICIO 36. Supongamos que tenemos cuerpos $F \leq E \leq K$ tales que $F \leq E$ y $E \leq K$ son extensiones de Galois. ¿Es necesariamente $F \leq K$ de Galois?

$$\begin{array}{c} F \leq E \leq K \xrightarrow{\text{Galos}} F \leq K \text{ Galos} \\ \text{Galos} \quad \# \text{Aut}_E(W) \\ [K:F] = [K:E][E:F] \quad \# \text{Aut}_E(W) \\ \quad \quad \quad \# \text{Aut}_F(E) \\ \hookrightarrow \# \text{Aut}_F(K) \quad \left| \begin{array}{l} \# \text{Aut}_F(W) \\ \text{separable} \\ K \text{ celd} \end{array} \right. \\ Q \subseteq Q(\sqrt[3]{2}, W) \subseteq Q(\sqrt[3]{2}, W, \sqrt[3]{2}) \\ Q \subseteq Q(\sqrt[3]{2}, W, \sqrt[3]{2}) \end{array}$$

Ejercicio 26. Sea $F \leq E$ una extensión finita. Demostrar que el orden de $\text{Aut}_F(E)$ es un divisor de $[E : F]$.

$$\text{Sea } G = \text{Aut}_F(E) \text{ y } H = E^G \text{ el subcuerpo fijo por } G. \text{ Como } [E:F] \text{ es finito} \Rightarrow G \text{ también lo es} \Rightarrow \# G = [E:H]$$

Por el lema de la torre, $[E:F] = [E:H][H:F] = \# G \cdot [H:F] \Rightarrow \# G \mid [E:F]$ teorema

Ejercicio 28. Sea $f \in F[X]$ un polinomio separable e irreducible de grado primo p . Demostrar que el grupo de Galois de f sobre el cuerpo F contiene un ciclo de orden p . (Pista: usar el Teorema de Cauchy de existencia de p -subgrupos).

$$\begin{array}{l} \# \text{FC}(f), \deg f = p \text{ primo} \\ \text{Sea } K \text{ el celd de } p \text{ con } d_1, \dots, d_p \text{ raíces} \Rightarrow [K:F] = [F(d_1, \dots, d_p) : F(d_1, \dots, d_{p-1})] \cdots [F(d_1) : F] \xrightarrow{\text{p divide a } [K:F]} \\ \text{Como } F \leq K \text{ es de Galois (por ser } p \text{ separable e irreducible)} \Rightarrow \# \text{Aut}_F(K) = [K:F] \\ \text{Luego, } p \mid \# \text{Aut}_F(K). \text{ Por el Thm Cauchy, } \# \text{Aut}_F(K) = G \text{ tiene un elemento de orden } p. \\ \text{Los únicos elementos de orden } p \text{ en } \mathbb{Z}_p \text{ son los } p\text{-ciclos} \Rightarrow G \text{ tiene un ciclo de orden } p \end{array}$$

Ejercicio 29. Sea $f \in \mathbb{Q}[X]$ irreducible de grado primo p . Demostrar que, si f tiene exactamente dos raíces complejas no reales, entonces el grupo de Galois de f sobre \mathbb{Q} es isomorfo a S_p . (Pista: usar el Ejercicio 28).

Como tiene dos raíces complejas, estas son conjugadas. Tomando a_1, \dots, a_{p-2} raíces reales, consideramos $E = \mathbb{F}(a_1, \dots, a_{p-2})$

$\text{Irr}(a_p, E) = \text{Irr}(a_{p-1}, E)$ y tiene grado 2 \Rightarrow sea $h(a_p) = a_{p-1}$, $h(E) = E$ es un automorfismo de $K \Rightarrow h \in \text{Aut}_\mathbb{Q}(K)$ y tiene orden 2

como el grupo S_n se puede generar con un n-ciclo y un 2-ciclo. Por el ej 28, tenemos un p-ciclo y hemos visto que h es un 2-ciclo $\Rightarrow \text{Aut}_\mathbb{Q}(K) \cong S_p$

Ejercicio 30. Estudiar si la extensión $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5})$ es de Galois. (es el "ejemplo de Halloween")

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) = E$ será de Galois si es normal y separable.

Como tiene que ser normal \Rightarrow el $\text{Irr}(a)$ descompone como producto de polinomios irreducibles de $\mathbb{Q}[x]$.

es claro que $[\mathbb{E} : \mathbb{Q}] = [\mathbb{E} : (\mathbb{Q}(\sqrt[3]{5}))][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 6$

$x^3 - 5$ es
irred en
 $\mathbb{Q}(\sqrt[3]{5})$ pues
sus raíces son
complejas y no están
en $\mathbb{Q}(\sqrt[3]{5})$

$x^2 + 5$ es irred por
Eisenstein para $p=5$

Teniendo $\text{Irr}(\sqrt[3]{5}, \mathbb{Q}) = x^3 - 5$, sus raíces son $\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}$ con $\omega = e^{\frac{i2\pi}{3}} = \frac{1}{2} + \frac{\sqrt{3}}{2}i \Rightarrow \sqrt[3]{5} \in E$

Si la extensión es de Galois $\Rightarrow \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) \leq E$

pero $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) = \mathbb{Q}(\sqrt[3]{5}, \frac{\sqrt{5}}{2}i)$ y $[\mathbb{Q}(\sqrt[3]{5}, \frac{\sqrt{5}}{2}i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5}, \frac{\sqrt{5}}{2}i) : \mathbb{Q}(\frac{\sqrt{5}}{2}i)][\mathbb{Q}(\frac{\sqrt{5}}{2}i) : \mathbb{Q}] = 4$

Pero 4 no divide a 6 !!! $\mathbb{Q} \leq E$ no es de Galois

EJERCICIO 37. Sea $\overline{\mathbb{Q}}$ la clausura algebraica de \mathbb{Q} en \mathbb{C} . Razonar que todo polinomio no constante $f \in \overline{\mathbb{Q}}[X]$ tiene todas sus raíces en $\overline{\mathbb{Q}}$.

Importante

Puedo eliminar la publi de este documento con 1 coin

→ Plan Turbo: barato
→ ¿Cómo consigo coins?
→ Planes pro: más coins

pierdo
espacio



Necesito
concentración

ali ali ooooh
esto con 1 coin me
lo quito yo...

wuolah

→ Tema 3

EJERCICIO 38 (Identidades de Cardano-Vieta). Sea $f \in F[X]$ un polinomio mónico de grado n con raíces $\alpha_1, \dots, \alpha_n$ en un cuerpo de descomposición suyo (no suponemos que f sea separable, así que entre las raíces puede haber repeticiones). Definamos

$$s_k = \sum_{1 < i_1 < \dots < i_k < n} \alpha_{i_1} \cdots \alpha_{i_k}.$$

para $k = 1, \dots, n$. Demostrar que

$$f = X^n - s_1 X^{n-1} + \dots + (-1)^n s_n.$$

EJERCICIO 41. Demostrar que el grupo de Galois de $f = X^5 - 4X - 1 \in \mathbb{Q}[X]$ es isomorfo a S_5 .

$f(x) = x^5 - 4x - 1 \in \mathbb{Q}[x]$. Veamos que f es irreducible. Reduciendo módulo 3 tenemos $\tilde{f} = x^5 + 2x + 2 \in \mathbb{F}_3[x]$. $\tilde{f}(0) = 2$, $\tilde{f}(1) = 2$, $\tilde{f}(2) = 2 \Rightarrow \tilde{f}$ no tiene raíces simples. Si descompone lo haría como un factor de grado 2 y otro de grado 3. Los factores irreducibles de grado 2 en $\mathbb{F}_3[x]$ son

$$\begin{array}{l} x^2 + 2x + 2 \\ x^2 + 1 \\ x^2 + x + 2 \end{array}$$

Veamos que ninguno divide a \tilde{f} :

$$\begin{array}{r} x^5 + 2x + 2 \mid x^2 + 1 \\ x^5 - x^3 \\ \hline 2x^3 + 2x + 2 \\ -2x^3 - 2x \\ \hline 2 \end{array}$$

$$\begin{array}{r} x^5 + 2x + 2 \mid x^2 + 2x + 2 \\ -x^5 - 2x^3 - 2x \\ \hline x^4 + 2x^2 + 2x + 2 \\ -x^4 - 2x^2 - 2x \\ \hline 2x^2 + 2x + 2 \\ -2x^2 - 2x - x \\ \hline x + 2 \end{array}$$

$$\begin{array}{r} x^5 + 2x + 2 \mid x^2 + x + 2 \\ -x^5 - x^3 - 2x^2 \\ \hline 2x^4 + x^3 + 2x + 2 \\ -2x^4 - 2x^3 - x^2 \\ \hline 2x^3 + 2x^2 + 2x + 2 \\ -2x^3 - 2x^2 - x \\ \hline x + 2 \end{array}$$

Luego, \tilde{f} es irreducible en $\mathbb{F}_3[x] \Rightarrow f$ es irreducible en $\mathbb{Q}[x] \Rightarrow$ el grupo de Galois G actúa transitivamente sobre las raíces de f .

Como $\deg f = 5$, G es un subgrupo transitivo de $S_5 \Rightarrow G$ contiene un 5-ciclo

Reduciendo módulo 2: $\tilde{f} = x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$

\Rightarrow Dedekind

el grupo de Galois de f tiene una permutación $\sigma = (abcd)$

A continuación, como hoy una raíz simple $(x+1)$ y un 4-ciclo, existe una permutación que intercambia la raíz simple con alguna de las raíces de $x^4 + x^3 + x^2 + x + 1$

Como el grupo de Galois de f contiene un 5-ciclo y una transposición, tenemos que $G \cong S_5$

Como S_5 se puede generar con un 4-ciclo y una transposición, tenemos que $G \cong S_5$

EJERCICIO 42. Calcular, en característica 0, Φ_8 .

$$x^8 - 1 = \phi_1 \phi_2 \phi_4 \phi_8$$

$$\begin{aligned} \phi_1 &= x - 1 \\ \phi_2 &= x + 1 \\ \phi_4 &= x^2 + 1 \end{aligned} \Rightarrow x^8 - 1 = \phi_1 \phi_2 \phi_4 \Rightarrow x^8 - 1 = (x^4 - 1) \phi_8$$

$$\begin{array}{r} x^8 - 1 \mid x^4 - 1 \\ -x^8 + x^4 \\ \hline x^4 - 1 \\ -x^4 + 1 \\ \hline 0 \end{array} \Rightarrow x^8 - 1 = (x^4 - 1)(x^4 + 1) \quad \text{|| } \phi_8$$

EJERCICIO 43. Demostrar que un polígono regular de n lados es constructible si, y sólo si, n es producto de una potencia de 2 y primos de Fermat distintos entre sí.

\Rightarrow los lados de un polígono regular vienen dados por una extensión cíclica.

El polígono será constructible $\Leftrightarrow \varphi(n) : 2^k$ es una potencia de 2 $\Rightarrow \varphi(n) = 2^n$ con $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$

$$\Rightarrow \varphi(n) = (p_1 - 1)p_1^{e_1 - 1} \cdot (p_2 - 1)p_2^{e_2 - 1} \cdots (p_m - 1)p_m^{e_m - 1}$$

Si $p_1 = 2 \Rightarrow e_1 \cdots e_m = 1$, ya que en caso contrario $p_m | 2^k$!!! $\Rightarrow \varphi(n) = (2 - 1)2^{e_1 - 1} (p_2 - 1) \cdots (p_m - 1) \Rightarrow p_1 - 1 = 2^k \Rightarrow p_1 = 2^{k+1}$
 $\Rightarrow p_1$ es un primo de Fermat

\Leftrightarrow si $n = 2^k \cdot p_1 \cdots p_m$ con p_i primos de Fermat distintos $\Rightarrow \varphi(n) = 2^{k-1} (p_2 - 1) \cdots (p_m - 1) = 2^N$, NEIN \Rightarrow es constructible

EJERCICIO 44. Razonar que toda extensión de cuerpos finitos es cíclica.

EJERCICIO 45. Supongamos que el polinomio $f = X^n - a \in F[X]$ es separable, con $a \neq 0$, y sea K su cuerpo de descomposición. Denotemos por $\zeta \in K$ una raíz primitiva n -ésima de la unidad, y $\sqrt[n]{a} \in K$ una raíz de f . Dado $\sigma \in \text{Aut}_F(K)$, denotemos por $j(\sigma), k(\sigma) \in \mathbb{Z}_n$ determinados por las condiciones $\sigma(\sqrt[n]{a}) = \zeta^{j(\sigma)} \sqrt[n]{a}, \sigma(\zeta) = \zeta^{k(\sigma)}$. Demostrar que la aplicación

$$\text{Aut}_F(K) \rightarrow \text{GL}_2(\mathbb{Z}_n), \quad (\sigma \mapsto \begin{pmatrix} 1 & 0 \\ j(\sigma) & k(\sigma) \end{pmatrix}).$$

es un homomorfismo inyectivo de grupos. Deducir que $\#\text{Aut}_F(K)$ es un divisor de $n\varphi(n)$. En el caso $F = \mathbb{Q}$, deducir que $\#\text{Aut}(K) = n\varphi(n)$ si, y sólo si, $X^n - a \in \mathbb{Q}(\zeta)[X]$ es irreducible.

EJERCICIO 46. Sea $K = \mathbb{Q}(\sqrt[4]{5}, i)$.

1. Razonar que K es una extensión de Galois de \mathbb{Q} y calcular el cardinal de su grupo de Galois.
2. Describir los elementos del grupo $\text{Aut}(K)$.
3. Calcular todos los subcuerpos de K que tienen grado 4 sobre \mathbb{Q} .
4. Calcular todos los subcuerpos de K .

1) Como $i \in K$ es una raíz cuarta primaria de la unidad, K es celd de $x^4 - 5 \in \mathbb{Q}[x]$ irreducible (por Eisenstein con $p=5$) y $\mathbb{Q} \subseteq K$ es de Galois. Además, $\#\text{Aut}(K) = [K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = \frac{[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}][\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})]} = 2 \cdot 4 = 8$
 $x^2 + 1$ es irreducible

2) Por la proposición de extensión: $\mathbb{Q}(\sqrt[4]{5}) \xrightarrow{\tau_0} K$ $\tau_0(\sqrt[4]{5}) = \sqrt[4]{5}$ $j=0, 1, 2, 3$ (raíces de $x^4 - 5$)
 " " " $K \longrightarrow K$ $\tau_k(1) = i^k$ $k=1, 3$ (raíces de $x^2 + 1$)

Luego, $\text{Aut}(K) = \langle \tau_{j,k} : j \in \mathbb{Z}_4, k \in \mathbb{Z}_2 \rangle$

3) Por la teoría de Galois, los subcuerpos de K de grado 4 corresponden a los subgrupos de $\text{Aut}(K)$ de índice 4 (es decir, los elementos de orden 2)

Calculamos los órdenes:

orden 2

$\langle \tau_{j,k} \rangle$ de orden 2.

$$\tau_{jk}(\sqrt[4]{5}) = \tau_{jk}(\tau_{jk}(\sqrt[4]{5})) = \tau_{jk}(i^4 \sqrt[4]{5}) = \tau_{jk}(1) \circ \tau_{jk}(\sqrt[4]{5}) = (i^k)^4 \circ i^4 \sqrt[4]{5} = i^{4k} \circ i^4 \sqrt[4]{5} = i^{4(k+1)} \sqrt[4]{5}$$

$$\tau_{jk}(\sqrt[4]{5}) = \tau_{jk}(i^k) = (i^k)^k = i^{k^2}$$

$$\Rightarrow \tau_{jk}^2 = \tau_{0,0} \Leftrightarrow \begin{cases} \delta(k+1) = 0 \\ k^2 = 1 \end{cases} \quad \begin{matrix} \text{(en } \mathbb{Z}_4, \text{ } \delta(2k) = 0) \\ \text{(en } \mathbb{Z}_4, \text{ } k=1) \end{matrix} \quad \Rightarrow k=1 \text{ se cumple siempre } (1^2 = 1, 3^2 = 9 = 1 \pmod 4) \\ \delta(k+1) = 0 \quad \begin{matrix} \text{---} \\ k=1 \Rightarrow 2j=0 \\ \delta=0 \end{matrix} \\ \delta=2 \\ \text{---} \\ k=3 \Rightarrow 4j=0 \text{ todo} \end{matrix}$$

$\tau_{0,0}$	$\tau_{1,0}$	$\tau_{2,0}$	$\tau_{3,0}$	$\tau_{0,1}$	$\tau_{1,1}$	$\tau_{2,1}$	$\tau_{3,1}$
1	4	2	4	2	2	2	2

G

Como hay 5 elementos de orden 2 sabemos que $\text{Aut}(K) \cong D_4 \Rightarrow$ el resto tiene orden 4

Subgrupos de D_4 $\begin{cases} 3 \text{ de orden 2} \\ 3 \text{ de orden 4 (uno cíclico y dos de Klein } \cong \text{)} \end{cases}$

Calculamos las extensiones de \mathbb{Q} de grado 4 dentro de K (los subcuerpos de grado 4) a partir de los subgrupos de orden 2. Los "darios" son $\mathbb{Q}(\sqrt[4]{5}), \mathbb{Q}(\sqrt[4]{-5}), \mathbb{Q}(\sqrt{-5})$
 Raíces de $x^4 - 5$

$\mathbb{Q}(\sqrt[4]{5})$: buscar uno que lo deje invariante: $\tau_{2,1}(\sqrt[4]{5}) = -\sqrt[4]{5}$ NO $\tau_{0,1}(\sqrt[4]{5}) = \sqrt[4]{5}$ SI
 $\mathbb{Q}(\sqrt[4]{5}) \subseteq K^{\langle \tau_{0,1} \rangle} \Rightarrow \mathbb{Q}(\sqrt[4]{5}) = K^{\langle \tau_{0,1} \rangle}$
 Cada grupo Galois

$$[K^{\langle \tau_{0,1} \rangle} : \mathbb{Q}] = (G : \langle \tau_{0,1} \rangle) = 4$$

" "

" "

$\mathbb{Q}(\sqrt[4]{-5})$: $\tau_{2,1}(\sqrt[4]{-5}) = \tau_{2,1}(i) \tau_{2,1}(\sqrt[4]{5}) = i^2 \sqrt[4]{5} = -i \sqrt[4]{5}$ NO
 $\tau_{2,1}(\sqrt[4]{-5}) = i^2 i^3 \sqrt[4]{5} = i^4 \sqrt[4]{5} = 1 \sqrt[4]{5}$ SI $\Rightarrow \mathbb{Q}(\sqrt[4]{-5}) = K^{\langle \tau_{2,1} \rangle}$ (explicación análoga a la anterior)

$\mathbb{Q}(\sqrt{-5})$: $\tau_{2,1}(\sqrt{-5})$
 $\tau_{2,1}(\sqrt{-5}) = \tau_{2,1}(\sqrt{5})^2 = \sqrt{5}$ $\Rightarrow \mathbb{Q}(\sqrt{-5}) = K^{\langle \tau_{2,1} \rangle}$
 $\tau_{2,1}(i) = i$

No faltan dos:

$$\Rightarrow \alpha = \sqrt[4]{5}(1+i)$$

$$\tau_{1,1}(\alpha) = \tau_{1,1}(\sqrt[4]{5}) + \tau_{1,1}(i\sqrt[4]{5}) = (\sqrt[4]{5} + \tau_{1,1}(i)) \tau_{1,1}(\sqrt[4]{5}) = i\sqrt[4]{5} - i(\sqrt[4]{5}) = i\sqrt[4]{5} + \sqrt[4]{5} = \sqrt[4]{5}(1+i) = \alpha$$

$$\Rightarrow \mathbb{Q}(\alpha) \subseteq K^{\langle \tau_{1,1} \rangle}$$

$$[K^{\langle \tau_{1,1} \rangle} : \mathbb{Q}] = (G : \langle \tau_{1,1} \rangle) = 4 \Rightarrow \mathbb{Q}(\alpha) = K^{\langle \tau_{1,1} \rangle}$$

" "

" "

Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato
→ Planes pro: más coins

pierdo
espacio



Necesito
concentración

ali ali ooooh
esto con 1 coin me
lo quito yo...

wuolah

$$\begin{aligned} \Rightarrow \beta = \sqrt[4]{5}(1-i) \Rightarrow \text{ord}(\beta) = \text{ord}(\sqrt[4]{5}) - \text{ord}(i) = \text{ord}(\sqrt[4]{5}) = -i\sqrt{5} + \frac{i^3\sqrt{5}}{2} = \sqrt{5}(1-i) = \beta \\ \beta \in K^{<\text{cub}>} \Rightarrow Q(\beta) \leq K^{<\text{cub}>} \\ [K^{<\text{cub}>} : Q] = (\mathbb{G} : <\text{cub}>) = 4 \Rightarrow Q(\alpha) = K^{<\text{cub}>} \end{aligned}$$

4) Calculamos ahora los subcuerpos de grado 2 \Rightarrow los subgrupos de 4 elementos.

que son Galois

Hay 3: uno cíclico y dos \cong Klein. Los demás son $(\mathbb{Q}(\sqrt{5}), Q(\sqrt{5}))$

$$Q(\text{cub}): \tau_1(i) = i, \tau_2(i) = -i \Rightarrow \langle i, K^{<\text{cub}>} \rangle \rightarrow Q(\text{cub}) \leq K^{<\text{cub}>} \quad \langle \tau_1, \tau_2 \rangle = \langle \tau_2 \rangle \text{ son los generadores del mismo grupo cíclico } Q$$

$$Q(\sqrt{5}): \tau_1(\sqrt{5}) = \tau_2(\sqrt{5})^2 = (\sqrt[4]{5})^2 = -\sqrt{5} \Rightarrow \sqrt{5} \in K^{<\text{cub}>} \Rightarrow Q(\sqrt{5}) \leq K^{<\text{cub}>} \Rightarrow Q(\sqrt{5}) = K^{<\text{cub}, \sqrt{5}>}$$

$$Q(\sqrt{5}): \tau_1(\sqrt{5}) = \tau_2(\sqrt{5}) \tau_3(\sqrt{5})^2 = i^2 (\sqrt[4]{5})^2 = i\sqrt{5} \Rightarrow \langle \sqrt{5} \in K^{<\text{cub}>} \rangle \rightarrow Q(\sqrt{5}) \leq K^{<\text{cub}>} \Rightarrow Q(\sqrt{5}) = K^{<\text{cub}, \sqrt{5}>}$$

Subcuerpos de K

$$Q(\sqrt{5}) = K^{<\text{cub}>}$$

$$Q(\sqrt[4]{5}) = K^{<\text{cub}>}$$

$$Q(\sqrt{5}, \sqrt{5}) = K^{<\text{cub}>}$$

$$Q(\sqrt[4]{5}, \sqrt{5}) = K^{<\text{cub}>}$$

$$Q(\sqrt[4]{5}(\sqrt{5})) = K^{<\text{cub}>}$$

subcuerpos de grado 4

$$Q(\text{cub}) = K^{<\text{cub}>}$$

$$Q(\sqrt{5}) = K^{<\text{cub}, \sqrt{5}>}$$

$$Q(\sqrt{5}, \sqrt{5}) = K^{<\text{cub}, \sqrt{5}>}$$

Sabemos que $Q(\sqrt{5})$ es el menor subcuerpo que contiene a cub y $Q(\sqrt{5}) \Rightarrow$ su grupo correspondiente $K^{<\text{cub}>}$ es el mayor subgrupo contenido en ambos

$$\tau_1, \tau_2, \tau_3$$

$$\text{Aut}_{\mathbb{Q}(\sqrt{5})}(K) = \{\text{id}, \tau_2, \tau_3, \tau_2\tau_3\}$$

$$\text{cub}(\sqrt{5}) = \text{cub}(\sqrt{5})^2 = (\sqrt[4]{5})^2 = \sqrt{5}$$

$$\tau_2(\sqrt{5}) = \tau_2(\sqrt{5})^2 = \sqrt{5}$$

$$\text{Aut}_{\mathbb{Q}(\sqrt{5})}(K) = \{\text{id}, \tau_2, \tau_3, \tau_2\tau_3\}$$

$$\tau_3(\sqrt{5}) = \tau_3(\sqrt{5}) \tau_2(\sqrt{5})^2 = i\sqrt{5}$$

$$\tau_2\tau_3(\sqrt{5}) = \tau_2(\tau_3(\sqrt{5})) = \tau_2(-i\sqrt{5})^2 = i\sqrt{5}$$

EJERCICIO 47. Sea $f \in F[X]$ y L un cuerpo de descomposición de f sobre F . Demostrar que, para cualquier extensión $F \leq E$, si K es cuerpo de descomposición de f sobre E , entonces $\text{Aut}_E(K)$ es isomorfo a un subgrupo de $\text{Aut}_F(L)$.

EJERCICIO 48. Demostrar que el discriminante de una resolvente cúbica, de entre las definidas durante este curso, de una cuártica coincide con el de ésta.

Ejercicio 33. Demostrar que, para un número natural impar n , las extensiones ciclotómicas n y $2n$ -ésima de \mathbb{Q} (dentro de \mathbb{C}) son iguales.

Ejercicio 34. Calcular las extensiones ciclotómicas de grado 2 de \mathbb{Q} .

Ejercicio 35. Describir el retículo de subcuerpos de la decimosexta extensión ciclotómica de \mathbb{Q} .

Ejercicio 36. Describir el retículo de subcuerpos de la séptima extensión ciclotómica de \mathbb{F}_2 .

EJERCICIO 61. Sea F un cuerpo de descomposición de $f = X^6 + X + 1 \in \mathbb{F}_2[X]$ y $\alpha \in F$ una raíz de f .

1. Razonar que $F = \mathbb{F}_2(\alpha)$.
2. Calcular el orden multiplicativo de α .
3. Resolver en F , expresando las soluciones en función de α , la ecuación $x^2 + x + 1 = 0$.

EJERCICIO 49. Determinar, salvo isomorfismos, el grupo de Galois del polinomio $X^4 + X + 1 \in \mathbb{Q}[X]$.

$f(x) = x^4 + x + 1 \in \mathbb{Q}[x]$. Veamos que es irreducible. Reduciendo módulo 2, $\tilde{f} = x^4 + x + 1$ no tiene raíces simples

$$\begin{aligned}\tilde{f}(0) &= 1 \\ \tilde{f}(1) &= 1\end{aligned}$$

Si \tilde{f} descompone lo hará como producto de dos irreducibles de grado 2.

Los irreducibles de grado 2 en \mathbb{F}_2 son: $x^2 + x + 1 \Rightarrow (x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1 \Rightarrow \tilde{f}$ es irreducible $\Rightarrow f$ es irreducible

Como f es irreducible \Rightarrow su grupo de Galois es un subgrupo transitivo de S_4 .

Calcularemos el discriminante de f :

$$\text{La resolvente cúbica de } f \text{ es } g = \underbrace{x^3 - 4x - 1}_{p} \underbrace{-1}_{q} \Rightarrow \text{Disc}(f) = \text{Disc}(g) = -4p^3 - 27q^2 = 256 - 27 = 229$$

229 es un entero primo ya que no es divisible por 2, 3, 5, 7, 11, 13 $\Rightarrow x^2 - 229 \in \mathbb{Z}[x]$ es irreducible por Eisenstein

$\Rightarrow \mathbb{F}_{229} \neq \mathbb{Q} \Rightarrow$ como el $\text{disc}(f)$ no es un cuadrado en $\mathbb{Q} \Rightarrow G$ no está incluido en A_4

Además, g es irreducible en $\mathbb{Q}[x]$ pero no tiene raíces ($g(1) = -1, g(-1) = 2$) \Rightarrow el grupo de Galois de g es un subgrupo transitivo de S_3 que no es $A_3 \Rightarrow$ es S_3

Sea $E = \mathbb{Q}(p_1, p_2, p_3)$ y $K = \mathbb{Q}(p_1, p_2, p_3, p_4)$ los cdd de g y de f tenemos: $\mathbb{Q} \subseteq E \subseteq K$

La conexión de Galois nos da: $\text{Aut}(K) = \text{Aut}(E) \cong \text{id}$

Por lo anterior tenemos $\text{Aut}(E)$ es normal en $\text{Aut}(K)$ y $\text{Aut}(E) \cong \text{Aut}(K)/\text{Aut}(E)$. Como $\text{Aut}(E) \cong S_3 \Rightarrow \text{Aut}(E)$ tiene cardinal un múltiplo de 6

Como es un subgrupo transitivo de S_4 que no es A_4 , la única posibilidad es que sea S_4 .

EJERCICIO 50. Sea F un cuerpo de descomposición de $f = X^3 + X + 1 \in \mathbb{F}_2[X]$ y $\alpha \in F$ una raíz de f . Razonar que $F = \mathbb{F}_2(\alpha)$. Resolver, en F , las siguientes ecuaciones, expresando las soluciones en función de α :

$$x^3 + x + 1 = 0; \quad x^3 + x^2 + 1 = 0; \quad x^2 + x + 1 = 0.$$

$f = x^3 + x + 1 \in \mathbb{F}_2[x]$, de f raíz de α
cdd de f

$\Rightarrow F = \mathbb{F}_2(\alpha)$

$\alpha^0 = 1 \wedge \alpha^3 = 0 \Rightarrow f$ es irreducible $\Rightarrow [\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \deg f = 3 \Rightarrow \mathbb{F}_2(\alpha)$ es un cuerpo con $2^3 = 8$ elementos

Además, $\mathbb{F}_2 \subset \mathbb{F}_2(\alpha)$ es de Galois por ser una extensión de cuerpos finitos

Como f tiene una raíz en $\mathbb{F}_2(\alpha)$ tiene las otras $\Rightarrow \mathbb{F}_2(\alpha)$ es cdd de $f \Rightarrow F = \mathbb{F}_2(\alpha)$

$$\alpha^3 + \alpha + 1 = 0 \quad F = \mathbb{F}_2(\alpha) \text{ con } \alpha^3 + \alpha + 1 = 0. \text{ Tenemos } \Rightarrow \text{raíces de } f: \alpha, \alpha^2, \alpha^4 = \alpha^2 + \alpha \Rightarrow \text{estas son las raíces de } f: \alpha, \alpha^2, \alpha^4$$

$$\alpha^8 = \alpha^3 + \alpha^2 + 1 \in \mathbb{F}_2[x] \Rightarrow g \text{ es irreducible} \Rightarrow g \text{ es divisor de } x^8 - x$$

$$\alpha^8 = \alpha^3 + \alpha^2 + 1 \quad \alpha^8 = (\alpha^3)^2 + \alpha^2 + 1 = (\alpha^2 + \alpha + 1)^2$$

$$\text{Las raíces de } g \text{ son las restantes: } \alpha^3, \alpha^5, \alpha^6 \quad \text{con } \alpha^3 = \alpha^2 + \alpha + 1, \alpha^5 = \alpha^2 + \alpha^2 + 1 = \alpha^2 + 1, \alpha^6 = \alpha^2 + \alpha + \alpha^2 = \alpha^2 + \alpha + 1 = \alpha^2 + 1$$

$$\alpha^2 + \alpha + 1 = 0$$

Sea $\beta \in F$ una solución de la ecuación, β sería raíz del polinomio $x^3 + x + 1 \in \mathbb{F}_2[x] \Rightarrow [\mathbb{F}_2(\beta) : \mathbb{F}_2] = 2 !!!$

$$\begin{aligned}h(\beta) &= 1 \\ h(\alpha) &= 1\end{aligned}$$

$$\begin{aligned}[\mathbb{F}_2(\alpha) : \mathbb{F}_2] &= [\mathbb{F}_2(\alpha) : \mathbb{F}_2(\beta)] \cap [\mathbb{F}_2(\beta) : \mathbb{F}_2] \\ &\stackrel{!!}{=} 2\end{aligned}$$

No existe un cuerpo de grado 2 dentro de uno de grado 3

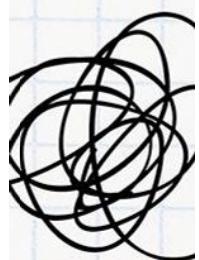


Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato
→ Planes pro: más coins

pierdo
espacio



Necesito
concentración

ali ali ooooh
esto con 1 coin me
lo quito yo...

wuolah

EJERCICIO 52. Calcular el número de polinomios irreducibles de grado 6 en $\mathbb{F}_2[X]$. (Nota: hay una fórmula general, si la encuentras en la web, no la uses, no se trata de eso).

$$2^6 = 64 \Rightarrow x^6 - x = x(x+1)(x^2+x+1)$$

$$\begin{array}{r} 6 \\ | \quad 1 \\ 6 \end{array}$$

Irreducibles de grado 3 en $\mathbb{F}_2 \rightarrow \begin{cases} x^3+x^2+1 \\ x^3+x^2+1 \end{cases} \Rightarrow 54/6 = 9$ polinomios de grado 6 irreducibles en $\mathbb{F}_2[X]$

EJERCICIO 51. Sea K un cuerpo de descomposición de $f = X^3 + X + 1 \in \mathbb{F}_4[X]$ y $\alpha \in K$ una raíz de f . Razonar que $K = \mathbb{F}_4(\alpha)$. Resolver, en K , las siguientes ecuaciones, expresando las soluciones en función de α :

$$x^3 + x + 1 = 0; \quad x^3 + x^2 + 1 = 0; \quad x^2 + x + 1 = 0.$$

Construir, si es posible, una base de K sobre \mathbb{F}_2 usando α y una solución de la tercera ecuación.

$$f = x^3 + x + 1 \in \mathbb{F}_4[x], \quad K \text{ cdd de } f, \quad \alpha \in K \text{ raíz de } f.$$

$$\gamma K = \mathbb{F}_4(\alpha)$$

Veremos que f es irreducible, $f(0) = 1, f(1) = 3, f(2) = 3, f(3) = 3 \Rightarrow f$ no tiene raíces simples $\Rightarrow f$ es irreducible en $\mathbb{F}_4[x]$

$[\mathbb{F}_4(\alpha) : \mathbb{F}_4] = \deg f = 3 \Rightarrow K(\alpha)$ es un cuerpo con $4^3 = 64$ elementos y $\mathbb{F}_4 \in \mathbb{F}_4(\alpha)$ es de Galois
Como f tiene una raíz en $\mathbb{F}_4(\alpha)$, tiene que tener las otras dos $\Rightarrow \mathbb{F}_4(\alpha)$ es de Galois

es cdd de f

$$\Rightarrow K = \mathbb{F}_4(\alpha) \text{ con } \alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = -\alpha - 1 = 3\alpha + 3$$

$\gamma x^3 + x + 1 = 0 \Rightarrow \alpha$ es raíz \Rightarrow por el Análogos del

Problema. $\alpha, \alpha^4, \alpha^{16}$ son las raíces de $x^3 + x + 1$

$$\gamma x^3 + x^2 + 1 = 0 \Rightarrow x^4 - x = x(x+1)(x+2)(x+3)$$

20 polinomios irreducibles de

grado 3 en \mathbb{F}_4

Veremos si α^2 es raíz: $(\alpha^2)^3 + \alpha^2 + 1 = (\alpha^2 + 3)^3 + (\alpha^2 + 3)\alpha^2 + 1 = \alpha^6 + 2\alpha^4 + 3\alpha^2 + 1 = \alpha^2 + 2$

Veremos si α^3 es raíz: $(\alpha^3)^3 + (\alpha^3)^2 + 1 = (\alpha^3 + 3)^3 + (\alpha^3 + 3)^2 + 1 = (\alpha^9 + 2\alpha^6 + 3\alpha^3 + 1) + 1 = 3\alpha^9 + 2\alpha^6 + 3\alpha^3 + 2\alpha^2 + 3 + \alpha^3 + 2\alpha + 2$

Las soluciones en K de $x^3 + x + 1 = 0$ son las raíces en K de f así que, por el Teorema 3.50, son $\alpha, \alpha^4, \alpha^{16}$. Comparando con la solución del Ejercicio 53, puesto que $F \leq K$, hemos de tener que las soluciones son $\alpha, \alpha^2, \alpha^4$. No hay contradicción ninguna, ya que, por ser F un cuerpo de 8 elementos, $\alpha^8 = \alpha$, por lo que $\alpha^{16} = \alpha^2$. La observación $F \leq K$ también permite deducir que las soluciones de la segunda ecuación son las dadas en el Ejercicio 53.

$\gamma x^2 + x + 1 = 0$. Como \mathbb{F}_4 es cdd de $x^2 + x + 1 \in \mathbb{F}_2[x]$, basta tomar $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ para que γ sea solución.

La base pedida es: $\{ \gamma^j \alpha^k : j=0,1; k=0,1,2 \}$

EJERCICIO 53. Calcular los grupos de Galois sobre \mathbb{Q} de los polinomios $f = (X^2 + X + 1)(X^2 - 3)$ y $g = (X^2 + X + 1)(X^2 + 3)$.

$$\gamma f = (x^2 + x + 1)(x^2 - 3) \in \mathbb{Q}[x]$$

Raíces de $x^2 - 3 \rightarrow \pm \sqrt{3}$

$$\text{Raíces de } x^2 + x + 1 \rightarrow -\frac{1 \pm \sqrt{1-4 \cdot 1}}{2} = -\frac{1 \pm \sqrt{-3}}{2} = -\frac{1 \pm i\sqrt{3}}{2}$$

$\Rightarrow K = \mathbb{Q}(\sqrt{3}, i\sqrt{3})$ es cdd de f

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i\sqrt{3}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4 = \# \text{Aut}(K)$$

$x^2 + 1$ es irred

en $\mathbb{Q}(\sqrt{3})$

$x^2 - 3$ irred en \mathbb{Q}

por elección de γ para $p=3$

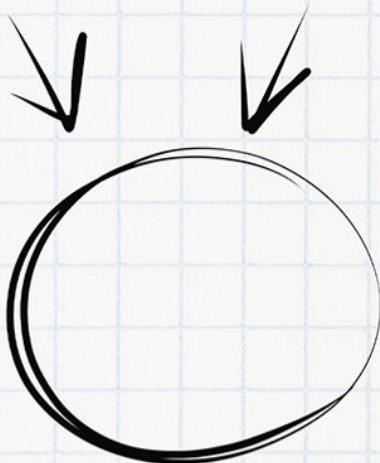
wuolah

Imagínate aprobando el examen

Necesitas tiempo y concentración

Planes	PLAN TURBO	PLAN PRO	PLAN PRO+
diamond Descargas sin publi al mes	10 🟡	40 🟡	80 🟡
clock Elimina el video entre descargas	✓	✓	✓
folder Descarga carpetas	✗	✓	✓
download Descarga archivos grandes	✗	✓	✓
circle Visualiza apuntes online sin publi	✗	✓	✓
glasses Elimina toda la publi web	✗	✗	✓
€ Precios	Anual <input type="checkbox"/>	0,99 € / mes	3,99 € / mes
			7,99 € / mes

Ahora que puedes conseguirlo,
¿Qué nota vas a sacar?



WUOLAH

Por la proposición de extensión, tenemos los homomorfismos $\mathbb{Q}(\sqrt{3}) \xrightarrow{\eta_j} K$

$$\sqrt{3} \mapsto (\pm i)^j \sqrt{3} \quad j=0,1$$

De nuevo, por la proposición de extensión, por cada uno de los homomorfismos anteriores tenemos otros dos:

$$\begin{aligned} K &\xrightarrow{\eta_{jk}} K \\ i &\mapsto i^k, \quad k=1,2 \end{aligned}$$

Luego, los homomorfismos son: $\text{Aut}(K) = \{\eta_{ijk}; j=0,1; k=1,2\}$

$$\eta_{jk}(\sqrt{3}) = (-1)^j \sqrt{3}$$

$$\eta_{jk}(i) = i^k$$

Veamos los órdenes de los elementos:

$$\begin{array}{cccc} \eta_{001} & \eta_{002} & \eta_{111} & \eta_{112} \\ 1 & 2 & 2 & 2 \end{array}$$

Como todos los elementos son de orden 2, el grupo de Galois es el de Klein.

$$\eta_{002}^2(\sqrt{3}) = \sqrt{3}$$

$$\eta_{002}^2(i) = \eta_{002}(-i) = -\eta_{002}(i) = i$$

$$\eta_{111}^2(\sqrt{3}) = \eta_{111}(-\sqrt{3}) = -\eta_{111}(\sqrt{3}) = \sqrt{3}$$

$$\eta_{111}^2(i) = i$$

$$\eta_{112}^2(\sqrt{3}) = \sqrt{3}$$

$$\eta_{112}^2(i) = i$$

$$g = (x^3 + x + 1)(x^2 + 1)$$

$$\begin{aligned} \text{Raíces de } x^2 + 1 = 0 &\Rightarrow \pm i\sqrt{3} = \pm i\sqrt{3} \\ \text{Raíces de } x^3 + x + 1 &\Rightarrow \frac{-1 \pm i\sqrt{3}}{2} \end{aligned} \quad \Rightarrow K = \mathbb{Q}(\sqrt{3}) \text{ es cdd de } g$$

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 = \#\text{Aut}(K) \quad \text{El único grupo con dos elementos es el cíclico } C_2$$

$x^2 + 1$ es irred sobre \mathbb{Q}

EJERCICIO 54. Calcular el cardinal del grupo de Galois sobre \mathbb{Q} del polinomio $f = (X^3 + X + 1)(X^2 + 1)$.

$g = (x^3 + x + 1)(x^2 + 1)$. Sea K el cdd de g sobre \mathbb{Q} , claramente $\mathbb{Q}(i) \subseteq K \Rightarrow K$ es cdd de $g = x^3 + x + 1$ sobre $\mathbb{Q}(i)$

Veamos que $g|_{\mathbb{Q}(i)}(x)$ es irreducible, es decir, que no tiene raíces en $\mathbb{Q}(i)$.

Como $g' = 3x^2 + 1$, tenemos que g tiene derivada estrictamente positiva $\Rightarrow g$ tiene una raíz real y las otras dos son complejas, $\pm i$

Veamos que $i \notin \mathbb{Q}(i)$, pues si lo hiciera, $i^2 = -1 \Rightarrow i = \pm 1$ lo cual no es cierto pues ± 1 no es raíz de g

Veamos que α y $\bar{\alpha}$ tampoco pertenecen a $\mathbb{Q}(i)$. Si $\alpha \in \mathbb{Q}(i) \Rightarrow \bar{\alpha} \in \mathbb{Q}(i) \Rightarrow \alpha = (x - \alpha)(x - \bar{\alpha}) \in \mathbb{Q}(i)$

Pero entonces $h(x)$ tiene coef en $\mathbb{Q} \Rightarrow (x - \alpha)(x - \bar{\alpha}) : (x - r)(x - s)(x - \bar{s}) = (x - r) \in \mathbb{Q} \Rightarrow r \in \mathbb{Q}$

Por lo tanto, g es irreducible en $\mathbb{Q}(i)$

En este punto sabemos que el grupo de Galois de g sobre $\mathbb{Q}(i)$ es un subgrupo transitivo de S_3 , es decir, es A_3 o S_3 .

Veamos el discriminante de g :

$$g = x^3 + x + 1 \Rightarrow p=1, q=1 \Rightarrow \text{Disc}(g) = -4p^3 - 27q^2 = -4 - 27 = -31. \quad \text{Veamos si } -31 \text{ es un cuadrado en } \mathbb{Q}(i).$$

Si $\sqrt{-31} = (i\beta) \in \mathbb{Q}(i) \Rightarrow i\beta \in \mathbb{Q}(i) \Rightarrow \beta \in \mathbb{Q}$, pero esto no es posible porque $x^2 - 31 \in \mathbb{Q}[x]$ es irreducible $\Rightarrow \text{Aut}_{\mathbb{Q}(i)}(i) \cong S_2$

$$\text{Luego, } [K : \mathbb{Q}(i)] = \#S_3 = 6 \Rightarrow \#\text{Aut}(K) = [K : \mathbb{Q}] = [K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 6 \cdot 2 = 12$$

EJERCICIO 55. Tomemos $f = (X^3 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ y K el cuerpo de descomposición sobre \mathbb{Q} de f .

1. Decidir razonadamente si $i + \sqrt{3} \in K$.
2. Calcular razonadamente $[K : \mathbb{Q}]$.
3. Describir los elementos del grupo $\text{Aut}(K)$.
4. Describir los elementos de $\text{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)$ y decidir si es un subgrupo normal de $\text{Aut}(K)$.

$$f = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x], K \text{ el cdd de } f \text{ sobre } \mathbb{Q}$$

a) Vamos a calcular el cdd de $f \Rightarrow$ raíces de $x^2 - 3 \rightarrow \pm\sqrt{3}$
 Raíces de $x^2 - 2 \rightarrow \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$
 $\Rightarrow K = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ como $w = -\frac{1}{2} + \frac{\sqrt{3}}{2} = \frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}} \in K \Rightarrow$ como $\sqrt{3} \in K$ tenemos que $i \in K$
 $\Rightarrow K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, i) \Rightarrow i + \sqrt[3]{3} \in K$

b) $[K : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})]}_{x+1 \text{ es irred en } \mathbb{Q}(\sqrt[3]{2})} \cdot \underbrace{[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})]}_{x^2 - 2 \text{ es irred en } \mathbb{Q}(\sqrt[3]{3})} \cdot \underbrace{[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}]}_{x-3 \text{ es irred en } \mathbb{Q} \text{ por Eisenstein para } p=3} = 2 \cdot 3 \cdot 2 = 12$

si $\sqrt[3]{2} \in \mathbb{Q}(i)$ $\Rightarrow \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(i)$ imposible por sus grados sobre \mathbb{Q}

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$
 $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 2$ como el resto de raíces son complejas no pertenecen a $\mathbb{Q}(i)$

c) $\# \text{Aut}(K) = [K : \mathbb{Q}] = 12$

Por la proposición de extensión, tenemos los homomorfismos: $\mathbb{Q}(i) \xrightarrow{\eta_j} K$

Por la proposición de extensión, por cada η_j tenemos otros 3 dodos por $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) \rightarrow K$

$$\begin{aligned} \eta_0(\sqrt[3]{2}) &= \sqrt[3]{2} \\ \eta_1(\sqrt[3]{2}) &= \omega\sqrt[3]{2} \quad \Rightarrow \eta_k(\sqrt[3]{2}) = \omega^k \sqrt[3]{2}, k=0,1,2 \\ \eta_2(\sqrt[3]{2}) &= \omega^2 \sqrt[3]{2} \end{aligned}$$

Por cada η_k tenemos otros dos homomorfismos: $K \rightarrow K$

$$\begin{aligned} \eta_0(i) &= i & \Rightarrow \eta_\ell(i) = \omega^\ell i, \ell=0,1 \\ \eta_1(i) &= -i \end{aligned}$$

En resumen, $\text{Aut}(K) = \{ \eta_{ijk\ell} : i=0,1; k=0,1,2; \ell=0,1,4 \}$

$$\eta_{ijk\ell} : \begin{cases} (-1)^i \sqrt{3} \\ \omega^k \sqrt[3]{2} \\ (-1)^\ell i \end{cases}$$

d) $\text{Aut}_{\mathbb{Q}(\sqrt[3]{3})}(K)$ son los automorfismos de K que dejan fijo a $i + \sqrt[3]{3}$

$$\eta_{ijk\ell}(i + \sqrt[3]{3}) = \eta_{ijk\ell}(i) + \eta_{ijk\ell}(\sqrt[3]{3}) = (-1)^\ell i + (-1)^\ell \sqrt[3]{3} \Rightarrow \text{Aut}_{\mathbb{Q}(\sqrt[3]{3})}(K) = \{ \eta_{0000} : k=0,1,2 \}$$

Por otro lado, $\text{Aut}_{\mathbb{Q}(\sqrt[3]{3})} = \{ \eta_{0000} : k=0,1,2 \} \Rightarrow \mathbb{Q}(i + \sqrt[3]{3}) \subseteq K$ y $\mathbb{Q}(i + \sqrt[3]{3}) \neq K$ tienen el mismo grupo de Galois

$$\Rightarrow \mathbb{Q}(i + \sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{3}) \Rightarrow \text{es cdd de } (x^2 + i\sqrt{3})(x^2 - 3) \in \mathbb{Q}[x] \Rightarrow \mathbb{Q} \subseteq \mathbb{Q}(i + \sqrt[3]{3}) \text{ es de Galois}$$

$\Rightarrow \mathbb{Q}(i + \sqrt[3]{3})$ es un subgrupo normal de $\text{Aut}(K)$

EJERCICIO 56. Sea $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$ y α cualquier raíz real de f .

Demostrar que el cuerpo de descomposición de f sobre \mathbb{Q} es $\mathbb{Q}(\alpha)$.

$$f = x^3 - 3x + 1 \in \mathbb{Q}[x], \text{ dR raíz de } f. \text{ Sea } K \text{ el cdd de } f \text{ sobre } \mathbb{Q}. \text{ Vemos que } K = \mathbb{Q}(\alpha)$$

Vemos que f es irreducible en \mathbb{Q} , es decir, que no tiene raíces, $f(1) = -1, f(-1) = 3 \Rightarrow f$ es irreducible
 \Rightarrow su grupo de Galois G es un subgrupo transitivo de S_3 .

$$\text{Vemos el discriminante } \Delta_f = -4p^3 - 27q^2 = -4(-3)^3 - 27 = 108 - 27 = 81. \text{ Como } 81 = 9^2 \Rightarrow G \cong A_3$$

$$\begin{aligned} p &= -3 \\ q &= 1 \end{aligned}$$

$$\text{Sea } \beta \in \mathbb{R} \text{ una raíz de } f, \text{ Im}(\alpha, \beta) = f \Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 3$$

$$\text{como } K \text{ es cdd de } f, \mathbb{Q}(\alpha) \subseteq K \text{ y } [K : \mathbb{Q}] = \# A_3 = 3$$

$$\Rightarrow K = \mathbb{Q}(\alpha)$$

EJERCICIO 60. Sea K el cuerpo de descomposición del polinomio $f = (X^2 + 3)(X^3 - 3) \in \mathbb{Q}[X]$. Calcular todos los subcuerpos de K . Demostrar que $\mathbb{Q}(\sqrt[3]{3} + i\sqrt{3}) = K$.

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

K el cdd de f

Raíces de $x^2 + 3 \rightarrow \pm i\sqrt{3}$

$$\text{Raíces de } x^3 - 3 \rightarrow \sqrt[3]{3}, \omega\sqrt[3]{3}, \omega^2\sqrt[3]{3} \text{ con } w = -\frac{1}{2} + \frac{i\sqrt{3}}{2} \Rightarrow K = \mathbb{Q}(\sqrt[3]{3}, \omega\sqrt[3]{3})$$

Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato
→ Planes pro: más coins

pierdo espacio



Necesito concentración

ali ali ooooh
esto con 1 coin me
lo quito yo...

wuolah

$$\text{Lema Torre} \rightarrow [K : Q(\sqrt[3]{3})] = [K : Q(\sqrt[3]{3})] \cdot [Q(\sqrt[3]{3}) : Q] = 2 \cdot 3 = 6 = \# \text{Aut}(K)$$

$\sqrt[3]{3}$ es irreducible
 porque sus raíces son irracionales
 y no están en $Q(\sqrt[3]{3})$

Por la proposición de extensión, como $x^3 - 3 \in Q[x]$ es irreducible y K contiene sus 3 raíces, tenemos 3 homomorfismos

$$\begin{aligned} Q(\sqrt[3]{3}) &\longrightarrow K \\ \eta_0(\sqrt[3]{3}) &= \sqrt[3]{3} \\ \eta_1(\sqrt[3]{3}) &= w^2 \sqrt[3]{3} \quad \Rightarrow \eta_1(\sqrt[3]{3}) = w^2 \sqrt[3]{3}, \delta = 0, 1, 2 \\ \eta_2(\sqrt[3]{3}) &= w \sqrt[3]{3} \end{aligned}$$

como $x^3 - 3 \in Q(\sqrt[3]{3})(x)$ es irr., por cada η_j tenemos dos extensiones $K \longrightarrow K$

En resumen, $G = \text{Aut}(K) = \{\eta_{jk} : j = 0, 1, 2; k = 0, 1, 2\}$

$$\eta_{jk} : \begin{cases} w^j \sqrt[3]{3} \\ w^{j+1} \sqrt[3]{3} \end{cases}$$

Calculamos los órdenes de los elementos:

$$\begin{array}{ccccccc} \eta_{00} & \eta_{01} & \eta_{10} & \eta_{11} & \eta_{20} & \eta_{21} \\ 1 & 2 & 3 & 2 & 3 & 2 \end{array} \Rightarrow G \cong S_3$$

$$\eta_{10}^2(\sqrt[3]{3}) = \sqrt[3]{3}$$

$$\eta_{01}^2(\sqrt[3]{3}) = \eta_{01}(-\sqrt[3]{3}) = \sqrt[3]{3}$$

$$\eta_{10}^2(\sqrt[3]{3}) = \eta_{10}(w^2 \sqrt[3]{3}) = \eta_{10}(w) \eta_{10}(\sqrt[3]{3}) = \eta_{10}\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right) = \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right) \eta_{10}(\sqrt[3]{3}) = \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right) w^2 \sqrt[3]{3} = w^2 \sqrt[3]{3}$$

$$\eta_{10}(w^2 \sqrt[3]{3}) = \eta_{10}(w)^2 \eta_{10}(\sqrt[3]{3}) = w^2 w^2 \sqrt[3]{3} = \sqrt[3]{3} \quad \eta_{10}(\sqrt[3]{3})$$

$$\eta_{10}^3(\sqrt[3]{3}) = \sqrt[3]{3}$$

$$\eta_{11}^2(\sqrt[3]{3}) = \eta_{11}(w^2 \sqrt[3]{3}) = \eta_{11}(w) \eta_{11}(\sqrt[3]{3}) = \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right) w^2 \sqrt[3]{3} = -\frac{1}{2} + \frac{i\sqrt{3}}{2} (-\sqrt[3]{3}) w^2 \sqrt[3]{3} = \bar{w} w^2 \sqrt[3]{3} = \sqrt[3]{3}$$

$$\eta_{11}^2(\sqrt[3]{3}) = \eta_{11}(-\sqrt[3]{3}) = \sqrt[3]{3}$$

$$\eta_{11}^2(\sqrt[3]{3}) = \eta_{12}(w^2 \sqrt[3]{3}) = \eta_{12}(w)^2 \eta_{12}(\sqrt[3]{3}) = w^2 w^2 \sqrt[3]{3} = w^3 \sqrt[3]{3} \Rightarrow \eta_{12}(w^2 \sqrt[3]{3}) = \eta_{12}(w) \eta_{12}(\sqrt[3]{3}) = w w^2 \sqrt[3]{3} = \sqrt[3]{3}$$

$$\eta_{12}^3(\sqrt[3]{3}) = \sqrt[3]{3}$$

$$\eta_{20}^2(\sqrt[3]{3}) = \eta_{20}(w^2 \sqrt[3]{3}) = \eta_{20}(w)^2 \eta_{20}(\sqrt[3]{3}) = \bar{w}^2 w^2 \sqrt[3]{3} = \sqrt[3]{3}$$

$$\eta_{21}^2(\sqrt[3]{3}) = \eta_{21}(-\sqrt[3]{3}) = \sqrt[3]{3}$$

veamos los subgrupos de G : se tiene 3 de orden 2 y uno de orden 3

El subgrupo de orden 3 corresponde a un subcuerpo de orden 2:

$$\eta_{10}(\sqrt[3]{3}) = \sqrt[3]{3} \Rightarrow \sqrt[3]{3} \in K^{<\eta_{10}>} \Rightarrow Q(\sqrt[3]{3}) \subseteq K^{<\eta_{10}>}$$

$$\text{Como } [K^{<\eta_{10}>} : Q] = (G : \langle \eta_{10} \rangle) = 2 \quad \text{y} \quad K^{<\eta_{10}>} = Q(\sqrt[3]{3})$$

$$\text{y} \quad [Q(\sqrt[3]{3}) : Q] = 2$$

" "

$K^{<\eta_{10}>}$

Los subgrupos de orden 2 corresponden a subcuerpos de orden 3:

$$K^{<\eta_{01}>}$$

$$\eta_{01}(\sqrt[3]{3}) = \sqrt[3]{3} \Rightarrow \sqrt[3]{3} \in K^{<\eta_{01}>} \Rightarrow Q(\sqrt[3]{3}) \subseteq K^{<\eta_{01}>}$$

$$\text{Como } [K^{<\eta_{01}>} : Q] = (G : \langle \eta_{01} \rangle) = 3 \quad \text{y} \quad K^{<\eta_{01}>} = Q(\sqrt[3]{3})$$

$$\text{y} \quad [Q(\sqrt[3]{3}) : Q] = 3$$

" "

$K^{<\eta_{01}>}$

$$K^{<\eta_{11}>}$$

$$\eta_{11}(\sqrt[3]{3}) = \eta_{11}(w^2 \sqrt[3]{3}) = \bar{w}^2 w^2 \sqrt[3]{3} = w^3 \sqrt[3]{3} \Rightarrow w^3 \sqrt[3]{3} \in K^{<\eta_{11}>} \Rightarrow Q(w^2 \sqrt[3]{3}) \subseteq K^{<\eta_{11}>}$$

$$\text{Como } [K^{<\eta_{11}>} : Q] = (G : \langle \eta_{11} \rangle) = 3 \quad \text{y} \quad K^{<\eta_{11}>} = Q(w^2 \sqrt[3]{3})$$

$$\text{y} \quad [Q(w^2 \sqrt[3]{3}) : Q] = 3$$

" "

$K^{<\eta_{11}>}$

$$K^{<\eta_{21}>}$$

$$\eta_{21}(\sqrt[3]{3}) = \eta_{21}(w) \eta_{21}(\sqrt[3]{3}) = \bar{w} w^2 \sqrt[3]{3} = w^3 \sqrt[3]{3} \Rightarrow w^3 \sqrt[3]{3} \in K^{<\eta_{21}>} \Rightarrow Q(w^2 \sqrt[3]{3}) \subseteq K^{<\eta_{21}>}$$

$$\text{Como } [K^{<\eta_{21}>} : Q] = (G : \langle \eta_{21} \rangle) = 3 \quad \text{y} \quad [Q(w^2 \sqrt[3]{3}) : Q] = 3$$

" "

$K^{<\eta_{21}>}$

$$K^{<\eta_{21}>}$$

Los subcuerpos de K son: $K, Q(\sqrt[3]{3}), Q(w^2 \sqrt[3]{3}), Q(w^2 \sqrt[3]{3}) : Q$

