Ejercicio 1. (4 puntos) Sea el polinomio irreducible $f(X) = X^4 + \frac{5}{2}X^2 + 11X + \frac{333}{16} \in \mathbb{Q}[x]$ cuyas raíces son

$$\alpha_1 = -\frac{\sqrt{-11}}{2} + \frac{\sqrt{2}\sqrt{3-\sqrt{-11}}}{2}, \alpha_2 = -\frac{\sqrt{-11}}{2} - \frac{\sqrt{2}\sqrt{3-\sqrt{-11}}}{2},$$

$$\alpha_3 = \frac{\sqrt{-11}}{2} + \frac{\sqrt{2}\sqrt{3+\sqrt{-11}}}{2}, \alpha_4 = \frac{\sqrt{-11}}{2} - \frac{\sqrt{2}\sqrt{3+\sqrt{-11}}}{2}.$$

La resolvente cúbica es

$$g(X) = (1/8)(2x+17)(4x^2 - 44x + 41)$$

que tiene a $-\frac{17}{2}$ como única raíz racional. De otro lado, se considera el polinomio

$$h(X) = (X^2 + (17/2)X + (333/16))(X^2 + 11),$$

como auxiliar para los cálculos. Sea K el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.

1. Escribir el grupo de Galois de $K : \mathbb{Q}$ como un subgrupo de S_4, para las etiquetas puestas a las raíces de $f(X)$.
2. Determinar generadores de cada una de las extensiones intermedias entre $\mathbb{Q}$ y K.

Solución del Ejercicio 1.-

• Apartado 1.-

Las raíces de la resolvente cúbica de $f(x)$ son $\eta = -17/2$, $\eta_1 = 11 + 4\sqrt{5}/2$ y $\eta_2 = 11 - 4\sqrt{5}/2$ luego su cuerpo de descomposición sobre $\mathbb{Q}$ es $K' = \mathbb{Q}[\sqrt{5}]$. Como sólo una de las raíces pertenece a $\mathbb{Q}$, G será isomorfo a un subgrupo cíclico de orden 4 o a uno de orden 8 de S_4.

Una de las raíces de $h(x)$ es $\sqrt{-11} \notin K'$ ($K' \subset \mathbb{R}$). Por tanto G es isomorfo a un subgrupo de orden 8 de S_4.

Veamos a cuál de ellos:

Sea $\beta_1 = \sqrt{2}\sqrt{3-\sqrt{-11}} \Rightarrow \beta_1^4 - 3\beta_1^2 + 80 = 0 \Rightarrow \beta_1$ es raíz de $x^4 - 3x^2 + 80$.

Este polinomio es irreducible sobre $\mathbb{Q}$ (aplicar criterio bicuadradas) y sus otras raíces son $\beta_2 = -\beta_1, \beta_3 = \sqrt{2}\sqrt{3+\sqrt{-11}}$, $\beta_4 = -\beta_3$. Queremos probar que $K = \mathbb{Q}[\beta_1, \beta_3]$.

$\mathbb{Q}[\beta_1, \beta_3] \subset K$ porque $\beta_1 = \alpha_1 - \alpha_2$ y $\beta_3 = \alpha_3 - \alpha_4$. Al ser $\sqrt{-11} = -\frac{1}{2}(\beta_1^2 - 6)$ se obtiene fácilmente que $K \subset \mathbb{Q}[\beta_1, \beta_3]$ (basta sustituir en las expresiones de α_i, $i = 1, 2, 3, 4$). En consecuencia, $K = \mathbb{Q}[\beta_1, \beta_3]$.

Sabemos que $[\mathbb{Q}[\beta_1] : \mathbb{Q}] = 4$ por tanto $[K : \mathbb{Q}[\beta_1]] = 2$; así, podemos considerar $\mathrm{Gal}(K : \mathbb{Q}[\beta_1]) = \{1, \sigma\}$ y como $\mathbb{Q} \subset \mathbb{Q}[\beta_1]$, $\sigma \in G$. Además $\sigma(\beta_1) = \beta_1$ luego $\sigma(\beta_2) = \beta_2$ y al ser $\sigma \neq 1$, $\sigma(\beta_3) = \beta_4$ y $\sigma(\beta_4) = \beta_3$; por tanto:

$$\sigma(\alpha_1) = \alpha_1\,, \qquad \sigma(\alpha_2) = \alpha_2\,, \qquad \sigma(\alpha_3) = \alpha_4\,, \qquad \sigma(\alpha_4) = \alpha_3\,.$$

pues $\sigma(\sqrt{-11}) = \sigma(-\frac{1}{2}(\beta_1^2 - 6)) = \sqrt{-11}$. En resumen, $(34) \in G$; entonces:

$$G \simeq \{1, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$$

Los subgrupos no triviales de G son los siguientes:

$H_1 = \{1, (12)\}$; $H_2 = \{1, (34)\}$; $H_3 = V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$; $H_4 = \{1, (14)(23)\}$; $H_5 = \{1, (13)(24)\}$; $H_6 = \{1, (12)(34)\}$.

$H_7 = \{1, (12)(34), (1324), (1423)\}$; $H_8 = \{1, (12), (34), (12)(34)\}$.

Notaremos $K_i = F(H_i)$, $i = 1, \ldots, 8$.

• Apartado 2

Cálculo de K_3

$K_3 = F(G \cap V_4) = \mathbb{Q}[\sqrt{5}]$.

Cálculo de K_1

$\alpha_3 \in K_1$ y $[\mathbb{Q}[\alpha_3] : \mathbb{Q}] = 4$ ya que el polinomio mínimo de α_3 es $f(x)$. Por tanto:

$$\underbrace{\overbrace{\mathbb{Q} \overset{4}{\subset} \mathbb{Q}[\alpha_3] \subset K_1}^{4} \overset{2}{\subset} K}_{8} \Rightarrow K_1 = \mathbb{Q}[\alpha_3]$$

Cálculo de K_2

De forma análoga al caso anterior se obtiene que $K_2 = \mathbb{Q}[\alpha_1]$.

Cálculo de K_5

$\beta = \beta_1 + \beta_3 = \sqrt{2}\sqrt{3-\sqrt{-11}} + \sqrt{2}\sqrt{3+\sqrt{-11}} \in K_5$ luego $\beta^4 - 24\beta^2 - 176 = 0$.
Por tanto, β es raíz del polinomio $x^4 - 24x^2 - 176$ que es irreducible sobre $\mathbb{Q}$ (criterio de bicuadradas) luego es su polinomio mínimo sobre $\mathbb{Q}$; así:

$$\underbrace{\overbrace{\mathbb{Q} \overset{4}{\subset} \mathbb{Q}[\beta_1+\beta_3] \subset K_5}^{4} \overset{2}{\subset} K}_{8} \Rightarrow K_5 = \mathbb{Q}[\beta_1+\beta_3]$$

<u>Cálculo de K_4</u>
Razonando como en el caso anterior se tiene que $K_4 = \mathbb{Q}[\beta_1 + \beta_4]$.

<u>Cálculo de K_8</u>
$-\sqrt{-11} = \alpha_1 + \alpha_2 \in K_8$ luego $\mathbb{Q}[\sqrt{-11}] \subset K_8$, además $[\mathbb{Q}[\sqrt{6}] : \mathbb{Q}] = 2 = [K_8 : \mathbb{Q}]$; así $K_8 = \mathbb{Q}[\sqrt{-11}]$.

<u>Cálculo de K_6</u>
$H_6 \subset H_8 \Rightarrow K_8 \subset K_6 \Rightarrow \sqrt{-11} \in K_6$.
$H_6 \subset H_3 \Rightarrow K_3 \subset K_6 \Rightarrow \sqrt{5} \in K_6$.
Por tanto $\mathbb{Q}[\sqrt{5}, \sqrt{-11}] \subset K_6$; además $[\mathbb{Q}[\sqrt{5}, \sqrt{-11}] : \mathbb{Q}] = 4 = [K_6 : \mathbb{Q}]$ luego $K_6 = \mathbb{Q}[\sqrt{5}, \sqrt{-11}]$.

<u>Cálculo de K_7</u>
Basta ver que $\mathbb{Q}[\sqrt{-55}]$ es un cuerpo intermedio de grado 4 y distinto de K_3 y K_8. Entonces $K_7 = \mathbb{Q}[\sqrt{-55}]$.

Ejercicio 2. (3 puntos) Este ejercicio consta de tres apartados independientes.

A) Sea ϵ es una raíz primitiva séptima de la unidad. Estudiar el grupo de Galois de $[\mathbb{Q}[\epsilon] : \mathbb{Q}]$, y establecer la correspondencia de Galois.

B) Demuéstrese que el polinomio $p(X) = X^3 + X + 1$ es irreducible en $\mathbf{F}_2[X]$. Si denotamos por α una de las raíces de $p(X)$, dar las otras dos raíces en función de α.

C) Calcular el polinomio mínimo sobre $\mathbb{Q}$ de $\sqrt[n]{2}$. ¿Es finita la extensión $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots]$? ¿por qué?

Solución del Ejercicio 2.-
A) Es conocido que $K = \mathbb{Q}[\epsilon]$ con $\epsilon = \cos\frac{2\pi}{7} + i \sin\frac{2\pi}{7}$ es una extensión de grado 6 pues $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ es irreducible sobre $\mathbb{Q}$. Se tiene que $G = Gal(K\,\mathbb{Q} \simeq U_7$, el grupo multiplicativo de las unidades en $\mathbf{F_7}$, cíclico de orden 6. La correspondencia de Galois es bien sencilla en este caso, pues G tiene dos subgrupos propios de órdenes 2 y 3 respectivamente H_2 y H_3 y sus cuerpos fijos son:

- $K^{H_2} = \mathbb{Q}[\epsilon + \epsilon^{-1}] = \mathbb{Q}[\cos\frac{2\pi}{7}]$, pues se sabe que el grado de $\mathbb{Q}[\cos\frac{2\pi}{7}] \subset K$ es 2.
- $K^{H_3} = \mathbb{Q}[\epsilon + \epsilon^2 + \epsilon^4]$, usando el periodo de Gauss. Basta con ver que el elemento no está en $\mathbb{Q}$ y que es invariante por H_3.

B) Para ver la irreducibilidad de un polinomio de grado 3 basta con ver que no tiene raíces en $\mathbf{F}_2$.
Si α es una raíz, hay que trabajar en el cuerpo $\mathbf{F}_2[\alpha] \simeq \mathbf{F}_2[X]/(X^3 + X + 1)$. Los elementos de dicho cuerpo se pueden describir como

$$\{c_0 + c_1\alpha + c_2\alpha^2, \quad c_i \in \mathbf{F}_2\}.$$

Se comprueba que α^2 y $\alpha^2 + \alpha + 1$ son raíces del polinomio (se usa que $\alpha^3 + \alpha + 1$.)
C) Por el criterio de Eisenstein para $p = 2$ el polinomio $X^n - 2$ es irreducible y por tanto el polinomio mínimo de $\sqrt[n]{2}$. Si

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots] = \mathbb{Q}[\alpha_1, \ldots, \alpha_s] = K$$

se tendría que

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[n]{2}] \subset K$$

y que por tanto n dividiría a

$$[K : \mathbb{Q}]$$

para todo n.

Ejercicio 3. (3 puntos) Este ejercicio consta de cuatro apartados independientes.
A) Dado un anillo A y un A-módulo M, definimos sobre el conjunto $A \times M$ la siguiente operación interna

$$(a, m) \cdot (b, n) = (ab, an + bm), \quad a, b \in A, m, n \in M.$$

Probar que el conjunto $A \times M$ dotado de la $+$ $((a, m) + (b, n) = (a + b, m + n))$ y de la operación interna $\cdot$ anterior es un anillo.

Definir un homomorfismo sobreyectivo de anillos $A \times M \to A$.

B) Sea A un DIP y $p \in A$ un elemento irreducible. Probar que los A-módulos $A/(p) \times A/(p)$ y $A/(p^2)$ no son isomorfos.

C) Probar que $\mathbb{Z}/\mathbb{Z}3 \otimes_{\mathbb{Z}} \mathbb{Z}/\mathbb{Z}5 = 0$.

D) Probar que todo ideal maximal de un anillo es primo.

Solución del Ejercicio 3.-
A) Hemos de probar que $A \times M$ con la operación $+$ es un grupo abeliano, y que la operación $\cdot$ es asociativa, conmutativa, tiene elemento neutro y es distributiva respecto de $+$.

Las propiedades de $+$ son fáciles y no las escribiremos.
Asociatividad de $\cdot$:

$$(a,m)\cdot[(b,n)\cdot(c,p)] = (a,m)\cdot(bc, bp+cn) = (a(bc), a(bp+cn)+(bc)m) = (abc, abp+acn+bcm),$$

$$[(a,m)\cdot(b,n)]\cdot(c,p) = (ab, an+bm)\cdot(c,p) = ((ab)c, (ab)p + c(an+bm)) = (abc, abp+can+cbm)$$

y ambas expresiones son iguales teniendo en cuenta que A es un anillo (conmutativo) y M es un A-módulo.

Conmutatividad de $\cdot$: Es una consecuencia directa de que la suma en M es conmutativa.
Elemento neutro de $\cdot$: Hemos de encontrar un $(e,e') \in A \times M$ tal que

$$(a,m) = (e,e')\cdot(a,m) = (ea, em+ae'), \quad \forall (a,m) \in A \times M.$$

Entonces ha de cumplirse que $ea = a$ para todo $a \in A$, y por tanto $e = 1$. Por otra parte $m = m + ae'$ para todo $m \in M$ y todo $a \in A$, de donde $e' = 0$ (el elemento neutro de M). Luego si $\cdot$ tiene elemento neutro, éste ha de ser $(1, 0$, y efectivamente comprobamos fácilmente que lo es.
Distributividad:

$$(a,m)\cdot[(b,n)+(c,p)] = (a,m)\cdot(b+c, n+p) = (a(b+c), a(n+p)+(b+c)m) = (ab+ac, an+ap+bm+cm),$$

$$(a,m)\cdot(b,n) + (a,m)\cdot(c,p) = (ab, an+bm) + (ac, ap+cm) = (ab+ac, an+bm+ap+cm)$$

y ambas expresiones son iguales.

Consideremos la proyección $p : A \times M \to A$, $p(a,m) = a$. Claramente p es sobreyectiva ($p(a,0) = a$ para todo $a \in A$).

$$p((a,m)+(b,n)) = p(a+b, m+n) = a+b = p(a,m)+p(b,n),$$

$$p((a,m)\cdot(b,n)) = p(ab, an+bm) = ab = p(a,m)p(b,n),$$

$$p(1,0) = 1$$

luego p es un homomorfismo.

B) Todo elemento del A-módulo $A/(p) \times A/(p)$ es anulado por p, mientras que en el A-módulo $A/(p^2)$ la clase de 1 no es anulada por p. Por tanto ambos módulos no pueden ser isomorfos.

C) El $\mathbb{Z}$-módulo $\mathbb{Z}/\mathbb{Z}3 \otimes_{\mathbb{Z}} \mathbb{Z}/\mathbb{Z}5$ está generado por los elementos de la forma $x \otimes y$, con $x \in \mathbb{Z}/\mathbb{Z}3$ e $y \in \mathbb{Z}/\mathbb{Z}5$. Para probar que es nulo es suficiente probar que dichos elementos son nulos, pero como 3 y 5 son primos entre sí, la identidad de Bézout nos da $2 \cdot 3 - 5 = 1$ de donde

$$x \otimes y = [(2\cdot 3 - 5)x] \otimes y = (6x)\otimes y - (5x)\otimes y = (6x)\otimes y - x \otimes (5y) = 0$$

pues $3x = 0$ para todo $x \in \mathbb{Z}/\mathbb{Z}3$ y $5y = 0$ para todo $y \in \mathbb{Z}/\mathbb{Z}5$.

D) Sea I un ideal maximal del anillo A y sean $x, y \in A$ tales que $xy \in I$. Hemos de probar que $x \in A$ o $y \in A$.

Supongamos que $x \notin I$. Como I es maximal y $I \neq I + (x)$, deducimos que $I + (x) = A$, y por tanto existe un $a \in I$ y un $b \in A$ tales que $1 = a + bx$.

Se tiene $y = (a+bx)y = ay + bxy \in I$ puesto que $a \in I$ y $xy \in I$.

[También podemos proceder probando que I es primo (resp. maximal) si y sólo si A/I es dominio de integridad (resp. cuerpo), y que todo cuerpo es dominio de integridad]