Problemas de Teoría de Cuerpos

Rodrigo Raya Castellano
Universidad de Granada

Problema 1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ejercicio 0.2: Calcular:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Repitiendo el proceso anterior, llegamos al polinomio

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

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

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

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

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

Problema 2

Ejercicio 0.3: Hallar $\sigma \in \mathbb{F}_{3^6}^X$ con $gr(Irr(\sigma, \mathbb{F}_3)) = 6$ y expresarlo como elemento de $\mathbb{F}_3(\alpha)$ donde α es una raíz del polinomio $q = X^6 + X + 2$ (que es un generador de $\mathbb{F}_{3^6}^X$).

Necesitamos un polinomio p mónico e irreducible sobre $\mathbb{F}_3$ tal que algún polinomio X^i con $i < 728$ al divirlo por p de resto 1.

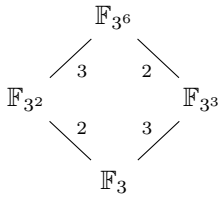
Los factores irreducibles del polinomio $X^{3^6} - X$ son los irreducibles sobre F_3 de grado divisor de 6. En Mathematica esta lista se puede obtener mediante el comando

$$Factor[X^{729} - X, Modulus- > 3]$$

Tras un par de comprobaciones el polinomio $p = 2 + x + x^2 + 2x^3 + x^6$ verifica que x^{104} da 1 de resto al dividirse por p. Tenemos entonces un σ que no puede ser generador. La expresión de σ en $\mathbb{F}_3(\alpha)$ se obtiene al dividir p mediante el polinomio q de donde obtenemos el polinomio $2X^3 + X^2$ visto como elemento en $\frac{\mathbb{F}_3[X]}{<X^6+X+2>}$ el correspondiente elemento en $\mathbb{F}_3(\alpha)$ es $\alpha^2 + 2\alpha^3$.

Ejercicio 0.4: Un elemento $\beta \in \mathbb{F}_{729}$ de orden 8 en $\mathbb{F}_{3^6}^X$ da una extensión $\mathbb{F}_3(\beta) = \mathbb{F}_9$

Observemos primero la construcción sobre la cual trabajan este ejercicio y el posterior.



Un cuerpo de p^m elementos es subcuerpo de otro con p^n si y sólo si $m|n$.

Volviendo a nuestro problema, si $\beta^8 = 1$ esto implica que β es raíz del polínomio $X^9 - X$ y por tanto, su polinomio mínimo será un factor irreducible de este. Pero los factores irreducibles de este deben tener grado divisor de 2. Luego deben ser de grado 1 o grado 2. De hecho, si observamos la descomposición en Mathematica mediante la orden

$$Factor[X^9 - X, Modulus- > 3]$$

obtenemos los polinomios $X, (1 + X), (2 + X), (1 + X^2), (2 + X + X^2), (2 + 2X + X^2)$. Como β es de orden 8 β no puede ser $0, 1, 2$ ya que estos tienen orden $\infty, 1, 2$ respectivamente luego tiene que ser raíz de los de grado 2. Esto implica que $\mathbb{F}_3(\beta) = \mathbb{F}_9$.

Ejercicio 0.5: Analiza qué ocurre al considerar el elemento σ para encontrar elementos que generen las extensiones $\mathbb{F}_{3^2}$ y $\mathbb{F}_{3^3}$.

Como ya habíamos comentado el orden es 104. En el primer caso, el método anterior donde tomamos $\sigma^{\frac{104}{8}} = \sigma^1 3$ entonces el método funciona y se obtiene cero al comprobar donde el polinomio irreducible del que es raíz σ resulta ser $X^2 + X + 2$. Sin embargo, aunque $\sigma^{\frac{104}{26}} = \sigma^4$ que es un elemento de orden 26, aparentemente no sirve para generar la extensión $\mathbb{F}_{3^3}$. Actualmente, no sabemos por qué se obtiene este resultado. Podríamos ser un poco tramposos y cambiar el polinomio por uno tal que 26 no divida su orden. Pero dejamos para una posterior revisión determinar la razón de que no funcione para este elemento.

Ejercicio 0.6: Determina el polinomio $Irr(\alpha, \mathbb{F}_{27})$. Para el elemento σ que encontraste al inicio calcula $Irr(\sigma, \mathbb{F}_9)$ y $Irr(\sigma, \mathbb{F}_{27})$

Primero hacemos algunos comentarios al método del guión de prácticas. α es raíz de un polinomio mónico irreducible de grado 3 sobre $\mathbb{F}_3(\delta)$ ya que el grado de la extensión $\frac{\mathbb{F}_{3^6}}{\mathbb{F}_{3^2}}$ es 3. El resto de cálculos tiene sentido porque los elementos de $\mathbb{F}_3(\delta)$ son las imágenes de clases de $\frac{\mathbb{F}_3[X]}{<X^2+X+2>}$ por la evaluación en δ esto es polinomios $a\delta + b$ con $a, b \in \mathbb{F}_3$.

Cálculo de $Irr(\alpha, \mathbb{F}_{27})$. Del mismo modo expresamos $\mathbb{F}_{27} = \mathbb{F}_3(\epsilon)$ con ϵ una raíz del polinomio X^3+2X+1. Se obtienen tres posibles valores para ϵ:

$$\alpha^2 + 2\alpha^3 + \alpha^4$$

$$1 + \alpha^2 + 2\alpha^3 + \alpha^4$$

$$2 + \alpha^2 + 2\alpha^3 + \alpha^4$$

Observamos que los elementos de $\mathbb{F}_3(\epsilon)$ son polinomios de grado dos evaluados en ϵ y como estamos buscando $Irr(\alpha, \mathbb{F}_{27})$ el sistema a resolver tendrá la forma:

$$(b00 + b01 * \epsilon + b02 * \epsilon^2) + (b10 + b11 * \epsilon + b12 * \epsilon^2)X + X^2$$

Realizando las sustituciones correspondientes a esta observación se obtiene el polinomio

$$2\epsilon + 2\epsilon^2 + X(1 + \epsilon) + X^2$$

Cálculo de $Irr(\sigma, \mathbb{F}_9)$. Repitiendo el proceso que aparece en el guión, cambiando el valor de PF a $X^6 + 2X^3 + X^2 + X + 2$ nos va a aparecer un irreducible de la forma:

$$2 + 2\delta + X(2 + \delta) + X^3$$

Cálculo de $Irr(\sigma, \mathbb{F}_{27})$. Tenemos que combinar las modificaciones de los apartados anteriores respecto al valor de PF y respecto al sistema de ecuaciones a resolver. Obtenemos el polinomio:

$$2 + 2\epsilon + 2\epsilon^2 + X(2 + \epsilon) + X^2$$

Ejercicio 0.7: Determinar el número de polinomios irreducibles de grado 30 sobre $\mathbb{F}_3$ y cuántos de ellos tienen raíces que son generadores del grupo multiplicativo de $\mathbb{F}_{3^{30}}$.

Vamos a clarificar el razonamiento empleado en el texto del ejercicio.

Proposición 0.3.
Cada seis raíces de $\mathbb{F}_{3^6} - \mathbb{F}_{3^2} - \mathbb{F}_{3^3}$ me están determinando polinomios irreducibles de grado 6 en $\mathbb{F}_3[X]$. Por tanto, hay 116 polinomios irreducibles de grado 6 sobre $\mathbb{F}_3$.

Demostración. Nosotros hemos visto que los factores irreducibles de $X^{6^n} - X$ en $\mathbb{F}_3[X]$ son exactamente los polinomios irreducibles de $\mathbb{F}_3[X]$ con grado divisor de 6.

Por otro lado, $\mathbb{F}_{3^6}$ es el cuerpo de descomposición del polinomio $X^{6^n} - X$ y por tanto, el cuerpo que contiene a todas sus raíces.

Entonces los polinomios irreducibles de $\mathbb{F}_3[X]$ con grado divisor de 6 tienen también sus raíces en $\mathbb{F}_{3^6}$.

Una observado lo anterior, cada seis raíces de $\mathbb{F}_{3^6} - \mathbb{F}_{3^2} - \mathbb{F}_{3^3}$ me están determinando polinomios irreducibles de grado 6 en $\mathbb{F}_3[X]$. □

Proposición 0.4.
Hay 248 generadores de $\mathbb{F}_{729}^x$. Además, si una raíz de un polinomio irreducible es generadora (no es generadora) entonces también el resto de las raíces son generadoras (no son generadoras). Como consecuencia de los 116 polinomios irreducibles de grado 6 hay 48 cuyas raíces son generadoras y 68 cuyas raíces no son generadoras.

Demostración. La proposición sobre las propiedades del orden de un elemento de mis apuntes sobre teoría de grupos muestra que un grupo cíclico tiene $\phi(ord(a))$ generadores donde a es un generador del grupo. Entonces, como $\mathbb{F}_{729}^x$ tiene 728 elementos, basta calcular $\phi(728) = \phi(8)\phi(7)\phi(13) = 248$.

Por otra parte, como todo polinomio de grado 6 irreducible sobre $\mathbb{F}_3[X]$ con una raíz α admite 6 raíces distintas α^{3^i} con $i = 0, \cdots, 5$, entonces si una raíz α es generadora esto quiere decir que $ord(\alpha) = 728$ y entonces $ord(\alpha^{3^i}) = \frac{728}{mcd(728,3^i)} = 728$ y por tanto siguen siendo generadoras. Si α no fuera generadora entonces el resto no pueden ser generadoras, ya que si alguna lo fuera entonces también lo sería α.

Agrupando las generadoras en grupos de 6 se obtienen 48 polinomios cuyas raíces son generadoras y agrupando los 68 polinomios restantes, se obtienen polinomios cuyas raíces no son generadoras. □

Veamos ahora el ejercicio.

En vez de calcular el número explícitamente utilizaremos la fórmula de Gauss para el número de polinomios mónicos irreducibles sobre $\mathbb{F}_p[X]$ de grado n (una prueba de este hecho basada en teoría de básica de cuerpos finitos y el principio de exclusión-inclusión aparece en nuestros apuntes):

$|N_n| = \frac{1}{n}\sum_{m|n}\mu(m)p^{\frac{n}{m}}$

donde μ es la función de Mobius:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^s & n = \prod_{i=1}^{s} p_i \text{ para primos distinos } p_i \\ 0 & \text{en otro caso} \end{cases}$$

Entonces

$$|N_{30}| = \frac{1}{30}(\mu(1)p^{30} + \mu(2)p^{15} + \mu(3)p^{10} + \mu(5)p^6 + \mu(6)p^5 + \mu(10)p^3 + \mu(15)p^2 + \mu(30)p)$$

$$|N_{30}| = \frac{1}{30}(p^{30} - p^{15} - p^{10} - p^6 + p^5 + p^3 + p^2 - p)$$

$$|N_{30}| = 6863037256208$$

Por otro lado hay $\phi(3^{30} - 1) = 70207948800000$ generadores de $\mathbb{F}_{30}$ el mismo argumento que hemos hecho para el caso del documento de la práctica sirve aquí y entonces basta dividir por 30 para obtener el número de polinomios irreducibles de grado 30 cuyas raíces son generadoras. Este número es 2340264960000. El resto, 67867683840000 no son generadoras.

Problema 3

EJERCICIO 0.8: Sea $\frac{E}{K}$ una extensión de cuerpos algebraica y normal y $f \in K[X]$ un polinomio irreducible. Si $f = f_1 f_2$ es una factorización en dos irreducibles de $E[X]$. Entonces:

1. Prueba que existe un automorfismo $\sigma : \frac{E}{K} \to \frac{E}{K}$ tal que $\overline{\sigma}(f_1) = f_2$ y por tanto $\sigma(f_2) = f_1$.
2. Considera el polinomio $f = X^4 - 2 \in \mathbb{Q}[X]$ y el cuerpo $E = \mathbb{Q}(\sqrt{2})$ En $\frac{E}{K}$ tenemos la factorización en irreducibles $f = (X^2 - \sqrt{2})(X^2 + \sqrt{2}) = f_1 f_2$. Describe σ en este caso.
3. Justifica que $\frac{\mathbb{Q}(\sqrt{2})}{\mathbb{Q}}, \frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}(\sqrt{2})}$ son extensiones normales y que $\frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}}$ no lo es.
4. Determina la clausura normal $\frac{F}{\mathbb{Q}}$ de $\frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}}$.
5. Calcular el grupo $Aut(\frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}})$ y los automorfismos que dejan fijo a $\mathbb{Q}(\sqrt{2})$.

Solución:

1. Con las mismas ideas con las que se prueba la unicidad del cuerpo de descomposición es fácil ver el siguiente resultado.

   Corolario 0.5 (Elementos conjugados en cuerpos de descomposición)**.**
   Sea $p \in K[X]$ irreducible con cuerpo de descomposición F. Sean $\alpha, \beta \in F$ raíces de p. Entonces existe un isomorfismo $\sigma : F \to F$ sobre K tal que $\alpha \mapsto \beta$.

   En nuestro caso para f podemos considerar que en la clausura algebraica descompone como

   $$f = \prod (x - \alpha_i) \prod (x - \beta_i) \prod (x - \gamma_i)$$

   donde α_i son raíces del polinomio f_1 y β_i son raíces del polinomio f_2. Seleccionamos dos de estas raíces, sean α_1, β_1. Por el corolario existe un isomorfismo $\sigma : F \to F$ sobre K tal que $\alpha_1 \mapsto \beta_1$ donde F es un cuerpo de descomposición de f.

   Como $\frac{F}{K}$ es algebraica y $\frac{E}{K}$ es normal, $\frac{FE}{F}$ es normal. Extendemos el codominio de $\sigma : F \to FE$ y obtenemos un homomorfismo sobre K.

   Extiendo σ a un automorfismo $\sigma_1 : FE \to FE$ sobre K y restringimos su dominio a $\sigma_2 : E \to FE$ obteniendo un homomorfismo sobre K. Observamos que $FE \subseteq \overline{F}$ ya que $\frac{FE}{F}$ es normal. También observamos que $\overline{F} = \overline{K}$ por la transitividad de la clausura. Esto permite ver σ_2 con codominio $\overline{K}$ y aplicar la caracterización de normalidad sobre K.

   Como $\frac{E}{K}$ es normal se tendrá que $\sigma_2(E) = E$ de modo que tenemos un automorfismo en E sobre K.

   Este automorfismo verifica $\sigma_2(f_1) = f_2$ ya que como α_1 es raíz de f_1 entonces

   $$0 = \sigma_2(f_1(\alpha_1)) = \sigma_1(f_1(\alpha_1)) = \overline{\sigma_1}(f)(\sigma_1(\alpha_1)) = \overline{\sigma_2}(f)(\beta_1)$$

   es decir que el polinomio imagen, que es irreducible, tiene a β_1 como raíz. Luego tiene que ser $Irr(\beta_1, E)$ que es igual a f_2.

2. Podemos representar $\mathbb{Q}(\sqrt{2})$ por expresiones de la forma $a + b\sqrt{2}$. Como todo los σ hallados fijaban K determinaremos el homomorfismo si determinamos $\sigma(\sqrt{2})$.

   Consideramos el cuerpo de descomposición del polinomio $X^4 - 2$. De forma natural este sería

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

donde la igualdad se comprueba viendo que la inclusión de los generadores en cada dirección. Por otro lado, en el cuerpo de descomposición

$$X^2+\sqrt{2}=(X-i\sqrt[4]{2})(X+i\sqrt[4]{2})$$

$$X^2-\sqrt{2}=(X-\sqrt[4]{2})(X+\sqrt[4]{2})$$

Simplemente elegimos que llevaremos $\sqrt[4]{2}\mapsto i\sqrt[4]{2}$ y entonces obtenemos que

$$\sigma(\sqrt{2})=\sigma((\sqrt[4]{2})^2)=(\sigma(\sqrt[4]{2}))^2=(i\sqrt[4]{2})^2=-\sqrt{2}$$

esto determina completamente el homomorfismo y comprobaciones rutinarias muestran que $\sigma(f_1)=f_2$.

3. Usamos que la extensiones finitas y normales se pueden caracterizar por ser cuerpo de descomposición de algún polinomio.

   Proposición 0.6.
   Toda extensión $\frac{F}{K}$ de grado dos de un cuerpo es normal.

   Si la extensión es de grado primo, en particular, es finita. Si es finita es algebraica. Tomo $u\in F\setminus K$ por el teorema del grado se verifica que

   $$[F:K]=[F:K(u)][K(u):K]$$

   Si $[K(u):K]=1$ entonces $K(u)=K$ pero $u\notin K$. Contradicción. Por tanto, $[K(u):K]$ es dos. Como la extensión es algebraica existe $Irr(u,K)$ y $gr(Irr(u,K))=2$. Este polinomio tendrá dos raíces en su cuerpo de descomposición, claramente $K(u)$ contiene una raíz pero por las ecuaciones de Cardano-Vieta

   $$(X-\alpha)(X-\beta)=X^2-(\alpha+\beta)X+\alpha\beta$$

   y sabemos que $\alpha+\beta\in K$ luego teniendo u tengo la otra raíz. De modo $K(u)$ es precisamente el cuerpo de descomposición de $Irr(u,K)$ y por tanto, $\frac{F}{K}$ es normal.

   a) $\frac{\mathbb{Q}(\sqrt{2})}{\mathbb{Q}}$ es normal ya que X^2-2 es irreducible sobre $\mathbb{Q}$ por el criterio de Eisenstein y por tanto la extensión tiene grado 2.

   b) $\frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}(\sqrt{2})}$ es normal ya que $X^2-\sqrt{2}$ es irreducible sobre $\mathbb{Q}(\sqrt{2})$ con lo cual la extensión tiene grado 2. En efecto, será irreducible si y solo si no tiene raíces. Las raíces son de la forma $a+b\sqrt{2}$ y operando se llega a la ecuación

   $$a^2+2b^2=\sqrt{2}(1-2ab)$$

   Por distinción de casos, si $1-2ab=0$ entonces se llega a $\sqrt{2}=0$ y si $1-2ab\neq 0$ entonces $\sqrt{2}=\frac{a^2+2b^2}{1-2ab}\in\mathbb{Q}$ ambos casos son contradicciones.

   c) $\frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}}$ no es normal. Si la extensión normal todo polinomio irreducible con una raíz en el cuerpo extensión descompondría en factores lineales. Pero X^4-2 es un polinomio irreducible sobre $\mathbb{Q}$ por el criterio de Eisenstein y $\sqrt[4]{2}$ es una raíz que está en el cuerpo extensión y sin embargo, no puede descomponer en polinomios lineales ya que este cuerpo sólo contiene las raíces reales y hay dos complejas.

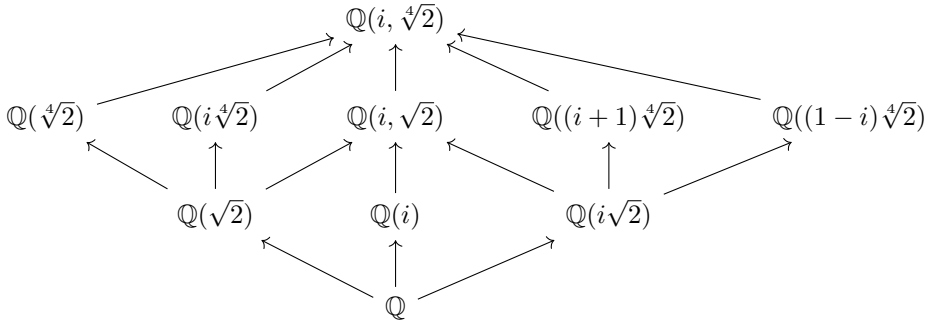
4. La clausura normal de una extensión de generación finita está caracterizada como el cuerpo de descomposición del producto de los irreducibles asociados a los generadores. En este caso sólo hay un generador y el cuerpo de descomposición del polinomio mínimo X^4-2 es conocido como $\mathbb{Q}(\sqrt[4]{2},i)$.

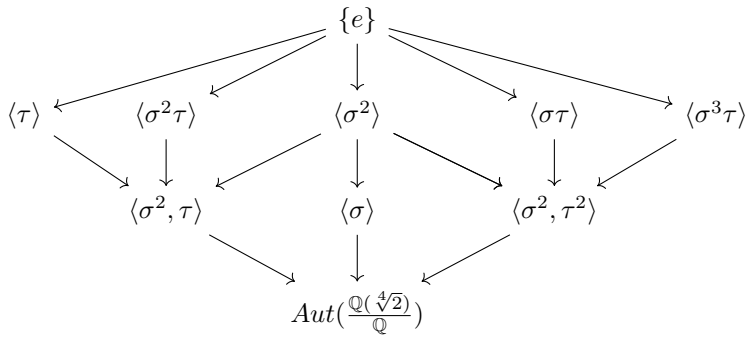
5. Claramente, $\mathbb{Q}(\sqrt[4]{2})$ es el cuerpo de descomposición del polinomio $X^4 - 2$ y como las extensiones finitas de $\mathbb{Q}$ son separables $\frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}}$ es una extensión de Galois. Por tanto,

$$Aut(\frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}}) = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8$$

Los candidatos para ser imagen de $\sqrt[4]{2}$ son $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$ y los candidatos para ser imagen de i son $i, -i$. Luego en efecto, todas estas posibilidades se dan.

La correspondencia de Galois viene expresada mediante los siguientes diagrmas:





donde

$$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$$
$$\sigma(i) = i$$
$$\tau(i) = -i$$
$$\tau(\sqrt[4]{2}) = \sqrt[4]{2}$$

Realizando los cálculo en una tabla, tenemos que τ deja fijo a $\alpha = \sqrt[4]{2}$ por tanto, también deja fijo a α^2. Por otro lado, σ^2 lleva α^2 a α^2. Por tanto, el subgrupo que deja fijo a $\mathbb{Q}(\sqrt{2})$ será $\langle\sigma^2, \tau\rangle$.

Problema 4

Ejercicio 0.9: Sea $\frac{E}{K}$ una extensión finita de Galois y $\alpha \in \frac{E}{K}$. Vamos a determinar el polinomio irreducible de α sobre K.

Consideramos todos los conjugados de α, esto es, el conjunto $C = \{\sigma(\alpha) : \sigma \in Gal(\frac{E}{K})\}$ en el que no hay elementos repetidos ya que es un conjunto, y definimos $f(X) = \prod_{\beta \in C}(X - \beta)$. Entonces α es una raíz de $f(X)$.

1. Prueba que $f(X) \in K[X]$
2. Prueba que $f(X)$ es irreducible sobre K. Como consecuencia $f(X) = Irr(\alpha, K)$.
3. Considera la extensión $\frac{\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})}{\mathbb{Q}}$, prueba que es una extensión de Galois.
4. Determinar $Gal\Big(\frac{\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})}{\mathbb{Q}}\Big)$ y $Irr(\sqrt[3]{3} + \sqrt{-3}, \mathbb{Q})$
5. Considera la clausura normal $E/\mathbb{Q}$ de $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, que es una extensión de Galois y describe E.
6. Determina $Gal(E/\mathbb{Q})$ e $Irr(i + \sqrt{2} + \sqrt{-2}, \mathbb{Q})$.

Solución:

Discutamos primero la información que proporciona el enunciado. Teníamos la definición de conjugados sobre un cuerpo K que podía ser caracterizada como aquellos elementos de la clausura $u, v \in \overline{K}$ que tenían el mismo polinomio mínimo sobre el cuerpo, $Irr(u, K) = Irr(v, K)$.

Desde aquí vamos a observar que dado un $\alpha \in E \setminus K$, sus elementos conjugados son precisamente los que dice el enunciado (si $\alpha \in K$ él es su único conjugado).

Observamos que los automorfismos $\sigma \in Gal(\frac{E}{K})$ extienden a la identidad en K pues por definición fijan los elementos de K. Como el isomorfismo extendido a polinomios con $X \to X$ de la identidad es $\overline{1_K} = 1_{K[X]}$ en particular se tiene que $Irr(\alpha, K) = Irr(\sigma(\alpha), K)$. Por tanto, C está incluido en los conjugados de α.

Pero también se da el recíproco, esto es los conjugados de α están todos en E. En efecto, como la extensión es de Galois finita entonces en particular es normal y entonces $Irr(\alpha, K)$ al ser irreducible y tener una raíz en E descompone en factores lineales en E luego cualquier conjugado de α también está en E.

Finalmente, como $Gal(\frac{E}{K})$ es un grupo claramente $\alpha \in C$ con $\sigma = 1$.

Volviendo al ejercicio:

1. Sea $\sigma \in Gal(\frac{E}{K})$ sabemos que como σ extiende a la identidad las raíces del polinomio f se aplican en raíces del polinomio f mediante σ y como σ es un automorfismo, determina sobre las raíces una permutación.

   Entonces cuando consideramos la extensión de σ a los polinomios con $X \to X$ que denotamos por $\overline{\sigma}$ lo que obtenemos es

   $$\overline{\sigma}(f)(x) = \overline{\sigma}(\prod(x - \beta)) = \prod(x - \sigma(\beta)) = f(x)$$

   Por tanto, σ deja invariantes a los coeficientes del polinomio y como esta igualdad no depende de σ se tiene que $f \in E^G[X] = K[X]$

2. Por la observación previa tenemos que C y el conjunto de los conjugados de α coinciden y en particular tienen el mismo cardinal.

   Observamos también que como la extensión es de Galois finita, es una extensión separable, esto quiere decir que el polinomio $Irr(\alpha, K)$ no tiene raíces múltiples en E, cuerpo en el que descompone totalmente. Por tanto, cada conjugado determina un único factor lineal esto es,

   $$gr(f) = |\{\text{conjugados de } \alpha\}| = gr(Irr(\alpha, K))$$

   y dado que α es raíz de f tenemos que f es un polinomio de grado mínimo del que α es raíz. Por tanto, f es irreducible sobre K y $f = Irr(\alpha, K)$.

3. La extensión es de Galois puesto que es el cuerpo de descomposición del polinomio:

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

   que es separable por ser $\mathbb{Q}$ un cuerpo de característica cero y por tanto perfecto.

4. Consideramos la torre:

   $$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{3}) \subseteq \mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})$$

   El polinomio $X^3 - 3$ es irreducible sobre $\mathbb{Q}$ ya que no tiene raíces en $\mathbb{Q}$ y entonces la primera extensión es de grado 3. La base de la segunda extensión está incluída en $\mathbb{R}$ y entonces claramente el polinomio $X^2 + 3$ es irreducible sobre $\mathbb{Q}(\sqrt[3]{3})$ y por tanto la segunda extensión es de grado 2. Por el teorema del grado, la extensión total es de grado 6. Por tanto, hay exactamente 6 elementos en el grupo de Galois de la extensión. Como grupos de orden $2p$ con p primo sólo hay un cíclico y un diédrico. Por tanto, para clasificar este grupo estudiamos el orden de sus elementos.

   Para hacer los cálculos hay que observar que $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ y que $\omega^2 = -\frac{1}{2} - \frac{\sqrt{-3}}{2}$.

notación	$\sqrt[3]{3}$	$\sqrt{-3}$	orden
Id	$\sqrt[3]{3}$	$\sqrt{-3}$	1
s	$\sqrt[3]{3}$	$-\sqrt{-3}$	2
r	$\omega\sqrt[3]{3}$	$\sqrt{-3}$	3
rs	$\omega\sqrt[3]{3}$	$-\sqrt{-3}$	2
r^2	$\omega^2\sqrt[3]{3}$	$\sqrt{-3}$	3
r^2s	$\omega^2\sqrt[3]{3}$	$-\sqrt{-3}$	2

   En estas condiciones es isomorfo a D_3.

   Para calcular $Irr(\sqrt[3]{3} + \sqrt{-3}, \mathbb{Q})$ tenemos que hacer algunos cálculos:

   $$\alpha = \sqrt[3]{3}+\sqrt{-3} \implies (\alpha-\sqrt{-3})^3 = 3 \implies \alpha^3-3\alpha-3 = \sqrt{-3}(\alpha^2-3) \implies \alpha^6-6\alpha^4-6\alpha^3+3\alpha^2+18\alpha+9 = 0$$

   Para investigar la naturaleza de este polinomio lo reducimos módulo 2 obteniendo $p(X) = X^6 + X^2 + 1$. Vemos que no tiene raíces y entonces no puede tener en $\mathbb{Z}[X]$ factores de grado 1 o 5. El único irreducible de grado en $\mathbb{Z}_2[X]$ es $X^2 + X + 1$ y comprobamos que el resto de la división euclídea es $X + 1$ y por tanto, el polinomio no tiene factores de grado 2 o 4. Sin embargo resulta que $p(X) = (X^3 + X + 1)^2$ lo que nos dice que si tuviera factores serían de grado 3.

   Volviendo a $\mathbb{Z}$ vemos por ensayo y error que $X^6 - 6X^4 - 6X^3 + 3X^2 + 18X + 9 = (X^3 - 3X - 3)^2$ y por el criterio de Eisenstein con $p = 3$ se obtiene que $X^3 - 3X - 3$ es irreducible. De donde, $Irr(\sqrt[3]{3} + \sqrt{-3}, \mathbb{Q}) = X^3 - 3X - 3$.

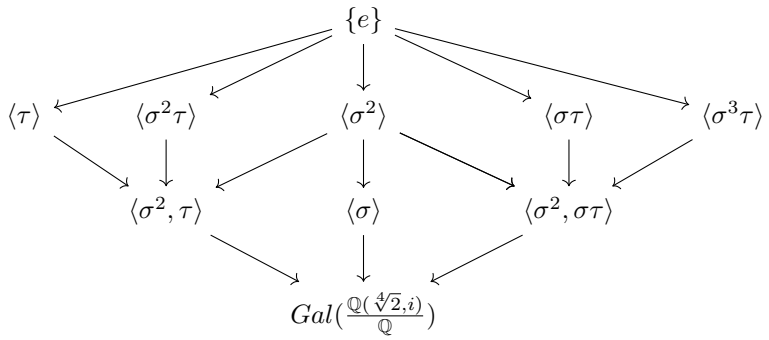
5. Claramente, $Irr(\sqrt[4]{2},\mathbb{Q}) = X^4 - 2$ y su cuerpo de descomposición es $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$. Esta es la clausura normal ya que la extensión es finita y tiene un solo generador. La clausura normal siempre es una extensión normal y en este caso vemos claramente que la extensión es separable puesto que los generadores tienen polinomios mínimos sobre $\mathbb{Q}$ son $X^4 - 2, X^2 + 1$ que tienen todas sus raíces distintas, luego son separables. Por tanto, tenemos una extensión de Galois. Vamos a describir esta extensión.

   Considerando la torre $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$ vemos claramente que la extensión tiene grado 8 y por el teorema de Artin, $|Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = 8$. Para determinar el grupo calculamos los de los elementos.

notación	i	$\sqrt[4]{2}$	orden
Id	i	$\sqrt[4]{2}$	1
σ	i	$i\sqrt[4]{2}$	4
σ^2	i	$-\sqrt[4]{2}$	2
σ^3	i	$-i\sqrt[4]{2}$	4
τ	$-i$	$\sqrt[4]{2}$	2
$\sigma\tau$	$-i$	$-\sqrt[4]{2}$	2
$\sigma^2\tau$	$-i$	$i\sqrt[4]{2}$	2
$\sigma^3\tau$	$-i$	$-i\sqrt[4]{2}$	2

   Si observamos que el grupo no es abeliano entonces tenemos que el grupo es D_4.

   La correspondencia de Galois viene expresada mediante los siguientes diagramas:



   Los subgrupos de orden 2 son cíclicos por ser 2 un primo y por tanto, están generados por los elementos del grupo de orden 2 y por tanto hay 5. Los subgrupos de orden $4 = 2^2$ son o bien cíclicos o bien producto de cíclicos de orden 2. Estos últimos son los llamados de tipo Klein y para identificarlos debemos tomar dos elementos de orden 2 que conmuten entre sí. Se obtienen los subgrupos representados en la figura superior.

   Observamos también que todos los de orden 4, por ser de índice 2 son subgrupos normales y entre los de orden 2 el único que es normal es el generado por el elemento que está el centro del grupo σ^2.

   Ahora pasamos a determinar la conexión de Galois entre estos subgrupos y los subcuerpos de la extensión $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$. Para ello determinamos los cuerpos fijos por cada subgrupo ya que están en biyección. Para elo vemos como actúa cada isomorfismo sobre los elementos de una $\mathbb{Q}$-base.

	α	α^2	α^3	i	$i\alpha$	$i\alpha^2$	$i\alpha^3$
σ	$i\alpha$	$-\alpha^2$	$-i\alpha^3$	i	$-\alpha$	$-i\alpha^2$	α^3
σ^2	$-\alpha$	α^2	$-\alpha^3$	i	$-i\alpha$	$i\alpha^2$	$-i\alpha^3$
σ^3	$-i\alpha$	$-\alpha^2$	$i\alpha^3$	i	α	$-i\alpha^2$	$-\alpha^3$
τ	α	α^2	α^3	$-i$	$-i\alpha$	$-i\alpha^2$	$-i\alpha^3$
$\sigma\tau$	$i\alpha$	$-\alpha^2$	$-i\alpha^3$	$-i$	α	$i\alpha^2$	$-\alpha^3$
$\sigma^2\tau$	$i\alpha$	$-\alpha^2$	$-i\alpha^3$	$-i$	α	$i\alpha^2$	$-\alpha^3$
$\sigma^3\tau$	$-i\alpha$	$-\alpha^2$	$-i\alpha^3$	$-i$	$-\alpha$	$i\alpha^2$	$-i\alpha^3$

Vamos a ir determinando los cuerpos fijos sencillos.

$E^G = \mathbb{Q}$

$E^\sigma = \mathbb{Q}(i)$

$E^{\sigma^2,\sigma\tau} = E^{\sigma^2} \cap E^\tau = \mathbb{Q}(\sqrt{2})$

$E^{\sigma^2,\sigma\tau} = E^{\sigma^2} \cap E^{\sigma\tau} = \mathbb{Q}(i\sqrt{2})$

$E^{\sigma^2} = E^{\sigma^2,\sigma\tau} E^{\sigma^2,\tau} = \mathbb{Q}(i, \sqrt{2})$

$E^\tau = \mathbb{Q}(\sqrt[4]{2})$

Cuando llegamos al $\sigma\tau$ obtendríamos que fija $i\alpha^2$ pero ya había un cuerpo fijo de esta forma. De hecho, ya que $\sigma\tau$ tiene orden 2, el teorema de Artin asegura que $[E : E^H] = 2$ pero como $i\alpha^2$ determina una extensión de grado 2 sobre $\mathbb{Q}$, en realidad el subgrupo debería tener 4 elementos lo cual no es posible. Tenemos que rellenar elementos hasta que el grado de la extensión sobre $\mathbb{Q}$ sea 4.

Para hallar los elementos fijos planteamos la ecuación para $\sigma^3\tau(u) = u$ y escribimos

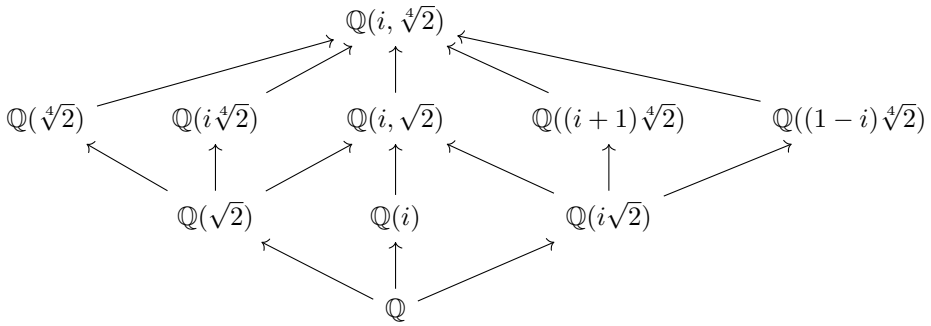
$$u = a_0 \cdot 1 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$

Operando se llega a que todos los coeficientes pueden ser elegidos como 0 y que $a_1 = -a_5$. Haciendo $a_1 = -a_5$ obtenemos un elemento $u = \alpha - i\alpha = (1 - i)\alpha$. El proceso análogo para $\sigma\tau$ da $u = (1 + i)\alpha$. Por tanto los cuerpos correspondientes son:

$E^{\sigma\tau} = \mathbb{Q}((1 + i)\alpha)$

$E^{\sigma^3\tau} = \mathbb{Q}((1 - i)\alpha)$

Tenemos entonces el siguiente diagrama de cuerpos:



6. Por cálculo directo, vemos que si $\alpha = i + \sqrt{2} + \sqrt{-2}$ entonces sería raíz de $p(X) = X^4 + 2X^2 + 16X + 17$. Comprobamos que es difícil reduciendo ver que el polinomio es irreducible. En vez ello

observamos que α está en la extensión $\mathbb{Q}(\sqrt{2}, i)$ y no está en ninguna de las subextensiones. Por tanto, $p(X) = Irr(\alpha, \mathbb{Q})$.

Problema 5

EJERCICIO 0.10: Sea F un cuerpo finito y $0 \neq \alpha \in F$. Prueba que existen elementos $a, b \in F$ tales que $1 + a^2 - \alpha b^2 = 0$.

Solución:

Resovemos la ecuación general $a_1x_1^2 + a_2x_2^2 = 1$ con $a_1, a_2 \neq 0$. Para ello consideremos los conjuntos:

$$S = \{a_1x_1^2 : x_1 \in \mathbb{F}\}$$

$$T = \{1 - a_2x_2^2 : x_2 \in \mathbb{F}\}$$

Vamos a calcular el número de elementos de estos conjuntos. Ahora,

$$a_1x_1^2 = a_2x_1'^2 \implies x_1^2 = x_1'^2 \implies 0 = (x_1 - x_1')(x_1 + x_1') \implies x_1 = x_1' \vee x_1 = -x_1' \implies x_1 = -x_1 \implies 2x_1 = 0$$

Si $Car(F) \neq 2$ entonces tenemos que $x_1 = 0$ eso me dice que cada elemento $a_1x_1^2$ tiene dos elementos de F, $x_1, -x_1$ salvo que $x_1 = 0$ donde el término recoge sólo el valor cero. En consecuencia, $|S| = (|F| - 1)/2 + 1 = (F + 1)/2$. Análogamente, se demuestra que $|T| = (F + 1)/2$. Como $|S| + |T| > |F|$ el principio del palomar da que $\exists x \in S \cap T$ de donde $\exists x_1, x_2, 1 - a_2x_2^2 = x = a_1x_1^2$ y por la igualdad de los extremos, la ecuación tiene solución.

Si $Car(F) = 2$ entonces las ecuaciones $x_1 = x_1' \vee x_1 = -x_1'$ dan que $x_1 = x_1'$ y por tanto, cada término $a_1x_1^2$ recoge un único elemento del cuerpo. Por tanto, $|S| = |T| = |F|$ y de nuevo por el principio del palomar existe un elemento en la intersección que determina una pareja de valores x_1, x_2 solución de la ecuación.

Obsérvese que si $a_1 = 0 \vee a_2 = 0$ entonces la ecuación degenera en una del tipo $a_1x_1^2 = 1$. que tiene solución si y sólo si a_1 es un cuadrado en $\mathbb{F}$ ya que por la conmutatividad del cuerpo finito (si hay dudas, úsese el teorema de Wedderburn) tendríamos $1 = a_1x_1^2 = (t_1x_1)^2$ y bastaría tomar $x_1 = t_1^{-1}$. Recíprocamente, si suponemos que a_1 no es cuadrado entonces a_1^{-1} tampoco lo es y entonces $a_1^{-1} = x_1^2$ no tiene solución.

Centrándonos en nuestra ecuación tenemos que $1 = \alpha b^2 - a^2$. El hecho de pedir $\alpha \neq 0$ es para evitar que degenere ya que entonces quedaría la ecuación $1 = (-1)a^2$ y no está claro a priori en qué cuerpos finitos -1 es un cuadrado de algún elemento. Tenemos que $a_1 = \alpha \neq 0 \wedge a_2 = -1 \neq 0$ y por lo anterior, está ecuación siempre tiene solución.

Problema 6

EJERCICIO 0.11: Sea $\xi = \xi_{14}$ una raíz primitiva décimo cuarta de la unidad sobre $\mathbb{Q}$.

1. Calcula el polinomio ciclotómico $\phi_{14}(X)$ y describe los elementos $\mathbb{Q}(\xi)/\mathbb{Q}$. En particular, queremos conocer el grado de esta extensión.
2. Calcula el grupo $G = Gal(\mathbb{Q}(\xi)/\mathbb{Q})$ y el retículo de subgrupos.
3. Da un generador σ del grupo G; sólo tienes que dar la imagen de ξ.
4. Observa que la extensión $\mathbb{Q}(\xi)/\mathbb{Q}(\xi) \cap \mathbb{R}$ es de grado 2 y que por tanto corresponde a un subgrupo N de G de orden 2 e índice 3, generado por σ^3.
5. Comprueba que $\mathbb{Q}(\xi) \cap \mathbb{R} = \mathbb{Q}(\xi + \xi^{-1})$. Estamos interesados en calcular $Irr(\xi + \xi^{-1}, \mathbb{Q})$; da un método para calcularlo. Entre otras formas puedes calcularlo: (1) resolviendo un sistema de ecuaciones lineales haciendo uso de las potencias, (2) directamente utilizando los conjugados ó (3) haciendo uso de la resultante.
6. A partir del subgrupo H, de orden 3, de G, determina el cuerpo intermedio $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\xi)$ tal que $[\mathbb{Q}(\xi) : F] = 2$ y da un generador θ de la extensión $F/\mathbb{Q}$. Calcula el polinomio irreducible $Irr(\theta, \mathbb{Q})$.

Solución:

1. Si aplicamos la fórmula del cálculo del n-ésimo polinomio ciclotómico mediante la función de Moebius, tenemos que:

$$\phi_{14}(x) = \frac{(x-1)(x^{14}-1)}{(x^2-1)(x^7-1)} = \frac{x^{14}-1}{(x+1)(x^7-1)} = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

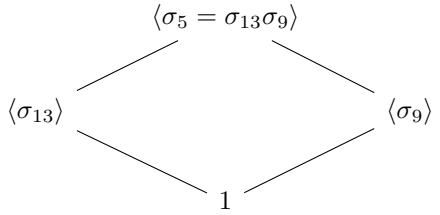
   Si retornamos a la demostración de que $\Phi_n(X)$ es irreducible teníamos un corolario que nos decía que el grado de una extensión ciclotómica era $\phi(n)$. En nuestro caso es $\phi(14) = \phi(2)\phi(7) = 6$. En particular, una base del espacio vectorial es $\{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5\}$ y los elementos de la extensión se expresan como combinaciones lineales de esta base.

2. Nosotros hemos dedicado en nuestras notas un apartado a clarificar el caso de polinomios ciclotómicos racionales basados en el libro de David Cox. En particular, resulta que el grupo de galois de las extensiones ciclotómicas racionales es isomorfo al grupo de las unidades correspondiente. En nuestro caso:

$$Gal(\mathbb{Q}(\xi)/\mathbb{Q}) \cong U(\mathbb{Z}_{14})$$

   Los órdenes de los elementos son $\{3 \mapsto 6, 5 \mapsto 6, 9 \mapsto 3, 11 \mapsto 3, 13 \mapsto 2\}$.

   El isomorfismo que construimos en los apuntes nos dice que de forma natural, los correspondientes a $\langle 13\rangle, \langle 9\rangle$ son $\sigma_{13}(\xi) = \xi^{13}, \sigma_9(\xi) = \xi^9$ y tendríamos el siguiente diagrama:



3. Hemos dado ya el generador σ_5 que actúa como $\sigma_5(\xi) = \xi^5$.

4. Sabemos que en general, el inverso de $c \in \mathbb{C}$ es $\overline{c}/N(c)$ donde N es la norma del complejo. Como trabajamos con raíces de la unidad $N(c) = 1$ y por tanto $c^{-1} = \overline{c}$. Esto es interesante pues entonces $c + c^{-1} = c + \overline{c} \in \mathbb{R}$. Vamos a demostrar que $\mathbb{Q}(\xi) \cap \mathbb{R} = \mathbb{Q}(\xi + \xi^{-1})$.

   En efecto, por lo observado, se tiene la siguiente torre de cuerpos:

   $$\mathbb{Q}(\xi) \supseteq \mathbb{Q}(\xi) \cap \mathbb{R} \supseteq \mathbb{Q}(\xi + \xi^{-1})$$

   Si observamos que ξ es raíz del polinomio $(X - \xi)(X - \xi^{-1}) = X^2 - (\xi^{-1} + \xi)X + 1$. La extensión total no puede ser de grado 1 pues entonces $\mathbb{Q}(\xi) \subseteq \mathbb{R}$. Tampoco puede ser la extensión de la izquierda de grado 1 por idénticos motivos. Queda por tanto, que la extensión de la derecha es de grado 1 y por tanto, $\mathbb{Q}(\xi) \cap \mathbb{R} = \mathbb{Q}(\xi + \xi^{-1})$. En particular, el grado de la extensión de la izquierda es 2 y por el teorema fundamental de la Teoría de Galois, el subgrupo que lo fija tendrá orden 2. Pero en nuestro retículo ya hemos visto que este sólo puede ser σ_{13} y, con nuestra notación, lo que pide el enunciado es comprobar que $(\sigma_5)^3 = \sigma_{13}$. Pero esto se sigue de que $125 \equiv 13\ mod(14)$.

5. La primera parte está hecha. Para calcular el irreducible, vamos a utilizar el método de los conjugados. La idea es que el grupo de Galois G es cíclico y por tanto es abeliano. Por tanto, sus subgrupos serán normales y por el teorema de fundamental de la Teoría de Galois:

   $$Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) = Gal(\mathbb{Q}(\xi)/\mathbb{Q})/Gal(\mathbb{Q}(\xi)/\mathbb{Q}(\alpha)) \cong Gal(\mathbb{Q}(\xi)/\mathbb{Q})/\langle\sigma_{13}\rangle$$

   donde $\alpha = \xi + \xi^{-1}$ y el grupo cociente tendrá tres clases de equivalencia que serán $\{1, \sigma_{13}\}$, $\{\sigma_3, \sigma_{11}\}$, $\{\sigma_5, \sigma_9\}$.

   El irreducible $f(X) = Irr(\alpha, \mathbb{Q})$ debe contener a todas las raíces conjugadas, es decir a todas las raíces que resultan de aplicar uno de los representantes de las clases del grupo de Galois. Como α es raíz y f es el mínimo polinomio del que es raíz necesarimente tendrá que ser f.

   $f(X) = (X - \alpha)(X - \sigma_3(\alpha))(X - \sigma_5(\alpha)) = (X - (\xi + \xi^{-1}))(X - (\xi^3 + \xi^{-3}))(X - (\xi^5 + \xi^{-5}))$

   Desarrollando este producto se tiene que:

   $f(X) = X^3 - (\xi + \xi^{-1} + \xi^3 + \xi^{-3} + \xi^5 + \xi^{-5})X^2 + ((\xi^3 + \xi^{-3})(\xi^5 + \xi^{-5}) + (\xi^3 + \xi^{-3})(\xi^1 + \xi^{-1}) + (\xi^1 + \xi^{-1})(\xi^5 + \xi^{-5}))X + (\xi^5 + \xi^{-5})(\xi^1 + \xi^{-1})(\xi^3 + \xi^{-3})$

   El proceso para obtener estos coeficientes, es calcular su expresión como polinomios (sin exponentes negativos) y luego dividir por el polinomio mínimo de ξ esto es, el polinomio ciclotómico calculado en el primer apartado. En estas condiciones se obtiene que:

   $f(X) = X^3 - X^2 - 2X + 1$

6. El subgrupo de orden 2 es el generado por σ_{13}. Por el teorema fundamental de la teoría de Galois tendremos que $|\langle\sigma_{13}\rangle| = [\mathbb{Q}(\xi) : F] = 2$ para un único subcuerpo F. De aquí, $[F : \mathbb{Q}] = 3$ y por tanto, la extensión tiene que ser primitiva. Observando que $\xi + \xi^{-1}$ queda fija por σ_{13}, la extensión admite como generador a $\xi + \xi^{-1}$ y su irreducible es el del apartado anterior.

Problema 7

EJERCICIO 0.12: Se considera $f \in \mathbb{Q}$ un polinomio de grado seis tal que $Gal(f/\mathbb{Q}) \cong S_6$. Llamamos $E = \mathbb{Q}[f]$ al cuerpo de descomposición de f.

1. Determina cuántos cuerpos intermedios $\mathbb{Q} \subseteq F \subseteq E$ existen tales que $[E : F] = 9$.
2. Prueba que la intersección de los cuerpos F,del apartado anterior, contiene propiamente a $\mathbb{Q}$.
3. Si $\alpha_1 \in E$ es una raíz de f, prueba que $Gal(E/\mathbb{Q}(\alpha_1)) \cong S_5$.
4. Prueba que $\mathbb{Q}(\alpha_1)$ no está contenido en ningún F.
5. Si $\alpha_1 \neq \alpha_2 \in E$ es otra raíz de f, prueba que $Irr(\alpha_2, \mathbb{Q}(\alpha_1))$ tiene grado 5.

Solución:

1. Si $[E : F] = 9$ habrá tantos como subgrupos de orden 9 tenga S_6. Estos pueden ser a priori, tipo C_9 o tipo $C_3 \times C_3$. Usando la descomposición de permutaciones en ciclos disjuntos y que permutaciones disjuntas tienen como orden el mínimo común múltiplo de los órdenes de las permutaciones, se deduce que el máximo orden es 6. Por tanto, todos deben ser tipo $C_3 \times C_3$.

   Los subgrupos de este tipo son generados por ciclos disjuntos de la forma $\langle (123), (456) \rangle$. Para ello, primero se observa que este grupo tiene que tener 9 elementos. En efecto, como los generadores conmutan, el grupo generado tiene que ser de la forma $(123)^{n_1}(456)^{n_2}$ con $n_1, n_2 \in \mathbb{N}$. Como los ciclos son de orden 3 tenemos a priori nueve elementos que serán claramente distintos.

   Por otro lado, observemos que los subgrupos de orden 9 son p-subgrupos de Sylow ya que 9 es la mayor potencia de 3 que divide a 6!. Por el segundo teorema de Sylow, los p-subgrupos son conjugados y recordando la acción de la conjugación $\alpha(123)\alpha^{-1} = (\alpha(1)\alpha(2)\alpha(3))$ sobre ciclos, observaremos que en la expresión $(123)^{n_1}(456)^{n_2}$ podemos hacer actuar la conjugación en cada elemento generador como $\alpha(123)^{n_1}(456)^{n_2}\alpha^{-1} = \alpha(123)^{n_1}\alpha^{-1}\alpha(456)^{n_2}\alpha^{-1}$ de modo que se obtiene la expresión del subgrupo $\langle (\alpha(1)\alpha(2)\alpha(3)), (\alpha(4)\alpha(5)\alpha(6)) \rangle$.

   Hay por tanto, $\frac{\binom{6}{3}}{2} = 10$ subgrupos.

2. Primero, por la teoría de Galois, sabemos que $\cap F$ se corresponde con $\vee H$ donde los H son los subgrupos que fijan los F.

   Segundo, para los ciclos anteriores se verifica $\langle (123), (456) \rangle = \langle (123) \rangle \cdot \langle (456) \rangle = \langle (123) \rangle \vee \langle (456) \rangle$ donde hemos utilizado la descripción de los subgrupos generados por conjuntos finitos y el teorema del producto de Lederman (en nuestras notas le damos este nombre).

   En consecuencia, el subgrupo buscado es $\vee H = \vee$ 3-ciclos de $S_6 \leq A_6$ está formado por permutaciones pares y en consecuencia, no puede ser el total. De nuevo, por la correspondencia de Galois el cuerpo correspondiente no es $\mathbb{Q}$.

3. Como $Gal(f/\mathbb{Q}) \cong S_6$ sabemos que f es irreducible ya que S_6 es transitivo en S_6. Por tanto, $[\mathbb{Q}(\alpha_1) : F] = 6$ y $|Gal(E/\mathbb{Q}(\alpha_1))| = [E : \mathbb{Q}(\alpha)] = 5!$. Pero es claro que las permutaciones de $Gal(f/\mathbb{Q})$ se ven como permutaciones de S_5 si las obligamos a fijar α_1. Por tanto, $Gal(E/\mathbb{Q}(\alpha_1)) \cong S_5$.

4. Si $\mathbb{Q}(\alpha_1) \subseteq F$ entonces $H \leq S_5$ donde H es el subgrupo que fija a F. Pero esto es imposible ya que $9 = |F| \nmid |S_5| = 120$.

5. El polinomio $\prod_{i=2}^{6}(x-\alpha_i) \in \mathbb{Q}(\alpha_1)[X]$ por el algoritmo de la división sobre cuerpos. Claramente, α_2 es una raíz de este polinomio y dado que hemos visto que el grupo de Galois es S_5 que es un subgrupo transitivo de S_5, tendremos que el polinomio es irreducible. Por tanto:

$$Irr(\alpha_2, \mathbb{Q}(\alpha_1)) = \prod_{i=2}^{6}(x-\alpha_i)$$

que tiene grado 5.

Problema 8

EJERCICIO 0.13: Se considera $f \in \mathbb{Q}$ un polinomio de grado seis tal que $Gal(f/\mathbb{Q}) \cong S_6$. Llamamos $E = \mathbb{Q}[f]$ al cuerpo de descomposición de f.

1. Determina cuántos cuerpos intermedios $\mathbb{Q} \subseteq F \subseteq E$ existen tales que $[E : F] = 9$.
2. Prueba que la intersección de los cuerpos F,del apartado anterior, contiene propiamente a $\mathbb{Q}$.
3. Si $\alpha_1 \in E$ es una raíz de f, prueba que $Gal(E/\mathbb{Q}(\alpha_1)) \cong S_5$.
4. Prueba que $\mathbb{Q}(\alpha_1)$ no está contenido en ningún F.
5. Si $\alpha_1 \neq \alpha_2 \in E$ es otra raíz de f, prueba que $Irr(\alpha_2, \mathbb{Q}(\alpha_1))$ tiene grado 5.

Solución:

1. Si $[E : F] = 9$ habrá tantos como subgrupos de orden 9 tenga S_6. Estos pueden ser a priori, tipo C_9 o tipo $C_3 \times C_3$. Usando la descomposición de permutaciones en ciclos disjuntos y que permutaciones disjuntas tienen como orden el mínimo común múltiplo de los órdenes de las permutaciones, se deduce que el máximo orden es 6. Por tanto, todos deben ser tipo $C_3 \times C_3$.

   Los subgrupos de este tipo son generados por ciclos disjuntos de la forma $\langle (123), (456) \rangle$. Para ello, primero se observa que este grupo tiene que tener 9 elementos. En efecto, como los generadores conmutan, el grupo generado tiene que ser de la forma $(123)^{n_1}(456)^{n_2}$ con $n_1, n_2 \in \mathbb{N}$. Como los ciclos son de orden 3 tenemos a priori nueve elementos que serán claramente distintos.

   Por otro lado, observemos que los subgrupos de orden 9 son p-subgrupos de Sylow ya que 9 es la mayor potencia de 3 que divide a 6!. Por el segundo teorema de Sylow, los p-subgrupos son conjugados y recordando la acción de la conjugación $\alpha(123)\alpha^{-1} = (\alpha(1)\alpha(2)\alpha(3))$ sobre ciclos, observaremos que en la expresión $(123)^{n_1}(456)^{n_2}$ podemos hacer actuar la conjugación en cada elemento generador como $\alpha(123)^{n_1}(456)^{n_2}\alpha^{-1} = \alpha(123)^{n_1}\alpha^{-1}\alpha(456)^{n_2}\alpha^{-1}$ de modo que se obtiene la expresión del subgrupo $\langle (\alpha(1)\alpha(2)\alpha(3)), (\alpha(4)\alpha(5)\alpha(6)) \rangle$.

   Hay por tanto, $\frac{\binom{6}{3}}{2} = 10$ subgrupos.

2. Primero, por la teoría de Galois, sabemos que $\cap F$ se corresponde con $\vee H$ donde los H son los subgrupos que fijan los F.

   Segundo, para los ciclos anteriores se verifica $\langle (123), (456) \rangle = \langle (123) \rangle \cdot \langle (456) \rangle = \langle (123) \rangle \vee \langle (456) \rangle$ donde hemos utilizado la descripción de los subgrupos generados por conjuntos finitos y el teorema del producto de Lederman (en nuestras notas le damos este nombre).

   En consecuencia, el subgrupo buscado es $\vee H = \vee$ 3-ciclos de $S_6 \leq A_6$ está formado por permutaciones pares y en consecuencia, no puede ser el total. De nuevo, por la correspondencia de Galois el cuerpo correspondiente no es $\mathbb{Q}$.

3. Como $Gal(f/\mathbb{Q}) \cong S_6$ sabemos que f es irreducible ya que S_6 es transitivo en S_6. Por tanto, $[\mathbb{Q}(\alpha_1) : F] = 6$ y $|Gal(E/\mathbb{Q}(\alpha_1))| = [E : \mathbb{Q}(\alpha)] = 5!$. Pero es claro que las permutaciones de $Gal(f/\mathbb{Q})$ se ven como permutaciones de S_5 si las obligamos a fijar α_1. Por tanto, $Gal(E/\mathbb{Q}(\alpha_1)) \cong S_5$.

4. Si $\mathbb{Q}(\alpha_1) \subseteq F$ entonces $H \leq S_5$ donde H es el subgrupo que fija a F. Pero esto es imposible ya que $9 = |F| \nmid |S_5| = 120$.

5. El polinomio $\prod_{i=2}^{6}(x-\alpha_i) \in \mathbb{Q}(\alpha_1)[X]$ por el algoritmo de la división sobre cuerpos. Claramente, α_2 es una raíz de este polinomio y dado que hemos visto que el grupo de Galois es S_5 que es un subgrupo transitivo de S_5, tendremos que el polinomio es irreducible. Por tanto:

$$Irr(\alpha_2, \mathbb{Q}(\alpha_1)) = \prod_{i=2}^{6}(x-\alpha_i)$$

que tiene grado 5.

Problema 9

Ejercicio 0.14: Elabora un programa, en el lenguaje de programación que desees, que calcule el grupo de Galois de un polinomio de grado 5 sobre el cuerpo de los números racionales. El polinomio dado no tiene por qué ser irreducible.

Solución:

Describimos a continuación los aspectos más relevantes de la implementación de este problema en Sage.

Nosotros hemos programado la clasificación de los grupos de Galois de los polinomios desde grado 2 hasta grado 5.

El caso 2 y 3 no tienen dificultad.

Para el caso 4 sugerimos utilizar la función discriminant() de la que nos provee Sage ya que o bien la fórmula de los apuntes es errónea o bien la traslación de la fórmula que nosotros hicimos era errónea pero daban resultados distintos. Una condición útil para comprobar que la fórmula es correcta es que vale cero si y sólo si dos coeficientes valen cero.

Otro aspecto interesante es la comprobación de la hipótesis c de la proposición 17.2 de los apuntes. Este apartado comprueba que el grupo de Galois es C4 comprobando la pertenecia de dos raíces a un cuerpo extensión por la raíz del discriminante. A la hora de llevar esto a la práctica nos ha resultado útil la observación de Keith Konrad en sus notas *Galois groups of cubics and quartics (not it characteristic 2)* que reduce esta comprobación a comprobar que las raíces multiplicadas por el discriminante del polinomio son cuadrados de números racionales.

Para estudiar la factorización de polinomios en cuerpos extensión debemos agradecer a la comunidad de `ask.sagemath.org` sus ideas si bien para obtener una solución en especial recomendamos las siguientes cuestiones:

- Factorization of $f \in \mathbb{Q}[X]$ in field extension $\mathbb{Q}(\alpha)$.
- Extension field adjoining two roots.

Como observación final notaremos que hemos utilizado en el código que $\mathbb{Q}$ es un cuerpo perfecto y por tanto todo irreducible es separable, esto es, tiene raíces distintas. Esto por ejemplo en el caso de la clasificación de C_5.

El programa completo se encuentra en el archivo *galois.ipynb*. También contiene algunos ejemplos para comprobar la implementación. En particular, tenemos infinitos ejemplos de cíclicas dadas por la expresión de la quíntica de Emma Lehmer. A este respecto recomendamos en `ask.sagemath.org` la pregunta *Any more cyclic quintics*. En concreto, notaremos que la segunda fórmula no puede ser utilizada para parámetros arbitrarios.