Problemas de Teoría de Cuerpos

Rodrigo Raya Castellano
Universidad de Granada

1. Problema 3

EJERCICIO 1.1: 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 1.1 (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 1.2.
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:

$$\begin{tikzcd}
 & & \mathbb{Q}(i, \sqrt[4]{2}) & & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[urr] & \mathbb{Q}(i\sqrt[4]{2}) \arrow[ur] & \mathbb{Q}(i, \sqrt{2}) \arrow[u] & \mathbb{Q}((i+1)\sqrt[4]{2}) \arrow[ul] & \mathbb{Q}((1-i)\sqrt[4]{2}) \arrow[ull] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[ul] \arrow[u] \arrow[ur] & \mathbb{Q}(i) \arrow[u] & \mathbb{Q}(i\sqrt{2}) \arrow[ul] \arrow[u] \arrow[ur] & \\
 & & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & & \{e\} \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\langle \tau \rangle \arrow[dr] & \langle \sigma^2\tau \rangle \arrow[d] & \langle \sigma^2 \rangle \arrow[dl] \arrow[d] \arrow[dr] & \langle \sigma\tau \rangle \arrow[d] & \langle \sigma^3\tau \rangle \arrow[dl] \\
 & \langle \sigma^2, \tau \rangle \arrow[dr] & \langle \sigma \rangle \arrow[d] & \langle \sigma^2, \tau^2 \rangle \arrow[dl] & \\
 & & Aut(\frac{\mathbb{Q}(\sqrt[4]{2})}{\mathbb{Q}}) & &
\end{tikzcd}$$

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 $\langle \sigma^2, \tau \rangle$.

2. Problema 4

EJERCICIO 2.1: 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 $Gal\left(\frac{\mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})}{\mathbb{Q}}\right)$ y $Irr(\sqrt[3]{3} + \sqrt{-3}, \mathbb{Q})$

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

En estas condiciones es isomorfo a D_3.