Departamento de Álgebra,
Geometría y Topología.
Universidad de Málaga.

Ejercicios de Álgabra Clásica

Relación 11.
Teorema fundamental de la teoría de Galois.

31 de mayo de 2014.

Profesor de la asignatura:
José Antonio Cuenca Mira.

11. Teorema fundamental de la teoría de Galois

11.1 Sea $K = \mathbb{Q}(x)$. Determinar los casos en que $K/\mathbb{Q}$ es una extensión de Galois, siendo:

a) x es raíz del polinomio $X^2 + bX + c$ $(b, c \in \mathbb{Q})$.

b) x es raíz del polinomio $X^3 - d$ $(d \in \mathbb{Z}, d > 0)$.

11.2 Sea K/F una extensión de Galois finita. Mostrar que si n es el grado de la extensión entonces el número de cuerpos intermedios no puede ser mayor que 2^n.

11.3 Sea K/F una extensión finita de cuerpos y G un grupo de F-automorfismos de K. Mostrar que G es finito y su orden $|G|$ divide a $[K : F]$. Comprobar que se da la igualdad $|G| = [K : F]$ si y sólo si $G(K/F) = G$.

11.4 Dar el cuerpo de descomposición sobre $\mathbb{Q}$ de cada uno de los polinomios siguientes:

$$(X^3 - 1)(X^2 - 3)(X^4 - 1), \quad (X^2 - 2)(X^2 + 1), \quad (X^3 - 2)(X^2 + 3).$$

Dar en cada uno de los casos el grado de las extensiones correspondientes y establecer explicitamente las biyecciones subgrupo-subcuerpo del teorema fundamental de la teoría de Galois.

11.5 Sea $K = \mathbb{Q}(\sqrt{3}, \sqrt{5}, x)$ donde $x^2 = (1 - \sqrt{3})(2 + \sqrt{5})$. Demostrar que $K/\mathbb{Q}$ no es una extensión de Galois. Determinar el grupo de los $\mathbb{Q}$-automorfismos de K.

11.6 Suponer que K/F es una extensión de Galois cuyo grupo de Galois G es de orden 8 y puede darse por generadores y relaciones por

$$G = \langle \alpha, \beta, \gamma : \ \alpha^2 = \beta^2 = \gamma^2 = 1, \beta\gamma = \alpha\gamma\beta, \alpha\beta = \beta\alpha, \alpha\gamma = \gamma\alpha \rangle$$

Determinar el número de cuerpos estrictamente comprendidos entre K y F. Dar los enteros n para los que existe algún cuerpo intermedio de grado n sobre F y determinar el número de ellos para cada uno de estos enteros.

11.7 Dar el grupo de Galois del cuerpo de descomposión del polinomio $X^4 - 5$ sobre cada uno de los cuerpos siguientes:

$$\mathbb{Q}, \quad \mathbb{Q}(\sqrt{5}), \quad \mathbb{Q}(\sqrt{-5}), \quad \mathbb{Q}(i).$$

11.8 Sea z un número algebraico y F un subcuerpo de $\mathbb{C}$. Mostrar que $[F(z) : F] \leq [\mathbb{Q}(z) : \mathbb{Q}]$ y que, en el caso en que $\mathbb{Q}(z)/\mathbb{Q}$ sea normal, también lo es la extensión $F(z)/F$, teniéndose entonces que $[F(z) : F]$ divide a $[\mathbb{Q}(z) : \mathbb{Q}]$.

11.9 Considérese el polinomio con coeficientes en $\mathbb{Z}/(2)$ siguiente $f(X) = X^6 + X + 1$.

a) Demostrar que $f(X)$ es un polinomio irreducible de $[\mathbb{Z}/(2)][X]$.

b) Sea x una raíz de f en una clausura algebraica de $\mathbb{Z}/(2)$ y $K = (\mathbb{Z}/(2))(x)$. ¿ Es K un cuerpo de descomposición de $f(X)$.

c) Determinar el grado del cuerpo de descomposición de f sobre $\mathbb{Z}/(2)$ y dar el retículo de cuerpos intermedios de dicha extensión.

11.10 Sea F un cuerpo finito de q elementos y K/F una extensión finita. Comprobar que la aplicación $\psi : K \longrightarrow K$ dada por $\psi : x \mapsto x^q$ es un F-automorfismo de K y que todo elemento del grupo de Galois $G(K/F)$ es una potencia de ψ. Mostrar, en particular, que los automorfismos de un cuerpo finito son potencia de su automorfismo de Frobenius.

11.11 Sea Ω una clausura algebraica de un cuerpo finito. Demostrar que la identidad es el único automorfismo de Ω que tien orden finito.

11.12 Demostrar que todos los cuerpos intermedios de la extensión $\mathbb{Q}(\sqrt{2}, i)$ son extensiones normales de $\mathbb{Q}$. Dar para cada uno de ellos un polinomio del que sea cuerpo de descomposición sobre $\mathbb{Q}$.

11.13 Sea K/F una extensión de Galois finita, p un primo positivo y s un entero tal que $p^s | [K : F]$ pero $p^{s+1} \not| [K : F]$. Demostrar que existe una cadena de subcuerpos

$$F = F_0 \subset F_1 \subset \cdots \subset F_{s+1} = K$$

tal que $p \not| [F_1 : F]$ y de manera que para cada $i \in \{1, \ldots, r\}$ la extensión F_{i+1}/F_i es normal de grado p.

11.14 Sea $K = \mathbb{C}(t)$ donde t es trascendente sobre $\mathbb{C}$ y ω un número complejo tal que $\omega^3 = 1$, $\omega \neq 1$. Sean σ y τ los automorfismos de K que dejan fijo cada elemento de $\mathbb{C}$ y para los que se satisfacen las igualdades $\sigma(t) = \omega t$ y $\tau(t) = t^{-1}$. Demostrar que

$$\sigma^3 = \mathrm{Id} = \tau^2, \quad \tau \circ \sigma = \sigma^{-1} \circ \tau$$

Comprobar que el grupo G de los automorfismos generado por σ y τ tiene orden 6. Demostrar que el cuerpo fijo de G es $\mathbb{C}(u)$, donde $u = t^3 + t^{-3}$.

11.15 Sea K/F una extensión de Galois de grado 4 cuyo grupo de Galois es isomorfo a $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Supóngase F de característica distinta de 2. Demostrar que $K = F(x, y)$, siendo x e y elementos con cuadrados en el cuerpo F.

11.16 Sea K/F una extensión de cuerpos finita, E_1 y E_2 cuerpos estrictamente comprendidos entre K y F y tales que K coincide con el menor subcuerpo $E_1 \vee E_2$ que contiene tanto a E_1 como a E_2. Demostrar:

a) Si E_1/F es una extensión de Galois entonces también lo es K/E_2, pudiéndose identificar $G(K/E_2)$ con un subgrupo de $G(E_1/F)$. Mostrar que si además $E_1 \cap E_2 = F$ entonces $G(K/E_2) \equiv G(E_1/F)$.

b) Si E_1 y E_2 son extensiones de Galois de F entonces K/F es una extensión de Galois y en el caso en que $E_1 \cap E_2 = F$ se tiene $G(K/F) \equiv G(K/E_1) \times G(K/E_2)$.

11.17 Sea F un cuerpo finito y K el cuerpo de descomposición sobre F de un polinomio irreducible de grado 3. Demostrar que el grupo de Galois de la extensión K/F es isomorfo al grupo alternado A_3.

11.18 Sea F un cuerpo que contiene alguna raíz primitiva n-ésima de la unidad y $X^n - a$, $X^n - b$ dos polinomios irreducibles de $F[X]$. Demostrar que estos dos polinomios tienen el mismo cuerpo de descomposición si existe algún entero positivo r primo relativo con n tal que $b = a^r c^n$ para algún $c \in F$. Comprobar que si los cuerpos de descomposición coinciden y F tiene característica cero o un primo que no divide a n entonces se satisface una igualdad como la precedente.

11.19 Sea F un cuerpo y $F(X)$ el cuerpo de funciones racionales en la indeterminada X. Considérese el conjunto de los automorfismos de $F(X)$ dados por

$$\begin{array}{lll} f(X) \mapsto f(X), & f(X) \mapsto f(1-X), & f(X) \mapsto f\left(\frac{1}{X}\right) \\ f(X) \mapsto f\left(1 - \frac{1}{X}\right), & f(X) \mapsto f\left(\frac{1}{1-X}\right), & f(X) \mapsto f\left(\frac{X}{X-1}\right) \end{array}$$

Demostrar que estos automorfismos constituyen un subgrupo G del grupo de todos los automorfismos de $F(X)$ que dejan fijo a cada uno de los elementos de F y que el cuerpo fijo de G coincide con $F(T)$, siendo T el elemento de $F(X)$ definido por la igualdad siguiente:

$$T(X) = \frac{(X^2 - X + 1)^3}{X^2(X-1)^2}$$

11.20 Sea F un cuerpo y $K = F(X)$ el cuerpo de funciones racionales sobre F. Demostrar que las aplicaciones dadas por

$$f(X) \mapsto f(X), \quad f(X) \mapsto f\left(\frac{1}{1-X}\right), \quad f(X) \mapsto f\left(1 - \frac{1}{X}\right)$$

constituyen un subgrupo del grupo de automorfismos del ejercicio anterior. Sea E su cuerpo fijo. Determinar $[E : F]$ y dar un elemento que genere K sobre E y otro que genere E sobre F.

11.21 Sea F un cuerpo de característica prima p y $K = F(t)$ un cuerpo extensión del cuerpo dado con t trascendente sobre F. Sean σ y τ los F-automorfismos de K que actúan sobre t del modo siguiente

$$\sigma : t \mapsto -t \qquad \tau : t \mapsto 1 - t.$$

Demostrar que el subgrupo de los F-automorfismos generado por σ y τ es finito. Determinar el cuerpo fijo del mismo.

11.22 Sea K/F una extensión normal. Mostrar la existencia de un cuerpo intemedio I de la extensión K/F tal que I/F es una extensión puramente inseparable y K/I es extensión separable. Comprobar que, si K_s es la clausura separable de la extensión K/F, entonces $K_s \cap I = F$.

11.23 Sea $F(t)/F$ una extensión de cuerpos en la que t es trascendente sobre F. Sea G el grupo de Galois de dicha extensión. Demostrar que existe un homomorfismo de grupos

$$\varphi : \mathrm{GL}_2(F) \longrightarrow G$$

cuyo dominio $\mathrm{GL}_2(F)$ es el grupo de todas las matrices no singulares 2×2 con coeficientes en F y que está definido del siguiente modo

$$\varphi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{Bmatrix} a & b \\ c & d \end{Bmatrix}.$$

Aquí se denota por

$$\begin{Bmatrix} a & b \\ c & d \end{Bmatrix}$$

al F-automorfismo de $F(t)$ que transforma el elemento t en $\frac{(at+b)}{(ct+d)}$. Demostrar que

$$\ker \varphi = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : \quad 0 \neq a \in F \right\}$$

y que G es isomorfo al grupo lineal proyectivo general $\mathrm{PGL}_2(F)$.

11.24 Sea F un cuerpo finito con q elementos y $K = F(X)$. Sea G el grupo de los F-automorfismos de K. Demostrar:

a) El orden de G es $q^3 - q$.

b) El cuerpo fijo de G es $F(Y)$ donde

$$Y = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}$$

c) Sea H_1 el subgrupo de los F-automorfismos de K tales que $X \mapsto aX + b$ con $a \neq 0$ y H_2 el subgrupo de H_1 formado por los F-automorfismos que tansforman X en $X+b$. Comprobar que los cuerpos fijos de H_1 y H_2 son $F(T)$ y $F(Z)$, donde $T = (X^q - X)^{q-1}$ y $Z = X^q - X$.

11.25 Sea F un cuerpo y $\bar{F}$ una clausura algebraica de F. Supóngase que τ es un automorfismo de $\bar{F}$ que deja fijo a cada elemento de F. Sea E el cuerpo fijo del subgrupo generado por τ. Demostrar que cualquier extensión finita de E es cíclica.

11.26 Un cuerpo F se dice cuasi-finito si es perfecto y para cada entero $n > 0$ existe una única extensión de F de grado n contenida en una clausura algebraica $\bar{F}$ de F. Demostrar que si F es un cuerpo cuasi-finito cualquier extensión finita K/F es de Galois y cíclica.

11.27 Sea F un cuerpo de característica el primo positivo p. Sea K/F una extensión cíclica de grado p y σ un automorfsmo generador del grupo de Galois. Demostrar que la aplicación lineal $S : K \longrightarrow K$ dada por $S : u \mapsto u - \sigma(u)$ es nilpotente y existe en consecuencia algún elemento x que está en el núcleo de S^2 y no en el de S. Mostrar que $y = x(\sigma(x) - x)^{-1}$ satisface $\sigma(y) = y + 1$. Obtener entonces que y es raíz de un polinomio de $F[X]$ del tipo $X^p - X - a$.