Ecuaciones Algebraicas. Examen de septiembre. 2006/7. Solución de los problemas

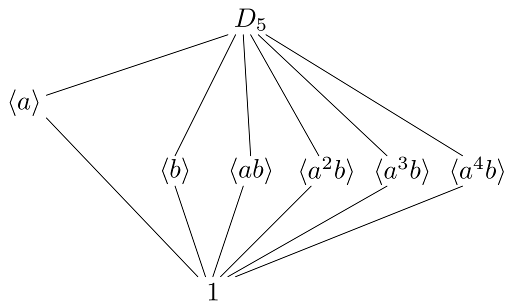
1. **Resolver el siguiente sistema de ecuaciones**

$$\begin{array}{rcl} x_1 + x_2 + x_3 &=& 2 \\ x_1^2 + x_2^2 + x_3^2 &=& 4 \\ x_1^3 + x_2^3 + x_3^3 &=& 5 \end{array}$$

Si ponemos $s_1 = S_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$, $s_2 = S_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ y $s_3 = S_3(x_1x_2x_3)$, entonces de las Fórmulas de Cardano-Vieta se deduce que x_1, x_2 y x_3 son las raíces del polinomio $T^3 - s_1T^2 + s_2T - s_3$. Sabemos que $s_1 = 2$. Además $4 = x_1^2 + x_2^2 + x_3^2 = s_1^2 - 2s_2 = 4 - 2s_2$, con lo que $s_2 = 0$, y $5 = x_1^3 + x_2^3 + x_3^3 = s_1^3 - 3s_1s_2 + 3s_3 = 8 + 3s_3$ y, por tanto, $s_3 = -1$. Luego x_1, x_2 y x_3 son las raíces del polinomio $T^3 - 2T^2 + 1$. Claramente una de estas raíces es 1 y tenemos $T^3 - 2T^2 + 1 = (T-1)(T^2 - T - 1)$. Por tanto $\{x_1, x_2, x_3\} = \left\{1, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}$.

2. **Calcular todos los subgrupos del grupo diédrico D_5 de orden 10 y decir cuales de ellos son normales. ¿Cuántos subcuerpos de grado 2 sobre $\mathbb{Q}$ tiene una extensión de Galois K de $\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_5$? ¿Y cuántos de grado 5 sobre $\mathbb{Q}$? ¿Cuantos subcuerpos de K son extensiones de Galois de $\mathbb{Q}$?**

Como D_5 tiene orden 10, los subgrupos propios no triviales de D_5 tienen orden 2 ó 5, con lo que todos son cíclicos y por tanto para calcular todos los subgrupos basta con calcular los grupos cíclicos. Si ponemos $D_5 = \langle a, b\rangle$ con a de orden 5, b de orden 2 y $ba = a^{-1}b$, entonces D_5 tiene un elemento de orden 1, cuatro elementos de orden 5 (a, a^2, a^3 y a^4) y cinco elementos de orden 2 (b, ab, a^2b, a^3b, a^4b) por tanto el diagrama de los subgrupos de D_5 es el siguiente y los únicos subgrupos normales son 1, $\langle a\rangle$ y D_5.



Utilizando el Teorema Fundamental de la Teoría de Galois, el cuerpo K tiene tantos subcuerpos de índice n sobre $\mathbb{Q}$ como subgrupos de índice n tenga el grupo D_5 y tiene tantos subcuerpos que sean extensiones de Galois de $\mathbb{Q}$ como subgrupos normales tenga D_5. Por tanto, K tiene un único subcuerpo de índice 2 sobre $\mathbb{Q}$, que es una extensión normal de $\mathbb{Q}$ y cinco subcuerpos de índice 5 sobre $\mathbb{Q}$, ninguno de los cuales es una extensión normal de $\mathbb{Q}$. Aparte del cuerpo de índice 2 sobre $\mathbb{Q}$, K tiene dos subcuerpos más que son extensiones normales de $\mathbb{Q}$, a saber K y $\mathbb{Q}$.

3. **Sea F un cuerpo con p^{30} elementos, donde p es un número primo. ¿Cuántos subcuerpos tiene F? ¿Cuántos elementos tiene cada uno de ellos?**

Sabemos que toda extensión de cuerpos finitos es de Galois con grupo de Galois cíclico. Por tanto $F/\mathbb{Z}_p$ es una extensión de Galois con $G = \mathrm{Gal}(F/\mathbb{Z}_p)$ cíclico de orden 30. Entonces G tiene exáctamente un subgrupo de orden d para cada divisor d de 30, es decir tiene seis subgrupos de órdenes 1, 2, 3, 5, 10, 15 y 30 respectivamente y por tanto F tiene seis subcuerpos con cardinales $p, p^2, p^3, p^5, p^{10}, p^{15}$ y p^{30} respectivamente.

4. **Sea L/K una extensión de Galois finita y sea H un subgrupo de $\mathrm{Gal}(L/K)$. Para cada $\alpha \in L$ ponemos $\mathrm{tr}_H(\alpha) = \sum_{h\in H} h(\alpha)$ y $N_H(\alpha) = \prod_{h\in H} h(\alpha)$. Demostrar que se verifican las siguientes condiciones para todo $\alpha, \beta \in L$:**

   (a) $\mathrm{tr}_H(\alpha)$ **y** $N_H(\alpha)$ **pertenecen a** $F^H = \{x \in L : h(x) = x,$ **para todo** $h \in H\}$**.**

   (b) $\mathrm{tr}_H(\alpha + \beta) = \mathrm{tr}_H(\alpha) + \mathrm{tr}_H(\beta)$ **y** $N_H(\alpha\beta) = N_H(\alpha)N_H(\beta)$**.**

   (c) Supongamos ahora que $L = \mathbb{Q}(\xi_5)$ y $K = \mathbb{Q}$ y $H = \langle\sigma\rangle$, donde σ es el automorfismo de L dado por $\sigma(\xi_5) = \xi_5^{-1}$. Encontrar un elemento de L^H que no pertenezca a $\mathbb{Q}$.

(a) Obsérvese que para cada $x \in H$ la aplicación $h \mapsto xh$ es una biyección de H en si mismo. Por tanto $x(\mathrm{tr}_H(\alpha)) = x(\sum_{h\in H} h(\alpha)) = \sum_{h\in H} xh(\alpha) = \sum_{h\in H} h(\alpha) = \mathrm{tr}_H(\alpha)$. Análogamente $x(N_H(\alpha)) = x(\prod_{h\in H} h(\alpha)) = \prod_{h\in H} xh(\alpha) = \prod_{h\in H} h(\alpha) = N_H(\alpha)$.

(b) $\mathrm{tr}_H(\alpha+\beta) = \sum_{h\in H} h(\alpha+\beta) = \sum_{h\in H} h(\alpha) + h(\beta) = \sum_{h\in H} h(\alpha) + \sum_{h\in H} h(\beta) = \mathrm{tr}_H(\alpha) + \mathrm{tr}_H(\beta)$.

$N_H(\alpha\beta) = \prod_{h\in H} h(\alpha\beta) = \prod_{h\in H} h(\alpha)h(\beta) = \left(\prod_{h\in H} h(\alpha)\right)\left(\sum_{h\in H} h(\beta)\right) = N_H(\alpha)N_H(\beta)$.

(c) Obsérvese que $\sigma^2 = 1$, con lo que H tiene orden 2. Entonces $\alpha = \mathrm{tr}(\xi_5) = \xi_5 + \xi_5^{-1}$ pertenece a L^H, por el apartado (a). Para ver que $\alpha \notin \mathbb{Q}$ observamos que $\xi_5^{-1} = \xi_5^4 = -1 - \xi_5 - \xi_5^2 - \xi_5^3$ y por tanto $\alpha = -1 - \xi_5^2 - \xi_5^3$ que no pertenece a $\mathbb{Q}$ pues $\{1, \xi_5, \xi_5^2, \xi_5^3\}$ es una base de L sobre $\mathbb{Q}$.

5. **Sean K un cuerpo de característica cero, $p = X^4 + aX^2 + b \in K[X]$ irreducible y $G = \mathrm{Gal}(p/K)$. Demostrar G tiene orden 4 ó es isomorfo a D_4, el grupo diédrico de orden 8.**

   Como p es irreducible, G es isomorfo a un subgrupo de S_4. Por otro lado, si α es una raíz de p, entonces $[K(\alpha):K] = 4$ y $-\alpha$ es otra raíz de K. Luego $p = (X-\alpha)(X+\alpha)q = (X-\alpha)(X+\alpha)(X-\beta)(X+\beta)$, con q un polinomio de grado 2 con coeficientes en $K(\alpha)$. Por tanto, si L es el cuerpo de descomposición p sobre K, entonces $[L:K(\alpha)] \le 2$. Eso implica $[L:K] = 4$ ú 8 y por tanto que G tiene orden 4 u 8.

   Supongamos que G tiene orden 8. Entonces $K(\alpha)/K$ no es una extensión normal y por tanto G no es un grupo abeliano. Eso implica que algún elemento de G tiene orden 4 (pues si tuviera uno de orden 8 sería cíclico y si todos los elementos fueran de orden 1 ó 2, G sería isomorfo a un producto directo de tres grupos cíclicos de orden 2. Podemos suponer que el elemento de orden 4 es $a = (1,2,3,4)$. Entonces $H = \langle a \rangle$ es un subgrupo normal de G y si b es un elemento de G que no pertenece a H, entonces bab^{-1} es un elemento de orden 4 de H diferente de a, con lo que $(b(1), b(2), b(3), b(4)) = bab^{-1} = a^{-1} = (1,4,3,2)$. Una sencilla cuenta muestra que b es necesariamente $(1,3)$ ó $(2,4)$ y por tanto b tiene orden 2. Ahora está claro que G es isomorfo al grupo diédrico de orden 8.

6. **Sea ξ una raíz tercera primitiva de la unidad y sean α y β dos números complejos tales que $\alpha^3 = \xi$ y $\beta^3 = \overline{\xi}$, el conjugado de ξ.**

   (a) Calcular $\mathrm{Irr}(\alpha, \mathbb{Q})$ e $\mathrm{Irr}(\beta, \mathbb{Q})$ y demostrar que existe un isomorfismo $f : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ tal que $f(\alpha) = \beta$.

   (b) ¿Se verifica la igualdad $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$?

   (c) Calcular $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ y hacer un diagrama de los subcuerpos de $\mathbb{Q}(\alpha)$.

   Claramente $\alpha^9 = \beta^9 = 1$, $\alpha^3 = \xi \ne 1$ y $\beta^3 = \overline{\xi} \ne 1$ y por tanto α como β son raíces novenas primitivas de la unidad. Con lo que $\mathrm{Irr}(\alpha, \mathbb{Q}) = \mathrm{Irr}(\beta, \mathbb{Q}) = \Phi_9 = \frac{X^9-1}{\Phi_1\Phi_3} = \frac{X^9-1}{X^3-1} = X^6 + X^3 + 1$, el noveno polinomio ciclotómico. Entonces $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, lo que responde a las dos primeras preguntas.

   Recordemos que $G = \mathrm{Gal}(K/\mathbb{Q})$ es isomorfo al grupo de unidades de $\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$. Obsérvese que 2 es un generador de $\mathbb{Z}_9^*$ y por tanto G es cíclico de orden 6. Eso implica que G tiene cuatro subgrupos de órdenes 1, 2, 3 y 6 respectivamente y aplicando el Teorema Fundamental de la Teoría de Galois concluímos que los subcuerpos de K forman un diagrama de la siguiente forma:

$$\begin{tikzcd} & K \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\ F_1 \arrow[dr, dash, "3"'] & & F_2 \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$