ÁLGEBRA **Examen de junio** **20-06-2003**

Apellidos **Nombre**

Cuestión 1. (*1 punto*) Defina y caracterice las extensiones normales de cuerpos.

Solución. Sea $K|k$ una extensión de cuerpos. Decimos que K es una extensión normal de k si es finita y $F(\mathrm{Gal}(K|k)) = k$.

Teorema de caracterización de las extensiones normales. Una extensión $K|k$ es normal si y solamente si K es el cuerpo de descomposición de un polinomio separable $f(X) \in k[X]$.

Cuestión 2. (*1 punto*) Pruebe que A_n es un subgrupo de S_n normal.

Solución. Recordemos que A_n es el conjunto de permutaciones pares de S_n. La factorización de una permutación como producto de trasposiciones no es única, pero sí permanece invariante el que dicha descomposición tenga un número par o impar de elementos. Es claro que $A_n \neq \emptyset$, pues $id \in A_n$. Además, si $\sigma \in A_n$ entonces $\sigma^{-1} \in A_n$, pues una descomposición de σ^{-1} en producto de trasposiciones se obtiene invirtiendo una factorización de σ. Por último, si $\sigma, \tau \in A_n$ entonces $\sigma^{-1}\tau \in A_n$ pues la suma de dos números pares es par.

Para ver la normalidad, sea $\sigma \in A_n, \tau \in S_n$. Si τ es par, entonces es claro que $\tau^{-1}\sigma\tau$ es par. Si τ es impar, entonces la unión de las factorizaciones de $\tau^{-1}\sigma\tau$ da lugar a un número par de trasposiciones, luego $\tau^{-1}\sigma\tau \in A_n$.

Ejercicio 1. (*3,5 puntos*) Se sabe que $f(X) = X^4 + X^3 + X^2 + X + 1 = \frac{X^5-1}{X-1}$ es un polinomio irreducible sobre $\mathbb{Q}$. Sean $\alpha = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\,\frac{2\pi}{5} \in \mathbb{C}$, $K = \mathbb{Q}(\alpha)$ y G_f el grupo de Galois de f sobre $\mathbb{Q}$.

1. Deduzca que $\{\alpha, \alpha^2, \alpha^3, \alpha^4\}$ son todas las raíces de f. Averigüe si K es un cuerpo de descomposición de f sobre $\mathbb{Q}$.
2. Calcule $|G_f|$.
3. Si $\sigma_j \in G_f$ viene dado por $\sigma_j(\alpha) = \alpha^j$, con $j = 1, 2, 3, 4$, deduzca si $G_f = \langle\sigma_j\rangle$ para algún valor de j.
4. Numerando las raíces de f por $x_j = \alpha^j$, con $j = 1, 2, 3, 4$, identifique G_f con un subgrupo de S_4. Razone si la conjugación en $\mathbb{C}$ define algún elemento de G_f.
5. Halle todos los subgrupos de G_f.
6. Halle todos los cuerpos intermedios entre $\mathbb{Q}$ y K. Deduzca si $\mathbb{Q}(\cos\frac{2\pi}{5})$ y $\mathbb{Q}(\cos\frac{\pi}{5})$ son algunos de estos cuerpos. Halle un valor $d \in \mathbb{Z}$, si existe, tal que $\mathbb{Q}(\cos\frac{2\pi}{5}) = \mathbb{Q}(\sqrt{d})$.

Solución.

1. Es evidente que $\alpha^5 = (\cos\frac{2\pi}{5} + i\,\mathrm{sen}(\frac{2\pi}{5}))^5 = \cos(2\pi) + i\,\mathrm{sen}(2\pi) = 1$. Luego $f(\alpha) = 0$. Del mismo modo, $f(\alpha^j) = \frac{(\alpha^j)^5-1}{\alpha^j-1} = \frac{(\alpha^5)^j-1}{\alpha^j-1} = 0$, para $j = 1, 2, 3, 4$.
   Un cuerpo de descomposición de f sobre $\mathbb{Q}$ es $\mathbb{Q}(\alpha, \alpha^2, \alpha^3, \alpha^4) = \mathbb{Q}(\alpha) = K$.
2. La extensión K es normal sobre $\mathbb{Q}$. Entonces $|G_f| = |\,\mathrm{Gal}(K|\mathbb{Q})| = [K : F(\mathrm{Gal}(K|\mathbb{Q})] = [K : \mathbb{Q}] = 4$, el grado del polinomio mínimo de α sobre $\mathbb{Q}$.

3. Sea $\sigma_j : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ definida por $\sigma_j(\alpha) = \alpha^j, j = 1, 2, 3, 4$.

   Para $j = 1$ tenemos que $\sigma_1(\alpha) = \alpha$ y entonces $\sigma_1 = id$.

   Para $j = 2$ tenemos las igualdades

$$\begin{aligned}
&\sigma_2(\alpha) = \alpha^2,\\
&\sigma_2^2(\alpha) = (\alpha^2)^2 = \alpha^4,\\
&\sigma_2^3(\alpha) = (\alpha^4)^2 = \alpha^8 = \alpha^3 \text{ porque } \alpha^5 = 1,\\
&\sigma_2^4(\alpha) = (\alpha^3)^2 = \alpha^6 = \alpha.
\end{aligned}$$

   Entonces el orden de σ_2 es 4 y $G_f = \langle \sigma_2 \rangle$.

   Aunque no es necesario, observemos qué ocurre con los restantes elementos. Para $j = 3$,

$$\begin{aligned}
&\sigma_3(\alpha) = \alpha^3,\\
&\sigma_3^2(\alpha) = (\alpha^3)^3 = \alpha^4,\\
&\sigma_3^3(\alpha) = (\alpha^4)^3 = \alpha^2,\\
&\sigma_3^4(\alpha) = (\alpha^2)^3 = \alpha.
\end{aligned}$$

   De aquí, el orden de σ_3 es 4 y también $G_f = \langle \sigma_3 \rangle$. Para $j = 4$,

$$\begin{aligned}
&\sigma_4(\alpha) = \alpha^4,\\
&\sigma_4^2(\alpha) = \alpha^{16} = \alpha.
\end{aligned}$$

   En este caso, σ_4 tiene orden 2.

4. Sean $x_1 = \alpha, x_2 = \alpha^2, x_3 = \alpha^3, x_4 = \alpha^4$. Veamos la acción de cada σ_j sobre las raíces. Para $\sigma_1 = id$, la permutación asociada es también la identidad.

$$\left.\begin{aligned}
&\sigma_2(x_1) = \alpha^2 = x_2,\\
&\sigma_2(x_2) = \alpha^4 = x_4,\\
&\sigma_2(x_3) = \alpha = x_1,\\
&\sigma_2(x_4) = \alpha^3 = x_3
\end{aligned}\right\} \quad \sigma_2 = (1243)$$

$$\left.\begin{aligned}
&\sigma_3(x_1) = x_3,\\
&\sigma_3(x_2) = x_1,\\
&\sigma_3(x_3) = x_4,\\
&\sigma_3(x_4) = x_2
\end{aligned}\right\} \quad \sigma_3 = (1342)$$

$$\left.\begin{aligned}
&\sigma_4(x_1) = x_4,\\
&\sigma_4(x_2) = x_3,\\
&\sigma_4(x_3) = x_2,\\
&\sigma_4(x_4) = x_1
\end{aligned}\right\} \quad \sigma_4 = (14)(23)$$

   Tenemos así que $G_f \simeq \{1, (1243), (1342), (14)(23)\}$.

5. La conjugación en $\mathbb{C}$ deja invariantes los elementos de $\mathbb{Q}$ y lleva α en $\bar{\alpha} = \cos\frac{8\pi}{5} + i\,\mathrm{sen}\,\frac{8\pi}{5} = \alpha^4$. Luego la conjugación es σ_4.

6. Los subgrupos G_f, que es un grupo cíclico, son todos cíclicos, de órdenes los divisores de 4. Así, los subgrupos son $\{1\}, G_f, H = \langle \sigma_4 \rangle$, pues σ_4 es el único elemento de orden 2.

7. Es claro que $F(\{1\}) = K, F(G_f) = \mathbb{Q}$. Por el teorema fundamental de la teoría de Galois, $[F(H) : \mathbb{Q}] = 2$. Sea $z = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \in K$, tal que $\sigma_4(z) = z$, esto es, que $z \in F(H)$. Entonces

$$\sigma_4(z) = a_0 + a_1\alpha^4 + a_2\alpha^3 + a_3\alpha^2 = z.$$

   Recordemos que $\alpha^4 = -1 - \alpha - \alpha^2 - \alpha^3$. Igualando coeficientes obtenemos que $a_1 = 0, a_2 = a_3$, y $z = a_0 + a_2(\alpha^2 + \alpha^3)$. Entonces $F(H) = \mathbb{Q}(\alpha^2 + \alpha^3)$ y $\alpha^2 + \alpha^3 = 2\cos(\frac{4\pi}{5}) = -2\cos(\frac{\pi}{5})$.

Así, $F(H) = \mathbb{Q}(\cos(\frac{pi}{5}))$. Observemos que $\alpha + \alpha^4 = -1 - \alpha^2 - \alpha^3$, por lo que también $F(H) = \mathbb{Q}(\alpha + \alpha^4) = \mathbb{Q}(\cos(\frac{2\pi}{5}))$.

Calculemos ahora el polinomio mínimo de $\cos(\frac{2\pi}{5})$ sobre $\mathbb{Q}$.

$$\cos(\tfrac{2\pi}{5}) = \tfrac{1}{2}(\alpha + \alpha^4) = \tfrac{1}{2}\alpha + \tfrac{1}{2}(-\alpha^3 - \alpha^2 - \alpha - 1) = -\tfrac{1}{2} - \tfrac{1}{2}\alpha^2 - \tfrac{1}{2}\alpha^3,$$
$$\cos^2(\tfrac{2\pi}{5}) = \tfrac{1}{4}(\alpha + \alpha^4)^2 = \tfrac{1}{4}\alpha^2 + \tfrac{1}{4}\alpha^3 + \tfrac{1}{2}$$

y sumando

$$2\cos^2(\frac{2\pi}{5}) + \cos(\frac{2\pi}{5}) - \frac{1}{2} = 0.$$

Entonces $\cos(\frac{2\pi}{5}) = \frac{-1+\sqrt{5}}{4}$ y $\mathbb{Q}(\cos(\frac{2\pi}{5})) = \mathbb{Q}(\sqrt{5})$.

Ejercicio 2. (*2 puntos*) Sea k un cuerpo y K_1, K_2 extensiones finitas.

1. Si $\mathrm{car}(k) = 0$ y $[K_1 : k] = [K_2 : k]$, ¿son K_1 y K_2 isomorfos como cuerpos? Justifique la respuesta. Indicación: considere, por ejemplo, $\mathbb{Q}[\sqrt{2}]$ y $\mathbb{Q}[\sqrt{3}]$.
2. Si k es finito y $[K_1 : k] = [K_2 : k]$, ¿son K_1 y K_2 isomorfos como cuerpos? Justifique la respuesta.

Solución.

1. Sea $k = \mathbb{Q}, K_1 = \mathbb{Q}[\sqrt{2}], K_2 = \mathbb{Q}[\sqrt{3}]$. Es claro que $[K_1 : k] = 2$, pues el polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es $X^2 - 2$. Análogamente, $[K_2 : k] = 2$. Sin embargo, vamos a probar que no existe ningún isomorfismo de cuerpos entre K_1 y K_2. Si $\varphi : K_1 \to K_2$ fuera un isomorfismo, entonces $\varphi(1) = 1$ y $\varphi(-1) = -1$. Por inducción, $\varphi(n) = n$ para todo $n \in \mathbb{Z}$. Entonces, $\varphi(1/n) = 1/n$ para todo $n \in \mathbb{Z} - \{0\}$ y de nuevo por inducción $\varphi(m/n) = m/n$ para todo $m \in \mathbb{Z}, n \in \mathbb{Z} - \{0\}$, es decir, $\varphi(a) = a$ para todo $a \in \mathbb{Q}$. Una base de K_2 como k-espacio vectorial está formada por los elementos $1, \sqrt{3}$. Entonces $\varphi(\sqrt{2}) = a + b\sqrt{3}$ para ciertos $a, b \in k$. Como $(\sqrt{2})^2 - 2 = 0$, aplicamos φ a esta igualdad y nos queda

$$(a + b\sqrt{3})^2 - 2 = 0, a^2 + 3b^2 - 2 + 2ab\sqrt{3} = 0.$$

Entonces $a = 0$ o bien $b = 0$. En el primer caso, $3b^2 - 2 = 0$, pero esta ecuación no tiene solución en k. En el segundo caso, $a^2 - 2 = 0$, que tampoco tiene solución en k. Por tanto, K_1 y K_2 no son isomorfos como cuerpos.

2. Si $[K_1 : k] = [K_2 : k] = n$, entonces K_1 y K_2 tienen $|k|^n$ elementos. Un resultado de teoría nos dice que dos cuerpos finitos con igual número de elementos son isomorfos, lo que nos da el resultado.

Ejercicio 3. *(2,5 puntos)* Sea G un grupo y $f : G \to G$ un homomorfismo de grupos tal que $f \circ f = f$. Sean $H = \ker(f)$ y $K = \mathrm{im}(f)$. Pruebe que:

1. Para todo $x \in G$, $xf(x)^{-1} \in H$. Deduzca que $G = H \cdot K$.
2. $H \cap K = \{1\}$.
3. Si $K \triangleleft G$, entonces la aplicación $f : H \times K \to H \cdot K$ definida por $f(h, k) = hk$ es un isomorfismo de grupos.

Solución.

1. Veamos que $f(xf(x)^{-1}) = 1$ para todo $x \in G$. Por ser f homomorfismo de grupos y $f \circ f = f$, tenemos que

$$f(xf(x)^{-1}) = f(x)f(f(x)^{-1}) = f(x)f(f(x))^{-1} = f(x)f(x)^{-1} = 1.$$

Por tanto $xf(x) = y \in \ker(f) = H$ y como consecuencia $x = yf(x) \in H \cdot K$.

2. Basta probar que para todo $x \in H \cap K$, $x = 1$. Ahora bien, como $x \in K = \mathrm{im}(f)$, $x = f(y)$ con $y \in G$. Además $x \in H = \ker(f)$ y usando de nuevo que $f \circ f = f$, se tiene que

$$1 = f(x) = f(f(y)) = f(y) = x,$$

y por tanto el resultado.

3. Si $K \triangleleft G$, veamos que la aplicación $g : H \times K \to H \cdot K$ definida por $g(h,k) = hk$ es un isomorfismo de grupos. Está bien definida de manera trivial, tenemos que probar:

   (a) g es homomorfismo de grupos, es decir, $g((h_1,k_1)(h_2,k_2)) = g(h_1,k_1)g(h_2,k_2)$. Como

   $$g((h_1,k_1)(h_2,k_2)) = g(h_1h_2, k_1k_2) = h_1h_2k_1k_2$$

   y

   $$g(h_1,k_1)g(h_2,k_2) = h_1k_1h_2k_2,$$

   basta probar que $h_2k_1 = k_1h_2$. Si $K \triangleleft G$, entonces $h_2k_1 \in h_2K = Kh_2$, por tanto $h_2k_1 = k_3h_2$ para un cierto $k_3 \in K$. Además $H = \ker(f) \triangleleft G$, luego $k_1h_2 \in Hk_1 = k_1H$, y por tanto $h_2k_1 = k_1h_3$ con $h_3 \in H$. Igualando obtenemos $k_1h_3 = k_3h_2$, de donde $k_3^{-1}k_1 = h_2h_3^{-1} \in H \cap K = \{1\}$; luego $k_3 = k_1$ y $h_3 = h_2$. Por tanto $h_2k_1 = k_3h_2 = k_1h_2$.

   (b) g es biyectiva puesto que es sobreyectiva (trivial) y probemos que es inyectiva: Sea $(h,k) \in \ker g$, es decir, $g(h,k) = hk = 1$, entonces $h = k^{-1} \in H \cap K = \{1\}$. Por tanto $(h,k) = (1,1)$.