**Álgebra** Examen de Junio (17-06-2005)

| APELLIDOS: | NOMBRE: |
|---|---|

**Cuestión teórica.** $(1,5$ *puntos*$)$.

1. Definición de subgrupo normal.
2. Definición de extensión normal de un cuerpo.
3. Relación entre ambos conceptos.

**Ejercicio 1.** *(*$2,5$ *puntos)* Sean $\alpha = \sqrt{2+\sqrt{2}}, \beta = \sqrt{2-\sqrt{2}}$.

1. Halle el polinomio mínimo de $\alpha$ sobre $\mathbb{Q}$.
2. Compruebe que $\beta = \frac{\alpha^2-2}{\alpha}$. Exprese $\beta$ como polinomio en $\alpha$ con coeficientes racionales.
3. Razone si $\sigma(\alpha) = \beta$ define un automorfismo $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})$. Demuestre que, en ese caso, $\sigma(\beta) = -\alpha$.
4. Razone si $\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q}) = \langle\sigma\rangle$.
5. Una extensión de cuerpos $F \subset L$ es radical si existen cuerpos
$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L$$
donde para $i = 1, \ldots, n$ existe $\gamma_i \in F_i$ con $F_i = F_{i-1}(\gamma_i), \gamma_i^{m_i} \in F_{i-1}$ para algún $m_i > 0$. Pruebe que $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ es una extensión radical.

**Solución.**

1. Tenemos que $\alpha^2 = 2+\sqrt{2}$, de donde $(\alpha^2-2)^2 = 2$, o lo que es lo mismo, $\alpha^4 - 4\alpha^2 - 2 = 0$. El polinomio $X^4 - 4X^2 + 2$ es mónico, tiene a $\alpha$ como raíz, y es irreducible por el criterio de Eisenstein. Por tanto, es el polinomio mínimo de $\alpha$ sobre $\mathbb{Q}$.
2. La primera parte es una comprobación trivial. Para la segunda, como $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$, una base de $\mathbb{Q}[\alpha]$ como $\mathbb{Q}$-espacio vectorial es $\{1, \alpha, \alpha^2, \alpha^3\}$. Entonces estamos buscando una expresión de la forma
$$\beta = \frac{\alpha^2-2}{\alpha} = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3, \text{ donde } a_i \in \mathbb{Q}, i = 0,1,2,3.$$
Entonces
$$\begin{aligned} \alpha^2 - 2 &= a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4 \\ &= a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3(4\alpha^2 - 2) \\ &= -2a_3 + a_0\alpha + (a_1 + 4a_3)\alpha^2 + a_2\alpha^3. \end{aligned}$$
Igualamos coeficientes, resolvemos el sistema, y nos queda $a_0 = 0, a_1 = -3, a_2 = 0, a_3 = 1$.
3. Basta comprobar que $\beta$ es raíz del polinomio mínimo de $\alpha$.
$$\beta^4 - 4\beta^2 + 2 = 6 - 4\sqrt{2} - 4(2-\sqrt{2}) + 2 = 0.$$
Por otro lado,
$$\sigma(\beta) = \frac{\sigma(\alpha)^2 - 2}{\sigma(\alpha)} = \frac{\beta^2-2}{\beta} = -\alpha.$$
4. Sabemos que $\mathbb{Q}(\alpha)$ es cuerpo de descomposición de $X^4 - X^2 + 2$ sobre $\mathbb{Q}$, por lo que $|\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q}| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Si probamos que el orden de $\sigma$ como elementos del grupo $\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})$ es 4 habremos terminado. Se tiene que $\sigma^2(\alpha) = -\alpha, \sigma^3(\alpha) = \beta, \sigma^4(\alpha) = \alpha$.
5. Es inmediato a partir de $F_0 = \mathbb{Q}, F_1 = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}), F_2 = \mathbb{Q}(\alpha)$.

**Ejercicio 2.** *(*$2$ *puntos)* Consideremos los grupos multiplicativos $G = \langle(1\ 3\ 4\ 2), (1\ 4)\rangle \subset S_4$ y $G' = \{1, -1\}$.

1. Halle todos los elementos de $G$.
2. Exhiba un subgrupo propio de $G$ que sea cíclico y otro que no los sea.

3. Sea $\epsilon : G \to G'$ el homomorfismo inducido por la paridad, es decir, si $\sigma \in G$ es par entonces $\epsilon(\sigma) = 1$, y si $\sigma \in G$ es impar entonces $\epsilon(\sigma) = -1$. Calcule $\ker(\epsilon)$.

4. Halle un homomorfismo $\delta : G' \to G$ tal que $\epsilon \circ \delta = \mathrm{id}_{G'}$. ¿Cuántas posibles soluciones existen?

**Solución.**

1. Es claro que el orden de $\sigma = (1\ 3\ 4\ 2)$ es 4 y el de $\tau = (1\ 4)$ es dos. Se tiene que

$$\sigma\tau = (1\ 2)(3\ 4), \sigma^2\tau = (3\ 2), \sigma^3\tau = ((1\ 3)(2\ 4), \tau\sigma = (1\ 3)(2\ 4) = \sigma^3\tau.$$

   Todo elemento de $G$ es de la forma

$$\sigma^{m_1}\tau^{n_1}\cdots\sigma^{m_r}\tau^{n_r},$$

   com $m_i \in \{0, 1, 2, 3\}, n_i \in \{0, 1\}$. Por inducción, y con la relación $\sigma^3\tau = \tau\sigma$, es posible probar que todo elemento de $G$ se puede llevar a la forma $\sigma^m\tau^n$, con $m \in \{0, 1, 2, 3\}, n \in \{0, 1\}$. Por tanto, los elementos de $G$ son

$$G = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}.$$

2. Un subgrupo propio de $G$ cíclico es $\langle\tau\rangle$. Un subgrupo propio de $G$ no cíclico es $\{\mathrm{id}, \sigma^2, \tau, \sigma^2\tau\}$, pues todos sus elementos son de orden dos.

3. Por la definición, $\ker\epsilon$ son las permutaciones pares de $G$. Como $\sigma$ es un ciclo de orden 4, es impar, de donde $\sigma^2$ es par y $\sigma^3$ es impar. La trasposición $\tau$ es impar, por lo que $\sigma\tau$ es par, $\sigma^2\tau$ es impar y $\sigma^3\tau$ es par. Por tanto, $\ker\epsilon = \{\mathrm{id}, \sigma^2, \sigma\tau, \sigma^3\tau\}$.

4. El homomorfismo $\delta$ queda determinado por $\delta(-1) = g$. Como $-1$ es de orden 2 en $G'$, entonces $g$ tiene orden un divisor de 2. No puede ser de orden 1, pues entonces $\epsilon \circ \delta$ sería constante e igual a 1. Los candidatos para los valores de $\delta(-1)$ son los elementos de orden 2 de $G$, es decir, $\sigma^2, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$. Se tiene que cumplir la condición $-1 = \epsilon(\delta(-1)) = \epsilon(g)$, por lo que $g$ tiene que ser impar. Los valores posibles son entonces $g = \tau$ y $g = \sigma^2\tau$.

**Ejercicio 3.** *(2 puntos)* Sea $f(X) = X^4 + X^2 + 1 \in k[X]$. Para $k = \mathbb{Q}, \mathbb{F}_5$ calcule un elemento $\gamma$ tal que el cuerpo de descomposición de $f(X)$ sobre $k$ sea $k(\gamma)$.

**Solución.** Para $k = \mathbb{Q}, \mathbb{F}_5$ se tiene que $f(X) = (X^2 + X + 1)(X^2 - X + 1)$. En $\mathbb{Q}$, las raíces de $f(X)$ son entonces $\alpha_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \alpha_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}, \beta_1 = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \beta_2 = \frac{1}{2} - i\frac{\sqrt{3}}{2}$. Es claro entonces que podemos tomar $\gamma = \sqrt{3}i$. En $\mathbb{F}_5$, recordemos que $-3 = 2$. Por un argumento similar, tomamos $\gamma$ tal que $\gamma^2 = 2$.

**Test.** *(2 puntos).* Marque como **verdadera** o **falsa** cada una de las siguientes conclusiones. Las respuestas correctas sumarán, y las erróneas restarán.

1. Todo grupo de orden 4 es
   - *a*) abeliano. Verdadero.
   - *b*) simple. Falso.
2. Sea $N = \{\sigma \in S_4 : \sigma(4) = 4\}$. Entonces
   - *a*) $N$ es simple. Falso.
   - *b*) $N$ es un subgrupo de $S_4$ isomorfo a $S_3$. Verdadero.
3. Sea $\mathbb{F}_1$ un cuerpo finito y $\mathbb{F}_2$ una extensión finita de $\mathbb{F}_1$. Entonces $\mathrm{Gal}(\mathbb{F}_2|\mathbb{F}_1)$ es un grupo
   - *a*) abeliano. Verdadero.
   - *b*) cíclico. Verdadero.
   - *c*) resoluble. Verdadero.
4. Sea $H = \langle (1\ 2\ 3\ 4), (1\ 3)(2\ 4) \rangle \subset S_4$. Entonces
   - *a*) $H$ tiene 6 elementos. Falso.
   - *b*) $H$ es cíclico. Verdadero.
5. Sea $f(X) = X^2 + 1 \in \mathbb{Q}[X]$. Entonces
   - *a*) $f(X)$ es irreducible sobre $\mathbb{Q}(i, \sqrt{2})$. Falso.
   - *b*) $\mathbb{Q}(i, \sqrt{2})$ es cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$. Falso.
   - *c*) $f(X)$ es reducible en $\mathbb{Q}[\sqrt{2}][X]$. Falso.