ÁLGEBRA **Problemas propuestos** **25-5-2004**

Apellidos **Nombre**

Ejercicio 1.– Sea $f(X) = 2X^5 - 10X + 5 \in \mathbb{Q}[X]$.

1. Pruebe que $f(X)$ es irreducible en $\mathbb{Q}[X]$ y que tiene 5 raíces distintas.
2. Deduzca que G_f es isomorfo a un subgrupo de S_5.
3. Pruebe que 5 divide a $|G_f|$.
4. El teorema de Cauchy para grupos dice: si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p. Con este resultado, pruebe que G_f tiene un elemento que se corresponde con un ciclo de orden 5 en S_5.
5. Compruebe que $f(-2) < 0, f(-1) > 0, f(1) < 0, f(2) > 0$, y deduzca que $f(X)$ tiene exactamente 3 raíces reales.
6. Pruebe que el automorfismo definido por la conjugación está en G_f.
7. Deduzca que $G_f \simeq S_5$. ¿Es $f(X)$ resoluble por radicales?

Solución 1 *1. Por el criterio de Eisenstein, para $p = 5$, se tiene que $f(X)$ es irreducible sobre $\mathbb{Q}[X]$.*

2. El grupo de Galois de $f(X)$ aplica raíces del polinomio en raíces de $f(X)$. Por tanto, un automorfismo de K, cuerpo de descomposición sobre $\mathbb{Q}$ de $f(X)$ viene definido por una permutación de las raíces, esto es, todo elemento de G_f se corresponde con un elemento de S_5, y tenemos el isomorfismo con un subgrupo de S_5.

3. Si $\alpha \in K$ es raíz de $f(X)$ entonces $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset K$, y por la fórmula del grado

$$[K : \mathbb{Q}] = [K : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}] = 5[K : \mathbb{Q}[\alpha]],$$

pues $\frac{1}{2}f(X)$ es el polinomio mínimo de α sobre $\mathbb{Q}$, y tiene grado 5.

4. Por el apartado anterior, G_f contiene un elemento de orden 5. Los únicos elementos de orden 5 en S_5 son los ciclos de longitud 5.

5. Las comprobaciones de los valores que toma el polinomio $f(X)$ en $-2, -1, 1$ y 2 es inmediata. La derivada de $f(X)$ es igual a

$$f'(X) = 10X^4 - 10 = 10(X^4 - 1).$$

Esto implica que la función es estrictamente creciente en $(-\infty, -1)$, en -1 alcanza un máximo local, decrece entre -1 y 1, tiene un mínimo local en 1 y vuelve a ser estrictamente creciente para valores mayores que 1. Por tanto, y por el teorema de Bolzano, tiene únicamente tres raíces reales, localizadas en los intervalos $(-2, -1), (-1, 1)$ y $(1, 2)$.

6. Como $f(X)$ tiene coeficientes reales, las dos restantes raíces tienen que ser complejas conjugadas. Entonces la aplicación

$$\begin{array}{rcl} \sigma : \mathbb{C} & \to & \mathbb{C} \\ a + bi & \mapsto & a - bi \end{array}$$

aplica el cuerpo K en K, por lo que pertenece a G_f. Si vemos este automorfismo como una permutación de S_5, se corresponde con una transposición, pues intercambia las raíces complejas, y deja invariantes las reales.

7. Los apartados anteriores prueban que G_f contiene un ciclo de orden 5 y una transposición. Sabemos que S_5 está generado por estos elementos, de donde $G_f \simeq S_5$.

Ejercicio 2.– Calcule el grupo de Galois de $X^4 - 5$ sobre $\mathbb{Q}[i]$.

Solución 2 *Las raíces de este polinomio son* $\alpha, \alpha i, -\alpha, -\alpha i$, *donde* $\alpha = \sqrt[4]{5}$. *Entonces el cuerpo de descomposición es igual a* $K = \mathbb{Q}[\alpha, i]$, *y es claro que* $[K : \mathbb{Q}] = 8$. *Por la fórmula del grado,* $[K : \mathbb{Q}[i]] = 4$. *Por definición,*

$$\mathrm{Gal}(K|\mathbb{Q}[i]) = \{\sigma \in \mathrm{Aut}(K) | \sigma_{|\mathbb{Q}[i]} = \mathrm{id}_{\mathbb{Q}[i]}\}.$$

Entonces, un elemento $\sigma \in \mathrm{Gal}(K|\mathbb{Q}[i])$ *lleva* α *en otra raíz y la unidad imaginaria* i *permanece invariante. Si definimos*

$$\sigma(\alpha) = \alpha i$$

es fácil ver que $\mathrm{Gal}(K|\mathbb{Q}[i]) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$, *que es un grupo cíclico de* 4 *elementos.*

Ejercicio 3.– (2) Sea $\mathbb{F}_2 = \mathbb{Z}/\mathbb{Z}2$ el cuerpo finito con dos elementos. Sea α raíz de $X^2 + X + 1$ sobre $\mathbb{F}_2$ y $K_1 = \mathbb{F}_2[\alpha]$. Sea $g(X) = X^2 + \alpha X + 1 \in K_1[X]$.

1. ¿Cuántos elementos tiene K_1? Expréselos en función de α.
2. Pruebe que $g(X)$ es irreducible sobre $K_1[X]$.
3. Sea β raíz de $g(X)$ y $K_2 = K_1[\beta]$. ¿Cuántos elementos tiene K_2? Calcule $[K_2 : \mathbb{F}_2]$.
4. Sea $\varphi : K_2 \to K_2$ definida por $\varphi(x) = x^2$. Pruebe que $\varphi \in \mathrm{Gal}(K_2|\mathbb{F}_2)$, y que el orden de φ es 4. Deduzca que $\mathrm{Gal}(K_2|\mathbb{F}_2) = \langle\varphi\rangle$.
5. Sea $\gamma = \alpha\beta$. Pruebe que γ no permanece invariante por ningún elemento de $\mathrm{Gal}(K_2|\mathbb{F}_2)$ distinto de la identidad. Concluya que $K_2 = \mathbb{F}_2[\gamma]$.

Solución 3

1. *Como* $X^2 + X + 1$ *es irreducible sobre* $\mathbb{F}_2[X]$ *(ni* 0 *ni* 1 *son raíces),* $[K_1 : \mathbb{F}_2] = 2$, *de donde* $\{1, \alpha\}$ *es una base de* K_1 *como* $\mathbb{F}_2$*-espacio vectorial. Entonces los elementos de* K_1 *son de la forma* $a_0 + a_1\alpha$, *con* $a_0, a_1 \in \mathbb{F}_2$. *Entonces, hay* $4 = 2^2$ *elementos en* K_1, *que son* $0, 1, \alpha, 1 + \alpha$.
2. *Basta ver que ninguno de los elementos anteriores es raíz de* $g(X)$.
3. *Se tiene que* $[K_2 : K_1] = 2$, *de donde* $[K_2 : \mathbb{F}_2] = 4$ *y el número de elementos de* K_2 *es* $2^4 = 16$.
4. *Como la característica de* K_2 *es* 2, *la aplicación* φ *no es más que el automorfismo de Frobenius, que deja invariante a* $\mathbb{F}_2$. *Entonces* $\varphi \in \mathrm{Gal}(K_2|\mathbb{F}_2)$. *Es más, genera a este grupo, que sabemos que es cíclico y de orden igual a* $[K_2 : \mathbb{F}_2] = 4$.
5. *Como una base de* K_1 *sobre* $\mathbb{F}_2$ *es* $\{1, \alpha\}$ *y una base de* K_2 *sobre* K_1 *es* $\{1, \beta\}$, *se tiene que una base de* K_2 *sobre* $\mathbb{F}_2$ *es* $\{1, \alpha, \beta, \alpha\beta\}$. *Se tiene que*

$$\varphi(\gamma) = \alpha^2\beta^2 = (\alpha + 1)(\alpha\beta + 1) = \ldots = \alpha + \beta + 1 \neq \alpha\beta, \quad \text{por la independencia de estos elementos sobre } \mathbb{F}_2,$$
$$\varphi^2(\gamma) = \alpha + \alpha\beta + 1 \neq \alpha\beta,$$
$$\varphi^3(\gamma) = \beta + 1 \neq \alpha\beta.$$

Es claro que $\mathbb{F}_2 \subset \mathbb{F}_2[\gamma] \subset K_2$. *Entonces* $\mathbb{F}_2[\gamma]$ *es un subcuerpo de* K_2 *que solamente permanece invariante por la acción de la identidad. Por la biyección que establece el teorema fundamental de la teoría de Galois entre subcuerpos y subgrupos, tiene que se* K_2, *que es el cuerpo fijo de la identidad.*

Ejercicio 4.– (2) Sea K un cuerpo finito, $\mathrm{car}(K) \neq 2$, y θ un generador del grupo multiplicativo K^*.

1. Sea $b \in K^*$ y $k \in \mathbb{N}$ tal que $\theta^k = b$. Pruebe que b es un cuadrado en K si y solamente si k es par.
2. Pruebe que si $a_1, a_2 \in K$ no son cuadrados entonces $a_1 a_2$ es un cuadrado en K.
3. Sea $a \in K$ no cuadrado y consideremos $K_1 = K[\sqrt{a}]$. Calcule el número de elementos de K_1.
4. Sea $b \in K$. Pruebe que existe $b_1 \in K_1$ tal que $b_1^2 = b$.
5. Pruebe que si $d_1, d_2 \in K$ no son cuadrados entonces $[K[\sqrt{d_1}, \sqrt{d_2}] : K] = 2$.

6. Pruebe que el cuerpo de descomposición de $f(X) = X^4 - 10X^2 + 1$ sobre $\mathbb{Q}$ es igual a $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Deduzca que para cualquier primo p, $f(X)$ es reducible sobre $\mathbb{F}_p[X]$.

Solución 4 *1. Si $b = \theta^k$ es un cuadrado, existe $a \in K$ tal que $\theta^k = a^2$. Para un cierto r se tiene que $\theta^r = a$. Entonces $\theta^k = \theta^{2r}$, de donde el orden de θ, como generador del grupo K^*, divide a $k - 2r$. Si la característica de K es p, entonces el número de elementos de K^* es $p^n - 1$ para un cierto n. De aquí, $2|(p^n - 1)|(k - 2r)$ y entonces 2 divide a k. Recíprocamente, si $k = 2l$ entonces $b = (\theta^l)^2$.*

2. *Si $a_1, a_2 \in K$ no son cuadrados entonces $a_1 = \theta^{k_1}, a_2 = \theta^{k_2}$, con k_1, k_2 impares. Entonces $a_1 a_2 = \theta^{k_1+k_2}$, y $k_1 + k_2$ es par. Por el apartado anterior, $a_1 a_2$ es un cuadrado en K.*

3. *La extensión K_1 tiene grado 2 sobre K, por lo que el número de elementos de K_1 es igual a $(\#K)^2$.*

4. *Si $b \in K$ es un cuadrado, no hay nada que probar. Supongamos entonces que b no es un cuadrado. Buscamos $b_1 = a_0 a_1 \sqrt{a}$, con $a_0, a_1 \in K$, tal que $b_1^2 = b$. Entonces*

$$b_1^2 = a_0^2 + a_1^2 a + 2a_0 a_1 \sqrt{a} = b.$$

De aquí, $a_0 a_1 = 0$. Si tomamos $a_0 = 0$, tenemos que ver si la ecuación $a_1^2 a = b$ tiene solución en K. Tiene que ocurrir que ba^{-1} sea cuadrado en K, pero como b y a no son cuadrados, por el apartado anterior tenemos que ba^{-1} es cuadrado. Por tanto, el sistema tiene solución.

5. *El apartado anterior nos indica que si $d_2 \in K$ entonces tiene raíz cuadrada en $K[\sqrt{d_1}]$. Entonces $K[\sqrt{d_1}, \sqrt{d_2}] = K[\sqrt{d_1}]$, y tenemos el resultado.*

6. *Es fácil calcular que las raíces de $f(X)$ son $\alpha_1 = \sqrt{5 + 2\sqrt{6}}, \alpha_2 = -\sqrt{5 + 2\sqrt{6}}, \alpha_3 = \sqrt{5 - 2\sqrt{6}}, \alpha_4 = -\sqrt{5 - 2\sqrt{6}}$. Se tiene que*

$$(X-\alpha_1)(X-\alpha_2) = X^2-5-2\sqrt{6}, (X-\alpha_1)(X-\alpha_3) = X^2-2\sqrt{3}X+1, (X-\alpha_1)(X-\alpha_4) = X^2 2\sqrt{2}X-1,$$

por lo que $f(X)$ es irreducible en $\mathbb{Q}[X]$, pues ninguna combinación de factores da coeficientes en $\mathbb{Q}$. Vamos a probar que $\alpha_1 \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. En efecto, si planteamos el sistema

$$\sqrt{5 + 2\sqrt{6}} = a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6},$$

con $a_0, a_1, a_2, a_3 \in \mathbb{Q}$, y elevamos al cuadrado, podemos identificar coeficientes y nos queda

$$a_0 2^2 + 2a_1^2 + 3a_2^2 + 6a_3^2 = 5, a_0 a_1 + 3a_2 a_3 = 0, a_0 a_2 + 2a_1 a_3 = 0, a_0 a_3 + a_1 a_2 = 1,$$

que tiene como soluciones $a_0 = a_3 = 0, a_1 = a_2 = 1$ y $a_0 = a_3 = 0, a_1 = a_2 = -1$. La primera es para α_1, de donde

$$\alpha_1 = \sqrt{3} + \sqrt{2}, \alpha_2 = -\sqrt{3} - \sqrt{2}, \alpha_3 = \sqrt{3} - \sqrt{2}, \alpha_4 = -\sqrt{3} + \sqrt{2}.$$

Entonces el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$ es $\mathbb{Q}[\sqrt{3} + \sqrt{2}, \sqrt{3} - \sqrt{2}] = \mathbb{Q}[\sqrt{3}, \sqrt{2}]$.

Si $p = 2$ es claro que $X^4 + 1 = (X + 1)^4$. Si $p \neq 2$, entonces puede ocurrir que 2 sea un cuadrado en $\mathbb{F}_p$, en cuyo caso $\sqrt{2} \in \mathbb{F}_p$ y $f(X) = g_1(X)g_2(X)$, donde $g_1(X) = (X - \alpha_1)(X - \alpha_4), g_2(X) = (X - \alpha_2)(X - \alpha_3)$ están en $\mathbb{F}_p[X]$. Si 3 es un cuadrado en $\mathbb{F}_p[X]$, entonces consideramos $h_1(X) = (X - \alpha_1)(X - \alpha_3), h_2(X) = (X - \alpha_2)(X - \alpha_4)$. Por último, si 2 y 3 no son cuadrados entonces $6 = 2 \cdot 3$ es cuadrado en $\mathbb{F}_p$, y la factorización es $m_1(X) = (X - \alpha_1)(X - \alpha_2), m_2(X) = (X - \alpha_3)(X - \alpha_4)$.

Ejercicio 5.– Construya cuerpos de descomposición de los polinomios $X^3 + 2X + 1$ y $X^3 + X^2 + X + 2$ sobre $\mathbb{Z}/3\mathbb{Z}$. Determine si son isomorfos y, en tal caso, calcule un isomorfismo.

Solución 5 *Sea $f(X) = X^3 + 2X + 1$, y llamemos $\alpha_1, \alpha_2, \alpha_3$ a sus raíces. Un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Z}/3\mathbb{Z}$ es, claramente, $K_1 = \mathbb{Z}/3\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$. Si dividimos por $X - \alpha_1$, se tiene que $f(X) = (X - \alpha_1)(X^2 + \alpha_1 X + (2 + \alpha_1^2))$. Entonces, las otras raíces, en función de α_1, son*

$$\alpha_2 = \frac{-\alpha_1 + \sqrt{\Delta}}{2}, \alpha_3 = \frac{-\alpha_1 - \sqrt{\Delta}}{2},$$

donde $\Delta = \alpha_1^2 - 4(2 + \alpha_1^2)$. Vamos a ver que $\alpha_2, \alpha_3 \in \mathbb{Z}/3\mathbb{Z}[\alpha_1]$. En efecto,

$$\Delta = \alpha_1^2 - 8 - 4\alpha_1^2 = 1 - 3\alpha_1^2 = 1,$$

de donde $\alpha_2 = 2(-\alpha_1 + 1), \alpha_3 = 2(-\alpha_1 - 1)$*, pues el inverso de* 2 *en* $\mathbb{Z}/3\mathbb{Z}$ *es* 2*. Nos queda entonces que* $K_1 = \mathbb{Z}/3\mathbb{Z}[\alpha_1]$*.*

El polinomio $g(X) = X^3 + X^2 + X + 2$ *es irreducible sobre* $\mathbb{Z}/3\mathbb{Z}[X]$*. Llamemos* $\beta_1, \beta_2, \beta_3$ *a sus raíces. Como antes, nos queda*

$$g(X) = (X - \beta_1)(X^2 + (1 + \beta_1)X + (1 + \beta_1 + \beta_1^2)),$$

y las otras raíces, en función de β_1*, quedan*

$$\beta_2 = 2(-(1 + \beta_1) + \sqrt{\Delta}), \beta_3 = 2(-(1 + \beta_1) - \sqrt{\Delta}),$$

donde $\Delta = (1 + \beta_1)^2 - 4(1 + \beta_1 + \beta_1^2) = \beta_1$*. Tenemos que ver si existe* $\gamma \in \mathbb{Z}/3\mathbb{Z}[\beta_1]$ *tal que* $\gamma^2 = \beta_1$*. Si llamamos* $\gamma = a_0 + a_1\beta_1 + a_2\beta_1^2$*, con* $a_0, a_1, a_2 \in \mathbb{Z}/3\mathbb{Z}$*, la condición* $\gamma^2 = \beta_1$ *nos lleva al sistema*

$$\begin{aligned} a_0^2 + 2a_2^2 - a_1a_2 &= 0 \\ -a_2^2 + 2a_0a_1 - 2a_1a_2 &= 1 \\ a_1^2 + 2a_0a_2 - 2a_1a_2 &= 0. \end{aligned}$$

Recordemos que si $a \in \mathbb{Z}/3\mathbb{Z}, a \neq 0$*, entonces* $a^2 = 1$*. Una solución es* $a_0 = 0, a_1 = 2, a_2 = 1$*. Por tanto, un cuerpo de descomposición de* $g(X)$ *sobre* $\mathbb{Z}/3\mathbb{Z}$ *es* $K_2 = \mathbb{Z}/3\mathbb{Z}[\beta_1]$*.*

Los cuerpos K_1 *y* K_2 *son cuerpos finitos de* 3^3 *elementos. Por tanto, son isomorfos. Vamos a encontrar explícitamente un isomorfismo. Buscamos una aplicación* $\varphi : K_1 \to K_2$*, que envía* α_1 *en* $\varphi(\alpha_1) = a_0 + a_1\beta_1 + a_2\beta_1^2$*, con* $a_0, a_1, a_2 \in \mathbb{Z}/3\mathbb{Z}$*. La condición que tiene que verificar para que sea homomorfismo es que* $\varphi(\alpha_1)^3 + 2\varphi(\alpha_1) + 1 = 0$*. Recordemos que* $a^3 = a$ *para todo* $a \in \mathbb{Z}/\mathbb{Z}3$*, y entonces nos queda el sistema*

$$\begin{aligned} a_1 + 2a_2 + 1 &= 0 \\ a_1 + a_2 &= 0 \end{aligned}$$

que tiene como solución $a_1 = 1, a_2 = 2$ *y* a_0 *libre. Como es un homomorfismo entre cuerpos no nulo, es inyectivo, y como tienen el mismo número de elementos, es sobreyectivo.*

Ejercicio 6.– Sea $L|k$ una extensión de cuerpos finitos, con $[L : k] = n$, y $f(X) \in k[X]$ un polinomio irreducible que tiene una raíz $a \in L$. Sea Φ generador del grupo $\mathrm{Gal}(L|k)$ y

$$g(X) = (X - a)(X - \Phi(a)) \cdots (X - \Phi^{n-1}(a)) \in L[X].$$

1. Pruebe que
$$g(X) = X^n - a_1X^{n-1} + \ldots + (-1)^n a_n,$$
donde $a_i = S_i(a, \Phi(a), \ldots, \Phi^{n-1}(a))$, y S_i las funciones simétricas elementales (ejercicio 107 de la relación).
2. Deduzca que $\Phi(a_i) = a_i$ para todo $i = 1, \ldots, n$.
3. A partir de lo anterior, concluya que $g(X) \in k[X]$ y que $f(X)$ factoriza en $L[X]$ en factores lineales.

Solución 6 *1. No es más que la expresión de los coeficientes de un polinomio en función de sus raíces.*

2. $\Phi(a_i) = \Phi(S_i(a, \Phi(a), \ldots, \Phi^{n-1}(a))) = S_i(\Phi(a), \Phi^2(a), \ldots, \Phi^{n-1}(a), a) = a_i$*.*

3. Lo anterior implica que a_i *pertenece al cuerpo fijo de* $\mathrm{Gal}(L|k)$*, que es* k*. Entonces* $g(X) \in k[X]$ *y* $f(X)$ *divide a* $g(X)$*. Entonces* $f(X)$ *factoriza en* $L[X]$ *en factores lineales, pues* g *lo hace.*

Ejercicio 7.– Construya un cuerpo finito de 16 elementos y calcule un generador del grupo multiplicativo. ¿Cuántos generadores hay?

Solución 7 *Consideremos el polinomio* $f(X) = X^4 + X + 1$*, que es irreducible sobre* $\mathbb{F}_2[X]$*. Entonces* $K = \mathbb{F}_2[X]/\langle f(X)\rangle$ *es un cuerpo con* $2^4 = 16$ *elementos. Si representamos la clase de* X *por* x*, un generador del grupo multiplicativo es* x*. Los restantes generadores son*

$$1 + x, x^2, 1 + x^2, 1 + x^3, 1 + x + x^3, 1 + x^2 + x^3, x + x^2 + x^3.$$

Ejercicio 8.– Pruebe que $2, 3$ o 6 es un cuadrado en $\mathbb{Z}/\mathbb{Z}p$ para todo primo p. Concluya que el polinomio $(x^2-2)(x^2-3)(x^2-6)$ tiene una raíz en $\mathbb{Z}/\mathbb{Z}p$ para todo primo p pero no tiene raíces en $\mathbb{Z}$.

Solución 8 *Si* 2 *y* 3 *no son cuadrados, sea* θ *un generador de* $\mathbb{F}_p^*$. *Entonces* $2 = \theta^{e_1}, 3 = \theta^{e_2}$, *para ciertos* $e_1, e_2 \in \mathbb{N}$. *Como* 2 *y* 2 *no son cuadrados, los números* e_1, e_2 *son impares. Entonces* $6 = 2 \cdot 3 = \theta^{e_1+e_2}$, *con* $e_1 + e_2$ *un número par. Sea* $e_1 + e_2 = 2e$. *Entonces* $6 = (\theta^e)^2$ *es un cuadrado. La conclusión sobre el polinomio* $(x^2-2)(x^2-3)(x^2-6)$ *es inmediata.*

Ejercicio 9.– Sea $k = \mathbb{Z}/\mathbb{Z}p$ y $a \in k, a \neq 0$. El cuerpo de descomposición del polinomio $f(x) = x^p - x - a$ sobre k es $k[\alpha]$, donde α es una raíz de $f(x)$ (ejercicio 2, 12 Mayo). Pruebe explícitamente que el grupo de Galois de $k[\alpha]$ sobre k es cíclico.

Solución 9 *Recordemos que las raíces de este polinomio son* $\alpha, \alpha+1, \ldots, \alpha+(p-1)$. *Sea* $\varphi : k[\alpha] \to k[\alpha]$ *definido por* $\phi(\alpha) = \alpha + 1$, *y que deje invariantes a los elementos de* k. *Entonces* φ *es un elemento de* $\mathrm{Gal}(k[\alpha]|k)$. *Sabemos que el orden del grupo de Galois* $\mathrm{Gal}(k[\alpha]|k]$ *es igual a* p, *y el grupo cíclico generado por* φ *tiene* p *elementos. En concreto,* $\varphi^i(\alpha) = \alpha + i$, *con* $i = 0, 1, \ldots, p-1$. *Entonces* $\mathrm{Gal}(k[\alpha]|k) = \langle\varphi\rangle$.