ÁLGEBRA 3
Segundo cuatrimestre — 2014

Segundo parcial

APELLIDO Y NOMBRE: .....

L.U.: ..... HOJAS: .....

---

1. Sean $E = \mathbb{Q}(\sqrt[3]{2})$ y $\alpha = 1 + \sqrt[3]{2}$. Muestre que para cada $n > 1$ el polinomio $X^n - \alpha$ no tiene raíces en E.

Solución. El conjunto $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ es una base de E sobre $\mathbb{Q}$ y la matriz de la multiplicación por α con respecto a esa base es $\left(\begin{smallmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right)$. Calculando el determinante de esta matriz vemos que $N_{E/\mathbb{Q}}(\alpha) = 3$. Sea $n > 1$ y supongamos que $\beta \in E$ es una raíz de $X^n - \alpha$, esto es, que $\beta^n = \alpha$. Debe ser entonces $N(\beta)^n = N(\alpha) = 3$ y, en consecuencia, $N(\beta) \in \mathbb{Q}$ es una raíz n-ésima de 3: esto es absurdo. □

2. Sea p un número primo y sea $n \geq 2$.

(*a*) Si $p \equiv 1 \mod n$, entonces para cada $a \in \mathbb{F}_p$ el polinomio $X^n - a$ se factoriza como producto de factores lineales en $\mathbb{F}_{p^n}[X]$.

(*b*) Sea $r \geq 1$ y supongamos que $p \nmid n$. El polinomio $\bar{\Phi}_n$ se descompone como producto de factores lineales en $\mathbb{F}_{p^r}[X]$ si y solamente si $p^r \equiv 1 \mod n$.

Solución. (*a*) Si $a = 0$, la conclusión deseada es evidente, así que podemos suponer que $a \neq 0$. Sea $f = X^n - a$ y sea b una raíz de f en una clausura algebraica de $\mathbb{F}_p$; es $b \neq 0$.

Como $p \equiv 1 \mod n$, es $(p^n - 1)/(p - 1) = p^{n-1} + \cdots + 1 \equiv n \equiv 0 \mod n$ y el número $(p^n - 1)/(n(p - 1))$ es un entero. Vemos así que $(p^n - 1)/n$ es un entero divisible por $p - 1$.

Es $b^{p^n-1} = (b^n)^{(p^n-1)/n} = a^{(p^n-1)/n} = 1$, porque $a^{p-1} = 1$, y esto nos dice que $b \in \mathbb{F}_{p^n}$ y, entonces, que f tiene una raíz en $\mathbb{F}_{p^n}$. Por otro lado, como n divide a $p^n - 1$, el grupo cíclico $\mathbb{F}_{p^n}^\times$, que tiene orden $p^n - 1$, tiene un subgrupo de orden n: esto significa que $\mathbb{F}_{p^n}$ contiene una raíz n-ésima primitiva de la unidad. Podemos concluir entonces que f tiene n raíces distintas en $\mathbb{F}_{p^n}$, lo que implica la conclusión del enunciado.

(*b*) Sabemos que $\bar{\Phi}_n$ se factoriza sobre $\mathbb{F}_{p^r}$ como producto de factores irreducibles de grado igual al orden de p^r módulo n. Es claro, entonces, que esta factorización es en factores lineales sii $p^p \equiv 1 \mod n$. □

3. Sea p un número primo, $r \geq 1$ y $\zeta \in \mathbb{C}$ una raíz p^r-ésima primitiva de la unidad. Calcule $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta)$.

Solución. El minimal de ζ sobre $\mathbb{Q}$ es $\Phi_{p^r}(X)$, así que el de $1-\zeta$ es $(-1)^{\phi(p^r)}\Phi_{p^r}(1-X)$. El término constante de este último, que es su valor en 0, es $d = (-1)^{\phi(p^r)}\Phi_{p^r}(1)$. Como $1-\zeta$ genera a $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ y tiene grado $\phi(p^r)$, tenemos que

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = (-1)^{\phi(p^r)}d = \Phi_{p^r}(1) = p,$$

ya que $\Phi_{p^r}(X) = \Phi_r(X^{p^{r-1}})$ y $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$. □

4. Sea $k \in \mathbb{Z}$ y $a = k^2+k+7$. Determine el grupo de Galois de $X^3 - aX + a$ sobre $\mathbb{Q}$.

Solución. Mostremos primero que el polinomio es irreducible; notemos que, como es cúbico, basta para ello con probar que no tiene raices racionales y que, de acuerdo al lema de Gauss, sus posibles raices racionales son enteras. Supongamos entonces, para llegar a un absurdo, que $b \in \mathbb{Z}$ es una raíz, de manera que $b^3 = a(b-1)$. Como b^3 y $b-1$ son coprimos, debe ser $b-1 = 1$, esto es, $b = 2$ y entonces $2^3 - 2a + a = 8 - a = 1 - k - k^2 = 0$. Esto es absurdo, porque el polinomio $X^2 + X - 1$ no tiene raíces enteras.

Ahora bien, el discriminante de un polinomio de la forma $X^3 + bX + c$ es $-4b^3 - 27c^2$, así que el discriminante de nuestro polinomio es

$$-4(-a)^3 - 27a^2 = (4a-27)a^2 = (4k^2+4k+1)a^2 = (2k+1)^2a^2.$$

Esto es un cuadrado en $\mathbb{Q}$, así que el grupo de Galois está contenido en A_3. Como A_3 tiene orden 3, el grupo de Galois debe ser entonces isomorfo a A_3. □

5. Si p es un primo impar, para cada $n \in \mathbb{N}$ el polinomio ciclotómico Φ_n es irreducible sobre $\mathbb{Q}(\sqrt[p]{2})$. Esto no es cierto si $p = 2$.

Solución. Sea $n \in \mathbb{N}$ y sea $\zeta \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad. Para mostrar que Φ_n es irreducible sobre $\mathbb{Q}(\sqrt[p]{2})$, hay que mostrar que $[\mathbb{Q}(\zeta, \sqrt[p]{2}) : \mathbb{Q}(\sqrt[p]{2})] = \phi(n)$. Supongamos que no es éste el caso, con lo que $[\mathbb{Q}(\zeta, \sqrt[p]{2}) : \mathbb{Q}(\sqrt[p]{2})] < \phi(n)$. Es entonces

$$\begin{aligned}\phi(n)[\mathbb{Q}(\zeta, \sqrt[p]{2}) : \mathbb{Q}(\zeta)] &= [\mathbb{Q}(\zeta, \sqrt[p]{2}) : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta, \sqrt[p]{2}) : \mathbb{Q}] \\ &= [\mathbb{Q}(\zeta, \sqrt[p]{2}) : \mathbb{Q}(\sqrt[p]{2})] \cdot [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] < p\phi(n),\end{aligned}$$

de manera que $[\mathbb{Q}(\zeta, \sqrt[p]{2}) : \mathbb{Q}(\zeta)] < p$: vemos así que el polinomio $X^p - 2$, que es irreducible sobre $\mathbb{Q}$, es reducible sobre $\mathbb{Q}(\zeta)$. Como la extensión $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ es Galoisiana, los factores irreducibles de $X^p - 2$ en $\mathbb{Q}(\zeta)[X]$ tienen todos el mismo grado d y, en consecuencia, $d \mid p$. Como $d < p$, debe ser $d = 1$, y esto nos dice que $X^p - 2$ tiene todas sus raíces en $\mathbb{Q}(\zeta)$. Así, $\mathbb{Q}(\zeta)$ contiene un cuerpo de descomposición E de $X^p - 2$ sobre $\mathbb{Q}$. La extensión $E/\mathbb{Q}$ es normal y su grupo de Galois es un cociente del grupo de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}$: como éste es abeliano, también tiene que serlo aquél. Esto es absurdo —sabemos que el grupo de Galois de $X^p - 2$ es no abeliano— y esto prueba que $[\mathbb{Q}(\zeta, \sqrt[p]{2}) : \mathbb{Q}(\sqrt[p]{2})] = \phi(n)$, como queríamos.

Veamos que el primo par no tiene la propiedad del enunciado. El número $z = (1+i)/\sqrt{2}$ es una raíz octava primitiva de la unidad y $z + z^{-1} = \sqrt{2}$. Esto nos dice que $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(z)$, así que $[\mathbb{Q}(z) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(z) : \mathbb{Q}]/[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \phi(8)/2$. Esto implica que Φ_8, que tiene grado $\phi(8)$, es reducible sobre $\mathbb{Q}(\sqrt{2})$. □