Práctica 2: Extensiones de cuerpos

1 Sean B un anillo conmutativo, A un subanillo de B y b un elemento de B. Se define $A[b]$ como el menor subanillo de B que contiene a A y a b.

(*a*) Probar que $A[b] = \left\{ \sum_{i=0}^{n} a_i \cdot b^i \;\middle|\; n \in \mathbb{N}_0,\ a_i \in A \text{ para todo } i \right\}$.

(*b*) Observar que $A[b]$ es la imagen del morfismo de anillos $\mathrm{ev}_b : A[X] \to B$ que manda X a b y actúa como la identidad sobre los elementos de A. Deducir que $A[b] \cong A[X]/\ker \mathrm{ev}_b$. En particular, si no existe ningún polinomio no nulo en $A[X]$ que anule a b, entonces $A[b] \cong A[X]$.

(*c*) Probar que si existe N tal que b^{N+1} es una combinación lineal con coeficientes en A del conjunto $\{1, b, b^2, \ldots, b^N\}$, entonces $A[b] = \left\{ \sum_{i=0}^{N} a_i \cdot b^i \;\middle|\; a_i \in A \text{ para todo } i \right\}$.

(*d*) Análogamente se define $A[S]$ para cualquier subconjunto $S \subseteq B$. ¿Cómo se pueden describir los elementos de $A[S]$?

2 Sea E/K una extensión de cuerpos y sea α un elemento de E. Probar que las siguientes afirmaciones son equivalentes:

(i) $K[\alpha]$ es un cuerpo.

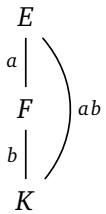
(ii) Existe algún polinomio no nulo $f \in K[X]$ tal que $f(\alpha) = 0$.

(iii) Existe un polinomio **irreducible** $f \in K[X]$ tal que $f(\alpha) = 0$.

El ítem (ii) es la definición de que α sea **algebraico** sobre K. Si esto no ocurre decimos que α es **trascendente** sobre K.

3 Sea E/K una extensión finita. Probar que todo elemento de E es algebraico sobre K (es decir, la extensión E/K es algebraica).

4 Sean E/F y F/K dos extensiones de cuerpos. Probar que $[E : K] = [E : F] \cdot [F : K]$. Deducir que la extensión E/K es finita si y sólo si E/F y F/K lo son.



5 Sean E/K una extensión de cuerpos y S un subconjunto de E. Se define $K(S)$ como el menor subcuerpo de E que contiene a K y a S. (También se podría decir: la menor *subextensión* de E/K que contiene a S.)

(*a*) Probar que si $\alpha_1, \ldots, \alpha_m \in E$ son algebraicos sobre K entonces $K[\alpha_1, \ldots, \alpha_m]$ es un cuerpo. Deducir que $K(\alpha_1, \ldots, \alpha_m) = K[\alpha_1, \ldots, \alpha_m]$.

(*b*) En las hipótesis de (*a*), probar que la extensión $K(\alpha_1, \ldots, \alpha_m)/K$ es algebraica.

(*c*) Probar que si $S \subseteq E$ es un subconjunto (no necesariamente finito) tal que todo elemento de S es algebraico sobre K, entonces $K(S) = K[S]$ y la extensión $K(S)/K$ es algebraica.

(*d*) Deducir que $E_{\text{alg}} = \{\alpha \in E \mid \alpha \text{ es algebraico sobre } K\}$ es un subcuerpo de E.

6 Sean E/K y F/K dos extensiones finitas, con E y F subcuerpos de un cuerpo L.

(*a*) Probar que $[EF : F] \leq [E : K]$.

(*b*) Probar que si $[E : K]$ y $[F : K]$ son coprimos entonces vale la igualdad en (*a*).

(*c*) Mostrar con un ejemplo que tener igualdad en (*a*) no implica que $[E : K]$ y $[F : K]$ sean coprimos.

(*d*) Probar que si $[E : K]$ y $[F : K]$ son coprimos entonces $E \cap F = K$. ¿Vale la vuelta?

7 Calcular el grado de cada una de las siguientes extensiones de cuerpos:

(*a*) $\mathbb{Q}\left(\sqrt[5]{3}\right)/\mathbb{Q}$

(*b*) $\mathbb{C}/\mathbb{R}$

(*c*) $\mathbb{Q}(i)/\mathbb{Q}$

(*d*) $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$

(*e*) $\mathbb{Q}\left(\sqrt[18]{5}\right)/\mathbb{Q}\left(\sqrt[3]{5}\right)$

(*f*) $\mathbb{Q}\left(\sqrt[3]{3+\sqrt{7}}\right)/\mathbb{Q}$

(*g*) $\mathbb{Q}\left(\sqrt{7+4\sqrt{3}}\right)/\mathbb{Q}(\sqrt{3})$

(*h*) $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)/\mathbb{Q}$

(*i*) $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{6})/\mathbb{Q}$

(*j*) $\mathbb{Q}\left(\sqrt{2}\,i\right)/\mathbb{Q}$

(*k*) $\mathbb{Q}\left(\sqrt[3]{2}, i\right)/\mathbb{Q}$

(*l*) $\mathbb{Q}\left(\sqrt[3]{2}\,i\right)/\mathbb{Q}$

(*m*) $\mathbb{Q}\left(\sqrt[4]{3}, i\right)/\mathbb{Q}(i)$

(*n*) $\mathbb{Q}\left(\sqrt[3]{5}, \sqrt[4]{7}\right)/\mathbb{Q}$

(*o*) $\mathbb{Q}\left(\sqrt[10]{3}, \sqrt[15]{3}\right)/\mathbb{Q}$

8 Consideramos el polinomio $f = X^3 + 6X + 3 \in \mathbb{Q}[X]$.

(*a*) Probar que f tiene exactamente una raíz real.

(*b*) Sea $\alpha \in \mathbb{C}$ una de las raíces no reales de f, y sea $E = \mathbb{Q}(\sqrt[8]{2}, \alpha)$. Calcular $[E : \mathbb{Q}]$.

(*c*) Calcular $E \cap \mathbb{R}$.

9 Sea $f \in \mathbb{Q}[X]$ un polinomio irreducible de grado 3 y sean $\alpha, \beta \in \mathbb{C}$ dos raíces de f.

(*a*) Probar que $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 3$ o 6.

(*b*) Probar que si $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 3$ entonces todas las raíces de f están en $\mathbb{R}$.

Nota. Más adelante podremos probar que no vale la vuelta en (*b*).

10 Probar que $[\mathbb{R} : \mathbb{Q}] > \aleph_0$.

11 Probar que el polinomio $X^{10} + 4$ es irreducible en $\mathbb{Q}[X]$.

12 Sea K un cuerpo **cuya característica no es 2** y sea E/K una extensión de cuerpos. Supongamos que $\alpha, \beta \in E$ son tales que $\alpha^2, \beta^2 \in K$ y $\alpha + \beta \neq 0$. Probar que $K(\alpha, \beta) = K(\alpha + \beta)$.

Sugerencia. Probar primero que $\alpha - \beta \in K(\alpha + \beta)$.

13 Sea E/K una extensión de grado impar y sea $\alpha \in E$. Probar que $K(\alpha) = K\left(\alpha^2\right)$.

14 Sea p un número primo. Hallar **todos** los valores de $n \in \mathbb{N}$ para los cuales el polinomio $X^n - p^2$ es irreducible en $\mathbb{Q}[X]$.

15 Sean p un número primo y E/K una extensión de grado p^2. Probar que existen $\alpha, \beta \in E$ tales que $E = K(\alpha, \beta)$.

16 Sea $p > 2$ un número primo. Sean $\alpha, \beta \in \mathbb{C}$ dos raíces distintas del polinomio $X^p - 2$. Probar que $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$.

17 (a) Sea K un cuerpo cuya característica no es 2 y sea E/K una extensión de grado 2. Probar que existe $\beta \in E$ tal que $E = K(\beta)$ y $\beta^2 \in K$. (En otras palabras, E se obtiene *agregando una raíz cuadrada de un elemento de* K.)
¿En qué paso se usa que K no tiene característica 2?

(b) Sea L/K una extensión de cuerpos y sean $\alpha, \beta \in L$ tales que $\alpha^2, \beta^2 \in K$ pero $\alpha, \beta \notin K$. Probar que $K(\alpha) = K(\beta)$ si y sólo si $\alpha\beta \in K$.

(c) Caracterizar completamente las subextensiones de grado 2 de $\mathbb{R}/\mathbb{Q}$. (Esto significa: dar una "lista" de subextensiones de modo que cualquier subextensión de grado 2 de $\mathbb{R}/\mathbb{Q}$ es igual a exactamente una de las de la lista.)

18 Sean $p_1, p_2, \ldots, p_n$ primos (positivos) distintos y sea $E = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$.

(a) Probar que si $\alpha \in E$ es tal que $\alpha^2 \in \mathbb{Q}$, entonces existen $q \in \mathbb{Q}$ y $J \subseteq \{1, 2, \ldots, n\}$ tales que $\alpha = q \cdot \sqrt{\prod_{j \in J} p_j}$.

(b) Calcular $[E : \mathbb{Q}]$.

19 Calcular el polinomio minimal de $\sqrt{3} + \sqrt{5}$ sobre $\mathbb{Q}$ y sobre $\mathbb{Q}(i)$.

Sugerencia. Mirar el ejercicio **12**.

20 Sea E/K una extensión algebraica de grado infinito. Probar que para todo $n_0 \in \mathbb{N}$ existe alguna subextensión **finita** F/K tal que $[F : K] > n_0$.

21 (a) Sean K un cuerpo y $f \in K[X]$ un polinomio no constante. Probar que existe una extensión de K en la cual f tiene una raíz.

Sugerencia. Si g es un factor irreducible de f, entonces $E = K[X]/\langle g \rangle$ es un cuerpo.

(b) Deducir que dada cualquier cantidad finita de polinomios no constantes de $K[X]$, existe una extensión de K sobre la cual todos ellos se factorizan linealmente.

22 Sea $f \in K[X]$ un polinomio irreducible de grado d. Sea E/K una extensión cuyo grado es coprimo con d. Probar que f es irreducible sobre E.

23 Sea K un cuerpo y sean f y g dos polinomios en $K[X]$, no constantes. Sea α una raíz de f en una extensión de K. Probar que el polinomio $h(X) = f(g(X))$ es irreducible sobre K si y sólo si se cumplen las siguientes dos condiciones:

- f es irreducible sobre K,
- $g - \alpha$ es irreducible sobre $K(\alpha)$.

24 **Convencerse** de que, con las herramientas que venimos usando, no es fácil calcular el grado de la extensión $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})/\mathbb{Q}$.
O encontrar una demostración que sirva como contraejemplo.