Álgebra III

Práctica 6 - Segundo cuatrimestre de 2016

Norma y traza. Extensiones resolubles.

Ejercicio 1.

1. Calcular la norma y la traza de $\sqrt[3]{2}$ en $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ y en $\mathbb{Q}[\sqrt[3]{2}, \xi_3]/\mathbb{Q}$.
2. Sea $p \in \mathbb{N}$ primo. Calcular la norma y la traza de ξ_p y de $1 - \xi_p$ en $\mathbb{Q}[\xi_p]/\mathbb{Q}$.
3. Sea $d \in \mathbb{N}$ libre de cuadrados y sea $\alpha \in \mathbb{Q}[\sqrt{d}] - \mathbb{Q}$. Probar que $m(\alpha, \mathbb{Q}) = X^2 - \mathrm{Tr}(\alpha)X + \mathrm{N}(\alpha)$.

Ejercicio 2. Sea K un cuerpo de característica $p > 0$ y sea t trascendente sobre K. Calcular la norma y la traza en $K(t)/K(t^p)$.

Ejercicio 3. Sea K un cuerpo y sea $f \in K[X]$ irreducible de grado n. Sea $\alpha \in \overline{K}$ una raíz. Probar que para todo $c \in K$ se tiene

$$N_{K[\alpha]/K}(\alpha - c) = (-1)^n f(c).$$

Ejercicio 4. Sea $p > 3$ un primo. Sean $E = \mathbb{F}_p(u, v)$ y $K = \mathbb{F}_p(u^3, v^2)$, donde u y v son algebraicamente independientes sobre $\mathbb{F}_p$. Calcular la norma y la traza de $u + v$ en E/K.

Ejercicio 5. Si $n > 1$, probar que el polinomio $X^n - (1 + \sqrt[3]{2})$ no tiene raices en $\mathbb{Q}(\sqrt[3]{2})$.

Ejercicio 6. Sea E/K una extensión finita. Probar que:

1. E/K es separable si y solo si $\mathrm{Tr} : E \to K$ es no nula.
2. Si E/K es separable, entonces $\mathrm{Tr} : E \to K$ es suryectiva.
3. La aplicación $\mathrm{Tr} : E \times E \to K$ dada por $\mathrm{Tr}(a, b) = \mathrm{Tr}(ab)$ es una forma bilineal simétrica.
4. Para cada $a \in E$ se define $\mathrm{Tr}_a : E \to K$ mediante $\mathrm{Tr}_a(b) = \mathrm{Tr}(ab)$.
   (a) Verificar que $\mathrm{Tr}_a \in E^*$ para todo $a \in E$.
   (b) Probar que si E/K es separable, entonces la aplicación $a \longmapsto \mathrm{Tr}_a$ es un isomorfismo de E en E^*.

Ejercicio 7. Sean $p, q \in \mathbb{N}$ primos distintos. Sea K un cuerpo de característica p y sea E/K una extensión de grado $[E : K] = q$. Probar que existe $\alpha \in E$ tal que $E = K[\alpha]$ y el coeficiente de grado $q - 1$ en $m(\alpha, K)$ es nulo.

Ejercicio 8.

1. Calcular el núcleo y la imagen del morfismo de grupos $\mathbb{C}^* \to \mathbb{R}^*$ dado por $x \longmapsto \mathrm{N}_{\mathbb{C}/\mathbb{R}}(x)$.
2. Probar que en $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ la norma no es inyectiva ni suryectiva.

Ejercicio 9. Sea K un cuerpo finito y sea L/K una extensión finita. Probar que la norma y la traza en L/K son suryectivas.

Ejercicio 10. Sea K un cuerpo de característica p y sea E/K una extensión de grado n, con $p \nmid n$. Sea $\alpha \in E$. Probar que si $\mathrm{Tr}_{E/K}(\alpha^i) = 0$ para todo $1 \leqslant i \leqslant n$, entonces $\alpha = 0$.

Ejercicio 11. Sea t trascendente sobre $\mathbb{F}_7$; sean $E = \mathbb{F}_7(t)$ y $K = \mathbb{F}_7(t^7 - t)$. Encontrar una base de E como K-espacio vectorial formada por elementos de traza 1.

Ejercicio 12. Sean $r, n \in \mathbb{N}$. Sean $p_1, \dots, p_n \in \mathbb{N}$ primos distintos. Probar que $\mathbb{Q}[\sqrt[r]{p_1}, \dots, \sqrt[r]{p_n}]/\mathbb{Q}$ es de grado r^n y que $\sqrt[r]{p_1} + \dots + \sqrt[r]{p_n}$ es un elemento primitivo.

Ejercicio 13. Sea $K/\mathbb{Q}$ una extensión de grado n donde $K = \mathbb{Q}(\sqrt[n]{a})$ con $a \in \mathbb{Q}_{>0}$. Sea E una subextensión de grado d. Calcular $N_{K/E}(\sqrt[n]{a})$ y probar que $E = \mathbb{Q}(\sqrt[d]{a})$.

Ejercicio 14. Sean K un cuerpo, C/K una clausura algebraica de K y $f \in K[X]$ un polinomio mónico de grado $n \geq 1$. Si $f = (X - a_1) \dots (X - a_n)$ (con $a_i \in C$) se define el discriminante de f en la forma:

$$\Delta(f) = \prod_{i<j} (a_i - a_j)^2$$

i) Probar que:

   a) Si $f = X^2 + bX + c$, entonces $\Delta(f) = b^2 - 4c$.

   b) Si $f = X^3 + bX + c$, entonces $\Delta(f) = -4b^3 - 27c^2$.

ii) Sea $E/\mathbb{Q}$ una extensión de grado n de $\mathbb{Q}$. Sea a tal que $E = \mathbb{Q}(a)$ y sea $f = m(a, \mathbb{Q})$. Probar que $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} N_{E/\mathbb{Q}}(f'(a))$, donde f' es el polinomio derivado de f.

Ejercicio 15. Sea $n \in \mathbb{N}N$, $n \geq 2$. Probar que si $f = X^n + bX + c \in \mathbb{Q}[X]$, entonces $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} (n^n c^{n-1} + (1-n)^{n-1} b^n)$.

Ejercicio 16. Sea k un entero y sea $a = k^2 + k + 7$. Calcular el grupo de Galois del polinomio $X^3 - aX + a$.

Ejercicio 17. Sea $E/\mathbb{Q}$ un cuerpo de descomposición de $X^3 + X + 1$. Probar que el polinomio $X^4 - 6X^2 + 40$ es reducible en $E[X]$.

Ejercicio 18. Sean $E = K(t_1, t_2, t_3, t_4)$ y $F = K(s_1, s_2, s_3, s_4)$, donde $\{t_1, t_2, t_3, t_4\}$ es una familia algebraicamente independiente sobre K y $\{s_1, s_2, s_3, s_4\}$ es el conjunto de polinomios simétricos elementales en t_1, t_2, t_3, t_4.

i) Probar que $F(t_1 + t_2)/F$ es una subextensión no normal de E/F y calcular su grado.

ii) Sean i, j tales que $1 \leq i < j \leq 4$. Probar que $t_i + t_j \in F(t_1 + t_2)$ si y sólo si $i = 1$, $j = 2$ o $i = 3$, $j = 4$.

iii) Caracterizar $Gal(F(t_1 + t_2)/F)$.

Ejercicio 19. Sea $\{t_1, \dots, t_n\}$ una familia algebraicamente independiente sobre un cuerpo K y sea $\{s_1, \dots, s_n\}$ el conjunto de los polinomios simétricos elementales en $\{t_1, \dots, t_n\}$.

i) Caracterizar las subextensiones de grado 2 de $K(t_1, \dots, t_n)/K(s_1, \dots, s_n)$.

ii) Sean $a_1, \dots, a_n \in \mathbb{N}$. Probar que $t_1^{a_1} + t_2^{a_2} + \dots + t_n^{a_n}$ genera $K(t_1, \dots, t_n)/K(s_1, \dots, s_n)$ si y sólo si $a_i \neq a_j \ \forall\, i \neq j$.

Ejercicio 20. Probar que:

1. Todo grupo abeliano es resoluble.
2. Todo p-grupo es resoluble.
3. D_n es resoluble.
4. $\mathbb{S}_n$ es resoluble si y solo si $n \leqslant 4$.

Ejercicio 21. Mostrar explicitamente que las siguientes extensiones son resolubles por radicales:

1. $\mathbb{Q}[\sqrt[3]{1+\sqrt{2}}, i+\sqrt{3}]/\mathbb{Q}$
2. $E/\mathbb{Q}$ cuerpo de descomposición de $f = (X^4 - 2)(X^2 - 5)$
3. $N/\mathbb{C}(a, b)$ cuerpo de descomposición de $f = X^2 + aX + b$
4. $N/\mathbb{C}(a, b, c)$ cuerpo de descomposición de $f = X^3 + aX^2 + bX + c$
5. $N/\mathbb{C}(a, b, c, d)$ cuerpo de descomposición de $f = X^4 + aX^3 + bX^2 + cX + d$

Ejercicio 22. Probar que ninguno de los siguientes polinomios es resoluble por radicales sobre $\mathbb{Q}$.

1. $X^5 - 14X + 7$
2. $X^5 - 7X^2 + 7$
3. $X^7 - 10X^5 + 15X + 5$

Ejercicio 23. Sea $f \in \mathbb{Q}[X]$ irreducible de grado primo $\geqslant 5$. Suponer que f tiene exactamente dos raices no reales. Probar que f no es resoluble por radicales sobre $\mathbb{Q}$.

Ejercicio 24. Sea $K \subseteq \mathbb{C}$ un cuerpo. Sea $f \in K[X]$ irreducible de grado primo $p \geqslant 5$. Sean $\alpha_1, \ldots, \alpha_p \in \mathbb{C}$ las raices de f y sea $N = K[\alpha_1, \ldots, \alpha_p]$ el cuerpo de descomposición de f sobre K. Probar que f es resoluble por radicales sobre K si y solo si $N = K[\alpha_i, \alpha_j]$ para todos $1 \leqslant i < j \leqslant p$.

Ejercicio 25.

1. Sea $m \in \mathbb{N}$ par y sean $a_1 < a_2 < \cdots < a_r$ enteros positivos pares con $r > 1$ impar. Sea $f = (X^2 + m)(X - a_1)\cdots(X - a_r) - 2$. Probar que:
   (a) f es irreducible en $\mathbb{Q}[X]$.
   (b) Para m suficientemente grande, f tiene exactamente dos raíces no reales en $\mathbb{C}$.
   (c) (Difícil) Probar que el item anterior sigue valiendo si se quita la hipótesis "m suficientemente grande".
2. Deducir que para cada primo $p \in \mathbb{N}$, existe una extensión normal $E/\mathbb{Q}$ con grupo de Galois isomorfo a $\mathbb{S}_p$.

Ejercicio 26. Sea $f = X^5 - bX - a$ un polinomio irreducible en $\mathbb{Q}[X]$. Sea α una raíz de f y sea $E = \mathbb{Q}(\alpha)$. Si se sabe que $N_{E/\mathbb{Q}}(\alpha + 1) = -77$ y $N_{E/\mathbb{Q}}(\alpha - 1) = 81$, decidir si f es resoluble por radicales.