

ÁLGEBRA III

Práctica 3 – Primer Cuatrimestre de 2004

Cuerpos de descomposición, extensiones normales y grupo de Galois

1. Determinar si las siguientes afirmaciones son verdaderas o falsas. Justificar.
 - i) Todo polinomio no constante se factoriza linealmente sobre algún cuerpo.
 - ii) El cuerpo de descomposición de un polinomio es único, salvo isomorfismos.
 - iii) Toda extensión de grado finito es el cuerpo de descomposición de algún polinomio.
 - iv) Toda extensión de grado finito es normal.
 - v) Toda extensión de grado finito tiene una clausura normal de grado finito.
 - vi) Todo K -morfismo de cuerpos $f : L/K \rightarrow L/K$ es un K -automorfismo.
 - vii) Sea L/K una extensión algebraica. Todo K -morfismo de cuerpos $f : L/K \rightarrow L/K$ es un K -automorfismo.
 - viii) Toda extensión de un cuerpo de característica cero es normal.
 - ix) Toda extensión con grupo de Galois trivial es normal.
 - x) Todo grupo de Galois es abeliano.
 - xi) El grupo de Galois de una extensión normal es cíclico.
 - xii) Sean $K \subseteq L \subseteq E$. Si E es el cuerpo de descomposición de un polinomio $f \in K[X]$ entonces E es el cuerpo de descomposición de f visto como polinomio en $L[X]$.
2. Exhibir cuerpos de descomposición, determinando su grado y sistemas de generadores, para cada uno de los siguientes polinomios sobre los cuerpos indicados:
 - i) $X^p - a$, sobre $\mathbb{Q}$, con $p \in \mathbb{N}$ primo y $a \in \mathbb{N} - \mathbb{N}^p$.
 - ii) $X^3 - 10$, sobre $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$ y $\mathbb{Q}[\sqrt{-3}]$.
 - iii) $X^4 - 5$, sobre $\mathbb{Q}$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{-5}]$ y $\mathbb{Q}[i]$.
 - iv) $X^4 + 2$, sobre $\mathbb{Q}$ y $\mathbb{Q}[i]$.
 - v) $\prod_{i=1}^n (X^2 - p_i)$, sobre $\mathbb{Q}$, con $p_1, \dots, p_n \in \mathbb{N}$ primos distintos.
 - vi) $X^3 - 2$, sobre $\mathbb{Z}_7$.
 - vii) $(X^3 - 2)(X^3 - 3)(X^2 - 2)$, sobre $\mathbb{Q}[\sqrt{-3}]$ y sobre $\mathbb{Z}_5$.
 - viii) $X^n - t$, sobre $\mathbb{C}(t)$, con t trascendente sobre $\mathbb{C}$ y $n \in \mathbb{N}$.
 - ix) $X^4 - t$, sobre $\mathbb{R}(t)$, con t trascendente sobre $\mathbb{R}$.
3. Caracterizar los cuerpos de descomposición de los polinomios $X^3 + 2X + 1$ y $X^3 + X^2 + X + 2$ sobre $\mathbb{Z}_3$. Probar que son isomorfos como extensiones de $\mathbb{Z}_3$.
4. Sea K un cuerpo de característica $p \neq 0$.
 - a) Probar que $\forall n \in \mathbb{N}$, $f : K \rightarrow K$ definido por $f(x) = x^{p^n}$ es un $\mathbb{Z}_p$ -morfismo de cuerpos.

- b) Probar que si K es un cuerpo finito de característica p , entonces el morfismo f definido en i) es un automorfismo. Dar ejemplos de K infinito con esta propiedad.
- c) Si $K = k(t)$, elevar a la p es suryectivo?
5. Sea K el cuerpo de descomposición de $X^{p^n} - X$ sobre $\mathbb{Z}_p$. Probar que $[K : \mathbb{Z}_p] = n$.
 6. Caracterizar $G(L/\mathbb{Z}_2)$ para L tal que $[L : \mathbb{Z}_2] = 2, 3$.
 7. Determinar el cuerpo de descomposición de $X^4 - 10X^2 + 5$ y su grupo de Galois, sobre $\mathbb{Q}$, $\mathbb{Z}_3$ y $\mathbb{Z}_7$.
 8. Sea E/K un cuerpo de descomposición de $f \in K[X]$, $f \neq 0$, y sea F/K una subextensión de E/K . Probar que todo morfismo de F/K en E/K puede ser extendido a un automorfismo de E/K .
 9. Sea $E/F/K$ con F/K subextensión puramente inseparable. Probar que $G(E/K) = G(E/F)$.
 10. Sea E/K una extensión separable que es cuerpo de descomposición de un polinomio $f \in K[X]$ y sea $n = \text{gr}(f)$. Probar que $[E : K] \mid n!$. Dar ejemplos de extensiones donde se cumpla la igualdad, y donde no se cumpla.
 11. Determinar cuáles de las siguientes extensiones E/K son normales. En cada caso calcular $G(E/K)$ y $\text{Hom}(E/K, C/K)$, donde C es una clausura algebraica de K .
 - i) $\mathbb{Q}[\sqrt[3]{5}]/\mathbb{Q}$
 - ii) $\mathbb{Q}[\sqrt[3]{5}, \sqrt{5}]/\mathbb{Q}[\sqrt[3]{5}]$
 - iii) $\mathbb{Q}[\sqrt{2}, \sqrt[3]{3}]/\mathbb{Q}$
 - iv) $\mathbb{Q}(\xi_p)/\mathbb{Q}$, con $p \in \mathbb{N}$ primo
 - v) $\mathbb{Z}_3[a]/\mathbb{Z}_3$, con a raíz de $X^3 + X^2 + 2X + 1$
 12. Sea K un cuerpo, $n \in \mathbb{N}$ y t trascendente sobre K . Probar que $K(t)/K(t^n)$ es normal si y sólo si el polinomio $X^n - 1$ se factoriza linealmente en $K[X]$.
 13.
 - i) Probar que $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}[\sqrt{2}]$ y $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ son normales, pero $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ no lo es (luego, las extensiones normales no son una clase distinguida). Calcular $G(\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q})$.
 - ii) Exhibir extensiones normales con subextensiones no normales.
 14. Sean E/K y F/K subextensiones normales de una extensión H/K . Probar que $E \cdot F/K$ y $E \cap F/K$ son normales.
 15. Probar que toda extensión E/K generada por elementos de grado 2 es normal. ¿Para qué valores de $n \in \mathbb{N}$ se cumple que toda extensión de grado n sobre $\mathbb{Q}$ es normal?
 16. Sea $p \in \mathbb{N}$ primo, $p \neq 2$. Sea $K = \mathbb{Z}_p(u, v)$, donde $\{u, v\}$ es una familia algebraicamente independiente sobre $\mathbb{Z}_p$ y sea α una raíz de $f = X^{2p} - uvX^p + v$ en una clausura algebraica C/K de K .
 - i) Probar que $K(\alpha)/K$ no es normal.
 - ii) Sea E/K un cuerpo de descomposición de f . Hallar $[E : K]$.
 17. Hallar $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ tal que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Idem para $\mathbb{Q}(\sqrt{2}, i)$.

18. Probar que $G(K(X)/K) \simeq \text{PGL}(2, K)$, donde $\text{PGL}(2, K)$ denota el grupo lineal proyectivo $GL(2, K)/(a \cdot Id)$ con $a \neq 0$.
19. Sea E/K una extensión de K y sea $G = G(E/K)$.
- Sea H un subgrupo de G . Probar que $E^H = \{t \in E / f(t) = t \forall f \in H\}$ es una subextensión de E/K .
 - Sea F/K una subextensión de E/K . Probar que $G_F = \{f \in G / f(t) = t \forall t \in F\}$ es un subgrupo de G .
20. Sea $E = K(t)$ con t trascendente y K de característica cero. Si H es el grupo generado por las traslaciones $t \mapsto t + a$, $a \in K$, mostrar que $K(t)^H = K$.
21. Sea $E = k(t)$ y σ el automorfismo determinado por $\sigma(t) = t^{-1}$. Calcular E^σ .
22. Sea $E = \mathbb{Z}_p(t)$ y H el grupo de traslaciones $t \mapsto t + a$, con $a \in \mathbb{Z}_p$. Muestre que $(t^p - t) \in \mathbb{Z}_p[t]^H$, más aun, $\mathbb{Z}_p(t)^H = \mathbb{Z}_p(t^p - t)$.
23. Sea $E = k(x, y, z)$ con x, y, z , trascendentes sobre k , consideremos $G = S_3$ el grupo de permutaciones de tres elementos que escribimos como $G = \{1, r, r^2, s, sr, sr^2\}$ donde r es la permutación cíclica $x \mapsto y \mapsto z \mapsto x$, y s es la trasposición $x \mapsto y \mapsto x, z \mapsto z$. Sea H el subgrupo generado por r . Sabiendo que $E^G = k(s, t, u)$ donde $s = x + y + z$, $t = xy + yz + zx$, $u = xyz$, describa E^H como extensión de E^G . Qué grado tiene? Describir también E^s .
24. Si A es una k -álgebra conmutativa y M un A -módulo, se define $\text{Der}_k(A, M)$ como las derivaciones k -lineales. Sean $k \rightarrow A$ y $A \rightarrow B$ dos morfismos de anillos conmutativos (con lo cual A es k -álgebra, y B es A -álgebra y k -álgebra) y sea M un B -módulo. Probar que se tiene la restricción $D \mapsto D|_A$ determina una sucesión exacta corta
- $$0 \rightarrow \text{Der}_A(B, M) \rightarrow \text{Der}_k(B, M) \rightarrow \text{Der}_k(A, M)$$
25. Sea E un cuerpo, $D : E \rightarrow E$ una derivación, si F es una subextensión tal que D es F -lineal, entonces $D(F) = 0$. Si $K := \text{Ker}(D)$, entonces K es un subcuerpo y D es K -lineal.
26. Con las notaciones anteriores, si $B/A/k$ son extensiones de cuerpos con B/A algebraica y separable, entonces $\text{Der}_k(B, M) \cong \text{Der}_k(A, M)$.
27. Sea E/K algebraica y separable, y $D : E \rightarrow E$ una derivación. Demuestre que si D es K -lineal, entonces es idénticamente cero.
28. Sea $E/F/K$ tal que F/K es algebraica y separable. Probar que $\text{Der}_k(E, E) = \text{Der}_F(E, E)$.
29. Sea $A = k[x_1, \dots, x_n]$. Entonces $\text{Der}_k(A, A) \cong \bigoplus_{i=1}^n A \partial_i$. Si $E = k(x_1, \dots, x_n)$, entonces $\text{Der}_k(E, E) \cong \bigoplus_{i=1}^n E \partial_i$.
30. Sea k de característica $p > 0$ y $D = \frac{d}{dt} : k(t) \rightarrow k(t)$. Calcular $K = \text{Ker}(D)$. Qué grado tiene $k(t)/K$?