Álgebra III

Práctica 3 – Segundo Cuatrimestre de 2007

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 $f : L/K \to L/K$ es un K-automorfismo.

   vii) Sea L/K una extensión algebraica. Todo K-morfismo de cuerpos $f : L/K \to L/K$ 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) $\prod_{i=1}^{n} \big(X^2 - p_i\big)$, sobre $\mathbb{Q}$, con $p_1, \ldots, p_n \in \mathbb{N}$ 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 $\forall\, n \in \mathbb{N}$, $f : K \to K$ 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 $G\left(L/\mathbb{Z}_2\right)$ 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 subextension 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 $n = \mathrm{gr}(f)$. 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 $\mathrm{Hom}(E/K, C/K)$, donde C es una clausura algebraica de K.

    i) $\mathbb{Q}\left[\sqrt[7]{5}\right]/\mathbb{Q}$
    ii) $\mathbb{Q}\left[\sqrt[7]{5}, \sqrt{5}\right]/\mathbb{Q}\left[\sqrt[7]{5}\right]$
    iii) $\mathbb{Q}\left[\sqrt{2}\,,\sqrt[3]{3}\right]/\,\mathbb{Q}$
    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 $\mathbb{Q}\left[\sqrt[4]{2}\right]/\mathbb{Q}\left[\sqrt{2}\right]$ y $\mathbb{Q}\left[\sqrt{2}\right]/\mathbb{Q}$ son normales, pero $\mathbb{Q}\left[\sqrt[4]{2}\right]/\mathbb{Q}$ no lo es (luego, las extensiones normales no son una clase distinguida). Calcular $G(\mathbb{Q}\left[\sqrt[4]{2}\right]/\mathbb{Q})$.
    ii) Exhibir extensiones normales con subextensiones no normales.

14. Sean E/K y F/K subextensiones normales de una extensión H/K. Probar que $E.\,F/K$ 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 $f = X^{2p} - uv\, X^p + v$ 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 $G\left(K(X)/K\right) \simeq \mathrm{PGL}(2,\mathrm{K})$, donde $\mathrm{PGL}(2,\mathrm{K})$ denota el grupo lineal proyectivo $GL(2,K)/(a.\,Id)$ con $a \neq 0$.

19. Sea E/K una extensión de K y sea $G = G(E/K)$.

    i) 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.

    ii) 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 $t \mapsto t + a$, $a \in t$, 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, $\mathbb{Z}_p(t)^H i = \mathbb{Z}_p(t^p - t)$.

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-algebra conmutativa y M un A-módulo, se define $\mathrm{Der}_k(A, M)$ como las derivaciones k-lineales. Sean $k \to A$ y $A \to B$ dos morfismos de anillos conmutativos (con lo cual A es k-algebra, y B es A-algebra y k-algebra) y sea M un B-módulo. Probar que se tiene la restricción $D \mapsto D|_A$ determina una sucesión exacta corta

$$0 \to \mathrm{Der}_A(B, M) \to \mathrm{Der}_k(B, M) \to \mathrm{Der}_k(A, M)$$

25. Sea E un cuerpo, $D : E \to E$ una derivación, si F es una subextensión tal que D es F lineal, entonces $D(F) = 0$. Si $K := \mathrm{Ker}(D)$, 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 $\mathrm{Der}_k(B, M) \cong \mathrm{Der}_k(A, M)$.

27. Sea E/K algebraica y separable, y $D : E \to E$ una derivación. Demuestre que si D es K-lineal, entonces es identicamente cero.

28. Sea $E/F/K$ tal que F/K es algebraica y separable. Probar que $\mathrm{Der}_k(E, E) = \mathrm{Der}_F(E, E)$.

29. Sea $A = k[x_1, \ldots, x_n]$. Entonces $\mathrm{Der}_k(A, A) \cong \oplus_{i=1}^n A\partial_i$. Si $E = k(x_1, \ldots, x_n)$, entonces $\mathrm{Der}_k(E, E) \cong \oplus_{i=1}^n E\partial_i$.

30. Sea k de característica $p > 0$ y $D = \frac{d}{dt} : k(t) \to k(t)$. Calcular $K = \mathrm{Ker}(D)$. Qué grado tiene $k(t)/K$?