ÁLGEBRA III

Práctica 6 – Segundo Cuatrimestre de 2007

Derivaciones

1. Sea E un cuerpo de característica p, $D : E \to E$ una derivación, y $F = E(\alpha)$ donde $\alpha^p = a$, $a \in E$ y $\alpha \notin E$. Demuestre que D se extiende a una derivación $\widetilde{D} : F \to F$ si y sólo si $D(a) = 0$. En caso que $D(a) = 0$, el valor de $\widetilde{D}(\alpha)$ puede ser elegido de manera arbitraria.

2. Sea k un cuerpo de característica cero. Sea E/k una extensión, y $x_1, \ldots, x_n$ en E. Demuestre que $\{x_1, \ldots, x_n\}$ son algebraicamente independientes si y sólo si existen $D_1, \ldots, D_n$ derivaciones de E en E tales que $D_i(x_j) = \delta_{ij}$.

3. Sea A un anillo, $D : A \to A$ una derivación y $g : A \to A$ un automorfismo (de anillos). Muestre que gDg^{-1} es una derivación. Llamaremos ${}^gD$ a esta derivación.

4. Sea G un subgrupo finito de automorfismos de un anillo A y $D : A \to A$ una derivación. Se define $\widetilde{D} : A^G \to A^G$ por
$$\widetilde{D}(a) = \sum_{g \in G} ({}^gD)(a) = \sum_{g \in G} g(D(g^{-1}(a)))$$
Probar que $\widetilde{D}$ es una derivación, y que es G-invariante. Si D era G-invariante (i.e. ${}^gD = D$ para todo $g \in G$) entonces $\widetilde{D} = |G|.D$.

5. Sea E un cuerpo y G un subgrupo finito de automorfismos. Demuestre que la restricción $D \mapsto D|_{E^G}$ define una aplicación *inyectiva* $\mathrm{Der}(E, E) \to \mathrm{Der}(E^G, E)$. Si D es una derivación invariante, muestre que $D(E^G) \subseteq E^G$. Más aún, muestre que la restricción define un isomorfismo $\mathrm{Der}(E, E)^G \cong \mathrm{Der}(E^G, E^G)$.

6. Sea E/K una extensión con la siguiente propiedad: "Si F es una subextensión y $D : F \to F$ es una derivación que se anula en K, entonces se anula en F".

   a) Demuestre que necesariamente E es algebraica y separable.

   b) Muestre que las extensiones algebraicas separables tiene esta propiedad.

Norma y traza

1. *a*) Calcular la norma y la traza de $\sqrt[3]{2}$ en $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ y en $\mathbb{Q}[\sqrt[3]{2}, \xi_3]/\mathbb{Q}$.

   b) Sea $p \in \mathbb{N}$ primo. Calcular la norma y la traza de ξ_p en $\mathbb{Q}[\xi_p]/\mathbb{Q}$.

   c) Sea d un entero libre de cuadrados y sea $a \in \mathbb{Q}[\sqrt{d}] - \mathbb{Q}$.
   Probar que $f(a, \mathbb{Q}) = X^2 - \mathrm{Tr}(a)\, X + N(a)$.

2. Sea K un cuerpo de característica $p > 0$ y sea X trascendente sobre K. Calcular la norma y la traza de X

   a) en $K(X)/K(X^p)$.

   b) en $K(X)/K(X^p - X - a)$, para a un elemento fijo cualquiera de K.

3. Sea $p \in \mathbb{N}$ primo mayor que 3 y sea $\{u, v\}$ una familia algebraicamente independiente sobre $\mathbb{Z}_p$. Sean $K = \mathbb{Z}_p(u^3, v^2)$ y $E = \mathbb{Z}_p(u, v)$. Calcular la norma y la traza de $u + v$ en E/K.

4. Sea E/K una extensión finita. Probar que:

   a) Si E/K es separable, entonces $\mathrm{Tr} : E \to K$ es suryectiva.
   b) La aplicación $\mathrm{Tr} : E \times E \to K$ definida por $\mathrm{Tr}(a, b) = \mathrm{Tr}(a.b)$ es una forma bilineal simétrica.
   c) Para cada $a \in E$ se define $\mathrm{Tr}_a : E \to K$ como $\mathrm{Tr}_a(b) = \mathrm{Tr}(a.b)$.
      1) Verificar que $\mathrm{Tr}_a \in E^*$ (E dual) para cada $a \in E$.
      2) Probar que si E/K es separable, la aplicación $a \mapsto \mathrm{Tr}_a$ es un isomorfismo entre E y E^*.

5. Sea K un cuerpo de característica $p > 0$ y sea E/K una extensión de grado q, con q un primo distinto de p. Probar que existe $\alpha \in E$ tal que $E = K[\alpha]$ y el coeficiente de grado $q - 1$ de $f(\alpha, K)$ es nulo.

6. a) Calcular núcleo e imagen del morfismo de grupos de $\mathbb{C}^*$ en $\mathbb{R}^*$ inducido por la aplicación $N : \mathbb{C} \to \mathbb{R}$.
   b) Probar que en $\mathbb{Q}[\sqrt{2}\,]/\mathbb{Q}$ la norma no es inyectiva ni suryectiva.

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

8. Sea u trascendente sobre $\mathbb{Z}_7$ y sean $K = \mathbb{Z}_7(u^7 - u)$ y $E = \mathbb{Z}_7(u)$.

   a) Hallar una base del núcleo de la transformación lineal $\mathrm{Tr}_{E/K} : E \to K$.
   b) Encontrar una base de E como K-espacio vectorial formada por elementos de traza 1.

9. Sea E/K una extensión de grado n de K tal que n es coprimo con la caracteristica de k, si ésta fuera p, o cualquier n en característica cero. Sea $x \in E$, probar que si $\mathrm{Tr}(x^i) = 0$ para todo $1 \leq i \leq n$, entonces $x = 0$.

10. Sea $\mathbb{Z}[i] \subset \mathbb{C}$ el subanillo generado por i. Utilizando la norma $N : \mathbb{Z}[i] \to \mathbb{Z}$ muestre que si $z = a + bi \in \mathbb{Z}[i]$ es tal que $N(z)$ es un número primo, entonces z es primo en el anillo $\mathbb{Z}[i]$.

11. Sea $d \in \mathbb{N}$ libre de cuadrados y $A = \mathbb{Z}[\sqrt{-d} \subset \mathbb{Q}[\sqrt{-d}]$. Muestre que si $d > 1$ entonces ± 1 son los únicos elementos de norma 1 (la norma de $\mathbb{Q}[\sqrt{-d}]$), y no hay elementos de norma -1. Muestre que $N(\mathbb{Z}[\sqrt{-d}]) \subseteq \mathbb{Z}$, y que si $z = \mathbb{Z}[\sqrt{-d}]$ es tal que $N(z)$ es un número primo, entonces z es primo en el anillo $\mathbb{Z}[\sqrt{-d}]$.

12. Sea $d \in \mathbb{N}$ libre de cuadrados. Muestre que si en $\mathbb{Z}[\sqrt{d}]$ hay un elemento $z \neq 1$ de norma 1, entonces hay infinitos elementos de norma uno. De cualquier manera, muestre que todos ellos son unidades. Muestre algun ejemplo en donde haya elementos de norma -1 (que tambien son unidades!). Muestre que $N(\mathbb{Z}[\sqrt{d}]) \subseteq \mathbb{Z}$, y que si $z = \mathbb{Z}[\sqrt{d}]$ es tal que $N(z)$ es un número primo, entonces z es primo en el anillo $\mathbb{Z}[\sqrt{d}]$.

13. Sea A un anillo y G un grupo finito de automorfismos de anillo de A. Definiendo $N_G : A \to A$ por $N_G(a) = \prod_{g \in G} g(a)$, muestre que $N_G : A \to A^G$, que $N_G(ab) = N_G(a)N_G(b)$, y que $N_G(a)$ es una unidad en A^G si y sólo si a es una unidad en A.

14. Utilizando el ejercicio anterior, caracterice y encuentre todas las unidades de $\mathbb{Z}[\sqrt[3]{2}, i]$. Nota: puede considerar $\mathbb{Q}[\sqrt[3]{2}, i]/\mathbb{Q}$ o $\mathbb{Q}[\sqrt[3]{2}, i]/\mathbb{Q}[i]$..