ÁLGEBRA III

Práctica 5 – Primer Cuatrimestre de 2004

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

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 $\mathrm{Tr}_a \in E^*$ 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 K un cuerpo de característica p y sea E/K una extensión de grado n tal que n es coprimo con p. Sea $x \in E$. Probar que si $\mathrm{Tr}(x^i) = 0$ para todo $1 \leq i \leq n$, entonces $x = 0$.

1. Derivaciones

1. 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 $g.D$ a esta derivación.

2. 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

$$\widetilde{D}(a) = \sum_{g \in G} (g.D)(a) = \sum_{g \in G} g(D(g^{-1}(a)))$$

   Probar que $\widetilde{D}$ es una derivación, y si D era G-invariante (i.e. $g.D = D$ para todo $g \in G$) entonces $\widetilde{D} = |G|.D$.

3. 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 $\mathrm{Der}(E, E)^G \cong \mathrm{Der}(E^G, E^G)$.

4. 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.

2. Separabilidad

1. Sea K un cuerpo de característica $p > 0$ y sea E/K una extensión algebraica. Sean

$$\begin{aligned} E_s &= \{a \in E : a \text{ es separable sobre } K\}, \\ E_i &= \{a \in E : a^{p^n} \in K \text{ para algún } n \in \mathbb{N}_0\}. \end{aligned}$$

   Probar que:

   a) E_s y E_i son subcuerpos de E.

   b) E es puramente inseparable sobre E_s.

   c) $E_s \cap E_i = K$.

   d) Si E/K es normal, entonces E es separable sobre E_i.

2. Sea K un cuerpo de característica p. Sea C una clausura algebraica de K y sea $G = G(C/K)$. Se define $K^{p^{-\infty}} = \{x \in C : \sigma(x) = x \; \forall \, \sigma \in G\}$.

   a) Probar que:

      1) Si $p = 0$, entonces $K^{p^{-\infty}} = K$.
      2) Si $p > 0$, entonces $K^{p^{-\infty}} = \{x \in C : x^{p^n} \in K \text{ para algún } n \in \mathbb{N}\}$.

   b) Probar que la construcción de $K^{p^{-\infty}}$ no depende de la clausura algebraica elegida.

3. Un cuerpo K de característica p se dice *perfecto* si $K^{p^{-\infty}} = K$.

a) Probar que todo cuerpo de característica 0 es perfecto.

b) Sea K un cuerpo de característica $p > 0$. Probar que K es perfecto si y sólo el morfismo $f : K \to K$ definido por $f(x) = x^p$ es un automorfismo.

c) Deducir que todo cuerpo finito es perfecto.

d) Probar que si K es un cuerpo de característica $p > 0$, entonces $K(X)$ no es perfecto.

e) Probar que si K no es perfecto, entonces $[K^{p^{-\infty}} : K] = \infty$.

4. Sea K un cuerpo de característica p y sea C una clausura algebraica de K. Probar que:

   a) $K^{p^{-\infty}}$ es perfecto.

   b) $C/K^{p^{-\infty}}$ es de Galois.

5. Probar que K es perfecto si y sólo si toda extensión algebraica de K es separable.

6. Sea K un cuerpo y sea E/K una extensión algebraica.

   a) Probar que si K es perfecto, entonces E es perfecto.

   b) Probar que si E es perfecto y E/K es separable, entonces K es perfecto.

   c) Probar que si $[E : K] < \infty$ y E es perfecto, entonces E/K es separable.

3. Cuerpos finitos

1. Sea K un cuerpo. Notemos $(K, +)$ al grupo aditivo de K y $(K^*, \cdot)$ al grupo multiplicativo. Probar que $(K, +)$ y $(K^*, \cdot)$ nunca son isomorfos como grupos. Caracterizar ambos grupos en el caso en que K sea finito.

2. Probar que dos cuerpos finitos de igual cardinal son isomorfos.

3. Sea C una clausura algebraica de $\mathbb{Z}_p$ y sean F_{p^m} y F_{p^n} los cuerpos de p^m y p^n elementos en C. Probar que $F_{p^m} \subset F_{p^n}$ si y sólo si $m \mid n$.

4. Sea K un cuerpo de $q = p^n$ elementos. Mostrar que $K/\mathbb{Z}_p$ es de Galois con grupo de Galois cíclico de orden n con generador $\sigma(x) = x^p$.

5. Sea E una extensión finita de K donde K es un cuerpo finito de $q = p^n$ elementos, supongamos que E tiene q^m elementos. Demuestre que E/K es de Galois con grupo de Galois cíclico generado por $g(x) = x^q$.

6. Sea K un cuerpo finito de q elementos.

   a) Sea $f \in K[X]$ irreducible. Probar que f divide a $X^{q^n} - X$ si y sólo si $\mathrm{gr}(f)$ divide a n.

   b) Probar que $X^{q^n} - X = \prod_{d|n} (\prod f_d)$, donde el producto de adentro recorre todos los polinomios irreducibles mónicos de grado d en $K[X]$.

   c) Deducir que $q^n = \sum_{d|n} d.u(d)$, donde $u(d)$ es la cantidad de polinomios irreducibles mónicos de grado d en $K[X]$.

   d) Dar una fórmula para $u(d)$.

   e) Calcular la cantidad de polinomios de grado 3 y 4 mónicos e irreducibles que hay en un cuerpo de 2^{12} y 3^{12} elementos.