Pontificia Universidad Católica de Chile y Universidad de Chile
Facultad de Matemáticas

Profesor: José Samper
Ayudante: José Cuevas Barrientos
Curso: Álgebra II
Sigla: MPG3201
Fecha: 27 de agosto de 2025

Norma y traza

1. Norma y traza

1. Sea k un cuerpo de característica $p > 0$. Para una extensión finita L/k, definimos su grado de separabilidad e inseparabilidad como $[L : k]_s := [L_{\text{sep}} : k]$ y $[L : k]_i = [L : L_{\text{sep}}]$.
   a) Pruebe que si $L/K/k$ es una torre de extensiones, entonces $[L : k]_s := [L : K]_s\,[K : k]_s$ y $[L : k]_i := [L : K]_i\,[K : k]_i$.
   b) Sea $L_{\text{ins}} := \{\alpha \in L : \alpha \text{ es puramente inseparable sobre } k\}$. Pruebe que $[L_{\text{ins}} : k] \leq [L : k]_i$.
   c) Pruebe que si L es normal, entonces hay igualdad $[L_{\text{ins}} : k] = [L : k]_i$.
2. Sea K/k una extensión finita. Dado $\alpha \in K$, denotamos por $m_\alpha(x) := \alpha \cdot x$ que determina un endomorfismo $m_\alpha \colon K \to K$. Se definen la norma y la traza de α como

$$\mathrm{Nm}_{K/k}(\alpha) := \det(m_\alpha), \qquad \mathrm{Tr}_{K/k}(\alpha) := \mathrm{tr}(m_\alpha).$$

   Pruebe que

$$\mathrm{Nm}_{K/k}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{Tr}_{K/k}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$

   donde $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_k(K, k^{\text{alg}})$. (Note que si K/k es de Galois, entonces $\mathrm{Hom}_k(K, k^{\text{alg}}) = \mathrm{Gal}(K/k)$.)

   Pista: Primero pruébelo para $K = k(\alpha)$, luego pruebe la transitividad de la traza y norma. □
3. Pruebe que una extensión finita K/k es separable syss $(x, y) \mapsto \mathrm{Tr}_{K/k}(xy)$ es una forma bilineal no degenerada (i.e., si $\mathrm{Tr}_{K/k}(\alpha x) = 0$ para todo x, entonces $\alpha = 0$).

2. Extensiones cíclicas

4. Una extensión K/k se dice ***cíclica*** si es finita, de Galois y $\mathrm{Gal}(K/k)$ es cíclico.
   a) Pruebe que toda subextensión de una cíclica es cíclica.

   En adelante, supondremos que K/k es cíclica con generador $\sigma \in \mathrm{Gal}(K/k)$.
   b) Pruebe que $\beta \in K$ tiene norma $\mathrm{Nm}_{K/k}(\beta) = 1$ syss existe $\alpha \in K$ tal que $\beta = \alpha/\sigma(\alpha)$.
   c) Pruebe que si K/k tiene grado n y k posee una raíz n-ésima primitiva de la unidad ζ_n, entonces $K = k(\sqrt[n]{\gamma})$ para algún $\gamma \in k$.
5. Sea K/k una extensión cíclica de grado n y sea $\sigma \in \mathrm{Gal}(K/k)$ un generador.
   a) Pruebe que $\beta \in K$ tiene traza $\mathrm{Tr}_{K/k}(\beta) = 0$ syss existe $\alpha \in K$ tal que $\beta = \alpha - \sigma(\alpha)$.
   b) Pruebe que si $\mathrm{car}\, k =: p > 0$ y $n = p$, entonces $K = k(\alpha)$, donde α es raíz de un polinomio de la forma $\wp(x) - \gamma \in k[x]$ y donde $\wp(x) := x^p - x$ se denomina el *endomorfismo de Artin-Schreier*. Ocasionalmente se escribe «$\alpha = \wp^{-1}(\gamma)$».

A. Comentarios adicionales

Dado un anillo A, se suele denotar por $\mathbb{G}_a(A) = (A, +)$ al «grupo aditivo» del anillo y por $\mathbb{G}_m(A) := (A^\times, \cdot)$ al «grupo multiplicativo» (la notación se debe a que son ejemplos importantes en la teoría de grupos algebraicos). Los ejercicios 4*b* y 5*a* pueden reescribirse como que hay sucesiones exactas:

$$1 \longrightarrow \mathbb{G}_m(k) \longrightarrow \mathbb{G}_m(K) \xrightarrow{\alpha/\sigma(\alpha)} \mathbb{G}_m(K) \xrightarrow{\mathrm{Nm}_{K/k}} \mathbb{G}_m(k)$$
$$1 \longrightarrow \mathbb{G}_a(k) \longrightarrow \mathbb{G}_a(K) \xrightarrow{\alpha-\sigma(\alpha)} \mathbb{G}_a(K) \xrightarrow{\mathrm{Tr}_{K/k}} \mathbb{G}_a(k)$$

Las sucesiones exactas son de grupos abelianos, pero el lector podría preguntarse qué sucede con la acción del grupo de Galois $G := \mathrm{Gal}(K/k)$. Llamemos $g \in G$ al generador y supongamos que M es un grupo abeliano con acción compatible de G (i.e., $h(m+n) = hm + hn$ para $h \in G$ y $m, n \in G$); entonces siempre tenemos el homomorfismo $m \mapsto m - gm$ y el homomorfismo $N\colon m \mapsto \sum_{h\in G} hm$. El lector puede verificar (es una suma telescópica) que $N(m - gm) = 0$ para todo m, de modo que podríamos definir $H^1(G, M) := \ker(N)/\operatorname{Img}(1-g)$ y, ahora, los ejercicios 4*b* y 5*a* dicen que $H^1(G, \mathbb{G}_m(K)) = H^1(G, \mathbb{G}_a(K)) = 0$. Este enunciado se conoce como el *teorema 90 de Hilbert*[1] y esta es la formulación de Noether. Puede leer más al respecto en Weibel **[2],** §§6.3-6.4.

B. Dos pruebas pendientes

Dos demostraciones de la afirmación de la semana pasada:

Demostración: Recordemos que K_{ins}/k es simple pues K/k lo es, luego $K_{\mathrm{ins}} = k(\alpha^{p^{-h}})$ con $\alpha \in k \smallsetminus k^p$. Luego $x^{p^h} - \alpha$ sigue siendo irreducible en $K_{\mathrm{sep}}[x]$, ya que $\alpha^{1/p} \notin K_{\mathrm{sep}}$ pues es inseparable; así que

$$[K_{\mathrm{ins}} : k] = p^h = [K_{\mathrm{sep}}(\alpha^{p^{-h}}) : K_{\mathrm{sep}}] \leq [K : K_{\mathrm{sep}}]. \qquad \square$$

Y otra directa:

Demostración: Sea $\alpha \in K$ un generador y sea $f(x) \in k[x]$ el polinomio minimal de α. Dada una subextensión $L \subseteq K$, sea $g(x) \in L[x]$ el polinomio minimal de α, sean $c_1, \ldots, c_r \in L$ los coeficientes de g, notemos que g es también minimal en $k(c_1, \ldots, c_r)$ y así $[K : L] = \deg g = [K : k(c_1, \ldots, c_r)]$, por lo que $L = k(c_1, \ldots, c_r)$. Así, hay a lo sumo, tantas subextensiones como divisores de f en $K[x]$ y como f tiene grado n, en el mejor de los casos tenemos n factores lineales y, por tanto, hay un máximo de 2^n factores distintos. $\square$

Referencias

1. Lang, S. *Algebra* (Springer-Verlag New York, 2002).
2. Weibel, C. A. *An introduction to homological algebra Cambridge Studies in Advanced Mathematics* **38** (Cambridge University Press, 1994).

Correo electrónico: josecuevasbtos@uc.cl
URL: https://josecuevas.xyz/teach/2025-2-alg/

[1] El nombre se debe a que era 90$^{\text{ésimo}}$ teorema en su libro *Die Theorie der algebraischen Zahlkörper* («teoría de cuerpos de números algebraicos»).