



**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  $m_\alpha : K \rightarrow K$ . Se definen la norma y la traza de  $\alpha$  como

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

Pruebe que

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

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

*PISTA:* Primero pruébelo para  $K = k(\alpha)$ , luego pruebe la transitividad de la traza y norma.  $\square$

3. Pruebe que una extensión finita  $K/k$  es separable si y sólo si  $(x, y) \mapsto \text{Tr}_{K/k}(xy)$  es una forma bilineal no degenerada (i.e., si  $\text{Tr}_{K/k}(\alpha x) = 0$  para todo  $x$ , entonces  $\alpha = 0$ ).

### 2. EXTENSIONES CÍCLICAS

4. Una extensión  $K/k$  se dice **cíclica** si es finita, de Galois y  $\text{Gal}(K/k)$  es cíclico.
  - a) Pruebe que toda subextensión de una cíclica es cíclica.
 En adelante, supondremos que  $K/k$  es cíclica con generador  $\sigma \in \text{Gal}(K/k)$ .
  - b) Pruebe que  $\beta \in K$  tiene norma  $\text{Nm}_{K/k}(\beta) = 1$  si y sólo si 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  $\zeta_n$ , entonces  $K = k(\sqrt[n]{\gamma})$  para algún  $\gamma \in k$ .
5. Sea  $K/k$  una extensión cíclica de grado  $n$  y sea  $\sigma \in \text{Gal}(K/k)$  un generador.
  - a) Pruebe que  $\beta \in K$  tiene traza  $\text{Tr}_{K/k}(\beta) = 0$  si y sólo si existe  $\alpha \in K$  tal que  $\beta = \alpha - \sigma(\alpha)$ .
  - b) Pruebe que si  $\text{car } k =: p > 0$  y  $n = p$ , entonces  $K = k(\alpha)$ , donde  $\alpha$  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 **4b** y **5a** pueden reescribirse como que hay sucesiones exactas:

$$\begin{aligned} 1 &\longrightarrow \mathbb{G}_m(k) \longrightarrow \mathbb{G}_m(K) \xrightarrow{\alpha/\sigma(\alpha)} \mathbb{G}_m(K) \xrightarrow{\text{Nm}_{K/k}} \mathbb{G}_m(k) \\ 1 &\longrightarrow \mathbb{G}_a(k) \longrightarrow \mathbb{G}_a(K) \xrightarrow{\alpha - \sigma(\alpha)} \mathbb{G}_a(K) \xrightarrow{\text{Tr}_{K/k}} \mathbb{G}_a(k) \end{aligned}$$

Las sucesiones exactas son de grupos abelianos, pero el lector podría preguntarse qué sucede con la acción del grupo de Galois  $G := \text{Gal}(K/k)$ . 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  $N: m \mapsto \sum_{h \in G} hm$ . El lector puede verificar (es una suma telescópica) que  $N(m - gm) = 0$  para todo  $m$ , de modo que podríamos definir  $H^1(G, M) := \ker(N)/\text{Im}(1 - g)$  y, ahora, los ejercicios 4b y 5a 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*<sup>1</sup> 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  $K_{\text{ins}}/k$  es simple pues  $K/k$  lo es, luego  $K_{\text{ins}} = k(\alpha^{p^{-h}})$  con  $\alpha \in k \setminus k^p$ . Luego  $x^{p^h} - \alpha$  sigue siendo irreducible en  $K_{\text{sep}}[x]$ , ya que  $\alpha^{1/p} \notin K_{\text{sep}}$  pues es inseparable; así que

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

Y otra directa:

*DEMOSTRACIÓN:* Sea  $\alpha \in K$  un generador y sea  $f(x) \in k[x]$  el polinomio minimal de  $\alpha$ . Dada una subextensión  $L \subseteq K$ , sea  $g(x) \in L[x]$  el polinomio minimal de  $\alpha$ , sean  $c_1, \dots, c_r \in L$  los coeficientes de  $g$ , notemos que  $g$  es también minimal en  $k(c_1, \dots, c_r)$  y así  $[K : L] = \deg g = [K : k(c_1, \dots, c_r)]$ , por lo que  $L = k(c_1, \dots, c_r)$ . 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/>

---

<sup>1</sup>El nombre se debe a que era 90<sup>ésimo</sup> teorema en su libro *Die Theorie der algebraischen Zahlkörper* («teoría de cuerpos de números algebraicos»).