Observación. Pequeño ejercicio

L/K t.i. , $[L:K]=p^t$

$\Rightarrow L^{p^t} \subseteq K$.

[4] $L/L_{t.i.}$ separable

Por demostrar que $L_{t.i.} \supseteq \mathbb{F}_p(g)$

$$f(x) = g(x^{p^r}) \qquad (g' \neq 0)$$

$\mathrm{irr}_{K(g),x}(T) = g(T) - g(x) \qquad (g' \neq 0)$

$\Rightarrow K(x)/K(g)$ separable

Por demostrar que $K(g)/K$ totalmente inseparable.

$K = \mathbb{F}_p(f)$, $f = g(x)^{p^r}$.

Algebras.

Sea A espacio vectorial sobre un cuerpo K con una estructura de anillo (con la misma suma), tal que:

$$\lambda(ab) = (\lambda a)b \qquad \forall \lambda \in K,\ \forall a,b \in A.$$
$$= a(\lambda b).$$

Ley distributiva mixta

$$\lambda(a+b) = \lambda a + \lambda b$$
$$(a+b)c = ac+bc \qquad ;\ a,b,c \in A.$$
$$c(a+b) = ca+cb.$$

Observación. $(a,b) \mapsto ab$ es bilineal.

Si A es un anillo unitario, podemos definir

$$\varphi : K \to A$$

por $\varphi(\lambda) = \lambda 1_A$,

$$\varphi(\lambda+\mu) = (\lambda+\mu)1_A = \lambda 1_A + \mu 1_A = \varphi(\lambda)+\varphi(\mu)$$
$$\varphi(\lambda\mu) = (\lambda\mu)1_A = \lambda(1_A)(\mu 1_A) = (\lambda 1_A)(\mu 1_A) = \varphi(\lambda)\varphi(\mu).$$

Podemos identificar K con su imagen en A.

Ejemplo. $A = \mathcal{M}_n(\mathbb{K})$, $\quad 1_A = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$

$$\lambda 1_A = \begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix}$$

Ejemplo. $A = \mathbb{K}[x]$, $\quad 1_{\mathbb{K}[x]} = 1$

$$\varphi : \mathbb{K} \hookrightarrow \mathbb{K}[x]$$

Ejemplo. L/K extensión, entonces L es una K-álgebra

$$1_L = 1_K, \quad \varphi : K \hookrightarrow L.$$

$$\mathbb{H} = \mathbb{R} \oplus i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R} \qquad ; \quad k = ij$$

$$\| $$

$$\left\langle i,j \;\middle|\; \begin{matrix} i^2 = j^2 = -1 \\ ij = -ji \end{matrix} \right\rangle_{\mathbb{R}}$$

$\mathbb{H}$ álgebra de división. Sea $q \in \mathbb{H}$

$$q = a + bi + cj + dk$$
$$\bar{q} = a - bi - cj - dk$$

$$\overline{q+p} = \bar{q} + \bar{p} \ , \quad \overline{qp} = \bar{p}\bar{q} .$$

$$N(q) = q\bar{q} = a^2 + b^2 + c^2 + d^2$$

$$q \neq 0 \Rightarrow N(q) \neq 0$$

$$q^{-1} = \frac{\bar{q}}{N(q)} \quad , \quad q\left(\frac{\bar{q}}{N(q)}\right) = \frac{N(q)}{N(q)} = 1$$

Si $q \in \mathbb{H}$, $\quad q + \bar{q} = 2a = tr(q)$.

Además, $\quad q^{-1} = \dfrac{N(q)}{q} = \bar{q}$.

También $\quad q + \bar{q} = tr(q)$

$$q^2 + q\bar{q} = q\, tr(q)$$
$$q^2 - q\, tr(q) + N(q) = 0$$

$q \notin \mathbb{R}$, $\quad m_q(x) = x^2 - x\, tr(q) + N(q) \quad$ (polinomio minimal)

$$\mathbb{R}[q] \cong \mathbb{R}[x] / (m_q(x)) .$$

$m_q(x) = (x-b)(x-a)$, $\quad a, b \in \mathbb{R} \Rightarrow (q-b)(q-a) = 0 \quad (\Rightarrow\!\Leftarrow)$

$\therefore$ m_q no tiene raices reales!

$\therefore$ $\mathbb{R}[q] \cong \mathbb{C}$.

$\tilde{\mathbb{H}} \subseteq M_2(\mathbb{C})$

$$\tilde{\mathbb{H}} = \mathbb{R}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \mathbb{R}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + \mathbb{R}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \mathbb{R}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

<u>Observación</u>. $\mathbb{H} \cong \tilde{\mathbb{H}}$.

función única y homomorfismo de anillos

$$\varphi : \mathbb{H} \longrightarrow \tilde{\mathbb{H}}$$
$$1 \longmapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = I_{\tilde{\mathbb{H}}}$$
$$i \longmapsto \begin{pmatrix} i & \\ & -i \end{pmatrix}$$
$$j \longmapsto \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$$
$$k \longmapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$\tilde{\mathbb{H}}$ es una $\mathbb{R}$-álgebra.

$\tilde{\mathbb{H}} \subseteq \tilde{\mathbb{H}}_{\mathbb{C}} \leftarrow \mathbb{C}$-álgebra generada por $\tilde{\mathbb{H}}$.

$$\tilde{\mathbb{H}}_{\mathbb{C}} = \mathbb{C}\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \oplus \mathbb{C}\begin{pmatrix} i & \\ & -i \end{pmatrix} \oplus \mathbb{C}\begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \oplus \mathbb{C}\begin{pmatrix} & i \\ i & \end{pmatrix}$$

$$\dim_{\mathbb{C}} \tilde{\mathbb{H}}_{\mathbb{C}} = 4 \quad , \quad \dim_{\mathbb{R}} \tilde{\mathbb{H}}_{\mathbb{C}} = 8$$

Extensión de una $\mathbb{R}$-álgebra a una $\mathbb{C}$-álgebra

$$\tilde{\mathbb{H}}_{\mathbb{C}} \cong M_2(\mathbb{C})$$

Extensión de escalares.

Producto Tensorial

$\mathbb{K}$ cuerpo, V, W espacios vectoriales sobre $\mathbb{K}$.

$V \otimes W$

$Z =$ ' $\mathbb{K}$- espacio vectorial con base $\{ e_{v,w} / \begin{smallmatrix} v \in V \\ w \in W \end{smallmatrix} \}$

$X =$ ' subespacio generado por todos los elementos de la forma '

$$e_{v_1+v_2, w} - e_{v_1, w} - e_{v_2, w}$$

$$e_{\lambda v, w} - \lambda e_{v,w}$$

$$e_{v, w_1+w_2} - e_{v, w_1} - e_{v, w_2}$$

$$e_{v, \lambda w} - \lambda e_{v,w}$$

Definición. $V \otimes W = Z / X$

$$\begin{matrix} \Psi \\ v \otimes w = \overline{e_{v,w}} \end{matrix}$$

$$(\lambda v) \otimes w = \lambda (v \otimes w)$$

$$\overline{e_{\lambda v, w}} = \lambda \overline{e_{v,w}}$$

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$$

$$v \otimes (\lambda w) = \lambda (v \otimes w)$$

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v_2 \otimes w.$$

· Propiedad universal del producto tensorial

$b: V\times W \longrightarrow Y$ ($\mathbb{K}$-ev)

es una función bilineal (lineal en cada variable)

entonces existe una función lineal única

$$\tilde{b}: V\otimes W \longrightarrow Y$$

$$b(v,w) = \tilde{b}(v\otimes w)$$

$v\otimes w = v'\otimes w'$

-Demostración- $\hat{b}: Z \to Y$, $\hat{b}(e_{v,w}) = b(v,w)$.

Afirmación: $\hat{b}(X) = \{0\}$ **1-1**

$$\hat{b}(e_{\lambda v,w} - \lambda e_{v,w}) = \hat{b}(e_{\lambda v,w}) - \lambda \hat{b}(e_{v,w}) = \underbrace{b(\lambda v,w) - \lambda b(v,w)}_{=0}$$

$$\exists!\ \tilde{b}: Z/X \to Y, \quad \tilde{b}(\overline{e_{v,w}}) = b(v,w)$$

$$\tilde{b}(v\otimes w) = b(v,w)$$

$$\begin{tikzcd} Z \arrow[r, "\hat{b}"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & Y \\ Z/X \arrow[ur, "\exists!\,\tilde{b}"'] & \end{tikzcd}$$

$\hat{b}(X) = 0$

$\hat{b} = \tilde{b}\circ\pi$

Proposición. Si $v_1,\dots,v_n \in V$ son l.i., $w_1,\dots,w_n \in W$,

entonces $\sum_{i=1}^{n} v_i\otimes w_i = 0 \Rightarrow w_i = 0 \quad \forall i$

-Demostración- Supongamos que no es así, $w_1 \neq 0$

$$\exists\, \sigma \in W^* = Hom_K(W, \mathbb{K}) \quad \text{con} \quad \sigma(w_1) \neq 0$$

$$b : V \times W \to V \quad ; \quad b(v,w) = \sigma(w)v$$

Ejercicio. b es bilineal

$$\exists!\ \tilde{b} : V \otimes W \to V \quad ; \quad \tilde{b}(v \otimes w) = \sigma(w)v$$

$$\tilde{b}\left(\sum_{i=1}^{n} v_i \otimes w_i\right) = \sum_{i=1}^{n} \sigma(w_i)v_i$$

$$\therefore \sum_{i=1}^{n} \sigma(w_i)v_i = 0 \qquad \therefore \sigma(w_1) = 0 \quad (\rightarrow\leftarrow)$$

Corolario. Si B es base de V y S es base de W, entonces

$B \bar{\otimes} S = \{b \otimes s / b \in B,\ s \in S\}$ es base de $V \otimes W$

-Demostración- $v \otimes w \in V \otimes W \Rightarrow v \otimes w \in \langle B \bar{\otimes} S \rangle$

$$v = \sum_{i=1}^{n} \lambda_i b_i \quad , \quad w = \sum_{j=1}^{m} \mu_j s_j$$

$$\Rightarrow v \otimes w = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_i \mu_j (b_i \otimes s_j)$$

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij}(b_i \otimes s_j) \text{ , ahora si } \sum_{i=1}^{n} b_i \otimes \underbrace{\left(\sum_{j=1}^{m} \lambda_{ij} s_j\right)}_{=0} = 0$$

$$\Rightarrow \lambda_{ij} = 0$$

Producto tensorial de álgebras en un álgebra

$$\therefore \dim_K (V \otimes W) = (\dim_K V)(\dim_K W)$$

Referencias. Greub - Multilinear Algebra } Producto tensorial
Mclane y Birkoff - Algebra
Jacobson - Basic Algebra } Algebras
Vander Waerden - Moder Algebra
(Números hipercomplejos)

Supongamos $f: V \to W$, $f': V' \to W'$

Podemos definir

$$b: V \times V' \longrightarrow W \otimes W'$$
$$b(v, v') = f(v) \otimes f'(v')$$

bilineal

Tenemos $b(v_1 + v_2, v') = b(v_1, v') + b(v_2, v')$

$\underline{f \otimes f'}$

$$\begin{tikzcd} V \otimes V' \arrow[r, dashed, "\exists! f\otimes f'"] & W \otimes W' \\ V \times V' \arrow[u] \arrow[ur, "b"'] & \end{tikzcd}$$

; $f \otimes f'$ lineal

$f \otimes f'(v \otimes v') = f(v) \otimes f'(v')$

Proposición. $\ker(f \otimes f') = (\ker f) \otimes V' + V \otimes (\ker f')$

(Suponiendo que $\dim V, \dim V' < \infty$)

-Demostración- $v \in \ker f$

$$(f \otimes f')(v \otimes v') = f(v) \otimes f'(v') = 0 \otimes f'(v') = 0$$

$$(\ker f) \otimes V' \subseteq \ker(f \otimes f')$$

Análogo $V \otimes (\ker f') \subseteq \ker(f \otimes f')$

V tiene base $b_1, \dots, b_n$; $n = \dim V$

$b_1, \dots, b_r$ base de $\ker f$

$f(b_{r+1}), \dots, f(b_n)$ base de $f(V)$

$$X = \langle b_{r+1}, \dots, b_n \rangle$$

$$V = X \oplus \ker f \ , \quad f|_X \text{ inyectiva}$$

$$\Rightarrow f|_X : X \xrightarrow{\sim} f(V) = f(X)$$

$$V' = X' \oplus \ker f' \ , \quad \ker f' = \langle b'_1, \dots, b'_s \rangle$$

$$X' = \langle b'_{s+1}, \dots, b'_m \rangle$$

__Observación__. $(f \otimes f')(V \otimes V') = f(V) \otimes f'(V')$

$(f \otimes f')(V \otimes V')$ tiene base $f(b_{r+1}) \otimes f'(b'_{s+1})$, $f(b_{r+1}) \otimes f'(b'_{s+2})$, $\dots$, $f(b_n) \otimes f(b'_m)$.

$V \otimes V'$ tiene base $\{b_i \otimes b'_j\}_{\substack{i \in \{1, \dots, n\} \\ j \in \{1, \dots, m\}}}$

$$\langle \underbrace{b_1 \otimes b'_1, b_1 \otimes b'_2, \dots, b_r \otimes b'_s}_{S_1} \rangle = (\ker f) \otimes (\ker f')$$

$$\langle \underbrace{b_1 \otimes b'_{s+1}, \dots, b_r \otimes b_m}_{S_2} \rangle = (\ker f) \otimes X'$$

$$\langle \underbrace{b_{r+1} \otimes b'_1, \dots, b_n \otimes b'_s}_{S_3} \rangle = X \otimes (\ker f')$$

$$\langle S_1 \cup S_2 \cup S_3 \rangle \subseteq (\ker f) \otimes V' + V \otimes (\ker f') \subseteq \ker(f \otimes f')$$

$$\dim \langle S_1 \cup S_2 \cup S_3 \rangle = |S_1| + |S_2| + |S_3| = rs + r(m-s) + (n-r)s \quad (*)$$

Además,

$$\dim(\ker(f\otimes f')) = \dim(V\otimes V') - \dim(f(V)\otimes f'(V'))$$
$$= nm - (n-r)(m-s) = (**)$$

$$\therefore \quad (*) = (**) \qquad \square$$

<u>Ejemplos de productos tensoriales.</u>

(1) $V = \{f : X \to K\} = K^X$; $|X|, |Y| < \infty$.
$W = \{g : Y \to K\} = K^Y$

$$K^{X\times Y} \cong K^X \otimes K^Y$$

$x \in X$, $e_x : X \to K$, $e_x(a) = \begin{cases} 1, & a = x \\ 0, & a \neq x \end{cases}$

$\{e_x \mid x \in X\}$ base de K^X, $\{e_y \mid y \in Y\}$ base de K^Y.

$$e_x \otimes e_y : X \times Y \longrightarrow K$$
$$(a,b) \longmapsto e_x(a)\, e_y(b) = \begin{cases} 1, & a = x,\ b = y \\ 0, & \text{si no} \end{cases}$$

$$e_x \otimes e_y \sim e_{(x,y)}$$

$(f\otimes g)(a,b) = f(a)g(b)$.

Ejemplo: $K[X] \otimes_K K[Y] \cong K[X,Y]$ | $f(x)\otimes g(x) \sim f(x)g(x)$

$x^n \otimes y^m \sim x^n y^m$ | $x^2 \otimes 1 + 1 \otimes y^2 \sim x^2 + y^2$

(2) V espacio vectorial $\dim < \infty$

$$V^* = \mathrm{Hom}_K(V, K)$$

definimos $\varphi : V^* \times V \longrightarrow \mathrm{Hom}_K(V,V)$

$$\varphi(s,v)(w) = s(w)\,v$$

$v \longmapsto s(w)v$ lineal

$s \longmapsto s(w) \longmapsto s(w)v$ lineal

φ bilineal, $\varphi(s_1+s_2, v) = \varphi(s_1,v) + \varphi(s_2,v)$

defino $\tilde{\varphi} : V^* \otimes V \longrightarrow \mathrm{Hom}_K(V,V)$

$$\tilde{\varphi}(s \otimes v)(w) = s(w)v$$

Los elementos de V son vectores columna

$$w = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \quad v = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

$$s = (b_1, \dots, b_n) \in V^*$$

$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ base de V

$\left.\begin{matrix} (1\,0 \dots 0) \\ (0\,1 \dots 0) \\ (0\,0 \dots 0\,1) \end{matrix}\right\}$ base de V^*

$$s(w) = a_1 b_1 + \dots + a_n b_n$$

Scanned with CamScanner

$$s(w)v = (a_1b_1 + \cdots + a_nb_n)\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

$$= \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}(a_1b_1 + \cdots + a_nb_n)$$

$$= \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}(b_1 \ldots b_n)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

$$\therefore\ v \otimes s = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}(b_1 \ldots b_n)$$

Recordatorio. $V \otimes W \cong W \otimes V$.

Tenemos,
$$v \otimes s = \begin{pmatrix} c_1b_1 & \cdots & c_1b_n \\ \vdots & & \\ c_nb_1 & \cdots & c_nb_n \end{pmatrix}$$ matriz de rango ≤ 1

Como toda matriz es suma de matrices de rango 1, φ es epi, y luego es un isomorfismo.

Si $T: V \to V$,

$$T = \varphi\left(\sum_{i=1}^{r} v_i \otimes s_i\right),$$ entonces $\rho(T) \leq r$

$$\operatorname{Im} T \subseteq \langle v_1, \ldots, v_r \rangle.$$

$\rho(T) = r$ si $T = \varphi\left(\sum_{i=1}^{r} v_i \otimes s_i\right)$ con r minimal.

Algebras.

A, B K-álgebras,

$$A \underset{K}{\otimes} B \quad K\text{-álgebra.}$$

$(a \otimes b)(a' \otimes b') = aa' \otimes bb'$, producto en $A \underset{K}{\otimes} B$

Falta demostrar que este producto está bien definido,

$a \otimes b \in A \underset{K}{\otimes} B$ fijo,

$$b : A \times B \longrightarrow A \underset{K}{\otimes} B \qquad (a', b') \longmapsto aa' \otimes bb'$$, (bilineal)

$\exists \tilde{b}$ lineal, $\tilde{b} : A \underset{K}{\otimes} B \longrightarrow A \underset{K}{\otimes} B$, $\tilde{b}(a' \otimes b') = aa' \otimes bb'$

Si considero $\tau' = \sum_{i=1}^{n} a_i' \otimes b_i' \in A \underset{K}{\otimes} B$,

$$\tilde{b}(\tau') = \sum_{i=1}^{n} aa_i' \otimes bb_i' = (a \otimes b)\tau' \quad \text{(bien definido)}$$

$$b_1 : A \times B \longrightarrow A \underset{K}{\otimes} B$$

$$(a, b) \longmapsto (a \otimes b)\tau' = \sum_{i=1}^{n} aa_i \otimes bb_i \quad \text{(bilineal)}$$

$$\therefore \exists \tilde{b}_1 : A \underset{K}{\otimes} B \longrightarrow A \underset{K}{\otimes} B$$

$$(a, b) \longmapsto (a \otimes b)\tau'$$

$\therefore \tilde{b}_1(\tau) = \tau\tau'$ (lineal en τ, $\forall \tau \in A \underset{K}{\otimes} B$)

Por simetría, la multiplicación es lineal en z' (pues el producto definido al revés es igual en los generadores, y por lo tanto es el mismo)

basta ver la asociatividad en los generadores

$$(a\otimes b)\left((a'\otimes b')(a''\otimes b'')\right) = \left((a\otimes b)(a'\otimes b')\right)(a''\otimes b'')$$

$\square$

$\exists$ isomorfismo $V\otimes W \cong W\otimes V$ natural

$$v\otimes w \mapsto w\otimes v$$
$$v\times w \mapsto w\otimes v$$

Del mismo modo $V\otimes(W\otimes Z) \cong (V\otimes W)\otimes Z$

$$v\otimes(w\otimes z) \mapsto (v\otimes w)\otimes z$$

<u>Observación</u>. En $V\otimes V$, $v, w\in V$: $v\otimes w \neq w\otimes v$.

Si $\lambda\in V\otimes W$, $\lambda = \sum_{i=1}^{r} v_i\otimes w_i$

El rango de λ es el menor valor posible de r. Si $r=\rho(\lambda)$ (rango)

$\{v_1,\dots,v_r\}$ es l.i, $\{w_1,\dots,w_r\}$ l.i.

$$v_r = \alpha_1 v_1 + \dots + \alpha_{r-1} v_{r-1}$$

$$\lambda = \sum_{i=1}^{r-1} v_i\otimes w_i + \sum_{i=1}^{r-1} (\alpha_i v_i)\otimes w_r$$

$$= \sum_{i=1}^{r-1} v_i\otimes(w_i + \alpha_i w_i)$$

Supongamos que ahora $v_1, \dots, v_r$ l.i. , $w_1, \dots, w_r$ l.i.

p.d : $r = \rho(\lambda)$

Basta ver que no hay expresión más corta.

$$\Psi : V^* \longrightarrow W \quad \text{(en principio depende de } v_i, w_i)$$

$$\Psi(s) = \sum_{i=1}^{r} s(v_i) w_i$$

$\operatorname{Im} \Psi \subseteq \langle w_1, \dots, w_r \rangle$

Pd : $w_i \in \operatorname{Im} \Psi$.

$v_1, \dots, v_r$ son l.i , $i \in \{1, \dots, r\}$

$\Rightarrow \exists s_i \in V^*$ con $s_i(v_i) = 1$, $s_i(v_j) = 0 \ \forall i \neq j$.

$$\Psi(s_i) = \sum_{j=1}^{r} s_i(v_j) w_j = w_i$$

$$\therefore w_i \in \operatorname{Im} \Psi$$

$$\therefore r = \dim(\operatorname{Im} \Psi)$$

<u>Afirmación</u>. Ψ depende sólo de λ.

$$V^* \otimes (V \otimes W) \xrightarrow[\tau]{\cong} (V^* \otimes V) \otimes W$$

$$\varphi : V^* \otimes V \to K$$
$$(s \otimes v) \mapsto s(v)$$
$$s \times v \mapsto s(v)$$

$\Psi_\lambda(s) = (\varphi \otimes \mathrm{Id}) \circ \tau(s \otimes \lambda)$, $\lambda \in V \otimes W$.

Como $\lambda \in V \otimes W$, $\lambda = \sum_{i=1}^{r} v_i \otimes w_i$

$$\Psi_\lambda(s) = (\varphi\otimes Id)\left(\tau\left(s\otimes\left(\sum_{i=1}^r v_i\otimes w_i\right)\right)\right)$$
$$= \varphi\otimes Id\left(\tau\left(\sum_{i=1}^r (s\otimes(v_i\otimes w_i))\right)\right)$$
$$= \varphi\otimes Id\left(\sum_{i=1}^r ((s\otimes v_i)\otimes w_i)\right)$$
$$= \sum_{i=1}^r \varphi\otimes Id((s\otimes v_i)\otimes w_i) = \sum_{i=1}^r s(v_i)\otimes w_i$$
$$= \sum_{i=1}^r \underbrace{1\otimes s(v_i)w_i}_{\in K\otimes W} \quad (*)$$

Observación. $K\otimes W \cong W \quad (1\otimes w \mapsto w)$

$$\therefore (*) \sim \sum_{i=1}^r s(v_i)w_i$$

Por lo tanto, $\Psi = \Psi_\lambda$ es independiente de la expresión. $r = \dim(\operatorname{Im}\Psi_\lambda) = \rho(\lambda)$

Supongamos que $V < V'$, $W < W'$, $\lambda \neq 0$ en $V\otimes W$

$$\lambda = \sum_{i=1}^r v_i\otimes w_i \quad , \quad r = \rho(\lambda) > 0$$

$$\therefore \lambda \neq 0 \text{ en } V'\otimes W'$$

$$\therefore V\otimes W < V'\otimes W'$$

Ejemplo. Sobre $\mathbb{Z}$, $M_1 = \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$, $M_2 = \mathbb{Z}/4\mathbb{Z}$, $M_3 = 2\mathbb{Z}/4\mathbb{Z} \subset M_2$

Tenemos $M_3 \cong M_1$

$$\bar{2}\otimes\bar{1} \in M_3\otimes_{\mathbb{Z}} M_1 \cong M_1\otimes_{\mathbb{Z}} M_1 \cong \mathbb{F}_2\otimes_{\mathbb{F}_2}\mathbb{F}_2 \cong \mathbb{F}_2$$

$$M_3 \subseteq M_2$$

En $M_2\otimes M_1$, $\bar{2}\otimes\bar{1} = 2(\bar{1}\otimes\bar{1}) = \bar{1}\otimes\bar{0} = 0$

Ejercicio. Estudiar $\mathbb{Z}/n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/m\mathbb{Z}$.

Para $A \leq V$, $B \leq W$

$$\frac{V \otimes W}{A \otimes W + V \otimes B} \cong V/A \otimes W/B \quad ; \quad \dim V, \dim W < \infty .$$

$$\lambda \in V \otimes W \xrightarrow{\Psi} V/A \otimes W/B$$

$$\lambda = \sum_{i=1}^{n} v_i \otimes w_i \quad , \quad \Psi(\lambda) \neq 0$$

$$\Psi(\lambda) = \sum_{i=1}^{n} \overline{v_i} \otimes \overline{w_i}$$

$V'' = \langle v_1, \ldots, v_n \rangle$, $W'' = \langle w_1, \ldots, w_n \rangle$

Supongamos $\pi : V \longrightarrow V/A$ (proyección canónica),

$$\pi(V'') = V''+A/A \cong V''/A \cap V'' .$$

Del mismo modo, la imagen de W'' en W/B es isomorfa a $W''/B \cap W''$.

Si $\sum_{i=1}^{n} \overline{v_i} \otimes \overline{w_i} = 0$ en $V/A \otimes W/B$, entonces $\sum_{i=1}^{n} \overline{v_i} \otimes \overline{w_i} = 0$ en $\frac{V''+A}{A} \otimes \frac{W''+B}{B}$

$$\frac{V''+A}{A} \otimes \frac{W''+B}{B} \cong \frac{V''}{A \cap V''} \otimes \frac{W''}{B \cap W''}$$

" " $\frac{V''}{A \cap V''} \otimes \frac{W''}{B \cap W''}$

$$\therefore \sum_{i=1}^{n} v_i \otimes w_i \in (A \cap V'') \otimes W'' + V'' \otimes (B \cap W'')$$

$$\subseteq A \otimes W + V \otimes B$$

Extensión de escalares

V espacio vectorial sobre K, L/K extensión

Definimos $V_L := L \otimes_K V$

V_L es espacio vectorial sobre L

$$\lambda \in L, \quad w \in V_L, \quad w = \sum_{i=1}^{r} \lambda_i \otimes v_i$$

$$\lambda w = \sum_{i=1}^{r} \lambda \lambda_i \otimes v_i$$

$(\lambda_1, \lambda_2) \mapsto \lambda_1 \lambda_2$ K-bilineal, entonces

$$\varphi : L \otimes_K L \to L$$

$$\varphi(\lambda_1 \otimes \lambda_2) = \lambda_1 \lambda_2$$

$\lambda w = (\varphi \otimes Id) \circ \tau (\lambda \otimes w)$ bien definido (ejercicio)

Ejemplo (Ejercicio). $\lambda_1(\lambda_2 w) = \lambda_1 \lambda_2 w$, $w = \sum_{i=1}^{r} \mu_i \otimes v_i$

$$\lambda_1 \left(\sum_{i=1}^{r} (\lambda_2 \mu_i) \otimes v_i \right) = \sum_{i=1}^{r} (\lambda_1 \lambda_2 \mu_i) \otimes v_i$$

Proposición. $\dim_L V_L = \dim_K V$

Supongamos que V tiene base $\{v_1, \dots, v_n\}$

$$w \in V_L, \quad w = \sum_{j=1}^{N} (\lambda_j \otimes v_j')$$

$$v_j' = \sum_{i=1}^{n} \alpha_{ji} v_i, \quad w = \sum_{i=1}^{n} \left(\sum_{j=1}^{N} \alpha_{ji} \lambda_j \right) \otimes v_i = \sum_{i=1}^{n} \underbrace{\left(\sum_{j=1}^{N} \alpha_{ji} \lambda_j \right)}_{\in L} (1 \otimes v_i)$$

$\therefore \{1\otimes v_1, \dots, 1\otimes v_n\}$ generan!

$v_1, \dots, v_n$ l.i.

$$\sum_{i=1}^{n} \lambda_i \otimes v_i = 0 \Rightarrow \lambda_1 = \dots = \lambda_n = 0$$

$$\overset{\parallel}{\sum_{i=1}^{r} \lambda_i (1\otimes v_i) = 0}$$

$V = K^n$, $V_L = L^n$.

__Ejemplo__. $L = \mathbb{C}$ como $\mathbb{R}$-álgebra.

$$L_{\mathbb{C}} = \{a + b\tilde{i} \; / a, b \in \mathbb{C}\}$$

$\{1, \tilde{i}\}$ son l.i $(1 \in \mathbb{C}\cdot 1, \tilde{i} \notin \mathbb{C}\cdot 1)$

$i^2 - \tilde{i}^2 = (i - \tilde{i})(i + \tilde{i}) = 0$ ($L_{\mathbb{C}}$ no es dominio)

$\tilde{i} = 1\otimes i$, $\tilde{i}^2 = (1\otimes i)(1\otimes i) = (1\cdot 1)\otimes(i\cdot i) = 1\otimes(-1) = -(1\otimes 1)$

$L = \mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$. __Afirmación__. $L_{\mathbb{C}} \cong \mathbb{C}[x]/(x^2+1)$

__Observación__. L/K extensión de cuerpos, $L \otimes K[x] \cong L[x]$

-Demostración de la afirmación-

$$\mathbb{C}[x]/(x^2+1) \cong \frac{\mathbb{C}\otimes_{\mathbb{R}} \mathbb{R}[x]}{\mathbb{C}\otimes_{\mathbb{R}}(x^2+1) + (0)\otimes \mathbb{R}[x]} \cong \mathbb{C}/(0) \otimes_{\mathbb{R}} \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}\otimes_{\mathbb{R}} L$$

$$L_{\mathbb{C}} \cong \mathbb{C}[x]/(x^2+1) \cong \mathbb{C}[x]/(x+i) \times \mathbb{C}[x]/(x-i) \quad \text{(teorema chino de los restos)}$$
$$\cong \mathbb{C}\times\mathbb{C} .$$

__Proposición__. Si F/K extensión de cuerpos y $L = F$ como K-álgebra,

$$L_{\overline{K}} \cong \underbrace{\overline{K} \times \dots \times \overline{K}}_{[L:K]-\text{veces}} \quad \text{ssi} \quad L/K \text{ separable}$$

$\mathbb{F}$

Contraejemplo. $\mathbb{F}_2(x)/\mathbb{F}_2(x^2)$ (no separable)

$$L = \mathbb{F}_2(x) = \frac{\mathbb{F}_2(x^2)[T]}{(T^2 - x^2)}$$

$$L_{\mathbb{F}_2(x)} = \frac{\mathbb{F}_2(x)[T]}{(T-x)^2} \cong \mathbb{F}_2(x) \oplus \mathbb{F}_2(x)u$$

$$u = \overline{T-x} \quad , u^2 = 0$$

Si $L = \mathbb{C}$ como $\mathbb{R}$-álgebra

en $L_{\mathbb{C}}$ hay idempotentes centrales

$$(x+i) - (x-i) = 2i$$

$$\frac{1}{2i} \cdot (x+i) + \frac{-1}{2i}(x-i) = 1$$

$$\frac{1}{2i}(\tilde{i} - i) = (0,1)$$

$$\frac{1}{2i}(\tilde{i} - i) = (1,0)$$

Scanned with CamScanner

17/10/13

Cuerpos y álgebras

Vimos que $f(X)=0$ es soluble por radicales si y solo si $Gal(L/K)$ es soluble, donde L es el cuerpo de descomposición.

Ejemplo: A_n es simple si $n \geq 5$, A_n y S_n no son solubles. $L = F(X_1, \dots, X_n)$, S_n actúa en L por permutaciones, $\sigma(X_i) = X_{\sigma(i)}$; $\sigma(h(X_1, \dots, X_n)) = h(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.

L^{S_n} = cuerpo de funciones simétricas.

$L^{S_n} = F(\sigma_1, \dots, \sigma_n) =: K$, donde:

$\sigma_1 = X_1 + X_2 + \dots + X_n$

$\sigma_2 = X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n$

$\vdots$

$\sigma_n = X_1X_2 \cdots X_n$.

$Gal(L/K) = S_n$, $X_1, \dots, X_n$ son raíces de

$$\prod_{i=1}^{n}(T - X_i) = T^n + \sum_{i=1}^{n} \sigma_i (-1)^i T^{n-i} = f(T) \overset{(*)}{,} \quad f(T) = 0$$

no es soluble por radicales.

Scanned with CamScanner

Proposición: para cada extensión E/F y $a_1, \ldots, a_n \in E$ existe $\varphi: F[\sigma_1, \ldots, \sigma_n] \to E$ homomorfismo tq $\varphi(\sigma_i) = a_i$.

Dem.: $g(T) = T^n + \sum_{i=1}^{n} a_i (-1)^i T^{n-i} = \prod_{i=1}^{n} (T - b_i)$ en $\overline{E}$.

Existe $\Psi: F[X_1, \ldots, X_n] \to \overline{E}$ con $\Psi(X_i) = b_i$.

$\Psi(f(T)) = \prod_{i=1}^{n} (T - \Psi(X_i)) = g(T)$. Comparando coef. a coef. se tiene $\Psi(\sigma_i) = a_i$.

$h(\sigma_1, \ldots, \sigma_n) = 0$, $h \in F[y_1, \ldots, y_n] \Rightarrow h = 0$.

$E = F(y_1, \ldots, y_n)$, $\varphi(\sigma_i) = y_i$, $\varphi(h(\sigma_1, \ldots, \sigma_n)) = h(y_1, \ldots, y_n)$

Como $h(\sigma_1, \ldots, \sigma_n) = 0$ y φ es homo $\Rightarrow h(y_1, \ldots, y_n) = 0$.

Obs.: obtener una fórmula general "casi" (podría haber un denominador q moleste) para resolver $g(T) = 0$ para todo polinomio g de grado 5 es equivalente a resolver $f(T) = 0$ por radicales en $(*)$.

Proposición: la ecuación general de grado 5 no es soluble por radicales.

Ejemplo: ecuación de grado 3 y supongamos $F = \mathbb{C}$.

$$\begin{array}{ccc} S_3 & \qquad & L \\ | & & | \\ C_3 & & L^{C_3} \\ | & & | \\ \{id\} & & L^{S_3} \end{array} \qquad \begin{array}{l} \left.\begin{array}{c} \\ \\ \end{array}\right\} 3 \\ \left.\begin{array}{c} \\ \\ \end{array}\right\} 2 \end{array}$$

Si $C_3 = \langle (123) \rangle$, $irr_{L^{C_3}, X_1}(T) = (T - X_1)(T - X_2)(T - X_3)$.

$L^{C_3} = L^{S_3}[\alpha]$, α es invariante por permutaciones cíclicas, $\alpha = (X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$, $\therefore \alpha \notin L^{S_3}$.

Si $\tau = (12) \Rightarrow \tau(\alpha) = -\alpha$, $\alpha = \sqrt{\delta}$, $\delta = \alpha^2$,

$\delta = (X_1 - X_2)^2 (X_2 - X_3)^2 (X_3 - X_1)^2$, $L^{C_3} = K(\sqrt{\delta})$.

Corolario: una ecuación cúbica irred. $g(T) = 0$ satisface $[L : K] = 3$ ssi el discriminante es un cuadrado.

Ejemplo: $\mathbb{Q}(\eta)/\mathbb{Q}$, $\eta = e^{\frac{2\pi i}{7}}$, $\mathbb{Q}(\eta + \eta^{-1})/\mathbb{Q}$ cúbica.

$$\theta(\eta + \eta^{-1}) = \{\eta + \eta^{-1}, \eta^2 + \eta^{-2}, \eta^3 + \eta^{-3}\}.$$

$$\alpha = (\eta + \eta^{-1} - \eta^2 - \eta^{-2})(\eta^2 + \eta^{-2} - \eta^3 - \eta^{-3})(\eta^3 + \eta^{-3} - \eta - \eta^{-1})$$

$$= (2(\eta + \eta^{-1}) - (\eta^{-3} + \eta^3) - 2)(\eta^3 + \eta^{-3} - \eta - \eta^{-1})$$

Si $u_i = \eta^i + \eta^{-i}$ se tiene $u_i u_j = u_{i+j} + u_{i-j}$,

$u_j = u_{-j}$, $u_j = u_{j+7}$, $u_j = u_{7-j}$, $u_0 = 2$.

$$(2u_1 - u_3 - 2)(u_3 - u_1) = 2u_1u_3 - 2u_1^2 - u_3^2 + u_3u_1 - 2u_3 + 2u_1$$

$$= 2u_3 + \cancel{2u_2} - \cancel{2u_2} - 4 - u_1 - 2 + u_3 + u_2 - 2u_3 + 2u$$

$$= u_3 + u_2 + u_1 - 6$$

$$= -7$$

$\therefore \alpha = -7 \Rightarrow \delta = (-7)^2$

$g(T) = 0$ tiene raíces $\alpha_1, \alpha_2, \alpha_3$. $L = K(\alpha) \Longleftrightarrow$
$\delta \in K^{*2}$.

$x^3 + Ax^2 + Bx + C = 0$. Cambiamos $y = x + \frac{A}{3}$:

$$y^3 = x^3 + Ax^2 + 3\left(\frac{A}{3}\right)^2 x + \left(\frac{A}{3}\right)^3$$

$\therefore$ queda $y^3 - py - q = 0$

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$, $y = a+b$, $p = 3ab$,

$q = a^3 + b^3$. Luego $ab = \frac{p}{3}$ (si la caract. es $\neq$ de 3),

$a^3 + b^3 = q \Rightarrow a^3b^3 = \frac{p^3}{27}$, $a^3 + b^3 = q$.

$$x^2 - qx + \frac{p^3}{27} = 0 = (x - a^3)(x - b^3)$$

$$x = \frac{q \pm \sqrt{q^2 - 4\cdot\frac{p^3}{27}}}{2} = \frac{q}{2} \pm \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}$$

$$\delta = \frac{q^2}{4} - \frac{p^3}{27}$$

$$y_1 = \sqrt[3]{\frac{q}{2}+\sqrt{\delta}} + \sqrt[3]{\frac{q}{2}-\sqrt{\delta}}$$

$$y_2 = \omega\sqrt[3]{\frac{q}{2}+\sqrt{\delta}} + \omega^2\sqrt[3]{\frac{q}{2}-\sqrt{\delta}}$$

$$y_3 = \omega^2\sqrt[3]{\frac{q}{2}+\sqrt{\delta}} + \omega\sqrt[3]{\frac{q}{2}-\sqrt{\delta}}$$

$g(T)=0$ tiene 3 raíces reales ssi $\delta<0$.

Ejemplo: $g(T)=T^3-a$ tiene raíz $\sqrt[3]{a}$.

$$\begin{array}{l} L = \text{cuerpo de desc. de } g(T) \\ | \\ K(\sqrt{\delta}) = K(\omega) \\ | \\ K \end{array}$$

Nota: la extensión L/K es galoisiana (tiene gr. 3) $\iff \delta = -3t^2$ es un cuadrado (esto ocurre $\iff -3$ es un cuadrado) $\iff$ las raíces cúbicas están en K.

24/10/13

Cuerpo de Luisito

Extensiones trascendentes

$\{x_1, \dots, x_n\}$ genera algebraicamente L/K si $L/K(x_1, \dots, x_n)$ es algebraica. $\{x_1, \dots, x_n\}$ es alg. ind. sobre K si $\varphi : K[X_1, \dots, X_n] \to K[x_1, \dots, x_n]$ es injectiva. Equivalentemente, $\{x_1, \dots, x_n\}$ es alg. ind. si $f(x_1, \dots, x_n) = 0 \Rightarrow f = 0$, $f \in K[X_1, \dots, X_n]$. $\alpha \in L$ es trascendente sobre K ssi $\{\alpha\}$ es alg. ind. sobre K.

Ejemplo: $R = K[[t]] = \{a_0 + a_1 t + a_2 t^2 + \dots \,/\, a_i \in K\}$

$$\left(\sum_{i=0}^{\infty} a_i t^i\right)\left(\sum_{i=0}^{\infty} b_i t^i\right) = \sum_{i=0}^{\infty} (a_i + b_i) t^i.$$

$$\left(\sum_{i=0}^{\infty} a_i t^i\right)\left(\sum_{i=0}^{\infty} b_i t^i\right) = \sum_{n=0}^{\infty} c_n t^n, \quad c_n = \sum_{i+j=n} a_i b_j$$

Sea $f = a_0 + a_1 t + \dots$, si $a_0 \neq 0 \Rightarrow f \in K[[t]]^*$.

$fg = 1 = 1 + 0 \cdot t + 0 \cdot t^2 + \dots$

$a_0 b_0 = 1 \Rightarrow b_0 = \frac{1}{a_0}$

$a_0 b_1 + a_1 b_0 = 0 \Rightarrow b_1 = \frac{1}{a_0}(-a_1 b_0)$

$\vdots$

Scanned with CamScanner

R es anillo local porque tR es el único ideal maximal.

$$\mathrm{Quot}(R) = \left\{ \frac{f}{t^n} \,/\, f \in R,\ n \geq 0 \right\}$$

$$\frac{f}{gt^n} = \frac{fg^{-1}}{t^n}, \quad g = b_0 + b_1 t + \cdots, \quad b_0 \neq 0$$

$$\mathrm{Quot}(R) = \{ a_{-n} t^{-n} + a_{-n+1} t^{-n+1} + \cdots \,/\, a_i \in K \} = K((t))$$

cuerpo de series de Laurent.

$$e^{\lambda t} \in \mathbb{C}((t)),\ \lambda \in \mathbb{C}, \quad e^{\lambda t} = \sum_{i=0}^{\infty} \frac{(\lambda t)^i}{i!}, \quad (e^{\lambda t})^{-1} = e^{-\lambda t}.$$

Lema: si $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$ son distintos, entonces $e^{\lambda_1 t}, \ldots, e^{\lambda_m t}$ son li sobre $\mathbb{C}$.

Dem.: $\sum_{i=1}^{m} \alpha_i e^{\lambda_i t} = 0 \Rightarrow \sum_i \alpha_i \lambda_i^n e^{\lambda_i t} = 0,\ \forall n.$

Evaluando en $t = 0$: $\sum_i \alpha_i \lambda_i^n = 0,\ \forall n.$

$$\det \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{m-1} \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_m & \lambda_m^2 & \cdots & \lambda_m^{m-1} \end{pmatrix} = 0 \quad \text{—}\!\!\times\!\!\text{—}$$

Proposición: si $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ son li sobre ~~$\mathbb{R}$~~ $\mathbb{Q}$ entonces $e^{\lambda_1 t}, \ldots, e^{\lambda_n t}$ son alg. ind. sobre $\mathbb{C}$.

Dem.: sea $f \in \mathbb{C}[x_1, \ldots, x_n]$, $f(e^{\lambda_1 t}, \ldots, e^{\lambda_n t}) = 0$

$$f(x_1, \ldots, x_n) = \sum_{\vec{m} = (m_1, \ldots, m_n)} a_{\vec{m}} x_1^{m_1} \cdots x_n^{m_n}.$$

$$f(e^{\lambda_1 t}, \ldots, e^{\lambda_n t}) = \sum_{\vec{m} = (m_1, \ldots, m_n)} a_{\vec{m}} (e^{\lambda_1 t})^{m_1} \cdots (e^{\lambda_n t})^{m_n}$$

$$= \sum_{\vec{m}} a_{\vec{m}} e^{\left(\sum_{i=1}^{n} m_i \lambda_i\right) t}$$

Afirmación: $\vec{m} \neq \vec{p} \Rightarrow \sum_{i=1}^{n} m_i \lambda_i \neq \sum_{i=1}^{n} p_i \lambda_i$

porque $\sum_{i=1}^{n} (m_i - p_i) \lambda_i \neq 0$ por ser $\lambda_1, \ldots, \lambda_n$ li sobre $\mathbb{Q}$.

$$\therefore \sum a_{\vec{m}} e^{\left(\sum_{i=1}^{n} m_i \lambda_i\right) t} = 0 \Rightarrow a_{\vec{m}} = 0 \quad \square$$

Hecho: si $q_1, \ldots, q_r$ son números algebraicos (ie, están en $\overline{\mathbb{Q}}$) distintos, $e^{q_1}, \ldots, e^{q_r}$ son li sobre $\overline{\mathbb{Q}}$.

Luego si $q_1, \dots, q_r \in \overline{\mathbb{Q}}$ son li sobre $\mathbb{Q}$ entonces $e^{q_1}, \dots, e^{q_r}$ son alg. ind. sobre $\mathbb{Q}$. En particular, si $q \in \overline{\mathbb{Q}} \setminus \{0\}$ entonces e^q es trascendente sobre $\mathbb{Q}$.

(1) e es trascendente (tomando $q = 1$)

(2) π es trascendente. Supongamos que π es algebraico, entonces $i\pi$ es algebraico, $\therefore$ $e^{i\pi}$ es trascendente pero $e^{i\pi} = -1$ $\times$

Proposición: $\{x_1, \dots, x_n\} \subseteq L$ tq $L/K(x_1, \dots, x_n)$ es algebraica entonces $\{x_1, \dots, x_n\}$ contiene una base de trascendencia (conjunto que genera algebraicamente y es alg. ind.).

Dem.: supongamos $\{x_1, \dots, x_r\}$ es subconjunto minimal que genera algebraicamente.

Afirmación: $\{x_1, \dots, x_r\}$ es alg. ind.

$f(x_1, \dots, x_r) = 0$, $f \notin K[X_1, \dots, X_{r-1}]$ (o reordenamos).

$$f(X_1, \ldots, X_r) = \sum_{i=0}^{N} g_i(X_1, \ldots, X_{r-1}) X_r^i .$$

$$F(t) = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{r-1}) t^i \in K(x_1, \ldots, x_{r-1})[t] .$$

$F(x_r) = 0$. Luego $K(x_1, \ldots, x_{r-1}, x_r) / F(x_1, \ldots, x_{r-1})$ es algebraica.

$$\begin{array}{c} L \\ | \text{ alg} \\ K(x_1, \ldots, x_{r-1}, x_r) \\ | \text{ alg} \\ K(x_1, \ldots, x_{r-1}) \end{array} \Bigg\} \text{ algebraica } \cancel{\longrightarrow} \text{ con la minimalidad de } \{x_1, \ldots, x_r\}.$$

Luego todo conjunto generador contiene una base de trascendencia.

Si existe $x_1, \ldots, x_n \in L$ con $L / K(x_1, \ldots, x_n)$ algebraica entonces existe base de trascendencia de L/K finita. En este caso diremos que el grado de trascendencia es finito.

Proposición: sea $\{x_1, \dots, x_n\}$ base de trascendencia de L/K y sea $\{y_1, \dots, y_m\} \subseteq L$ alg. ind. Entonces $m \leq n$.

Dem.: $y_1 \in L$, y_1 es algebraico sobre $K(x_1, \dots, x_n)$, $\exists\, F \in K(x_1, \dots, x_n)[t]$ tq $F(y_1) = 0$.

$$F(t) = \sum_{i=0}^{N} \frac{f_i(x_1, \dots, x_n)}{g_i(x_1, \dots, x_n)}\, t^i .$$

Multiplicando por el denominador común podemos suponer ~~$F \in K[X_1, \dots, X_n, t]$~~, ~~$f(x_1, \dots, x_n)$~~ $\exists\, f \in K[x_1, \dots, x_n, t]$ tal que $f(x_1, \dots, x_n, t) = F(t)\, g(x_1, \dots, x_n)$, $f(x_1, \dots, x_n, y_1) = 0$.

Si ningún x_i aparece en f, y es algebraico sobre K ~~$\times$~~. Podemos suponer que x_1 aparece en f.

$F' \in K(x_2, \dots, x_n, y_1)[t]$, $F'(t) = f(t, x_2, \dots, x_n, y_1)$,
$F'(x_1) = 0 \Rightarrow x_1$ es alg. sobre $K(x_2, \dots, x_n, y_1)$.

$$
\begin{tikzcd}
& L \arrow[d, dash, "alg"] \arrow[ddl, dash, bend right, "alg"'] \arrow[ddr, dash, bend left, "alg"] & \\
& K(x_1,\dots,x_n,y_1) \arrow[dl, dash] \arrow[dr, dash, "\text{alg (se demostró)}"] & \\
K(x_1,\dots,x_n) & & K(x_2,\dots,x_n,y_1)
\end{tikzcd}
$$

$\{y_1, x_2, \dots, x_n\}$ genera algebraica %. Iterando podemos reemplazar alguno de $y_1, x_2, \dots, x_n$ por y_2. Si solo podemos reemplazar y_1, entonces $\{y_1, y_2\}$ es alg. dep. $-\!\!\times\!\!-$, y_2 puede reemplazar algún x_i, digamos x_2, y se continúa de este modo.

Al final, si $m > n$ entonces $L/K(y_1, \dots, y_n)$ es algebraica, y_{n+1} es alg. sobre $K(y_1, \dots, y_n)$, $F(y_1, \dots, y_n, y_{n+1}) = 0$ $-\!\!\times\!\!-$ $\square$

Obs.: $\{x_1, \dots, x_n, x_{n+1}\}$ es alg. dep. si y solo si se cumple una de las siguientes:

(1) $\{x_1, \dots, x_n\}$ es alg. dep.

(2) x_{n+1} es alg. sobre $K(x_1, \dots, x_n)$.

Corolario: si $\{x_1, \ldots, x_n\}$ y $\{y_1, \ldots, y_m\}$ son bases de trascendencia entonces $n = m$.

Definición: el grado de trascendencia de L/K es el nº de elementos de una base de trascendencia.

Corolario: si $\{x_1, \ldots, x_n\}$ genera alg. L/K y $n = \deg tr(L/K)$ entonces $\{x_1, \ldots, x_n\}$ es base de trascendencia.

Corolario: si $\{y_1, \ldots, y_n\}$ son alg. ind. sobre K con $y_1, \ldots, y_n \in L$ y $n = \deg tr(L/K)$, entonces $\{y_1, \ldots, y_n\}$ es base de trascendencia.

Dem.: si $b \in L \Rightarrow \{y_1, \ldots, y_n, b\}$ es alg. dep. luego b es alg. sobre $K(y_1, \ldots, y_n)$, luego $L/K(y_1, \ldots, y_n)$ es algebraico $\square$.

Paradero 7° Gran avenida (San miguel) San Miguel

Soto aguilar 1202 (jumbo, metro, norte, ½ ~ # cuadra, U. autónoma, liceo de hombres)

29/10/13

Cuerpo de Luisito

$F(x_1, \ldots, x_n) / F(\sigma_1, \ldots, \sigma_n)$ algebraica

$\Rightarrow \{\sigma_1, \ldots, \sigma_n\}$ generan algebraicamente.

$\Rightarrow \{\sigma_1, \ldots, \sigma_n\}$ base de trascendencia

$\Rightarrow \{\sigma_1, \ldots, \sigma_n\}$ alg. ind.

$\Rightarrow F[\sigma_1, \ldots, \sigma_n] \cong F[x_1, \ldots, x_n]$ anillo de polinomios.

Extensión entera

Sean $A \subseteq B$ anillos conmutativos. $\beta \in B$ se dice entero sobre A si existe $f(x) \in A[x]$ mónico con $f(\beta) = 0$.

Proposición: sean $A \subseteq B$ anillos conmutativos, $\beta \in B$. Las sig. afirmaciones son equivalentes:

(1) β es entero sobre A.

(2) $A[\beta]$ es finitamente generado como A-módulo.

(3) $\exists M \subseteq B$ A-módulo f.g. con $1 \in M$ tq $\beta M \subseteq M$.

Dem.: (1) $\Rightarrow$ (2): $\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0 = 0$

$$\beta^n = -a_{n-1}\beta^{n-1} - \cdots - a_1\beta - a_0.$$

$\therefore \beta^n \in A\beta^{n-1} + \cdots + A\beta + A\cdot 1$

$$\beta^{n+1} \in A\beta^n + \cdots + A\beta^2 + A\beta \subseteq A\beta^{n-1} + \cdots + A\beta + A\cdot 1$$

$\therefore \beta^N \in A\beta^{n-1} + \cdots + A\beta + A\cdot 1, \ \forall N \geq n.$

$\therefore A[\beta] = A\beta^{n-1} + \cdots + A\beta + A\cdot 1$ //

(2) $\Rightarrow$ (3): $M = A[\beta]$ //

(3) $\Rightarrow$ (1): $M = Am_1 + \cdots + Am_r$, $\beta M \subseteq M$.

$$\beta m_i = a_{i1}m_1 + a_{i2}m_2 + \cdots + a_{ir}m_r.$$

$$\beta \underbrace{\begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}}_{= \vec{m}} = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rr} \end{pmatrix}}_{= \tilde{A}} \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}.$$

$$\beta\vec{m} = \tilde{A}\vec{m} \Rightarrow (\beta I - \tilde{A})\vec{m} = 0$$

$$(\beta I - \tilde{A})^* (\beta I - \tilde{A}) = \det(\beta I - \tilde{A})$$

↳ traspuesta conjugada

$\det(\beta I - \tilde{A})\vec{m} = 0$, $\det(\beta I - \tilde{A}) M = 0$

$$\det(\beta I - \tilde{A}) \cdot 1 = 0$$

← polinomio mónico en β //

Scanned with CamScanner

Proposición: sean $A \subseteq B$ anillos conmutativos, $\beta_1, \ldots, \beta_n \in B$. Las sig. afirmaciones son equivalentes:

(1) $\beta_1, \ldots, \beta_n$ son enteros sobre A.

(2) Todo $\beta \in A[\beta_1, \ldots, \beta_n]$ es entero sobre A.

(3) $A[\beta_1, \ldots, \beta_n]$ es f.g. como A-módulo.

Dem.: $(2) \Rightarrow (1)$ ✓

$(3) \Rightarrow (2)$: sigue del resultado anterior pues $\beta \in A[\beta_1, \ldots, \beta_n] \Rightarrow \beta A[\beta_1, \ldots, \beta_n] \subseteq A[\beta_1, \ldots, \beta_n]$

$(1) \Rightarrow (3)$:

$$\begin{array}{c} A[\beta_1, \beta_2] \\ | \\ A[\beta_1] \\ | \\ A \end{array}$$

$A[\beta_1] = Am_1 + \cdots + Am_r$.

β_2 es entero sobre $A[\beta_1]$.

$A[\beta_1, \beta_2] = A[\beta_1]n_1 + \cdots + A[\beta_1]n_s$.

$= Am_1n_1 + \cdots + Am_rn_1 + \cdots + An_sm_1 + \cdots + An_sm_r$

El mismo argumento funciona con n generadores $\square$

Proposición: sean $A \subseteq B$ anillos conmutativos y sea $B_{ent} = \{\beta \in B / \beta$ es entero sobre $A\}$. Entonces B_{ent} es subanillo de B.

Dem.: si $\beta_1, \beta_2 \in B_{ent} \Rightarrow 0, 1, \beta_1+\beta_2, \beta_1-\beta_2, \beta_1\beta_2 \in A[\beta_1, \beta_2]$ (y usamos (2)).

$K/\mathbb{Q}$ extensión finita, $\mathcal{O}_K = \{\beta \in K / \beta$ entero sobre $\mathbb{Z}\}$
↳ anillo de enteros de K

B entero sobre A si cada $\beta \in B$ es entero sobre A.

Ejercicio: si $A \subseteq B \subseteq C$ con B entero sobre A y $\gamma \in C$ entero sobre B, entonces γ es entero sobre A.

Obs.: sea $\beta \in \mathcal{O}_K$, $f(x) = irr_{\mathbb{Q},\beta}(x)$, $g(x) \in \mathbb{Z}[x]$ con $g(\beta) = 0$.

$f(x) \mid g(x)$ en $\mathbb{Q}[x]$. Si β' es raíz de $f(x) = 0$ entonces $g(\beta') = 0$, luego β' es entero algebraico, $\beta' \in \mathcal{O}_{\overline{\mathbb{Q}}}$.

$$f(x) = \prod_{\beta' \text{ raíz de } f} (x-\beta') \in \mathcal{O}_{\overline{\mathbb{Q}}}[x].$$

$$f(x) \in \mathbb{Q}[x] \cap \mathcal{O}_{\overline{\mathbb{Q}}}[x] = \mathbb{Z}[x]$$

$\therefore f$ tiene coef. enteros.

Ejemplo: $K=\mathbb{Q}(\sqrt{d})$, d libre de cuadrados.

$a+b\sqrt{d}$, $a,b\in\mathbb{Q}$.

$$(X-a-b\sqrt{d})(X-a+b\sqrt{d}) = (X-a)^2-b^2d$$
$$= X^2-2aX+(a^2-b^2d).$$

$a+b\sqrt{d}\in\mathcal{O}_K$ entero alg. ssi $2a$ y a^2-b^2d son enteros.

$t=2a$, $a=\frac{t}{2} \Rightarrow \frac{t^2}{4}-b^2d = s$ entero.

$b^2d=\frac{t^2}{4}-s \Rightarrow (2b)^2d = t^2-4s$

$2b=\frac{p}{q} \Rightarrow \frac{p^2}{q^2}d = t^2-4s$ ← no puede cancelar.

$\therefore 2b\in\mathbb{Z}$, $b=\frac{s}{2}$.

$X^2-2aX+(a^2-b^2d) = X^2-tX+\frac{t^2-s^2d}{4}$

$d=2n$ par, n impar $\Rightarrow t$ par $(a\in\mathbb{Z})$

$\frac{t^2-s^2d}{4} = \frac{4a^2-2s^2n}{4} = \frac{2a^2-s^2n}{2} \Rightarrow s$ par

Veamos el caso d impar

t impar $\Leftrightarrow s$ impar.

s, t impar $\Rightarrow t^2 \equiv 1 \pmod 4$, $s^2 \equiv 1 \pmod 4$

$d \equiv 1 \pmod 4$, $t^2 - s^2 d \equiv 0 \pmod 4$, $d \equiv 3 \pmod 4$.

$t^2 - s^2 d \equiv 1 - 3 \equiv 2 \pmod 4 \Rightarrow a + b\sqrt{d}$ no es entero

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \text{ par o } d \equiv 3 \pmod 4 \\ \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right], & d \equiv 1 \pmod 4. \end{cases}$$

Ejemplo: $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\omega]$.

Definición: A es integralmente cerrado en B si $B_{ent} = A$. A dominio, A se dice normal si es integralmente cerrado en su cuerpo de cocientes.

$\mathcal{O}_K$ normal pero si $\mathbb{Z} \subsetneq \Omega \subseteq \mathcal{O}_K$, $\mathbb{Q} \cdot \Omega = K$.

Ω normal $\Rightarrow \Omega = \mathcal{O}_K$.

Proposición: todo DFU es normal.

$\leftarrow$ irreductible.

Dem.: sea D DFU, $\frac{a}{b} \in Quot(D)$.

$f(X) \in D[X]$ mónico con $f\left(\frac{a}{b}\right) = 0$

$f(X) = X^n + d_{n-1}X^{n-1} + \cdots + d_1 X + d_0$.

$0 = \left(\frac{a}{b}\right)^n + d_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + d_1\left(\frac{a}{b}\right) + d_0$.

$0 = a^n + d_{n-1}a^{n-1}b + \cdots + d_1 a b^{n-1} + d_0 b^n$ (*)

p primo con $p|b$, $(*) \Rightarrow p|a$ $\times$.

Luego $b \in D^*$.

Ejemplo: $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, $K[X_1, \ldots, X_n]$ con K cu

Proposición: sea $f \in K[X_1, \ldots, X_n]$ polinomio simétrico. Entonces existe $h \in K[X_1, \ldots, X_n]$ tq $f(X_1, \ldots, X_n) = h(\sigma_1, \ldots$

Dem.: $f \in K(\sigma_1, \ldots, \sigma_n)$ (teo. de Galois), $R = K[\sigma_1, \ldots, \sigma_n] \cong K[y_1, \ldots, y_n]$, luego es normal. Basta probar que f es entero sobre R.