

Introducción:

Trabajaremos sobre cuerpos relevantes en la teoría de los anillos como \mathbb{N} , K = cuerpo de números, \mathbb{Q}_p , \mathbb{R} , \mathbb{C} , K_p cuerpo local. Luego trabajaremos en anillos de enteros. Es decir: nuestros anillos serán \mathbb{Z}_L , \mathcal{O}_K , \mathbb{M}_p , más gen. \mathcal{O}_p anillo de entero.

Y vincularemos con reticulados.

Forma bilineal:

Sea K cuerpo tal que $\text{car } K \neq 2$. Sea V vectorial de dimensión finita, y sea $B: V \times V \rightarrow K$ tal que $B(v_1 + v_2, w) = B(v_1, w) + B(v_2, w)$, $B(\lambda v, w) = \lambda B(v, w)$, $B(v, w_1 + w_2) = B(v, w_1) + B(v, w_2)$, $B(v, \lambda w) = \lambda B(v, w)$. A B le decimos forma bilineal.

B se dice Simétrica si $B(v, w) = B(w, v)$.

Definición: Una forma cuadrática es una función $\mathbb{V}: V \rightarrow B(V, V)$ para B forma bilineal simétrica.

$$\text{Observación: } ① \mathbb{V}(\lambda v) = B(\lambda v, \lambda v) = \lambda^2 \mathbb{V}(v)$$

$$② \mathbb{V}(v+w) = B(v+w, v+w) = B(v, v) + B(v, w) + B(w, v) + B(w, w) = 2B(v, w) + \mathbb{V}(v) + \mathbb{V}(w)$$

$$\text{ed: } \mathbb{V}(v+w) - \mathbb{V}(v) - \mathbb{V}(w) = B(v, w) \text{ f. b. sim.}$$

Este fórmula recibe el nombre de fórmula de polarización.

o.s.: En la fórmula anterior $B(v, v) = \frac{1}{2} (\mathbb{V}(2v) - 2\mathbb{V}(v)) = \mathbb{V}(v)$, si se satisface ①.

Primera lectura: Miércoles 12 julio 2017.

Prop: La función $v \mapsto \psi(v)$ es f.c.s s.s $\psi(\lambda v) = \lambda^2 \psi(v)$

Y $\forall v, w \in V$ y $\psi(v+w) - \psi(v) - \psi(w) =: \tilde{B}(v, w)$ es una

f. bilineal. (En este caso $\tilde{B} = 2B$)

Supongamos que $\dim_K V < \infty$. Tomemos $\{e_1, \dots, e_n\}$ base de V

ed: $\forall v \in V, \exists (a_i)_{i=1}^n : v = \sum_{i=1}^n a_i e_i$.

Entonces:

$B(v, w) = \sum_{i,j=1}^n a_i b_j B(e_i, e_j)$, si
 $w = \sum_{j=1}^n b_j e_j$. Se asocia a B la matriz:

$$G = [B] = (B(e_i, e_j))_{i,j=1}^n$$

le llamamos la matriz de Gramm de la forma cuadrática.

Si x es un vector lo identificamos con:

$$v \rightsquigarrow \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

$$\beta \rightsquigarrow \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

entonces $B(v, w) = v^t G w$.

obs: $G^t = G$, pues B simétrica

Observación: Si V e.v dim finita, $V \cong K^n$. Sea A matriz
 Simétrica, entonces $B(v, w) = v^t A w$ es una f. bilineal sim.
 En particular $\psi(v) = v^t A v$ es una f. cuadrática.

Observación: Si $c_{ij} = \sum_{k=1}^n x_{ik} e_k$ forman una base, Sea $P = (x_{ik})$ matriz cambio de base en \mathbb{E} :

$$v \rightsquigarrow P \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$$w \rightsquigarrow P \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

Su representación en \mathbb{E} : $B(v, w) = (Pv)^t G Pw = v^t (P^t G P) w$

red: $v^t (P^t G P) w = v^t G w, \forall v, w$. Evaluando en $v = (e_i), w = (e_j)$ se obtiene que $P^t G P = G$.

Observe que: $\det(G) = \det(G) (\text{mod } k^2)$.

Definición: Definimos el discriminante de G (o de la f.c. o de la f.b.s.) por $\text{disc}(B) = \text{disc}(G) / k^{k^2} / \in k^*/k^{k^2} \cup \{0\}$.

Dicho número es un invariante.

Definición: ① B se dice regular o no singular si $\text{disc}(B) \neq 0$.

② $v \in V$ se dice isotrópico si $\mathcal{W}(v) = 0$.

③ El radical de una forma bilineal es:

$$R(B) = \{v \in V : B(v, w) = 0, \forall w \in V\}$$

Ejemplo: ① $G = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ cumple con $\mathcal{W}_1(x, y) = (xy) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = (y, x) \begin{pmatrix} x \\ y \end{pmatrix} = 2xy$.

Sea $\mathcal{Q}(x, y) = 2xy$ polinomio homogéneo en geo. algebraica.

Observe que $\det(G) = -1 \Rightarrow G$ no singular, pero $(0, 1), (1, 0)$

son vectores isotrópicos.

$R(B) \neq \emptyset$ $\forall v \in V / B(v, w) \Rightarrow \forall w \in V \{$

$$B(v, w) = v^T B w$$

$B(e_i, w) \Rightarrow e_i \Rightarrow B \cdot w = 0$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} ae_1 + be_2 \\ ce_1 + de_2 \end{pmatrix}$$

$$(1 \ 0) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = ae_1 + be_2$$

② $G = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ entonces $(01) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = 0$, así
 $(0,1) \in R(G) = R(B)$.

(pueden ser radicales izquierdos o derechos)

Proposición: B singular $\Leftrightarrow R(B) \neq \emptyset$

Demonstración: $R(B) \neq \emptyset \Leftrightarrow \exists v \in B$ tal que $Bv = 0 \vee v \neq 0$
 $\Leftrightarrow 0$ vector propio de G
 $\Leftrightarrow \det G = 0$

Ejemplo) $R(G) = \{v : \forall u \in V \, u \neq 0 \} = \{v \in V \mid Gv = 0\}$.

Ejemplo: Si $G = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ entonces $R(G) = \langle (0,1) \rangle$, pues
solamente dichas vectores anulan G . $(0,1) \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (0,1) \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$

Observación: $R(B) \leq V$ ($v, w \in V$, pues es el espacio propio de 0).

Observación: Si $r \in R(B)$ entonces

$$B(v+r, w) = B(v, w) + B(r, w) = B(v, w).$$

Luego B se factoriza a:

$$\overline{B}: \sqrt{|R(B)|} \times \sqrt{|R(B)|} \rightarrow V$$

forma bilineal simétrica, $(\sqrt{|R(B)|}, \sqrt{|R(B)|}) \mapsto B(v, w)$

no singulares, es: $R(\overline{B}) = \{\bar{0}\}$.

Una forma bilineal induce una forma bilineal no singular.

obien...

$$\bar{B}: V_{R(B)} \times V_{R(B)} \rightarrow K$$

$$\bar{B}(\bar{v}, \bar{w}) = B(v, w)$$

$$\bar{B}(v, w) = B(v, w)$$

$$\begin{array}{c} V \\ R \\ W \\ R \cap W \\ W \\ W \end{array}$$

Observación: $R(B) \subseteq V$. Sea $V = R \oplus W$, es decir W .

Sea $\Psi: W \rightarrow V/R$ isomorfismo. Así

$$\bar{B}(\Psi(w_1), \Psi(w_2)) = B(w_1, w_2)$$

Por ello Ψ es isometría.

[ots. Deben llamarse una \bar{B} -isometría.]

Definición: ① Decimos que v es ortogonal a w si $B(v, w) = 0$.

o anotamos $v \perp w$.

② Decimos que $W \perp U$ si $w \perp u$, $\forall w \in W, \forall u \in U$. pueden compartir vectores isotropios

③ Si $W, U \subseteq V$ con $W \perp U$ y $W \cap U = \{0\}$ entonces $W \oplus U$ se denota por $W \perp U$. puede existir intersección no trivial

$W \perp U \Leftrightarrow W \cap U = \{0\}$ [revisar producto interno]

Observación: Si W, U e. cuadráticos, entonces $W \perp U$ se define por

$$W \oplus U := \begin{pmatrix} Cu & 0 \\ 0 & Cu \end{pmatrix}$$

[const. en Abstracción].

Tomando partes de W y U se obtiene que Esta def. generaliza ③

Definición: Dado V e. vectorial cuadrático (e. c.). no singular

y $W \subseteq V$, decimos $W^\perp = \{v \in V : B(v, w) = 0, \forall w \in W\}$

En particular, escribimos $N^\perp = \langle v \rangle^\perp$

S: B es una f. bilineal cumpliendo:

$$B: V \rightarrow V^*, B(w)(v) = B(v, w).$$

Como $\dim V = \dim V^*$ y $\ker(\bar{B}) = R(B)$: [ejercicio]

se tiene que \bar{B} es isomorfismo $\Leftrightarrow B$ no singular.

Primera lectura: miércoles 12 julio 2017,

Si B no singular:

Sea $\{e_1, \dots, e_n\}$ base de V entonces $\{\tilde{B}(e_1), \dots, \tilde{B}(e_n)\}$ es base de V^\perp . Sea $W \subseteq V$ y supongamos $W = \langle v_1, \dots, v_r \rangle$.
Supongo $v_i \in W^\perp \Leftrightarrow \tilde{B}(e_i)(v) = \dots = \tilde{B}(e_n)(v) = 0$.

ed: $\left\{ \begin{array}{l} \tilde{B}(e_1)(v) = 0 \\ \vdots \\ \tilde{B}(e_n)(v) = 0 \end{array} \right.$

Como $\{\tilde{B}(e_i)\}_{i=1}^n$ son l.i. se tiene que

$$\begin{aligned} \Psi: V &\rightarrow K^r \\ v &\mapsto (\tilde{B}(e_i)(v))_{i=1}^n \end{aligned} \quad \text{es epiyectiva.}$$

Observe que $W^\perp = \text{Ker } \Psi$ en particular $\dim W^\perp = n-r$. Juego $V = W \oplus W^\perp$.

Por otro lado W no singular si $W \cap W^\perp = \{0\}$ así:

Proposición: $W \subseteq V$, W, V no singulares entonces $V = W \oplus W^\perp$.

Proposición: Todo V no singular tiene base ortogonal. (Car K-2)

Demonstración: Sea $V \subsetneq V$. Existe $w \in V$: $B(v, w) \neq 0$.

Si $B(v, w) \neq 0 \Rightarrow B(v, v) \neq 0$ (Algoritmo G.S.)

Si w , $B(v+w, v+w) = 2 B(v, w) \neq 0$.

ed: $\exists z \in V$ con $B(z, z) \neq 0$. Supongo $\{z\}$ no singular.

Supongo $V = \langle z \rangle \perp \mathbb{R}^4$ no singular, pero $V \perp \mathbb{R}^4$.

Se concluye por inducción.

Corolario: V no singular $\Rightarrow V = W + W^\perp$, para cualquier W sub. de V .

Si W no singular $\Rightarrow V = W \oplus W^\perp = W \perp W^\perp$.

Ejemplo: Sea $G = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Entonces

$\mathcal{Q}(1,1) = 2$. Necesitamos condición $(1,1)^\perp$. Observa que
 $(1,0)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 0$

Agr $N = (1,-1)$ es otro paralelo a $(1,1)$. $\mathcal{Q}(1,-1) = -2$.

Por lo tanto:

$$G \sim \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}.$$

Observación: W no singular si no existe $v \in W$ tal que $B(v,w) = 0, \forall w \in W$

Agr $s \in W \cap W^\perp \Rightarrow B(s,w) = 0, \forall w \in W$, por lo que

$\therefore v = 0$. Inversamente si $W \cap W^\perp = \{0\}$ entonces

Si $w \in W$ tal que $B(v,w) = 0, \forall v \in W \Rightarrow w \in W \cap W^\perp \Rightarrow w = 0$

$\therefore W$ no singular.

Observación: Sea $\tilde{B}: V \rightarrow V^*$, $\tilde{B}(w)(v) = B(v,w)$. Entonces

$\text{Ker } \tilde{B} = \{v \in V : B(v,w) = 0, \forall w \in V\} = R(B)$.

Ejemplo: Sea $A = \langle i,j : i^2 = \alpha, j^2 = \beta, ij = -ji \rangle$, d. $\beta \in K^*$.

Sea $B(p,q) = \frac{1}{2}(\bar{p}f + f\bar{p})$, para car. $K \neq \mathbb{R}$.

Se sabe que $\dim A = 4$; se lección $\{1, i, j, ij\}$ base de A sobre K .
 En dicha base:

$$B(1, \alpha_i) = \frac{1}{2} (\alpha_i + \bar{\alpha}_i) = 0, \quad \alpha_i \in \{i, j, i+j\}.$$

$$B(i, j) = \frac{1}{2} (ij + ji) = 0$$

$$B(i, ij) = \frac{1}{2} (ij + ij) = \frac{1}{2} (ij + ji\alpha) = 0$$

$$B(j, ij) = \frac{1}{2} (ji + i\beta) = 0$$

Entonces $G = [B] = \begin{pmatrix} 1 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & -\alpha\beta \end{pmatrix}$. Así B es no

Singular simple Si $Gv = G \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} = 0 \Rightarrow (v_1, \alpha v_2, \beta v_3 - \alpha\beta v_4) = 0$

Como $\alpha, \beta \in \mathbb{K}^*$: $v = 0$.

Definición: (H, f) , $H = \langle x, y \rangle$ con $f(x) = f(y) = 0$ y $b(x, y) = 1$.

A este espacio cuadrático se le llama Plano hiperbólico.

Observe que: $G_H = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

Si (V, f) es un espacio cuadrático, $v \in V$ es un vector isotrópico, es decir: $f(v) = 0$ entonces existe un plano hiperbólico $H \subseteq V$ con $v \in H$.

Democión: $\exists w \in V$ con $b(vw) \neq 0$, pues (V, f) no singular.

Asumimos $b(v, w) = 1$, tomando $\hat{w} = w/b(v, w)$.

Observe que:

$$f(w + \alpha v) = f(w) + 2\alpha b(v, w), \quad \text{sea } w' = w + \alpha v$$

Si $\alpha = -\frac{f(w)}{2b(v, w)}$ entonces $f(w') = 0$.

$$b(v, w') = b(v, w) - \frac{f(w)}{2b(v, w)} = 1 - \frac{1}{2} = \frac{1}{2}$$

Observación: $\det(G_H) = -1$ ed: H no singular.

Corolario: Si V tiene vector isotrópico, entonces. (V no singular)
 $V \cong H \oplus V'$, algún V' subespacio de V .

Corolario: Si V es cuadrático no singular, entonces.

$V \cong H \oplus \dots \oplus V'$, algún V' sea anisotrópico.

Dem: Si $V = W \oplus W'$, V no singular $\Rightarrow G_W = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$
 $\Rightarrow \det G_W = \det A \det B + 0 \Leftrightarrow \det A, \det B \neq 0$
 $\therefore W, W'$ no singulares y aplicamos inducción sobre la dimensión.

Definición: ① Sean (V, f) , (V', g') espacios cuadráticos. Una transformación lineal $\Psi: V \rightarrow V'$ es una isometría si es un isomorfismo y $f'(\Psi(v)) = g'(v)$, $\forall v \in V$.

Ejercicio: Es equivalente a Ψ ser lineal $\Leftrightarrow b'(f(u), f(w)) = b(u, w)$.

② V, V' se dicen isométricos si hay una isometría entre ellos.

Proposición: (Teorema de Cancelación de Witt)

(V, f) espacio cuadrático no singular. Si $W, U \subseteq V$ isométricos,

entonces w^\perp y U^\perp son isomorfos. ed:

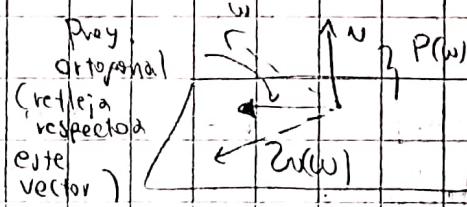
$$w^\perp \cap U^\perp \sim U^\perp \cap U^\perp \quad , \quad U \cap W \Rightarrow w^\perp \sim U^\perp.$$

Ejemplo: Sea $V \in V$ con $f(v) \neq 0$. Sea $\varphi_v: V \rightarrow V$ definida por:
 $\varphi_v(w) = w - \frac{2b(v, w)}{f(v)}v$, a φ_v le llamamos
reflexión asociada a v .

Observe que:

$$b\left(w - \frac{2b(v, w)}{f(v)}v, v\right) = 0.$$

Ds: $f(\varphi_v(w)) = f(w)$



Demotración: $f(\varphi_v(w)) = f\left(w - \frac{2b(v, w)}{f(v)}v\right)$

$$\begin{aligned} &= f(w) - \frac{4b(v, w)}{f(v)} b(v, w) - \left(\frac{2b(v, w)}{f(v)}\right)^2 f(v) \\ &= f(w). \end{aligned}$$

Por ello φ_v son isometrias de V . [ejercicio: φ_v isomorfismo lineal]

Proposición V e.c.n.s. Sean $v, v' \in V$ con $f(v) = f(v') \neq 0$ entonces existe $\varphi: V \rightarrow V$ isometria con $\varphi(v) = v'$.

Demotración:

$$\textcircled{1} \quad \text{Si } f(v-v') \neq 0. \quad \text{Sea } \varphi_v(v-v') = v - \frac{2b(v, v'-v)}{f(v-v')} (v-v')$$

$$\text{Así } Z_{v-v'}(v) = v - 2 \frac{f(v) - b(v-v')}{f(v) - 2b(v-v') + f(v')} (v-v') = v'.$$

(caso 2): $f(v+v') \neq 0$, entonces $Z_{v+v'}(v) = -v'$

Observemos $Z_{v'}(-v') = -v' - 2 \frac{f(-v', v)}{f(v')} v = v'$. Así ...
 $Z_{v'} \circ Z_{v+v'}(v) = v'$

(caso 3): Si $f(v+v') = f(v-v') = 0$.

Entonces $0 = f(v+v') + f(v-v') = 2(f(v) + f(v)) = 4f(v) \neq 0$.

Notación: Si $\dim_k V = 1$, $V = \langle v \rangle$ ($f(v) \neq 0$ escribimos
 $V = [2]$). Así $H \cong [2] \perp [-2]$.

Observación: Por lo visto, V e.i.n.s. $\Rightarrow V = [2] \perp \dots \perp [2^n]$.

1º): Teorema de Witt:

Observación: Si $V + V' \cong U + U'$ y $V \cong U \cong [2] \perp \dots \perp [2^n]$
 entonces Cancelando,

$$\Rightarrow [2] \perp \dots \perp [2^n] \perp V' \cong [2] \perp \dots \perp [2^n] \perp U'$$

implica $V' \cong U'$. Por ello basta probar el teo. de Witt para
 S.e.v de dimensión 1.

$V = W \perp W^\perp = U \perp U^\perp$. Si $W = \langle v \rangle$, $U = \langle v' \rangle$ con
 $W \cong U \cong [2]$, donde $f(v) = f(v')$, $v' = \text{Imagen de } v$
 de W en U . Por Prop. previa, existe $Z: V \rightarrow V$ isomorfía

$$\begin{aligned} Z(v) = v' \Rightarrow Z(w) = w \\ \Rightarrow Z(w^+) = w^+ \quad (\text{ejercicio}) \end{aligned}$$

$\therefore Z|_{W^+} : W^+ \rightarrow U^+$ isomorfismo, pues es isometria (biy. f. resp. producto de espacios con igual dimensión).

Corolario: Si:

$$\underbrace{H \perp \dots \perp H}_{r} \perp V_1 \cong \underbrace{H \perp \dots \perp H}_{s} \perp V_2$$

V_1, V_2 esp. anisotropicos extremos $r=s$ y $V_1 \cong V_2$. en: "P.9
Parte anisotropica está bien dada".

Dom: Cancelamos cada H y así $V_1 \cong \underbrace{H \perp \dots \perp H}_{s-r} \perp V_2$. Si $s-r > 0$
luego V_1 es isotropico (pues es $s-r$ isométrico a un esp.
conectores isotropicos), así $r=s$ y $V_1 \cong V_2$.

Observación: Si (V, f) e. c. n. s, definimos (IV, f) por
 $V = V_a$ y $f_a(v) = \alpha f(v)$, $\alpha \in F^*$.

$$\textcircled{1} \quad V \cong V' \iff V_a \cong V'_a$$

Observación: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cong \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}$
 $\langle v, w \rangle \equiv \langle v, 2w \rangle$, luego:

$$[2] \perp [-2] \equiv [2] \perp [-2] \cong [6] \perp [-6], \text{ si } \text{Car } F \neq 2.$$

Además $[a] \cong [a^*a]$, llevando $n \rightarrow d_n$

Ejemplo: Si $K = \mathbb{R}$ entonces

$$V \cong \underbrace{[1]}_{(r,s)} \perp \dots \perp \underbrace{[1]}_{(r,s)} \perp \underbrace{[1]}_{(r,s)} \perp \dots \perp \underbrace{[1]}_{(r,s)}$$

espacio de signaturas (r,s) .

(r,s) y $(0,s)$ son las signaturas de los espacios anisotrópicos.

Ejemplo: $V = \underbrace{[1]}_n \perp \dots \perp \underbrace{[1]}_r \perp \underbrace{[1]}_s \perp \underbrace{[1]}_{d-n}$. Sea $\{e_i\}_{i=1}^n$ base del espacio V

para la de composición. Entonces $e_i + e_i^*$ son isotrópicos ($H_i = \{e_i\}$, $i = 1, \dots, n$).

Por ello los espacios hiperbólicos no son únicos, pues podemos sacar un solo esp. hiperbólico. (luego me fijé en el más usual en el Subespacio Complementario, que es anisotrópico)

Sea $N \in \mathbb{N}, n, s$ y sean $v, v' \in V$, $\varphi(v) = \varphi(v') = 0$

$H, H' \subseteq V$ planos hiperbólicos, entonces

$$V = H + H^\perp = H' + H'^\perp$$

$\forall v \in V \rightarrow v = v' + v''$ (por componente), $\varphi(v) = \varphi(v')$.

Sea $\varphi(v) \in H$:

Sea $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, con $\varphi: H \rightarrow H$ tal que $\varphi(v) = \varphi(v')$

AH: como P sólo cambia la base:

$$P \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} P^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

así $\det P = \pm 1$. Supongo si $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $P^{-1} = \begin{cases} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \det P = 1 \\ \begin{pmatrix} -d & b \\ c & a \end{pmatrix}, \det P = -1 \end{cases}$

$$\text{Así } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} P^{-1} = P^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

$$\textcircled{1} \quad \text{Si } \det P = 1 \Rightarrow \begin{pmatrix} b & d \\ a & c \end{pmatrix} = \begin{pmatrix} -b & a \\ a & -c \end{pmatrix} \\ \Rightarrow b=c=0, ad=1 \quad \Rightarrow P = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, a \neq 0.$$

$$\textcircled{2} \quad \text{Si } \det P = -1 \Rightarrow \begin{pmatrix} b & d \\ a & c \end{pmatrix} = \begin{pmatrix} -b & -d \\ -a & c \end{pmatrix} \Rightarrow a=d=0, bc=1 \\ \text{Por ello: } P = \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}, b \neq 0.$$

Sea $\Psi_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, $\Psi_b = \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}$. Siendo los vectores isotópicos e_1, e_2 están en la misma órbita, pues $\Psi_a(e_1) = a e_1$, $\Psi_b(e_2) = b' e_1$.

Ejercicio: Todo isometría $\Psi: V \rightarrow V$ es el producto de $n = \dim V$ reflexiones a lo más.

Hint: $v, \Psi(v)$ de igual largo o encontrar reflexión que lleve uno al otro y red. dimensión.

Proposición: Sea (V, f) espacio cuadrático y $r \in K^*$ entonces existe $v \in V$ con $f(v) = r$ si y sólo si $\sqrt{|r|}$ es isotópico.

Ejercicio 1: ℓ isométrica ssi ℓ es lineal tal que $b'(\ell(v), \ell(w)) = b(v, w)$.

Demarcación: ℓ isométrica \Rightarrow ℓ es lineal y s: car $F \neq 2$:

$$\begin{aligned} b'(\ell(v), \ell(w)) &= \frac{1}{2} (\ell'(f(v+w)) - f(v) - f(w)) \\ &= \frac{1}{2} (f(v+w) - f(v) - f(w)) \\ &= b(v, w). \end{aligned}$$

Recíprocamente tenemos que ℓ es lineal $b'(\ell(v), \ell(w)) = b(v, w)$
es: $f'(\ell(v)) = f(v)$.

Ejercicio 2: $2v$ = reflexión asociada a v . Pruebe que $2v$ es isomorfismo lineal.

Demarcación: Si $2v(w) = w - \frac{2b(v, w)}{f(v)} v = 0$

entonces $w = \frac{2b(v, w)}{f(v)} v = \lambda v$, pero $2v(\lambda v) = \lambda v - 2\lambda v = -\lambda v$
Asi $2v(w) = 0 \Rightarrow \lambda = 0 \quad \therefore v = 0 \quad \therefore 2v$ inyectiva, $2v: V \rightarrow V$
así $2v$ es lineal $\therefore 2v$ isométrica.

Ejercicio 3: Sea $\mathcal{Z}: V \rightarrow V'$ isométrica. Con $\mathcal{Z}(W) = U$ entonces
 $\mathcal{Z}(W^\perp) = U^\perp$

Demarcación: Obsérvese que si $u \in U^\perp$ entonces

$$0 = b(u, u') \quad \forall u' \in U$$

entonces si $u = \mathcal{Z}(v)$, cierto $v \in V$ (por \mathcal{Z} es monomorfismo)

se tiene que $0 = b(u, u') = b(\mathcal{Z}(v), \mathcal{Z}(v')) \quad \forall \mathcal{Z}(v) = u' \in U$
 $\therefore \mathcal{Z}(v) \in U^\perp$

Obsérvese que $b(v, w) = b'(\mathcal{Z}(v), \mathcal{Z}(w)) = 0, \forall w \in W$
 $\therefore \mathcal{Z}(W^\perp) \supseteq U^\perp$

Por otro lado Si tomamos $\mathcal{Z}(w')$, $w' \in W^\perp$
entonces para $v \in V$: $b'(\mathcal{Z}(w'), v) = b'(\mathcal{Z}(w'), \mathcal{Z}(v))$, sierto que V^\perp
 $= b(w', v)$, como $\mathcal{Z}^\perp(V) = W$

Se tiene que $v \in W$, así $b'(\mathcal{Z}(w'), v) = b(w', v) = 0$, por lo tanto
 $\mathcal{Z}(w') \in V^\perp$. Así: $\mathcal{Z}(W^\perp) = V^\perp$.

\mathbb{H} plano hiperbólico, $\mathbb{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Proposición:

Sea $(V, \langle \cdot, \cdot \rangle)$ espacio cuadrático con una matriz de Gramm G , con $\dim V = 2$

$$\det G = \dim V = -1$$

entonces $V \cong \mathbb{H}$.

Demotración: $V \cong [a] \perp [b]$ en este caso $\det G = ab$.

$$S. ab \in (-1)K^{\times} \text{ entonces } b = -at^2$$

Luego como $[-at^2] \cong [-a]$. Luego

$$V \cong [a] \perp [-a]$$

Si $s, t \in K$ tales que $f(s) = a, f(t) = -a$

Luego $f(s+t) = f(s) + f(t) = 0, f(s-t) = f(s) + f(-t) = 0$.

$$\text{y } B(s+t, s-t) = f(s) - f(t) = 2a.$$

En la base $\{s+t, s-t\}$ (car $F \neq 2$), la matriz de Gram es:

$$\begin{pmatrix} 0 & -2a \\ -2a & 0 \end{pmatrix} \cong G$$

Luego en la base $\{s+t, \frac{s-t}{-2a}\}$ la matriz de Gram es:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cong G$$

Observación: Si $r \neq 0$ y \mathbb{H} tiene base u, v : $f(u) = f(v) = 0$ $b(u, v) = r$ en la base $\{ru, rv\}$ la matriz de Gram es $\begin{pmatrix} 0 & r \\ r & 0 \end{pmatrix}$.

Definición: Diremos que una f. cuadrática f en un e. vectorial V representa a $a \in K$ si $\exists v \in V$ tal que $f(v) = a$.

f se dice universal si rep. cada elemento de K .

Corolario: El plano hiperbólico es universal. ((ark + 2))

Demotstración: Basta tomar $u+rv$, u, rv como en la observación previa.

En general $V = \underbrace{|H| \perp \dots \perp |H|}_{S} + U$, U anisotrópico. Se dice el plano de isotropía de V .

Proposición: Si es la dimensión del mayor subespacio totalmente isotrópico en V , $W \subseteq V$ se dice k -isotrópico.
Si $f(w) = 0$, $w \in V$. (V no singular).

Demotstración: Si $\exists V = |H| \perp \dots \perp |H| + U$ corresponde a una base $(s_1, t_1), \dots, (s_r, t_r), u_1, \dots, u_m$, $f(s_i) = 0 = f(t_i)$, $b(s_i, t_i) = 1$ entonces $W = Ks_1 \oplus \dots \oplus Ks_r$.

Inversamente, si W isotrópico totalmente

$$W = K\tilde{s}_1 \oplus \dots \oplus K\tilde{s}_r$$

Luego $\exists t_i \in V$ tal que $b(t_i, \tilde{s}_i) = 1$. Sea $U \subseteq W$

$$U = \{w \in W \mid b(s_i, t_i) = 0\}$$

Como b no nula en $W \Rightarrow \dim U = r-1$.

Sea $\tilde{s}_1, \dots, \tilde{s}_{r-1}$ base de U y $\tilde{s}_r = \tilde{s}_1$. Sea $H_1 = Ks_1 \oplus Kt_1$ plano hiperbólico. (pues $G|_{H_1} = \begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix}$ como $\det G \sim 1$)

$\Rightarrow H_1$ plano hiperbólico).

Luego $V = H_1 \perp H_1^\perp$.

$$H_1^\perp = \underbrace{|H| \perp \dots \perp |H|}_{l-1} + U$$

$W_1 = Ks_2 \oplus \dots \oplus Ks_r \subseteq H^{\perp}$. Por hipótesis de Inducción

$$r-1 = \dim W_1 \leq \dim(H) = l-1 \Rightarrow r \leq l.$$

Falta el caso $l=0$.

$$V = 0 \text{ nulo trivio} \Rightarrow \dim V = \{0\}.$$

Supongamos que
entonces:

$$V \cong [a_1] \perp \dots \perp [a_n], \quad V' \cong [-a_1] \perp \dots \perp [-a_n].$$

$$V \perp V' \cong \underbrace{H \perp \dots \perp H}_{n \text{ veces}} \quad (\text{Hacen})$$

Los espacios cuadráticos, modulos planos hiperbólicos; define un grupo.
A este grupo se le llama grupo de Witt de K .

$$W(K) = \langle [a] \mid a \in K^* \rangle.$$

Ejemplo: Si $K = \mathbb{K} \Rightarrow [a] = [-a]$. Por ello $2[2] = 0$
genera $W(K)$. $W(K) \cong \mathbb{C}^*$

Ejemplo: En \mathbb{R} : $V \cong [1] \perp \dots \perp [1] \perp [-1] \perp \dots \perp [-1]$

$$\text{Ns. } W(K) = n[1] + m[-1] = (n-m)[+1]$$

siguiente $W(K) \cong \mathbb{Z}$.

Ejemplo: $K = \mathbb{F}_p$, p impar. $a^2 = b^2 \Rightarrow a = -b, a = b$.

Porello:

$$|K^*/K^{*2}| = 2$$

Siguiente: $W(K) = \langle [1], [\Delta] \rangle$ si Δ no cuadrado en \mathbb{F}_p

donde $-[1] = \bar{E}$ = $\begin{cases} [\Delta], & \text{s. } -1 \notin K^{*2} \\ [1], & \text{s. } -1 \in K^{*2} \end{cases}$

caso 1: $-1 \in K^{*2}$ ($f = \frac{1}{2}$ es pán)

En este caso $\langle I \rangle + \langle I \rangle = 0$, $\langle \Delta \rangle + \langle \Delta \rangle = 0$, $\langle I \rangle + \langle \Delta \rangle \neq 0$.
Por ello $w(K) = C_2 \times C_2$.

Caso 2: $-1 \notin K^{*2}$

$\langle I \rangle + \langle \Delta \rangle = 0$, pero $\langle I \rangle + \langle I \rangle \neq 0$, pero $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ anisotrópico.

Pero $x^2 + y^2 = \Delta t^2$ tiene solución, así (x, y) representa Δt^2 , no I .

Cuadrado rep. Δ .

$$\langle I \rangle + \langle I \rangle \approx \langle \Delta \rangle + \langle \Delta \rangle$$

Ay $\langle I \rangle + \langle I \rangle + \langle I \rangle = \langle \Delta \rangle + \langle \Delta \rangle + \langle I \rangle = \langle \Delta \rangle$, así: $\langle I \rangle \wedge \langle I \rangle \wedge \langle I \rangle \approx \langle \Delta \rangle \wedge \langle \Delta \rangle$

Por ello $\langle I \rangle + \langle I \rangle + \langle I \rangle + \langle I \rangle = 0$. Así $w(K) = C_4$.

En el primer caso los espacios anisotrópicos son $\{0\}, \langle I \rangle, \langle \Delta \rangle, \langle I \rangle \wedge \langle \Delta \rangle$.

En el segundo caso son $\{0\}, \langle I \rangle, \langle \Delta \rangle, \langle I \rangle \wedge \langle \Delta \rangle$.

En los dos casos hay un único espacio anisotrópico de dimensión 1.
mayor al. (De discriminante). Son $1, \Delta = \det C$)

Proposición: Sea (V, f) e cuadrático, $d \in K^*$ entonces
 V representado $\Leftrightarrow V \perp \langle -d \rangle$ si y sólo si isotrópico. (V no singular).

Demostración: Si V no representado, $\exists v \in V$ con $f(v) = -d$

Luego $(v, 1) \in V \perp \langle -d \rangle$ con $\tilde{f}(v, r) = f(v) - dr^2$

Por lo tanto $\tilde{f}(v, 1) = 0$.

Supongamos que $N \perp \langle -\delta \rangle$ isotrópico luego $\exists v \in N$, re^k
 tal que: $f(v) - \delta r^2 = 0$

Caso 1: $r \neq 0$, en este caso $f(\frac{v}{r}) = \delta$.

Caso 2: $r = 0$, entonces $f(v) = 0, v \neq 0$
 $\therefore v$ isotrópico.

ts decin $V \cong H \sqcup U$ y H universal. Por ello $\exists w \in H \setminus \{0\}$
 tal que $f(w) = \delta$.

Corolario: Todo espacio de dimensión 2 sobre \mathbb{F}_p es universal.
 (Se usa el método de que si $\dim V = 2$ $V \perp \langle -\delta \rangle$ es isotrópico).

$K = \mathbb{F}_p$, $p = \text{impar}$, $\dim V = 2$ entonces $V \cong [1] \perp [\Delta]$, $[1] \perp [1]$
 o $[\Delta] \perp [\Delta]$.

	$-1 \cdot \alpha^2$	$-1 \otimes K^2$
$[1] \perp [\Delta]$	isot	isot
$[1] \perp [1]$	isol	n.i.
$[\Delta] \perp [\Delta]$	isol	n.i.

Corolario: Todo espacio de dimensión ≥ 3 es isotrópico. (En ff)

Corolario: Dos espacios cuadráticos sobre \mathbb{F}_p de la misma
 dimensión y el mismo discriminante son isométricos.

Dom

$V \cong M \perp V$ $\rightarrow W \cong M \perp W_1$ y se cumple por
inducción en el caso de dimensión 1 o 2. Encuéntrelo
dej e.o. Son isomorfos si tienen igual discriminante.



Álgebra de Cuaterniones

Formas Cuadráticas Locales

Álgebra de Watermanes:

Sea K (cuerpo), $\text{car } K \neq 2$.

Una álgebra generada por i, j donde:

$$A = K\langle i, j \rangle = \langle i, j : i^2 = a, j^2 = b, ij = -ji \rangle$$

Se dice álg. de Watermanes, para abreviar. Se denota por $\left(\frac{a}{K} \right)$

Observación: $\left(\frac{a}{K} \right) \cong \left(\frac{a^2, b^2}{K} \right)$.

$A = \left(\frac{a}{K} \right)$ es un álgebra central simple. Es decir, $A \cong M_n(D)$, D alg. división central.

Observación: $A = K \oplus K_i \oplus K_j \oplus K_{ij}$. Si $\bar{K} = K$ entonces $A \cong M_n(K)$ vía $i \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{pmatrix}$ y $j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$.

En nuestro caso $\dim A = 4$. Así:

1) A es alg. división

2) $A \cong M_2(K)$

Si $\varphi = xiiy + yij + wij$ definimos su conjugado por $\bar{\varphi} = x - yi - uj - wi$.

Así $N(\varphi) = \varphi \bar{\varphi} = x^2 - ay^2 - bw^2 + abw^2 \in K$

Lema: $\varphi^{-1} = \bar{\varphi} / N(\varphi)$, si $N(\varphi) \neq 0$. Por otro lado

Si $\varphi \circ S = 1$, con $\bar{\varphi} \circ \bar{S} = \bar{\varphi}^{-1}$ se tiene que $1 = N(\varphi \circ S) = N(\varphi)N(S)$

Por lo tanto $N(\varphi) = 0$.

A la división $\Leftrightarrow \forall q \in A, N(q) \neq 0$

No es una forma cuadrática,

(A, N) es un espacio cuadrático isométrico si:

$$[1] \perp [-a] \perp [-b] \perp [ab]$$

A es álgebra de división si este espacio es anisotrópico. (ed: $N(f) = 0$, para $f \neq 0$).

Corolario: Toda alg. sobre \mathbb{F}_p es isomorfa a un álgebra de matrices, ed: $M_2(\mathbb{F}_p)$.

Observación: $\dim N = 1$.

Si N es isotrópica: $A \cong M_2 \perp M_1$. (Usando que $\dim V = 2$ y disc $B \neq 1 \Rightarrow B \cong M_1$)

- Existe Subespacio $W \subseteq A$ totalmente isotrópico de dim. 2.

S: $A^\circ = \langle i_i j_j, i j \rangle$ esp. cual puros entres $A^\circ \cap W \neq 0$ por dimensión.

Corolario: $A \cong M_2(k)$ ssi existe un nat. puro de norma cero no trivial.

(Nóisstro.) Sea $p \in A^\circ$. Existen $\mathbf{f} \in A^\circ$ con $\mathbf{f} \perp \mathbf{p}$, ed: $B(p, f) < 0$ donde $B(p, f) = \frac{1}{2}(N(p + f) - N(p) - N(f))$, podemos assumir $N(f) \neq 0$.

Por lo tanto: $N(p + f) = N(p) + N(f)$.

$$\text{ed: } p\bar{p} + \bar{p}p = 0.$$

$$\text{Si: } p, \bar{p} \in A^0: \quad p\bar{p} + \bar{p}p = 0.$$

($V = \langle 1 \rangle$ es no singular)

obs: $A^0 = 1^\perp$, por ello es no singular. Sea $V = \langle p \rangle$ no singular.
así, $p^\perp \cap A^0$ tiene dimensión 2 en A^0 , es no singular $\Rightarrow \exists p \in p^\perp \cap A^0$

Con $N(p) \neq 0$.

Dicho tanto, como $p(p) + (p)p = 0 \Rightarrow p, p \in p^\perp \cap A^0$

Supongo: $p^\perp \cap A^0 = \langle p, p \rangle = K[p]_p$ (pues p es invertible,
así imp: $A \rightarrow A$ invertible, así $\dim \langle p, p \rangle = \dim \langle 1, p \rangle = 2$)

Propiedad: $A \cong M_2(K)$ ssi $b = x^2 - xy^2$ tiene soluciones.

Demonstración: Esto es equivalente a

$\Leftrightarrow [1] \perp [-x]$ representan b .

$\Leftrightarrow [1] \perp [-x] \perp [-b]$ es isotrópico.

$\Leftrightarrow \exists p \in \langle (i, j) \rangle$ con $N(p) = 0$; $p \neq 0$.

Claramente si existe p , $p \neq 0$, $N(p) = 0 \Rightarrow A \cong M_2(K)$.

$A \cong M_2(K) \Rightarrow \exists W \subseteq A$. t. isotrópico, $\dim W = 2$

$\therefore W \cap \langle (i, j) \rangle = \{0\}$.

• puede medir con anterioridad

Corolario: $\left(\frac{a, b}{K}\right) \cong M_2(K)$ ssi $b \in N_{M_2}(L)$ donde $L = K(\sqrt{a})$.

[pues $N(x+y\sqrt{a}) = x^2 - ay^2$]

Proposición: Si $L = K(\sqrt{c})$, $c \neq 0$, $c \in K$ se incrusta en $\left(\frac{a, b}{K}\right)$

cuales:

$\left(\frac{a, b}{K}\right) \cong \left(\frac{c, d}{K}\right)$, algún d $\in K$.

(L es separado).

Demarcación: Sea $\psi: L \rightarrow A$, $\psi(\sqrt{c}) = p$. Es fácil ver que
 $p^2 = c \rightarrow N(p) \neq 0$. Luego $f^{-1} = \overline{f}/N(p)$
 $\therefore \sqrt{p} = \pm c$ Así $\hat{f} = \frac{N(p)}{c} f$.

Caso 1: $N(p)/c = 1 \rightarrow p \in K \Rightarrow c = p^2 \in K^{\times 2}$ (\star)

Caso 2: $N(p)/c = -1 \Rightarrow p \in A^\circ$, con $N(p) \neq 0$.

Por ello $\exists q \in A^\circ$, $p + q$ con: $qp + fp = 0$, $p^2 = c$, $p^2 = -N(p)$

Sea $d = -N(p)$.

No existe $\Psi: (\frac{c}{K}) \rightarrow A$, $\Psi(i) = p$, $\Psi(j) = p$ porque

Como $(\frac{c}{K})$ simple $\Rightarrow \Psi$ inyectiva. Por dimensión Ψ sobreactiva.

Ejemplo: $K = \mathbb{R}$. Sea $|H| = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$ cuat. de Hamilton.

$p \in A^\circ \subset [1] \perp [1] \perp [1]$. $N(p) > 0$, $p \neq 0$. Así

$\mathbb{R}[\sqrt{-1}]$ es la única ex. que se incrusta en $|H|$

Ejemplo: $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$ alg. división. Observa que $[1] \perp [1] \perp [1]$
 no representa a \mathbb{R} .

Estos modulos si se reducenmos a un par. $\therefore x^2 + y^2 + z^2 = 0$ (mod 4)

$\Rightarrow x, y, z$ pares (\star)

$\therefore \mathbb{R}(\sqrt{-1})$ no se incrusta en $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$ (pues no hay cuat. de norma pura)

A y si hay humo: $\phi(\sqrt{-1}) = \text{cuat. puro de norma } \frac{1}{2}$.

Cuerpos locales No arquimedios.

+ Cuerpo, p = valor absoluto con:

$$p(a, b) = p(a)p(b)$$

$$p(a) = 0 \Leftrightarrow a = 0$$

$$p(a+b) \leq \max\{p(a), p(b)\}$$

p discreta si $p(K^\times) = c \in \mathbb{N}^*, c > 1$. Un cuerpoo de este tipo es un cuerpo local no arquimediano. Un elemento $\bar{x} \in K$ tiene

$p(\bar{x}) = 1$ se denominó punto uniformizante. Así para $a \in K$, $a = \bar{x}^{m_K}$ con $p(a) = 1$. Además $O_K = \{x \in K : p(x) \leq 1\}$ es un anillo y $m_K = \{a \in K : p(a) < 1\}$ es su único ideal maximal. Esto pues $O_K^\times = \{a \in K : p(a) = 1\}$. Se define el cuerpoo residual de K por $R_K = O_K/m_K$. Suponemos R_K finito. Suponemos K completo.

Observación: $p(a) < p(a_0)$ implica

$$p(a_0 + \dots + a_n) = p(a_0)$$

Además $\sum_{i=1}^n a_i$ converge ssi $p(a_i) \rightarrow 0$

Lema: (Hewitt) Sea $f \in \mathcal{O}_K[[x]]$. Si existe $a \in O_K$ tal que

$f(a) \in m_K$, $f'(a) \notin m_K$ entonces existe $b \in O_K$

tal que $f(b) = 0$. De hecho $a \equiv b \pmod{m_K}$.

Demarcación: Tomamos $a_0 = a$. Definimos $a_{n+1} = a_n + \epsilon \bar{x}^{m_K^n}$

Como $f(x+y) = f(x)+y f'(x) \pmod{\bar{x}^{m_K}}$. Entonces

$$f(a_{n+1}) \equiv f(a_n) + \pi^{n+1} \in f'(a_n) \pmod{\pi^{n+2}}$$

Si $f(a_n) \equiv 0 \pmod{\pi^{n+1}}$, $f'(a_n) \not\equiv 0 \pmod{\pi}$, se tiene que

$$\epsilon = -\frac{f(a_n)}{\pi^{n+1}} \cdot \frac{1}{f'(a_n)}.$$

y pues $f'(a_{n+1}) \equiv f'(a_n) \pmod{\pi}$
 $\neq 0$.

(Teorema de los cuadrados locales)

Proposición: Sea $\alpha \in \mathbb{O}_K$, entonces existe $\beta \in \mathbb{O}_K$ tal que

$$1+4\pi\alpha = (1+2\pi\beta)^2$$

Demonstración: Considera la ecuación $\pi x^2 + x + \alpha = 0$, en $\mathbb{I}\mathbb{K} \subset \mathbb{O}_K/\pi\mathbb{O}_K$

$f(x) = \pi x^2 + x + \alpha$ cumple con $f(\bar{x}) = \bar{x} - \bar{\alpha}$, tiene una raíz y $f'(\bar{x}) = 1$. Por teorema de Hensel, se tiene que:

$$f(x) = \pi(x - \beta)(x - \beta')$$

tal que β, β' raíz, con $\beta \equiv \alpha \pmod{\pi}$, $\beta \in \mathbb{O}_K$. Luego:

$$\beta = \frac{-1 \pm \sqrt{1+4\pi\alpha}}{2\pi}$$

ed: $(1+2\pi\beta)^2 = 1+4\pi\alpha$.

Corolario: $1+4\pi\mathbb{O}_K \subseteq \mathbb{K}^*$

Sea $a \in \mathbb{K}^*$: Definimos el defecto cuadrático de a por

$$\delta(a) = \left(\bigcap \{(n) \mid a = b_1 + x^2, \exists \text{ } x \in \mathbb{K}\} \right)$$

Suego:

$$f(x) = 0 \Leftrightarrow x = x_n^2 + h_n, \text{ where } h_n \text{ is a pefect square}$$

Si $\lim_{n \rightarrow \infty} x_n$ demande limite

$$f(x) = 0 \Leftrightarrow x = x^2, \quad x = \lim x_n.$$

Definición: $v(\alpha) = n \Leftrightarrow \alpha = u\pi^n, u \in \mathbb{Q}_K^*$.

S: $v(\alpha) = n$ impar entonces $v(\alpha) = v(x^2), \forall x \in K$. Así si $\alpha = u + x^2$
 $v(u) = \max\{v(\alpha), v(x^2)\}$, pero entonces $f(\alpha) = (u)$.

Supongamos que $v(\alpha) = 2n \Rightarrow \alpha = u\pi^{2n}, u \in \mathbb{Q}_K^*$. Así $f(u) = f(\alpha)/\pi^{2n}$.
Basta calcular el d. cuadrático de las unidades:

Caso: K No diádico; $2 \notin m_K$.

Sea $\alpha \in \mathbb{Q}_K^*$. Entonces $f(x) = x^2 - \alpha$ cumple con $f(x) = x^2 - \alpha$

$f'(x) = 2x + 0$ en IK . Por Hensel, si $x \in K^2 \Rightarrow x$ es cuadrado en K

Si $x \notin K^{*2} \Rightarrow x \notin K^{*2}$.

Sabemos que $\mathbb{Q}_K^*/\mathbb{Q}_K^{*2} = \{\bar{1}, \bar{\Delta}\}$. Como $K^* \cong \mathbb{Q}_K^* \times \mathbb{Z}_2$

Así $\mathbb{Q}_K^*/K^{*2} \cong \mathbb{Q}_K^*/\mathbb{Q}_K^{*2} \times \mathbb{Z}/2\mathbb{Z} = \{\bar{1}, \bar{\Delta}, \bar{\tau}, \bar{\Delta\tau}\}$

Caso: K diádico, $2 \in m_K$.

Definimos $e = v(2)$.

Sea u unaidad no cuadrada. $i \in \mathbb{N} \setminus \{0, e\} \Rightarrow \bar{u} = \bar{1}^i$ (pero).

If finito $\Rightarrow I\Gamma$ perfecto $\Rightarrow \bar{I\Gamma}^2 = \bar{I\Gamma}$. Pero ello $u|b^2 \equiv 1 \pmod{n}$

pd: $u = 1 + \varepsilon, |\varepsilon| < 1$

Agr $\delta(u) \subseteq (\varepsilon)$, pero $|k| < k^{\frac{1}{2}}$. $u = x^2 + h$, como $\delta(u) \subseteq (\varepsilon) \nsubseteq (1)$
 Asumimos $|h| < 1$, por ello $\bar{x}^2 \equiv \bar{u} \equiv 1 \pmod{\pi}$
 $\therefore \bar{x} \equiv 1 \pmod{\pi}$

Sí $|h| < |\varepsilon|$: Sí $|x+y| = |x|$ necesitamos que:
 $(x+y)^2 \equiv 1 + \varepsilon \pmod{\pi\varepsilon}$
 $1 + 2y + y^2 \equiv 1 + \varepsilon \pmod{\pi\varepsilon}$
 $y(y+\varepsilon) \equiv \varepsilon \pmod{\pi\varepsilon}$

(2) $|y| > |z|$

entonces $|y+z| = |y|$, por ello $|\varepsilon| = |y|^2$

(ap2) $|y| \leq |z|$

en tal caso $|\varepsilon| = |y||y+z| \leq |y|$. Sí $|\varepsilon| < |y| \Rightarrow$

$u = 1 + 4\pi z^2 \in k^{*2}$. Contradicción. Por ello $|\varepsilon| = |y|$

ed: $\varepsilon = 4\lambda, \lambda \in k^{*}$

Agr: $u = 1 + \varepsilon = 1 + 4\lambda = (1+t)^2$ no tiene solución.

col: $1 + 4\lambda = 1 + 2t + t^2 \quad " \quad \text{en } k$

$t^2 - 2t - 4\lambda = 0$ no tiene solución en k . Sea $t = 2z$

$\therefore z^2 + \varepsilon - \lambda = 0 \quad \text{no tiene sol. en } k$.

$\therefore z^2 + z - \bar{\lambda} = 0 \quad \text{no tiene sol. en } k$

Sí ζ es solución de $z^2 + z - \bar{\lambda} = 0 \quad \therefore k(\zeta)$ es la única ext. normalizada
 de grado 2 de k . Sea $\Delta = 1 + 4\lambda$. Δ se dice la cuadrática
de def. cuadrática minimal!

S: unicidad de $\det \square$ mínima $\Rightarrow |\varepsilon| < 14$.

Hay dos casos:

(1) $v(\varepsilon) = p\alpha$, $|v(\varepsilon)| = |\pi|^{2t}$. Sea p unidad:

$$(1 + \pi^t p)^2 = 1 + 2\pi^t p + \pi^{2t} p^2$$

π^{2t} dominante en (1). Pues: $|\varepsilon| > 14 \Rightarrow |\pi^{2t}| > 12$.

Sea $\varepsilon = \pi^{2t} \lambda \Rightarrow p^2 \equiv \lambda \pmod{\pi}$, tomamos este p .

$$(1 + \pi^t p)^2 = 1 + 2\pi^t p + \pi^{2t} p^2 \equiv 1 + \pi^{2t} \lambda \pmod{\pi^{2t+1}}$$

Dor ello reemplazamos $1 + \varepsilon$ por $\frac{1 + \pi^{2t} \lambda}{(1 + \pi^t p)^2}$.

(2) Si $v(\varepsilon)$ impar. En este caso también $|v(\varepsilon)| > 14$

$$(1 + y)^2 \equiv 1 + \varepsilon \pmod{\pi^e} \Rightarrow y(y+2) \equiv \varepsilon \pmod{\pi^e}$$

Por lo tanto $|(1+y)(y+2)| = |y|^2 = |\varepsilon| > 14$. $v(\varepsilon)$ impar, y impar, y no puede ocurrir.

$\therefore f(n) \in \{(1), (1)^3, \dots, (\pi^{2e-1}), (\pi^{2e}) = (14)\}$.

Unidades ramificadas.

Unidad ramificada.

Teorema: Sea $\psi: G \rightarrow G'$ un homomorfismo. Sea $H \subseteq G$ subgrupo.

Entonces: $[G : H] = [\psi(G) : \psi(H)] [Ker \psi : H \cap Ker \psi]$.

$$[G : H] = [\psi(G) : \psi(H)] [Ker \psi : H \cap Ker \psi].$$

Demonstración: Al igual que el 1º teo. de ISo, sea $K = Ker \psi$.

$$\begin{aligned}[G : H] &= [G : KH][KH : H] \\ &= [G/K : KKH][K : KKH] \\ &= [\psi(G) : \psi(H)][K : KKH].\end{aligned}$$

Sea $\psi: \mathbb{O}_K^* \rightarrow \mathbb{O}_K^*, \psi(x) = x^2$. Sea $H = (1 + \pi^r \mathbb{O}_K)$

entonces

$$|\mathbb{O}_K^* / (1 + \pi^r \mathbb{O}_K)| = |\mathbb{K}| - 1 = p - 1$$

$$|\mathbb{O}_K^* / (1 + \pi^{s-1} \mathbb{O}_K)| = |\mathbb{K}| = p, \quad |\mathbb{K}| = p.$$

Abr $[G : H] = (p-1)^{r-s}$. Por otro lado, si $\psi(G) = \mathbb{O}_K^{*2}$
 $[\psi(G) : \psi(H)] = ?$

Calculo mdo.

$$(1 + \pi^r \lambda)^2 = 1 + 2\pi^r \lambda + \pi^{2r} \lambda^2 \in 1 + \pi^{r+s} \mathbb{O}_K$$

Si $r = e + 1 + s, s \geq 0$:

$$\begin{aligned} 1 + \pi^{r+s} \alpha' &= 1 + \pi^{2e} \pi^r (\pi^s \alpha') = 1 + \pi^r \left(\frac{\pi^s \alpha'}{\pi^e} \right) = (1 + \pi^r \beta)^2 \\ &= (1 + \pi^r (\beta/\pi^s u))^2 = 1 + \pi^r \beta, \quad \beta' = \beta/\pi^s u \in \mathbb{O}_K. \end{aligned}$$

por lo tanto $|\beta| \leq |\pi^s|$.

$$\therefore \psi(H) = 1 + \pi^{r+s} \mathbb{O}_K$$

$N = \ker \psi = \{ \pm 1 \}$, por ello $|N| = 2$. Si $r > 1$, se tiene que
 $|NNH| = 1$, por lo tanto $\pm 1 \notin H$.

Abr:

$$[\psi(G) : \psi(H)] = [\mathbb{O}_K^{*2} : 1 + \pi^{r+s} \mathbb{O}_K]$$

Luego

$$[G : H] = 2 [\psi(G) : \psi(H)] = 2 [\mathbb{O}_K^{*2} : 1 + \pi^{r+s} \mathbb{O}_K]$$

$$\text{Asi: } (p-1)^{r+s} = 2 [\mathbb{O}_K^{*2} : 1 + \pi^{r+s} \mathbb{O}_K]$$

$$[\mathbb{O}_K^{*2} : \mathbb{O}_K^{*2}]$$

Finalmente:

$$[\mathbb{Q}_k^* : \mathbb{Q}_{k^{*2}}] = 2 \frac{(p-1)p^{r+e-1}}{(p-1)p^{r-1}} \\ = 2 p^e.$$

Ejemplo: $[\mathbb{K}^* : \mathbb{K}^{*2}] = 4 p^e$.

Ejemplo: $\mathbb{K} = \mathbb{Q}_2$ entonces $[\mathbb{Q}_2^* : \mathbb{Q}_2^{*2}] = 8$.

175 Buscar extensión no ramificada

Álgebras de cuaterniones sobre K

$$B \cong K \oplus Ki \oplus Kj \oplus Kij, i^2 = a, j^2 = b, ij + ji = 0.$$

Entonces $B \cong M_2(K)$. Si B ál. de división. Podemos escribir

$$B = \begin{pmatrix} a & b \\ 0 & K \end{pmatrix} \text{ y } B \cong M_2(K) \Leftrightarrow b \in N_{K}(L^*) \text{, } L = K(\sqrt{a})$$

$$N_{K}(a + b\sqrt{a}) = a^2 - b^2$$

Supongamos que $d = \Delta$, así L/k no ramificada

Ecuación de la clase: $N_{K}(L^*) = \mathbb{O}_K^* \cdot K^{*2}$

Así $\pi \notin N_{K}(L^*)$. Por ello $\begin{pmatrix} 0 & \pi \\ 0 & K \end{pmatrix}$ no es alg. de matrices.

Observación: $x \in L \Rightarrow x = u\pi^k$, si $ad \neq 0$, $u \in \mathbb{O}_L^*$

$$\Rightarrow |x|_L = |N(x)|_K^{1/2} \rightarrow N(x) \in \mathbb{O}_K^*, \text{ pues } |x|_L = 1.$$

$$\therefore N_{L/K}(L^*) \subseteq \mathbb{O}_K^* \cdot K^{*2}.$$

Sed K cuerpo local. Buscar álgebra de cuaterniones sobre K , de división.
(En general ál. de división). Sed L/k extensión de cuerpos, entonces L es cuerpo local. Si $x \in L$ entonces $|x|_L = |N_{K}(x)|_K^{1/n}$ es el v.a. absoluto en L .

Algebra de división central, de dimensión n ? Se $x \in B$, entonces $x \in L$, con L cuerpo, $[L : K] = n$ entonces.

$$N(x) = N_{L/K}(x) = (N_{K(x)/K}(x))^{[L : K(x)]}, \alpha = \frac{[L : K(x)]}{[K : K(x)]}$$

entonces definimos en B el v.a. absoluto: $|x|_B = |N(x)|_K^{1/n}$, este v.a. cumple con $||x+y||_B \leq \max\{|x|_B, |y|_B\}$.

Siendo B tiene un \mathbb{N} . absolujo que cumple con:

$$① |a|_B |b|_B = |ab|_B;$$

$$② |a|_B > 0, \text{ si } a \neq 0.$$

$$③ |a+b|_B \leq \max\{|a|_B, |b|_B\}.$$

Sea $\pi_B \in \mathbb{R}$ parámetro uniformizante. Asumiremos desde ahora que

$n=2$. Sabemos que $|B^*|_B \subseteq \mathbb{R}^+$ y $[|B^*|_B, |L^*|_B] = e(B|k) \leq 2$

De hecho: $e(B|k) = \max_{\substack{L \subseteq B \\ L \text{ k-wadiotica}}} e(L|k).$

Observemos que $|B^*|_B$ es un conjunto discreto. Por ello existe un generador de $|B^*|_B \subseteq \mathbb{R}^+$ ed: $|B^*|_B = \pi_B^{\mathbb{Z}}$. De lo tanto, todo $a \in B^*$:

$$a = n \pi_B^t, t \in \mathbb{Z}, n \in \mathbb{N}_0.$$

donde $\Omega_B = \{x : |x|_B \leq 1\}$ anillo con un solo ideal maximal

$M_B = \{x : |x|_B < 1\}$. No comunitativo.

Sea $S = \text{Conj. de representantes para } \Omega_B/M_B = \text{Cuerpos comunitarios finitos.}$

Dem: $\bar{a} \in \Omega_B/M_B$. $\bar{a} \neq 0$ entonces $\bar{a} \in S$ $Q \in \Omega_B - M_B = \Omega^*$. Siendo
 $a' \in \Omega_B - M_B$ $a'^{-1} \in \Omega_B/M_B$, $\bar{a}'^{-1} \neq 0$.

$\therefore \Omega_B/M_B = \text{cuadro o alp. div. de dimensión 4}$

$\therefore \Omega_B/M_B$ Cuerpo.

Supongamos que $0 \in S$. Puedo para n unidad $\exists A \in S - \{0\}$ con $n = ScMB$

$\therefore \bar{a} = n \pi_B^t$ se escribe como:

$$\begin{aligned} Q &= a \pi_B^t + (n-a) \pi_B^t, \quad \pi = \pi_B \\ &= a \pi_B^t + n \pi_B^t \pi_B^{-1} \\ &= a \pi_B^t + a_{t+1} \pi_B^{t+1} + (n-a_{t+1}) \pi_B^{t+1} \\ &= \dots \end{aligned}$$



Supongamos que $e(B|K) = 1$. Entonces podemos suponer que $\bar{B} = K$.

Además, para $L|K$ ext. no ramificada se tiene que:

$$\frac{OL}{ML} \geq \text{ext. cuadrática de } L|K$$

$$\frac{OL}{ML} = \frac{OB}{m_B}$$

Pues $m_L = m_B n_{OL}$, así, $\frac{OL}{m_L} \leq \frac{OB}{m_B} = \text{ext. de } L|K$ además de que $L|K$ tiene solo una ext. cuadrática. Así podemos elegir $S \subseteq L$.

Supongo $B = L$, pues $\alpha = \frac{1}{2} \pi^i \pi^j | eL$.
 $\therefore e(B|K) = 2$, luego $| \pi_K | = | \pi_B |^2$.

Supongamos que $f(B|K) = 1$, entonces $S \subseteq K$. Pues $B = K(\bar{\pi}_B)$
 ext. cuadrática de $K \Rightarrow B$ es miembro de $(*)$ $\therefore f(B|K) = 2$.

B contiene una ext. no ramificada de dimensión 2 (\mathbb{H} para el caso Watermanico). $[S: \forall L \subseteq B, e(L|K) = 1 \Rightarrow B|K$ de grado 1 $\Rightarrow B = K$ (*)]

Sea $D \in \Omega_K^*$ unididad no ramificada de def. cuadrática máxima, $e =$

$$K(\sqrt{D})|K$$
 no ramificada.

$\therefore K(\sqrt{D}) \subseteq B$ al Cuaterniones.

Por lo tanto $B = \left(\frac{D_{ij}}{k} \right)$, donde $k \in \mathbb{K}^*$, con $\det N(k(L)) = k(\sqrt{\Delta})$.

Ejemplo: $B_0 = \left(\frac{D_{ij}\pi}{k} \right) = k \oplus k_i \oplus k_j \oplus k_{ij}$, $i^2 = \pi$, $j^2 = \Delta$.

Sea $L = k(j) = k(\sqrt{\Delta})$ y escribamos $B_0 = L \oplus L_i$. Entonces:

$$\lambda_1 + i\lambda_2 = \bar{\lambda}_1 - i\bar{\lambda}_2$$

Siempre $N(\lambda_1 + i\lambda_2) = (\lambda_1 + i\lambda_2)(\bar{\lambda}_1 - i\bar{\lambda}_2) = N(\lambda_1) - i\lambda_2\bar{\lambda}_1 - \lambda_1\bar{\lambda}_2 + i\lambda_2\bar{\lambda}_2$

Pero $\lambda_i = i\bar{\lambda}$, así:

$$N(\lambda_1 + i\lambda_2) = N(\lambda_1) + \pi N(\lambda_2) \neq 0$$

Valuación par Valuación impar

Entonces $|N(\lambda)|_L = |\pi|_k^{1/2} |N(\lambda)|_k^{1/2}$ tiene valuación par $|B|_L = 1 \Leftrightarrow |N(\lambda)|_k^{1/2} = 1$.

∴ B_0 álgebra de división.

Sea B_1 otra álgebra de división de cuaterniones.

Proposición: $\left(\frac{a+b}{k} \right) \otimes \left(\frac{c+d}{k} \right) \cong M_2 \left(\left(\frac{a+bc}{k} \right) \right)$

[Contiene a $k(\sqrt{a}) \oplus k(\sqrt{a})$ por lo tanto es de la forma $M_2(Q)$, $(Q = a/b)$.
Cuaterniones].

Siempre $\left(\frac{D_1\pi}{k} \right) \otimes \left(\frac{D_2\pi u}{k} \right) \cong M_2(W_3)$, $W_3 = \left(\frac{D_1\pi^2 u}{k} \right) \cong \left(\frac{D_1 u}{k} \right)$, $|W| = 1$.

Afirmación: $\left(\frac{D_1 u}{k} \right)$ es álgebra de matrices, si $|u| = 1$.

Sabiendo que es un álgebra de matrices

$$\left(\frac{D_1\pi}{k} \right) \otimes \left(\frac{D_2\pi u}{k} \right) \cong M_4(k)$$

Supuesto en $\text{Br}(K)$:

$$\left[\left(\frac{D_{1,II}}{K} \right) \right] = \left[\left(\frac{D_{1,II}}{K} \right) \right]^{-1}$$

$$= \left[\left(\frac{D_{1,II}}{K} \right) \right]$$

Por lo tanto: $\left(\frac{D_{1,II}}{K} \right) \cong \left(\frac{D_{1,II}}{K} \right)$ por igualdad en dimensión.

\therefore Si: $|z| = |\Pi^{2t}| \Rightarrow \left(\frac{D_{1,z}}{K} \right)$ álgebra de matrices y si: $|z| = |\Pi^{2t+1}|$ entonces ($\frac{D_{1,z}}{K} \cong \left(\frac{D_{1,II}}{K} \right)$) álgebra de división.

\therefore Hay dos tipos de álgebras de cuat. sobre K (cuerpo local), con $\text{Car } K \neq 2$.

Demonstración de la afirmación: Si no, $B = \left(\frac{D_{1,II}}{K} \right)$ es álgebra de división.

Sup. $i^2 = u$, $j^2 = D$ (Sea $L = K(ij)$). Sabemos que $1 \in OK$, sea $\bar{u} \in LK = OK/LK$. Así:

$$\therefore \bar{u} = N_{LK}(x)$$

Esta forma es universal, si $\text{Car } K \neq 2$ (por ello): $N_{LK}(x) = \bar{u}$.

S: $\text{Car } K = 2$, $L = K(\alpha)$, para $\alpha^2 + \alpha \in OK$. Supojo $f = i(i\alpha, \alpha)$ cumple con:

$$f(x) = (x+\alpha)(x+\alpha+1)$$

Supuesto $N_{LK}(\alpha) = \alpha^2 + \alpha$. Así si \bar{u} cumple con $\bar{u}^2 + \bar{u} = 0$ (Si: $\bar{u} = \bar{x}^2 + \bar{\alpha}$ $\Rightarrow \bar{u}^2 + \bar{\alpha} \Rightarrow N_{LK}(\bar{\alpha}) = \bar{\alpha}^2 + \bar{\alpha} = \bar{u}$). Si no, $N_{LK}(\bar{u}) = \bar{u}^2 = \bar{u}$

$\therefore f = x^2 + \bar{b}x + \bar{u}$ tiene soluciones en L . Levantando, $f(x) = x^2 + bx + u$ tiene sol. en L (pues $f'(x) \neq 0$, y L tiene L/K separable y f irred)

$\therefore N: O^* L \rightarrow OK^*$ es sobre y estricta, y pues \bar{u} es una raíz.

$\therefore u \in N_{LK}(L^*)$, así $\left(\frac{D_{1,u}}{K} \right) \cong M_2(K)$.

(En la dem $\bar{b} = \bar{1} \circ \bar{0}$).

Premio: Sea V el vectorial cuadratíco binario con div $V \in K^*$ uniformizante.
 Entonces V representa exactamente a un elemento de $\{w, Dn\}$,
 no K^* .

Demonstración: Sea $V = [b] \sqcup [-ab]$. V representa a n si, y sólo si,
 $[1] \sqcup [-2]$ representa n/b .

ed: $V = F(V_0)$ y $f = N$ representan a n/b .

Aj: $-a = \text{div } V \in K^*$ uniformizante. Luego.

$$\left(\begin{matrix} 2, h \\ K \end{matrix} \right) \text{ alp. división} \Leftrightarrow \left(\begin{matrix} 2, hD \\ K \end{matrix} \right) \text{ alp. matrizes}$$

Demonstración: Observa que como $V(a) = \text{impar}$:

$$\left(\begin{matrix} 2, h \\ K \end{matrix} \right) \otimes_K \left(\begin{matrix} 2, hD \\ K \end{matrix} \right) \cong M_2 \left(\left(\begin{matrix} 2, hD^n \\ K \end{matrix} \right) \right) \cong M_2 \left(\left(\begin{matrix} 2, D \\ K \end{matrix} \right)^n \right) = \text{div}$$

Luego como:

$$\begin{matrix} B & K & B \\ K & K & B \\ B & B & K \end{matrix}$$

Analizando elemento a elemento se concluye
 lo pedido.

Luego como

$$[1] \sqcup [-2] \text{ rep. } n \text{ ss: } \left(\begin{matrix} 2, h \\ K \end{matrix} \right) \text{ alp. matrizes}$$

$$\text{ss: } \left(\begin{matrix} 2, hD \\ K \end{matrix} \right) \text{ alp. división}$$

$$\text{ss: } [1] \sqcup [-a] \text{ no representa } n$$