UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CIENCIAS

ULTRAMETRICA

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A :

NITTAI MADRID RINCON

MEXICO, D. F. 1995

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

UNIVERSIDAD NACIONAL AVENIDA DE MEXICO

M. EN C. VIRGINIA ABRIN BATULE
Jefe de la División de Estudios Profesionales
Facultad de Ciencias
P r e s e n t e

Los abajo firmantes, comunicamos a Usted, que habiendo revisado el trabajo de Tesis que realiz(ó)ron LA pasante(s) MITTAI MADRID RINCON

con número de cuenta 8837115 - 7 con el Título:

ULTRAMETRICA

Otorgamos nuestro **Voto Aprobatorio** y consideramos que a la brevedad deberá presentar su Examen Profesional para obtener el título de MATEMATICO

GRADO	NOMBRE(S)	APELLIDOS COMPLETOS	FIRMA
M. EN C.	CESAR ALEJANDRO	RINCON ORTA	
Director de Tesis			
DR.	EMILIO	LLUIS RIERA	
M. EN C.	ALEJANDRO	BRAVO MOJICA	
DR.	ALEJANDRO JAVIER	DIAZ BARRIGA CASALES	
Suplente			
DR.	HUGO ALBERTO	RINCON MEJIA	
Suplente			

A LOS SEÑORES PADRES: JUAN ANTONIO Y ERÉNDIRA.

AGRADECIMIENTOS

Primero que todo, quiero agradecer a mi director de tesis, César Rincón Orta, por su excelente labor de rey Midas y por todo el cariño y apoyo. También gracias a mis sinodales: Emilio Lluis Riera, Alejandro Bravo, Hugo Rincón y Alejandro Díaz Barriga, quienes además de haberme ayudado con la tesis me ayudaron en toda la carrera y fueron muy queridos amigos y maestros.

Gracias también a los demás maestros que ayudaron a mi nacimiento como matemática. Principalmente quiero mencionar a Javier Fernández y a Guillermo Grabinsky.

Gracias a mi familia : A Eren - parte de la misma persona que yo -, por hacerme un poco más humana, y a Juan, por ser un gran padre y por el mar de cristalitos-conocimiento. A Alina, por tener cara de calabaza y un chorro de poesía, y a Sara, por compartir conmigo todo lo que comparte (canciones, dientes, mariposas y demás). A Ian, que aunque juega al psicótico es en el fondo un buen hermano. A César Ariel, porque hay poca gente tan buena onda como él y porque seguramente me habría costado más trabajo la tesis sin su ayuda. A los Hermanos Rincón, por tantas cosas; y a todos los demás, que también son muy queridos.

Gracias a Russell, a Luis, a Arturo, a Randy, a Jaime, y a todos los demás musos.

Gracias a mi muy querida amiga Lucía Buenrostro, que muchas veces me enseña a ser amable y buena y a su igualmente querida hermana Raquel Buenrostro, con quienes comparto ya gran parte de la vida ; a Julio César Cedillo (con C), sin cuya ayuda probable-

mente no habría acabado la carrera ; a Eugenia O' Reilly, que aparte de ser una persona maravillosa es muy buena amiga ; a Victoria Santillana, un ente pequeño lleno de magia que una vez me acompañó a subir un árbol grande grande donde había pociones mágicas y tesoros y pájaros para comer ; a Anni Bravo, un comprimido de amor y de sabiduría ; a Julia y Emilia Pool y a Bandy Gomar, mis hermanititas ; a Emmanuel, que aunque nunca me enseñó Cello inventó conmigo muchas historias, y a todos los demás amigos que he tenido o tendré.

Finalmente, pero no menos importante, quiero dar gracias al maestro Roberto Bañuelas, que es un manantial de agua para el espíritu que ha refrescado intensamente mi vida.

PRÓLOGO

La antigua concepción de que la matemática trata de las verdades absolutas quedó destruida para siempre con el nacimiento de las geometrías no euclidianas. Nacimiento que marca un **"punto crucial en el desarrollo del pensamiento matemático"**, y que puede considerarse **"tan trascendente como la revolución producida por Copérnico en la Astronomía, o desde el punto de vista filosófico, tan importante como la teoría Darwiniana de la evolución"**.

Contrario a lo que sucede en las ciencias experimentales como la física, la química o la biología, los objetos que la matemática estudia no son observables. Nacen como producto del razonamiento puro, y en cada teoría se originan como resultado de definiciones puntuales. Tienen propiedades explícitamente prescritas por sus axiomas, y las relaciones que surgen entre ellos se rigen por las leyes de una lógica precisa. Sus argumentos válidos son tan contundentes que con frecuencia llevan a identificar aspectos importantes de nuestro **"mundo real"** con las teorías matemáticas que se usaron para modelarlos.

¡Claro que **" 2 y 2 son cuatro"**! ¿Podría existir acaso otra aritmética?; o en geometría: **"por dos puntos pasa una recta y sólo una"**. ¿Cómo concebir otra realidad? Cualquier cosa que se afirme en contrario, es **"repugnante a la naturaleza de la línea recta"**, y el tratar de marchar en ese sentido es **"iniciar el viaje hacia una noche sin fondo capaz de extinguir toda luz y la alegría de vivir"** . . .

Y entonces Riemann, Bolyai, Lobachewsky y Gauss, entre otros, desarrollan las geometrías no euclidianas. Geometrías en las que se derrumban definitivamente algunas

"**verdades**" tan evidentes, que nunca nadie había osado poner en duda. Derrumbe este que tuvo, entre otras cosas, un efecto fortalecedor de la autonomía de los matemáticos, quienes sintieron reconfirmada su libertad – su privilegio – de poder establecer cualquier conjunto consistente de axiomas y ponerse a deducir – válidamente – conclusiones a partir de estos.

Ahora existen geometrías en las que por un punto fuera de una recta pasan muchas paralelas a ella (o ninguna, según sea el caso), la suma de las medidas de los ángulos interiores de cualquier triángulo es distinta de 180°, no existen figuras semejantes no congruentes, ni vale el celebrado teorema de Pitágoras, y aunque contrarias a nuestra intuición (?), son tan consistentes (y por lo tanto tan válidas) como la clásica geometría de Euclides, ni más ni menos; e incluso resultan más adecuadas para modelar algunos aspectos de nuestra realidad. Einstein afirma que "**. . . sin el advenimiento estas nuevas ideas acerca de la geometría, no hubiera sido posible desarrollar la teoría de la relatividad**". Y años después, J. J. Thompson escribe "**. . . existe el espacio de Einstein, el de Sitter, universos en expansión, universos que se contraen, universos que vibran . . . De hecho, un matemático puede crearlos con sólo escribir ecuaciones ; y aún si fuera egocéntrico, incluso podría tener un universo de su propiedad**".

En 1949 Gödel propuso un modelo para el universo físico en el que se cumplen las ecuaciones gravitacionales de Einstein y en el que, teóricamente, es posible viajar hacia atrás en el tiempo (Hasta la fecha, todos los intentos que se han hecho para rechazarlo, ya sea desde el punto de vista matemático o bien desde el filosófico, han tenido un rotundo fracaso).

¿Porqué no elucubrar un poco en geometrías peculiares? Esta tesis resume algunas consideraciones sobre resultados que se obtienen alterando ligeramente (?) uno de los axiomas que caracterizan a la métrica canónica. Explícitamente, la desigualdad del triángulo.

En el primer capítulo hablamos de *espacios con producto interior*, y ejemplificamos brevemente cómo a partir del producto interior usual definido en el espacio vectorial $\mathbf{R}^2$ se puede reconstruír la geometría euclidiana, y finalmente mostramos, con unos ejemplos, cómo la mayoría de los teoremas de tal geometría se vuelven trivialmente demostrables.

En el segundo capítulo introducimos el concepto de ***ultramétrica***, y jugamos un poco con la geometría en un espacio ultramétrico para mostrar sus "peculiaridades"

En el tercer capítulo describimos la construcción de la *compleción de un campo* mediante sucesiones de Cauchy.

En el cuarto capítulo, con el fin de generalizar la construcción descrita en el capítulo anterior, definimos las *valuaciones* y probamos algunos resultados útiles para trabajar con ellas. Como caso particular importante de estas valuaciones, definimos las *valuaciones p-ádicas*, y demostramos que las únicas valuaciones que se pueden definir en el campo de los racionales son las p-ádicas y las potencias del valor absoluto usual.

En el último capítulo nos concentramos en la compleción del campo de los racionales con respecto a una valuación p-ádica: los *números p-ádicos* ($\mathbf{Q}_p$); y demostramos algunas de sus propiedades. Para finalizar la tesis, damos un ejemplo de "geometría poco usual", el de una *circunferencia p-ádica*.

PRODUCTOS INTERIORES

DEF 1 Sea V un espacio vectorial sobre el campo k (a lo largo de este trabajo, k denotará siempre a R o a C, a menos que se especifique lo contrario). Un **producto interior** en V es una función que asigna a cada par ordenado de vectores $\mathbf{x}$ y $\mathbf{y}$ en V un escalar en k, representado como $(\mathbf{x}, \mathbf{y})$ tal que $\forall\ \mathbf{x}, \mathbf{y}, \mathbf{z} \in V$, $\forall\ \alpha_1, \alpha_2 \in k$ se tiene que:

a) $(\alpha_1 \mathbf{x} + \alpha_2 \mathbf{z}, \mathbf{y}) = \alpha_1 (\mathbf{x}, \mathbf{y}) + \alpha_2 (\mathbf{z}, \mathbf{y})$

b) $\overline{(\mathbf{x}, \mathbf{y})} = (\mathbf{y}, \mathbf{x})$, donde la barra indica conjugación compleja

c) $(\mathbf{x}, \mathbf{x}) > 0$, si $\mathbf{x} \neq 0$

Obs 1: Nótese que (*c*) se reduce a la simetría en el caso real.

Obs 2: (*a*) y (*b*) piden que el producto interior sea lineal en la primera componente.

Obs 3: Se puede ver fácilmente que si $a_1, \ldots, a_n \in k$ y $x_1, \ldots, x_n \in V$, entonces:

$$(\sum_{i=1}^{n} a_i x_i, y) = \sum_{i=1}^{n} a_i (x_i, y)$$

Obs 4: $\forall\ \mathbf{x} \in V$, $(\mathbf{x}, \mathbf{x}) \in R$. (Es por esto que la propiedad (*c*) de la definición tiene sentido, y así, $(\ ,\ )$ permite definir una "norma", $\|\mathbf{x}\| = (\mathbf{x}, \mathbf{x})^{1/2}$).

Un espacio vectorial V sobre k dotado con un producto interior específico se llama **espacio con producto interior**. Cabe hacer la observación de que un espacio vectorial dotado con dos productos interiores distintos puede resultar en dos espacios con producto interior distintos.

Ejemplo 1 :

1) Dados $\mathbf{x} = (a_1, a_2, \ldots, a_n)$, $\mathbf{y} = (b_1, b_2, \ldots, b_n) \in \mathbf{R}^n$, definimos

$$(\mathbf{x}, \mathbf{y}) = a_1 b_1 + \ldots + a_n b_n .$$

Y así definido, $(\ ,\ )$ es un producto interior. (El producto usual de $\mathbf{R}^n$).

Dem :

i) Sean $\mathbf{x} = (a_1, a_2, \ldots, a_n)$, $\mathbf{y} = (b_1, b_2, \ldots, b_n)$, $\mathbf{z} = (c_1, c_2, \ldots, c_n) \in \mathbb{R}^n$,

$\alpha, \beta \in \mathbb{R}$. Así,

$$(\alpha\mathbf{x} + \beta\mathbf{z}, \mathbf{y}) = \sum_{i=1}^{n} (\alpha a_i + \beta c_i) b_i = \sum_{i=1}^{n} \alpha a_i b_i + \beta c_i b_i = \alpha \cdot \sum_{i=1}^{n} a_i b_i + \beta \sum_{i=1}^{n} c_i b_i =$$

$$= \alpha(\mathbf{x}, \mathbf{y}) + \beta(\mathbf{z}, \mathbf{y})$$

ii) $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} a_i \cdot b_i = \sum_{i=1}^{n} b_i \cdot a_i = (\mathbf{y}, \mathbf{x})$.

iii) $(\mathbf{x}, \mathbf{x}) = \sum_{i=1}^{n} a_i^2 > 0$ si $\mathbf{x} \neq 0$.

†.

2) Sea X el conjunto de funciones complejas continuas definidas en el intervalo, e.d. $X = \{f: [0, 1] \to \mathbb{C}\ ; f$ es continua$\}$. Definimos un producto interior para este espacio de la siguiente manera:

$$(f(t), g(t)) = \int_0^1 f(t)\,\overline{g(t)}\,dt.$$ Así definido, $(\ ,\ )$ es un producto interior.

Dem:

i) Sean $f(t) = u(t) + iv(t)$; $g(t) = r(t) + is(t)$, $h(t) = p(t) + iq(t) \in X$, $\alpha, \beta \in \mathbb{R}$. Así ,

$$(\alpha f(t) + \beta g(t), h(t)) = \int_0^1 ((\alpha u + \alpha vi) + (\beta r + \beta si))(p - iq)dt =$$

$$\int_0^1 (((\alpha u + \beta r)p + (\alpha v + \beta s)q) + ((\alpha v + \beta s)p - (\alpha u + \beta r)q)i)dt = \alpha \int_0^1 (up + vq)dt +$$

$$+i\alpha \int_0^1 (vp - uq) + \beta \int_0^1 (rp + sq)dt + i\beta \int_0^1 (ps - qr)dt = \alpha \int_0^1 ((up + vq) + (vp - uq)i)dt +$$

$$+\beta \int_0^1 ((rp + sq) + (ps - qr)i)dt = \alpha(f(t), h(t)) + \beta(g(t), h(t)).$$

ii) $(f, g) = \int_0^1 (u + vi)(r - is)dt = \int_0^1 ((ur + vs) + (rv - us)i)dt = \int_0^1 (ur + vs)dt + i \int_0^1 (rv - us)dt =$

$$= \overline{\int_0^1 (ur + vs)dt - i \int_0^1 (us - rv)dt} = \overline{\int_0^1 (ur + vs)dt + i \int_0^1 (us - rv)dt} = \overline{\int_0^1 ((ur + vs) + (rv - us)i)dt}$$

$$= (g(t), f(t)).$$

iii) $(f, f) = \int_0^1 (u^2 + v^2)dt; > 0$, si $f \neq 0$.

†.

TEO1 El producto interior tiene las siguientes propiedades:

$\forall\, x, y, z \in V,\ c \in k$:

a) Si $x = 0$, entonces $(x, x) = 0$.

b) $(x, y + z) = (x, y) + (x, z)$.

c) $(x, cy) = \bar{c}\,(x, y)$.

d) Si $(x, y) = (x, z)\ \ \forall x \in V$, entonces $y = z$.

Dem *a*) $0 + (0, 0) = (0, 0) = (0 + 0, 0) = (0, 0) + (0, 0)$. $\therefore\ (0, 0) = 0$.

b) $(x, y + z) = \overline{(y + z, x)} = \overline{(y, x) + (z, x)} = \overline{(x, y) + (x, z)} = (x, y) + (x, z)$.

c) $(x, cy) = \overline{(cy, x)} = \overline{c\,(y, x)} = \bar{c}\,\overline{(y, x)} = \bar{c}\,(x, y)$.

d) Consideremos $y - z \in V$.

$(y - z, y) = (y - z, z) \Rightarrow (y, y) - (z, y) - (y, z) + (z, z) = 0$.

Pero $(y - z, y - z) = (y, y) - (z, y) - (y, z) + (z, z) = 0\ \ \therefore\ y - z = 0 \Rightarrow y = z$.

†.

DEF 2 En el caso general de un espacio con producto interior, se puede definir a partir del producto interior una norma, y a partir de esta una distancia. Precisaremos ahora estos dos conceptos y veremos como derivarlos en el caso particular de R^2.

Dado $x \in V$, definimos $\|x\| = (x, x)^{1/2}$, y así definida, la función

$\|\ \| : V \to R$ tiene las propiedades usuales de una norma, a saber:

i) $\|x\| \geq 0$; $\|x\| = 0 \Leftrightarrow x = 0$.

ii) $\|ax\| = |a| \|x\|$.

iii) $\|x + y\| \leq \|x\| + \|y\|$.

Dem i) $\|x\| = (x, x)^{1/2} \geq 0$; $(x, x)^{1/2} = 0 \Leftrightarrow (x, x) = 0 \Leftrightarrow x = 0$.

ii) $\|ax\| = (ax, ax)^{1/2} = ((a)^2 (x, x))^{1/2} = |a| \cdot \|x\|$

iii) $\|x + y\|^2 = (x + y, x + y) = (x, x + y) + (y, x + y) = (x, x) + (y, x) + (x, y) + (y, y) =$

$= (x, x) + (y, x) + (x, y) + (y, y) \leq \|x\|^2 + 2(\|x\| \|y\|) + \|y\|^2 = (\|x\| + \|y\|)^2$.

(Ya que, para el caso real $(x, y) \leq \|x\| \|y\|$. (Ver teorema 2),

y en el caso complejo, $(y, x) + (x, y) = \overline{(x, y)} + (x, y) = 2\mathrm{Re}\,((x, y)) \leq$

$\leq 2\|x\| \|y\|)$ †.

Un espacio dotado de una norma se llama ***espacio normado.***

Ejemplo2: Daremos ahora algunos ejemplos de normas, considerando como definición las propiedades i) ii) y iii), que las caracterizan.

1) Dado $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, definimos $\|x\| = \sum_{i=1}^{n} x_i^2$

2) Dado $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, definimos $\|x\| = \sum_{i=1}^{n} |x_i|$, donde $|\ |$ es el valor absoluto usual definido en $\mathbb{R}^n$.

3) Dado $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, definimos $\|x\| = \max \{|x_i|\}_{i=1}^{n}$.

En estos tres casos es relativamente fácil probar que la función definida es una norma.

Una vez definida la norma, derivaremos la **métrica** o **distancia** inducida por ella:

Dados dos puntos $x, y \in V$, definimos la distancia entre x, y como $d(x, y) = \|x - y\|$.

Así definida, la función $d : V \times V \to \mathbb{R}$ tiene las propiedades usuales de una métrica, que son:

i) $d(x, y) \geq 0$; $d(x, y) = 0 \Leftrightarrow x = y$

ii) $d(x, y) = d(y, x)$.

iii) $d(x, y) \leq d(x, z) + d(z, y) \quad \forall x, y, z \in V$.

Dem i) $d(x, y) = \|x - y\| \geq 0$; $d(x, y) = \|x - y\| = 0 \Leftrightarrow x - y = 0 \Leftrightarrow x = y$.

ii) $d(x, y) = \|x - y\| = |-1| \|x - y\| = \|(-1)(x - y)\| = \|y - x\| = d(y, x)$.

iii) $d(x, y) = \|x - y\| = \|x - z + z - y\| \leq \|x - z\| + \|z - y\| = d(x, z) + d(y, z) =$

$= d(x, z) + d(z, y)$. †.

*Un espacio dotado de una distancia se llama **espacio métrico**.*

Ejemplo 3: Daremos ahora unos ejemplos de espacios métricos.

1) $V = \mathbb{R}^n$, $d(x, y) = \|x - y\|$.

2) V subespacio de $\mathbb{R}^n$, $d(x, y) = \|x - y\|$. (V se llama entonces subespacio métrico de $\mathbb{R}^n$).

3) $V \neq \emptyset$, $d(x, y) = \begin{cases} 0, & \text{si } x = y \\ 1, & \text{si } x \neq y \end{cases}$

A esta métrica se le llama *metrica discreta.*

4) $V = \mathbb{R}^2$, $d(x, y) = \max \{ |x_1 - y_1|, |x_2 - y_2| \}$.

5) $V = \mathbb{R}^2$, $d(x, y) = |x_1 - y_1| + |x_2 - y_2|$.

6) $V = (\{x_i\}; i \in \mathbb{N}, x_i \in \mathbb{R}, \sum_{i=1}^{\infty} x_i^2 < \infty)$,

$$d(x, y) = \sqrt{\sum_{i=1}^{\infty} (y_i - x_i)^2} .$$

A este espacio se le denota en análisis usualmente como ℓ_2.

7) $V = (x : [0,1] \to \mathbb{R}$; x es continua),

$$d(x, y) = \sqrt{\int_0^1 (x(t) - y(t))^2 dt}$$

8) $V = (x : [0,1] \to \mathbb{R}$; x es continua),

$$d(x, y) = \max \{ |x(t) - y(t)|; t \in [0,1] \}$$

9) $V = (x : [0,1] \to \mathbb{R}^2$; x es continua, $x(0) = x(1)$),

$$d(x, y) = \max \{ |x(t) - y(t)|; t \in [0,1] \}$$

Obs1: Dos funciones distintas pueden tener imágenes iguales, pero tener distancia distinta de 0. Por ejemplo considérense $x, y : [0,1] \to \mathbb{R}^2$, $x(t) = (\cos(2\pi t), \operatorname{sen}(2\pi t))$, $y(t) = (\cos(4\pi t), \operatorname{sen}(4\pi t))$.

Entonces $d(x, y) = 2$, pero las dos tienen imagen $S^1 = \{x \in \mathbb{R}^2; \|x\| = 1\}$.

9) $V = (f : B \neq \varnothing \to \mathbb{R}; f$ es acotada)

$$d(f, g) = \sup \{ |f(t) - g(t)|; t \in B \}.$$

Obs2: El inciso (3) muestra como darle estructura de espacio métrico a cualquier espacio no vacío. Los incisos (6) y (7) muestran que al mismo espacio pueden dársele métricas no discretas diferentes. De aquí en adelante, $\mathbf{R}^n$ denotará siempre al espacio métrico del ejemplo 1.

TEO 1 Sea V un espacio con producto interior. Entonces $\forall\, x, y \in V$ y $c \in k$,

$|(x, y)| \leq \|x\| \|y\|$ (Desigualdad de Cauchy-Schwarz-Buniakowsky).

Dem: Si $x = 0$ ó $y = 0$, se cumple trivialmente la igualdad. Supongamos entonces que $x \neq 0 \neq y$, y consideremos al elemento $a = (x\|y\| - y\|x\|)$.

$(x\|y\| - y\|x\|, x\|y\| - y\|x\|) = (x\|y\|, x\|y\|) - (x\|y\|, y\|x\|) - (x\|x\|, y\|y\|) +$

$+ (y\|x\|, y\|x\|) = (x, x)\|y\|^2 - (x, y)\|x\|\|y\| - (x, y)\|x\|\|y\| + (y, y)\|x\|^2.$

Entonces $0 \leq \|a\|^2 = \|x\|^2\|y\|^2 - 2(x, y)\|x\|\|y\| + \|x\|^2\|y\|^2$

$\Rightarrow 2\|x\|^2\|y\|^2 \geq 2(x, y)\|x\|\|y\| \Rightarrow (x, y) \leq \|x\|\|y\|$ .... (1)

Considerando ahora al elemento $b = (x\|y\| - y\|x\|)$, y siguiendo una argumentación análoga a la anterior, llegamos a que :

$-\|x\|\|y\| \leq (x, y)$ .... (2)

Combinando las igualdades (1) y (2), concluímos que

$|(x, y)| \leq \|x\|\|y\|$

†.

Obs 1 : A partir del producto punto en un espacio, y las definiciones de los conceptos primarios se puede reconstruir la geometría euclidiana :

Se llama geometría plana de Euclides a un sistema que consta de dos conjuntos:

$\mathcal{P}$ el conjunto de los puntos, y $\mathcal{R}$ el conjunto de las rectas, (a partir de los cuales se definen el conjunto de segmentos, "Seg.", el de ángulos, "Ang." y otros conceptos, como triángulos y lados de una recta, entre otros), con las relaciones de :

Incidencia $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{R}$,

Congruencia entre segmentos, $\mathcal{C}_1 \subseteq Seg. \times Seg.$,

Congruencia entre ángulos, $\mathcal{C}_2 \subseteq Ang. \times Ang.$

Estar entre, $\mathcal{E} \subseteq \mathcal{P} \times (\mathcal{P} \times \mathcal{P})$;

que cumple con los axiomas de Hilbert :

A_1 Dos puntos distintos A y B determinan una única recta.

A_2 Toda recta tiene al menos dos puntos.

B_1 Si A, B y C son puntos de una recta y B está entre A y C, entonces B está entre C y A.

B_2 Si A y C son dos puntos de una recta, entonces existen B y D tales que B está entre A y C, y C está entre A y D.

B_3 De cualesquiera tres puntos situados sobre una recta, hay uno y sólo uno que está entre los otros dos.

B_4 (Separación de planos) Para toda recta ℓ, y para cualesquiera puntos A, B y C que no están en ℓ,

i) Si A y B están del mismo lado de ℓ y B y C están del mismo lado de ℓ, entonces A y C están del mismo lado de ℓ.

ii) Si A y B están en lados opuestos de ℓ y B y C están en lados opuestos de ℓ, entonces A y C están del mismo lado de ℓ.

C_1 Dado un segmento $\overline{AB}$ y un punto A', sobre toda recta que pasa por A' existen dos puntos B_1 y B_2 tales que A' está entre B_1 y B_2 y el segmento $\overline{AB}$ es congruente a cada uno de los segmentos $\overline{AB}_1$ y $\overline{AB}_2$.

C_2 Sean $\overline{AB}$, $\overline{A'B'}$ y $\overline{A''B''}$ segmentos. Si el segmento $\overline{A'B'}$ es congruente al segmento $\overline{AB}$, y el segmento $\overline{A''B''}$ es congruente al segmento $\overline{AB}$, entonces el segmento $\overline{A'B'}$ es congruente al segmento $\overline{A''B''}$.

C_3 Si B es un punto del segmento $\overline{AC}$ y B' es punto del segmento $\overline{A'C'}$, y el segmento $\overline{AB}$ es congruente al segmento $\overline{A'B'}$, y el segmento $\overline{BC}$ es congruente al segmento $\overline{B'C'}$, entonces el segmento $\overline{AC}$ es congruente al segmento $\overline{A'C'}$.

C_4 Sea $\angle$ (h, k) un ángulo dado; $\mathcal{a}$ una recta, α uno de los semiplanos definidos por $\mathcal{a}$ y h' un rayo sobre $\mathcal{a}$. Entonces existe un único rayo k' tal que $\angle$ (h, k) es congruente a $\angle$ (h', k') y tal que un punto de k' (al menos) está en el semiplano α.

C_5 Cualquier ángulo es congruente consigo mismo.

C_6 (Criterio LAL). Sean ABC y A'B'C' dos triángulos tales que el segmento $\overline{AB}$ es congruente al segmento $\overline{A'B'}$, y el segmento $\overline{AC}$ es congruente al segmento $\overline{A'C'}$ y el $\angle$ BAC

es congruente al $\angle$ B'A'C'. Entonces el $\angle$ ABC es congruente al $\angle$ A'B'C' y el $\angle$ ACB es congruente al $\angle$ A'C'B'.

D_1 (Postulado de Arquímedes).

Sean A, B y A_1 tres puntos colineales, A_1 entre A y B. Se construyen los puntos $A_2, A_3, A_4, \ldots$ tales que A_1 está entre A y A_2, A_2 está entre A_1 y A_3, A_3 está entre A_2 y A_4, etcétera, y tales que los segmentos $\overline{AA_1}$, $\overline{A_1A_2}, \overline{A_2A_3}, \ldots$ son congruentes. Entonces la sucesión de puntos $A_2, A_3, A_4, \ldots$ contiene un punto A_n tal que B está entre A y A_n.

D_2 (Postulado de Dedekind)

Sea $\overline{AB}$ un segmento y sean $\{A_n\}$, $\{B_n\}$ dos sucesiones de puntos interiores de $\overline{AB}$ con las propiedades siguientes:

a) El segmento $\overline{A_nB_n}$ está en el interior del segmento $\overline{A_{n-1}B_{n-1}}$, para toda n.

b) No existe ningún segmento cuyos puntos extremos pertenezcan a todos los segmentos $\overline{A_nB_n}$.

Entonces existe un único punto x común a todods los segmentos $\overline{A_nB_n}$.

E_1 (Versión "Playfair") Sea ℓ una recta y P un punto que no está sobre ℓ. Entonces existe una única recta que pasa por P y que no interseca a ℓ.

Procederemos ahora a definir los conceptos primarios de esta geometría a partir de las propiedades de espacio vectorial de $\mathbf{R}^2$ y del producto punto definido en él. Posteriormente demostraremos, como ejemplo, un axioma de cada uno de los grupos de axiomas de Hilbert (de conexión, de orden, de congruencia, de continuidad y axioma de las paralelas), y finalmente demostraremos un teorema de gran importancia en la geometría Euclidiana.

DEF 3 $\mathcal{P} = \mathbf{R}^2 = \{(x, y);\ x \in \mathbf{R}, y \in \mathbf{R}\}$. Es decir, los puntos en nuestra geometría son exactamente los pares ordenados de números reales.

DEF 4 $\mathcal{R} = \{ (P_0 + t\,\bar{a}\,; t \in \mathbf{R}); P_0 \in \mathbf{R}^2, \bar{a} \in \mathbf{R}^2 - \{0\}\}$. Es decir, un conjunto ℓ de puntos de $\mathbf{R}^2$ se llama recta si hay un punto $P_0 = (x_0, y_0) \in \mathbf{R}^2$ y un vector no nulo $\bar{a} = (a_1, a_2) \in \mathbf{R}^2$ tales que $\ell = \{P_0 + t\,\bar{a}\,; t \in \mathbf{R}\}$.

Usaremos la notación $\ell\,(P_0\,;\,\bar{a})$ para denotar a la recta que pasa por P_0 en la dirección $\bar{a}$.

DEF 5 La relación de "incidencia" o "estar en" $(\mathcal{I} \subseteq \mathcal{P} \times \mathcal{R})$., se define como sigue :

$(P, \ell\,(P_0\,;\bar{a})) \in \mathcal{I} \Leftrightarrow \exists\ t_0 \in \mathbf{R}\ \ni\ P = P_0 + t_0\,\bar{a}$

(e.d., P está en ℓ sii P satisface la ecuación de ℓ).

DEF 6 La relación de "estar entre" $(\mathcal{E} \subseteq \mathcal{P} \times (\mathcal{P} \times \mathcal{P}))$ se define como sigue :

Si A, B y C son puntos distintos de una recta $\ell\,(P_0\,;\,\bar{a})$, entonces $\exists\ t_1, t_2, t_3 \in \mathbf{R}\ \ni$

$A = P_0 + t_1\,\bar{a}$

$B = P_0 + t_2\,\bar{a}$

$C = P_0 + t_3\,\bar{a}$

Diremos entonces que B está entre A y C si t_2 está entre t_1 y t_3 , e.d.

$t_1 < t_2 < t_3$ ó $t_3 < t_2 < t_1$.

DEF 7 Sean A y $B \in \mathbf{R}^2$. Entonces $\overline{AB} = \{P \in \mathbf{R}^2; P = A + t\,(B - A), t \in [0, 1]\}$ es el segmento con extremos A y B.

Obs : Si $t = 0$, $P = A$. Si $t = 1$, $P = B$, y para todo $t \in (0,1)$, P está entre A y B.

DEF 8 Sean A y $B \in \mathbf{R}^2$, $A \neq B$. Entonces $AB = \{P \in \mathbf{R}^2; P = A + t\,(B - A), t \in [0, \infty)\}$ es el rayo $\overrightarrow{AB}$.

Asociamos a los segmentos en $\mathbb{R}^2$ una medida por medio de la norma euclidiana

$$m(\overline{AB}) = \|B - A\|$$

Obs : Si $\ell(P_0; \hat{u})$ es una recta generada por un vector unitario $\hat{u}$, entonces

i) Si $P \in \ell$, $P = P_0 + t\hat{u}$, entonces $m(\overline{P_0P}) = |t|$

ii) Si A, B y $C \in \ell$ y B está entre A y C, entonces

$$m(\overline{AB}) + m(\overline{BC}) = m(\overline{AC}).$$

DEF 9 Sea $\overline{AB}$ y $\overline{CD}$ segmentos. Decimos que $\overline{AB}$ es congruente con $\overline{CD}$ si :

$$m(\overline{AB}) = m(\overline{CD}).$$

DEF 10 Sea $\bar{a}$ y $\bar{b}$ vectores diferentes de cero. Entonces se dice que el ángulo que forman, $\angle(\bar{a}, \bar{b})$, es aquel cuya medida θ satisface la ecuación $\cos\theta = \dfrac{\bar{a}\cdot\bar{b}}{\|\bar{a}\|\|\bar{b}\|}$ y que está en el intervalo $[0, 2\pi)$.

Obs : Si en un rayo se cambia el vector que lo genera, el nuevo vector debe ser múltiplo positivo del anterior, y por lo tanto, si $\bar{a}$ y $\bar{b}$ son generadores de los lados de un ángulo, y $\bar{a}'$ y $\bar{b}'$ también, resulta que $\bar{a} = h\bar{a}'$ y $\bar{b} = k\bar{b}'$, $h, k \in \mathbb{R}^+$, y entonces

$$m(\angle(\bar{a}, \bar{b})) = \cos^{-1}\frac{\bar{a}\cdot\bar{b}}{\|\bar{a}\|\|\bar{b}\|} = \cos^{-1}\frac{hk(\bar{a}\cdot\bar{b})}{hk\|\bar{a}\|\|\bar{b}\|} = \cos^{-1}\frac{\bar{a}'\cdot\bar{b}'}{\|\bar{a}'\|\|\bar{b}'\|} = m(\angle(\bar{a}', \bar{b}')).$$

es decir que la medida del ángulo es independiente de los vectores que se usen para generar sus lados.

DEF 11 Sean $\angle(\bar{a}, \bar{b})$ y $\angle(\bar{c}, \bar{d})$ dos ángulos. Decimos que $\angle(\bar{a}, \bar{b})$ es congruente con $\angle(\bar{c}, \bar{d})$ $(\angle(\bar{a}, \bar{b}) \cong \angle(\bar{c}, \bar{d}))$ si $m(\angle(\bar{a}, \bar{b})) = m(\angle(\bar{c}, \bar{d}))$

DEF 12 Sea $\ell(P_0; \hat{u})$ una recta y $N = \hat{u}^{\perp}$ su "normal" (si $\hat{u} = (a, b)$, entonces $N = (-b, a)$, y así $\|N\| = \|\hat{u}\| = 1$.

Entonces ℓ se puede describir como $\ell = \{P \in \mathbf{R}^2 ; N \cdot (P - P_0) = 0\}$.

$(P \in \ell \Leftrightarrow \exists\ t_0 \in \mathbf{R} \ni P = P_0 + t_0 \hat{u} \Leftrightarrow N \cdot (P - P_0) = t_0 (N \cdot \hat{u}) = 0)$.

Sean $\Sigma_+ = \{P \in \mathbf{R}^2 ; N \cdot (P - P_0) > 0\}$, y

$$\Sigma_- = \{P \in \mathbf{R}^2 ; N \cdot (P - P_0) < 0\}.$$

Entonces Σ_+ y Σ_- son los semiplanos determinados por ℓ, o bien los lados de ℓ.

Decimos que P y Q están del mismo lado de la recta ℓ si ambos están en el mismo semiplano. En caso contrario se dice que están en lados diferentes.

Obs : Es claro que para todo $P \in \mathbf{R}^2$ se cumple una y sólo una de las siguientes condiciones:

$P \in \ell$, $P \in \Sigma_+$ ó $P \in \Sigma_-$. Además, cada uno de estos semiplanos es un conjunto convexo.

Demostraremos ahora un axioma de cada uno de los grupos de axiomas de Hilbert :

TEO 3 (A_3) Existen al menos tres puntos que no están alineados.

Dem Sean P y Q distintos en $\mathbf{R}^2$ y sea $\ell(P ; (Q - P))$ la única recta que los contiene (A_1).

Entonces, como $P \neq Q$, $(Q - P) = (a, b) \neq (0, 0) \Rightarrow N = (-b, a) \neq (0, 0)$. Sea $R = P + N$.

Así, $R \notin \ell$, ya que si $R \in \ell$, $R = P + N = P + t_0 (Q - P)$, p. a. $t_0 \in \mathbf{R} \Rightarrow N = t_0 (Q - P) \Rightarrow$

$N \cdot N = t_0 (N \cdot (Q - P)) = 0 \quad \forall$ (Ya que $N \neq 0 \Rightarrow N \cdot N = \|N\|^2 > 0$).

$\therefore R = (P + N) \notin \ell$, y dado que ℓ es la única recta que contiene tanto a P como a Q,

P, Q y R no pueden estar alineados.

TEO 4 (B_3) De cualesquiera tres puntos situados sobre una recta, hay uno y sólo uno que está entre los otros dos.

Dem Sean A, B y $C \in \ell$, t_1, t_2 y $t_3 \in \mathbf{R}$ sus parámetros. Entonces, con base en las propiedades de los reales, sabemos que hay uno y sólo uno que está entre los otros dos.

TEO 5 (C_2) Sean $\overline{AB}$, $\overline{A'B'}$ y $\overline{A''B''}$ segmentos. Entonces $\overline{AB} \equiv \overline{A'B'}$ y $\overline{AB} \equiv \overline{A''B''} \Rightarrow$ $\overline{A'B'} \equiv \overline{A''B''}$.

Dem El resultado es trivial, ya que las congruencias geométricas se traducen en igualdades entre números.

TEO 6 (D_2) Sea $\overline{AB}$ un segmento y sean $\{A_n\}$, $\{B_n\}$ dos sucesiones de puntos interiores de $\overline{AB}$ con las propiedades siguientes:

a) El segmento $\overline{A_n B_n}$ está en el interior del segmento $\overline{A_{n-1} B_{n-1}}$, para toda n.

b) No existe ningún segmento cuyos puntos extremos pertenezcan a todos los segmentos $\overline{A_n B_n}$.

Entonces existe un único punto x común a todods los segmentos $\overline{A_n B_n}$.

Dem Para demostrar este teorema requerimos del axioma de los encajes de intervalos, que se cumple en $\mathbf{R}$ y que dice que:

Si $\{[a_n, b_n]; n \in \mathbf{N}\}$ es una colección de intervalos cerrados tales que para toda $n \in \mathbf{N}$, $a_n < b_n$ y $[a_n, b_n] \supseteq [a_{n+1}, b_{n+1}]$, entonces $\bigcap_{n \in \mathbf{N}} [a_n, b_n] \neq \varnothing$.

Entonces, regresando al axioma D_2, notamos que si la recta que contiene a todos los segmentos $[a_n, b_n]$, $n \in \mathbf{N}$ es $\ell(P_0; \hat{d})$, entonces para cada a_n existe un $s_n \in \mathbf{R}$ tal que $a_n = P_0 + s_n \hat{d}$. Y análogamente, para cada b_n existe un $t_n \in \mathbf{R}$ tal que

$b_n = P_0 + t_n a$.^ Además, las hipótesis implican que los intervalos cerrados $[s_n, t_n] \neq \varnothing$ satisfacen las hipótesis del axioma de los encajes de intervalos.

$$\therefore \bigcap_{n \in \mathbb{N}} [s_n, t_n] \neq \varnothing \Rightarrow \bigcap_{n \in \mathbb{N}} [a_n, b_n] \neq \varnothing.$$

Además no puede haber dos puntos en la intersección de los $[a_n, b_n]$, ya que entonces habría un intervalo cerrado no vacío contenido en todos los $[s_n, t_n]$, el cual define un segmento contenido en todos los segmentos $[a_n, b_n]$, lo que viola la segunda hipótesis del axioma. Así, si llamamos x al único punto que está en todos los $[a_n, b_n]$, tenemos:

$$\therefore \bigcap_{n \in \mathbb{N}} [a_n, b_n] = \{x\}$$

TEO.7 (E_1) Si ℓ es una recta y P un punto que no está en ℓ, entonces existe una única recta ℓ' tal que :

i) $P \in \ell'$

ii) ℓ' es paralela a ℓ.

Obs: La demostración de este axioma, que fue tan controvertido en el pasado, resulta ser una cuestión trivial en esta construcción de la geometría plana. En efecto :

Dem Sea $\ell(P_0; \vec{a})$ una recta, y $P \notin \ell$ un punto. Definimos $\ell' = \ell'(P; \vec{a})$.

Evidentemente se trata de una recta que pasa por P y que es paralela a ℓ.(Si $Q \in \ell \cap \ell'$, entonces $Q = P_0 + t_1 \vec{a} = P + t_2 \vec{a} \Rightarrow (P - P_0) = t_3 \vec{a}$, p.a. $t_3 \in \mathbb{R} \Rightarrow P = P_0 + t_3 \vec{a}$ $\forall$). Para demostrar la unicidad, supongamos que $\ell''(Q; \vec{b})$ es otra recta con tales propiedades. Entonces, puesto que pasa por P, puede tomarse este como punto de apoyo, es decir : $\ell'' = \ell''(P; \vec{b})$, y como ℓ'' es paralela a ℓ; $\vec{b} \parallel \vec{a}$, y por lo tanto $\ell'' = \ell''(P; \vec{a}) = \ell'$.

TEO 8 (Axioma de Pasch)

Sean A, B y C tres puntos que no están alineados; y sea ℓ una recta que no pasa por ninguno de estos puntos. Entonces, si la recta ℓ pasa a través de un punto del segmento $\overline{AB}$, también pasará a través de un punto del segmento $\overline{BC}$ o por un punto del segmento $\overline{AC}$.

Dem Dado que la recta ℓ pasa a través de un punto del segmento $\overline{AB}$, entonces A y B están en lados opuestos con respecto a ℓ, es decir, están en diferente semiplano. Además, como ℓ no pasa por ninguno de los tres puntos, C no está sobre ℓ y por lo tanto debe estar en alguno de los semiplanos generados por ℓ.

Supongamos que $B \in \Sigma_-$ y consideremos que C está del mismo lado que B. Entonces $C \in \Sigma_-$ y $A \in \Sigma_+$. Como los semiplanos son conjuntos convexos, resulta que el segmento $\overline{BC}$ está contenido en Σ_-.

Entonces la intersección del segmento del segmento $\overline{AC}$ con ℓ es no vacía (si lo fuera, A estaría en Σ_- ó C estaría en Σ_+, lo cual no es cierto). En caso de que C estuviera del mismo lado que A, el segmento $\overline{AC}$ estaría contenido en Σ_+, y así la intersección del segmento $\overline{BC}$ con ℓ sería diferente del vacío.

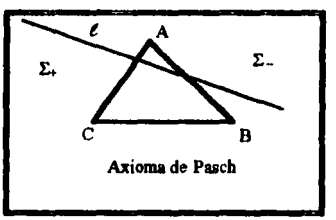

FIGURA 1

Obs 2: Un producto punto induce, de la forma que ya vimos, una norma, y una norma induce una métrica.Cabe preguntarse si habrá normas que no se deriven de un producto punto, o métricas que no se deriven de una distancia. Aquí damos un ejemplo de cada una de estas situaciones, y para esto, probaremos primero un resultado que nos será útil.

PROPOSICIÓN 1 En todo espacio vectorial sobre el campo $\mathbf{R}$ con una norma inducida por un producto interior, se cumple la siguiente igualdad:

$(x, y) = \frac{1}{4}\|x + y\|^2 - \frac{1}{4}\|x - y\|^2$. ,que se conoce como la *identidad polar*.

Dem $\frac{1}{4}\|x + y\|^2 - \frac{1}{4}\|x - y\|^2 = \frac{1}{4}(x + y, x + y) - \frac{1}{4}(x - y, x - y) =$

$\frac{1}{4}((x, x + y) + (y, x + y)) - \frac{1}{4}((x, x - y) - (y, x - y)) = \frac{1}{4}((x, x) + (x, y) + (x, y) + (y, y)) -$

$\frac{1}{4}((x, x) - (x, y) - (x, y) + (y, y)) = \frac{1}{4}(x, y) + \frac{1}{4}(x, y) + \frac{1}{4}(x, y) + \frac{1}{4}(x, y) = (x, y).$

†.

Una vez probado este resultado pasamos a los ejemplos de normas y distancias no inducidas.

Ejemplo 5: Sea $V = \mathbf{R}^2$.

Definimos $\|\ \|: \mathbf{R}^2 \to \mathbf{R}$ como en el ejemplo 3.3.

AFIRMACIÓN: Así definida, $\|\ \|: \mathbf{R}^2 \to \mathbf{R}$ es una norma que no puede derivarse de un producto interior.

Veamos primero que $\|\ \|$ cumple las propiedades de norma:

i) $\|x\| = \max\{|x_1|, |x_2|\} \geq 0$, ya que $|x_1|, |x_2| \geq 0$. $\|x\| = 0 \Leftrightarrow \max\{|x_1|, |x_2|\} = 0$

$\Leftrightarrow |x_1| = |x_2| = 0 \Leftrightarrow x_1 = x_2 = 0 \Leftrightarrow x = 0.$

ii) $\|ax\| = \|(ax_1, ax_2)\| = \max\{|ax_1|, |ax_2|\} = \max\{|a||x_1|, |a||x_2|\} =$

$= |a| \max\{|x_1|, |x_2|\} = |a| \|x\|.$

iii) $\|x + y\| = \|(x_1 + y_1, x_2 + y_2)\| = \max\{|x_1 + y_1|, |x_2 + y_2|\} \leq$

$\max\{|x_1| + |y_1|, |x_2| + |y_2|\} \leq \max\{|x_1|, |x_2|\} + \max\{|y_1|, |y_2|\} = \|x\| + \|y\|.$

†.

Ahora veremos que $\| \ \|$ no proviene de un producto interior.

Sean $x = (1, \frac{1}{2})$

$y = (1, \frac{1}{3})$.

Si $\| \ \|$ viniera de un producto interior $(,)$, se cumpliría la identidad polar, e.d.,

$$(x, y) = \tfrac{1}{4}\|x + y\|^2 - \tfrac{1}{4}\|x - y\|^2 = \tfrac{1}{4}(2)^2 - \tfrac{1}{4}\left(\tfrac{1}{6}\right)^2 = \tfrac{4}{4} - \tfrac{1}{144} = \tfrac{143}{144}$$

Por otro lado, $2x = (2,1) \Rightarrow \|2x + y\| = 3$; $\|2x - y\| = 1 \Rightarrow (2x, y) = \frac{9}{4} - \frac{1}{4} = 2$

pero por el punto (b) de la definición de producto interior, $(2x, y) = 2(x, y)$,

e.d. $2 = 2\left(\frac{143}{144}\right)$ $\forall$ $\therefore$ $\| \ \|$ no puede ser inducida por un producto interior.

†.

Ejemplo 4: Sea V un espacio vectorial sobre R con más de un elemento, d^* la métrica discreta definida en el ejemplo 4.3.

AFIRMACIÓN : d^* no es inducida por una norma.

$\forall\, x, y \in V,\ x \neq y \Rightarrow 2x \neq 2y,$

e.d., $d^*(x, y) = 1 \Rightarrow d^*(2x, 2y) = 1$. Pero si d^* proviniera de una norma, e.d. si $\forall x, y \in V$, $d^*(x, y) = \|x - y\|$, con $\| \ \| : V \to R$ una norma cualquiera, entonces se cumpliría que si $x \neq y$, $1 = d^*(2x, 2y) = \|2x - 2y\| = 2\|x - y\| = 2\, d^*(x, y) = 2$ $\forall$.

$\therefore$ d^* no proviene de una norma.

†.

Es natural suponer que las distancias definidas en el ejemplo 4 dan lugar a geometrías que no coinciden con la geometría euclidiana. Ejemplificaremos un poco esta situación.

DEF 13 Sea (X, d) un espacio métrico.

Sean $a, b, c \in X$. Entonces el conjunto $T = \{a, b, c\}$ se llama **triángulo**. (con lados $\{a, b\}$, $\{b, c\}$, $\{c, a\}$, cuyas medidas o longitudes son $d(a, b)$, $d(b, c)$ y $d(c, a)$ respectivamente).

DEF 14 Sea O un elemento arbitrario de X y r un número real no negativo.

Entonces $\mathcal{C}_r(O) = \{P \in X, d^*(P, O) = r\}$ es la **circunferencia de radio r con centro en O**,

$\{P \in X; d^*(P, O) \leq r\}$ **es el círculo de radio r con centro en O**.

¿Cómo son estos conjuntos con las distintas métricas del ejemplo 4? Veamos algunos ejemplos.

1) Con la métrica del ejemplo 4.4, la circunferencia unitaria ($\mathcal{C}_1(0) = \{(x, y) \in R^2;$ $d((x, y), 0 = 1)\}$, e.d. los puntos (x, y) del plano cumplen con máx $\{|x|, |y|\} = 1)$---(*) es como se ve en la figura 2. Para demostrar esto trataremos a los cuatro cuadrantes del plano por separado:

Primer cuadrante : $x \geq 0, y \geq 0$.

En este caso la expresión (*) se reduce a máx $\{x, y\} = 1$.

Caso 1 : $x = y$.

Es obvio que en este caso el único punto del plano que cumple con (*) es el $(1, 1)$.

Caso 2 : $x > y$.

En este caso $(x, y) \in \mathcal{C}_1(0) \Leftrightarrow x = 1$. Análogamente, si $x < y$, $(x, y) \in \mathcal{C}_1(0) \Leftrightarrow$ $y = 1$.

Hemos visto hasta ahora que la circunferencia en el primer cuadrante consta de todos los puntos (x, y) ∋ $x = 1$ y $0 \leq y \leq 1$ ó $y = 1$ y $0 \leq x \leq 1$. (Ver figura 2)

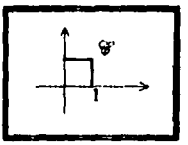

FIGURA 2

Segundo cuadrante : $x < 0$, $y > 0$.

En este caso la expresión (*) se reduce a máx $(-x, y) = 1$.

Caso 1 : $-x = y$.

Es obvio que en este caso el único punto del plano que cumple con (*) es el $(-1, 1)$.

Caso 2 : $-x > y$.

En este caso $(x, y) \in \mathcal{C}_1(0) \Leftrightarrow -x = 1 \Leftrightarrow x = -1$. Análogamente, si $-x < y$, $(x, y) \in \mathcal{C}_1(0)$ $\Leftrightarrow$ $y = 1$. Así, la circunferencia en el segundo cuadrante consta de todos los puntos (x, y) ∋ $x = -1$ y $0 \leq y \leq 1$ ó $y = 1$ y $-1 \geq x \geq 0$.

El análisis en los dos cuadrantes que quedan es similar, y así concluímos que $\mathcal{B}_1(0)$ es como se muestra en la figura 3.

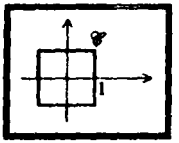

FIGURA 3

2) Con la métrica del ejemplo 4.5, la circunferencia unitaria ($\mathcal{B}_1(0) = \{(x, y) \in \mathbb{R}^2 ; |x|+|y|=1\}$) es como se ve en la figura 3. La demostración de esto es muy similar a la del ejemplo anterior, así que discutiremos únicamente el primer cuadrante.

$x \geq 0,\ y \geq 0.$

En este caso, $(x, y) \in \mathcal{B}_1(0) \Leftrightarrow x + y = 1 \Leftrightarrow y = -x$. Puesto en otras palabras, la "imagen" de la circunferencia en el primer cuadrante es precisamente la recta de pendiente -1 que pasa por el origen. Tomando en cuenta que el razonamiento es básicamente el mismo para los otros cuadrantes, concluímos que la circunferencia se vé así:

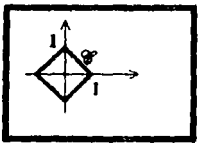

FIGURA 4

3) Con la métrica del ejemplo 4.8, la circunferencia unitaria $\mathcal{B}_1(0)$,

(donde $\mathbf{0}(t) = 0$

$\forall\, t \in [0, 1]$), es como se ve en la figura 4. La argumentación requerida por este ejemplo es distinta a las anteriores 2, pero es también muy sencilla:

Sea $x(t) \in V$. Entonces $x(t) \in \mathcal{B}_1(\mathbf{0}) \Leftrightarrow \max\{|x(t)|; t \in [0, 1]\} = 1 \Leftrightarrow$

$|x(t)| \leq 1$

$\forall\, t \in [0, 1]$, y $\exists\, t_0 \in [0, 1]$ ∍ $|x(t_0)| = 1$.

Es obvio que para cualquier punto (a, b) dentro de la franja delimitada por $x = 0$, $x = 1$, $y = -1$ y $y = 1$, existe un elemento de $\mathcal{B}_1(\mathbf{0})$ que "cae" dentro de ella (por ejemplo la función $x(t)$ tal que $x(t) = 1 \;\; \forall\, t \in ([0, 1] - \{a\})$, $x(a) = b$), así como lo es también que cualquier función que se salga de la franja, cuando menos en un punto, no puede ser elemento de la circunferencia.

Entonces la circunferencia efectivamente se puede representar así:

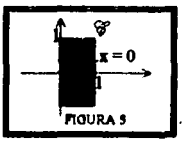

FIGURA 5

Obs 1 : No cualquier función que caiga dentro de la franja es un elemento de la circunferencia:

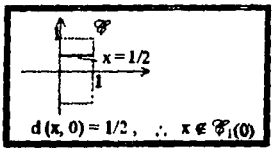

FIGURA 6

Obs 2 : El conjunto de todas las funciones que caen dentro de la franja es en realidad el círculo de radio 1 con centro en el 0.

Obs 3 : La circunferencia de radio 1 con centro en $y = \text{sen } x$, $x \in [0, 1]$ se puede representar así:

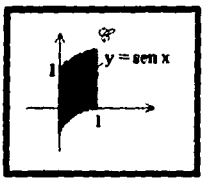

FIGURA 7

4) Veamos cómo es $\mathcal{B}_1(0)$, el círculo de radio 1 con centro en 0 con la métrica del ejemplo 4.9 (Aquí convenimos en que 0 es el elemento de V que asocia a todo punto del intervalo unitario el origen del plano, e.d. $0 : [0, 1] \to \mathbb{R}^2$, $0(x) = (0, 0) \quad \forall x \in [0, 1]$).

Así como en el ejemplo anterior, vemos que cualquier curva cerrada que pasa por el (0, 0) y que caiga dentro de D^1, el círculo unitario usual en $\mathbb{R}^2$,

($D^1 = \{(x, y) \in R^2 ; \sqrt{x^2+y^2} \leq 1\}$), puede ser vista como imagen de un elemento de V. Así, las imágenes de los elementos de $\mathcal{B}_1(0)$ "llenan" completamente a D^1, o mejor dicho, cualquier punto en D^1 es imagen de algún punto de [0, 1] bajo alguna función de V.

Por otro lado, vemos también que cualquier función f cuya imagen caiga dentro de D^1 es en efecto un elemento de $\mathcal{B}_1(0)$, ya que $\forall t \in [0, 1]$, $|f(t) - 0| = |f(t)| \leq 1$, $\Rightarrow$

$d(f, 0) = \text{máx}\{|f(t)|\} \leq 1 \Rightarrow f \in \mathcal{B}_1(0)$.

Entonces podemos representar a $\mathcal{B}_1(0)$ como se vé en la figura 8.

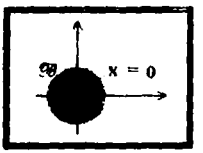

FIGURA 8

Obs 1: El dibujo de la circunferencia es el mismo, aunque hay funciones cuya imagen cae dentro de D^1 que no son elementos de ella. (ejemplo: $x(t) = (\frac{1}{2}\cos 2\pi t, \frac{1}{2}\text{sen } 2\pi t)$).

Obs 2: Los círculos alrededor de cualquier elemento de V distinto de el cero no se pueden dibujar tan exactamente :

Ejemplo : Sea $x \in V$, $x(t) = (\cos(2\pi t), \text{sen}(2\pi t))$.

Entonces las imágenes de las funciones que son elementos del círculo (con respecto a la métrica del ejemplo 4.9) de radio 1 con centro en x llenan todo $\mathcal{B}_2 = \{(y, z) \in R^2 ; \sqrt{y^2+z^2} \leq 2\}$. (Para cualquier punto $P \in \mathcal{B}_2$, $\exists f \in \mathcal{B}_1(x) \ni f(t) = P$ *p.a.* $t \in [0, 1]$).

pero no cualquier función cuya imagen caiga en $\mathcal{B}_2$ es en efecto un elemento de $\mathcal{C}_1(x)$, por ejemplo $x'(t) = (\cos(4\pi t), \operatorname{sen}(4\pi t))$, ya que entonces $d(x, x') = 2$.

Veamos ahora un poco de geometría según la métrica del ejemplo 4.3, la métrica discreta.

TEO 9 Todo triángulo "no degenerado" es equilátero.

Dem Si $T = \{a, b, c\}$ es un triángulo, y a, b y c son distintos (T es "no degenerado"), entonces $d^*(a, b) = d^*(b, c) = d^*(c, a) = 1$ †.

TEO 10 Sea $O \in X$ un punto cualquiera. Entonces

$$\mathcal{C}_1(O) = \begin{cases} \varnothing, \text{ si } 0 < r < 1 \\ X - \{O\}, \text{ si } r = 1 \\ \varnothing, \text{ si } r > 1 \end{cases}$$

Obs: En la métrica discreta, como ya vimos, todo círculo de radio distinto de uno es vacío. Como en general este caso no es de interés, podemos suponer siempre que se habla de circunferencias de radio 1, y así estas quedan determinadas por su centro.

TEO 11 Si $\mathcal{C}(P) \neq \mathcal{C}(P')$, e.d. $P \neq P'$, entonces $\mathcal{C}(P) = \mathcal{C}(P') - \{P\} \cup \{P'\}$. Puesto en palabras, las dos circunferencias coinciden en todos sus puntos salvo por los centros.

Dem Por el teorema anterior, y dado que no estamos en el caso trivial,

$$\mathcal{C}(P) = X - \{P\} = X - \{P'\} - \{P\} \cup \{P'\} = \mathcal{C}(P') \quad \dagger.$$

ULTRAMÉTRICAS

Observemos que la métrica discreta cumple una desigualdad más fuerte que la del triángulo, que es la siguiente $\forall\, a, b, c \in X,\ d^*(a,b) \leq \max\{d^*(a,c), d^*(c,b)\}$.

A las métricas que cumplen esta desigualdad se les llama **ULTRAMÉTRICAS**, o métricas no arquimedianas.

DEF 6 Sea E un espacio con una función $d: E \times E \to R$ que satisface, $\forall\, a, b, c \in E$, las siguientes propiedades.

i) $d(a,b) \geq 0$; $d(a,b) = 0 \Leftrightarrow a = b$.

ii) $d(a,b) = d(b,a)$

iii) $d(a,b) \leq \max\{d(a,c), d(c,b)\}$.

Entonces d es una **ultramétrica** y (E,d) es un **espacio ultramétrico**.

Obs: La condición (iii) de la definición es una condición más fuerte que la que se pide para que d sea una métrica, ya que $d(a,b) \leq \max\{d(a,c), d(c,b)\} \leq d(a,c) + d(c,b)$, por lo que toda ultramétrica es en particular métrica.

Definiremos ahora algunos objetos geométricos. Se definen los triángulos y los círculos de manera análoga a los casos antes vistos, y en general, como queremos una geometría derivada de la ultramétrica, adoptaremos únicamente los conceptos que puedan ser definidos a partir de ella. En algunos casos escogeremos, por lo tanto, de entre las definiciones de un concepto, aquella que dependa de la métrica.

DEF 15 Un **triángulo** es cualquier terna de puntos. Los **lados** del triángulo son las parejas de puntos obtenidas a partir de la terna, y en este caso los puntos de la pareja son los **extremos** del lado. La **longitud** de un lado es la distancia que hay entre sus extremos.

Obs: Si $\{A,B,C\} \subseteq E$ es un triángulo, la condición de ultramétrica garantiza que:

i) $a \leq$ máx $\{b, c\}$ $\qquad a = d(A,B)$

ii) $b \leq$ máx $\{a, c\}$; donde $\qquad b = d(B,C)$

iii) $c \leq$ máx $\{a, b\}$ $\qquad c = d(A,C)$

$\therefore$ en $\{a, b, c\} \subset \mathbf{R}$ no hay ningún número que sea mayor que los otros dos. Así, tiene que haber dos lados iguales y el tercero menor o igual. Es decir que, todos los triángulos son isósceles y "flacos", cosa que obviamente no pasa en la geometría euclidiana. (¿O sí?) Considere la siguiente "demostración":

Sea $\{A, B, C\}$ un triángulo cualquiera.

Trazamos la mediatriz del lado AB y le llamamos $\mathcal{M}$.

Trazamos la bisectriz del $\angle ACB$ y le llamamos $\mathcal{N}$.

Sea $P = \mathcal{M} \cap \mathcal{N}$. Trazamos PB y PA, y trazamos también por P una línea ortogonal al lado CB, que lo corta en Q, y una línea ortogonal al lado AC que lo corta en R. (Ver figura 9).

Ahora bien, PQ = PR, por ser $\mathcal{N}$ bisectriz de $\angle ACB$.

Por otro lado, PB = PA, por ser $\mathcal{M}$ mediatriz de AB.

Como además $\angle PQB = \angle PRA$, los triángulos $\{A, P, R\}$ y $\{B, P, R\}$ son semejantes.

$\therefore$ BQ = AR.

Análogamente, dado que los triángulos $\{C, P, Q\}$ y $\{C, P, R\}$ comparten dos lados y un ángulo, son semejantes $\Rightarrow$ QC = RC.

Así, BC = BQ + QC = AR + RC = AC

$\therefore$ $\{A, B, C\}$ es isósceles. ¡Todos los triángulos son isósceles!.

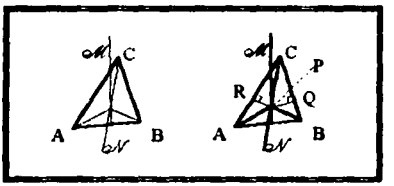

FIGURA 9

Obs : El procedimiento que usamos arriba para demostrar que dos lados del triángulo son iguales se puede volver a aplicar, y demostramos así que el tercer lado es igual a los primeros dos:

:"Corolario": Todos los triángulos son equiláteros. (Lo cual ya no nos sorprende)

DEF.16 Dados $O \in E$ y $r \geq 0$,

$\mathcal{C}_r(O) = \{P \in E ; d(O, P) = r\}$ es la circunferencia con centro en O y radio r.

$\text{Int}\mathscr{C}_r(O) = \{P \in E ; d(O, P) < r\}$ es el interior del circunferencia,

$\text{Ext}\mathscr{C}_r(O) = \{P \in E ; d(O, P) > r\}$ es el exterior del circunferencia, y

$\mathscr{C}_r(O) = \{P \in E ; d(O, P) \leq r\}$ es el círculo de radio r con centro en O.

DEF 17 Dados $F_1, F_2 \in E, r \in \mathbb{R}^+$ con $r > d(F_1, F_2)$,

$\mathscr{E}_r(F_1, F_2) = \{P \in E ; d(P, F_1) + d(P, F_2) = r\}$ es la elipse con focos F_1, F_2 y eje mayor r.

DEF 18 Dados $F_1, F_2 \in E, r \in \mathbb{R}^+$ con $r < d(F_1, F_2)$,

$\mathscr{H}_r(F_1, F_2) = \{P \in E ; |d(P, F_1) - d(P, F_2)| = r\}$ es la hipérbola con focos F_1, F_2 y radio r.

Enunciaremos ahora algunos resultados sencillos pero asombrosos de esta geometría:

TEO 12 En la métrica discreta existe un único círculo de radio 1: El total.

TEO 13 Dada una circunferencia $\mathscr{C}_r(O)$, todo punto interior es centro.

$(\forall P \in \text{Int}\mathscr{C}_r(O), \forall Q \in \mathscr{C}_r(O), d(P,Q) = r)$

Dem Sea $P \in \text{Int}\mathscr{C}_r(O)$, $Q \in \mathscr{C}_r(O)$. Nos fijamos en el triángulo $\{P,Q,O\}$.

$P \in \text{Int}\mathscr{C}_r(O) \Rightarrow d(P,O) < r$, y $Q \in \mathscr{C}_r(O) \Rightarrow d(Q,O) = r$. $\therefore d(P,Q) = r$ (todos los triángulos son isósceles y "flacos"), e.d. P es un centro de la circunferencia. †.

TEO 14 Sean $\mathscr{C}_1, \mathscr{C}_2$ circunferencias. Si $\text{Int}\mathscr{C}_1 \cap \text{Int}\mathscr{C}_2 \neq \emptyset$, entonces $\mathscr{C}_1$ y $\mathscr{C}_2$ son concéntricos.

Dem Sea $x \in \text{Int}\mathscr{C}_1 \cap \text{Int}\mathscr{C}_2$. Entonces, por el teorema anterior, x es centro de $\mathscr{C}_1$ y x es centro de $\mathscr{C}_2$, $\therefore \mathscr{C}_1$ y $\mathscr{C}_2$ son concéntricos. †.

Corolario1 Si $\text{Int}\mathscr{C}_1 \cap \text{Int}\mathscr{C}_2 \neq \emptyset$ y $r_1 = r_2$, entonces $\mathscr{C}_1 = \mathscr{C}_2$.

Dem $\mathcal{C}_1$, $\mathcal{C}_2$ son concéntricas y tienen el mismo radio, por lo tanto son iguales.

Obs: Si $\text{Int}\mathcal{C}_1 \cap \text{Int}\mathcal{C}_2 \neq \emptyset$ y $\mathcal{C}_1 \cap \mathcal{C}_2 \neq \emptyset$, entonces $\mathcal{C}_1 = \mathcal{C}_2$.

Corol 2 Si $\text{Int}\mathcal{C}_1 \cap \text{Int}\mathcal{C}_2 \neq \emptyset$ y $r_1 < r_2$, entonces todos los puntos de $\mathcal{C}_1$ son centros de $\mathcal{C}_2$.

Dem Si $r_1 < r_2$, entonces $\mathcal{C}_1 \subseteq \text{Int}\mathcal{C}_2$.

TEO 15 Todo punto exterior a $\mathcal{C}_r(O)$ está "bien lejos" de $\mathcal{C}_r(O)$. (Si $P \in \text{Ext}\mathcal{C}_r(O)$, y $Q \in \mathcal{C}_r(O)$, entonces $d(P,Q) > r$).

Dem Sea $P \in \text{Ext}\mathcal{C}_r(O)$, y $Q \in \mathcal{C}_r(O)$. Consideremos el triángulo (P,Q,O). Dada la naturaleza de los triángulos ultramétricos, $d(Q,O) = r$ y $d(P,O) > r \Rightarrow$

$d(P,Q) = d(P,O) > r$. †.

Nótese que, en el caso discreto el teorema se cumple trivialmente, ya que cualquier circunferencia no trivial no tiene exterior, y obviamente si la circunferencia es trivial, cualquier punto del exterior está "bien lejos".

En este caso (discreto), existen circunferencias "bien llenas" con interior vacío excepto por un punto, que es el centro ($r = 1$), y circunferencias vacías con interior repleto de puntos. ($r < 1$).

Si se define diámetro como el máximo de las distancias que hay entre los puntos de una circunferencia, podemos enunciar el siguiente teorema:

TEO 16 Sea $\mathcal{C}_r(O)$ un circunferencia. Entonces el radio es mayor o igual a la distancia que hay entre cualesquiera dos puntos de la circunferencia. En particular, cualquier diámetro es menor o igual al radio.

Obs : En el caso discreto se da siempre la igualdad:

Si $r = 0$ ó $r = 1$, la observación se cumple trivialmente. En cualquier otro caso, dado que entonces $\mathcal{B}_r(O) = \varnothing$, se cumple que

$\forall P_1, P_2 \in \mathcal{B}_r(O)$, $d(P_1, P_2) =$ *la que se desee*, en particular, $d(P_1, P_2) = r$.

Dem Sean $P_1, P_2 \in \mathcal{B}_r(O)$ dos puntos cualesquiera. Consideremos el triángulo $\{O, P_1, P_2\}$.

$d(P_1, O) = r = d(P_2, O) \Rightarrow d(P_1, P_2) \leq r$.

†.

TEO 17 No es posible alinear 3 puntos distintos, en el sentido de que

$d(a, b) + d(b, c) = d(a, c)$.

Dem Como a, b, c son distintos, $A = d(a, b) \neq 0$; $B = d(b, c) \neq 0$; $C = d(a, c) \neq 0$,

$\Rightarrow A \leq$ máx $\{B, C\} < B + C$

$B \leq$ máx $\{A, C\} < A + C$

$C \leq$ máx $\{A, B\} < A + B$. ∴ es imposible que estén alineados.

†.

Examinemos ahora otro concepto interesante . ¿Será posible definir circunferencias tangentes en un espacio ultramétrico? Y si lo es, ¿Existirán tales circunferencias?, y ¿Cómo serán?.

Entendamos por circunferencias tangentes a dos circunferencias que sólo se intersecan en un punto, y veamos en que casos puede suceder esto.

CASO 1 Sean $\mathcal{B}_r(O)$, $\mathcal{B}_{r'}(O')$ dos circunferencias en E. Supongamos primero que $r' < r$, y supongamos también que $\mathcal{B}_r(O) \cap \mathcal{B}_{r'}(O') \neq \varnothing$.

PROP 1 $O' \in \mathcal{C}_r(O)$.

Dem Consideremos el triángulo $\{O, O', P\}$, donde $P \in \mathcal{C}_r(O) \cap \mathcal{C}_{r'}(O')$ es un punto arbitrario. Entonces $d(O, P) = r$, $d(O', P) = r'$. Como $r < r'$, sabemos que $d(O,O') = r$,

$\therefore O' \in \mathcal{C}_r(O)$.

†.

PROP 2 *"$\mathcal{C}_r(O)$ se unta a $\mathcal{C}_{r'}(O')$ aunque no tan bien"*: ¡ $\mathcal{C}_{r'}(O') \subseteq \mathcal{C}_r(O)$!

Dem Sea $P \in \mathcal{C}_{r'}(O')$. Consideremos el triángulo $\{O, O', P\}$. $d(O,O') = r$, $d(P,O') = r'$,

y $r' < r \Rightarrow d(O, P) = r$ $\therefore P \in \mathcal{C}_r(O)$.

†.

Pregunta: ¿Podrá suceder que $\mathcal{C}_{r'}(O') = \mathcal{C}_r(O)$? La respuesta es que no (y a esto es a lo que nos referíamos con el "no tan bien"):

Por lo menos $O' \in \mathcal{C}_r(O) - \mathcal{C}_{r'}(O')$.

CASO 1 Supongamos ahora que $r = r'$, e.d. nos fijamos en dos circunferencias con el mismo radio pero no concéntricas. Supongamos también que $\mathcal{C}_r(O) \cap \mathcal{C}_{r'}(O') \neq \varnothing$.

Sea $P \in \mathcal{C}_r(O) \cap \mathcal{C}_{r'}(O')$. Veamos el triángulo $\{O, O', P\}$.

$d(O, P) = r = d(O', P) \Rightarrow d(O,O') \leq r$. Si $d(O, O') < r$, entonces $O' \in \text{Int}\mathcal{C}_r(O)$ $\Rightarrow O'$ es centro de $\mathcal{C}$, pero eso contradice la hipótesis de que no son concéntricas

$\therefore d(O, O') = r$. entonces $O' \in \mathcal{C}_r(O)$ y $O \in \mathcal{C}_r(O')$. Sea ahora $Q \in \mathcal{C}_r(O)$. Consideremos el triángulo $\{Q, O, O'\}$. Siguiendo el razonamiento que hemos usado hasta ahora llegamos a

que $d(Q,O') \leq r \Rightarrow Q \in \mathcal{C}_r(O') \cup Int\mathcal{C}_r(O')$, conjunto al cual hemos llamado círculo con centro en O' y radio r.

$\therefore \mathcal{C}_r(O) \subseteq \mathcal{C}_r(O') \cup Int\mathcal{C}_r(O')$.

Sea ahora $Q \in Int\mathcal{C}_r(O)$. Considerando el triángulo (P,O,O'), vemos que $d(Q,O') = r$ $\therefore P \in \mathcal{C}_r(O')$. Concluímos entonces que $\mathcal{C}_r(O) \cup Int\mathcal{C}_r(O) \subseteq \mathcal{C}_r(O') \cup Int\mathcal{C}_r(O')$.

Análogamente, $\mathcal{C}_r(O') \cup Int\mathcal{C}_r(O') \subseteq \mathcal{C}_r(O) \cup Int\mathcal{C}_r(O')$.

$\therefore |\mathcal{C}_r(O') \cup Int\mathcal{C}_r(O')| = |\mathcal{C}_r(O) \cup Int\mathcal{C}_r(O)|$ (Pero $\mathcal{C}_r(O) \neq \mathcal{C}_r(O')$).

Obs1 : De hecho, $Int\mathcal{C}_r(O') \subseteq \mathcal{C}_r(O)$ y $Int\mathcal{C}_r(O) \subseteq \mathcal{C}_r(O')$, ya que si $P \in Int\mathcal{C}_r(O')$, entonces $d(P, O')$. Como ya sabemos que $d(O, O') = r$, concluímos que $d(P, O) = r$. Análogamente para el otro caso.

Obs2 : No podemos concluír que $Int\mathcal{C}_r(O') = \mathcal{C}_r(O)$, ya que si tomamos un elemento arbitrario P en $\mathcal{C}_r(O)$, la naturaleza ultramétrica del triángulo (P, O, O') sólo nos garantiza que $d(P, O') \leq r$, y no se llega a ninguna contradicción suponiendo $d(P, O') = r$. Así, la existencia de circunferencias tangentes dependerá de la ultramétrica en cuestión.

Obs: Si dos circunferencias no concéntricas no se cortan, entonces estan "bien alejadas". Esto es una consecuencia directa del teorema 7.

Obs: En el caso discreto, en un conjunto con más de dos elementos, dos circunferencias no triviales necesariamente se cortan, y en un conjunto con más de tres elementos, las circunferencias no pueden ser "tangentes".

DEF 19 **Un cuadrilátero** en E es una cuaterna de elementos ordenada cíclicamente.

Una **pareja** cuyos elementos son consecutivos en la cuaterna es un **lado** del cuadrilátero.En este caso, los dos elementos son los **extremos** del lado. Una pareja cuyos elementos no son consecutivos en la cuaterna es una **diagonal** del cuadrilátero.

La longitud de un lado es la distancia que hay entre sus extremos.

Un **cuadrado** es un cuadrilátero que tiene todos los lados de igual longitud.

TEO 18 Si $(a, b, c, d) \subseteq E$ es un cuadrado, las diagonales son menores o iguales que los lados.

Dem Consideremos el triángulo $\{a, b, c\}$. Como $d(a, b) = d(b, c)$, necesariamente $d(a, c) \leq d(a, b)$.

Obs: En el caso discreto, todo cuadrilátero es cuadrado y si existen 6 o más puntos, no es posible encerrar a los circunferencias no triviales en cuadrados (cualquier circunferencia no trivial es el todo el espacio menos el centro).

Para ver como se ven las elipses en esta geometría, examinaremos los distintos casos, tomando en cuenta que la expresión general de una elipse es $\mathcal{E}_k(F_1, F_2)$, donde $k > d(F_1, F_2)$.

Caso 1: $k > 2d(F_1, F_2)$

TEO 19 Si F_1, F_2, k determinan una elipse ($\mathcal{E} = \{P \in E; d(P, F_1) + d(P, F_2) = k\}$), y $k > 2d(F_1, F_2)$, entonces la elipse se puede describir como la circunferencia de radio $k/2$ con centro en F_1 (o eqivalentemente en F_2).

Dem Sea $P \in \mathcal{E}$. Entonces, por definición, $d(P, F_1) + d(P, F_2) = k > 2d(F_1, F_2) \Rightarrow$

$d(P, F_1) > d(F_1, F_2)$ ó $d(P, F_2) > d(F_1, F_2)$. Pero cualquiera de estas dos condiciones garantiza que $d(P, F_1) = d(P, F_2)$. De esto y de que $d(P, F_1) + d(P, F_2) = k$, concluímos que $d(P, F_1) = d(P, F_2) = k/2$. $\therefore P \in \mathcal{C}_{k/2}(F_1) \cap \mathcal{C}_{k/2}(F_2)$.

Pero dado que $k/2 > d(F_1, F_2), F_2 \in \text{Int}\mathcal{C}_{k/2}(F_1) \Rightarrow \mathcal{C}_{k/2}(F_1) = \mathcal{C}_{k/2}(F_2)$.

$\therefore \mathcal{E} \subseteq \mathcal{C}_{k/2}(F_1)$.

Por otro lado, $\forall P \in \mathcal{C}_{k/2}(F_1) = \mathcal{C}_{k/2}(F_2)$, $d(P, F_1) = k/2 = d(P, F_2) \Rightarrow P \in \mathcal{E}$.

$\therefore \mathcal{E} = \mathcal{C}_{k/2}(F_1) = \mathcal{C}_{k/2}(F_2)$

†.

Obs: En este caso, $\mathcal{E}_k(F_1, F_2) = \mathcal{E}_k(F_1', F_2')$, siempre que $d(F_i', F_i) < k/2$, $i = 1,2$. Es decir que la elipse es independiente de los puntos que tomemos como focos, siempre que sean centros de la circunferencia $\mathcal{C}_{k/2}(F_1)$.

Caso 2: $k = 2d(F_1, F_2)$.

TEO 2º Si F_1, F_2, k determinan una elipse, y $k = 2d(F_1, F_2)$, entonces la elipse se puede describir como la intersección de las circunferencias de radio $d(F_1, F_2)$ con centro en F_1 y F_2.

($\mathcal{E} = \mathcal{C}_r(F_1) \cap \mathcal{C}_r(F_2)$, donde $r = d(F_1, F_2)$).

Dem Por definición, un punto P está en la elipse si $d(P, F_1) + d(P, F_2) = 2r$.

Si $d(P, F_1) > r$, entonces, considerando el triángulo $\{F_1, F_2, P\}$ vemos que necesariamente $d(P, F_1) = d(P, F_2) \Rightarrow d(P, F_1) + d(P, F_2) > 2r \Rightarrow P \notin \mathcal{E}$ $\forall$ $\therefore d(P, F_1) \leq r$.

Análogamente, $d(P, F_2) \leq r$. $\therefore d(P, F_1) = d(P, F_2) = r$. $\therefore$ la elipse consta de todos los puntos que están a una distancia r de F_1 y de F_2.

$$\therefore \mathscr{E} = \mathscr{C}_r(F_1) \cap \mathscr{C}_r(F_2)$$

†.

Obs: En este caso, $\mathscr{E}_k(F_1, F_2) = \mathscr{E}_k(F_1', F_2')$, siempre que $F_i' \in \mathscr{C}_r(F_i)$, $i = 1,2$.

Caso 3 $d(F_1, F_2) < k < 2d(F_1, F_2)$.

TEO 21 Si F_1, F_2, k determinan una elipse, y $d(F_1, F_2) < k < 2d(F_1, F_2)$, entonces la elipse se puede describir como la unión de las circunferencias de radio $k - d(F_1, F_2)$ con centro en F_1 y F_2.

($\mathscr{E} = \mathscr{C}_\alpha(F_1) \cup \mathscr{C}_\alpha(F_2)$, donde $\alpha = k - d(F_1, F_2)$).

Dem Sea $r = d(F_1, F_2)$. Supongamos que $P \in \mathscr{E}$, y supongamos que $d(P, F_1) > r$.
Entonces $d(P, F_1) = d(P, F_2)$ $\forall$, ya que entonces $d(P, F_1) + d(P, F_2) > 2r$.
$\therefore d(P, F_1) \leq r$. Análogamente, $d(P, F_2) \leq r$.

$$\therefore \quad d(P, F_1) = r \Rightarrow d(P, F_2) = k - r$$
$$\text{ó}$$
$$d(P, F_2) = r \Rightarrow d(P, F_1) = k - r.$$

Entonces, si $\alpha = k - r$, $\mathscr{E} = (\mathscr{C}_r(F_1) \cap \mathscr{C}_\alpha(F_2)) \cup (\mathscr{C}_\alpha(F_1) \cap \mathscr{C}_r(F_2))$.

Dado que $\alpha < r$, $(k < 2r)$, vemos que $\mathscr{C}_r(F_1) \cap \mathscr{C}_\alpha(F_2) = \mathscr{C}_\alpha(F_2)$ ó

$\mathscr{C}_r(F_1) \cap \mathscr{C}_\alpha(F_2) = \varnothing$ y $\mathscr{C}_\alpha(F_1) \cap \mathscr{C}_r(F_2) = \mathscr{C}_\alpha(F_1)$ ó $\mathscr{C}_\alpha(F_1) \cap \mathscr{C}_r(F_2) = \varnothing$,

ya que si $\mathscr{C}_r(F_1) \cap \mathscr{C}_\alpha(F_2) \neq \varnothing$, por la proposición 2 demostrada anteriormente,

$\mathscr{C}_\alpha(F_2) \subset \mathscr{C}_r(F_1)$. y análogamente para el otro caso.

¿Pero que querría decir que $\mathcal{C}_r(F_1) \cap \mathcal{C}_\alpha(F_2) = \emptyset$?. Supongamos primero que $\mathcal{C}_\alpha(F_1) \cap \mathcal{C}_r(F_2) \neq \emptyset$. Si $P \in \mathcal{C}_\alpha(F_2)$, forzosamente $d(P, F_1) = r \Rightarrow P \in \mathcal{C}_r(F_1)$.

Entonces $\mathcal{C}_r(F_1) \cap \mathcal{C}_\alpha(F_2) = \emptyset \Rightarrow \mathcal{C}_\gamma(F_2) = \emptyset$. Por otro lado, si $\mathcal{C}_r(F_1) \cap \mathcal{C}_\alpha(F_2) = \emptyset$,

$\forall\ P \in \mathcal{C}$, $d(P, F_1) \neq r$ (si no $(P) \subseteq \mathcal{C}_r(F_1) \cap \mathcal{C}_\alpha(F_2)) \Rightarrow d(P, F_2) = r \Rightarrow$

$d(P, F_1) = \alpha$, e.d. $P \in \mathcal{C}_\alpha(F_1) \cap \mathcal{C}_r(F_2)$.

En otras palabras $\mathcal{C}_r(F_1) \cap \mathcal{C}_\alpha(F_2) = \emptyset \Rightarrow \mathcal{C} \subseteq \mathcal{C}_\alpha(F_1) \cap \mathcal{C}_r(F_2) = \mathcal{C}_\alpha(F_1) =$

$= \mathcal{C}_\alpha(F_1) \cup \mathcal{C}_\alpha(F_2)$.

Ahora bien, si $\mathcal{C}_r(F_1) \cap \mathcal{C}_\alpha(F_2) = \emptyset$ y $\mathcal{C}_\alpha(F_1) \cap \mathcal{C}_r(F_2) = \emptyset$, entonces, por la argumentación dada anteriormente, necesariamente $\mathcal{C} = \emptyset$, por lo tanto se cumple el resultado del teorema.

Análogamente para el caso $\mathcal{C}_\alpha(F_1) \cap \mathcal{C}_r(F_2) = \emptyset$. Hemos demostrado entonces que el resultado es el mismo en todos los casos, e.d.

$\mathcal{C} = \mathcal{C}_\alpha(F_1) \cup \mathcal{C}_\alpha(F_2)$, donde $\alpha = k - d(F_1, F_2)$

†.

Obs: En este caso, $\mathcal{C}_k(F_1, F_2) = \mathcal{C}_k(F_1', F_2')$, si $F_i' \in \mathcal{C}_\alpha(F_i)$.

Resumiendo, una elipse es o bien una circunferencia, la intersección de dos circunferencias, o bien la unión de dos circunferencias. ¿Sucederá algo similar con las hipérbolas?.

TEO 22 Sea $\mathcal{H}_k(F_1, F_2)$ una hipérbola. Entonces, si $\alpha = d(F_1, F_2)$,

$\mathcal{H}_k(4_1, F_2) = \mathcal{C}_\alpha(F_1) \cup \mathcal{C}_\alpha(F_2)$.

COMPLECIÓN DE UN CAMPO

DEF 20 **Sea k un campo.** $k^+ \subseteq k$ **es una clase positiva, si**

•) $a, b \in k^+ \Rightarrow ab \in k^+, a+b \in k^+$.

••) Si $a \in k$, entonces sucede una y solo una de

i) $a \in k^+$

ii) $-a \in k^+$

iii) $a = 0$.

DEF 21 **Un campo k se llama campo ordenado si tiene una clase positiva.**

En tal caso la relación de orden " $<$" se define como $b < a \Leftrightarrow a - b \in k^+$, y se agregan las convenciones usuales,

$$b > a \Leftrightarrow a < b$$

$$b \leq a \Leftrightarrow b < a \ \vee \ b = a.$$

$$b \geq a \Leftrightarrow a \leq b.$$

Podemos probar fácilmente que esta relación satisface las propiedades de orden estricto, a saber:

•) $\forall a, b, c \in k$, $a < b \wedge b < c \Rightarrow a < c$ **(transitividad).**

••) $\forall a, b \in k$, debe suceder una (y solo una) de las siguientes condiciones:

i) $a < b$

ii) $b < a$

iii) $a = b$ **(tricotomía).**

Dem :

•) $\forall\, a,b,c \in \mathbf{k},\ a<b \wedge b<c \Rightarrow b-a, c-b \in \mathbf{k}^+ \Rightarrow (c-b)+(b-a) =$

$= c-a \in \mathbf{k}^+ \Rightarrow a<c.$

••) Sean $a, b \in \mathbf{k}$. Entonces sucede una (y solo una) de las sig. condiciones:

i) $b-a \in \mathbf{k}^+ \Rightarrow a<b$

ii) $a-b \in \mathbf{k}^+ \Rightarrow b<a$

iii) $b-a=0 \Rightarrow a=b$

$\therefore$ "$<$" es un orden estricto en k.

Y además resulta compatible con las operaciones, es decir, $\forall\, a,b,c \in \mathbf{k}$,

•) $a<b \Rightarrow a+c<b+c$, y

••) $a<b$ y $c \in \mathbf{k}^+ \Rightarrow ac<bc$.

Dem :

Dados $a, b \in \mathbf{k}$, $a<b \Rightarrow b-a \in \mathbf{k}^+ \Rightarrow b+(c-c)-a \in \mathbf{k}^+ \Rightarrow a+c<b+c$.

Si $c \in \mathbf{k}^+, a<b \Rightarrow b-a \in \mathbf{k}^+ \Rightarrow bc-ac \in \mathbf{k}^+ \Rightarrow ac<bc$.

†.

Nota : En álgebra, se consideran campos ordenados sólo aquellos cuyo orden es compatible con las operaciones (y que por lo tanto tienen clase positiva).

1) Corolario : $\forall\, a \in \mathbf{k},\ a \neq 0 \Rightarrow a^2 \in \mathbf{k}^+$. $\therefore 1$ (el idéntico multiplicativo del campo, que por definición debe ser $\neq 0$) es $1=1^2 \in \mathbf{k}^+$, y si $\{a_i\}_{i\in I} \subseteq \mathbf{k}$, $\sum a_i^2 = 0 \Leftrightarrow a_i = 0\ \forall\, a_i$.

$\therefore$ todo campo ordenado es de característica 0 (Ver apéndice).

2) Nótese que en C, $i \neq 0$, $i^2 = -1$, lo cual implica que C no es ordenable con un orden compatible con las operaciones (aunque sí es bien-ordenable como conjunto, según garantiza el axioma de elección).

3) Si se identifican los enteros como elementos de k vía la inmersión $i : Z \to k$

$$i(0) = 0_k$$
$$i(n+1) = i(n) + e$$
$$i(-n) = -i(n),$$

se tiene que $n \in k^+ \Rightarrow n+1 \in k^+$, y $\therefore Z^+ \subseteq k^+$. (Es decir, todo campo ordenado contiene un subconjunto isomorfo a Z^+ y es por lo tanto infinito, lo que asegura en particular que ningún campo finito es ordenable).

4) $\forall a \in k,\ a \in k^+ \Leftrightarrow a^{-1} \in k^+$.

5) $a < b \Leftrightarrow \forall n \in Z^+\ a^n < b^n$.

6) Una clase positiva definida en cualquier campo permite definir un valor absoluto como sigue:

DEF 22 Sea k un campo ordenado, k^+ su clase positiva.

Definimos $|\ |: k \to k^+ \cup \{0\}$ como

$$|a| = \begin{cases} a, \text{ si } a \in k^+ \\ -a, \text{ si } -a \in k^+ \\ 0, \text{ si } a = 0 \end{cases}$$

TEOREMA 23 $|\ |$ cumple con las propiedades de valor absoluto:

') $|a| \in k^+ \cup \{0\}$, $|a| = 0 \Leftrightarrow a = 0$.

'') $|ab| = |a|\,|b|$.

$\cdots$) $|a+b| \le |a|+|b|$.

Dem ·) es obvia.

··) Analicemos todos los casos:

a	b	$\lvert ab\rvert$	$\lvert a\rvert\lvert b\rvert$
$a \ge 0$	$b \ge 0$	ab	ab
$a \ge 0$	$b < 0$	$a(-b)$	$a(-b)$
$a < 0$	$b \ge 0$	$(-a)b$	$(-a)b$
$a < 0$	$b < 0$	$(-a)(-b)$	$(-a)(-b)$

$\cdots$) $(|a+b|)^2 = (a+b)^2 = a^2+2ab+b^2 \le |a|^2+2|ab|+|b|^2 = (|a|+|b|)^2$.

Con esta ecuación y con la observación (5) de clase positiva ($a<b \Leftrightarrow \forall\, n \in \mathbb{Z}^+$ $a^n < b^n$), concluimos la demostración.

†.

TEOREMA 24 Si k es el campo de cocientes de un anillo R, y si R es ordenado, entonces hay un único orden en k tal que su restricción a R coincide con el orden en R, (que extiende el orden en R)

Dem Si $\frac{b}{c} \in k$, definimos $\frac{b}{c} \in k^+ \Leftrightarrow bc > 0$. Entonces k^+ es clase positiva:

·) $\frac{b}{c}, \frac{d}{e} \in k^+ \Rightarrow bc, de > 0 \Rightarrow bdce > 0 \Rightarrow \frac{bd}{ce} \in k^+$.

··) $\frac{b}{c}, \frac{d}{e} \in k^+ \Rightarrow bc, de > 0 \Rightarrow bce^2, dec^2 > 0 \Rightarrow bece + decc = (be+dc)ce > 0 \Rightarrow$

$$\frac{be+dc}{ce} = \frac{b}{c} + \frac{d}{c} \in k^+$$

$\cdots$) Si $\frac{b}{c} \in k$, entonces se cumple una (y sólo una) de:

$bc > 0 \Rightarrow \frac{b}{c} \in k^+$, $-(bc) > 0 \Rightarrow \frac{-b}{c} \in k^+$, ó $\qquad bc = 0 \Rightarrow b = 0 \Rightarrow \frac{b}{c} = 0$.

Si $b \in R$, $b > 0$, entonces $b = b \cdot 1 > 0 \Rightarrow b = \frac{b}{1} \in k^+$, e.d. el orden inducido por k' preserva el orden en R.

Se hará ver ahora que el orden que extiende al de R es único. Supongamos que k está ordenado, y que este orden extiende al de R.

Sea $a = \frac{b}{c} \in k$. Entonces, multiplicando por c^2,

$$\frac{b}{c} > 0 \Rightarrow bc > 0.$$

$$\frac{b}{c} = 0 \Rightarrow bc = 0.$$

$$\frac{b}{c} < 0 \Rightarrow bc < 0.$$

$\therefore$ El orden en k sólo puede ser el que definimos.

†.

DEF 23 Sean $(k_1, k_1^+), (k_2, k_2^+)$ dos campos ordenados. Decimos que k_1 es orden - isomorfo a k_2 si existe un isomorfismo $f: k_1 \to k_2$ ∋ $\forall a \in k_1$, $a \in k_1^+ \Leftrightarrow f(a) \in k_2^+$.

DEF 24 El orden en un campo k se llama **arquimediano** si $\forall a \in k \; \exists n \in N$ ∋ $n \cdot 1 > a$. En este caso también existe $n \in N$ ∋ $-n \cdot 1 < a$, y $n \in Z$ ∋ $\frac{1}{n \cdot 1} < a$.

Obs: Si $a \in k$, definimos "multiplicación por n" con la siguiente recursión:

$$\begin{cases} 0 \cdot a = \theta \\ (n+1) \cdot a = n \cdot a \oplus a \\ (-n) \cdot a = -(n \cdot a) \end{cases}$$

(Nótese que en el lado derecho de estas igualdades, θ es el neutro aditivo del campo, y la suma ⊕ es la suma del campo).

DEF 25 Sea k un campo ordenado y $S \subseteq k$, $S \neq \varnothing$.

$M \in k$ es una cota superior de S si $\forall x \in S$, $x \leq M$.

Si $\{M \in k;\ M$ es cota superior de $S\}$ tiene mínimo M_0, $M_0 = \text{Sup } S$ es el **supremo de S.**

Análogamente, se define cota inferior e ínfimo (la mayor de las cotas inferiores).

DEF 18 Se dice que en **k** se cumple el principio del supremo si todo subconjunto no vacío de **k** acotado superiormente tiene supremo.

Ejemplo 1: En **R** vale el principio del supremo.

Ejemplo 2: Es sabido que en el campo de los números racionales no se cumple el principio del supremo, e.d. $\exists\ S \subseteq \mathbf{Q},\ S \neq \varnothing$, S acotado superiormente tal que S no tiene supremo.

$(S = \{x \in \mathbf{Q};\ x^2 < 2\}$ es un ejemplo de esto).

Tratemos ahora de encontrar para cada campo ordenado k, una extensión ordenada Ω en la que se cumpla el principio del sumpremo. Este campo Ω se puede construir de varias formas (encajes, cortaduras de Dedekind y sucesiones de Cauchy entre otras). Aquí describiremos brevemente la construcción por sucesiones de Cauchy.

DEF 26 Una sucesión $\{a_n\}_{n \in \mathbf{N}}$ es una sucesión de Cauchy si $\forall\ \varepsilon \in k^+\ \exists\ n = n(\varepsilon) \in \mathbf{N}\ \ni$

$$|a_p - a_q| < \varepsilon \quad \forall\ p, q > n.$$

Obs: Si $\{a_n\}_{n \in \mathbf{N}}$ es una sucesión de Cauchy, entonces está acotada superior e inferiormente.

(Para $p > n, q = n+1$, $|a_p| \leq |a_q| + |a_p - a_q| < |a_{n+1}| + \varepsilon = M$

$\Rightarrow N = \text{máx}\ \{|a_1|, \ldots, |a_{p-1}|, M\}$ es una cota superior de $\{a_n\}_{n \in \mathbf{N}}$, y $-N$ es cota inferior).

La suma y el producto de dos sucesiones de Cauchy se define de la manera natural:

$$\{a_n\}_{n\in\mathbf{N}} + \{b_n\}_{n\in\mathbf{N}} = \{c_n\}_{n\in\mathbf{N}}, \text{ donde } \forall\, i \in \mathbf{N}, c_i = a_i + b_i$$

$$\{a_n\}_{n\in\mathbf{N}} \cdot \{b_n\}_{n\in\mathbf{N}} = \{c_n\}_{n\in\mathbf{N}}, \text{ donde } \forall\, i \in \mathbf{N}, c_i = a_i \cdot b_i$$

Es fácil demostrar que la suma y el producto de sucesiones de Cauchy vuelve a ser sucesión de Cauchy, y por lo tanto ver que las sucesiones de Cauchy forman un anillo R.

DEF 27 Una sucesión de Cauchy $\{a_p\}$ es una **sucesión nula** si converge a cero,

e.d. si $\forall\, \varepsilon \in k^+$,

$$\exists\, n \in \mathbf{N} \ \ni\ |a_p| < \varepsilon \quad \forall\, p > n.$$

TEO 25 El conjunto I de sucesiones nulas es un ideal del anillo R.

Dem Sean $\{a_p\}, \{b_p\}$ sucesiones nulas. Entonces $\forall\, \varepsilon \in k^+\ \exists\, n_1, n_2 \in \mathbf{N} \ \ni$

$$|a_p| < \tfrac{1}{2}\varepsilon \quad , \text{ si } p > n_1, \qquad |b_p| < \tfrac{1}{2}\varepsilon \quad , \text{ si } p > n_2.$$

Sea $n = \max\{n_1, n_2\}$. Entonces $|a_p - b_p| < |a_p| + |b_p| < \varepsilon$, si $p > n$.

$\therefore\ \{a_p - b_p\}$ es también una sucesión nula.

Ahora, si $\{c_p\}$ es una sucesión de Cauchy cualquiera, sabemos que $\exists\, M \in k \ \ni$

$|c_p| < M \quad \forall\, p \in \mathbf{N}$, y $\forall\, \varepsilon \in k^+\ \exists\, n(\varepsilon) \in \mathbf{N} \ \ni\ |a_p| < \varepsilon/M$, si $p > n$.

Entonces $|a_p|\,|c_p| = |a_p c_p| < \varepsilon$, si $p > n$. $\therefore\ \{a_p c_p\}$ es una sucesión nula.

$\therefore$ I es un ideal.

DEF 28 Sea $\Omega = R/I$ el anillo de clases residuales.

TEO 26 Ω es campo.

Dem P.D. $ax \equiv 1$ (I) tiene solución siempre que $a \not\equiv 0$ (I)

(donde 1 es el neutro multiplicativo de R y 0 el neutro aditivo, e.d. $1 = \{1,1,1,\ldots\}$; $0 = \{0,0,0,\ldots\}$).

Tiene que existir $n \in \mathbb{N}$ y $\eta > 0 \ni |a_q| \geq \eta \ \ \forall \ q > n$ (Porque si no fuera así, $\forall\, n$ y $\forall \eta > 0$, tendríamos $|a_q| < \eta$ p.a. $q > n$. Y entonces podríamos escoger una n suficientemente grande para que para $p > n, q > n$, $|a_p - a_q| < \eta \Rightarrow |a_p| < 2\eta$ $\forall\, p > n$, y así la sucesión $\{a_p\}$ sería nula, lo cual contradice la hipótesis.).

Claramente, la sucesión $\{a_p\}$ se mantiene en la misma clase residual módulo I, si intercambiamos $a_1, \ldots, a_n$ por η. Si a estos nuevos n elementos η de la sucesión les volvemos a llamar $a_1, \ldots, a_n$, podemos escribir:

$\forall\ p$, $|a_p| \geq 2\eta$. En particular , $a_p \neq 0 \ \ \forall\ p$.

Ahora, $\{a_p^{-1}\}$ es una sucesión de cauchy, porque $\forall\, \varepsilon > 0$, $\exists\, n \in \mathbb{N}$ tal que

$$|a_p - a_q| < \varepsilon\eta^2, \qquad \text{para } p > n, q > n.$$

Ahora, si tuviéramos que $|a_p^{-1} - a_q^{-1}| \geq \varepsilon$ para alguna $p > n$ y alguna $q > n$, entonces, multiplicando por $|a_p| \geq \eta$ y por $|a_q| \geq \eta$, se seguiría que:

$$|a_p - a_q| = |a_p a_q (a_p^{-1} - a_q^{-1})| \geq \varepsilon\eta^2, \text{ lo cual no sucede.}$$

$$\therefore \qquad |a_p^{-1} - a_q^{-1}| < \varepsilon, \qquad \text{para } p > n, q > n.$$

Naturalmente, la sucesión de Cauchy $\{a_p^{-1}\}$ resuelve la congruencia. †.

Si $k' = (\{\overline{a, a, a, \ldots}\}; a \in k) \subset \Omega$ (donde $\overline{a, a, a, \ldots}$ es la clase residual representada por $\{a, a, a, \ldots\}$), entonces $k' \equiv k$, porque

$f : k \to k'$
$a \to \overline{a, a, a, \ldots}$ es un isomorfismo:

$a+b \to \{\overline{a+b, a+b, \dots}\} = \{\overline{a, a, a, \dots}\} + \{\overline{b, b, b, \dots}\} = f(a) + f(b)$

$a \cdot b \to \{\overline{a \cdot b, a \cdot b, \dots}\} = \{\overline{a, a, a, \dots}\} \cdot \{\overline{b, b, b, \dots}\} = f(a) \cdot f(b)$.

Si $f(a) = \{\overline{0, 0, 0, \dots}\}$, entonces $a = 0$.

Y finalmente, dada $\{\overline{a, a, a, \dots}\} \in k'$, **obviamente** $a \in k \quad \therefore \{\overline{a, a, a, \dots}\} = f(a)$.

Si identificamos a los elementos de k' con los de k, podemos decir que Ω es una extensión de k.

Veamos ahora que Ω es un campo ordenado.

DEF 29 Una sucesión de Cauchy $\{a_p\}$ se llama positiva si $\exists\, \varepsilon \in k^+, n \in N \ni a_p > \varepsilon \ \forall p > n$.

Una clase residual $\{\overline{a_p}\}$ se llama positiva si $\{a_p\}$ es positiva.

Obs: Para ver que la definición no depende del representante,

Sea $\{a_p\}$ una sucesión positiva y $\{b_p\}$ una sucesión nula.

Sabemos que $\exists\, \varepsilon \in k^+, n \in N \ni a_p > \varepsilon \quad \forall p > n$, y que $\exists\, n' \in N \ni$ $|b_p| < \varepsilon/2$, si $p > n'$.

$\therefore$ Si $m = \text{máx}\{n, n'\}$, $a_p + b_p > \varepsilon/2$, si $p > m \quad \Rightarrow \{a_p + b_p\}$ es positiva.

TEO 27 $S = \{\{\overline{a_p}\}; \{a_p\}$ es positiva$\}$ es una clase positiva.

DEF 28 Una clase residual $\{\overline{a_p}\}$ es negativa si $-\{\overline{a_p}\}$ es positiva. $(-\{\overline{a_p}\}$ es la clase representada por $-\{a_p\}$, que es la sucesión $\{c_p\}$, donde $c_p = -a_p \ \forall p)$.

PROP 4 Si ni $\{a_p\}$ ni $-\{a_p\}$ son positivas, entonces $\{a_p\}$ es nula.

Dem $\forall \varepsilon \in k^+, \forall n \in N, \exists\, r, s > n \ni a_r \le \varepsilon$, $-a_s \le \varepsilon$.

Entonces, para $n >> 0$, $|a_p - a_q| < \varepsilon$, si $p, q > n$.

Si tomamos $q = r$ y una $p > n$ arbitraria, concluímos que $a_p = (a_p - a_q) + a_r < \varepsilon + \varepsilon = 2\varepsilon$

Luego tomamos $q = s$, y $p > n$ arbitraria, de donde

$-a_p = (a_p - a_q) - a_s < 2\varepsilon$. $\therefore |a_p| < 2\varepsilon$.

$\therefore \{a_p\}$ es nula.

Entonces, dada $\{a_p\}$ de Cauchy, siempre pasa que $\{a_p\}$ es positiva, $-\{a_p\}$ es positiva, o $\{a_p\}$ es nula. $\therefore$ cada clase residual es positiva, negativa, o cero.

Trivialmente, la suma y el producto de sucesiones positivas es también positiva, y así concluímos la demostración del teorema.

†.

COROLARIO **Ω es un campo ordenado.**

Veamos ahora que con esta construcción de Ω, todo queda como queremos:

·) El orden en Ω extiende al orden de k, ya que si $\{a\} > \{b\}$,

entonces $\{a\} - \{b\} = \{a - b\} > 0$

$\Rightarrow \exists\, \varepsilon \in k^+ \ni a - b > \varepsilon > 0 \Rightarrow a > b$.

··) Si una sucesión $\{a_p\}$ define a un elemento α, y la sucesión $\{b_p\}$ define a $\beta \in \Omega$, de $a_p \geq b_p$ para $p > n$ se sigue que $\alpha \geq \beta$, ya que si $\alpha < \beta$, y por lo tanto $\beta - \alpha > 0$, existiría una ε y una $m \ni b_p - a_p > \varepsilon > 0 \quad \forall p > m$.

Si escogemos $p = m + n$, llegamos a una contradicción con la hipótesis $a_p \geq b_p$.

···) Si el orden de k es arquimedeano, entonces el orden en Ω es arquimedeano:

Sabemos que cada sucesión de Cauchy está acotada por arriba , y por lo tanto para cada elemento $w \in \Omega$, $\exists\, s \in k \ni w < s$. Si el orden de k es arquimedeano, entonces existe un "natural" (la imagen en k de $n \in \mathbf{N}$ es $n \cdot 1$, $1 \in k$). en k tal que $n > s$.

$\therefore \forall\, w \in \Omega \ \exists\, n > w$, e.d. el orden de Ω es arquimedeano.

TEO 28 **(Teorema de convergencia de Cauchy)**

El campo Ω no se puede extender propiamente con sucesiones de Cauchy, e.d. Cada sucesión de Cauchy $\{\alpha_p\}$ de Ω $(\alpha_p \in \Omega \ \ \forall p \in \mathbf{N})$ tiene límite en Ω.

Para demostrar este teorema, suponemos definidos en Ω los conceptos de valor absoluto, sucesión de Cauchy, sucesión nula y límite, de la manera natural, y hacemos las observaciones siguientes:

PRO 5 **Las sucesiones nulas de Ω forman un ideal.**

(La demostración es análoga a la que se hizo para R).

DEF 30 Decimos que $\{\alpha_p\}$ converge al límite α (En símbolos $\lim_{p\to\infty} \alpha_p = \alpha$, $\{\alpha_p\} \to \alpha$), si $\{\alpha_p\}$ es congruente a la sucesión constante $\{\alpha\}$ módulo el ideal de sucesiones nulas, e.d. sii $\{\alpha_p - \alpha\}$ es una sucesión nula.

Las sucesiones de Cauchy $\{\alpha_p\}$ que usamos para definir los elementos de Ω , se pueden pensar también como sucesiones de Cauchy en Ω , ya que $k \hookrightarrow \Omega$.

LEMA Si la sucesión $\{a_p\}$ de k define al elemento α de Ω, entonces $\lim a_p = \alpha$.

Dem Para cada $\varepsilon \in \Omega \ \exists\, \varepsilon' \in \Omega \ni \varepsilon' < \varepsilon$, $\exists\, n \in \mathbf{N} \ni$ si $p, q > n$, la relación

$|a_p - a_q| < \varepsilon'$ es válida. Si dejamos p fijo y hacemos tender q a ∞, se sigue que $a_p - \alpha \leq \varepsilon$, y

$\alpha - a_p \leq \varepsilon'$, $\therefore |a_p - \alpha| \leq \varepsilon' < \varepsilon$, $\therefore \{a_p - \alpha\}$ es nula.

Procedamos ahora a probar el teorema de convergencia de Cauchy.

En la prueba supondremos que en una sucesión $\{\alpha_p\}$, dos elementos sucesivos α_p, α_{p+1} siempre son distintos, o la sucesión es constante a partir de cierto momento (si no, escogemos una subsucesión que sí cumpla esto; la convergencia de esta subsucesión implica entonces la convergencia de la sucesión). En el segundo caso la sucesión converge trivialmente, así que supondremos siempre la primera condición.

Sea $\varepsilon_p = |\alpha_p - \alpha_{p+1}|$.

Como $\{\alpha_p\}$ es de Cauchy, $\{\varepsilon_p\}$ es nula. Por hipótesis, $\varepsilon_p > 0 \quad \forall p \in \mathbf{N}$.

$\forall \alpha_p \quad \exists a_p \in k \ni |a_p - \alpha_p| < \varepsilon_p$, porque α_p fue definido como el límite de una sucesión $\{a_{p_1}, a_{p_2}, \ldots\}$. Además, $\forall \varepsilon > 0 \ \exists n' \in \mathbf{N} \ni |\alpha_p - \alpha_q| < 1/3\varepsilon$ si $p, q > n'$, y $\exists n'' \in \mathbf{N} \ni \varepsilon_p < 1/3\varepsilon$ si $p > n''$.

Sea $n = \text{máx}\,(n', n'')$. Entonces, si $p, q > m$, $|a_p - \alpha_p| < 1/3\varepsilon$, $|\alpha_p - \alpha_q| < 1/3\varepsilon$ y $|\alpha_q - a_q| < 1/3\varepsilon$ $\therefore |a_p - a_q| \leq |a_p - \alpha_p| + |\alpha_p - \alpha_q| + |\alpha_q - a_q| < \varepsilon$.

$\therefore$ la sucesión $\{\alpha_p\}$ es congruente con $\{a_p - \alpha_p\}$ módulo una sucesión nula, y $\therefore$ tiene el mismo límite en Ω. †.

Probaremos ahora el principio del supremo:

TEO 29 Todo conjunto $S \subset \Omega$, $S \neq \varnothing$ y acotado superiormente tiene supremo.

Dem Sea s una cota superior de S, M un entero mayor que s, μ un elemento arbitrario de S, y m un entero mayor que $-\mu$. Entonces

$$-m < \mu < M.$$

Para cada número natural p, formamos el conjunto $\{k \cdot 2^{-p};\ k \in \mathbb{Z}\ \text{y}\ -m < k \cdot 2^{-p} < M\}$, que es un conjunto finito.

Sea a_p la más pequeña de estas fracciones, que son cotas superiores de S. Entonces $a_p - 2^{-p}$ ya no es cota superior. Por lo tanto, para cada $q > p$, tenemos:

$$(1) \ldots\ldots\ldots\ a_p - 2^{-p} < a_q \le a_p.$$

$$\Rightarrow |a_p - a_q| < 2^{-p},$$

$$\Rightarrow \quad (2) \ldots\ldots\ldots\ |a_p - a_q| < 2^{-n}, \qquad \text{ya que } p, q > n.$$

Para una ε dada, siempre podemos encontrar un entero $h < \varepsilon^{-1}$ que cumpla además $2^n > h > \varepsilon^{-1}$. Así (2) implica que $\{a_p\}$ es una sucesión de Cauchy. Esta sucesión define a un elemento $\omega \in \Omega$. Además, d. (1),

$$a_p - 2^{-p} < \omega \le a_p.$$

ω es un a cota superior de S, porque si existiera $\mu \in S \ni \mu > \omega$, podríamos encontrar un número $2^{-p} > (\mu - \omega)^{-1}$, y tendríamos entonces que $2^{-p} < (\mu - \omega)$. Sumando $a_p - 2^{-p} < \omega$, llegamos a que $a_p < \mu$, lo cual contradice el hecho de que a_p es una cota superior de S.

ω es la más chica de las cotas superiores de S, porque si σ fuera una cota superior menor, podríamos hallar otra vez un número p tal que $2^{-p} < \omega - \sigma$.

Como $a_p - 2^{-p}$ no es cota superior de S, existe una $\mu \in S$ tal que $a_p - 2^{-p} < \mu$. Esto implica que $a_p - 2^{-p} < \sigma$, y sumando esto con la expresión anterior obtenemos $a_p < \mu$, lo cual es falso. $\therefore \omega$ es el supremo de S.

T.

Resumiendo, diremos que la construcción descrita produce, para todo campo ordenado k, una única extensión ordenada Ω en la cual el principio del supremo es válido siempre que k sea arquimedeano. En particular, si k es el campo de los números racionales, entonces Ω es el campo de los números reales, que se ven entonces como clases residuales módulo I (el conjunto de sucesiones nulas) en el dominio de sucesiones de Cauchy de números racionales.

VALUACIONES

Se ha visto que una norma definida en un campo ordenado sirve para construir su completación. ¿Porqué no generalizar esta construcción?.

Se extiende el concepto de valor absoluto como sigue.

DEF 31 Sea **k** un campo. Una valuación en **k** es una función

$| \ | : \mathbf{k} \to \mathbf{R}$ que cumple las siguientes propiedades:

1) $|a| \geq 0$; $|a| = 0 \Leftrightarrow a = 0$.

2) $|ab| = |a||b|$

3) $|a+b| \leq |a| + |b|$

$\forall\, a, b \in \mathbf{k}$.

Si la valuación cumple además la propiedad

4) $|a+b| \leq \text{máx}\,\{|a|, |b|\}$ $\forall\, a, b \in \mathbf{k}$,

diremos que la valuación es no arquimedeana.

Obs 1 : Así como en el caso de las normas, una valuación induce una métrica:

$\mathbf{d}(a, b) = |a - b|$

i) $\mathbf{d}(a, b) = |a - b| \geq 0$; $\mathbf{d}(a, b) = |a - b| = 0 \Leftrightarrow (a - b) = 0 \Leftrightarrow a = b$.

ii) $\mathbf{d}(a, b) = |a - b| = |-1|\,|a - b|$ (ver teorema 31)

$\Rightarrow \mathbf{d}(a, b) = |(-1)(a - b)| = |b - a| = \mathbf{d}(b, a)$.

iii) $\mathbf{d}(a, c) = |a - c| = |a - b + b - c| \leq |a - b| + |b - c| = \mathbf{d}(a, b) + \mathbf{d}(b, c)$

Obs 2 : Si la valuación es no arquimedeana, la métrica inducida es una *ultramétrica*:

iv) $\mathbf{d}(a, c) = |a - c| = |a - b + b - c| \leq \text{máx}\,\{|a - b| + |b - c|\} =$

$\text{máx}\,\{\mathbf{d}(a, b), \mathbf{d}(b, c)\}$.

Unos resultados útiles:

TEO 30 Sea $|\ |: k \to \mathbb{R}$ una valuación no arquimedeana. Entonces $\forall a, b \in k$,

$$|a|>|b| \Rightarrow |a+b|=|a|$$

Dem $|a|=|(a+b)-b| \leq \text{máx}\{|a+b|,|b|\}$.

$|a+b|$ tiene que ser el máximo, porque si no tendríamos $|a| \leq |b|$, que contradice a la hipótesis. Entonces, $|a| \leq |a+b|$.

Por otro lado, $|a+b| \leq \text{máx}\{|a|,|b|\} = |a|$.

$\therefore |a+b|=|a|$ †.

TEO 31 Toda valuación $|\ |$ satisface:

$$|1|=1,\ |-1|=1,\ \left|\frac{a}{b}\right|=\frac{|a|}{|b|},\ ||a|-|b||_\infty \leq |a-b|.$$

(donde $|\ |_\infty$ es el valor absoluto usual definido en $\mathbb{R}$)

Dem i) $|1|=|1\cdot 1|=|1||1| \Rightarrow |1|=1$, ó $|1|=-1$. Pero $|a| \geq 0\ \forall a \in k$

$\therefore |1|=1$.

ii) $|-1|=|(-1)(-1)|=|-1||-1| \Rightarrow |-1|=1$.

iii) $|a/b|=|a\cdot b^{-1}|=|a||b^{-1}|=\frac{|a|}{|b|}$

iv) $|a|=|a-b+b| \leq |a-b|+|b| \Rightarrow |a|-|b| \leq |a-b| \ldots.(1)$

$|b|=|b-a+a| \leq |b-a|+|a|=|-1||b-a|+|a|=$

$|(-1)(b-a)|+|a|=|a-b|+|a|$, ent. $|b| \leq |a-b|+|a|$

$\Rightarrow -|b| \geq -|a-b|-|a| \Rightarrow -|b|-|a| \geq -|a-b| \ldots.(2)$

Combinando (1) y (2), obtenemos $||a|-|b||_\infty \leq |a-b|$ †.

TEO 32 Sea $|\ |: k \to \mathbf{R}$ una valuación.

Entonces $|\ |$ es no arquimedeana $\Leftrightarrow |n \cdot 1| \leq 1 \ \forall n \in \mathbf{Z}$.

Dem Si $|\ |$ es no arquimedeana, entonces $|a_1 + \ldots + a_n| \leq \text{máx}\,(|a_i|)$.

Entonces $|n \cdot 1| \leq |1| = 1 \ \forall n \in \mathbf{Z}$.

Inversamente, supongamos $|n \cdot 1| \leq 1 \ \ \forall n \in \mathbf{Z}$, y sean $a, b \in k$. Entonces $\forall n \in \mathbf{Z}^+$ tenemos $|a+b|^n = |a^n + \binom{n}{1} a^{n-1}b + \ldots + b^n| \leq |a|^n + |a^{n-1}|\,|b| + \ldots + |b|^n \leq$

$\leq (n+1)\text{máx}\,(|a|^n, |b|^n)$.

$\therefore \ |a+b| \leq (n+1)^{1/n}\,\text{máx}\,(|a|, |b|)$. Como $(n+1)^{1/n} \to 1$,

$|a+b| \leq \text{máx}\,(|a|, |b|)$.

Corolario1 Sea $|\ |: k \to \mathbf{R}$ una valuación, k un campo de característica p (Ver apéndice). Entonces $|\ |$ es no arquimedeana.

Dem Si $n \cdot 1 = 0 \pmod p$, entonces $(n \cdot 1)^{p-1} = 1 \pmod p$ (Ver teorema de Euler en el apéndice) y $\therefore |n \cdot 1|^{p-1} = 1 \ \Rightarrow |n \cdot 1| = 1$. Entonces $|\ |$ es no arquimedeana por el teorema anterior.

Corolario2 Sea $|\ |: k \to \mathbf{R}$ una valuación, k' un subcampo de k. Si $|\ |$ es trivial en k', entonces es no arquimedeana.

Dem Dado que $|\ |$ es trivial en k', $|n \cdot 1| = 1 \ \forall n \in \mathbf{Z}$. †

TEO 33 Sea $|\ |_1$ una función de un dominio entero A en R que satisface las condiciones que definen a una valuación, es decir:

$$|a| \geq 0; \quad |a| = 0 \Leftrightarrow a = 0, \qquad |ab| = |a|\,|b|, \text{ y}$$

$$|a+b| \leq |a| + |b|.$$

entonces $|\ |_1$ puede ser extendida de manera única a una valuación, $|\ |$, del campo de cocientes k.

Dem Si $|\ |$ es una valuación que extiende a $|\ |_1$, entonces es claro que $\forall\ x \in k$, $x = a/b$, $a, b \in A$, tiene que suceder que $|x| = \dfrac{|a|}{|b|} = \dfrac{|a|_1}{|b|_1}$. (*)

Así, queda demostrada la unicidad. Probemos ahora que (*) en efecto define una extensión $|\ |$ de $|\ |_1$ que es valuación.

Debemos probar primero que $|\ |$ está bien definida.

Supongamos entonces que $a/b = c/d$. Entonces $ad = bc$, y $|ad|_1 = |bc|_1$,

ó $|a|_1\,|d|_1 = |b|_1\,|c|_1$, $\dfrac{|a|_1}{|b|_1} = \dfrac{|c|_1}{|d|_1}$.

Probemos ahora que $|\ |$ satisface las condiciones de valuación :

Las primeras dos condiciones son claras. Para demostrar la tercera, sean $c, d \in A$, $y = c/d$.

Entonces $x + y = \dfrac{ad+bc}{bd}$, y $|x+y| = \dfrac{|ad+bc|_1}{|bd|_1} \leq \dfrac{|ad|_1}{|bd|_1} + \dfrac{|bc|_1}{|bd|_1} =$

$$= \frac{|a|_1}{|b|_1} + \frac{|c|_1}{|d|_1} = |x| + |y|.$$

Finalmente, es claro que $|\ |$ extiende a $|\ |_1$, porque si $a \in A$, entonces $a = ab/b$, donde $b \in A$, y $|a| = \dfrac{|ab|_1}{|b|_1} = \dfrac{|a|_1\,|b|_1}{|b|_1} = |a|_1$, lo cual termina la demostración †.

DEF 11 Sea $c \in \mathbb{R}$, $0 < c < 1$ un número real fijo.

Sea también $p \in \mathcal{P}$ un número primo fijo.

Si $x \in \mathbb{Q}^*$, podemos escribir x de la forma $x = p^{\alpha}\frac{a}{b}$, donde $a, b \in \mathbb{Z}$, $p \nmid ab$ y donde $\alpha \in \mathbb{Z}$ (α puede ser positiva, negativa o cero).

Entonces definimos la valuación p - ádica, $|\ |_p$, como $|x|_p = c^{\alpha}$, $|0|_p = 0$.

PROP 6 Así definida, $|\ |_p$ es una valuación arquimedeana.

Dem 1) Se sigue de la definición que $|x|_p \geq 0$, y que $|x|_p = 0 \Leftrightarrow x = 0$.

2) Si $y = p^{\beta}\frac{a'}{b'}$, donde $p \nmid a'b'$, entonces

$$xy = p^{\alpha+\beta}\frac{aa'}{bb'}, \text{ donde } p \nmid aa'bb'.$$

Por lo tanto $|xy|_p = c^{\alpha+\beta} = |x|_p\,|y|_p$.

3) Probaremos la condición $|x|_p \leq 1 \Rightarrow |1+x|_p \leq 1$.....(5), y probaremos que (5) ≡ (4)

i) Si $x \neq 0$, $|x|_p \leq 1 \Rightarrow \alpha \geq 0 \Rightarrow \exists\ c, d \in \mathbb{Q} \ni x = c/d$, donde $p \nmid d$, $(c, d) = 1$.

Entonces $1 + x = 1 + c/d = (c + d)/d$, que tiene denominador primo relativo con p,

$\therefore\ |1+x|_p \leq 1$. Como la condición (5) se cumple trivialmente en el caso $x = 0$, hemos demostrado la condición para todos los casos.

ii) (5) ≡ (4).

Si se satisface (4), entonces, $|x|_p \leq 1 \Rightarrow |1+x|_p \leq \text{máx}\{|x|_p, |1|\} = 1$.

Supongamos ahora (5) y supongamos que $y \neq 0$. (Si $y = 0$, (4) se cumple trivialmente).

También, s.p.g., supongamos que $|x|_p \leq |y|_p$. Entonces $|x/y|_p \leq 1$, y, por (5),

$\left|1+\frac{x}{y}\right|_p \leq 1 \Rightarrow |x+y|_p \leq |y|_p = \text{máx}\{|x|_p, |y|_p\}$ ∎

TEO 34 Sea $|\ |: \mathbf{Q} \to \mathbf{R}$ una valuación. Entonces pasa una de las siguientes posibilidades:

1) $|\ |$ es la valuación trivial; e.d. $|0| = 0$ y $|a| = 1 \quad \forall a \in \mathbf{Q}^*$.

2) $|\ | = |\ |_p$, una valuación p-ádica.

3) $|\ | = |\ |_\infty^\alpha$ una potencia del valor absoluto usual, con $0 < \alpha \leq 1$

Dem Sean $m, n \in \mathbf{Z}$, $m, n > 1$. Podemos escribir en base n, e.d.

(1) $m = a_0 + a_1 n + a_2 n^2 + \ldots + a_k n^k$

donde $0 \leq a_i \leq n-1, \forall i \in \{0, \ldots, k\}, a_i \in \mathbf{Z}$.

Esto se demuestra fácilmente con el segundo principio de inducción :

Sea n un natural mayor que 1 fijo, y supongamos que $\forall t \in \mathbf{N}$, $0 \leq t \leq m$, t se puede escribir "base n".

Aplicando el algoritmo de la división, sabemos que $\exists\, q, r \in \mathbf{N}$ ∋

$$m = qn + r, \quad 0 \leq r < n \quad \Rightarrow q < m.$$

$\therefore \exists\ a_1, \ldots, a_k \in \mathbf{N}$ ∋ $q = a_1 + a_2 n + \ldots + a_k n^{k-1}$, con $0 \leq a_i \leq n-1$, $\forall i \in \{0, \ldots, k\}$.

$m = qn + r \Rightarrow m = (a_1 + a_2 n + \ldots + a_k n^{k-1})n + r = a_1 n + a_2 n^2 + \ldots + a_k n^k + r.$

Si hacemos $a_0 = r$, ya que $r < n$, nos queda $m = a_0 + a_1 n + a_2 n^2 + \ldots + a_k n^k$,

con $0 \leq a_i \leq n-1, \forall i \in \{0, \ldots, k\}$.

Claramente, en la expresión (1), $n^k \leq m$, y ya que $n > 1$, esto implica que

$k \leq \dfrac{\log m}{\log n}$

Ahora, si $|\ |$ es una valuación en $\mathbf{Q}$,

$|a_i| = |1 + \ldots + 1| \leq |1| + \ldots + |1| \leq n.$

$\Rightarrow |m| \leq |a_0| + |a_1||n| + \ldots + |a_k||n|^k \leq n + n|n| + \ldots + n|n|^k =$

$= n(1+|n|+\ldots+|n|^k) \le n\ (k+1)\ \text{máx}\ (1,|n|)^k$,

(ya que $1,|n|,\ldots,|n|^k \le \text{máx}\ (1,|n|)^k$)

$\therefore\ |m| \le n\left(\frac{\log m}{\log n}+1\right)\text{máx}\ (1,|n|)^{\log m/\log n}$ (2).

La ecuación (2) es válida para cualesquiera enteros positivos mayores que uno, entonces, para el entero m^τ, (2) queda $|m^\tau| \le n\left(\frac{\tau \log m}{\log n}+1\right)\text{máx}\ (1,|n|)^{\tau \log m/\log n}$

$$\therefore\quad |m| \le \sqrt[\tau]{n\left(\frac{\tau \log m}{\log n}+1\right)}\ \text{máx}\ (1,|n|)^{\log m/\log n} \qquad (3)$$

Lemal $\sqrt[\tau]{\tau} \underset{\tau\to\infty}{\longrightarrow} 1$

Dem ι) Basta con probar que $\frac{\log \tau}{\tau} \underset{\tau\to\infty}{\longrightarrow} 0$, ya que si hacemos

$$x = \sqrt[\tau]{\tau},\ \text{entonces}\quad x^\tau = \tau \ \Rightarrow\ \tau \log x = \log \tau \ \Rightarrow\ \log x = (\log \tau)/\tau$$

$$\therefore\ x = e^{\frac{\log \tau}{\tau}}\ ,\ \text{y así, si}\ \frac{\log \tau}{\tau} \underset{\tau\to\infty}{\longrightarrow} 0,\ e^{\frac{\log \tau}{\tau}} = \sqrt[\tau]{\tau} \underset{\tau\to\infty}{\longrightarrow} 0$$

ιι) Dado que $\log \tau \underset{\tau\to\infty}{\longrightarrow} \infty$, y $\tau \underset{\tau\to\infty}{\longrightarrow} \infty$, $\lim_{\tau\to\infty} \frac{\log \tau}{\tau} = \lim_{\tau\to\infty} \frac{(\log \tau)'}{(\tau)'} = \lim_{\tau\to\infty} \frac{1/\tau}{1} = \lim_{\tau\to\infty} \frac{1}{\tau} =$

Usando el lema 1, y haciendo tender $\tau \to \infty$, obtenemos, de (3):

$$|m| \le \text{máx}\ (1,|n|)^{\log m/\log n} \qquad (4).$$

Para terminar esta demostración necesitaremos de un lema más, que enunciamos en seguida:

Lema 2 Sea k un campo y $|\ |: k \to \mathbf{R}$ una valuación. Supongamos que $|m| \le d$ para todos los enteros m de k. Entonces $|\ |$ es no arquimedeana.

Dem $|a+b|^\tau = |(a+b)^\tau| = |a^\tau + \binom{\tau}{1} a^{\tau-1}b + \binom{\tau}{2} a^{\tau-2}b^2 + \ldots + b^\tau| \le$

$\le |a|^\tau + \left|\binom{\tau}{1}\right| |a|^{\tau-1}|b| + \ldots + |b|^\tau \le (\tau+1)\, d\ \text{máx}\ (|a|,|b|)^\tau$.

Tomando raíz τ-ésima de los dos lados, y haciendo que τ tienda a infinito, llegamos a que $|a+b| \leq \text{máx}(|a|,|b|)$, lo que implica que la valuación es no arquimedeana.

Para concluír la demostración del teorema, tomaremos en cuenta los siguientes dos casos:

1) $\exists\ n>1 \ni |n| \leq 1$.
2) $\forall\ n>1,\ |n|>1$.

Caso 1) $\exists\ n>1 \ni |n| \leq 1$. De (4), llegamos a que $|m| \leq 1 \quad \forall\ m>1$.

Además, dado que $|-1|=1$, concluímos que $|m| \leq 1 \quad \forall\ m \in \mathbb{Z}$.

por lo tanto, usando el lema 2, $|\ |$ es no arquimedeana.

En vista del teorema 33, si $|m|=1 \quad \forall\ m \in \mathbb{Z}^*$, necesariamente $|\ |$ es la valuación trivial.

Supongamos entonces que $\exists\ m \in \mathbb{Z},\ m>1 \ni |m|<1$. Entonces $\{x \in \mathbb{Z}^+ ; |x|<1\} \neq \varnothing$ tiene primer elemento p. p es primo, ya que si $p=ab$ con $a,b \in \mathbb{Z}^+$, $a, b<p$, entonces

$$|p|=|a|\,|b|=1 \quad \Rightarrow \quad |a|=|b|=1 \ \forall .$$

PROP 7 Sea $m \in \mathbb{Z}$. Entonces $|m|<1 \Leftrightarrow p \mid m$.

Dem $\Leftarrow$) Si $p \mid m$, sea $x \in \mathbb{Z} \ni px=m$. Entonces $|m|=|m|=|px| \leq |p|+\ldots+|p| \leq$

$\leq |p|<1$.

$\Rightarrow$) Sean $q, r \in \mathbb{Z}^+ \ni m=qp+r,\ 0 \leq r<p$. Supongamos $r \neq 0$. Como $r<p$, $|r|=1$. $\therefore |m|=1$, ya que $|qp|=|p+\ldots+p| \leq |p|<1$, y $|\ |$ es no arquimedeana.

Pero $|m|=1$ es una contradicción, $\therefore r=0 \Rightarrow p \mid m$.

Sea $x \in \mathbb{Q}$. Sabemos que $\exists\ \alpha, a,b \in \mathbb{Z} \ni x=p^{\alpha}\frac{a}{b}$, donde $p \nmid a,\ p \nmid b$.

Por la discusión anterior, $|a|=|b|=1 \Rightarrow \left|\frac{a}{b}\right| = \frac{|a|}{|b|} = 1$.

$\therefore |x| = \left|p^{\alpha}\frac{a}{b}\right| = |p^{\alpha}|\left|\frac{a}{b}\right| = |p^{\alpha}| = |p|^{\alpha}$.

Sea $c = |p|$. Dado que $0 < c < 1$, hemos probado ya que $|\ |$ es una valuación p-ádica.

Pasemos ahora al caso 2.

Caso 2) $\forall n > 1,\ |n| > 1$.

Se sigue entonces de (4), que $|m| \le |n|^{\log m/\log n} \Rightarrow |m|^{1/\log m} \le |n|^{1/\log n}$.

Como esta ecuación es válida $\forall m, n \in \mathbb{Z}\ \ni m, n > 1$, podemos intercambiar n y m y así obtenemos $|m|^{1/\log m} = |n|^{1/\log n}\ \forall m, n > 1$.

$\therefore |m|^{1/\log m} = c$, una constante $\forall m > 1$.

Dado que $\log m$ es positivo $\forall m > 1$, c tiene que ser una constante positiva.

Por conveniencia, podemos escribir $c = e^{\alpha}$, $\alpha > 0$. Entonces $|m| = e^{\alpha \log m} = m^{\alpha}$.

Como $|-1| = 1, |-m| = |m| = m^{\alpha}\ \forall m \in \mathbb{Z}$. Así, si $|m| = |m|_{\infty}\ \forall m \in \mathbb{Z}$, aplicando otra vez el teorema 33, si $x = \frac{m}{n}$, $|x| = \frac{|m|}{|n|} = \frac{|m|_{\infty}^{\alpha}}{|n|_{\infty}^{\alpha}} = \left|\frac{m}{n}\right|_{\infty}^{\alpha} = |x|_{\infty}^{\alpha}$

y así queda demostrado el teorema. †

Obs: Si convenimos en que dos valuaciones $|\ |_1$ y $|\ |_2$ son equivalentes ($|\ |_1 \sim |\ |_2$) si y sólo si $\forall a \in k\ \ |a|_1 < 1 \Rightarrow |a|_2 < 1$, entonces:

1) La relación $\sim$ es de equivalencia.

Reflexividad: $|a|_1 < 1 \Leftrightarrow |a|_1 < 1$

Transitividad: $(|a|_1 < 1 \Rightarrow |a|_2 < 1$ y $|a|_2 < 1 \Rightarrow |a|_3) \Rightarrow$

$(|a|_1 < 1 \Rightarrow |a|_2 < 1)$.

Simetría: $|a|_1 > 1 \Rightarrow \left|\frac{1}{a}\right|_1 < 1 \Rightarrow \left|\frac{1}{a}\right|_2 \Rightarrow |a|_2 > 1.$

P.D. $|a|_1 = 1 \Rightarrow |a|_2 = 1$. Supongamos que $|a|_1 = 1$. Sabemos que

$\exists\ b \in k^*$ ∋ $|b|_1 < 1$ (Si no, $|\ |_1$ sería trivial). Entonces $|a^n b|_1 = |a|_1^n$

$|b|_1 < 1 \Rightarrow |a|_2 < \left(\frac{1}{|b|}\right)^{\frac{1}{n}}$. Si hacemos $n \to \infty$, obtenemos $|a|_2 \leq 1$.

Repitiendo todo lo anterior para $1/a$, llegamos a que $|1/a|_2 \leq 1 \Rightarrow$

$|a|_2 \geq 1,\ \therefore |a|_2 = 1.$

†.

2) Todas las valuaciones de la forma $|\ |_\infty^\alpha$ son equivalentes:

Sean $|\ |_1 = |\ |_\infty^{\alpha_1}$ y $|\ |_2 = |\ |_\infty^{\alpha_2}$ dos potencias del valor absoluto $|\ |_\infty$,

y sea $a \in k$ tal que $|a|_1 < 1$.

Dado que tanto α_1 como α_2 necesariamente son positivas,

$|a|_\infty^{\alpha_1} < 1 \Rightarrow |a|_\infty^{\alpha_2} < 1 \Rightarrow |a|_2 = |a|_\infty < 1.$

†.

3) Dado $p \in \mathbb{P}$ fijo, la definición de valuación p-ádica $|\ |_p$ requiere de un número $c \in \mathbb{R}$, $0 < c < 1$. Si cambiamos ese número c por otro real $d \in \mathbb{R}$, $0 < d < 1$, las valuaciones resultantes son equivalentes.

TEO 35 Sea $k = F(x)$ el campo de funciones racionales con coeficientes en el campo F. Entonces las únicas valuaciones que extienden a la valuación trivial en F son de la forma $|h(x)| = c^{\partial(\mathfrak{h}) - \partial(\mathfrak{g})}$, donde $h(x) = \frac{f(x)}{g(x)} \in F(x)$, y $c = |x|$

Dem Por el lema2, cualquier valuación $|\ |$ que sea trivial en F debe ser no arquimedeana.

° Caso 1 $|x| \leq 1$.

Entonces, $\forall f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$, $|f(x)| \leq \max\{1, |x|, \ldots, |x|^n\} \leq 1$, ya que $|\ |$ es no arquimedeana. Si $|f(x)| = 1 \ \forall f(x) \in F[x] \ni f(x) \neq 0$, entonces el teorema 33 asegura que $|\ |$ es la valuación trivial.

Lema 3 Sea $|\ |$ una valuación no arquimedeana en un campo k.

Sean $V = \{a \in k ; |a| \leq 1\}$. $P = \{a \in k ; |a| < 1\}$.

Entonces V es un anillo con uno y P es el único ideal maximal de V (y por lo tanto es un ideal primo).

Dem $|0| = 0$; $|1| = 1$.

Si $a, b \in V$, entonces $|a - b| \leq \max\{|a|, |b|\} < 1$; $|ca| = |c||a| < 1$.

$\therefore$ P es ideal. Además, si $d \in (V - P)$, entonces $|d| = 1 \Rightarrow d^{-1} \in (V - P)$, e.d. P es el único ideal maximal de V. †.

Sabemos, por el lema 3, que $P = \{f(x) \in F[x]; |f(x)| < 1\}$ es un ideal maximal, y por lo tanto un ideal principal generado por un polinomio irreducible $p(x)$ (Ver Apéndice).

$\therefore |f(x)| < 1 \Leftrightarrow p(x) | f(x)$.

Ahora, si $h(x) \in F(x)$, sabemos que $\exists a(x), b(x) \in F[x]$ y $\alpha \in \mathbb{Z} \ni$ $h(x) = p(x)^{\alpha} \dfrac{a(x)}{b(x)}$, con $p(x) \nmid a(x) b(x)$. Entonces $|h(x)| = |p(x)|^{\alpha} = c^{\alpha}$, con $0 < c < 1$.

Caso 2 $|x| > 1$.

Sea $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$. Entonces $|f(x)| = |x|^n = c^{\partial(f(x))}$, $c > 1$.

Si $h(x) \in F(x)$, $h(x) = \dfrac{f(x)}{g(x)}$, y $|h(x)| = \dfrac{|f(x)|}{|g(x)|} = |x|^{\partial(f(x)) - \partial(g(x))}$.

Obs: Se puede generalizar lo visto en los teoremas 34 y 35 de la siguiente manera:

Sea A un dominio de factorización única, y $c \in \mathbf{R}$, $0 < c < 1$. Entonces, para $x \in A$, con $x = \prod p^{\alpha_p}$ su factorización, definimos $|x|_p = c^{\alpha_p}$.

Es fácil ver que así definida, $|\ |_p$ es una valuación. Por el teorema 33 , $|\ |$ se extiende de manera única al campo de cocientes de A, k. $|\ |_p$ se llama valuación p-ádica de k.

TEO 36 Dadas n valuaciones p-ádicas $|\ |_{p_i}$, $i = 1, \ldots, n$ de $\mathbf{Q}$, y n elementos arbitrarios a_i, $i = 1, \ldots, n$ de $\mathbf{Q}$ y $\varepsilon > 0$, existe $a \in \mathbf{Q}$ ∋ $|a - a_i|_{p_i} < \varepsilon$ $(i = 1, \ldots, n)$

y $|a|_p \leq 1$ para toda otra valuación.

Dem Para demostrar este resultado necesitaremos primero de dos lemas, que a su vez son importantes teoremas de aproximación.

Lema1 Dadas n valuaciones no triviales y no equivalentes $|\ |_i$, $i = 1, \ldots, n$ de un campo k, $\exists\, a \in k$ ∋ $|a|_1 > 1$ y $|a|_i < 1$, $i = 2, \ldots, n$.

Dem (Inducción)

$n = 2$. $\exists\, b \in k$ ∋ $|b|_1 > 1$ y $|b|_2 \leq 1$, porque $|\ |_1 \neq |\ |_2$. También existe $c \in k$ ∋ $|c|_1 \leq 1$ y $|c|_2 > 1$. Así, $\left|\frac{b}{c}\right|_1 = \frac{|b|_1}{|c|_1} > 1$ y $\left|\frac{b}{c}\right|_2 = \frac{|b|_2}{|c|_2} < 1$, $\therefore a = \frac{b}{c}$ es el elemento buscado.

Supongamos ahora válido el teorema para el caso $n - 1$, y demostrémoslo para n:

Por hipótesis de inducción, $\exists\ d \in k \ni |d|_1 > 1$, y $|d|_i < 1$ para $i = 2, \ldots, n-1$.

También $\exists\ c \in k \ni |c|_1 > 1$ y $|c|_n < 1$, como en el caso particular $n = 2$..

Caso 1 $|d|_n \leq 1$.

Sea $a = d^j c$, con j suficientemente grande para que $|a|_i = |d|_i^j |c|_i < 1$, $2 \leq i < n$.

Entonces a funciona, porque $|a|_1 = |d|_1^j |c|_1$, $|a|_n = |d|_n^j |c|_n < 1$.

Caso 2 $|d|_n > 1$. Sea $a \in k$,

$a = \frac{d^j c}{1+d^j}$. Entonces $\frac{d^j c}{1+d^j} \underset{j\to\infty}{\to} c$, porque $\left|\frac{d^j}{1+d^j} - 1\right|_i = \left|\frac{1}{1+d^j}\right|_i = \left|\frac{(1/d)^j}{1+(1/d)^j}\right| \underset{j\to\infty}{\to} 0$

$\therefore |a|_i \underset{c\to\infty}{\to} |c|_i$, ya que $||a|-|b|| \leq |a-b|$.

Ahora, $|a|_n \leq \frac{|d|_n^j |c|_n}{|d|_n^j - 1}$. Y análogamente al caso anterior, el lado derecho de esta desigualdad tiende a $|c|_n$. $\therefore |a|_n < 1$ para $j >> 0$. Por último, si $2 \leq i < n$,

$|a|_i \leq \frac{|d|_i^j |c|_i}{1-|d|_i^j}$, y el lado derecho de esta desigualdad tiende a c. $\therefore\ \exists\ j >> 0 \ni$

$a = \frac{d^j c}{1+d^j}$ satisface las condiciones del lema.

Lema 2 Dadas $|\ |_i$, $i = 1, \ldots, n$, n valuaciones no triviales y no equivalentes de un campo k, y dado $\varepsilon > 0$ un número real, $\exists\ d \in k \ni |d-1|_1 < \varepsilon$ y $|d|_i < \varepsilon$

$\forall\ i = 2, \ldots, n$.

Dem Por el lema 1, existe $a \in k \ni |a|_1 > 1$ y $|a|_i < 1 \quad \forall\ i = 2, \ldots, n$.

Sea $d = \frac{a^j}{1+a^j}$. Entonces $|d-1|_1 = \left|\frac{-1}{1+a^j}\right|_1 \leq \frac{1}{|a|_1^j - 1}$, ya que

$|-1-a^j| \geq |a^j| - 1\ (||a|-|b|| \leq |a-b|)$. Y así, $|d-1|_1 < \varepsilon$ para $j >> 0$. †.

Continuamos ahora con la demostración del teorema 36. Sea $\varepsilon' < \varepsilon / n\alpha$, donde

$\alpha = \max \{|a_i|_j\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,n}}$. Sabemos (lema 2) que existen n elementos en k, d_i, i = 1, . . . , n tales que $|d_i - 1| < \varepsilon'$, y $|d_i|_j \leq \varepsilon'$ para $j \neq i$.

Sea $a = a_1 d_1 + \ldots + a_n d_n$.

Entonces $|a - a_i|_i = |a_1 d_1 + \ldots + a_i(d_i - 1) + \ldots + a_n d_n|_i \leq$

$\leq |a_1|_i \varepsilon' + \ldots + |a_i|_i \varepsilon' + \ldots + |a_n|_i \leq \varepsilon' (n\alpha) < \varepsilon$, con lo cual queda demostrada la primera parte del teorema.

Demostraremos ahora que $|a|_p \leq 1$ para toda otra valuación p-ádica.

Primero probaremos esta afirmación en el caso en el que todos los elementos involucrados son enteros. Así, dados enteros c_i, y primos distintos p_i (i = 1, . . . , n), suponiendo que podemos encontrar un entero c ∋ $|c - c_i|_{p_i} < \delta$ (i = 1, . . . ,m) y $|c|_p \leq 1$ para todo otro primo p, demostraremos que el problema original tiene solución.

Sea d el m.c.d. de las a_i y sean $c_i = da_i$ (i = 1, . . . , n) y $c_i = 0$ (i = n +1, . . . , m), donde $m - n$ es el número de primos para los cuales $|d|_p \neq 1$, y finalmente, sean

$\delta_1 = \min_{1 \leq i \leq n} |d|_{p_i} \varepsilon$, $\quad \delta_2 = \min_{p \in A} |d|_p$,donde A = ($p \in \mathcal{P}$; $|p| \neq 1$).

Sea $\delta = \min(\delta_1, \delta_2)$. Entonces existe $c \in \mathbb{Z}$ ∋

$|c - da_i|_{p_i} < \delta < |d|_{p_i} \varepsilon$. (i = 1, . . . , n),

$|c - 0|_p < \delta < |d|_p \quad \forall p$ ∋ $|d|_p \neq 1$, y $|c|_p \leq 1 = |d|_p \quad \forall p$ ∋ $|d|_p = 1$.

Entonces claramente $a = c/d$ es el racional que resuelve el problema original.

Sabemos que siempre existe un entero a tal que $|a|_p \leq 1$, así que basta con ver que se cumplen las condiciones $|a - a_i|_{p_i} < \varepsilon$ (i = 1, . . . , n).

Pero esto es equivalente a decir $a \equiv a_1 \pmod{p_1}$, con un natural n_1 suficientemente grande. Los módulos son primos relativos, y entonces el teorema chino del residuo garantiza que las congruencias tienen solución (Ver apéndice),con lo cual terminamos la demostración. Obs: Puede probarse que el teorema que acabamos de demostrar para Q es, de hecho, equivalente al teorema chino del residuo, pero en este trabajo no daremos la demostración.

El proceso para completar campos con respecto a una valuación es igual al descrito en el capítulo anterior. Veamos ahora cómo resultan estas *compleciones*.

NÚMEROS P - ÁDICOS

El campo que resulta de la compleción del campo de los número racionales con respecto a la valuación $|\ |_p$ es el campo de los números p-ádicos. $(\mathbf{Q}_p)$. En los siguientes párrafos trataremos de averiguar un poco la naturaleza de este campo.

TEO 37 Sea $\alpha \in \mathbf{Q}_p$ un número p-ádico. Entonces α se puede escribir de la forma:

$$\alpha = \sum_{j=n}^{\infty} a_j p^j \text{, donde las } a_j \in \mathbf{Z} \text{ y } n \in \mathbf{N} \text{ es } \ni\ |\alpha|_p = |p|_p^n.$$

Dem Sea $\alpha \in \mathbf{Q}_p$, $\alpha \neq 0$. Sabemos por el teorema 1 del apéndice que $|\mathbf{Q}_p|_p = |\mathbf{Q}|_p$, donde la extensión de $|\ |_p$ a $\mathbf{Q}_p$ la denotamos también como $|\ |_p$. Entonces $|\alpha|_p = |p|_p^n \Rightarrow$

si $\beta = \alpha/p^n$, $|\beta|_p = 1$, e.d. β es una unidad del anillo de valuación $\mathbf{V}$ de $|\ |_p$ en $\mathbf{Q}$ descrito en el capítulo anterior. Sean $\mathbf{P}$ el único ideal maximal de $\mathbf{V}$, $\hat{\mathbf{V}}$ el anillo de valuación de $|\ |_p$ en $\mathbf{Q}_p$ y $\hat{\mathbf{P}}$ el único ideal maximal de $\hat{\mathbf{V}}$.

Ya que $|\beta|_p = 1, \beta \in \hat{\mathbf{V}}$. Pero $\beta = \lim c_k \in \mathbf{Q}$. Entonces $\exists\, n \in \mathbf{N} \ni \forall\, k \geq n$, $|\beta - c_k|_p < 1$. Y entonces $|c_n|_p = |\beta + (c_n - \beta)|_p = \text{máx}\,(|\beta|_p, |c_n - \beta|_p) = |\beta|_p = 1 \Rightarrow$ $c_n \in \mathbf{V}$. Dado que $|\beta - c_n|_p < 1$, $(\beta - c_n) \in \hat{\mathbf{P}} \Rightarrow \beta + \hat{\mathbf{P}} = c_n + \hat{\mathbf{P}}$. Ya que $|c_n|_p = 1$, es posible encontrar dos enteros e_n, d_n primos relativos con p tales que $c_n = e_n/d_n$.

$(p, d_n) = 1 \Rightarrow \exists\, \mathbf{x}, \mathbf{y} \in \mathbf{Z} \ni \quad \mathbf{x}d_n + \mathbf{y}p = 1$ (Ver apéndice).

Entonces $\dfrac{e_n}{d_n} - e_n\mathbf{x} = \dfrac{e_n(1 - d_n\mathbf{x})}{d_n} \equiv 0 \pmod{\mathbf{P}} \Rightarrow c_n - e_n\mathbf{x} \in \hat{\mathbf{P}}$.

Si hacemos $e_n\mathbf{x} = a_n$, entonces $a_n \in \mathbf{Z}$, y $\beta + \hat{\mathbf{P}} = b_n + \hat{\mathbf{P}} = a_n + \hat{\mathbf{P}}$. Ahora,

$|a_n - \beta|_p < 1$, y tenemos $\quad |a_n p^n - \beta p^n|_p < |p^n|_p, \quad$ (*)

o $\alpha = \beta p^n = a_n p^n + (\beta - a_n)p^n = a_n p^n + \gamma_1$, donde $\gamma_1 = (\beta - a_n)p^n$,

y $\quad$ (*) $\Rightarrow |\gamma_1|_p < |p|_p^n$.

Entonces $|\gamma_1|_p = |p|_p^m$, donde $m > n$, y tenemos entonces el mismo tipo de relación con el que empezamos para α al principio de esta disertación. Así, si repetimos todo para γ_1, depués de k pasos llegamos a

$\alpha = a_n p^n + a_{n+1} p^{n+1} + \ldots + a_{n+k-1} p^{n+k-1} + \gamma_k$, donde $a_i \in Z$ y $|a_i|_p = 1$, ó $a_i = 0$, y donde $|\gamma_k|_p \leq |p|_p$.

Como $|p|_p^{n+k} \underset{k\to\infty}{\to} 0$, hemos acabado la demostración del teorema. †.

Obs: Los coeficientes a_i de la expansión p-ádica de un número sólo son únicos módulo p. Si se acepta la convención de tomar en vez de cada a_i su residuo módulo p, entonces podemos decir que son únicos.

Ejemplo Ejemplificaremos lo anterior para el elemento 3/8 de $\mathbf{Q}_5$.

Como $|3/8|_5 = |5|_5^0 = 1$. $n = 0$.

$x = 2$ es una solución de la congruencia $8x \equiv 1 \pmod 5$, y como $2 \cdot 3 \equiv 1 \pmod 5$, concluímos que $a_0 = 1$. Entonces $\gamma_1 = (3/8 - 1) = -5/8$, y $|-5/8|_5 = |5|_5$, de donde $a_1 \neq 0$, y $-(5/8 \cdot 5) = -1/8$. Otra vez, $x = 2$ es una solución de la congruencia $8x \equiv 1 \pmod 5$, y $2(-1) \equiv 3 \pmod 5$. Por lo tanto, $a_1 = 3$. Ahora, $\gamma_2 = (-1/8 - 3)\,5 = (-25/8)\,5$, por lo que $|\gamma_2|_5 = |5|_5^3$, de donde concluímos que $a_2 = 0$, pero $a_3 \neq 0$, y como $\gamma_2 / 5^3 = -1/8$, análogamente a lo anterior, $a_3 = 3$.

Es fácil ver que $a_4 = a_6 = \ldots = 0$; $a_5 = a_7 = \ldots = 3$.

Obs: Si $\alpha \in \mathbf{Q}_p$, digamos $\alpha = \frac{a_{-v}}{p^v} + \frac{a_{-v+1}}{p^{v+1}} + \ldots + a_0 + a_1 p + a_2 p + \ldots$, se acostumbra abreviar como sigue: $\alpha = a_{-v} a_{-v+1} \ldots a_0, a_1 a_2 \ldots \ (p)$.

Entonces el ejemplo quedaría $3/8 = 1, 30\,30\,30\ldots \pmod 5$

Terminaremos este trabajo con un ejemplo de "geometría poco usual" derivada de una ultramétrica.

Ejemplo Veamos como es una circunferencia en $\mathbf{Q}_p$

Sea $p = 2$, $c = 1/p$.

($|u|_2 = 2^{-\alpha}$, donde $u = 2^{\alpha} a/b$, $2 \nmid ab$

Entonces $\mathcal{C}_1(0) = \{u \in \mathbf{Q};\ |u|_2 = 1\}$.

$$|m/n|_p = 1 \Leftrightarrow m/n = p^0 (m_1/n_1), \text{ donde } 2 \nmid m_1 n_1.$$

e.d., $m/n \in \mathcal{C}_1(0) \Leftrightarrow m/n = (2a+1)/(2b+1)$. e.d., m/n = impar/impar.

Int $\mathcal{C}_1(0) = \{v \in \mathbf{Q};\ |v|_2 < 1\}$.

$$m/n \in \text{Int } \mathcal{C}_1(0) \Leftrightarrow m/n = p^{\alpha} (m_1/n_1), \text{ donde } p \nmid m_1 n_1,\ \alpha > 0.$$

e.d., $m/n \in$ Int $\mathcal{C}_1(0) \Leftrightarrow m/n = (2a)/(2b+1)$. e.d., m/n = par/impar.

Ext $\mathcal{C}_1(0) = \{v \in \mathbf{Q};\ |v|_2 < 1\}$.

$$m/n \in \text{Ext } \mathcal{C}_1(0) \Leftrightarrow m/n = p^{\alpha} (m_1/n_1), \text{ donde } p \nmid m_1 n_1,\ \alpha < 0.$$

e.d., $m/n \in$ Ext $\mathcal{C}_1(0) \Leftrightarrow m/n = (2a+1)/(2b)$. e.d., m/n = impar/par.

Grafiquemos algunos puntos de la circunferencia, algunos puntos "centro" (puntos del interior) y algunos del exterior, para tener una idea más clara de cómo es.

1) – 2, 0, 4/3, 4, 100, etc, son centros.

2) 1/3, 1/5, $1/5^n$, 5, 5^n, etc, son puntos de la circunferencia.

3) 1/2, $1/2^n$, 5/2, – 321/2, etc, son puntos del exterior.

(Ver figura 10)

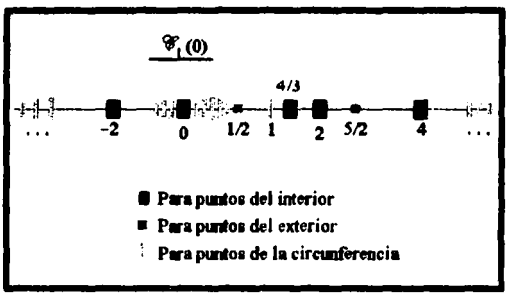

FIGURA 10

APÉNDICE

TEOREMA 1

Sea $|\ |: k \to \mathbb{R}$ una valuación no arquimedeana. Entonces $|k| = |\hat{k}|$, donde $\hat{k}$ es la compleción de k con respecto a $|\ |$.

Dem Sea $\alpha \in \hat{k}$. Si $\alpha = 0$, $|\alpha| = 0$. Supongamos entonces que $\alpha \neq 0$. Como k es denso en $\hat{k}$, existe una sucesión de Cauchy (a_n) de elementos de k tal que $\lim a_n = \alpha$. Como $|\ |$ es no arquimedeana, $|a_n| = |\alpha + (a_n - \alpha)| = \text{máx}\,\{|\alpha|, |a_n - \alpha|\} = |\alpha|$, para $n \in \mathbb{N}$ suficientemente grande, dado que se puede hacer a $|a_n - \alpha|$ tan chico como se quiera. Entonces $|a_n| = |\alpha|$ para n suficientemente grandes, con lo cual queda demostrado el teorema.

TEOREMA 2 Sean $a, b \in \mathbb{Z}^+$. Entonces la congruencia $ax \equiv b \pmod{m}$ tiene solución $\Leftrightarrow$ $(m, a) \mid b$.

Dem $\Leftarrow$) Si $(m, a) \mid b$, entonces $\exists\, \alpha, \beta, c \in \mathbb{Z} \ni (\alpha c)m + (-\beta c)a = (-b) \Rightarrow$ $m \mid (\beta c)a - b \Rightarrow ax \equiv b \pmod{m}$ tiene solución.

$\Rightarrow$) $ax \equiv b \pmod{m}$ tiene solución $\Rightarrow \exists\, x \in \mathbb{Z} \ni m \mid (ax - b) \Rightarrow$ $\exists\, \alpha \in \mathbb{Z} \ni m\alpha = (ax - b) \Rightarrow -m\alpha + ax = b \Rightarrow (m, a) \mid b$.

TEOREMA 3 Sean $a, b \in \mathbb{Z}^+$ tales que $(a, b) = 1$. Entonces $\exists\, x, y \in \mathbb{Z} \ni$ $xa + yb = 1$.

Dem Dado que $(a, b) = 1$, la congruencia $ax \equiv 1 \pmod{b}$ tiene solución $\Rightarrow \exists\, x, y \in \mathbb{Z}$ tales que $b(-y) = ax - 1 \Rightarrow ax + by = 1$.

DEFINICIÓN 1 La función ϕ de Euler se define para todos los enteros positivos de la siguiente manera:

$$\begin{cases} \phi(1) = 1, \\ \phi(n) = |\{m \in \mathbb{Z}^+ ; m < n, (m,n) = 1\}| \end{cases}$$

TEOREMA 4 (EULER) Si n es un entero positivo y $a \in \mathbb{Z}$ es primo relativo con n, entonces

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Dem Sabemos que el conjunto de números enteros positivos menores que n y primos relativos con n forma un grupo bajo la multiplicación módulo n, y sabemos también que en todo grupo finito G, $a^{o(G)} = e$. (Teorema de Lagrange). Combinando estos dos resultados, obtenemos $a^{\phi(n)} \equiv 1 \pmod{n}$.

DEFINICIÓN 2 Sea k un campo. Si $\forall\ a \in \mathbf{k}^*$, $\forall\ m \in \mathbb{Z}$, $am = 0 \Rightarrow m = 0$, decimos que k es de característica 0.

Decimos que k es de característica finita, si existe un entero $m \neq 0$ tal que $ma = 0$ para algún $a \in \mathbf{k}^*$.

En este caso definimos a la característica de k como el primer elemento del conjunto $\{m \in \mathbb{Z}^+ ; ma = 0 \text{ p.a. } a \in \mathbf{k}^*\} \subseteq \mathbb{Z}^+$ (Si $m \in \mathbb{Z}$ es tal que $ma = 0$, entonces $(-m)a = -(ma) = 0 \Rightarrow \{m \in \mathbb{Z}^+ ; ma = 0 \text{ p.a. } a \in \mathbf{k}^*\} \neq \varnothing$.

PROPOSICIÓN Sea k un campo, y $m \in \mathbb{Z}^+$ ∋ $ma = 0$ para alguna $a \in k^*$. Entonces

$mb = 0 \ \forall \ b \in k$.

Dem Dado que $m \in k^*$, $\exists \ a^{-1} \in k^*$ ∋ $aa^{-1} = 1 \Rightarrow m \cdot 1 = maa^{-1} = 0a^{-1} = 0$. Y así, para todo $b \in k$, $mb = m(1 \cdot b) = (m \cdot 1)b = 0$.

PROPOSICIÓN Sea k un campo de característica finita. Entonces su característica es un número primo.

Dem Sea p la característica de k. Supongamos que $p = bc$, $1 < b, c < p$.
Entonces $p \cdot 1 = 1 \Rightarrow bc \cdot 1 = (b \cdot 1)(c \cdot 1) = 0 \Rightarrow b \cdot 1 = 0$ ó $c \cdot 1 = 0$ ∇, porque p es el primer elemento del conjunto $\{m \in \mathbb{Z}^+; ma = 0 \text{ p.a. } a \in k^*\}$.

$\therefore p$ es primo.

TEOREMA 5 (TEOREMA CHINO DEL RESIDUO)

Si $m_1, \ldots, m_n \in \mathbb{Z}^*$ son primos relativos dos a dos, y $a_1, \ldots, a_n \in \mathbb{Z}$, entonces $\exists! \, x \in \mathbb{Z} \pmod{\prod_{i=1}^{n} m_i}$ ∋ $x \equiv a_i \pmod{m_i} \ \forall \ i \in \{1, \ldots, n\}$.

Dem Sea $M_i = \frac{\prod_{k=1}^{n} m_k}{m_i}$. Entonces $M_i x \equiv a_i \pmod{m_i}$ tiene solución, porque $(m_i, M_i) = 1$. Sea t_i la solución de $M_i x \equiv a_i \pmod{m_i}$. Sea $x = M_1 t_1 + \ldots + M_n t_n$. En general, $m_i \mid M_j$, si $i \neq j$. Entonces $x \equiv_{m_i} M_i \equiv_{m_i} a_i \ \therefore x \equiv_{m_i} a_i \ \forall \ i \ \therefore x$ es solución del sistema de congruencias. Para demostrar que es única supongamos que x, y son dos soluciones. Entonces

$x \equiv y \pmod{m_i}\ \forall\ i \Rightarrow m_i \mid (x-y)\ \forall\ i \Rightarrow m_1 \ldots m_n \mid (x-y)$ ($a \mid c, b \mid c$ y $(a,b)=1 \Rightarrow ab \mid c$).

$\therefore\ x \equiv y \pmod{\Pi m_i}$.

DEFINICIÓN 3 Una función euclidiana en un dominio entero D es una función $\nu : D^* \to Z^+ \cup \{0\}$ que cumple las siguientes condiciones:

i) $\forall\ a, b \in D^*\ \exists\ q, r \in D\ \ni\ a = bq + r$, donde $r = 0$ ó $\nu(r) < \nu(b)$.

ii) $\forall\ a, b \in D^*,\ \nu(a) \leq \nu(ab)$.

DEFINICIÓN 4 Un dominio entero D se llama anillo euclidiano, si existe una función euclidiana en D.

Obs : Para todo campo F, F[x] es un anillo euclidiano. (Su función euclidiana es la función grado).

TEOREMA 6 Sea D un anillo euclidiano, y sea I un ideal de D. Entonces existe un elemento $a_0 \in I\ \ni\ I = (a_0 x;\ x \in D)$.

Dem Si $I = \{0\}$, entonces $a_0 = 0$. Supongamos ahora que $I \neq \{0\}$.

Sea $a \neq 0 \in I$. Sea $a_0 \in I\ \ni\ \nu(a_0)$ es mínimo (Esto siempre es posible, ya que ν toma únicamente valores no negativos). Sea $a \in I$ un elemento cualquiera. Por las propiedades de función euclideana, existen $q, r \in D$ tales que $a = qa_0 + r$, donde $r = 0$ ó $\nu(r) < \nu(a_0)$. Como I es ideal, $qa_0 \in I \Rightarrow r = a - qa_0 \in I$. Si $r \neq 0$, entonces hemos encontrado un elemento de I tal que $\nu(r) < \nu(a_0)\ \forall$. $\therefore\ r = 0$ y $a = qa_0$.

$\therefore\ I = (a_0)$.

TEOREMA 7 Sea D un anillo euclidiano, y sea $M = (a_0)$ un ideal maximal de D. Entonces a_0 es un elemento irreducible de D.

Dem Supongamos que a_0 no es irreducible, e.d. $a_0 = bc$, donde $b, c \in D$ no son unidades. Demostraremos ahora que entonces M no puede ser ideal maximal.

Sea $B = (b)$; entonces ciertamente $a_0 \in B \Rightarrow M \subseteq B$. Afirmamos que $M \neq B \neq D$.

Si $B = D$, entonces $1 \in B \Rightarrow 1 = xb$ p. a. $x \in D \Rightarrow b$ es unidad ∇

Por otro lado, si $M = B$, entonces $b \in M \Rightarrow b = xa_0$ p.a. $x \in D$. Como además $a_0 = bc$, concluímos que $a_0 = xca_0 \Rightarrow xc = 1$ ∇ (porque c no es unidad).

Hemos encotrado entonces un ideal B tal que $M \subsetneq B \subsetneq D$, por lo que M no puede ser maximal.

ALGUNA BIBLIOGRAFÍA CONSULTADA

[1] **Bachman,** George. *Introduction to p - adic numbers and valuation theory.* **Academic Press,1964.**

[2] **Bartle,** Robert G., *The elements of real analysis.* **John Wiley and Sons, 1982.**

[3] **Birkhoff,** George D. *A set of postulates for plane geometry, based on scale and protractor.* **Annals of Mathematics Vol 33, 1932.**

[4] **Fraleigh,** John B. *Álgebra abstracta.* **Addison Wesley Iberoamericana, 1982.**

[5] **Halmos, Paul R.** *Espacios vectoriales de dimensión finita.* **Compañía Editorial Continental, 1971.**

[6] Herstein, I.N. *Topics in algebra.* **John Wiley & Sons, 1975.**

[7] Jacobson, Nathan. *Basic algebra.* W. H. Freeman and Company, 1989.

[8] Lluis - Rincón. *El quinto postulado de Euclides: Punto crucial en el desarrollo del pensamiento matemático.* **Conferencia.**

[9] Sánchez Sosa, M. *Sobre la categoricidad de los axiomas de Hilbert para la geometría del plano.* **Tesis profesional, UNAM, 1986.**

[10] **Shively, Levi S.** *Geometría moderna.* **Compañía Editorial Continental, 1982.**

[11] **Van der Waerden,** B.L. *Modern algebra.* **Ungar, 1953.**

[12] **Wooton, Beckenbach, Fleming.** *Geometría analítica moderna.* **Publicaciones cultural, 1985.**