UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

UN CAMPO EXTRAÑO

T E S I S

QUE PARA OBTENER EL TITULO DE

MATEMATICO

P R E S E N T A :

EUGENIA O'REILLY REGUEIRO

MEXICO, D.F. 1995

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

M. en C. Virginia Abrín Batule
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
P r e s e n t e

Comunicamos a usted que hemos revisado el trabajo de Tesis:

" Un Campo Extraño "

realizado por Eugenia O'Reilly Regueiro

con número de cuenta 9150849-2 , pasante de la carrera de matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. Emilio Lluis Riera
Propietario	Mat. César Alejandro Rincón Orta
Propietario	Dr. Hugo Alberto Rincón Mejía
Suplente	M. en C. Alejandro Bravo Mojica
Suplente	Dr. Alejandro Javier Díaz Barriga Casales

Consejo Departamental de Matemáticas

AGRADECIMIENTOS

Quiero agradecer a mi padre, que con su inmensa sabiduría y claridad me abrió los ojos hacia el maravilloso mundo de las matemáticas. A mi madre, que es una fuente inagotable de amor incondicional. A Federico, que tiene un pozo sin fondo lleno de tiempo destinado a escucharme. A María y Benjamín, que han sabido encontrar la escencia de la vida. A Alberto, que guarda en su sonrisa la llave de las puertas de la felicidad. A mis abuelitas, que no me enseñaron matemáicas, sino algo mucho más importante... A Constanza, mi hermana espiritual desde la infancia. A Nittai, mi hermana de tantas otras cosas... A César, que siempre ha puesto la amistad por encima de la relación de trabajo.

También quiero agradecer a Emilio Lluis, Hugo Rincón, Alejandro Bravo, y a Alejandro Díaz Barriga; porque sin reserva alguna me han brindado su cariño y apoyo.

MUCHAS GRACIAS.

PROLOGO (EXISTENCIAL)

La matemática clásica -la que estamos acostumbrados a estudiar-, y que utiliza la lógica "clásica" para sustentar sus argumentos, incluye muchos aspectos conceptuales que rebasan sobradamente lo que nuestra intuición nos permite interpretar con precisión o justificar de alguna manera valiéndonos de nuestro "sentido común". A principios de este siglo, Hilbert, tratando de remediar esta situación tan incómoda para el matemático riguroso, propuso que la matemática clásica se formulara como una teoría axiomática formal, y que luego se tratara de probar que tal teoría estaba libre de contradicciones. Por supuesto que la pretendida demostración de consistencia quedaría necesariamente condicionada -limitada- por la naturaleza y rigor de los métodos (metamatemáticos) usados en ella. No resulta sorpresivo, pues, que otros matemáticos (Brower, principalmente) rechazaran todas aquellas partes que se demuestran utilizando conceptos "poco claros" y sustituyéndolos por "métodos que la intuición acepta".

Los objetos matemáticos -según esta escuela "INTUICIONISTA"- deben generarse por métodos constructivos y nunca a partir de "algún conjunto cuya existencia se presupone y en el que se cumplen a priori ciertas condiciones". No se acepta la calidad existencial del conjunto $\mathbb{N}$ de los números naturales como un todo

dado de antemano.

Se pone en duda la validez de las leyes de la lógica clásica, que tradicionalmente se han tomado como ciertas universalmente -con independencia del contexto en el que se apliquen-. Explícitamente, se rechaza la "ley del tercero excluído". Para un conjunto finito S y una condición $P : S \longrightarrow \{si,no\}$, es claro que -potencialmente- puede probarse que "existe $x \in S$ tal que $P(x)$" o que "no existe $x \in S$ tal que $P(x)$", y en este caso "$P \vee \neg P$ " se cumple, pero para conjuntos infinitos, si no sucede que pueda encontrarse una $x \in S$ tal que $P(x)$, y de ahí se pretenda concluír que entonces debe ser cierto que no existe $x \in S$ tal que $P(x)$, es porque se está utilizando un argumento que no es justificable bajo ninguna razón lógica y no se vale extrapolar a partir de lo que en los conjuntos finitos si sucede.

Entre los teoremas más fuertes y también más "polémicos" de la matemática, merecen un lugar distinguido los de "existencia" -los teoremas que afirman que "algo" existe- que cuando se demuestran de una manera constructiva se aceptan, en general, sin objeción. Tal es el caso, por ejemplo, de los teoremas que afirman que: "Existe un método para resolver por radicales las ecuaciones de 2°, 3°, y 4° grado"; "Existe la bisectriz de un ángulo cualquiera en el plano"; "Si $M(x,y)dx+N(x,y)dy$ es una forma diferencial exacta, entonces existe una función potencial *i.e.* existe $\varphi(x,y)$ tal que $d\varphi = M(x,y)dx+N(x,y)dy$ "; "Para cada $z \in \mathbb{C}$ existe $w \in \mathbb{C}$ tal que $w^2 = z$ "; "Cuando $A\bar{x} = \bar{k}$ representa un sistema de m ecuaciones lineales con n incógnitas, y el rango de la matriz A

coincide con el rango de la matriz aumentada A^* (llamémosle r), entonces existe una variedad lineal "solución" de $n-r$ parámetros"; y muchos otros más cuyas demostraciones (genéticas o constructivas) pueden hacerse diseñando algoritmos que produzcan lo que los teoremas aseguran que existe.

La cosa es diferente cuando la multimencionada existencia se pretende demostrar por reducción al absurdo, es decir, cuando al suponer que tal objeto no existe se llega a una contradicción. Concluir que entonces el mencionado ente debe existir no es un argumento que todos acepten.

Para ejemplificar este tipo de teoremas mencionamos aquí la demostración -elegantísima- del teorema fundamental del álgebra que asegura que todo polinomio complejo $f(z)$ tiene al menos un cero complejo; demostración que consiste en suponer que tal no es el caso y que entonces la función $1/f(z)$ está definida (y acotada) en todo el plano y que por lo tanto tiene que ser constante. $f(z)$ constante y $f(z)$ no constante es una contradicción que prueba que la hipótesis de que $f(z)$ no se anula en $\mathbb{C}$ es absurda y que por lo tanto $f(z)$ tiene que tener al menos un cero complejo.

Existe toda una colección de "teoremas existenciales" que se derivan del teorema de compacidad de la lógica matemática que asegura que si $\{A_i\}_{i\in\mathbb{N}}$ es una familia de axiomas tal que cada subconjunto finito de ellos es consistente, entonces debe existir un modelo[1] para la familia completa de axiomas.

1:En una teoria axiomatica, un modelo es una coleccion de conjuntos que pueden interpretarse como los objetos y las relaciones de la teoria, y en los que, dada esa interpretacion, todos los axiomas resultan verdaderos. Uno de los teoremas de Godel asegura que "una teoria es consistente sii tiene un modelo".

La hipótesis de que cada colección finita de axiomas es consistente implica la imposibilidad de derivar una contradicción a partir de la familia completa, ya que tal contradicción tendría que construírse con un número finito de proposiciones, y por lo tanto con un número finito de axiomas. Esto contradiría el hecho de que tal colección, por ser finita, es necesariamente consistente. Aplicado al caso de los números reales, y a la familia $\{A_i\}_{i\in\mathbb{N}}$ A_i : "Existe un campo que contiene a $\mathbb{R}$ con un positivo menor que $1/i$ " produce el sorprendente resultado de que deben existir campos ordenados que contengan a $\mathbb{R}$, en los que todos los axiomas de la familia anterior son válidos, es decir, en los que existen "infinitésimos", y por lo tanto, sus inversos, "infinitos", (ver capítulo 13).

Por supuesto que este teorema -de existencia- está avalado por métodos constructivos que exhiben campos de "super reales" que son el habitat natural del "análisis no-estándar" creado en 1960 por Robinson y sus seguidores. En esta tesis se construye uno de tales campos que no tiene la pretensión de permitir en él el desarrollo completo del análisis, sino que se limita a mostrar cómo pueden interpretarse en un contexto sumamente familiar los infinitésimos de diferentes órdenes de magnitud, sus distinguidos inversos infinitos, infinitotes e infinitísimos, junto con una métrica "extraña" que permite la existencia de "auras" y "galaxias".

El trabajo comienza con un recordatorio de lo que es un anillo, siguiendo con las condiciones necesarias para que éste sea un dominio entero, y un campo; mencionando específicamente, lo que es

una clase positiva, y un orden definido a partir de ésta. Posteriormente, se mencionan algunos resultados relativos a elementos primos, irreducibles, ideales principales, e ideales máximos.

En los siguientes capítulos, se "construye" el campo de los números racionales a partir de el dominio entero de los números enteros; y siguiendo esta construcción como modelo, se construye, en general, el campo de cocientes de un dominio entero.

Después, se habla de los polinimios en una indeterminada x con coeficientes en un campo, con la suma y el producto que se enseña en la secundaria, y se ve que es un dominio entero. Se definen las funciones polinomiales; y para todo esto se mencionan algunos resultados acerca de las extensiones de campos, y, en particular, de las extensiones algebraicas.

Recordando la construcción del campo de cocientes de un dominio entero, se expone, en particular, el campo de cocientes del dominio entero de los polinomios en una indeterminada x con coeficientes en un campo.

La primera parte de este trabajo termina con un teorema acerca de los campos finitos.

La segunda es relativa a la lógica. Primero se define lo que es una teoría formal, y después se ve cómo la existencia de infinitésimos e infinitos se sigue del teorema de compacidad.

Finalmente, se exhibe un campo extraño.

DOMINIOS ENTEROS

Sea D un conjunto, y $\bullet : DxD \to D$; $\circ : DxD \to D$ dos operaciones binarias definidas en D.Sabemos que $(D,\bullet,\circ)$ es un anillo si $(D,\bullet)$ es un grupo abeliano, y $\circ$ se distribuye sobre $\bullet$ por ambos lados.

NOTACION: $\bullet(a,b) = a \bullet b$, $\circ(a,b) = a \circ b$.

A $\bullet$ le llamaremos suma, al neutro aditivo lo denotaremos θ, y al inverso aditivo de $a \in D$ lo denotaremos $a^{\bullet}$. A $\circ$ le llamaremos producto o multiplicación, al neutro multiplicativo (si existe) lo denotaremos e, y si existe el inverso multiplicativo de $a \in D^{*}$ lo denotaremos a°, donde $D^{*} = D - \{\theta\}$.

Si además el producto conmuta, tiene neutro, y $\forall\ a,b \in D$, $a \circ b = \theta \Rightarrow a = \theta \vee b = \theta$; entonces la terna $(D,\bullet,\circ)$ es un dominio entero.

Por ejemplo, $(\mathbb{Z},+,\cdot)$ con los neutros 0 y 1 respectivamente es un dominio entero.

DEFINICION: $\forall\ n \in \mathbb{N}$, $a \in D$ dominio entero, definimos na por recursión:

i) $0a = e$.

ii) $(n+1)a = na \circ a$.

Con objeto de extender la definición a $\mathbb{Z}$, definimos

iii) $(-n)a = (na)^{*}$.

NOTA: Si se quiere demostrar una propiedad F para todo $\mathbb{Z}$ utilizando inducción, se procede de la siguiente manera:

i) Se demuestra $F(0)$.

ii) Se demuestra $[\forall\, n \in \mathbb{N},\ F(n) \Rightarrow F(n+1)]$. } Inducción en $\mathbb{N}$.

iii) Se demuestra $[\forall\, n \in \mathbb{N},\ F(n) \Rightarrow F(-n)]$.- Generalización a $\mathbb{Z}$.

CARACTERISTICA DE UN DOMINIO ENTERO

DEFINICION: Sea D un dominio entero. Decimos que D es de "característica 0" (cero), si $\forall\, a \in D^{*}$, $m \in \mathbb{Z}$; $ma = e \Rightarrow m = 0$.

Decimos que D es de "característica finita" si no es de característica 0, es decir, $\exists\, a \in D^{*}$, $m \in \mathbb{Z}^{*}$ tales que $ma = e$.

AFIRMACION Si existen $a \in D^{*}, m \in \mathbb{Z}^{*}$ tales que $ma = e$, entonces $\forall\, b \in D^{*}$, $mb = e$.

Dem: Demostraremos primero, por inducción sobre $\mathbb{Z}$, que $\forall\, m \in \mathbb{Z}$, $\forall\, a,b \in D$; $(ma) \circ b = a \circ (mb)$.

i) $m = 0 \Rightarrow (ma)\circ b = e\circ b = e = a\circ e = a\circ(mb)$.

ii) Supongamos que $(na)\circ b = a\circ(nb)$; $n \in \mathbb{N}$.

P.d. $[(n+1)a]\circ b = a\circ[(n+1)b]$.

$[(n+1)a]\circ b = [na*a]\circ b = [(na)\circ b]*[a\circ b] = [a\circ(nb)]*[a\circ b] = a\circ[nb*b] = a\circ[(n+1)b]$.

iii) Supongamos que $(na)\circ b = a\circ(nb)$; $n \in \mathbb{N}$.

P.d. $[(-n)a]\circ b = a\circ[(-n)b]$.

$[(-n)a]\circ b = [(na)^{*}]\circ b = [(na)\circ b]^{*} = [a\circ(nb)]^{*} = a\circ[(nb)^{*}] = a\circ[(-n)b]$.

De lo anterior, tenemos que si $a \in D^{*}$, $m \in \mathbb{Z}^{*}$ son tales que $ma = e$, entonces $\forall\, b \in D^{*}$, $mb = e$, pues $e = (ma)\circ b = a\circ(mb)$. Como $a \in D^{*}$, $mb = e$.

†.

DEFINICION: Sea D un dominio entero. Si D es de característica finita, decimos que D es de "característica p" si p es el mínimo entero positivo tal que $\forall\, a \in D$, $pa = e$.

AFIRMACION: Si D es de característica p, entonces p es primo.

Dem: Supongamos que $p = q_1q_2$; $q_1, q_2 \in \mathbb{Z}^{+}$.

Entonces, $e = pa = (q_1q_2)a = q_1(q_2a)$. $q_1 \leq p$, $q_2a \in D$.

$\therefore q_1 = p \wedge q_2 = 1$ ó $q_1 = 1 \wedge q_2 = p$.

†.

Con objeto de definir un orden en un dominio entero que sea compatible con las operaciones, daremos a continuación la definición de clase positiva.

DEFINICION: $D^+ \subset D$ dominio entero es una "clase positiva" sii:
i) $a,b \in D^+ \Rightarrow a \oplus b,\ a \odot b \in D^+$. (Cerradura bajo las operaciones).
ii) $\forall\ a \in D$, sucede uno y sólo uno de los siguientes incisos:
a) $a \in D^+$ b) $a = e$ c) $a^* \in D^+$.

Por ejemplo, en $\{\mathbb{Z},+,\cdot\}$ con 0 y 1, tenemos $\mathbb{Z}^+ = \mathbb{N}^*$, es decir, $\mathbb{N} - \{0\}$ es una clase positiva en $\mathbb{Z}$.

ORDEN EN UN DOMINIO ENTERO

Sea D un dominio entero. Si existe $D^+ \subset D$ clase positiva, esta induce automáticamente un orden $< \subset D \times D$ definido de la siguiente manera:

DEFINICION: $\forall\ a,b \in D,\ a < b \Leftrightarrow b-a \in D^+$, (donde $b-a = b \oplus a^*$ y $a < b \equiv (a,b) \in <$).

OBS: $a \in D^+ \Leftrightarrow e < a$.

Un orden definido así es compatible con las operaciones, es decir:

$$\forall\, a,b,c \in D;\ a < b \Leftrightarrow \begin{cases} a*c < b*c \\ a \circ c < b \circ c, \text{ si } c \in D^+. \end{cases}$$

De aquí se deducen algunas propiedades, por ejemplo:

i) $a < b \wedge c^* \in D^+ \Rightarrow b*c < a \circ c$

ii) $\forall\, a \in D^*$, $a^2 \in D^+$, pues $a \in D^* \Rightarrow a \in D^+ \vee a^* \in D^+$; entonces:

$a \in D^+ \Rightarrow e < a \Rightarrow e \circ a = a \circ e < a \circ a = a^2$. $\therefore a^2 \in D^+$.

$a^* \in D^+ \Rightarrow a < e \Rightarrow e \circ a = a \circ e < a \circ a = a^2$. $\therefore a^2 \in D^+$.

Por consiguiente, $(e \neq 0 \wedge e^2 = e) \Rightarrow e \in D^+$.

Como $e \in D^+$, si $a \in D^+$ entonces $a*e \in D^+$; por lo tanto toda clase positiva contiene a un subconjunto con tantos elementos como $\mathbb{N}^*$, y por lo tanto debe ser infinita.

De lo anterior vemos que:

i) Ningún dominio entero finito es "ordenable".

ii) $\mathbb{C}$ no es ordenable, ya que si lo fuera; $i \neq 0 \Rightarrow i^2 \in \mathbb{C}^+$, pero $i^2 = -1$, y por lo tanto 1 y $-1 \in \mathbb{C}^+$!.

NOTA: Cuando hablamos de orden en un dominio entero, hacemos referencia a un orden compatible con las operaciones, es decir, un dominio entero se considera un dominio entero ordenado sii tiene clase positiva, y el orden es el que se deriva de ella.

CAMPOS

Sea $(D,\oplus,\odot)$ un dominio entero. Si además $(D^*,\odot)$ es un grupo abeliano, entonces $(D,\oplus,\odot)$ es un campo.

EJEMPLOS:

$\mathbb{Z}_2 = \{0,1\}$ con la suma y producto mod. 2 es un campo.

$\mathbb{R},\mathbb{C}$ con la suma y producto usuales, son campos.

$\mathbb{Z}$ no es campo con la suma y producto usuales.

Siendo los campos un caso particular de los dominios enteros, podemos extender la definición de característica de manera natural, así como las definiciones de clase positiva y orden.

OBS: Sea K un campo, $K^+ \subset K$, clase positiva. Entonces:
$a \in K^+ \Leftrightarrow a^* \in K^+$, pues $a \odot a^* = e \in K^+$.

Como ya se dijo, no en todos los campos se puede definir una clase positiva y un orden compatible, por ejemplo, en $\mathbb{Z}_2$, si hubiera $\mathbb{Z}_2^+$ clase positiva, tendríamos:

$1 \in \mathbb{Z}_2^{\bullet}$, $\therefore 1 \in \mathbb{Z}_2^{+}$, y $1 = 1^{\bullet}$. $\therefore 1^{\bullet} \in \mathbb{Z}_2^{+}$!.

IDEALES MAXIMOS, PRIMOS, Y PRINCIPALES

Para poder precisar algunas de las cosas que se usarán después, conviene definir ideales máximos, ideales primos, e ideales principales.

DEFINICION 1: Sea A un anillo conmutativo. M un ideal propio de A es "máximo" sii $\forall$ I ideal de A, $M \subseteq I \subseteq A \rightarrow M = I \vee M = A$.

DEFINICION 2: Sea A un anillo conmutativo. P un ideal propio de A es "primo" sii $\forall$ $a,b \in A$, $ab \in P \rightarrow a \in P \vee b \in P$.

DEFINICION 3: Sea A un anillo conmutativo. R un ideal de A es "principal" sii $\exists$ $r_0 \in A$ tal que $R = (r_0)$; donde (r_0) es el ideal generado por r_0, es decir, $r_0 A$.

DEFINICION 4: A es un "anillo principal" sii todo ideal de A es ideal principal.

El concepto de ideal máximo es importante per se, y en nuestro

caso, el siguiente teorema resulta relevante:

TEOREMA: Sea A un anillo conmutativo con 1. M ideal de A es máximo sii A/M es campo.

Dem: $\Rightarrow$) Sea M ideal máximo de A. Dada la correspondencia biunívoca que existe entre los ideales de A/M y los ideales de A que contienen a M, tenemos que A/M tiene sólo dos ideales, el total y el trivial. Además, como A es conmutativo y tiene 1, A/M cumple con estas condiciones. Por lo tanto, A/M es campo.

$\Leftarrow$) Sea M ideal de A tal que A/M es campo. Entonces, los únicos ideales de A/M son el trivial y el total. Por la correspondencia ya mencionada, existen solamente dos ideales de A que contienen a M. Como A y M cumplen con esta condición, son todos. Por lo tanto, M es máximo.

+.

Si A es $\mathbb{Z}$, es fácil ver que los ideales máximos se corresponden biyectivamente con los números primos, ($p\mathbb{Z}$ es máximo sii $p \in \mathcal{P}$). (Aclaramos aquí que $\mathcal{P}$ es el conjunto de los números primos).

Otra correspondencia bonita es la que hay entre los ideales máximos de $A = \{f:[a,b] \longrightarrow \mathbb{R} \ / \ f$ es continua$\}$, y los puntos de $[a,b]$. En efecto, se cumplen los siguientes teoremas:

TEOREMA: Sea $A = \{f:[a,b] \longrightarrow R \ / \ f$ es continua$\}$, y $c \in [a,b]$. Se define $M_c = \{f \in A \ / \ f(c) = 0\}$. Entonces, M_c es máximo.

Dem: Sea I ideal de A tal que $M_c \subset I$ propiamente. Sea $f \in I\text{-}M$. Entonces, $f(c) = \alpha \neq 0$. Sea $g = \alpha$. Tenemos que $(f\text{-}g)(c) = 0$. Es decir, $f\text{-}g \in M_c \subset I$, entonces $g \in I$; pero $g \in U_A$, por lo tanto, $I = A$, es decir, M_c es máximo.

+.

TEOREMA: Para cada ideal máximo M de A, existe $c \in [a,b]$ tal que $M = M_c$.

Dem: Sea M ideal máximo de A. Supongamos que no existe tal c, es decir, $\forall\, x \in [a,b]$, $\exists\, f_x \in M$ tal que $f_x(x) \neq 0$, y por lo tanto es diferente de cero en una vecindad abierta V_x de x, (por ser continua). El conjunto de estas vecindades es una cubierta abierta de $[a,b]$, que por ser cerrado y acotado es compacto. Por lo tanto, la cubierta tiene una subcubierta finita $\{V_{x_1},\ldots,V_{x_n}\}$ que corresponde a las funciones $f_{x_1},\ldots,f_{x_n}$. Los productos finitos y las sumas finitas de funciones de M están en M, por lo tanto $f = (f_{x_1})^2+\ldots+(f_{x_n})^2 \in M$, y como no se anula en ningún punto de $[a,b]$, es invertible, es decir, $f \in U_A$!

+.

COROLARIO: La relación entre los ideales máximos de A, y los puntos de $[a,b]$ es 1-1.

El Lema de Zorn se utiliza en la demostración de los dos siguientes teoremas:

TEOREMA: Si un anillo conmutativo tiene idéntico, entonces tiene ideales máximos.

Dem: Sea A un anillo conmutativo con 1. Sea $\beta = \{I \subset A \ / \ I$ es ideal propio$\}$. $\beta \neq \emptyset$, pues $\{0\} \in \beta$. Ordenamos β por contención, y tenemos un conjunto parcialmente ordenado. Sea C una cadena en β. Consideremos $\cup C$. $\cup C$ es ideal de A, pues la unión de subgrupos es subgrupo, y si tomamos $a \in A$, $c \in \cup C$, tenemos que $\exists \ I \in C$ tal que $c \in I$, entonces $ac \in I$, y por lo tanto $ac \in \cup C$. Además, $\forall \ I \in \beta$, $U_A \cap I = \emptyset$, por lo tanto $\cup C \cap U_A = \emptyset$, es decir, $\cup C$ es ideal propio de A, o sea, $\cup C \in \beta$; y claramente es cota superior de C. Satisfechas todas las condiciones del Lema de Zorn, tenemos que en A hay elementos máximos, que evidentemente resultan, ideales maximales.

+.

TEOREMA: En un anillo conmutativo con 1, todo ideal propio está contenido en un máximo.

Dem: Sean A un anillo conmutativo con 1, e I un ideal propio de A. Sea $\beta = \{M \subset A \ / \ M$ es ideal propio de A, y contiene a $I\}$. Ordenando β por contención, es un conjunto parcialmente ordenado. Sea C una cadena en β. Consideremos $\cup C$. Como se vió anteriormente,

$\cup C$ es ideal propio de A, además, $\forall M \in C$, M contiene a I, por lo tanto $\cup C$ contiene a I. Es decir, $\cup C \in \beta$, y es cota superior de C. Por el Lema de Zorn, en A hay elementos maximales, es decir, I está contenido en un ideal máximo.

†.

TEOREMA: Sea A un anillo conmutativo con 1. Entonces, P un ideal propio de A es primo sii A/P es dominio entero.

Dem: $\Rightarrow$) Sea P un ideal propio de A primo. Sean $\bar{a},\bar{b} \in A/P$ tales que $\bar{a}\cdot\bar{b} = \bar{0} = \bar{a}\bar{b}$. Entonces $ab \in P$, pero como P es primo, $a \in P$ ó $b \in P$, es decir, $\bar{a} = \bar{0}$ ó $\bar{b} = \bar{0}$; por lo tanto A/P es dominio entero.

$\Leftarrow$) Sea P un ideal propio de A tal que A/P es dominio entero. Sean $a,b \in A$ tales que $ab \in P$. Entonces, $\bar{a}\bar{b} = \bar{a}\cdot\bar{b} = \bar{0}$, pero como A/P es dominio entero, tenemos que $\bar{a} = \bar{0} \vee \bar{b} = \bar{0}$, es decir, $a \in P$ ó $b \in P$; por lo tanto, P es primo.

†.

COROLARIO: En todo anillo conmutativo con 1, si M es ideal máximo, entonces es primo.

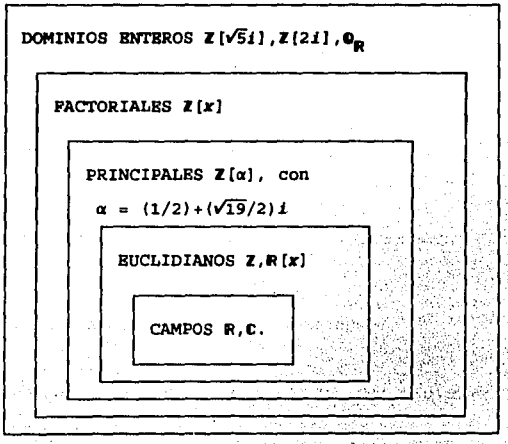
A continuación, daremos un ejemplo de un ideal máximo que no es primo, (aquí es relevante la existencia del 1); y un ideal primo que no es máximo.

EJEMPLO 1: Sea $A = \mathbb{Z}_p$, $p \in \mathcal{P}$, y definimos el producto en A como sigue: $\forall\ a,b \in A$, $ab = 0$. Evidentemente, todo subgrupo de $\mathbb{Z}_p$ es ideal de $\mathbb{Z}_p$, pero los únicos subgrupos son $\{0\}$ y $\mathbb{Z}_p$; por lo tanto $\{0\}$ es máximo, y $1 \cdot 1 = 0 \in \{0\}$, pero $1 \notin \{0\}$, por lo tanto $\{0\}$ no es primo.

+.

EJEMPLO 2: Sea $A = \mathbb{Z}[x]$. $P = (x) = \{a_1x+a_2x^2+\ldots+a_nx^n \ /\ a_i \in \mathbb{Z}\}$ es primo. $N = \{a_0+a_1x+\ldots+a_nx^n \ /\ a_i \in \mathbb{Z},\ a_1 \equiv 0\ (2)\}$ es ideal de A. Además, $P \subset N \subset A$, y ambas contenciones son propias; por lo tanto P no es máximo.

Terminamos aquí con una visión panorámica:



ELEMENTOS IRREDUCIBLES Y ELEMENTOS PRIMOS

Sea A un anillo conmutativo con 1; y U sus unidades. $p \in A^{\bullet}-U_A$ es "irreducible" sii:

DEFINICION: $\forall\, m,n \in A,\ p = mn \rightarrow (m \in U_A) \vee (n \in U_A)$.

En otras palabras, p es un elemento irreducible si no siendo cero ni unidad, sólo tiene factorizaciones triviales. Se puede demostrar que en $\mathbb{Z}$, la definición anterior es equivalente a cualquiera de las tres siguientes:

DEFINICION: $\forall\, a,b \in A,\ p|ab \rightarrow p|a \vee p|b$.

DEFINICION: $\forall\, a \in A,\ p|a \vee (p,a) = 1$.

DEFINICION: $\forall\, a \in A,\ 1 \leq a < p \rightarrow (p,a) = 1$.

Se da sin demostración el siguiente:

TEOREMA: En $\mathbb{Z}$, las cuatro definiciones anteriores son equivalentes.

TEOREMA: $p \in \mathcal{P}^+ \leftrightarrow p \geq 2 \wedge p|(p-1)!+1$. Es decir, un entero no cero ni unidad es primo positivo sii $(p-1)! \equiv -1\ (p)$, que en un sentido ($\rightarrow$) es el Lema de Wilson.

Dem: $\rightarrow$) Sea $p \in \mathcal{P}^+$. Consideremos $\mathbb{Z}_p^* = \{1,\ldots,p-1\}$. Supongamos que $i \in \mathbb{Z}_p^*$ es tal que $i^2 \equiv 1\ (p)$. Es decir, $p|i^2-1 = (i+1)(i-1)$, esto sii $p|i+1 \vee p|i-1$, sii $i \equiv p-1 \vee i \equiv 1$. Entonces $(p-1)! \equiv (p-1)\ (p)$, y por lo tanto $(p-1)! \equiv -1\ (p)$.

$\leftarrow$) Supongamos que $p \notin \mathcal{P}$, entonces existen $m,n \in \mathbb{Z}$ tales que $p = mn$, con $2 \leq m < p$, $2 \leq n < p$. Si $p|(p-1)!+1$, tenemos que $m|(p-1)!+1$, pero como $m < p$, $m|(p-1)!$, por lo tanto $m|1$! $\dagger$.

Aun cuando en $\mathbb{Z}$ coincide el concepto de "primo" con el de "irreducible", (que se usan indistintamente), en la teoría general de anillos no es así. Conviene definir como "número" primo a un elemento p en A tal que (p) es un ideal primo.

Se mencionan, a continuación, algunos teoremas relativos a "primos" e "irreducibles".

TEOREMA: Si A es un dominio entero, entonces, $\forall\ p \in A$, p primo $\rightarrow p$ irreducible.

Dem: Sea A un dominio entero. Sea $p \in A$ tal que (p) es primo.

Supongamos que $p = mn$. Entonces $mn \in (p)$, pero como (p) es primo, tenemos que $m \in (p)$, $\vee$ $n \in (p)$. $m \in (p) \Rightarrow p|m \Rightarrow n \in \mathcal{U}_A$. Del mismo modo, $n \in (p) \Rightarrow p|n \Rightarrow m \in \mathcal{U}_A$.

+.

Hacemos ver que la contención es propia con el siguiente ejemplo:

Sea $A = \mathbb{Z}[\sqrt{5}i] = \{a+b\sqrt{5}i \ / \ a,b \in \mathbb{Z}\}$ que es un subanillo de $\mathbb{C}$, y por lo tanto es un dominio entero, $(1 \in A)$. Se define en A una "norma" de la manera siguiente: $N(z) = a^2+5b^2$ si $z = a+b\sqrt{5}i$. Es decir, $N(z) = z\bar{z}$, y por lo tanto es "multiplicativa":

$N(zv) = zv\bar{z}\bar{v} = zv\bar{z}\cdot\bar{v} = z\bar{z}v\bar{v} = N(z)N(v)$. Esto permite identificar a las unidades de A como los elementos de tamaño 1, o sea $\mathcal{U}_A = \{1,-1\}$.

Sea $z = 2+\sqrt{5}i$, entonces $N(z) = 9$. z es irreducible, si $z = xy$, $N(x)N(y) = 9$; por lo tanto $N(x) = 1,3,$ó 9, pero si $x = c+d\sqrt{5}i$, $N(x) = 3 \Rightarrow c^2+5d^2 = 3$; que no tiene solución en $\mathbb{Z}$. Por lo tanto, $N(x) = 1 \wedge x \in \mathcal{U}_A$, ó $N(x) = 9 \wedge y \in \mathcal{U}_A$. Sin embargo, z no es primo, ya que $9 = 3\cdot3 = z\bar{z} \in (z)$, pero $3 \notin (z)$.

+.

TEOREMA: Si A es dominio principal, entonces $\forall$ $p \in A$, p irreducible $\Rightarrow$ p primo, (y por lo tanto "primo" o "irreducible" es equivalente).

Dem: Sea A dominio principal, $p \in A$ irreducible. Supongamos que $ab \in (p)$. Entonces $p|ab$. Como A es principal, $p|a \vee p|b$; entonces $a \in (p) \vee b \in (p)$. +.

CONSTRUCCION DE Q

Consideremos la ecuación $a = bx$; $a,b \in \mathbb{Z}$. Esta ecuación tiene solución en $\mathbb{Z}$ sii $b|a$. Queremos construir el conjunto de soluciones a estas ecuaciones aún cuando $b \nmid a$. A este conjunto, además, le queremos dar estructura de anillo. Esto nos lleva inmediatamente a un problema: ¿ Qué pasa si $b = 0$?

Si $b = 0$ y $a = 0$, entonces x puede ser cualquier elemento del conjunto, y no llegamos a ningún lado. Si $b = 0$ y $a \neq 0$, entonces rompemos la estructura de anillo, pues en un anillo no puede suceder que $0x \neq 0$.

Por lo anterior, para conservar la estructura, y la unicidad de las soluciones, consideraremos sólo aquellas ecuaciones en las que $b \neq 0$.

Como la solución de la ecuación $a = bx$ está unicamente en función de a y b, la representaremos con la pareja ordenada (a,b).

¿ Cuándo son iguales dos elementos del conjunto ? Es decir, ¿ Cuándo dos ecuaciones tienen la misma solución ?

Supongamos que $a = bx_0$, $c = dx_0$; $a,b,c,d \in \mathbb{Z}$; $b,d \neq 0$. Entonces $ad = bdx_0$, $bc = bdx_0$; $\therefore ad = bc$.

Es decir, para que un elemento sea solución de dos ecuaciones (a,b), (c,d); es necesario que $ad = bc$. Esta condición, ¿ Será suficiente ?

Supongamos que $a = bx$, $c = dy$, y $ad = bc$; $b,d \neq 0$. Entonces, $ad = bdx$, $bc = bdy$. Como $ad = bc$, $bdx = bdy$. $b,d \neq 0 \Rightarrow bd \neq 0 \Rightarrow x = y$.

$\therefore$ Las ecuaciones $a = bx$, $c = dy$ tienen la misma solución sii $ad = bc$.

Con este resultado, podemos entonces definir una relación de equivalencia en el conjunto:

DEFINICION: Sean $a,b,c,d \in \mathbb{Z}$, $b,d \neq 0$. Decimos que (a,b) es equivalente a (c,d) sii $ad = bc$. O sea, $(a,b) \sim (c,d) \Leftrightarrow ad = bc$.

Es decir, si dos ecuaciones tienen la misma solución, entonces las representaciones de esta, en función de las diferentes ecuaciones, las consideramos equivalentes; lo que coincide con nuestro propósito ya que, en ese caso, ambas ecuaciones son representaciones del mismo elemento que queremos construir; a saber, su solución.

De esta manera, consideraremos a las soluciones de las ecuaciones como las clases de equivalencia; (a la clase de (a,b) la denotaremos $(\overline{a,b})$).

Tenemos ahora un conjunto, conocemos sus elementos, y queremos que sea un anillo. ¿ Cómo sumamos ? ¿ Cómo multiplicamos ?

Supongamos que $x = (\overline{a,b})$, $y = (\overline{c,d})$. Queremos encontrar un elemento $x+y$ que sea solución de alguna ecuación. Entonces:

$x = (\overline{a,b}) \rightarrow a = bx \rightarrow ad = bdx$.

$y = (\overline{c,d}) \rightarrow c = dy \rightarrow bc = bdy$.

$\therefore ad+bc = bd(x+y) \therefore x+y = (\overline{ad+bc,bd})$. Esto está en el conjunto, pues $a,b,c,d \in \mathbb{Z}$; $b,d \neq 0 \rightarrow bd \neq 0$. Es decir, $x+y$ es solución de la ecuación $ad+bc = bdz$.

¿ Y la multiplicación ? Queremos encontrar una ecuación cuya solución sea xy.

$a = bx$, $c = dy$; $\therefore ac = (bd)(xy) \therefore xy = (ac,bd)$, que también está en nuestro conjunto. O sea, xy es solución de $ac = bdz$.

Ya tenemos nuestro conjunto, y las dos operaciones binarias que en vista de lo anterior quedan definidas como sigue:

$(\overline{a,b}) + (\overline{c,d}) = (\overline{ad+bc,bd})$.

$(\overline{a,b})(\overline{c,d}) = (\overline{ac,bd})$.

A este conjunto, le llamaremos $\mathbb{Q}$.

Dadas las definiciones anteriores, se puede demostrar que $\{\mathbb{Q},+,\cdot\}$ es campo, con $\theta = \overline{(0,b)}$, $e = \overline{(1,1)}$; $b \in \mathbb{Z}^*$.

OBS: Podemos pedir $b > 0$, pues $\overline{(a,b)} = \overline{(-a,-b)}$; y entonces no perdemos nada considerando $\mathbb{Q} = \{[a,b] \ / \ a \in \mathbb{Z},\ b \in \mathbb{Z}^+\}$; lo que haremos en lo sucesivo, y en donde $[a,b] = \overline{(a,b)}$ si $b > 0$.

Recordemos que una inmersión de un conjunto A en un conjunto B es una función inyectiva $i : A \longrightarrow B$, (es como ver a A dentro de B) tal que preserva la estructura de A en su imagen.

Es fácil ver que $i : \mathbb{Z} \longrightarrow \mathbb{Q}$ definida por $i(a) = [a,1]\ \forall\ a \in \mathbb{Z}$ es una inmersión.

OBS: En vista de que $\mathbb{Z}$ es de característica cero, $\mathbb{Q}$ es de característica cero.

En $\mathbb{Q}$ podemos definir una clase positiva $\mathbb{Q}^+$ a partir de $\mathbb{Z}^+$, y así extender el orden de $\mathbb{Z}$ a $\mathbb{Q}$.

DEFINICION: $\mathbb{Q}^+ = \{[a,b] \in \mathbb{Q} \ / \ a \in \mathbb{Z}^+\}$.

TEOREMA: $\mathbb{Q}^+$ es clase positiva.

Dem: Sean $[a,b], [c,d] \in \mathbb{Q}^+$. Entonces $a,b,c,d \in \mathbb{Z}^+$. Por lo tanto $ad+bc, ac, bd \in \mathbb{Z}^+$. $\therefore$ $[ad+bc, bd]$, $[ac, bd] \in \mathbb{Q}^+$.

Sea $[a,b] \in \mathbb{Q}$. Si $a \in \mathbb{Z}^+$ entonces $[a,b] \in \mathbb{Q}^+$. Si $a = 0$ entonces $[a,b] = 0$. Si $-a \in \mathbb{Z}^+$ entonces $[-a,b] = -[a,b] \in \mathbb{Q}^+$. $\dagger$.

DEFINICION: Sean $[a,b]$, $[c,d] \in \mathbb{Q}$. Entonces:

$[a,b] < [c,d] \leftrightarrow [c,d] - [a,b] \in \mathbb{Q}^+$. *i.e.* $ad < bc$.

Como consecuencia de que $\mathbb{Q}^+$ sea una clase positiva, y de la definición anterior, tenemos que el orden está bien definido, es compatible con las operaciones de $\mathbb{Q}$, y extiende al de $\mathbb{Z}$.

CAMPO DE COCIENTES DE UN DOMINIO ENTERO

De la misma manera en la que se construyó $\mathbb{Q}$ a partir de $\mathbb{Z}$, se construye el campo de cocientes de un dominio entero arbitrario.

Sea D un dominio entero. Decimos que K es su campo de cocientes si $K = \{(\overline{a,b}) \ / \ a,b \in D, \ b \neq 0\}$, con la siguiente relación de equivalencia: $(a,b) \sim (c,d) \leftrightarrow ad = bc$.

La suma y el producto se dan, de manera natural, (ver construcción de $\mathbb{Q}$); como sigue:

$(\overline{a,b}) \bullet (\overline{c,d}) = (\overline{ad+bc,bd})$.

$(\overline{a,b}) \circ (\overline{c,d}) = (\overline{ac,bd})$.

Los neutros, los inversos:

$o = (\overline{0,1})$, $e = (\overline{1,1})$, $(\overline{a,b})^{\bullet} = (\overline{-a,b})$, $(\overline{a,b})^{\circ} = (\overline{b,a})$, $(a \neq 0)$.

Tenemos, por supuesto, la inmersión:

$$\iota : D \longrightarrow K$$
$$a \mapsto (\overline{a,1})$$

Si D es ordenado, su orden induce el correspondiente en K.

POLINOMIOS

Sea K un campo. Como primer intento de definición de $K[x]$, (los polinomios en una indeterminada x con coeficientes en K), tenemos la siguiente, (que es la que nos dan en secundaria):

$$K[x] = \{a_0+a_1x+\ldots+a_nx^n \ / \ n \in \mathbb{N},\ a_i \in K\ \forall\ i = 0,\ldots,n\}.$$

Ahora bien, ¿ Qué es x ? Es algo cuya naturaleza no se ha precisado hasta aquí, pero lo elevamos a una potencia natural. ¿ Cómo ? Luego resulta que las potencias de x se pueden multiplicar por elementos de K. ¿ Qué ? Y no sólo eso, sino que estos productos, que quién sabe dónde andan, se suman; pero, ¿ Cómo es esta suma ?

Digamos que esta definición no nos deja nada claro, así que definámoslo de otra manera:

DEFINICION: $K[x] = \{s : \mathbb{N} \longrightarrow K \ / \ s$ es casi nula$\}$, aclarando que las sucesiones casi nulas son aquellas en las que sólo un número finito de términos son distintos de cero.

OBS: Si $s : \mathbb{N} \longrightarrow K$ es casi nula, entonces $\exists\, n_0 \in \mathbb{N}$ tal que $\forall\, n > n_0,\ s(n) = 0$.

Habiendo definido así $K[x]$, tenemos que $\forall\ f,g \in K[x]$, $f = g \leftrightarrow f(n) = g(n)\ \forall\ n \in \mathbb{N}$.

La suma de polinomios la definiremos tal como la suma de funciones, es decir; $(f \circ g)(n) = f(n)+g(n)$, lo que resulta en una suma término a término.

$\oplus : K[x] \longrightarrow K[x]$ es la suma definida así:

Si $f = \{a_i\}_{i\in\mathbb{N}}$, $g = \{b_i\}_{i\in\mathbb{N}} \in K[x]$, entonces $\oplus(f,g) = f \oplus g = \{a_i+b_i\}_{i\in\mathbb{N}}$

Hasta aquí, tenemos un conjunto en el que los elementos son iguales sii coinciden término a término, y una operación binaria definida en este conjunto. Se puede ver que $(K[x],\oplus)$ es un grupo abeliano, con $\theta = (0,0,\ldots)$, y si $f = \{a_i\}_{i\in\mathbb{N}}$, $f^* = -f = \{-a_i\}_{i\in\mathbb{N}}$.

El producto de polinomios no es el producto de imágenes, sino que se define de manera conveniente para obtener un homomorfismo de anillos entre $K[x]$ y las funciones polinomiales sobre K. (Ver mas adelante). La definición, que es la conocemos desde secundaria es:

DEFINICION: Sean $f = (a_i)_{i\in\mathbb{N}}$, $g = (b_i)_{i\in\mathbb{N}} \in K[x]$. Entonces:

$f\circ g = (c_i)_{i\in\mathbb{N}}$, donde $c_i = \sum_{j=0}^{i} a_j b_{i-j}$.

Es decir, $c_i = a_0b_i+a_1b_{i-1}+\ldots+a_{i-1}b_1+a_ib_0$.

Entonces, tenemos que $(K[x],\bullet,\circ)$ es un anillo conmutativo con uno, en el que $e = (1,0,\ldots)$.

DEFINICION: El grado de un polinomio es una función $d : K[x]^* \longrightarrow \mathbb{N}$ definida como sigue:

$\forall\, f = (a_i)_{i\in\mathbb{N}} \in K[x]^*$, $d(f) = n \leftrightarrow a_n \neq 0$ y $a_m = 0\ \forall\ m > n$.

(Pedimos $f \neq e$, ya que la definición no tiene sentido para $f = (0,0,\ldots)$, y declaramos al polinomio cero "degradado").

A partir de la definición, podemos ver que el grado de la suma y producto de polinomios satisface:

i) $\forall\ f,g \in K[x]^*$, $f\circ g = e$ ó $d(f\circ g) \leq$ máx $\{d(f),d(g)\}$, (ya que en la suma pudieran cancelarse algunos o todos los términos). Si $d(f) \neq d(g)$, entonces $d(f\circ g) =$ máx $\{d(f),d(g)\}$.

ii) $\forall\ f,g \in K[x]^*$, $d(f\circ g) = d(f)+d(g)$. Es decir, el producto de polinomios distintos de cero tiene grado, por lo tanto es distinto de cero.

COROLARIO: $\{K[x],\oplus,\circ\}$ es un dominio entero.

Podemos ver al campo K dentro de $K[x]$ bajo la siguiente inmersión:

$$\begin{aligned} i : K &\longrightarrow K[x] \\ a &\mapsto (a,0,0,\ldots) \end{aligned}$$

Esto nos permite escribir simplemente a en vez de $(a,0,0,\ldots)$; lo que haremos cuando sea conveniente.

Ahora, definamos x :

$x = (0,1,0,0,\ldots)$.

Entonces, con el producto definido, tenemos:

$x^2 = x \circ x = (0,1,0,0,\ldots)\circ(0,1,0,0,\ldots) = (0,0,1,0,0,\ldots)$.

$x^3 = x^2 \circ x = (0,0,1,0,0,\ldots) \circ (0,1,0,0,\ldots) = (0,0,0,1,0,\ldots)$.

En general:

$x^n = (0,0,\ldots,1,0,0,\ldots)$.El 1 está en el n-ésimo lugar, contando los lugares desde 0.

Ahora sí, podemos ver:

$a^n x^n = (a^n,0,\ldots)\circ(0,\ldots,1,0,\ldots) = (0,\ldots,a^n,0,\ldots)$.

Entonces:

$a_0 = (a_0, 0,0,\ldots)$

$a_1 x = (0,a_1,0,0,\ldots)$

$a_n x^n = (0,0,\ldots,a_n,0,0,\ldots)$.

O sea que $a_0+a_1x+\ldots+a_nx^n = (a_0,a_1,\ldots,a_n,0,0,\ldots)$, lo que nos permite recuperar las extrañas sumas formales con las que empezamos, pero sin obscuridades ni indeterminaciones. Las "sumas" son sumas en $K[x]$, y los "productos" son productos en $K[x]$.

EXTENSIONES DE CAMPOS

A continuación, veremos algunos resultados útiles para el estudio de los polinomios y sus raíces.

DEFINICION: Sea F un campo. Se dice que un campo K es una extensión de F si F es subcampo de K.

OBS: Si K es una extensión de F, entonces bajo las operaciones usuales de campo en K; K es un espacio vectorial sobre F.

Esta observación, da lugar a la siguiente

DEFINICION: El grado de la extensión de K sobre F, que denotamos $[K:F]$, es la dimensión de K como espacio vectorial sobre F.

Por ejemplo, $\mathbb{C}$ es una extensión de $\mathbb{R}$ de grado 2.

TEOREMA: Si L es una extensión finita de K, y K es una extensión finita de F, entonces L es una extensión finita de F; y además, $[L:F] = [L:K][K:F]$.

Aunque no daremos la demostración completa, la idea es la siguiente:

Si $[L:K] = m$, y $[K:F] = n$; tomamos $\{v_1,\ldots,v_m\} \subset L$ base de L sobre K, y $\{w_1,\ldots,w_n\} \subset K$ base de K sobre F. Se demuestra que $\{v_i w_j\}_{i,j=1}^{m,n} \subset L$ es una base de L sobre F. De este modo, tenemos que $[L:F] = mn$, es decir, la extensión es finita, y es $[L:K][K:F]$.

COROLARIO: Si L es una extensión finita de F, y $K \subset L$ es un subcampo tal que $F \subset K$; entonces $[K:F] \mid [L:F]$.

Esto nos lleva a la siguiente

OBS: Si $[L:F]$ es primo, entonces no existen subcampos propios de L que contengan propiamente a F.

Por ejemplo, $\mathbb{R}$ no es subcampo propio de algún subcampo propio de $\mathbb{C}$.

FUNCIONES POLINOMIALES

Sean $F \subseteq K$ campos. Consideremos el mapeo:

$\eta : F[x] \longrightarrow \{f : K \longrightarrow K \ / \ f$ es función$\}$, donde si $f(x) = (a_0, a_1, \ldots, a_n, 0, \ldots) \in F[x]$, entonces $\eta(f(x)) = f : K \longrightarrow K$ es la función definida de la manera siguiente:

$\forall\ \alpha \in K,\ f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$.

$f(\alpha)$ se llama la imagen de α bajo f, o el valor de f cuando $x = \alpha$.

OBS: Dado que las definiciones de suma y producto en $F[x]$ se hicieron convenientemente, η resulta un homomorfismo de anillos.

Si K es infinito, η es inyectivo, como se verá después. (En particular, $car(K) = 0 \Rightarrow K$ infinito).

TEOREMA (del residuo): Si $f(x) \in F[x]$, y K es una extensión de F, entonces $\forall\ b \in K$, $f(x) = (x-b)q(x) + f(b)$, donde $q(x) \in K[x]$, y si $q(x) \neq 0$, entonces $d(q(x)) = d(f(x))-1$.

Dem: Dado que $F \leq K$, podemos considerar a $f(x)$ en $K[x]$. Por el algoritmo de la división, tenemos que existen únicos $q(x), r(x) \in K[x]$ tales que $f(x) = (x-b)q(x)+r(x)$, donde $r(x) = 0$, ó $d(r(x)) < d(x-b) = 1$. $\therefore r = 0$, ó $d(r) = 0$. $\therefore r \in K$.

Utilizando ahora el homomorfismo η; si $f(x) = (x-b)q(x)+r$, entonces $f(b) = (b-b)q(b)+r = r$. $\therefore r = f(b)$.

Nótese que si $r \neq 0$, entonces $d(r) = 0$, y por lo tanto si $d(f(x)) \geq 1$, $d(f(x)) = d[(x-b)q(x)] = d(x-b)+d(q(x)) = 1+d(q(x))$. $\therefore d(q(x)) = d(f(x))-1$.

+.

COROLARIO (factor): Sea $a \in K$, y $f(x) \in K[x]$. Entonces a es raíz de $f(x) \leftrightarrow (x-a) \mid f(x)$.

Dem: $\rightarrow$) $f(x) = (x-a)q(x)+f(a)$, pero a es raíz de $f(x)$, entonces $f(a) = 0$. Por lo tanto $(x-a) \mid f(x)$, pues $f(x) = (x-a)q(x)$.
$\leftarrow$) Si $(x-a) \mid f(x)$, entonces $f(x) = (x-a)q(x) = (x-a)q(x)+0$ y por la unicidad del residuo, $f(a) = 0$. $\therefore a$ es raíz de $f(x)$.

+.

DEFINICION: Sea $a \in K$, $f(x) \in F[x]$. Se dice que a es raíz de $f(x)$ de multiplicidad m si $(x-a)^m \mid f(x)$, y $(x-a)^{m+1} \nmid f(x)$.

Se puede demostrar ahora el siguiente

TEOREMA: Un polinomio $f(x) \in F[x]$ de grado n, tiene a lo más n raíces en cualquier extensión de F.

NOTA: Si a es raíz de multiplicidad m, se cuenta como m raíces distintas.

Podemos justificar ahora, la observación anterior relacionada con η:

Sea F infinito. Entonces $\eta : F[x] \longrightarrow \mathcal{F}_{P_F}$ es isomorfismo:

($\mathcal{F}_{P_F}$ = Funciones polinomiales sobre F).

Sea $f(x) \in \ker(\eta)$. Entonces, $\forall\ \alpha \in K$, $f(\alpha) = 0$, de aquí que en K, f tiene un número infinito de raíces, por lo tanto $f(x) = 0$.

$\therefore\ \eta$ es monomorfismo.

Por definición de $\mathcal{F}_{P_F}$, η es epimorfismo.

$\dagger$.

Obsérvese que la condición " F campo " es indispensable en la demostración del teorema que se refiere al número de raíces de un polinomio, (misma que aquí no se hizo). En particular, se requiere de la conmutatividad del producto. Esto se puede ver considerando los cuaternios reales, cuyas operaciones tienen todas las propiedades de las operaciones de campo, excepto la conmutatividad del producto; y en los que el polinomio de grado 2 x^2+1 tiene un número infinito de raíces, ya que la falta de conmutatividad del producto ocasiona que las factorizaciones de los polinomios con coeficientes cuaternios no sean únicas. En efecto, $x^2+1 = (x+i)(x-i) = \ldots = (x+z)(x-z)$, $z = bi+cj+dk$ tales

que $b^2+c^2+d^2 = 1$. Nótese que en particular x^2+1 coincide con $(x+i)(x-i)$ como producto de polinomios, pero no como producto de funciones. En efecto, x^2+1 valuado en k es $k^2+1 = 0$, pero $(k+i)(k-i) = -2j \neq 0$.

Cabe aclarar, además, que si se consideran diferentes extensiones de F, puede suceder que en ellas existan polinomios con "juegos de raíces" diferentes; aunque cada juego con el número adecuado de raíces, a saber, $\leq d(f)$.

A continuación, mostramos un ejemplo de un polinomio de grado 2 en $\mathbb{Z}_2[x]$, con pares de raíces diferentes en cada una de dos extensiones diferentes:

Sean $K_0 = \mathbb{Z}_2$, $f(x) = x^2+x+1 \in K_0[x] = \mathbb{Z}_2[x]$. $f(x)$ no tiene raíces en $\mathbb{Z}_2$. Sea α una raíz de $f(x)$.

Sea $K_1 = K_0(\alpha) = \{a+b\alpha \ / \ a,b \in K_0, \ \alpha^2 = 1+\alpha\}$. $1+\alpha$ también es raíz de $f(x)$:

$(1+\alpha)^2+(1+\alpha)+1 = 1+\alpha^2+1+\alpha+1 = \alpha^2+\alpha+1 = 0$ en $\mathbb{Z}_2$. $1+\alpha \in K_1$. Por lo tanto, K_1 es una extensión de K_0 en la que $f(x)$ tiene las dos raíces $\{\alpha, 1+\alpha\}$.

Ahora consideremos $p(x) = x^4+x+1$ en $\mathbb{Z}_2[x]$. $p(x)$ no tiene raíces en $\mathbb{Z}_2$. Sea β una raíz de $p(x)$.

Sea $K_2 = K_0(\beta) = \{a+b\beta+c\beta^2+d\beta^3 \ / \ a,b,c,d \in \mathbb{Z}_2, \ \beta^4 = \beta+1\}$. Si consideramos el grupo multiplicativo K_2^*, todos los elementos son de orden 1,3,5, ó 15, (ya que K_2 tiene 16 elementos). Dado que

$\beta^5 = \beta+\beta^2 \neq 1$, $(\beta) > 5$, por lo tanto $o(\beta) = 15$. Es decir, β^5 y β^{10} (que son diferentes de 1) satisfacen el polinomio x^3+1, pero $x^3+1 = (x+1)(x^2+x+1)$; por lo tanto $\beta^5 = \beta+\beta^2$ y $\beta^{10} = 1+\beta+\beta^2$ son raíces de x^2+x+1. Es decir, K_2 es una extensión de K_0 en la que $f(x)$ tiene las dos raíces $\{\beta^2+\beta, \beta^2+\beta+1\}$.

Por supuesto, $K_1 \neq K_2$, ya que $[K_1:K_0] = 2$, y $[K_2:K_0] = 4$.

Se mencionó, que un polinomio de grado n no puede tener más de n raíces en cualquier extensión del campo de sus coeficientes; ahora nos preguntamos: ¿ Existe una extensión en la que tenga al menos una raíz ? ¿ Y todas ?

TEOREMA: Sea $f(x) \in F[x]$ irreducible, de grado $n \geq 1$. Entonces, existe una extensión E de F tal que $[E:F] = n$, y en E $f(x)$ tiene al menos una raíz.

Aunque no se dará la demostración completa, el campo que se se considera es $E = \dfrac{F[x]}{(f(x))}$. Dado que $f(x)$ es irreducible en $F[x]$, $(f(x))$ es un ideal máximo, por lo que $\dfrac{F[x]}{(f(x))}$ es campo, (ver cap. 3), isomorfo a la extensión requerida, en la que la imagen de x bajo el epimorfismo canónico $\phi : F[x] \longrightarrow \dfrac{F[x]}{(f(x))}$ es raíz de $f(x)$.

COROLARIO: Si $f(x) \in F[x]$, entonces existe una extensión finita E de F en la que $f(x)$ tiene una raíz, es más, $[E:F] \leq d(f(x))$.

Dem: Sea $p(x)$ un factor irreducible de $f(x)$. Entonces, $d(p(x)) \leq d(f(x))$, y existe E extensión de F en la que $p(x)$ tiene una raíz, y $[E:F] = d(p(x))$;pero una raíz de $p(x)$ es raíz de $f(x)$; por lo tanto $f(x)$ tiene una raíz en E, y $[E:F] = d(p(x) \leq d(f(x))$. +.

TEOREMA: Sea $f(x) \in F[x]$ de grado $n \geq 1$. Entonces existe una extensión E de F en la que $f(x)$ tiene n raíces, (un juego completo), y $[E:F] \leq n!$.

Se omite la demostración, que puede hacerse por inducción sobre n.

DEFINICION: Sea $f(x) \in F[x]$. Una extensión E de F es un "campo de descomposición de $f(x)$ sobre F" si en $E[x]$ $f(x)$ se puede factorizar como producto de factores lineales; y no en cualquier subcampo propio de E, que contenga a F.

Se puede probar, finalmente, que todos los campos de descomposición de un mismo polinomio sobre un campo fijo son isomorfos; por eso podemos hablar "del" campo de descomposición de $f(x)$ sobre F.

EXTENSIONES ALGEBRAICAS

DEFINICION: Un elemento $a \in K$ es algebraico sobre F, si existen en F $\alpha_0,\ldots,\alpha_n$ no todos cero, tales que $\alpha_0+\alpha_1 a+\ldots+\alpha_n a^n = 0$; es decir, $a \in K$ es algebraico sobre F si es raíz de algún polinomio distinto de cero en $F[x]$.

Dado un campo K, un subcampo F, y un elemento $a \in K$, definiremos $F(a)$ como el menor campo, (en el sentido de la contención), tal que $F \subseteq F(a)$, y $a \in F(a)$. Se puede ver que $F(a) = \cap C$, donde $C = \{L \subseteq K \ / \ L$ es subcampo de K, $F \subseteq L$, $a \in L\}$.

TEOREMA: $a \in K$ es algebraico sobre $F \Leftrightarrow [F(a):F]$ es finito.

Una parte de la demotración es muy sencilla:

$\Rightarrow$) $[F(a):F]$ es finito. Supongamos que $[F(a):F] = m$, entonces consideremos $1,a,\ldots,a^m \in F(a)$, son $m+1$ elementos, por lo tanto son linealmente dependientes; es decir, existen $\alpha_0,\ldots,\alpha_m \in F$, no todos cero, tales que $\alpha_0+\alpha_1 a+\ldots+\alpha_m a^m = 0$. Entonces, a es raíz del polinomio $\alpha_0+\alpha_1 x+\ldots+\alpha_m x^m$ en $F[x]$. $\therefore a$ es algebraico sobre F.

La otra parte de la demostración es más tediosa, y se omite.

DEFINICION: $a \in K$ es algebraico sobre F de grado n, si satisface un polinomio de grado n en $F[x]$, y ningún polinomio en $F[x]$ de grado menor que n.

Por ejemplo, $i \in \mathbb{C}$ es algebraico de grado 2 sobre $\mathbb{R}$, pues satisface x^2+1 en $\mathbb{R}[x]$, y ningún polinomio en $\mathbb{R}[x]$ de la forma $ax+b$; $a,b \in \mathbb{R}$, $a \neq 0$ ó $b \neq 0$.

Enunciamos ahora tres teoremas que se dejan aquí sin demostración:

TEOREMA: Si $a \in K$ es algebraico sobre F de grado n, entonces $[F(a):F] = n$.

TEOREMA: Si $a,b \in K$ son algebraicos sobre F de grados m y n respectivamente, entonces $a \pm b$, ab, y ab^{-1} $(b \neq 0)$; son algebraicos sobre F de grado a lo más mn.

COROLARIO: Los elementos de K algebraicos sobre F forman un subcampo de K.

DEFINICION: K es una extensión algebraica sobre F si todo elemento de K es algebraico sobre F.

Por ejemplo, $\mathbb{C}$ es algebraico sobre $\mathbb{R}$, y en general toda extensión finita K de F, es algebraica sobre F (la demostración es idéntica

a la primera parte de la demostración del primer teorema de esta sección). La recíproca no es cierta, existen extensiones infinitas de $\mathbb{Q}$ que son algebraicas sobre $\mathbb{Q}$.

TEOREMA: Si L es extensión algebraica sobre K, y K es extensión algebraica sobre F, entonces L es extensión algebraica sobre F.

$K(x)$, EL CAMPO DE COCIENTES DE $K[x]$

Como se vió anteriormente, si K es campo, entonces $K[x]$ es un dominio entero; de tal manera que podemos construir su campo de cocientes, $K(x)$.

De esta construcción resulta:

$K(x) = \{\overline{(f(x),g(x))} \ / \ f(x),g(x) \in K[x], \ g(x) \neq 0\}$, con la siguiente relación de equivalencia:

$(f(x),g(x)) \sim (h(x),k(x)) \Leftrightarrow f(x)k(x) = g(x)h(x)$.

Las operaciones se definen como ya se hizo anteriormente, o sea:

$(\overline{f(x),g(x)}) \oplus (\overline{h(x),k(x)}) = (\overline{f(x)k(x)+h(x)g(x),g(x)k(x)})$.

$(\overline{f(x),g(x)}) \odot (\overline{h(x),k(x)}) = (\overline{f(x)h(x),g(x)k(x)})$.

En el caso particular de $\mathbb{Q}$, se vió de qué manera se puede extender el orden de $\mathbb{Z}$ a un orden en $\mathbb{Q}$; esto siempre se puede hacer si el dominio entero es ordenado.

Veamos qué pasa en el caso de $K(x)$:

Supongamos que K es un campo ordenado, y por lo tanto tiene una clase positiva K^+. Definamos ahora la clase positiva $K[x]^+$ de $K[x]$:

Si $f(x) = (a_0, a_1, \ldots, a_n, 0, \ldots) \in K[x]$, entonces:

$f(x) \in K[x]^+ \leftrightarrow a_n \in K^+$.

Es decir, un polinomio de $K[x]$ es "positivo", sii su coeficiente principal, (el que le da el grado), es positivo.

Resulta inmediato de aquí que $K[x]^+ \subset K[x]$ es una clase positiva, y con ella definimos el orden en $K[x]$ de la forma canónica, es decir; $f(x) < g(x) \leftrightarrow g(x)-f(x) \in K[x]^+$.

Una vez ordenado el dominio $K[x]$, calcamos el procedimiento que se usó en $\mathbb{Q}$, para extender el orden del dominio a un orden en el campo de cocientes; haciendo notar que tal como se hizo en $\mathbb{Q}$, podemos tomar siempre representantes de cada clase que tengan "denominador" positivo, y así:

$K(x)^+ = \{[f(x),g(x)] \in K(x) \ / \ f(x) \in K[x]^+\}$.

Teniendo definida la clase positiva en el campo de cocientes, sólo queda mencionar que el orden, como es natural, queda definido de la siguiente manera:

$[f(x),g(x)] < [h(x),k(x)] \leftrightarrow [h(x),k(x)]-[f(x),g(x)] \in K(x)^+$, que es compatible con las operaciones, y que extiende el de $K[x]$ y por lo tanto el de K. Es decir, $K^+ \subset K[x]^+ \subset K(x)^+$.

CAMPOS FINITOS

Los campos con un número finito de elementos se llaman campos finitos, y con objeto de caracterizarlos, enunciamos el siguiente

TEOREMA: Dados $n \in \mathbb{Z}^+, p \in P$; existe un único campo K, (excepto por isomorfismos), tal que $o(K) = p^n$. La característica de K resulta ser p, y además, cualquier campo finito es de esta forma.

Dem: Sean $p \in P$, $n \in \mathbb{Z}^+$. Consideremos $f(x) = x^{p^n} - x$ en $\mathbb{Z}_p[x]$. Sabemos que existe F campo de descomposición de $f(x)$ sobre $\mathbb{Z}_p$. Sea $R = \{r_1, \ldots, r_{p^n} / r_i \text{es raíz de } f(x) \ \forall \ i = 1, \ldots, p^n\} \subset F$. Dado que $x^{p^n} - x \in \mathbb{Z}_p[x]$, $f'(x) = -1$, de manera que $(f(x), f'(x)) = 1$, y por lo tanto todas las raíces de $f(x)$ son de multiplicidad 1, es decir, $r_i \neq r_j$ si $i \neq j \ \forall \ i, j = 1, \ldots, p^n$.

Por lo tanto R tiene p^n elementos.

Veamos que R es campo:

i) $0, 1 \in R$, pues son raíces de $f(x)$.

ii) Sean $r_i, r_j \in R$. Como son raíces de $f(x)$, $r_i^{p^n} = r_i$, $r_j^{p^n} = r_j$.

Entonces:

$(r_i+r_j)^{p^n} = r_i^{p^n}+r_j^{p^n} = r_i+r_j$, por lo tanto $r_i+r_j \in R$.

$(r_ir_j)^{p^n} = r_i^{p^n}r_j^{p^n} = r_ir_j$, por lo tanto $r_ir_j \in R$.

iii) Sea $r_i \in R$, $(-r_i)^{p^n} = -(r_i^{p^n}) = -r_i$, por lo tanto $-r_i \in R$. (Si $p \neq 2$). Si $p = 2$, entonces, $r_i = -r_i$, y por lo tanto $-r_i \in R$.

Sea $r_i \neq 0$, entonces $r_i^{-1} \in F$, y $(r_i^{-1})^{p^n} = (r_i^{p^n})^{-1} = r_i^{-1}$.

Por lo tanto, $r_i^{-1} \in R$.

Ya que en R están los neutros y los inversos aditivos y multliplicativos, y las operaciones son cerradas; R es campo.

Por lo tanto R es campo con p^n elementos.

Reciprocamente, sea K un campo finito. Entonces existe $p \in P$ tal que $car(K) = p$. Sea $q \in P$ tal que $q \mid o(K)$. Entonces existe $a \in K$ tal que $o(a) = q$, es decir, $qa = 0$.

Por otra parte, por el algoritmo de la división, tenemos que $q = bp+r$; $b,r \in \mathbb{N}$, $0 \leq r < p$. Entonces, $0 = qa = (bp+r)a = ra$, pero $r < p$, o sea que $r = 0$.

De lo anterior tenemos que $q = bp$, es decir, $p \mid q$. Como p y q son primos, tenemos que $p = q$. Es decir que no existe ningún primo distinto de p que divida al orden de K, por lo tanto $o(K) = p^n$. +.

TEORIA FORMAL

DEFINICION: Una teoría "axiomática" formal es una teoría axiomática que tiene explícitamente incorporado un sistema lógico.

En una teoría formal se consideran varios aspectos. Se establece un conjunto a lo más numerable de símbolos. Las sucesiones finitas de símbolos serán, por definición, expresiones. Al conjunto de expresiones lo denotaremos **E**.

Se determina un subconjunto de **E**, cuyos elementos son las fórmulas; y al que denotaremos **F**.

Para determinar este subconjunto, es conveniente establecer un criterio que en un número finito de pasos nos permita decidir si una expresión es o no una fórmula. A este criterio le llamaremos procedimiento efectivo.

Del conjunto de fórmulas se selecciona un subconjunto, que denotaremos **A**, cuyos elementos son los axiomas de la teoría.

Se establece, además, un conjunto finito de relaciones a las que llamaremos reglas de inferencia. A este conjunto lo

denotaremos $\mathbf{B}$.

Si $\mathbf{B} = \{R_1,\ldots,R_k\}$, entonces R_j $j = 1,\ldots,k$ es una relación $n(j)+1$-aria, es decir, $R_j \subset \mathbf{F}^{n(j)}x\mathbf{F}$.

Si $[(F_1,\ldots,F_{n(j)}),G] \in R_j$, diremos que $F_1,\ldots,F_{n(j)}$ son las premisas; y G la conclusión, o la consecuencia inmediata de $F_1,\ldots,F_{n(j)}$ bajo R_j.

Cabe mencionar, que el orden de las premisas es irrelevante, es decir:
$[(F_1,\ldots,F_{n(j)}),G] \in R_j \leftrightarrow [(F_{s(1)},\ldots,F_{s(n(j))}),G] \in R_j \ \forall\ s \in S_n$; donde S_n es el conjunto de las permutaciones de n elementos.

DEMOSTRACIONES

DEFINICION: En una teoría formal, una demostración de una fórmula $F \in \mathbf{F}$ es una lista finita de fórmulas $F_1,\ldots,F_n \in \mathbf{F}$ tal que:

i) $F_n = F$

ii) $\forall\ i = 1,\ldots,n;\ F_i$ es:

a) un axioma, ó

b) la conclusión de una regla válida de inferencia cuyas premisas aparecen anteriormente en la lista.

Si en una teoría $\mathbf{T}$, una fórmula $F \in \mathbf{F}$ tiene demostración, diremos que F es demostrable, y lo denotaremos $\mathbf{T} \vdash F$, (en $\mathbf{T}$, se demuestra F). Si no hay duda acerca de qué teoría se trata, abreviamos: $\vdash F$.

Por supuesto que si una fórmula F es demostrable; la demostración, en general, no es única.

DEFINICION: En una teoría $\mathbf{T}$, un teorema es una fórmula que tiene demostración.

DEDUCCIONES A PARTIR DE HIPOTESIS "Γ"

Sea $\Gamma \subset \mathbf{F}$, a cuyos elementos $H_1,\ldots,H_m$ llamaremos hipótesis; y sea $F \in \mathbf{F}$.

DEFINICION: Una deducción de F en $\mathbf{T}$, a partir de Γ, es una lista finita de fórmulas $F_1,\ldots,F_n \in \mathbf{F}$ tal que:

i) $F_n = F$.

ii) $\forall\, i = 1,\ldots,n$; se cumple una de las siguientes condiciones:

a) $F_i \in \mathbf{A}$.

b) F_i es consecuencia inmediata de una regla válida de

inferencia cuyas hipótesis aparecen anteriormente en la lista.

c) $F_i \in \Gamma$.

En general, las deducciones completas están formadas por listas muy largas de proposiciones, y se acostumbra suprimir algunas cuando son obvias, y no representa problema alguno incluírlas en caso de ser requerido; o cuando son la demostración de algún teorema, y en su lugar se incluye solamente el teorema. (Por ejemplo, si en una deducción se utiliza el teorema de Pitágoras, no se escribe su demostración, sino que solamente se enuncia, y se aclara que se está haciendo referencia a él).

Si una fórmula $F \in \mathbf{F}$ tiene en $\mathbf{T}$ una deducción a partir de Γ, escribimos: En $\mathbf{T}$, $\Gamma \vdash F$, (en $\mathbf{T}$, de Γ se deduce F). Si no hay duda de la teoría, abreviamos: $\Gamma \vdash F$.

Al conjunto de deducciones de F a partir de Γ lo denotamos $D(\Gamma,F)$.

Obviamente, si para una fórmula $F \in \mathbf{F}$ tenemos $\Gamma \vdash F$, y $\Gamma = \emptyset$, entonces la deducción es una demostración. De aquí que toda demostración es una deducción.

Mencionamos tres propiedades importantes relativas al concepto de deducción:

1) Sea Γ el conjunto de hipótesis de una deducción, y $H \in \Gamma$. Entonces, $\Gamma \vdash H$, y la deducción tiene un sólo paso: H.

ii) Sea G un conjunto de fórmulas. Si $\Gamma \vdash G$, y $G \vdash F$, entonces $\Gamma \vdash F$; donde $\Gamma \vdash G$ significa que toda fórmula de G se deduce de Γ.

iii) Si $\Gamma \vdash F$, y $\Gamma \subseteq G$, entonces $G \vdash F$.

DEFINICION: Sea $\mathbf{T}$ una teoría formal, F_1, $F_2 \in \mathbf{F}$. Decimos que F_1 y F_2 son equivalentes en $\mathbf{T}$, ($F_1 \equiv F_2$ en $\mathbf{T}$); si en $\mathbf{T}$ $F_1 \vdash F_2$, y $F_1 \vdash F_2$. Si no hay duda de la teoría, abreviamos $F_1 \equiv F_2$.

TEORIAS AXIOMATICAS INTUITIVAS

Por lo general, una teoría se desarrolla y se utiliza para formalizar y dar cierta estructura a un conocimiento que ya se tiene de manera intuitiva, y en ese caso, las fórmulas son las expresiones que "tienen sentido", y los axiomas están inspirados por las propiedades que se desean para los objetos de la parte del conocimiento que se quiere formalizar. Cuando este es el caso, si en una teoría existe un procedimiento efectivo para determinar si una fórmula es o no un axioma, entonces la teoría se llama "teoría axiomática formal".

Si en una teoría formal existe un procedimiento efectivo para determinar si una fórmula es teorema, entonces la teoría es "decidible". En general, las teorías decidibles no son de mayor

interés.

El cálculo proposicional es decidible, el cálculo de predicados no lo es. En el cálculo proposicional las fórmulas son las proposiciones, y su definición nos da un procedimiento efectivo para determinar cúales expresiones son fórmulas.

Partimos de un conjunto no vacío cuyos elementos llamamos "proposiciones simples", y definimos:

DEFINICION: P es una proposición sii $P \in \mathbb{P}_i$, $i \in \mathbb{N}$, donde:

i) $\mathbb{P}_0 = \{p \in \mathbb{E} \ / \ p$ es proposición simple$\}$.

ii) $\mathbb{P}_{n+1} = \{r \in \mathbb{E} \ / \ r$ es de la forma $p \vee q$, $p \wedge q$, $p \rightarrow q$, $p \leftrightarrow q$, $\neg p$, donde $p,q \in \bigcup_{i=0}^{n} \mathbb{P}_i\}$.

Existen teorías formales en las que se define la negación de una fórmula. (Como en el cálculo proposicional, por ejemplo).

DEFINICION: Una teoría formal es completa respecto a la negación, si $\forall F \in \mathbb{F}$, F es teorema, o la negación de F es teorema.

Una teoría formal con negación es simplemente consistente si no existe $F \in \mathbb{F}$ tal que F y su negación sean teoremas.

En una teoría formal con negación en la que vale "modus ponens" como regla válida de inferencia, si una fórmula y su negación son teoremas, entonces toda fórmula es teorema.

Es decir, en una teoría inconsistente, (que no es simplemente consistente), con modus ponens como regla válida de inferencia; toda fórmula es demostrable. Como consecuencia, en un sistema formal con modus ponens como regla válida de inferencia; si existe una fórmula que no sea teorema; entonces el sistema no puede ser inconsistente.

Cuando una teoría se desarrolla para formalizar algún conocimiento, generalmente hay ciertas propiedades de los objetos que se están estudiando que son de interés. (Por ejemplo, en el cálculo proposicional nos interesa saber si una proposición es o no verdadera, es decir, si tiene o no la propiedad de ser verdadera).

Cuando este es el caso, se define una función que llamamos función propiedad, como sigue:

Sean $\mathbb{T}$ una teoría formal, y $\mathbb{F}$ el conjunto de fórmulas de $\mathbb{T}$. Sea $p : \mathbb{F} \longrightarrow \{ 0,1 \}$ una función. Entonces a p la llamamos función propiedad, y diremos que si para $F \in \mathbb{F}$, $p(F) = 1$, entonces "F tiene la propiedad p"; y si $p(F) = 0$, entonces "F no tiene la propiedad p". Se suele convenir en llamar a "1" y a "0" de alguna manera, por ejemplo "verdadero" y "falso". En este caso, si $p(F) = 1$ entonces decimos que la fórmula F es "verdadera", y si $p(F) = 0$, decimos que F es "falsa".

DEFINICION: Sea T una teoría formal, F el conjunto de fórmulas de T, $H = \{F \in F \ / \ F$ es teorema$\}$, p una propiedad, y por último $K = \{F \in F \ / \ p(F) = 1\}$. Entonces:

i) T es consistente con respecto a p si $H \subseteq K$, es decir, si toda fórmula que es teorema tiene la propiedad p.

ii) T es completo con respecto a p si $K \subseteq H$, es decir, si toda fórmula que tiene la propiedad p es teorema.

Claramente, T es consistente y completo con respecto a p sii $H = K$.

Cuando la teoría se utiliza para estudiar alguna propiedad p, es deseable escoger como axiomas fórmulas que tengan la propiedad p. Si además, cada regla válida de inferencia preserva la propiedad p; es decir, que siempre que todas las premisas tengan la propiedad p, la conclusión también necesariamente tenga la propiedad p; entonces, obviamente, la teoría resulta consistente con respecto a la propiedad p.

Por ejemplo, en el cálculo proposicional, en el que se estudia la propiedad de ser "tautología", todos los axiomas tienen esa propiedad, y además, la regla válida de inferencia, que es "modus ponens" preserva la propiedad de ser "tautología", de manera tal que el cálculo proposicional es consistente con respecto a la propiedad de ser verdadero; es decir, en el cálculo proposicional, todo teorema es "tautológico". Dado que hay proposiciones que no

son tautologías, (y que por tanto no son demostrables), el cálculo proposicional es simplemente consistente y se puede probar además, que puesto que todo renglón de las tablas de verdad "básicas", (la de $\neg$, $\wedge$, $\vee$, e $\rightarrow$), es demostrable, entonces toda tautología es demostrable, y en este sentido el cálculo proposicional es completo (con respecto a la propiedad de ser tautología).

A continuación, se da un par de lo que se afirma aquí:

Ej.1: En la tabla de la implicación, el tercer renglón se lee:

P	Q	$P \rightarrow Q$
1	0	0

, y entonces, de acuerdo con lo que se aseguró, veremos que $P, \neg Q \vdash \neg(P \rightarrow Q)$.

Dem (Reducción al absurdo): Supongamos, (hipótesis adicional) $P \rightarrow Q$, que es lo contrario a lo que se quiere demostrar. Entonces:

1) $P \rightarrow Q$ ...Hip. ad.

2) P ...Hip.

3) Q ...M.P.(2,1)

4) $\neg Q$ ...Hip.

5) $Q \wedge \neg Q$ ...(3,4) !

$\dagger$.

Habiendo mostrado como se puede probar un renglón de la tabla de la implicación, y aceptando que de igual modo pueden probarse todos los demás, dado que la tabla de una proposición se construye

aplicando iteradamente las tablas básicas, (demostrables), aceptemos que todo renglón de toda tabla es igualmente demostrable y pasemos al

Ej.2: Sea T una tautología que está formada por fórmulas P, Q, y R. Entonces, su tabla es:

P	Q	R	T
1	1	1	1
0	1	1	1
1	0	1	1
0	0	1	1
1	1	0	1
0	1	0	1
1	0	0	1
0	0	0	1

De los renglones 1 y 2 se obtiene:

$P,Q,R \vdash T$

$\neg P,Q,R \vdash T \quad \therefore (P \vee \neg P),Q,R \vdash T \quad \therefore Q,R \vdash T$ (ya que $\vdash P \vee \neg P$).

Análogamente, de 3,4 se obtiene:

$\neg Q,R \vdash T \quad \therefore R \vdash T$.

Haciendo lo mismo con los últimos cuatro renglones, se llega a:

$\neg R \vdash T \quad \therefore (R \vee \neg R) \vdash T \quad \therefore \vdash T$.

$\dagger$.

Remarquemos pues que, como consecuencia de los párrafos anteriores, el cálculo proposicional es consistente y completo.

INFINITESIMOS E INFINITOS

Kurt Gödel demostró que una teoría axiomática es consistente, es decir, que de los axiomas no se puede deducir una contradicción; si y sólo si tiene un modelo, es decir, si y sólo si existe un "universo de interpretación de las fórmulas" en el que todos los axiomas son verdaderos.

Como consecuencia, tenemos el siguiente "teorema de compacidad":

TEOREMA: Si en una teoría **T** existe una colección numerable de axiomas tal que para cada subcolección finita existe un modelo; entonces existe un modelo para la colección completa.

Es fácil ver que el teorema de compacidad se deriva del resultado anterior; pues si toda subcolección finita de la colección numerable de axiomas tiene un modelo, entonces toda subcolección finita es lógicamente consistente. De aquí se sigue que la colección completa tiene que ser consistente, ya que cualquier deducción se da en un número finito de pasos, que por tanto utilizan un número finito de axiomas; luego cualquier inconsistencia contradiría la hipótesis que asegura que toda subcolección finita de axiomas es consistente. Siendo consistente

la colección completa, tiene que tener un modelo.

Demostraremos ahora que la existencia de infinitésimos es consecuencia directa del teorema de compacidad:

DEFINICION: Sea K un campo ordenado tal que $\mathbb{R} \subset K$. (El orden de K extiende al de $\mathbb{R}$). $c \in K$ es un "infinitésimo positivo" sii $\forall\, n \in \mathbb{N}$, $0 < c < 1/n$. (Nótese que este no es un enunciado de existencia, simplemente dice qué características debe tener un infinitésimo, si es que tal cosa existe).

Consideremos la colección de axiomas $\{A_i\}_{i\in\mathbb{N}}$, donde:

$A_i \equiv \exists\, a$ en alguna extensión orednada de $\mathbb{R}$ tal que $0 < a < 1/i$.

En el "universo" $\mathbb{R}$, cada subcolección finita de los axiomas anteriores es verdadera, pues en cada subcolección finita C de la colección de axiomas existe $k \in \mathbb{N}$ tal que $A_k \in C$, y $A_j \notin C\ \forall j > k$. Si tomamos $a = 1/2k$, tenemos $0 < 1/2k < 1/i\ \forall\, i$ tal que $A_i \in C$. Además, $a \in \mathbb{R}$.

Sin embargo, en $\mathbb{R}$ la colección completa no es verdadera. Por el teorema de compacidad debe existir un universo en el que la colección completa sea verdadera; es decir, debe existir un campo ordenado K, con un elemento c, tal que $0 < c < 1/n\ \forall\, n \in \mathbb{N}^*$; y que de acuerdo con la definición, es un infinitésimo.

A continuación, daremos un ejemplo de un campo que contiene a R, en el que existen los infinitésimos; o sea, un modelo para la colección $\{A_i\}_{i\in N}$.

UN CAMPO EXTRAÑO

Siendo este un caso particular de $K(x)$, en el que el campo es R, podemos aplicar todas las definiciones anteriores.

Tenemos entonces:

$$R(x) = \{ [f(x),g(x)] \ / \ f(x),\ g(x) \in R[x],\ g(x) \neq 0 \}/R$$

La relación R de equivalencia, que ya ha sido mencionada en capítulos anteriores, es:

$$[f(x),g(x)] \sim [h(x),k(x)] \leftrightarrow f(x)k(x) = g(x)h(x).$$

Dado que $\{R,+,\cdot\}$ es un campo ordenado, $R[x]$ es un dominio entero ordenable, y por lo tanto podemos hablar de orden en $R(x)$; (este orden, por supuesto, extiende al orden de R). Repetimos:

DEFINICION: $R[x]^+=\{f(x) \in R[x] \ / \ cp(f(x)) \in R^+\}$, donde $cp(f(x))$ es el coeficiente principal de $f(x)$.

Como se vió anteriormente, $\mathbb{R}[x]^+$ es una clase positiva, y definimos el orden en $\mathbb{R}[x]$ como sigue:

$$f(x) < g(x) \iff g(x)-f(x) \in \mathbb{R}[x]^+.$$

Ahora, extendemos lo anterior a $\mathbb{R}(x)$:

DEFINICION: $\mathbb{R}(x)^+ = \{[f(x),g(x)] \in \mathbb{R}(x) \ / \ f(x) \in \mathbb{R}[x]^+\}$.

Damos por hecho que $g(x) \in \mathbb{R}[x]^+$, pues ya vimos que si el dominio está ordenado, siempre se pueden tomar representantes con "denominador" positivo.

NOTACION: Por comodidad, para $f(x) \in \mathbb{R}[x]$ escribiremos f, y para $[f(x),g(x)] \in \mathbb{R}(x)$ escribiremos $\frac{f}{g}$.

$\mathbb{R}(x)^+$ resulta entonces ser una clase positiva. Definimos el orden:

$$\frac{f}{g} < \frac{h}{k} \iff \frac{h}{k} - \frac{f}{g} \in \mathbb{R}(x)^+.$$

Como conclusión de las observaciones anteriores, se tiene que $\mathbb{R}$ es un subcampo de $\mathbb{R}(x)$, y que en $\mathbb{R}(x)$ hemos definido un orden que extiende al de $\mathbb{R}$.

Ahora, definimos la "norma", o "tamaño" de los elementos de $\mathbb{R}(x)$:

DEFINICION: Sea $\frac{f}{g} \in \mathbb{R}(x)$.

$$\left\| \frac{f}{g} \right\| = \begin{cases} \frac{f}{g} & \text{si } \frac{f}{g} \geq 0 \\ -\frac{f}{g} & \text{si } \frac{f}{g} < 0 \end{cases}$$

que es la definición de siempre, (la canónica), y por lo tanto en ella se cumple el siguiente teorema, cuya demostración se omite:

TEOREMA:

i) $\left\| \frac{f}{g} \right\| \geq 0$; $\left\| \frac{f}{g} \right\| = 0 \Leftrightarrow \frac{f}{g} = 0$.

ii) $\left\| \frac{f}{g} \right\| = \left\| -\frac{f}{g} \right\|$.

iii) $\left\| \frac{f}{g} + \frac{h}{k} \right\| \leq \left\| \frac{f}{g} \right\| + \left\| \frac{h}{k} \right\|$.

COROLARIO: Si definimos $D : \mathbb{R}(x) \times \mathbb{R}(x) \to \mathbb{R}(x)$ como sigue:

$D\left(\frac{f}{g}, \frac{h}{k}\right) = \left\| \frac{f}{g} - \frac{h}{k} \right\|$, entonces D es una métrica.

Repetimos la

DEFINICION: $\alpha \in \mathbb{R}(x)$ es un infinitésimo positivo sii :

$0 < \alpha < \frac{1}{n} \quad \forall\, n \in \mathbb{Z}^+$.

Denotamos al conjunto de los infinitésimos positivos por inf., y nos referiremos exclusivamente a estos.

TEOREMA: inf. $\neq \emptyset$.

Dem: Sea $\alpha = \frac{1}{x^n}$, $n \in \mathbb{Z}^+$. $x \in \mathbb{R}[x]^+$, entonces $x^n \in \mathbb{R}[x]^+$, por lo tanto $\frac{1}{x^n} \in \mathbb{R}(x)^+$, puesto que $1 \in \mathbb{R}^+$. $\therefore 0 < \alpha$.

Por otra parte, sea $m \in \mathbb{Z}^+$. $\frac{1}{m} - \frac{1}{x^n} = \frac{x^n - m}{mx^n}$, y como $x^n \in \mathbb{R}[x]^+, m \in \mathbb{Z}^+ \implies mx^n \in \mathbb{R}[x]^+$; y $x^n - m \in \mathbb{R}[x]^+$; tenemos que $\frac{1}{m} - \frac{1}{x^n} \in \mathbb{R}(x)^+$, y por lo tanto $\alpha < \frac{1}{m}$. Resumiendo, $0 < \alpha < \frac{1}{m}$ $\forall\, m \in \mathbb{Z}^+$, es decir, $\alpha \in$ inf.

+.

DEFINICION: Sean $\alpha,\beta \in \inf.$

α es de oredn superior a $\beta \leftrightarrow \dfrac{\alpha}{\beta} \in \inf.$

Por ejemplo, $\dfrac{1}{x^n}$ es de orden superior a $\dfrac{1}{x^m} \leftrightarrow n > m$, pues:

$$\frac{\frac{1}{x^n}}{\frac{1}{x^m}} = \frac{x^m}{x^n} = x^{m-n} = \frac{1}{x^{n-m}} \in \inf. \leftrightarrow n-m \in \mathbb{Z}^+ \leftrightarrow n > m.$$

TEOREMA: $\dfrac{f}{g} \in \mathbb{R}(x) \cap \inf. \leftrightarrow d(f) < d(g).$

Dem: $\leftarrow$) Supongamos que $d(f) = a < b = d(g)$. Sea $n \in \mathbb{Z}^+$.

$$\frac{1}{n} - \frac{f}{g} = \frac{g - nf}{ng}. \quad ng \in \mathbb{R}[x]^+, \text{ y } cp(g - nf) = cp(g) > 0.$$

Entonces, $\dfrac{1}{n} - \dfrac{f}{g} \in \mathbb{R}(x)^+$, de donde $-\dfrac{f}{g} < \dfrac{1}{n}$, además, obviamente $0 > -\dfrac{f}{g}$, y por lo tanto está en inf.

$\rightarrow$) Supongamos que $d(g) < d(f)$. Sea $n = 1$.

$$1 - \frac{f}{g} = \frac{g - f}{g}. \; cp(g - f) = -cp(f); \text{ entonces } g - f \in \mathbb{R}[x]^+, \text{ por lo tanto; } \frac{f}{g} \in \inf.$$

Ahora supongamos que $d(f) = d(g)$; $cp(f) = a$, $cp(g) = b$.

Entonces existe $n_0 \in \mathbb{N}$ tal que $b < n_0 a$, entonces:

$$\frac{1}{n_0} - \frac{f}{g} = \frac{g - n_0 f}{n_0 g} \cdot cp(g - n_0 f) = b - n_0 a < 0, \text{ por lo tanto,}$$

$$-\frac{f}{g} \notin \text{inf.}, \text{ entonces } \frac{f}{g} \in \text{inf.} \Leftrightarrow d(f) < d(g).$$

+.

OBSERVACION: Como $\mathbb{R}(x)$ es campo, $\forall\, \alpha \in \text{inf.}$, $\exists\, \alpha^{-1} \in \mathbb{R}(x)$.

Definimos entonces: $\text{Inf.} = \{A \in \mathbb{R}(x) \;/\; A = \alpha^{-1} \text{ p.a. } \alpha \in \text{inf.}\}$.

Inf. es el conjunto de los "infinitos" positivos.

COROLARIO: $\frac{f}{g} \in \text{Inf.} \Leftrightarrow d(g) < d(f)$.

DEFINICION: Si $A, B \in \text{Inf.}$:

A es de orden superior a $B \Leftrightarrow \frac{A}{B} \in \text{Inf.}$

TEOREMA: Sea $\alpha \in \mathbb{R}(x)$. Entonces $\alpha < c\ \forall\, c \in \mathbb{R}^+ \Leftrightarrow \alpha \in \text{inf.}$.

Dem:$\Rightarrow$) Sea $n \in \mathbb{Z}^+$. $\exists\, c_0 \in \mathbb{R}^+$ tal que $c_0 < \frac{1}{n}$, pero $\alpha < c_0 < \frac{1}{n}$;

por lo tanto $\alpha \in \text{inf.}$.

$\Leftarrow$) Sea $\varepsilon \in \mathbb{R}^+$. $\exists\, n_0 \in \mathbb{Z}^+$ tal que $\frac{1}{n_0} < \varepsilon$.

$\alpha \in$ inf. $\Rightarrow \alpha < \frac{1}{n}\ \forall\, n \in \mathbb{Z}^+$. Por lo tanto $\alpha < \frac{1}{n_0} < \varepsilon$.

+.

TEOREMA: inf. es cerrado bajo sumas y productos.

Dem: Sean $\frac{f}{g}, \frac{h}{k} \in$ inf.. Entonces, $d(f) < d(g)$, y $d(h) < d(k)$.

$\frac{f}{g} + \frac{h}{k} = \frac{fk + gh}{gk}$. Como $d(f) < d(g)$, tenemos que $d(fk) < d(gk)$, y como $d(h) < d(k)$, $d(gh) < d(gk)$. Por lo tanto $d(fk+gh) < d(gk)$.

$\therefore \frac{f}{g} + \frac{h}{k} \in$ inf..

Además; $\frac{f}{g} \cdot \frac{h}{k} = \frac{fg}{hk}$. Claramente, $d(fg) < d(hk)$; $\therefore \frac{fg}{hk} \in$ inf..

Por lo tanto, inf. es cerrado bajo sumas y productos.

+.

COROLARIO: Inf. es cerrado bajo sumas y productos.

TEOREMA: Sean $\alpha, \beta \in$ inf., $t \in \mathbb{R}^+$. Entonces, $t\alpha \in$ inf..

Dem: $\alpha \in \text{inf.} \Rightarrow \alpha < c$, $\forall\, c \in \mathbb{R}^+$; entonces, $\alpha < \frac{1}{nt}$, $\forall\, n \in \mathbb{Z}^+$.

Por lo tanto, $t\alpha < \frac{1}{n}$, es decir; $t\alpha \in$ inf..

†.

COROLARIO: Sean $A \in$ Inf., $t \in \mathbb{R}^+$. Entonces, $tA \in$ Inf..

A continuación, daremos algunas definiciones:

Sean $P,Q \in \mathbb{R}(x)$.

i) Si $D(P,Q) \in \mathbb{R} \cup$ inf., entonces P y Q están en la misma "galaxia".

ii) Si $D(P,Q) \in$ inf., entonces P y Q están en la misma "aura", (infinitamente próximos).

iii) Si $D(P,Q) \in$ Inf., entonces P y Q están en diferentes "galaxias", (infinitamente separados).

RECTAS

DEFINICION: Sean $P,Q,R \in \mathbb{R}(X)$ tales que $P^2+Q^2 > 0$. Llamamos "RECTA" al conjunto $\mathcal{L} = \{(t,u) \in \mathbb{R}(x)x\mathbb{R}(x) \;/\; Pt+Qu+R = 0\}$.

Así, por ejemplo, las rectas t = cte. son las verticales, y las rectas u = cte. son las horizontales. Cuando este no es el caso, y

$u = u(t)$, entonces $\forall\ t \in \mathbb{R}(x)$, $\mathcal{L}(t)$ es el punto $(t,u(t))$ de la recta $\mathcal{L}$; y, de igual manera, si $u \in \mathbb{R}(x)$, y $t = t(u)$, $\mathcal{L}(u)$ es el punto $(t(u),u)$ de la recta $\mathcal{L}$.

DEFINICION: Sean $\mathcal{L}_1, \mathcal{L}_2$ dos rectas no verticales. Decimos que $\mathcal{L}_1$ y $\mathcal{L}_2$ están infinitamente cercanas en una galaxia G, sii $\forall\ t \in G$, $\mathcal{D}(\mathcal{L}_1(t),\mathcal{L}_2(t)) \in \text{inf.} \cup \{0\}$.

(Recordemos que $\mathcal{D} : [\mathbb{R}(x)x\mathbb{R}(x)]x[\mathbb{R}(x)x\mathbb{R}(x)] \to \mathbb{R}(x)$ está definida por: $\mathcal{D}\ [(a,b),(c,d)] = (D^2(b,d)+D^2(a,c))^{1/2}$).

Si al menos una es vertical, son infinitamente cercanas en G sii $\forall\ u \in G$, $\mathcal{D}(\mathcal{L}_1(u),\mathcal{L}_2(u)) \in \text{inf.} \cup \{0\}$.

DEFINICION: Sean $\mathcal{L}_1$ y $\mathcal{L}_2$ rectas no verticales. Decimos que $\mathcal{L}_1$ es "casi paralela" a $\mathcal{L}_2$ en G, si $\forall\ t_1, t_2 \in G$:

$$\mathcal{D}(\mathcal{L}_1(t_1),\mathcal{L}_2(t_1))-\mathcal{D}(\mathcal{L}_1(t_2),\mathcal{L}_2(t_2)) \in \text{inf.} \cup \{0\}.$$

Si al menos una es vertical, entonces son "casi paralelas" en G si $\forall\ u_1, u_2 \in G$:

$$\mathcal{D}(\mathcal{L}_1(u_1),\mathcal{L}_2(u_1))-\mathcal{D}(\mathcal{L}_1(u_2),\mathcal{L}_2(u_2)) \in \text{inf.} \cup \{0\}.$$

A continuación veremos un ejemplo de dos rectas paralelas, y otras dos que son "casi paralelas" a ellas (y entre sí), en una galaxia, pero se intersectan en otra galaxia. Además concluímos que toda recta en $\mathbb{R}(x)x\mathbb{R}(x)$, tiene puntos en un número infinito de galaxias.

Sean $\mathcal{L}_A = \{(t,0) \ / \ t \in \mathbb{R}(x)\}$, $\mathcal{L}_B = \{(t,1) \ / \ t \in \mathbb{R}(x)\}$, dos rectas paralelas, (horizontales).

Construímos $\mathcal{L}_1 = \{(t,t/x) \ / \ t \in \mathbb{R}(x)\}$,

$\mathcal{L}_2 = \{(t,1-t/x) \ / \ t \in \mathbb{R}(x)\}$. Entonces:

$\mathcal{L}_1$ y $\mathcal{L}_A$ pasan por (0,0), y son "casi paralelas". Lo mismo sucede con las rectas $\mathcal{L}_2$ y $\mathcal{L}_B$ y el punto (0,1).

Además, $\mathcal{L}_1$ y $\mathcal{L}_2$ son "casi paralelas"; pero se intersectan en el punto $(x/2,1/2)$ que no está en la galaxia de (0,0) y (0,1).

Sea G_0 la galaxia en la que están (0,0) y (0,1); y G_1 la galaxia en la que está $(x/2,1/2)$.

(Nótese que estamos en $\mathbb{R}(x)x\mathbb{R}(x)$, y por supuesto que aquí decimos que dos puntos $(a,b),(c,d) \in \mathbb{R}(x)x\mathbb{R}(x)$ están en diferentes galaxias si $\mathcal{D}((a,b),(c,d)) \in$ Inf.).

En cada galaxia "intermedia" entre G_0 y G_1, $\mathcal{L}_1$ y $\mathcal{L}_2$ se acercan "infinitamente poco", de donde concluímos que entre G_0 y G_1 hay un número infinito de galaxias.

Esto se ve claramente del hecho de que si P y Q son puntos de $\mathbb{R}(x) = \mathbb{R}(x)x\{0\}$ que están en diferentes galaxias, entonces $\frac{P+Q}{2}$ está en una galaxia intermedia, lo que muestra que $\forall\, G_0,G_1$

galaxias diferentes, siempre hay puntos de una tercera galaxia intermedia, (en la misma recta); y por lo tanto, hay al menos aleph cero de ellas.

A continuación, veremos un ejemplo del uso de infinitésimos:

Sea $M = \{(t,t^2) \ / \ t \in \mathbb{R}(x)\}$ una parábola en $\mathbb{R}(x)x\mathbb{R}(x)$. ¿ Cómo calculamos su tangente en un punto $P \in \mathbb{R}x\mathbb{R}$ usando infinitésimos ? Por supuesto, estamos considerando que la pendiente de esta tangente sea un número real.

Sea $P = (1,1) \in M$, y sea $\alpha \in$ inf.. Consideremos los puntos $Q = (1 + \alpha, (1 + \alpha)^2)$, y $R = (1 - \alpha, (1 - \alpha)^2)$; ambos en M. La pendiente de la recta tangente a M por el punto P está entre las pendientes de las rectas PQ, y PR.

La pendiente de la recta PQ es $\dfrac{(1 + \alpha)^2 - 1}{1 + \alpha - 1} = \dfrac{\alpha(2 + \alpha)}{\alpha} = 2 + \alpha.$

La pendiente de la recta PR es $\dfrac{(1 - \alpha)^2 - 1}{1 - \alpha - 1} = \dfrac{\alpha(\alpha - 2)}{-\alpha} = 2 - \alpha.$

Como buscamos un número real entre $2+\alpha$, y $2-\alpha$, concluímos que la pendiente de la recta tangente a M en P es 2; pues es el único número real en ese intervalo.

ALGUNAS OBSERVACIONES FINALES

OBSERVACION: En $\mathbb{R}(x)$, existen subconjuntos no vacíos y acotados por arriba que no tienen supremo. $\mathbb{N}$ es uno de ellos.

Se sabe, que $\mathbb{N}$ no tiene supremo en $\mathbb{R}(x)$. (Si $t_0 \in \mathbb{R}(x)$ fuera $t_0 = \sup \mathbb{N}$, entonces dada $\varepsilon = 1/2$, existe $n_0 \in \mathbb{N}$ tal que $t_0 - 1/2 < n_0 \leq t_0 + 1/2$, y por lo tanto $n_0 + 1 \in \mathbb{N}$ resultaría $t_0 < n_0 + 1$ lo cual es absurdo) ;y sin embargo $x \in \mathbb{R}(x)$ es cota superior de $\mathbb{N}$.

COROLARIO: El orden en $\mathbb{R}(x)$ no es arquimediano.

Por supuesto que la observación anterior es redundante en vista del carácter categórico de la definición de $\mathbb{R}$ como el único campo ordenado en el que vale el Teorema de Dedekind, que implica, entre otras cosas, que el orden de $\mathbb{R}$ es arquimediano, y que por lo tanto, en un campo tal, no existen los infinitésimos.

Resumiendo: En todo campo ordenado:

Teorema de Dedekind $\Longrightarrow$ Orden Arquimediano $\Longrightarrow$ No Infinitésimos; y por lo tanto, por contrapuesta:

Infinitésimos $\Longrightarrow$ Orden NO Arquimediano $\Longrightarrow$ No Teo. de Dedekind; es decir que en todo campo ordenado en el que haya infinitésimos,

TIENEN que existir conjuntos no vacios acotados por arriba y sin supremo, como $\mathbb{N}$; acotados por abajo sin ínfimo, como $\mathbb{Z}$; y conjuntos cerrados y acotados no compactos, como $\mathbb{N}$, que es cerrado y acotado por $\mathbb{R}$, pero la cubierta abierta $\{(n-1/4, n+1/4)\}_{n\in\mathbb{N}}$ no tiene una subcubierta finita.

En este trabajo se demostró que existe, y se construyó explícitamente, un campo que contiene a $\mathbb{R}$, y además tiene infinitésimos. Sin embargo, no es un campo de "Super-Reales", pues entre otras cosas no vale el Principio de Transferencia, es decir, que las propiedades de $\mathbb{R}$ se puedan extrapolar a él. En este campo no sucede que cualquier elemento tiene raíces n-ésimas dentro de él. Por ejemplo, no existe $\alpha \in \mathbb{R}(x)$ tal que $\alpha^n = x$; pues todos los elementos de $\mathbb{R}(x)$ son de la forma $f(x)/g(x)$, y ninguna potencia mayor que 1 de ellos puede dejarlos con grado 1. Es decir, este trabajo no tiene más pretensiones que ilustrar un campo con infinitésimos.

BIBLIOGRAFIA

[1] **DAVIS, MARTIN; HERSH, REUBEN.** *Nonstandard Analysis.* Scientific American, 7, 78-86. 1972.

[2] **HERSTEIN, I.,** *Topics in Algebra.* Xerox, Massachusetts. 1975.

[3] **KLEENE, COLE STEPPHEN,** *Mathematical Logic.* John Wiley and Sons, Inc., New York. 1967.

[4] **PADILLA GONZALEZ, ALEJANDRO,** *El Calculo Proposicional como un Sistema Formal.* Tesis, Universidad Autonóma de Querétaro, Querétaro. 9-20. 1989.

[5] **STOLL,** *Set Theory and Logic.* W.H. Freeman and Co.

Impresiones Aries al Instante, S.A. de C.V.
Rep. de Colombia No. 5, Col. Centro
06020 México, D. F.
526 04 72, 526 29 13, Fax 526 29 06