2
2ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

ALGUNOS RESULTADOS SOBRE ALGEBRA CONSTRUCTIVA.

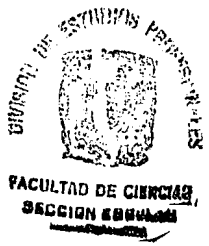
T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A :

ALEJANDRO ALVARADO GARCIA



MEXICO, D. F. 1994

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

CIUDAD UNIVERSITARIA

UNIVERSIDAD NACIONAL AVENIDA DE MEXICO

FACULTAD DE CIENCIAS
División de Estudios Profesionales
Exp. Núm. 55

M. EN C. VIRGINIA ABRIN BATULE
Jefe de la División de Estudios Profesionales
Universidad Nacional Autónoma de México.
P r e s e n t e .

Por medio de la presente, nos permitimos informar a Usted, que habiendo revisado el trabajo de tesis que realizó el pasante ALVARADO GARCIA ALEJANDRO

con número de cuenta 8607410-6 con el título: ALGUNOS RESULTADOS SOBRE ALGEBRA BOOLEANA

Consideramos que reune los méritos necesarios para que pueda continuar el trámite de su Examen Profesional para obtener el título de - MATEMATICO.

GRADO NOMBRE Y APELLIDOS COMPLETOS	FIRMA
Dr. [illegible]	Hugo A. Rincón M.
Director de Tesis Dr. JOSE RIOS PUENTE	José Ríos M.
M. en C. JOSE [illegible]	[illegible]
[illegible]	RRB.
Suplente [illegible]	Virginia Abrín Batule
Suplente	

Ciudad Universitaria, D.F., a 4 de Abril de 1994

A la memoria de mi Madre...

A mi Padre...

A Lulú.

Deseo expresar mi agradecimiento a las siguientes personas:

A mi madre, Rosa García, quién desde lo alto (junto a Dios), me ha transmitido la fuerza interior para seguir adelante en mi carrera y en mi vida.

A mi padre, José Alvarado, quién siempre se ha esforzado por darme lo mejor de lo que tiene, así como su comprensión, cariño y apoyo.

A mi hermano, José A. Alvarado, eres un estupendo hermano. Y a su esposa, Mary, y a mi sobrino, Toñito.

A Luiú, porque siempre me ha apoyado a seguir adelante, en la escuela en mi vida y en mi corazón, (Te amo). A sus padres, por su confianza y apoyo en todo momento.

A Angel, porque en todo momento me ha ayudado como un hermano. Gracias a ti he podido escribir este trabajo.

A todo el grupo de amigos de la comunidad.

A Martín, por ser mi compañero y amigo.

Al Dr. Hugo A. Rincón M. (mi asesor), por ser un gran profesor, compañero y amigo, por todo el apoyo y confianza que me ha brindado.

Alejandro Alvarado García.

INDICE.

INTRODUCCION.

Durante los últimos cien años se han formado diversas " *tendencias* " ó " *escuelas* " que se aproximan a lo que podría ser llamado " *constructivista* " en un sentido amplio, sin embargo, todas ellas difieren en aspectos considerables.

"*Constructivismo*", en sentido amplio, no tiene un significado homogéneo y aún existen representantes de las mismas escuelas que discrepan entre sí, e incluso con sigo mismos en distintos tiempos.
Nosotros trabajaremos dentro de la tendencia principal, llamada *Intuicionismo*.

Aquí, el *intuicionismo* será entendido como la aproximación constructiva a las matemáticas en el espíritu de Brouwer (1881 - 1966) y Heyting (1898 - 1980). Las bases filosóficas de esta aproximación fueron presentadas en la tesis de Brouwer en 1907.

En nuestro trabajo solo desarrollaremos las bases para la lógica de predicados intuicionista, para obtener reglas de inferencia que nos permitan hacer demostraciones de proposiciones sin necesidad de volver a nuestras definiciones originales.

El trabajo se divide esencialmente en dos partes. La primera, que abarca los tres primeros capítulos, está dirigida a resolver, en alguna medida, lo expuesto en el párrafo anterior:

- En el primer capítulo se explica lo que se va a entender por una demostración de una proposición en base a su complejidad lógica (es decir, si se trata de una disyunción, una conjunción, una implicación etc.) y, con base en esas explicaciones se demuestra que ciertas proposiciones deberían ser válidas, mientras que otras no podrían ser válidas (esto no quiere decir que dichas proposiciones no sean verdaderas).

- En el segundo capítulo se define formalmente el sistema de la lógica de predicados intuicionista, anexando ejemplos de deducciones válidas en nuestro sistema. El capítulo concluye haciendo ver que dicho sistema difiere del sistema de la lógica clásica solo en un axioma.

- En el tercer capítulo desarrollamos otra forma del cálculo proposicional, llamado cálculo de *secuencias* (desarrollado por Gentzen), definiendo claramente sus axiomas y reglas de inferencia (también, se le es asignado a cada secuencia, su *fórmula imagen*, que es una proposición en el cálculo de predicados intuicionista) . Después de demostrar una serie de lemas con relación a dicho cálculo demostramos que es equivalente al cálculo de predicados intuicionista en el sentido de que, una secuencia es deducible en su sistema si y solo si su fórmula imagen es deducible en el cálculo intuicionista. A partir de esa demostración, se obtiene el resultado principal: Las proposiciones $\neg\neg P \Rightarrow P$ y el principio del tercer excluído $P \vee P$, no son válidos en nuestro sistema intuicionista.

La segunda parte (capítulos 4 y 5) se adentra ya en el tema del álgebra y su principal objetivo es el de poder obtener resultados acerca de la teoría de grupos y de anillos que sean lo más cercanos a los correspondientes en las teorías clásicas.

El principal obstáculo para ello, es el hecho de tener que, las estructuras algebraicas no conllevan una relación de igualdad decidible entre los elementos de sus conjuntos, es decir que no es posible (constructivamente) saber si dos elementos son iguales o no, creando algunos problemas en las subestructuras que se definen (subgrupos, ideales, estructuras cociente etc.).

Estos problemas se evitan un poco al introducir una relación entre los elementos del conjunto, la llamada relación de separabilidad (cuyos axiomas fueron formulados por Heyting en 1925). Esta relación generaliza en un sentido la noción de ser distintos (estar "separados" implica que los elementos son distintos pero, el que los elementos sean distintos no nos asegura que esten separados).
Entonces para poder desarrollar un poco más de teoría se les pide a las estructuras algebraicas que posean una relación de separabilidad.

Con base en lo anterior se dan las definiciones y conseptos que son básicos en la teoría de grupos y de anillos llegando a algunos resultados muy interesantes y semejantes a los de la teoría clásica como se buscaba.

CAPITULO 1.

LA INTERPRETACION BHK.

OPERACIONES LOGICAS.

1) La Interpretación BHK.

En realidad en el desarrollo de la matemática constructiva no necesitamos lógica; sin embargo encontramos conveniente utilizar simbolismos lógicos.

Explicaremos el uso de las operaciones lógicas en un contexto constructivo por medio de las siguientes estipulaciones, las cuales nos dicen las formas que las demostraciones de proposiciones compuestas (logicamente) toman en términos de las demostraciones de sus proposiciones simples.

H1) Una demostración para $A \wedge B$ está dada al presentar una demostración de A y una demostración de B.

H2) Una demostración para $A \vee B$ está dada al presentar una demostración de A ó una demostración de B. (mas la suposición de que deseamos ver la demostración presentada como evidencia para $A \vee B$).

H3) Una demostración de $A \Rightarrow B$ es una construcción la cual nos permite transformar cualquier demostración de A en una demostración de B.

H4) El absurdo $\perp$ (contradicción), no tiene demostración; una demostración de $\neg A$ es una construcción que transforma cualquier demostración hipotética de A en una demostración de una contradicción.

H5) Una demostración de $(\forall x)\, A(x)$ es una construcción que transforma una demostración de que $d \in D$ (donde D es el dominio de interpretación de la variable x), en una demostración de A(d).

H6) Una demostración de $(\exists x)\, A(x)$ está dada al mostrar alguna $d \in D$, y una demostración de A(d).

Esta explicación es muy informal y se sostiene por ella misma sólo en nuestro entendimiento de la noción de *construcción* e, implícitamente, la noción de *mapear*. No es difícil notar casi de inmediato que a tal matemática se le puede asociar con cada fórmula A un valor de verdad $z(A)$ por medio de una inducción matemática fuerte con respecto a la construcción de la fórmula A. El valor $z(A)$ será 0 , " *falso* ", ó 1 , " *verdadera* ", y el *"cálculo"* de $z(A)$ procede de acuerdo con la interpretación clásica usual de los conectivos :

$$z(A_1 \wedge A_2) = \min \{ z(A_1), z(A_2) \}$$
$$z(\perp) = 0$$
$$z(A_1 \vee A_2) = \max \{ z(A_1), z(A_2) \}$$
$$z((\forall x) A(x)) = \min \{ z(A(y)) \mid y \in D \}$$

etc. Ahora denominamos 1 a la construcción que verifica A si y solo si z(A) es 1. Uno puede mostrar que los requerimientos **H1-6** son se satisfacen si las palabras que se refieren a la efectividad de la construcción son interpretadas simplemente como afirmaciones a cerca de la existencia desde un punto de vista intuitivo de la teoría de conjuntos. Por ejemplo:
si $z(A_1 \Rightarrow A_2) = 1$, entonces , para cada construcción que verifica A_1 (esto solo puede ser 1), uno puede especificar una construcción que verifique A_2 (nombrada, uno debe tomar a la unidad). Vemos que esto nos lleva a que en una muy *clásica* interpretación de *mapeo* y *construcción*, **H1-6** justifican los principios de la *lógica dos-valuada*.

En **H4**, la noción de una *contradicción* está siendo vista como una noción primitiva, (no explicada).

Si en los puntos **H5**, **H6** el dominio D es *suficientemente simple* puede suceder que cualquier d en D así hablando, representa su propia demostración de pertenecer a D (d nos es presentado como un objeto de D). N es un ejemplo: un número natural está dado como tal, no necesitamos una demostración separada de este hecho.

Para tales dominios *simples*, la referencia a *una demostración de* $d \in D$ en **H5** y **H6** podría ser eliminada, obteniendo:

H5') Una demostración de $(\forall x)\, A(x)$ es una construcción que transforma a cualquier $d \in D$ en una demostración de $A(d)$.

H6') Una demostración de $(\exists x)\, A(x)$ está dada al exhibir una $d \in D$ y una demostración de $A(d)$.

En lo siguiente nos referiremos a las cláusulas **H1-6** como la ***interpretación BROUWER-HEYTING-KOLMOGOROV*** (**BHK**).

Incluso si las explicaciones **H1-6** dejan algunas preguntas abiertas, son suficientes para mostrar que ciertos principios lógicos deberían ser generalmente aceptados desde un punto de vista constructivo, mientras que algunos otros principios de la lógica clásica no son aceptables.

Como un ejemplo positivo tenemos la siguiente:

Proposición *1.1: Para proposiciones matemáticas arbitrarias* A *y* B *son válidas las siguientes reglas en la interpretación* ***BHK****.*

a) $A \Rightarrow (B \Rightarrow A)$
b) $A \Rightarrow \neg\neg A$
c) $\neg A \Leftrightarrow \neg\neg\neg A$
d) si $A \Rightarrow B$ *entonces* $\neg B \Rightarrow \neg A$
e) $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

f) $\neg(A \wedge B) \Leftrightarrow (A \Rightarrow \neg B) \Leftrightarrow (B \Rightarrow \neg A)$
g) $\neg(A \Rightarrow B) \Leftrightarrow \neg(\neg A \vee B)$
h) $\neg\neg(A \Rightarrow B) \Leftrightarrow (\neg\neg A \Rightarrow \neg\neg B) \Leftrightarrow (A \Rightarrow \neg\neg B)$
$\Leftrightarrow \neg\neg(\neg A \vee B)$

Y con cuantificadores:

i) $\neg(\exists x)\, A(x) \Leftrightarrow (\forall x)\, \neg A(x)$
j) $\neg\neg(\forall x)\, A(x) \Rightarrow (\forall x)\, \neg\neg A(x)$
k) $\neg\neg(\exists x)\, A(x) \Leftrightarrow \neg(\forall x)\, \neg A(x)$

Demostración:

Nota: Denotaremos d_A cuando supongamos una demostración de A y al conjunto de las demostraciones de A como $\mathcal{D}(A)$.

a) Supongamos d_A una demostración fija de A, entonces el mapeo:

$F_{d_A} : \mathcal{D}(B) \to \mathcal{D}(A)$ tal que $d_B \Rightarrow d_A$ (el mapeo que manda a cada demostración de B a la demostración fija d_A).

entonces F_{d_A} es una demostración de $B \Rightarrow A$.

Por lo tanto el mapeo definido por:

$$\Phi : \mathcal{D}(A) \to \mathcal{D}(B \Rightarrow A) \text{ tal que}$$
$$d_A \Rightarrow F_{d_A}$$

transforma una demostración de A en una demostración de $B \Rightarrow A$.

$\therefore$ Φ es una demostración de $A \Rightarrow (B \Rightarrow A)$.

b) Supongamos d_A una demostración de A cualquiera.

Si tenemos F una demostración de $\neg A$ es decir: $F : \mathcal{D}(A) \to \mathcal{D}(\perp)$
$d_A \Rightarrow F(d_A)$

entonces definimos el mapeo:

$$G : \mathcal{D}(\neg A) \to \mathcal{D}(\bot) \text{ tal que}$$
$$F \Rightarrow F(d_A)$$

G es una demostración de $\neg\neg A$. Luego definiendo:

$$\Phi : \mathcal{D}(A) \to \mathcal{D}(\neg\neg A)$$
$$d_A \Rightarrow G$$

Φ es una demostración de $A \Rightarrow \neg\neg A$.

c) ($\Rightarrow$) Es trivial aplicando (b) a la proposición $\neg A$.

($\Leftarrow$) Sea $F \in \mathcal{D}(\neg\neg\neg A)$ es decir: $F : \mathcal{D}(\neg\neg A) \to \mathcal{D}(\bot)$ tal que
$G \Rightarrow F(G)$.

Sea $d_A \in \mathcal{D}(A)$, por (b) existe un mapeo $\Phi : \mathcal{D}(A) \to \mathcal{D}(\neg\neg A)$
entonces $F \circ \Phi$ es una demostración de $\neg A$.

Sea $\Psi : \mathcal{D}(\neg\neg\neg A) \to \mathcal{D}(\neg A)$ tal que
$F \Rightarrow F \circ \Phi$

$\therefore \Psi$ demuestra $\neg\neg\neg A \Rightarrow \neg A$.

d) Sea $F \in \mathcal{D}(A \Rightarrow B)$ y sea $H \in \mathcal{D}(\neg B)$ y d_A una demostración de A
entonces el mapeo:

$$G : \mathcal{D}(\neg B) \to \mathcal{D}(\neg A) \text{ tal que}$$
$$H \Rightarrow K$$

donde $K : \mathcal{D}(A) \to \mathcal{D}(\bot)$ con
$d_A \Rightarrow (H \circ F)(d_A)$ es decir K demuestra $\neg A$

entonces G demuestra $\neg B \Rightarrow \neg A$. Y por lo tanto, el mapeo definido por

$$\Phi : \mathcal{D}(A \Rightarrow B) \to \mathcal{D}(\neg B \Rightarrow \neg A) \text{ tal que}$$
$$F \Rightarrow G$$

es una demostración de $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$

e) ($\Rightarrow$) Sea $F \in \mathcal{D}(\neg(A \vee B))$ es decir $F : \mathcal{D}(A) \cup \mathcal{D}(B) \to \mathcal{D}(\bot)$

sean $i_A : \mathcal{D}(A) \to \mathcal{D}(A) \cup \mathcal{D}(B)$
$d_A \Rightarrow d_A^*$ (d_A^* es una demotración de A vista como demostración de $A \vee B$)
$i_B : \mathcal{D}(B) \to \mathcal{D}(A) \cup \mathcal{D}(B)$
$d_B \Rightarrow d_B^*$

entonces $F \circ i_A$ $F \circ i_B$ demuestran $\neg A$ y $\neg B$ respectivamente.

$\therefore \Phi : \mathcal{D}(\neg(A \vee B)) \to \mathcal{D}(\neg A \wedge \neg B)$ tal que
$F \Rightarrow (F \circ i_A, F \circ i_B)$

demuestra lo requerido.

($\Leftarrow$) Sea $(G_1, G_2) \in \mathcal{D}(\neg A \wedge \neg B)$ es decir $G_1 \in \mathcal{D}(\neg A)$ y $G_2 \in \mathcal{D}(\neg B)$

sean $p_A : \mathcal{D}(\neg A \wedge \neg B) \to \mathcal{D}(\neg A)$
$(G_1, G_2) \Rightarrow G_1$

$p_B : \mathcal{D}(\neg A \wedge \neg B) \to \mathcal{D}(\neg B)$
$(G_1, G_2) \Rightarrow G_2$

sea $\Phi : \mathcal{D}(\neg A \wedge \neg B) \to \mathcal{D}(\neg(A \vee B))$ tal que
$(G_1, G_2) \Rightarrow \Theta$

donde $\Theta(d_A^*) = p_A(G_1, G_2)(d_A)$ y
$\Theta(d_B^*) = p_B(G_1, G_2)(d_B)$ (otra vez d_A^* y d_B^* son las demostraciones de A y B vistas como demostraciones de $A \vee B$).

$\therefore \Theta$ demuestra lo deseado.

f) Demostremos primero $\neg (A \wedge B) \Leftrightarrow (A \Rightarrow \neg B)$

($\Rightarrow$) Sea F una demostración de $\neg (A \wedge B)$ es decir:

$$F : \mathcal{B}(A \wedge B) \to \mathcal{B}(\bot) \quad \text{tal que}$$
$$(d_A, d_B) \Rightarrow F(d_A, d_B)$$

Sean d_A y d_B demostraciones de A y B respectivamente.

Definimos: $G_F \in \mathcal{B}(A \Rightarrow \neg B)$ mediante $d_A \Rightarrow H_{dA}$
donde: $H_{dA} = F(d_A, \_)$ con $H_{dA}(d_B) = F(d_A, d_B)$

$\therefore \Phi : \mathcal{B}(\neg (A \wedge B)) \to \mathcal{B}(A \Rightarrow \neg B)$
$F \quad \Rightarrow \quad G_F$ demuestra lo querido.

($\Leftarrow$) Sea $G \in \mathcal{B}(A \Rightarrow \neg B)$ entonces: $G : \mathcal{B}(A) \to \mathcal{B}(\neg B)$
$d_A \Rightarrow G(d_A)$

supongamos una demostración de $A \wedge B$ es decir (d_A, d_B)

Definimos $F_G : \mathcal{B}(A \wedge B) \to \mathcal{B}(\bot)$
$(d_A, d_B) \Rightarrow G(d_A)(d_B)$ (que demuestra falso)

entonces el mapeo $\Phi : \mathcal{B}(A \Rightarrow \neg B) \to \mathcal{B}(\neg (A \wedge B))$ tal que
$G \quad \Rightarrow \quad F_G$

demuestra lo pedido.

Ahora demostremos $(A \Rightarrow \neg B) \Leftrightarrow (B \Rightarrow \neg A)$

($\Rightarrow$) Sea $G \in \mathcal{B}(A \Rightarrow \neg B)$ como antes, y d_B una demostración de B.

Dada d_A una demostración de A definimos $F_G \in \mathcal{B}(B \Rightarrow \neg A)$ por:

$F_G : \mathcal{B}(B) \to \mathcal{B}(\neg A)$ donde: $K_{d_B} : \mathcal{B}(A) \to \mathcal{B}(\bot)$

$d_B \Rightarrow K_{d_B}$ $\qquad$ $d_A \Rightarrow G(d_A)(d_B)$

entonces $\Phi : \mathcal{B}(A \Rightarrow \neg B) \to \mathcal{B}(B \Rightarrow \neg A)$ tal que

$G \Rightarrow F_G$

demuestra lo requerido.

($\Leftarrow$) La demostración es simétrica a la anterior.

g) observación: sabemos por (e) que $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$ para cualesquiera proposiciones A y B Por lo tanto si tomamos a la primera proposición como $\neg A$ tenemos $\neg(\neg A \vee B) \Leftrightarrow (\neg\neg A \wedge \neg B)$. Entonces existen construcciones Ω_1 y Ω_2 que demuestran $\neg(\neg A \vee B) \Rightarrow (\neg\neg A \wedge \neg B)$ y el regreso respectivamente. Por lo tanto es suficiente dar construcciones para $(\neg\neg A \wedge \neg B) \Rightarrow \neg(A \Rightarrow B)$ y su regreso para demostrar (g) ya que componiendo estas con con las Ω se obtienen las construcciones deseadas.

($\Rightarrow$) Sea $K \in \mathcal{B}(\neg(A \Rightarrow B))$ $\qquad$ $K : \mathcal{B}(A \Rightarrow B) \to \mathcal{B}(\bot)$

$H \Rightarrow K(H)$

Supongamos d_B una demostración de B entonces el mapeo constante que manda cualquier demostración de A a d_B, C_{d_B} es una demostración de $A \Rightarrow B$.

Por lo tanto el mapeo $\Phi : \mathcal{B}(B) \to \mathcal{B}(\bot)$

$d_B \Rightarrow K(C_{d_B})$ demuestra $\neg B$.

Ahora supongamos $F \in \mathcal{B}(\neg A)$ es decir $F : \mathcal{B}(A) \to \mathcal{B}(\bot)$

$d_A \Rightarrow F(d_A)$

entonces $\mathcal{B}(A) = \varnothing$ y el mapeo:

$H_F : \mathcal{B}(\neg A) \to \mathcal{B}(A \Rightarrow B)$

$F \Rightarrow \varnothing$

($\varnothing$ es la función vacía, entonces $\varnothing$ demuestra $A \Rightarrow B$)
entonces H_F demuestra $\neg A \Rightarrow (A \Rightarrow B)$

Por lo tanto el mapeo $\Psi : \mathcal{B}(\neg A) \to \mathcal{B}(\bot)$

$F \Rightarrow K(\varnothing)$ demuestra $\neg\neg A$.

Entonces el mapeo $\Theta : \mathcal{B}(\neg(A \Rightarrow B)) \to \mathcal{B}(\neg\neg A \wedge \neg B)$

$K \Rightarrow (\Phi, \Psi)$

demuestra lo deseado.

($\Leftarrow$) Sea (Φ, Ψ) una demostración de $\neg\neg A \wedge \neg B$ donde:

$\Phi : \mathcal{B}(\neg A) \to \mathcal{B}(\bot)$ $\qquad$ $\Psi : \mathcal{B}(B) \to \mathcal{B}(\bot)$

$F \Rightarrow \Phi(F)$ $\qquad$ $d_B \Rightarrow \Psi(d_B)$

Supongamos $H \in \mathcal{B}(A \Rightarrow B)$ es decir $H : \mathcal{B}(A) \to \mathcal{B}(B)$

$d_A \Rightarrow H(d_A)$

Definimos $K : \mathcal{B}(A \Rightarrow B) \to \mathcal{B}(\bot)$ mediante

$H \Rightarrow \Phi(\Psi \circ H)$

$\Phi(\Psi \circ H)$ es una construcción para una contradicción porque $\Psi \circ H$ es una construcción para $\neg A$, luego entonces puedo aplicarle Φ.

$\therefore$ Definimos $\Theta : \mathcal{B}(\neg\neg A \wedge \neg B) \to \mathcal{B}(\neg(A \Rightarrow B))$

$(\Phi, \Psi) \Rightarrow K$

la cual demuestra lo requerido.

h) $\neg\neg(A \Rightarrow B) \Leftrightarrow \neg\neg(\neg A \vee B)$ se tiene aplicando (d) y (g).

Tenemos que $\neg\neg(A \Rightarrow B) \Leftrightarrow (\neg\neg A \Rightarrow \neg\neg B)$ ya que:

$\neg\neg(A \Rightarrow B) \Leftrightarrow \neg\neg(\neg A \vee B) \Leftrightarrow \neg(\neg\neg A \wedge \neg B)$

$\Leftrightarrow (\neg\neg A \Rightarrow \neg\neg B)$

Entonces componiendo los respectivos mapeos se tiene lo deseado.

Solo falta demostrar $(\neg\neg A \Rightarrow \neg\neg B) \Leftrightarrow (A \Rightarrow \neg\neg B)$

($\Leftarrow$) Esto se tiene debido a que:
$(A \Rightarrow \neg\neg B) \Rightarrow (\neg B \Rightarrow \neg A) \Rightarrow (\neg\neg A \Rightarrow \neg\neg B)$.

($\Rightarrow$) Sea $F \in \mathcal{D}(\neg\neg A \Rightarrow \neg\neg B)$ es decir $F : \mathcal{D}(\neg\neg A) \to \mathcal{D}(\neg\neg B)$
$G \Rightarrow F(G)$

Supongamos d_A una demostración de A.

por (a) existe un mapeo $\Omega : \mathcal{D}(A) \to \mathcal{D}(\neg\neg A)$
$d_A \Rightarrow \Omega(d_A)$

Definimos $H \in \mathcal{D}(A \Rightarrow \neg\neg B)$ mediante

$H : \mathcal{D}(A) \to \mathcal{D}(\neg\neg B)$
$d_A \Rightarrow (F \circ \Omega)(d_A)$

entonces H demuestra $A \Rightarrow \neg\neg B$.

$\therefore$ El mapeo $\Phi : \mathcal{D}(\neg\neg A \Rightarrow \neg\neg B) \to \mathcal{D}(A \Rightarrow \neg\neg B)$ tal que
$F \Rightarrow H$

demuestra lo deseado.

De todo lo anterior se demuestran las cuatro equivalencias.

i) ($\Rightarrow$) Sea $F \in \mathcal{D}(\neg(\exists x)A(x))$ es decir $F : \mathcal{D}((\exists x)A(x)) \to \mathcal{D}(\perp)$
$(d_y, d_{A(y)}) \Rightarrow F(d_{A(y)})$

Sean z tal que d_z se tenga y $d_{A(z)}$ una demostración de A(z).
Definimos $H : \mathcal{D}(x \in D) \to \mathcal{D}(\neg A(x))$ por
$d_z \Rightarrow K$

Donde K está definida como sigue:
$K : \mathcal{D}(A(x)) \to \mathcal{D}(\perp)$
$d_{A(z)} \Rightarrow F(d_{A(z)})$

entonces H demuestra $(\forall x)\neg A(x)$.

($\Leftarrow$) Sea $G \in \mathcal{B}((\forall x) \neg A(x))$ o sea: $G : \mathcal{B}(x \in D) \to \mathcal{B}(\neg A(x))$

$d_x \Rightarrow F : \mathcal{B} A(x) \to \mathcal{B}(\bot)$

$d_{A(x)} \Rightarrow F(d_{A(x)})$

Definimos: $H : \mathcal{B}((\exists x) A(x)) \to \mathcal{B}(\bot)$ mediante

$(d_x, d_{A(x)}) \Rightarrow F(d_{A(x)})$

H demuestra $\neg (\exists x) A(x)$

$\therefore \Phi : \mathcal{B}((\forall x) \neg A(x)) \to \mathcal{B}(\neg (\exists x) A(x))$ tal que

$G \Rightarrow H$

demuestra lo requerido.

j) Sea $F \in \mathcal{B}(\neg\neg (\forall x) A(x))$ es decir: $F : \mathcal{B}(\neg (\forall x) A(x)) \to \mathcal{B}(\bot)$

$G \Rightarrow F(G)$

Sean y (es decir (y, d_y) y junto con su demostración de pertenecer al rango de las variables).

$H \in \mathcal{B}((\forall x) A(x))$ tal que $H : \mathcal{B}(x \in D) \to \mathcal{B}(A(x))$

$x \Rightarrow A(x)$

y $\Phi \in \mathcal{B}(\neg A(y))$ tal que $\Phi : \mathcal{B}(A(y)) \to \mathcal{B}(\bot)$

Entonces H (y) demuestra A(y) y Φ (H(y)) demuestra $\bot$.

Por lo tanto el mapeo $\Omega : \mathcal{B}((\forall x) A(x)) \to \mathcal{B}(\bot)$

$H \Rightarrow \Phi(H(y))$

demuestra $\neg (\forall x) A(x)$.

Por otro lado $F(\Omega)$ demuestra $\bot$, entonces el mapeo :

$\Theta : \mathcal{B}(\neg A(y)) \to \mathcal{B}(\bot)$ tal que

$\Phi \Rightarrow F(\Omega)$ demuestra $\neg\neg A(y)$

Esto fue para cualquier $y \in D$. Es decir tengo una demostración para $(\forall x) \neg\neg A(x)$.

Y el mapeo definido como : $\Psi : \mathcal{B}(\neg\neg(\forall x)\,A(x)) \to \mathcal{B}((\forall x)\,\neg\neg\,A(x))$

$F \quad \Rightarrow \quad \Theta$

demuestra la implicación.

k) ($\Rightarrow$) Sea $F \in \mathcal{B}(\neg\neg(\exists x)\,A(x))$ es decir: $F : \mathcal{B}(\neg(\exists x)\,A(x)) \to \mathcal{B}(\bot)$

$G \quad \Rightarrow F(G)$

por (i) tenemos que existe una construcción, llamemosle Φ, tal que manda demostraciones de $(\forall x)\,\neg\,A(x)$ a demostraciones de $\neg\,(\exists x)\,A(x)$. Entonces definimos el mapeo:

$\Psi : \mathcal{B}(\neg\neg(\exists x)\,A(x)) \to \mathcal{B}(\neg(\forall x)\,\neg\,A(x))$ tal que

$F \quad \Rightarrow \quad F^*$ donde

$F^* : \mathcal{B}((\forall x)\,\neg\,A(x)) \to \mathcal{B}(\bot)$

$H \quad \Rightarrow F \circ \Phi(H)$

Entonces Ψ demuestra la implicación.

($\Leftarrow$) Hacemos el mismo procedimiento ahora usando la otra implicación de (i).

■

Otra consecuencia es que $(\bot \Rightarrow A)$ es generalmente demostrable: ya que no hay demostración de $\bot$, el mapeo vacío (o cualquier otro mapeo) podría contar como una demostración de $(\bot \Rightarrow A)$, debido a que tiene que ser aplicado a un dominio vacío. Tal principio ha sido a veces rechazado como *no constructivo*, nosotros lo veremos como una suposición extra fijando el significado y uso de $\bot$ y $\Rightarrow$.

Como ejemplo negativo consideremos el principio del *tercer excluído* (**PTE**)

$A \vee \neg A$

el cual es válido clásicamente. Constructivamente, aceptar **PTE** como un principio general significa que tenemos un método *universal* para obtenerlo, para cualquier proposición A , una demostración de A o una de $\neg$ A, es decir un método para obtener una contradicción a partir de una demostración hipotética de A.

Pero si tal método fuera obtenible, también podríamos decidir de una oración A su valor de verdad a partir de lo que no se ha decidido todavía, el cual no es el caso.

Por lo tanto, no podemos aceptar **PTE** como un principio universalmente válido en la interpretación **BHK**.

Nos dedicaremos a una demostración más formal de esto en el capítulo 3, por ahora veremos que tampoco lo podemos rechazar.

Hasta ahora no se ha mostrado como deducir una contradicción a partir de suponer que **PTE** es válido. Sólo decimos que no es aceptado como un principio válido. De hecho no podemos rechazar cualquier instancia individual de **PTE**, es decir que no podemos encontrar una proposición matemática A tal que $\neg (A \vee \neg A)$. Esto es imposible, ya que $\neg\neg (A \vee \neg A)$ se tiene universalmente, es una ley de la lógica intuicionista.

Esto puede ser visto en las bases de la interpretación **BHK** como sigue:

Proposición 1.2: *$\neg\neg (A \vee \neg A)$ es válida en la interpretación **BHK**.*

Demostración: Supongamos $F \in \mathcal{B}(\neg (A \vee \neg A))$ entonces:

$$F : \mathcal{B}(A \vee \neg A) \to \mathcal{B}(\bot) \quad \text{tal que}$$
$$G \quad \Rightarrow \quad F(G)$$

entonces existen $i_A : \mathcal{B}(A) \to \mathcal{B}(A \vee \neg A)$
$$d_A \Rightarrow \quad d_A^*$$

$$i_{\neg A} : \mathcal{B}(\neg A) \to \mathcal{B}(A \vee \neg A)$$
$$H \quad \Rightarrow \quad H^*$$

Definimos: $K_1 : \mathcal{B}(A) \to \mathcal{B}(\bot)$ $\qquad$ $K_2 : \mathcal{B}(\neg A) \to \mathcal{B}(\bot)$
$d_A \Rightarrow F(d_A^*)$ $\qquad$ $H \Rightarrow F(H^*)$

Entonces $K_1 \in \mathcal{D}(\neg A)$ y $K_2 \in \mathcal{D}(\neg\neg A)$
(observemos que $K_1 = F \circ i_A$, $K_2 = F \circ i_{\neg A}$)

$\therefore$ $K_2(K_1)$ demuestra $\bot$. y el mapeo:

$$\Phi : \mathcal{D}(\neg(A \vee \neg A)) \to \mathcal{D}(\bot)$$
$$F \quad \Rightarrow K_2(K_1)$$

es una demostración para $\neg\neg(A \vee \neg A)$

■

Por otro lado junto con **PTE**, los siguientes son ejemplos de principios que son válidos clásicamente pero no lo son en la interpretación **BHK**.

(a) $\neg\neg A \Rightarrow A$
(b) $\neg A \vee \neg\neg A$
(c) $(A \Rightarrow B) \vee (B \Rightarrow A)$
(d) $\neg(\neg A \wedge \neg B) \Rightarrow A \vee B$
(e) $\neg(\neg A \vee \neg B) \Rightarrow A \wedge B$
(f) $(\forall x)\neg\neg A(x) \Rightarrow \neg\neg(\forall x) A(x)$
(g) $\neg\neg(\exists x) A(x) \Rightarrow (\exists x)\neg\neg A(x)$
(h) $(A \Rightarrow (\exists x) B(x)) \Rightarrow ((\exists x)(A \Rightarrow B(x)))$ donde x no está en las variables libres de A.

En este trabajo no desarrollaremos métodos para demostrar su no validez. Solamente demostraremos en el capítulo 3 la no validez de **PTE** y (a).

En el formalismo usual se denota **IQC** a la lógica de predicados intuicionista, en ella los términos se supone están siempre definidos, es decir que ellos siempre denotan algo, como en el formalismo usual de la lógica de predicados clásica.

Como siempre en las matemáticas intuicionistas posiblemente términos no definidos o expresiones que están bien definidas solo para ciertos valores de los parámetros, surgen naturalmente (por ejemplo x^{-1} para los reales); mientras el sentido clásico los elimina, para garantizar que tales expresiones siempre denoten algo con significado de suposiciones arbitrarias, aquí no son aceptados.

Por lo tanto, algo de cuidado se necesita al manejar tales expresiones; si usamos Et para *t está bien definido*, tenemos en particular:

$$(1)\quad (\forall x)\, A(x) \wedge Et \Rightarrow A(t)$$
$$A(x) \wedge Et \Rightarrow (\exists x)\, A(x)$$

Reemplazar los principios usuales de las proposiciones anteriores (sin Et) por las más cuidadosas expresadas en (1) corresponde al nivel formal de la E^+-lógica (no la desarrollaremos en este trabajo).

2. La no decidibilidad de la igualdad para los números reales.

Sea A(n) un predicado de los números naturales tal que A(n) es decidible, pero la validez de (∀n) A(n) es desconocida, es decir, (∀n) [A(n) ∨ ¬ A(n)] .

Como ejemplo de tal A podemos citar la siguiente, llamada " *Ultimo teorema de Fermat* " :

Tomando $A(n) := \forall m_1,m_2,m_3,k\,(m1 + m2 + m3 + k \leq n \Rightarrow (m_1 + 1)^{k+3} + (m_2 + 1)^{k+3} \neq (m_3 + 1)^{k+3})$, donde m_1, m_2, m_3, k, n corren sobre los números naturales.

Definición 1.3 : *a) Una <u>sucesión fundamental</u> es una sucesión* $\langle r_n^A \rangle_n$ *de racionales, junto con una sucesión* β, *su Cauchy-módulo, tal que*

$$\forall k,m\, m'\, (\, | r_{\beta(k)+m} - r_{\beta(k)+m'} | < 2^{-k}).$$

b) Dos sucesiones fundamentales $\langle r_n \rangle_n$, $\langle s_n \rangle_n$ *se dice que <u>coinciden</u> o son <u>equivalentes</u>* ($\approx$) *si:*

$$\forall k\, \exists n\, \forall m\, (\, | r_{n+m} - s_{n+m} | < 2^{-k})$$

Definición 1.4: *Para* $r \in Q$ *definimos* r^* *como la sucesión fundamental* $< r_n >_n$ *con* $r_n = r \ \forall n \in N$.

Supongamos que definimos un número real x^A por medio de una sucesión fundamental de racionales $< r_n{}^A >_n$ definida como sigue:

$$r_n{}^A := \begin{cases} 2^{-n} & \text{si } \forall k \leq n \ A(k) \text{ se tiene.} \\ 2^{-k} & \text{si } \neg A(k) \wedge k \leq n \wedge \forall k' < k \ A(k') \text{ se tiene.} \end{cases}$$

La sucesión así definida es una sucesión fundamental ya que $\forall n$ si $m \leq n$ se tiene $(\mid r_n{}^A - r_m{}^A \mid < 2^{-m})$ claramente y donde $\alpha(n) = n$ es su *Cauchy-módulo.* También tenemos que:

Proposición 1.5: $x^A = 0$ *si y solo si* $(\forall n) A(n)$.

Demostración: La implicación de derecha a izquierda es sencilla ya que:

$(\forall n) A(n) \Rightarrow r_n{}^A = 2^{-n}$ $(\forall n) \in N$ y esta sucesión es equivalente a $< s_n >_n$ con $s_n = 0$ $(\forall n)$ debido a que:

$\forall k \exists n \forall m \ (\mid r_{n+m}{}^A - 0 \mid < 2^{-k})$ es cierta si $n > k$.

Para demostrar la ida, supongamos $x^A = 0$ entonces se tiene que $< r_n{}^A >_n \approx < 0 >_n$

$$\therefore \ \forall k \exists s \forall m \ (\mid r_{s+m}{}^A \mid < 2^{-k})$$

sea $k = n$ entonces $\exists s \forall m \mid r_{s+m}{}^A \mid < 2^{-n}$
y si tomamos $m = 0$ tenemos:

$$\exists s \mid r_s{}^A \mid < 2^{-n}$$

Pero $r_s{}^A := 2^{-s}$ ó 2^{-t} con $t \leq s$ y $r_s{}^A < 2^{-n}$

entonces: si pasa el primero se tiene $s = n + u$ $(2^{-s} < 2^{-n})$
si pasa el segundo se tiene $t = n + u'$
y $n < s$ ó t $(2^{-t} < 2^{-n})$ $(u, u' \in N)$

$\therefore\ r_{n+1}{}^{A} < 2^{-n}$ $\forall n \in N$.

Esto nos dice que A(n) se tiene para toda n.

■

De la anterior proposición se sigue que $(x_{\dot{A}} = 0 \vee x^{A} \neq 0)$ es equivalente a la proposición $(\forall n)$ A(n) $\vee \neg (\forall n)$ A(n). Por lo tanto tenemos un ejemplo en el cual no es posible decidir sobre la igualdad de dos números reales, por lo tanto se dice que ***la igualdad en los números reales no es decidible.*** (ver capítulo 4).

CAPITULO 2.

EL CALCULO DE PREDICADOS INTUICIONISTA.

DEDUCCION NATURAL.

Para el desarrollo de la matemática constructivista como tal, no necesitamos un sistema formal de lógica. Sin embargo, es conveniente tener un conjunto de reglas lógicas disponibles. Por ende no necesitamos regresar a la interpretación **BHK** cada vez que queramos justificar el uso de un principio lógico en nuestro argumento.

Hemos escogido deducción natural como nuestro punto de partida porque concuerda con razonamientos informales. Además, sus reglas son motivadas por la interpretación **BHK** de una manera directa.

El lenguaje de la Lógica de predicados. El lenguaje Ω de la lógica de predicados está basada en una infinidad (numerable) de variables $v_0, v_1, v_2, \ldots, v_n \ldots$ (como metavariables para variables que usaremos x, y, z), símbolos de relaciones n-arias $R_0^n, R_1^n, \ldots$ (n corriendo sobre N; con metavariables R, $R^1, \ldots$), y símbolos de funciones n-arias $f_0^n, f_1^n, \ldots$ (con metavariables f, g). Los símbolos de funciones sin lugares f_i^0 son llamadas constantes (individuales) y se usan las metavariables c, d.

Este lenguaje puede ser facilmente generalizado en dos direcciones:

(i) Desechando la restricción de cantidad numerable de símbolos de cada tipo y

(ii) Extendiendo a un lenguaje de *multi-clases*, con una colección de clases I, y variables v_0^i, v_1^i, ... para cada clase i de I. Proveer símbolos de relaciones n-arias $R_k^{i_0,\dots,i_{n-1}}$, con k en **N** para cada sucesión $i_0, i_1, \dots,$ i_{n-1} de clases en I. Y proveer símbolos de funciones $f_k^{i_0,\dots,i_{n-1}}$, con k en **N** para cada sucesión $i_0, i_1, \dots, i_{n-1}$ de clases en I.

El lenguaje de la llamada *lógica de orden superior* es tratada como una instancia especial de un lenguaje de *multi-clases*.

Los términos y fórmulas en la base de $\wedge, \vee, \forall, \exists, \bot, \Rightarrow$ son primitivas, son definidas como siempre, t y s serán usadas como metavariables para términos. P, Q, R, S como metavariables para fórmulas y A, B denotarán fórmulas atómicas.

El lenguaje de la lógica proposicional Ω_0 tiene solo símbolos de relación de 0-lugar; estas son llamadas variables proposicionales (metavariables A,B).

Ejemplos de reglas de deducciones naturales. Supongamos que tenemos establecido Q, repetidamente apelando a la suposición P. Esto significa que hemos mostrado como construir una deducción de Q a partir de una deducción hipotética de P ; por lo tanto en la interpretación **BHK** ésto significa que hemos establecido la implicación $P \Rightarrow Q$. En esta conclusión P ya no es una suposición (P ha sido *cancelada, descargada* o *eliminad* como una suposición), esquematicamente podemos ver esto como sigue:

$$\dfrac{\begin{array}{c}\not{P}\\ \vdots \\ Q\end{array}}{P \Rightarrow Q}$$

El que P este cruzada significa que ha sido eliminada como una suposición en la conclusión. El tipo de inferencia descrito es llamado *introducción de implicación* ($\Rightarrow$ I) debido a que en la conclusión final un signo de implicación ha sido introducido.

Existe también una regla de eliminación de la implicación ($\Rightarrow$ E); si hemos mostrado $P \Rightarrow Q$ y P, podemos demostrar Q, ya que una demostración de $P \Rightarrow Q$ debe proveer una construcción para transformar una demostración de P en una de Q. Esquematicamente:

$$\dfrac{\begin{array}{cc} \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ P \Rightarrow Q & P \end{array}}{Q}$$

Como ejemplo de una deducción por medio de ($\Rightarrow$ I) y ($\Rightarrow$ E) mostraremos como deducir $P \Rightarrow R$ a partir de las proposiciones $P \Rightarrow Q$ y $Q \Rightarrow R$.

$$\dfrac{\dfrac{Q \Rightarrow R \qquad \dfrac{P \Rightarrow Q \qquad P}{Q}\ (\Rightarrow E)}{R}\ (\Rightarrow I)\ (\text{P cancelada})}{P \Rightarrow R}$$

En cada linea horizontal hemos indicado la regla que ha sido aplicada.

Para conjunción podemos justificar una regla de introducción ($\wedge$ I) y dos reglas de eliminación (izquierda y derecha) ($\wedge E_I$) ($\wedge E_d$):

$$(\wedge I)\ \dfrac{\begin{array}{cc} \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ P & Q \end{array}}{P \wedge Q} \qquad (\wedge EI)\ \dfrac{\begin{array}{c} \cdot \\ \cdot \\ \cdot \\ P \wedge Q \end{array}}{P} \qquad (\wedge Ed)\ \dfrac{\begin{array}{c} \cdot \\ \cdot \\ \cdot \\ P \wedge Q \end{array}}{Q}$$

Un ejemplo de una deducción basada en estas reglas es:

$$\dfrac{\dfrac{\dfrac{P \wedge Q}{Q}\,(\wedge Ed) \qquad \dfrac{P \wedge Q}{P}\,(\wedge Ei)}{Q \wedge P}\,(\wedge I)}{P \wedge Q \Rightarrow Q \wedge P}\,(\Rightarrow I)\ (P \wedge Q \text{ es cancelada})$$

Finalmente consideremos una regla de cuantificadores, llámese ($\forall$ I) (introducción de para todo).

$$\dfrac{\begin{array}{c}\vdots \\ P(y)\end{array}}{\forall x\ P(x)}$$

Esto es, si hemos deducido P(y) para una y arbitraria nosotros podemos de hecho inferir $\forall x$ P(x) ya que nuestra deducción de P(y) sirve como un esquema el cual puede ser aplicado a cualquier objeto particular en el rango de la variable y, así que tenemos la construcción requerida por la interpretación **BHK** para una demostración de $\forall x$ P(x). En una aplicación de esta regla, la demostración de P(y) no debería depender en otras suposiciones que contengan a y, porque entonces no podríamos ver a y como completamente arbitraria.

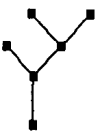
El que sin tal restricción en efecto lleguemos a conclusiones falsas se vuelve claro por el siguiente ejemplo de una *"deducción"* en la cual la condición es violada:

$$\dfrac{\dfrac{\begin{array}{c}P(x)\\ \vdots \end{array}}{\forall y\ P(y)}}{P(x) \Rightarrow \forall y\ P(y)}\,(\Rightarrow I)\ (P(x) \text{ cancelada})$$

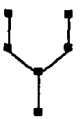
Las deducciones en nuestros ejemplos anteriores pueden ser vistos como árboles etiquetados, la etiqueta atada a un nodo que consiste de una proposición, junto con el nombre de la regla que ha sido aplicada para obtener la proposición.

Por razones de comprensión hemos puesto el nombre de la regla seguido de las líneas horizontales en vez de seguido de la fórmula. Los árboles en nuestros ejemplos de deducciones son:

Para $P \Rightarrow R$ de $P \Rightarrow Q$ y $Q \Rightarrow R$



Y para $P \wedge Q \Rightarrow Q \wedge P$



Definiciones inductivas de deducciones lógicas. Ahora daremos una definición formal de deducción, suposición abierta, y suposiciones eliminadas. La definición tomará la forma de una definición simultanea por recursión de la longitud de los árboles de deducción.

Usaremos D para deducciones arbitrarias. Escribimos $\begin{matrix} D \\ Q \end{matrix}$ para indicar que Q es una conclusión de D (Q es parte de D). Usamos [P] por un (posiblemente vacío) conjunto de ocurrencias de la fórmula P en una deducción, por lo tanto $\begin{matrix} [P] \\ D \\ Q \end{matrix}$ es una deducción D con conclusión Q conteniendo un conjunto [P] de ocurrencias de P (los elementos del cual son usados como suposiciones en D) como regla suponemos que [P] contiene todas las ocurrencias supuestas de la forma P en D.

Definición *2.1 : (De deducción, suposiciones abiertas y canceladas de una deducción).*

Base: El árbol de nodo simple con etiqueta P es una deducción a partir de la suposición abierta P ; no hay suposiciones canceladas.

Paso Inductivo : Ahora sean D_1, D_2, D_3 deducciones. Una deducción D puede ser construída acorde a una de las siguientes reglas. Algunas de estas reglas estan sujetas a restricciones especificadas después.

Para $\perp$ tenemos la regla del absurdo intuicionista:

$$\dfrac{\dfrac{D_1}{\perp}\ \perp}{P}$$

Para los demás operadores lógicos tenemos reglas de introducción y eliminación:

Reglas de Introducción.

$$\dfrac{\begin{matrix}D_1 & D_2\\ P & Q\end{matrix}}{P \wedge Q}\ \wedge I$$

$$\vee Id\ \dfrac{\begin{matrix}D_1\\ P\end{matrix}}{P \vee Q} \qquad \vee II\ \dfrac{\begin{matrix}D_2\\ Q\end{matrix}}{P \vee Q}$$

$$\dfrac{\begin{matrix}[P]\\ D_1\\ Q\end{matrix}}{P \Rightarrow Q}\ \Rightarrow I$$

$$\dfrac{\begin{matrix}D_1\\ P\end{matrix}}{\forall y\, P[x/y]}\ \forall I$$

Reglas de Eliminación.

$$\wedge Ed\ \dfrac{\begin{matrix}D_1\\ P \wedge Q\end{matrix}}{P} \qquad \dfrac{\begin{matrix}D_2\\ P \wedge Q\end{matrix}}{Q}\ \wedge EI$$

$$\vee E\ \dfrac{\begin{matrix}D_1 & [P]\ D_2 & [Q]\ D_3\\ P \vee Q & R & R\end{matrix}}{R}$$

$$\dfrac{\begin{matrix}D_1 & D_2\\ P \Rightarrow Q & P\end{matrix}}{Q}\ \Rightarrow E$$

$$\dfrac{\begin{matrix}D_1\\ \forall x\ P\end{matrix}}{P[x/t]}\ \forall E$$

$$\frac{\begin{array}{c} D_1 \\ P[x/t] \end{array}}{\exists x\ P}\ \exists I \qquad\qquad \frac{\begin{array}{cc} & [P] \\ D_1 & D_2 \\ \exists y\ P[x/y] & R \end{array}}{R}\ \exists E$$

Las suposiciones abiertas y canceladas son dadas por las siguientes estipulaciones:
(i) En ($\Rightarrow I$) todas las suposiciones abiertas de la forma P en D_1 indicadas por el conjunto [P] son canceladas; en una aplicación de ($\vee E$) los conjuntos [P] en D_2 y [Q] en D_3 son cancelados. En ($\exists E$) el conjunto [P] en D_2 es cancelado.
(ii) Si D_1 es una deducción de una premisa de la aplicación de la última regla en D_1 entonces las suposiciones abiertas en D_1 siguen siendo abiertas en D excepto las especificadas por (i). Por lo tanto las suposiciones que no son canceladas son abiertas.

Las reglas para los cuantificadores están sujetas a las siguientes restricciónes:
(iii) En ($\forall E$) y ($\exists I$) t debe ser libre para x en P.
(iv) En ($\forall I$), D_1 no debe contener suposiciones abiertas teniendo a x libre, y $y \equiv x$ ó y no es libre en P. En ($\exists E$) D_2 no debe contener suposiciones abiertas teniendo a x libre, excepto el conjunto [P]; x no libre en R, $y \equiv x$ ó y no libre en P.

Si P está entre las suposiciones abiertas de una deducción D con conclusión Q. La conclusión Q en D se dice que depende de P en D. A partir de ahora veremos la " suposición de D " y " suposición abierta de D " como sinónimos.

Nota:

(i) Pondremos un número a las suposiciones en los nodos superiores las cuales van a ser canceladas después y repetiremos el número en el nodo en el que se cancela. Las suposiciones que se cancelarán simultaneamente serán numeradas igual.

(ii) Las reglas ($\forall$ I) y ($\exists$ E) pueden ser simplificadas a:

$$\forall I\ \frac{\begin{array}{c}D_1\\ P\end{array}}{\forall x\ P} \qquad\qquad \frac{\begin{array}{cc}D_1 & [P]\\ \exists x P & D_2\\ & R\end{array}}{R}\ \exists E$$

Donde en ($\forall$ I), P no depende de suposiciones abiertas en D_1 conteniendo a x libre. Y en ($\exists$ E) R no contiene a x libre y la deducción D_2 de R no contiene suposiciones abiertas teniendo a x excepto [P]. La forma más general de las reglas dadas antes pueden ser obtenidas de estos casos especiales de la siguiente forma:

$$\frac{\begin{array}{c}D_1\\ P\end{array}}{\begin{array}{c}\forall x\ P\\ P[x/t]\\ \forall y\ P[y/x]\end{array}} \qquad\qquad \frac{\begin{array}{ccc}D_1 & (1)\ P[x/y] & [P]\ (2)\\ \exists y\ P[x/y] & \exists x\ P & D_2\\ & R\ (1) & R\end{array}}{R\ (2)}$$

Encontramos más conveniente, sin embargo, combinar ($\forall$ I), ($\exists$ E) con la posibilidad de renombrar variables acotadas, debido a que queremos fórmulas que difieren solo en los nombres de sus variables acotadas como equivalentes.

EJEMPLOS.

(a) Argumentamos en el capítulo 1 que $\neg\neg(P \vee \neg P)$ debería ser válido para nuestro entendimiento de $\neg$, $\vee$; e aquí una deducción formal de ello.

$$\cfrac{\cfrac{\cfrac{\cfrac{}{(2)\ \neg(P\vee\neg P)}\qquad \cfrac{(1)\ P}{P\vee\neg P}\ \vee I}{\bot}\Rightarrow E}{(1)\ \neg P}\ \Rightarrow I \qquad \cfrac{\cfrac{\cfrac{}{(2)\ \neg(P\vee\neg P)}\qquad \cfrac{(1)\ \neg P}{P\vee\neg P}\ \vee I}{\bot}\Rightarrow E}{\neg\neg(P\vee\neg P)}\ \Rightarrow I$$

Recordando que $\neg P \equiv P \Rightarrow \bot$.

(b) Y con cuantificadores tenemos el siguiente (ver inciso j de la proposición 1.1) ejemplo.

$$\dfrac{\dfrac{(3)\ \neg\neg\forall x\,P(x) \qquad \dfrac{\dfrac{\dfrac{(2)\ \neg P(y) \qquad \dfrac{(1)\ \forall x\,P(x)}{P(y)}\ \Rightarrow E}{\bot}\ \Rightarrow I}{(1)\ \neg\forall x\,P(x)}\ \Rightarrow E}{\bot}\ \Rightarrow I}{\dfrac{(2)\ \neg\neg P(y)}{\forall x\,\neg\neg P(x)}\ \forall I}\ \Rightarrow I$$

$$(3)\ \neg\neg\forall x\,P(x) \Rightarrow \forall x\,\neg\neg P(x)$$

Al confrontar con el problema de construír una deducción de una proposición dada. La mejor táctica es comenzar por el final, y asumir, si es posible, que el paso final fue una instancia de una regla de introducción. Esto es repetido tantas veces como sea posible. Por lo tanto, si se quiere dar una deducción para $\neg\neg\ \forall x\ P(x) \Rightarrow \forall x\ \neg\neg\ P(x)$, reducimos el problema a construír una deducción de una contradicción ($\bot$) de suponer $\neg\neg\ \forall x\ P(x)$, $\neg\ P(y)$.
Ahora intentamos aplicar reglas de eliminación a las supociciones. Para aplicar una regla de eliminación a $\neg\neg\ \forall x\ P(x)$, necesitamos $\neg\ \forall x\ P(x)$, así que intentamos encontrar una deducción:

$$\begin{array}{c}[\,\neg\neg\ \forall x\,P(x)\,]\ [\,\neg\ \forall x\,P(x)\,]\\ D\\ \neg\ \forall x\,P(x)\ ;\end{array}$$

Otra vez, suponiendo que la conclusión es obtenida de ($\Rightarrow$ I), buscamos una deducción D' tal que :

$$\dfrac{\begin{array}{c}[\,\neg\neg\ \forall x\,P(x)\,]\ [\,\neg\ P(y)\,]\ [\forall x\,P(x)\,]\\ D'\\ \bot\end{array}}{\neg\ \forall x\,P(x)}$$

y D' es facilmente construída como:

$$\dfrac{\dfrac{\forall x\,P(x)}{P(y)}}{\bot}$$

(c) $\dfrac{\dfrac{P \quad \neg P}{\bot}\,(2)}{\dfrac{\neg\neg\neg P \quad \neg\neg P}{\bot}\,(2)}\,(3)$ y $\dfrac{\dfrac{\neg Q \quad Q}{\bot}\,(2)}{\neg\neg Q}\,(1)$

$\dfrac{}{\neg\neg\neg P \Rightarrow \neg\neg P}\,(1)$ $\qquad$ $Q \Rightarrow \neg\neg Q$ (2)

Si en la segunda deducción tomamos $\neg P$ por Q vemos que :

$$\neg P \Leftrightarrow \neg\neg\neg P$$

(d) La táctica descrita antes no siempre es tan directa, consideremos por ejemplo:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P \Rightarrow \exists x\, Q(x)}\,(4) \quad P\,(2)}{\exists x\, Q(x)} \quad \dfrac{\dfrac{Q(y)\,(3) \quad P \Rightarrow Q(y)}{\exists x\,(P \Rightarrow Q(y))}}{\exists x\,(P \Rightarrow Q(y))\,(3)}}{\exists x\,(P \Rightarrow Q(y))\,(1)}}{(4)\,(P \Rightarrow \exists x\, Q(x)) \Rightarrow \exists x\,(P \Rightarrow Q(y))}}{(5)\; P \vee \neg P \Rightarrow [\,(P \Rightarrow \exists x\, Q(x)) \Rightarrow \exists x\,(P \Rightarrow Q(y))\,]}\,(5) \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\bot}}{Q(y)}}{P \Rightarrow Q(y)}\,(2)}{\exists x\,(P \Rightarrow Q(y))}}{\exists x\,(P \Rightarrow Q(y))}}{P \vee \neg P}\,(5) \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg P \quad P}\,(1)}{\bot}}{Q(y)}}{P \Rightarrow Q(y)}\,(2)}{\exists x\,(P \Rightarrow Q(y))}}{\exists x\,(P \Rightarrow Q(y))}$$

Un intento directo de construir a partir de lo de abajo nos sugiere obtener: " $\exists x\,(P \Rightarrow Q(x))$ " a partir de " $P \Rightarrow Q(y)$ " pero entonces estaríamos atrapados. Así que debemos contar con la posibilidad, mientras regresamos en la conclusión, que aplicaciones de ($\vee$ E) ó ($\exists$ E) intervienen cuando subimos.

(e) $\dfrac{\dfrac{\dfrac{\dfrac{P \quad P \Rightarrow Q\,(1)}{Q} \quad \neg Q\,(3)}{\bot}}{\neg P\,(2)}}{\neg Q \Rightarrow \neg P\,(3),}$

$(P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)\,(1)$

(f) Demostremos que $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(P\vee Q)}(1) \quad \dfrac{\dfrac{P}{P\vee Q}(2)}{\bot}}{\neg P}(2) \quad \dfrac{\dfrac{\dfrac{Q}{P\vee Q}(3)}{\bot}}{\neg Q}(3)}{\neg P \wedge \neg Q}}{\neg(P\vee Q)\Rightarrow(\neg P\wedge\neg Q)}(1)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg P\wedge\neg Q}(1) \quad \dfrac{P\vee Q}{}(2)}{\neg P} \quad \dfrac{\dfrac{\dfrac{}{\neg P\wedge\neg Q}(1)}{\neg Q}}{Q}}{\bot}}{\neg(P\vee Q)}(2) \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\neg P\wedge\neg Q}(1)}{\neg Q}}{P} \quad \dfrac{\dfrac{}{\neg P\wedge\neg Q}(1)}{\neg P}}{\bot}}{\neg(P\vee Q)}(2)$$

$$(\neg P\wedge\neg Q)\Rightarrow\neg(P\vee Q)$$

(g) Veamos ahora que $\neg(P \Rightarrow Q) \Leftrightarrow (\neg\neg P \wedge \neg Q)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(P\Rightarrow Q)}(1) \quad \dfrac{\dfrac{Q}{P\Rightarrow Q}(2)}{\bot}}{\neg Q}(2)}{\neg(P\Rightarrow Q)\Rightarrow\neg Q}(1) \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg P}(2) \quad P}{\bot}}{Q}}{\neg(P\Rightarrow Q)}(1) \quad \dfrac{}{P\Rightarrow Q}(3)}{\bot}}{\neg\neg P}(2)}{\neg(P\Rightarrow Q)\Rightarrow\neg\neg P}(1)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\neg P\wedge\neg Q}(1) \quad \dfrac{P\Rightarrow Q}{}(2) \quad \dfrac{}{P}(3)}{\neg Q}}{Q} \quad \dfrac{}{\neg P}}{\bot}}{\neg\neg P}(3)}{\bot}}{\neg(P\Rightarrow Q)}(2)}{(\neg\neg P\wedge\neg Q)\Rightarrow\neg(P\Rightarrow Q)}$$

(h) Y que $\neg(P \wedge Q) \Leftrightarrow (P \Rightarrow \neg Q)$

$(\Rightarrow)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(P\wedge Q)}\,(1) \qquad \dfrac{\dfrac{}{P}\,(2)\quad \dfrac{}{Q}\,(3)}{P\wedge Q}}{\bot}}{\neg Q\,(3)}}{P\Rightarrow\neg Q\,(2)}}{\neg(P\wedge Q)\Rightarrow(P\Rightarrow\neg Q)\,(1)}$$

$(\Leftarrow)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P\Rightarrow\neg Q}\,(1) \qquad \dfrac{}{P\wedge Q}\,(2)}{\neg Q}}{\bot}}{\neg(P\wedge Q)\,(2)}}{(P\Rightarrow\neg Q)\Rightarrow\neg(P\wedge Q)\,(1)}$$

(i) Aplicando los incisos (f), (g) y (h) obtenemos el siguiente resultado:

$$\neg\neg(P \Rightarrow Q) \Leftrightarrow (\neg\neg P \Rightarrow \neg\neg Q)$$

(j) Demostremos ahora que $\neg\neg(P \Rightarrow Q) \Rightarrow (P \Rightarrow \neg\neg Q)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P}\,(1)\quad \dfrac{}{\neg P}\,(2)}{\bot}}{\neg\neg P\,(2)} \qquad \dfrac{}{\neg\neg(P\Rightarrow Q)}\,(3)}{\neg\neg Q}\,(*)}{P\Rightarrow\neg\neg Q\,(1)}}{\neg\neg(P\Rightarrow Q)\Rightarrow(P\Rightarrow\neg\neg Q)\,(3)}$$

(*) Aquí se aplicó implícitamente la deducción que corresponde.

(k) Demostremos que $(P \Rightarrow (Q \Rightarrow R)) \Leftrightarrow ((P \Rightarrow Q) \Rightarrow (P \Rightarrow R))$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(P \Rightarrow (Q \Rightarrow R))\ (3)\ P \qquad (2)\ P \Rightarrow Q \qquad P\ (3)}{Q \Rightarrow R \qquad\qquad Q}}{R}\,,}{P \Rightarrow R}\,(3)}{(P \Rightarrow Q) \Rightarrow (P \Rightarrow R)}\ (2)}{(P \Rightarrow (Q \Rightarrow R)) \Rightarrow ((P \Rightarrow Q) \Rightarrow (P \Rightarrow R))}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{(3)\ Q}{(P \Rightarrow Q) \Rightarrow (P \Rightarrow R) \qquad P \Rightarrow Q}\,,}{P \Rightarrow R \qquad\qquad (2)\ P}}{R}\,,}{Q \Rightarrow R\ (3)}}{P \Rightarrow (Q \Rightarrow R)\ (2)}\,,$$

$$((P \Rightarrow Q) \Rightarrow (P \Rightarrow R)) \Rightarrow ((P \Rightarrow (Q \Rightarrow R))\ (1)$$

(l) Ahora que $(P \wedge Q \Rightarrow R) \Leftrightarrow (P \Rightarrow (Q \Rightarrow R))$

$$\dfrac{\dfrac{\dfrac{\dfrac{(2)\ P \qquad (3)\ Q}{(1)\ P \wedge Q \Rightarrow R \qquad\qquad P \wedge Q}}{R}\,,}{Q \Rightarrow R\ (3)}}{P \Rightarrow (Q \Rightarrow R)\ (2)}\,,$$

$$(P \wedge Q \Rightarrow R) \Rightarrow (P \Rightarrow (Q \Rightarrow R))\ \ (1)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{(2)\ P \wedge Q}{(1)\ P \Rightarrow (Q \Rightarrow R) \qquad\qquad P \qquad (2)\ P \wedge Q}}{Q \Rightarrow R \qquad\qquad\qquad Q}}{R}\,,}{P \wedge Q \Rightarrow R\ (2)}\,,}{(P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \wedge Q \Rightarrow R)\ \ (1)}$$

Es decir que el *teorema de la deducción* vale en esta interpretación.

■

En la práctica uno utiliza muchos tipos de cortes al dar deducciones. Cualquier ley lógica puede ser usada como una suposición que no es cancelada pero no cuenta como una premisa para las conclusiones; similarmente, podemos usar deducciones a partir de suposiciones como reglas adicionales. Por ejemplo la deducción de $P \Rightarrow Q$, $Q \Rightarrow R$ nos permite introducir la regla de deducción:

$$R\ \frac{\begin{matrix} D_1 & D_2 \\ P \Rightarrow Q & Q \Rightarrow R \end{matrix}}{P \Rightarrow R}.$$

O un esquema de sustitución para proposiciones equivalentes:

$$R'\ \frac{\begin{matrix} D_1 & D_2 \\ F(R) & R \Leftrightarrow S \end{matrix}}{F(S)}.$$

Como un ejemplo de una deducción que involucra estas dos reglas tenemos:

$$\dfrac{\dfrac{\begin{matrix} D_1 & D_2 \\ (P \Rightarrow \neg\neg Q) \Rightarrow (\neg\neg\neg Q \Rightarrow \neg P) & (\neg\neg\neg Q \Rightarrow \neg P) \Rightarrow (\neg\neg P \Rightarrow \neg\neg\neg\neg Q) \end{matrix}}{(P \Rightarrow \neg\neg Q) \Rightarrow (\neg\neg P \Rightarrow \neg\neg\neg\neg Q)}\ R \qquad D_3}{(P \Rightarrow \neg\neg Q) \Rightarrow (\neg\neg P \Rightarrow \neg\neg Q)}\ R'$$

Donde D_1, D_2 existen por (f) y D_3 por (c).
Combinando esta deducción con (i) y (j) encontramos:

$$(P \Rightarrow \neg\neg Q) \Leftrightarrow \neg\neg(P \Rightarrow Q) \Leftrightarrow (\neg\neg P \Rightarrow \neg\neg Q)$$

Lógica clásica. La lógica clásica es obtenida al reforzar la regla de absurdo intuicionista por la regla de absurdo clásica:

$$\perp c\ \frac{\begin{matrix} [\neg P] \\ D \\ \perp \end{matrix}}{P}.$$

Las suposiciones indicadas por $[\neg P]$ han sido canceladas. Observe que por $(\Rightarrow I)$:

$$\Rightarrow I\ \frac{\begin{array}{c}[\neg P]\\ \vdots\\ \bot\end{array}}{\neg\neg P}$$

Y que por lo tanto el adoptar $(\bot_c)$ sería equivalente a tener proposiciones de la forma $\neg\neg P \Rightarrow P$ como axiomas.

$$\frac{\neg\neg P \Rightarrow P \qquad \dfrac{\begin{array}{c}[\neg P]\\ D\\ \bot\end{array}}{\neg\neg P}}{P}$$

Consideremos ahora el cálculo de predicados clásico en el lenguaje Ω. El lenguaje **CPC** contiene los siguientes, ya conocidos, axiomas y reglas de inferencia:

(1) $P \Rightarrow (Q \Rightarrow P)$

(2) $(P \Rightarrow (Q \Rightarrow R)) \Rightarrow ((P \Rightarrow Q) \Rightarrow (P \Rightarrow R))$

(3) $P \Rightarrow (Q \Rightarrow P \wedge Q)$

(4) $P \wedge Q \Rightarrow P$ (5) $P \wedge Q \Rightarrow Q$

(6) $(P \Rightarrow R) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \vee Q \Rightarrow R))$

(7) $P \Rightarrow P \vee Q$ (8) $Q \Rightarrow P \vee Q$

(9) $\bot \Rightarrow P$ (10) $\neg\neg P \Rightarrow P$

(11) $\forall x P \Rightarrow P(x/t)$

(12) $\forall x\,(P \Rightarrow Q(x)) \Rightarrow (P \Rightarrow \forall x\,Q(x))$

(13) $P(x/t) \Rightarrow \exists x\,P$

(14) $\forall x\,(Q(x) \Rightarrow P) \Rightarrow (\exists x\,Q(x) \Rightarrow P)$

(15) $\dfrac{P \;;\; P \Rightarrow Q}{Q}$ (16) $\dfrac{P}{\forall x\,P}$

Aquí, las fórmulas del lenguaje Ω figuran en los esquemas axiomáticos y en las reglas de inferencia.

En los esquemas (12) y (14), como siempre, la fórmula P no tiene ocurrencias libres de la variable x.

Desde el punto de vista de la discusión anterior, solo uno de tales axiomas puede ser rechazado, este es el esquema (10), la ley de eliminación de una doble negación. Consideremos entonces el cálculo **HPC** (cálculo de predicados intuicionista, debido a Heyting en su mayoría), que es obtenido a partir de **CPC** al eliminar el esquema (10). Al hacer esto, nos quedaremos con el esquema (9) (el cual es deducible con la ayuda de (10) a partir de los demás axiomas) que ahora es esencial.

Por una lista de fórmulas queremos decir un conjunto finito de fórmulas del lenguaje Ω en el cual, sin embargo, repeticiones de fórmulas son permitidas. Por lo tanto el orden de las fórmulas en una lista Γ es inesencial; pero, para cada fórmula, uno debe especificar cuantas veces ocurre en Γ. En acuerdo con esto, es necesario comprender relaciones y operaciones en listas.

La relación $\Gamma \subseteq \Delta$ significa que toda fórmula P que ocurre en Γ también ocurre en Δ y además, Δ contiene al menos tantas copias de P como en Γ. Al tomar una unión de listas $\Gamma \cup \Delta$ de listas, el número de fórmulas en cada lista es sumada. Abreviaremos la unión $\Gamma \cup \Delta$ por $\Gamma\Delta$. Por lo tanto $\Delta\Gamma$ y $\Gamma\Delta$ son la misma lista. La lista $P\Gamma$ es obtenida de Γ al añadirle una copia de la fórmula P.

Usamos **PC** como un nombre general de uno de los cálculos **CPC** ó **HPC**. Si Γ es una lista de fórmulas y P es una fórmula, la expresión $\Gamma \vdash P$ (que se lee " P es deducible de Γ "), o más explicitamente, **PC** , $\Gamma \vdash P$ significa que P puede ser deducido de la lista Γ con la ayuda de los esquemas axiomáticos y reglas de inferencia de **PC**, donde la regla de generalización (16) no es aplicada con respecto a los parámetros en Γ.

***Teorema** 2.1 : (Teorema de la deducción) Para un cálculo dado **PC** y lenguaje Ω, $\Gamma, P \vdash Q \Leftrightarrow \Gamma \vdash (P \Rightarrow Q)$.*

La demostración de este teorema es exactamente la misma que se da en los cursos de lógica clásica y por ende omitimos la demostración (Para una demostración ver **[4]**).

■

En ocaciones es más conveniente utilizar otra formulación equivalente de **CPC** y **HPC** para algunas demostraciones. Nos referiremos a tales formulaciones como $\mathbf{CPC_1}$ y $\mathbf{HPC_1}$:

(1) $\dfrac{P \; ; \; P \Rightarrow Q}{Q}$ (2) $\dfrac{P \Rightarrow Q \; ; \; Q \Rightarrow R}{P \Rightarrow R}$ (3) $\dfrac{P \wedge Q \Rightarrow R \,.}{P \Rightarrow (Q \Rightarrow R)}$

(4) $\dfrac{P \Rightarrow (Q \Rightarrow R)}{P \wedge Q \Rightarrow R}$ (5) $P \wedge Q \Rightarrow P$ (6) $P \wedge Q \Rightarrow Q \wedge P$

(7) $P \Rightarrow (P \wedge P)$ (8) $\dfrac{P \Rightarrow R \; ; \; Q \Rightarrow R}{P \vee Q \Rightarrow R}$ (9) $P \Rightarrow (P \vee Q)$

(10) $P \vee Q \Rightarrow Q \vee P$ (11) $\bot \Rightarrow P$ (12) $\dfrac{\neg\neg P \,.}{P}$

(13) $\forall x P \Rightarrow P(x/t)$ (14) $\dfrac{P \Rightarrow Q(y) \,.}{P \Rightarrow \forall x Q(x)}$

(15) $\dfrac{Q(x) \Rightarrow P}{\exists x Q(x) \Rightarrow P}$ (16) $P(x/t) \Rightarrow \exists x P$

El cálculo intuicionista $\mathbf{HPC_1}$ se obtiene de $\mathbf{CPC_1}$ al eliminar la regla de inferencia (12).

Proposición 2.2*: Las formulaciones* ***CPC*** *y* $\mathbf{CPC_1}$*, así como las formulaciones* ***HPC*** *y* $\mathbf{HPC_1}$ *son equivalentes, así mismo, estas últimas lo son con las formulaciones obtenidas de la interpretación* ***BHK****; en el sentido de que toda fórmula es deducible en un sistema si y solamente si es deducible en el otro .*

Demostración : La demostración de este teorema consiste en la verificación de que los axiomas y reglas de inferencia de un sistema son admisibles en el otro sistema. La verificación es inmediata por lo que la omitimos.

■

CAPITULO 3.

CALCULO DE SECUENCIAS.

En el presente capítulo presentaremos otra formulación del cálculo de predicados, esta vez como un cálculo de *secuencias*.

Por una *secuencia* queremos decir una figura de la forma $\Gamma \rightarrow \Delta$, donde Γ y Δ son listas de fórmulas. Con cada secuencia asociaremos de una manera estandar una fórmula - la *fórmula imagen* - de la secuencia dada.

De hecho, si se nos es dada una secuencia S de la forma:

$$P_1, P_2, \ldots, P_n \rightarrow Q_1, Q_2, \ldots, Q_m$$

entonces le asociamos la fórmula S^{Φ} teniendo la forma:

$$T \wedge P_1 \wedge P_2 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee Q_2 \vee \ldots \vee Q_m \vee \bot$$

donde $T \equiv (\bot \Rightarrow \bot)$. El orden de las fórmulas a la derecha y a la izquierda es inesencial. En particular, si el lado derecho de la secuencia es vacío, es decir $m = 0$, entonces S^{Φ} es equivalente en la lógica de predicados a la fórmula $\neg (P_1 \wedge P_2 \wedge \ldots \wedge P_n)$. La secuencia vacía $\rightarrow$ tiene como su fórmula imagen a la fórmula $T \Rightarrow \bot$, la cual es equivalente a $\bot$.

El cáculo **GHPC** (Cálculo de predicados intuicionista como un cálculo de secuencias ó Cálculo de predicados al estilo de Gentzen) se establece para la deducción de secuencias.

Tal cálculo contiene axiomas de las siguientes dos formas:

a) $P\,\Gamma \to \Delta\,P$ Donde P es una fórmula atómica del lenguaje Ω.
b) $\bot\,\Gamma \to \Delta$ Notamos que $\bot$ no es considerado como una fórmula atómica, es solo una *constante lógica* .

Las reglas de inferencia del cálculo son muy simétricas e introducen conectivos lógicos a la derecha y a la izquierda:

$$(\Rightarrow \to)\ \frac{(P \Rightarrow Q)\,\Gamma \to P\ ;\ Q\,\Gamma \to \Delta}{(P \Rightarrow Q)\,\Gamma \to \Delta} \qquad (\to \Rightarrow)\ \frac{P\,\Gamma \to Q}{\Gamma \to \Delta\,(P \Rightarrow Q)}$$

$$(\wedge \to)\ \frac{P\,Q\,\Gamma \to \Delta}{(P \wedge Q)\,\Gamma \to \Delta} \qquad (\to \wedge)\ \frac{\Gamma \to \Delta\,P\ ;\ \Gamma \to \Delta\,Q}{\Gamma \to \Delta\,(P \wedge Q)}$$

$$(\vee \to)\ \frac{P\,\Gamma \to \Delta\ ;\ Q\,\Gamma \to \Delta}{(P \vee Q)\,\Gamma \to \Delta} \qquad (\to \vee)\ \frac{\Gamma \to \Delta\,P\,Q}{\Gamma \to \Delta\,(P \vee Q)}$$

$$(\forall \to)\ \frac{\forall x\,Q(x)\,Q(t)\,\Gamma \to \Delta}{\forall x\,Q(x)\,\Gamma \to \Delta} \qquad (\to \forall)\ \frac{\Gamma \to Q(y)}{\Gamma \to \Delta\,\forall x\,Q(x)}$$

$$(\exists \to)\ \frac{Q(y)\,\Gamma \to \Delta}{\exists x\,Q(x)\,\Gamma \to \Delta} \qquad (\to \exists)\ \frac{\Gamma \to \Delta\,\exists x\,Q(x)\,Q(t)}{\Gamma \to \Delta\,\exists x\,Q(x)}$$

En la regla $(\to \forall)$ la lista Γ no contiene ocurrencias libres de la variable y, y en la regla $(\exists \to)$ las listas Γ y Δ no contienen ocurrencias libres de la variable y , e $y = x$ ó x no es un parámetro de $Q(y)$. La notación $Q(t)$ es la abreviación de $Q(x/t)$.

Observe que en las reglas $(\to \Rightarrow)$ y $(\to \forall)$ la lista Δ aparece en la conclusión de la regla pero no en sus premisas. Esta es una característica especial de la lógica de secuencias intuicionista. En la regla $(\Rightarrow \to)$ la fórmula principal de la conclusión es repetida en la premisa de la izquierda.

La expresión $\vdash S$ significa que la secuencia S es deducible en este caso en el cálculo **GHPC**.

Una deducción puede ser expresada en forma de un árbol. La *longitud* de la deducción es el número de secuencias en la rama más larga.

El siguiente teorema afirma la equivalencia de **GHPC** y **HPC**.

Teorema *3.1. Si una secuencia es deducible en GHPC, entonces su fórmula imagen S^{Φ}, es deducible en HPC. Recíprocamente, si S^{Φ} es deducible en HPC, entonces S es deducible en GHPC.*

Demostración: La primera parte se demostrará por inducción con respecto a la construcción de la deducción de S en **GHPC**. Es necesario verificar sólo que la fórmula imagen de los axiomas y las reglas de inferencia de **GHPC** son admisibles en **HPC**. Veámoslo.

Si se tiene un axioma de la forma $P\,\Gamma \rightarrow \Delta\,P$ con P una fórmula atómica. Entonces su fórmula imagen es:
$P \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot \vee P$ y por las reglas de **HPC** se tiene:

$$P \wedge T \wedge \ldots \wedge P_n \Rightarrow P \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot \vee P$$ que es lo deseado.

Si el axioma es de la forma $\bot\,\Gamma \rightarrow \Delta$ entonces su fórmula imagen es:
$\bot \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot$ que se obtiene de:
$\bot \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow \bot \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot$.

$\therefore$ para los axiomas se cumple.

Veámoslo ahora para las reglas de inferencia:

$(\Rightarrow \rightarrow)$ entonces por hipótesis de inducción tenemos que las fórmulas imágenes de las premisas se deducen en **HPC** es decir se tienen:

$$(P \Rightarrow Q) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow P\ ;$$
$$Q \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot$$

Pero $(P \Rightarrow Q) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow (P \Rightarrow Q)$ por lo tanto, de la primera hipótesis y lo anterior se tiene:

$$(P \Rightarrow Q) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow (P \Rightarrow Q) \wedge P \Rightarrow Q$$

y $$(P \Rightarrow Q) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow T \wedge P_1 \wedge \ldots \wedge P_n$$

$$\therefore (P \Rightarrow Q) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q \wedge T \wedge P_1 \wedge \ldots \wedge P_n$$
$$\Rightarrow Q_1 \vee \ldots \vee Q_m \vee \perp$$

lo deseado.

$(\wedge \rightarrow)$ entonces tenemos que se deduce la fórmula:

$$(P \wedge Q) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \perp$$

Que es la misma de la conclusión salvo los paréntesis.

$(\vee \rightarrow)$ Aquí suponemos que se deducen por hipótesis las fórmulas:

$$P \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \perp$$
$$Q \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \perp$$

De las cuales se concluye:

1) $(P \wedge T \wedge P_1 \wedge \ldots \wedge P_n) \vee (Q \wedge T \wedge P_1 \wedge \ldots \wedge P_n) \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \perp$

Por otro lado tenemos que:

2) $(P \vee Q) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Leftrightarrow (T \wedge P) \vee (T \wedge Q) \wedge P_1 \wedge \ldots \wedge P_n$
$\Leftrightarrow (P \wedge T \wedge P_1 \wedge \ldots \wedge P_n) \vee (Q \wedge T \wedge P_1 \wedge \ldots \wedge P_n)$

De 1) y 2) se obtiene lo deseado.

$(\forall \rightarrow)$ Se tiene por hipótesis:

$$\forall x\, Q(x) \wedge Q(t) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \perp$$

Por otro lado: $\forall x\, Q(x) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow \forall x\, Q(x) \Rightarrow Q(t)$ y
$\forall x\, Q(x) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow \forall x\, Q(x) \wedge T \wedge P_1 \wedge \ldots \wedge P_n$

$\therefore\ \forall x\, Q(x) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow \forall x\, Q(x) \wedge T \wedge P_1 \wedge \ldots \wedge P_n \wedge Q(t)$

lo cual, junto con la hipótesis, implican lo deseado.

$(\exists \rightarrow)$ Se tiene directamente de la regla (15) de HPC_1.

$(\rightarrow \Rightarrow)$ Se tiene por hipótesis:

$$P \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q$$

Tenemos que:

$$(P \wedge T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q) \Rightarrow (T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow (P \Rightarrow Q))$$

Por lo tanto se tiene: $T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow (P \Rightarrow Q)$ y en la conclusión estamos suponiendo $T \wedge P_1 \wedge \ldots \wedge P_n$ por lo tanto concluyo $P \Rightarrow Q$. De lo anterior se obtiene que:

$T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow (P \Rightarrow Q) \vee Q_1 \vee \ldots \vee Q_m \vee \perp$

que es lo deseado.

$(\rightarrow \wedge)$ Por hipótesis tenemos:

$$T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \perp \vee P$$
$$T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \perp \vee Q$$

Entonces:

$$\begin{aligned} T \wedge P_1 \wedge \ldots \wedge P_n &\Rightarrow (Q_1 \vee \ldots \vee Q_m \vee \perp \vee P) \wedge (Q_1 \vee \ldots \vee Q_m \vee \perp \vee Q) \\ &\Rightarrow ((Q_1 \vee \ldots \vee Q_m \vee \perp) \vee P) \wedge ((Q_1 \vee \ldots \vee Q_m \vee \perp) \vee Q) \\ &\Rightarrow (Q_1 \vee \ldots \vee Q_m \vee \perp) \vee (P \wedge Q) \end{aligned}$$

Que es lo deseado.

($\rightarrow \vee$) Por hipótesis se tiene:

$$T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot \vee P \vee Q$$

Que es lo que hay que demostrar.

($\rightarrow \forall$) Por hipótesis tenemos:

$$T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q(y)$$

Esto implica, por la regla (14) de $\mathbf{HPC_1}$: $T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow \forall x\, Q(x)$

Y $\quad T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow \forall x\, Q(x) \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot \vee \forall x\, Q(x)$

$\therefore \; T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot \vee \forall x\, Q(x)$

que es lo deseado.

($\rightarrow \exists$) Ahora tenemos por hipótesis:

$$T \wedge P_1 \wedge \ldots \wedge P_n \Rightarrow Q_1 \vee \ldots \vee Q_m \vee \bot \vee \exists x\, Q(x) \vee Q(t)$$

Entonces aplicamos la regla (16) de $\mathbf{HPC_1}$ y simplificamos un $\exists x\, Q(x)$ obteniendo lo deseado.

□

La demostración de la segunda parte está dividida en una serie de lemas, los cuales tienen que ver con la deducibilidad en **GHPC**.

Lema 3.1.1: *Si una secuencia S es deducible, entonces la secuencia S(x / t) también lo es, y además, por una deducción de la misma longitud.*

Demostración:

Supongamos una deducción de S dada. Entonces llevamos a cabo en esta deducción, el reemplazamiento de ocurrencias libres del parámetro x por el término t. (Cuando hacemos esto, por supuesto, si es necesario renombramos las variables acotadas y propias de la deducción S ; por variables propias queremos decir variables usadas explicitamente en las reglas $(\rightarrow \forall)$ y $(\exists \rightarrow)$ en lugar de y.

La demostración se hace por inducción con respecto a la construcción de la deducción.

Si S es un axioma, claramente $S(x/t)$ también lo es. Ahora, si S se obtuvo por medio de alguna de las reglas de inferencia se procede como se explicó en el párrafo anterior.

■

Lema 3.1.2: Si una secuencia $\Gamma \rightarrow \Delta \perp$ es deducible, entonces la secuencia $\Gamma \rightarrow \Delta$ también lo es, y además por una deducción de la misma longitud.

Demostración: Por inducción con respecto a la construcción de la deducción de S. Si S es un axioma del primer tipo, quiere decir que tanto Γ como Δ conllevan una fórmula atómica P. y por lo tanto $\Gamma \rightarrow \Delta$ es un axioma.

Si S es un axioma del segundo tipo, entonces $S = \perp \Gamma \rightarrow \Delta \perp$. y por lo tanto $\perp \Gamma \rightarrow \Delta$ también lo es.

Si S se obtuvo por alguna de las reglas de inferencia, entonces moviendonos de abajo hacia arriba en la deducción de $\Gamma \rightarrow \Delta \perp$, borramos todas las ocurrencias de $\perp$ (por hipótesis de inducción) en la derecha que resulta en la deducción de la ocurrencia especificada de $\perp$ en la última secuencia, así obtenemos una deducción de la misma longitud de la secuencia $\Gamma \rightarrow \Delta$.

■

Lema 3.1.3 : *(Admisibilidad de una regla de adición) La deducibilidad de* $\Gamma \rightarrow \Delta$ *implica la deducibilidad de* $\Gamma \Pi \rightarrow \Delta \Phi$ *y además, por una deducción de la misma longitud.*

Demostración: Por inducción con respecto a la construcción de la deducción de S.

Obviamente si S es un axioma se tiene que la secuencia $\Gamma \Pi \rightarrow \Delta \Phi$ también lo es.

Si se obtuvo a partir de una regla de inferencia se aplica la hipótesis de inducción a las premisas obteniendo duducciones de ellas de la misma longitud agregandoles Π y Φ donde lo requieran, y entonces aplico la misma regla de inferencia que antes obteniendo la secuencia deseada con una deducción de la misma longitud que la original ya que las premisas tenían una deducción de longitud un número menor. Al tratar con el caso donde $\Gamma \rightarrow \Delta$ se obtuvo por las reglas $(\rightarrow \forall)$ y $(\exists \rightarrow)$ usamos 3.1.1.

Por ejemplo si se obtuvo por $(\rightarrow \forall)$ $\dfrac{\Gamma \rightarrow Q(y)}{\Gamma \rightarrow \Delta' \forall x\, Q(x)}$

entonces $\Delta = \Delta' \forall x\, Q(x)$

y Γ no contiene ocurrencias libres de la variable y. Entonces por hipótesis de inducción obtenemos la secuencia:

$$\Gamma \Pi \rightarrow Q(y)$$

y por el lema 3.1.1 puedo cambiar y por una variable y' que no ocurre libremente ni en Γ ni en Π, y así poder aplicar de nuevo la regla para obtener:

$$\Gamma \Pi \rightarrow \Phi \Delta' \forall x\, Q(x) = \Gamma \Pi \rightarrow \Phi \Delta .$$

■

***Lema** 3.1.4 : (Invertibilidad de ciertas reglas de inferencia) Todas las reglas de inferencia de **GHPC** con excepción de $(\Rightarrow \rightarrow)$, $(\rightarrow \Rightarrow)$ y $(\rightarrow \forall)$, son invertibles, esto es, la deducibilidad de la conclusión de cada una de las reglas implica la deducibilidad de cualquiera de las premisas. Así como para la regla $(\Rightarrow \rightarrow)$ la deducibilidad de la conclusión implica la deducibilidad de la premisa de la derecha :*
$Q\,\Gamma \rightarrow \Delta$. Añadiendo a todos los casos que la deducción de las premisas tiene una longitud que no excede la longitud de la deducción de la conclusión.

Demostración: Para las reglas $(\forall \rightarrow)$ y $(\rightarrow \exists)$ se sigue el resultado del lema anterior.

Para los demás casos probaremos el lema individualmente por inducción con respecto a la construcción de la deducción de la conclusión de la regla:

1) Supongamos que se deduce $(P \Rightarrow Q)\,\Gamma \rightarrow \Delta$.
si es un axioma, entonces $Q\,\Gamma \rightarrow \Delta$ también lo es. Ahora, si se deduce por $(\Rightarrow \rightarrow)$ no hay nada que demostrar ya que entonces las premisas ya eran deducibles, por lo tanto debemos analizar el caso cuando se dedujo la conclusión por medio de las demás reglas.

a) Supongamos que la conclusión proviene de la regla $(\rightarrow \Rightarrow)$ entonces Γ' debe tener la forma $(P \Rightarrow Q)\,\Gamma$ y Δ tiene la forma $\Delta'\,(R \Rightarrow S)$, es decir la regla tiene la forma:

$$(1) \qquad \frac{R\,(P \Rightarrow Q)\,\Gamma \rightarrow S}{(P \Rightarrow Q)\,\Gamma \rightarrow \Delta} = \frac{R\,\Gamma' \rightarrow S}{\Gamma' \rightarrow \Delta'\,(R \Rightarrow S)}$$

Entonces, por hipótesis de inducción es deducible la inversa de (1) con una deducción que no excede la longitud de la deducción de (1) es decir:

$$\frac{Q\,R\,\Gamma \rightarrow S}{R\,(P \Rightarrow Q)\,\Gamma \rightarrow S} \quad (2)$$

(2) es deducible.
y aplicando la regla $(\rightarrow \Rightarrow)$ a (2) obtenemos: $Q\,\Gamma \rightarrow \Delta'\,(R \Rightarrow S)$ o sea

$Q\,\Gamma \rightarrow \Delta$ que es lo deseado.

b) Supongamos que la conclusión proviene de la regla $(\wedge \rightarrow)$ entonces la regla tiene la forma:

$$(P \Rightarrow Q)\,\Gamma \rightarrow \Delta \quad = \quad \begin{array}{c}(1)\\ \hline (R \wedge S)\,(P \Rightarrow Q)\,\Gamma' \rightarrow \Delta\end{array} \quad \begin{array}{c} R\,S\,(P \Rightarrow Q)\,\Gamma' \rightarrow \Delta \end{array}$$

Entonces es deducible la inversa de (1) o sea: $Q\,R\,S\,\Gamma' \rightarrow \Delta$ y aplicando otra vez la regla $(\wedge \rightarrow)$ obtenemos:

$$(R \wedge S)\,Q\,\Gamma' \rightarrow \Delta \quad \text{es decir } Q\,\Gamma \rightarrow \Delta .$$

c) Si la conclusión proviene de aplicar la regla $(\rightarrow \wedge)$ entonces la regla tiene la forma:

$$(P \Rightarrow Q)\,\Gamma \rightarrow \Delta \quad = \quad \begin{array}{c}(1)\\ \hline \Gamma' \rightarrow \Delta'\,(R \wedge S)\end{array} \quad \begin{array}{c} (P \Rightarrow Q)\,\Gamma \rightarrow \Delta'R \;;\; (P \Rightarrow Q)\,\Gamma \rightarrow \Delta'S \end{array}$$

Entonces es deducible la inversa de (1) o sea:

$$Q\,\Gamma \rightarrow \Delta'R \qquad y \qquad Q\,\Gamma \rightarrow \Delta'S$$

Entonces aplico la regla nuevamente para obtener:

$$Q\,\Gamma \rightarrow \Delta'(R \wedge S) \;=\; Q\,\Gamma \rightarrow \Delta \quad \text{lo deseado.}$$

d) y e) es decir si la conclusión provino de las reglas $(\vee \rightarrow)$ y $(\rightarrow \vee)$ son muy similares a las demostraciones de b) y c).

f) Supongamos que la deducción proviene de aplicar la regla $(\forall \rightarrow)$, entonces la regla tiene la forma:

$$(P \Rightarrow Q)\,\Gamma \rightarrow \Delta \quad = \quad \begin{array}{c}(1)\\ \hline \forall x\,R(x)\,(P \Rightarrow Q)\,\Gamma' \rightarrow \Delta\end{array} \quad \begin{array}{c} \forall x\,R(x)\,R(t)\,(P \Rightarrow Q)\,\Gamma' \rightarrow \Delta \end{array}$$

Entonces es deducible la inversa de (1) es decir se tiene:

$$\forall x\,R(x)\,R(t)\,Q\,\Gamma' \rightarrow \Delta$$

Y aplicando nuevamente la regla se obtiene:

$$\forall x\, R(x)\; Q\, \Gamma' \rightarrow \Delta \;=\; Q\, \Gamma \rightarrow \Delta \quad \text{lo deseado.}$$

g) Si la deducción provino de aplicar la regla $(\rightarrow \forall)$ entonces la regla tiene la forma:

$$(P \Rightarrow Q)\, \Gamma \rightarrow \Delta \quad = \quad \frac{(1)\ \ \Gamma' \rightarrow R(y)}{\Gamma' \rightarrow \Delta'\, \forall x\, R(x)}$$

donde $\Gamma' = (P \Rightarrow Q)\, \Gamma$ no contiene ocurrencias libres de la variable y.

Entonces la inversa de (1) es deducible, y aplicando la regla otra vez obtengo:

$$\frac{Q\, \Gamma \rightarrow R(y)}{Q\, \Gamma \rightarrow \Delta}$$ Donde $Q\, \Gamma$ no contiene ocurrencias libres de la variable y.

h) Si la deducción proviene de la regla $(\exists \rightarrow)$ entonces se tiene la figura:

$$(P \Rightarrow Q)\, \Gamma \rightarrow \Delta \quad = \quad \frac{(1)\ R(y)\, (P \Rightarrow Q)\, \Gamma' \rightarrow \Delta}{\exists x\, R(x)\, (P \Rightarrow Q)\, \Gamma' \rightarrow \Delta}$$

donde las listas $(P \Rightarrow Q)\, \Gamma'$ y Δ no contienen ocurrencias libres de la variable y e $y \equiv x$ ó x no es un parámetro de $R(y)$.

Entonces la inversa de (1) es deducible, y aplicando la regla nuevamente tenemos:

$$\frac{R(y)\, Q\, \Gamma' \rightarrow \Delta}{\exists x\, R(x)\, Q\, \Gamma' \rightarrow \Delta}$$ donde $Q\, \Gamma'$ tampoco tiene ocurrencias libres de la variable y e $y \equiv x$ ó x no es un parámetro de $R(y)$.

Que es lo deseado ya que $\exists x\, R(x)\, Q\, \Gamma' \rightarrow \Delta = (P \Rightarrow Q)\, \Gamma \rightarrow \Delta$.

i) La demostración de este caso es igual al del caso (f).

De todo lo anterior se duduce que en la regla $(\Rightarrow \rightarrow)$, la deducibilidad de la conclusión implica la deducibilidad de la premisa de la derecha, además con una deducción que no excede la longitud de la deducción de la conclusión.
La demostración de las demás reglas lleva un método muy similar y hemos decidido omitirlas.

■

***Lema** 3.1.5: (Regla de contracción). Las siguientes reglas son admisibles en **GHPC**.*

$$\frac{\Gamma \rightarrow \Delta P P}{\Gamma \rightarrow \Delta P} \qquad \frac{P P \Gamma \rightarrow \Delta}{P \Gamma \rightarrow \Delta}$$

además, la conclusión puede ser deducida por una demostración cuya longitud no excede la longitud de la demostración de las premisas.

Demostración: Por inducción con respecto a la estructura de la fórmula P; para una fórmula fija P usaremos inducción con respecto a la longitud de la deducción de las premisas.

(a) Supongamos que $P = (R \Rightarrow S)$. Si $\Gamma \rightarrow \Delta P P$ es un axioma entonces: $\Gamma \rightarrow \Delta P$ también lo es y la proposición es demostrada.

Lo mismo pasa si $P P \Gamma \rightarrow \Delta$ es un axioma. Ahora si $\Gamma \rightarrow \Delta P P$ (y respectivamente $P P \Gamma \rightarrow \Delta$) es obtenida por una regla de inferencia que no tiene que ver explícitamente con la P indicada entonces usando la hipótesis inductiva, se llega a la contracción de P en las premisas y aplicando la misma regla obtenemos la secuencia $\Gamma \rightarrow \Delta P$ ($P \Gamma \rightarrow \Delta$).

Asuma que $P P \Gamma \rightarrow \Delta$ fue obtenida por la regla $(\Rightarrow \rightarrow)$ con referencia a las fórmulas en consideración. Entonces en las premisas de esta última regla están las secuencias:

$$(R \Rightarrow S)(R \Rightarrow S)\Gamma \rightarrow R \quad \text{y} \quad (R \Rightarrow S) S \Gamma \rightarrow \Delta$$

Es decir: $$\frac{(R \Rightarrow S)(R \Rightarrow S)\Gamma \rightarrow R \;;\; (R \Rightarrow S) S \Gamma \rightarrow \Delta}{(R \Rightarrow S)(R \Rightarrow S)\Gamma \rightarrow \Delta}$$

Por hipótesis de inducción, de la primer secuencia obtenemos:

$$(R \Rightarrow S)\, \Gamma \rightarrow R$$

De la segunda secuencia obtenemos por (3.1.4) la secuencia:

$$S\, S\, \Gamma \rightarrow \Delta$$

al aplicar la inversa de la regla $(\Rightarrow \rightarrow)$ a dicha secuencia, y así por hipótesis de inducción obtenemos:

$$S\, \Gamma \rightarrow \Delta$$

y aplicando la regla $(\Rightarrow \rightarrow)$ deducimos $(R \Rightarrow S)\, \Gamma \rightarrow \Delta$ que es lo deseado. Esto termina con el primer caso y la primera regla de contracción.

Solo resta, para este primer caso, en la segunda regla de contracción, suponer que $\Gamma \rightarrow \Delta\, P\, P$ se obtuvo de la regla $(\rightarrow \Rightarrow)$ con referencia a P. Entonces las premisas tienen la forma:

$$\frac{R\, \Gamma \rightarrow S}{\Gamma \rightarrow \Delta\, (R \Rightarrow S)\, (R \Rightarrow S)}$$

Y se obtiene $\Gamma \rightarrow \Delta\, (R \Rightarrow S)$ directamente de ella por $(\rightarrow \Rightarrow)$. Esto termina con el caso (a).

Para los siguientes casos tenemos que si la secuencia es un axioma, también lo es omitiendo una P. Y si la secuencia fue obtenida por una regla de inferencia que no involucre explícitamente a la P indicada, entonces aplicando la hipótesis inductiva a las premisas obtenemos lo deseado directamente al aplicar la misma regla. Por lo tanto solo veremos los casos en los que se utilizaron reglas con referencia a la fórmula en consideración.

(b) Supongamos que $P = (R \wedge S)$.

Si $P\, P\, \Gamma \rightarrow \Delta$ se obtuvo por la regla $(\wedge \rightarrow)$ entonces:

$$\frac{R\, S\, (R \wedge S)\, \Gamma \rightarrow \Delta}{(R \wedge S)\, (R \wedge S)\, \Gamma \rightarrow \Delta}$$

Y por (3.1.4) tenemos: $R\,S\,R\,S\,\Gamma \rightarrow \Delta$ de la premisa.

y por hipótesis de inducción obtenemos $R\,S\,\Gamma \rightarrow \Delta$ de ahí aplicamos $(\wedge \rightarrow)$ para obtener lo deseado.

Si $\Gamma \rightarrow \Delta\,P\,P$ se obtuvo por la regla $(\rightarrow \wedge)$ se tiene:

$$\frac{\Gamma \rightarrow \Delta\,(R \wedge S)\,R \;;\; \Gamma \rightarrow \Delta\,(R \wedge S)\,S}{\Gamma \rightarrow \Delta\,(R \wedge S)\,(R \wedge S)}$$

Y por (3.1.4) de las premisas obtenemos:

$\Gamma \rightarrow \Delta\,R\,R$ y $\Gamma \rightarrow \Delta\,S\,S$ entonces por hipótesis de inducción obtenemos:

$\Gamma \rightarrow \Delta\,R$ y $\Gamma \rightarrow \Delta\,S$ y aplicando la regla $(\rightarrow \wedge)$ se sigue lo deseado.

(c) El caso de suponer que $P = (R \vee S)$ es muy simétrico al caso (b) y por lo tanto lo omitimos.

(d) Supongamos que $P = \forall x\,Q(x)$.

Si $P\,P\,\Gamma \rightarrow \Delta$ se obtuvo por la regla $(\forall \rightarrow)$ se tiene:

$$\frac{\forall x\,Q(x)\;Q(t)\;\forall x\,Q(x)\;\Gamma \rightarrow \Delta}{\forall x\,Q(x)\;\forall x\,Q(x)\;\Gamma \rightarrow \Delta}$$

Y por (3.1.4) se tiene lo siguiente:

$\forall x\,Q(x)\;Q(t)\;\forall x\,Q(x)\;Q(t)\;\Gamma \rightarrow \Delta$ Y aplicando la hipótesis de inducción:

$\forall x\,Q(x)\;Q(t)\;\Gamma \rightarrow \Delta$ y por último aplico de nuevo la regla $(\forall \rightarrow)$

Si $\Gamma \rightarrow \Delta\,P\,P$ se obtuvo por la regla $(\rightarrow \forall)$ se tiene directamente la conclusión aplicando $(\rightarrow \forall)$ a la premisa.

(e) Por último supongamos que $P = \exists x\,Q(x)$.

Si $P\,P\,\Gamma \rightarrow \Delta$ se obtuvo por la regla $(\exists \rightarrow)$ se tiene:

$$\frac{Q(y)\;\exists x\,Q(x)\;\Gamma \rightarrow \Delta}{\exists x\,Q(x)\;\exists x\,Q(x)\;\Gamma \rightarrow \Delta}$$

Y por (3.1.4) $Q(y)\;Q(y)\;\Gamma \rightarrow \Delta$

Aplicando la hipótesis de inducción: $Q(y)\ \Gamma \rightarrow \Delta$ y aplicando otra vez la regla $(\exists \rightarrow)$ se tiene lo deseado.

Si $\Gamma \rightarrow \Delta\ P\ P$ se obtuvo por la regla $(\rightarrow \exists)$ se procede igual que en la regla $(\forall \rightarrow)$. Esto termina con el caso (e).

Hay que notar que si P es una fórmula atómica el resultado es inmediato ya que en todos los casos la regla de inferencia no tiene que ver explícitamente con P entonces se procede como se dijo en un principio.

Esto completa nuestra demostración por doble inducción.

■

Lema 3.1.6 : *(La regla del corte, el llamado* ***TEOREMA FUNDAMENTAL DE GENTZEN****). La siguiente regla de inferencia, llamada un corte, es admisible en* ***GHPC.***

$$\frac{\Gamma \rightarrow \Delta P \ ;\ P \Pi \rightarrow \Phi}{\Gamma \Pi \rightarrow \Delta \Phi}$$

Demostración:

Supongamos dadas las deducciónes de las secuencias $\Gamma \rightarrow \Delta\ P$ y de $P \Pi \rightarrow \Phi$ en **GHPC.**

Asignamos a este par de demostraciones una tema de números naturales: (k , l , m) donde k es la complejidad lógica de la fórmula P (es decir el número de simbolismos lógicos y cuantificadores que hay en P), l es la longitud de la deducción $\Gamma \rightarrow \Delta\ P$ y m es la longitud de la deducción $P \Pi \rightarrow \Phi$.

Daremos la demostración de la deducibilidad de la conclusión por inducción con respecto a k, para una k fija, por inducción sobre l, y para k y l fijas por inducción sobre m.

En realidad, para la demostración uno debe especificar en que sentido uno debe reemplazar el corte dado por una figura de una deducción sin cortes o, al menos, por una figura de una deducción con cortes de longitud menor (k,l,m).

Examinemos los casos de la estructura del par dado de deducciones.

(1) Una de las premisas del corte es un axioma. entonces la conclusión es facilmente deducible en **GHPC**. Por ejemplo Si P es una fórmula atómica y $\Gamma = P\,\Gamma'$ entonces $\Gamma \to \Delta\, P$ es un axioma y se sigue $\Gamma\,\Pi \to \Delta\,\Phi$ a partir de $P\,\Pi \to \Phi$ por (3.1.3).

(2) Una de las premisas del corte es obtenida por una regla que no refiere a la fórmula especial P, entonces uno debe aplicar un corte a las premisas de esta regla (porque decreció l ó m) y entonces aplicar la misma regla.

(3) Ninguno de los otros dos casos se da y, por lo tanto, cada una de las reglas es obtenida por una regla de inferencia que introduce la fórmula P.
Aquí es necesario proceder en distintas formas dependiendo de la estructura de P:

(a) $P = (R \Rightarrow S)$. entonces el corte dado tiene la forma:

$$\dfrac{\dfrac{R\,\Gamma \to S}{\Gamma \to \Delta\,(R \Rightarrow S)} \qquad \dfrac{(R \Rightarrow S)\,\Pi \to R \;;\; S\,\Pi \to \Phi}{(R \Rightarrow S)\,\Pi \to \Phi}}{\Gamma\,\Pi \to \Delta\,\Phi}$$

Esta figura la transformamos por la siguiente:

$$\dfrac{\Gamma \to \Delta\,(R \Rightarrow S) \;;\; (R \Rightarrow S)\,\Pi \to R \qquad \dfrac{\dfrac{\Gamma\,\Pi \to \Delta\,R \;;\; R\,\Gamma \to S}{\Gamma\,\Gamma\,\Pi \to \Delta\,S} \;;\; S\,\Pi \to \Phi}{\Gamma\,\Gamma\,\Pi\,\Pi \to \Delta\,\Phi}}{\Gamma\;\Pi \to \Delta\,\Phi}$$

Aquí el corte de hasta arriba tiene longitud menor que la deducción de la derecha y los dos menores cortes son aplicados a fórmulas de menor complejidad lógica así que por la hipótesis de inducción, estos cortes son admisibles. La línea punteada significa, de aquí en adelante, una serie de aplicaciones de contracciones y adiciones que son admisibles por (3.1.3) y (3.1.5).

(b) $P = (R \wedge S)$. entonces el corte dado tiene la forma:

$$\dfrac{\dfrac{\Gamma \to \Delta R \;;\; \Gamma \to \Delta S \qquad R S \Pi \to \Phi}{\Gamma \to \Delta (R \wedge S) \;;\; (R \wedge S) \Pi \to \Phi}}{\Gamma \Pi \to \Delta \Phi}$$

El cual transformamos a la forma:

$$\dfrac{\dfrac{\Gamma \to \Delta R \;;\; R S \Pi \to \Phi}{S \Gamma \Pi \to \Delta \Phi \;\;;\;\; \Gamma \to \Delta S}}{\Gamma \Gamma \Pi \to \Delta \Phi}$$

$$\Gamma \Pi \to \Delta \Phi$$

Con las mismas acotaciones que antes.

(c) $P = (R \vee S)$ Entonces el corte tiene la forma:

$$\dfrac{\dfrac{\Gamma \to \Delta R S \qquad R \Pi \to \Phi \;;\; S \Pi \to \Phi}{\Gamma \to \Delta (R \vee S) \qquad (R \vee S) \Pi \to \Phi}}{\Gamma \Pi \to \Delta \Phi}$$

La cual la transformamos a la forma:

$$\dfrac{\dfrac{\dfrac{\Gamma \to \Delta R S ;\; S \Pi \to \Phi}{\Gamma \Pi \to \Delta \Phi R \;\;;\;\; R \Pi \to \Phi}}{\Gamma \Pi \Pi \to \Delta \Phi \Phi}}{\Gamma \Pi \to \Delta \Phi}$$

(d) $P = \forall x\, Q(x)$ entonces el corte tiene la forma:

$$\dfrac{\dfrac{\Gamma \to Q(y) \qquad \forall x\, Q(x)\, Q(t) \Pi \to \Phi}{\Gamma \to \forall x\, Q(x) \qquad \forall x\, Q(x)\; \Pi \to \Phi}}{\Gamma \Pi \to \Delta \Phi}$$

Transformamos esta figura a la forma;

$$\dfrac{\dfrac{\Gamma \to \Delta\ \forall x\, Q(x) \quad ; \quad \forall x\, Q(x)\ Q(t)\ \Pi \to \Phi}{\Gamma \to Q(t) \quad ; \quad Q(t)\ \Gamma\ \Pi \to \Delta\ \Phi}}{\Gamma\ \Gamma\ \Pi \to \Delta\ \Phi}$$

$$\dfrac{\Gamma\ \Gamma\ \Pi \to \Delta\ \Phi}{\Gamma\ \Pi \to \Delta\ \Phi}$$

Aquí, aparte, la deducción $\Gamma \to Q(t)$ es obtenida de $\Gamma \to Q(y)$ por (3.1.1) .

(e) $P = \exists x\, Q(x)$ entonces la figura tiene la forma:

$$\dfrac{\dfrac{\Gamma \to \Delta\ \exists x\, Q(x)\ Q(t) \qquad Q(y)\ \Pi \to \Phi}{\Gamma \to \Delta\ \exists x\, Q(x) \qquad \exists x\, Q(x)\ \Pi \to \Phi}}{\Gamma\ \Pi \to \Delta\ \Phi}$$

Y lo transformamos a la forma:

$$\dfrac{\dfrac{\dfrac{\Gamma \to \Delta\ \exists x\, Q(x)\ Q(t) \quad , \quad \exists x\, Q(x)\ \Pi \to \Phi}{\Gamma\ \Pi \to \Delta\ \Phi\ Q(t) \qquad ; \qquad Q(y)\ \Pi \to \Phi}}{\Gamma\ \Pi\ \Pi \to \Delta\ \Phi\ \Phi}}{\Gamma\ \Pi \to \Delta\ \Phi}$$

Aquí también utilizando (3.1.1).

Con lo anterior se ha completado la inducción.

■

***Lema** 3.1.7 : Para toda fórmula P , la secuencia $P \to P$ es deducible en **GHPC**.*

Demostración: Por inducción con respecto a la construcción de P .

Si P es una fórmula atómica entonces $P \to P$ es un axioma y por lo tanto deducible en **GHPC**.

(a) Si $P = (R \Rightarrow S)$ entonces R y S tienen menor complejidad y por lo tanto son deducibles por hipótesis de inducción las secuencias:

$$R \to R \qquad y \qquad S \to S$$

Entonces hacemos la figura:

$$\dfrac{\dfrac{\dfrac{R \to R}{(R \Rightarrow S)R \to R} \quad \dfrac{S \to S}{RS \to S}}{(R \Rightarrow S)R \to S}}{(R \Rightarrow S) \to (R \Rightarrow S)}$$

$$P \to P$$

(b) Si $P = (R \wedge S)$ entonces tenemos las secuencias $R \to R$ y $S \to S$.

Y formamos la figura:

$$\dfrac{\dfrac{\dfrac{R \to R}{SR \to R} \quad \dfrac{S \to S}{SR \to S}}{(R \wedge S) \to R \quad (R \wedge S) \to S}}{(R \wedge S) \to (R \wedge S)}$$

$$P \to P$$

(c) Si $P = (R \vee S)$ formamos la figura:

$$\dfrac{\dfrac{\dfrac{R \to R}{R \to RS} \quad \dfrac{S \to S}{S \to SR}}{R \to (R \vee S) \quad S \to (R \vee S)}}{(R \vee S) \to (R \vee S)}$$

$$P \to P$$

(d) Si $P = \forall x\, Q(x)$ formamos la figura:

$$\dfrac{\dfrac{\dfrac{Q(x) \to Q(x)}{Q(x) \to \forall x\, Q(x)}}{\forall x\, Q(x)\, Q(x) \to \forall x\, Q(x)}}{\forall x\, Q(x) \to \forall x\, Q(x)}$$

$$P \to P$$

(e) Por último, si $P = \exists x\, Q(x)$ tenemos la figura:

$$\dfrac{\dfrac{\dfrac{\dfrac{Q(x) \to Q(x)}{\exists x\, Q(x) \to Q(x)}}{\exists x\, Q(x) \to \exists x\, Q(x)\ Q(x)}}{\exists x\, Q(x) \to \exists x\, Q(x)}}{P \to P}$$

Esto completa la inducción.

■

Lema 3.1.8: *Si P es deducible en HPC, entonces la secuencia* $\to P$ *es deducible en GHPC.*

Demostración: Por inducción con respecto a la construcción de la deducción de P en HPC.

Primero, supongamos que P es un axioma de HPC, entonces tenemos trece casos:

(1) $P = R \Rightarrow (S \Rightarrow R)$ entonces construímos la deducción:

$$\dfrac{\dfrac{\dfrac{R \to R}{S\, R \to R}}{R \to (S \Rightarrow R)}}{\to R \Rightarrow (S \Rightarrow R)}}{\to P}$$

La primera secuencia de la deducción es demostrable en GHPC por (3.1.7), las demás inferencias son válidas por los lemas anteriores y reglas de inferencia de GHPC.

(2) $P = (Q \Rightarrow (R \Rightarrow S)) \Rightarrow ((Q \Rightarrow R) \Rightarrow (Q \Rightarrow S))$ entonces construímos la deducción siguiente:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{Q \to Q} \quad \dfrac{\dfrac{}{R \to R} \quad \dfrac{}{S \to S}}{(R \Rightarrow S)\,Q\,R \to R;\, Q\,R\,S \to S}}{Q \to Q \quad (Q \Rightarrow R)(R \Rightarrow S)\,Q \to Q \;;\; (R \Rightarrow S)\,Q\,R \to S}}{(Q \Rightarrow R)(Q \Rightarrow (R \Rightarrow S)\,Q \to Q \;;\; (R \Rightarrow S)\,Q\,(Q \Rightarrow R) \to S}}{(Q \Rightarrow R)(Q \Rightarrow (R \Rightarrow S)\,Q \to S}$$

$$\dfrac{(Q \Rightarrow R)(Q \Rightarrow (R \Rightarrow S) \to Q \Rightarrow S}{Q \Rightarrow (R \Rightarrow S) \to (Q \Rightarrow R) \Rightarrow (Q \Rightarrow S)}$$

$$\dfrac{}{\to (Q \Rightarrow (R \Rightarrow S)) \Rightarrow ((Q \Rightarrow R) \Rightarrow (Q \Rightarrow S))}$$

$$\to P$$

(3) $P = Q \Rightarrow (R \Rightarrow Q \wedge R)$ entonces construímos:

$$\dfrac{\dfrac{\dfrac{}{Q \to Q} \quad \dfrac{}{R \to R}}{Q\,R \to Q \quad , \quad Q\,R \to R}}{Q\,R \to Q \wedge R}$$

$$\dfrac{Q \to R \Rightarrow Q \wedge R}{\to Q \Rightarrow (R \Rightarrow Q \wedge R)}$$

$$\to P$$

(4) $P = Q \wedge R \Rightarrow Q$ entonces construímos:

$$\dfrac{\dfrac{\dfrac{}{Q \to Q}}{Q\,R \to Q}}{Q \wedge R \to Q}$$

$$\dfrac{}{\to Q \wedge R \Rightarrow Q}$$

$$\to P$$

(5) $P = Q \wedge R \Rightarrow R$ es simétrica a la anterior.

(6) $P = (Q \Rightarrow S) \Rightarrow ((R \Rightarrow S) \Rightarrow (Q \vee R \Rightarrow S))$. Construímos:

$$\dfrac{\dfrac{\dfrac{}{Q \to Q} \quad \dfrac{}{S \to S}}{(Q \Rightarrow S)\,Q\,(R \Rightarrow S) \to Q \;,\; Q\,(R \Rightarrow S)\,S \to S}}{(Q \Rightarrow S)\,Q\,(R \Rightarrow S) \to S} \qquad (a)$$

Por otra parte:

$$\dfrac{\dfrac{R \to R}{(R \Rightarrow S), R, (Q \Rightarrow S) \to R} \quad ; \quad \dfrac{S \to S}{S, R, (R \Rightarrow S)}}{(R \Rightarrow S), R, (Q \Rightarrow S) \to S} \qquad (b)$$

De (a) y (b) deducimos lo siguiente:

$$\dfrac{\dfrac{\dfrac{\dfrac{(Q \Rightarrow S), Q, (R \Rightarrow S) \to S \quad ; \quad (R \Rightarrow S), R, (Q \Rightarrow S) \to S}{(Q \Rightarrow S), (R \Rightarrow S), (Q \vee R) \to S}}{(Q \Rightarrow S), (R \Rightarrow S) \to (Q \vee R \Rightarrow S)}}{(Q \Rightarrow S) \to (R \Rightarrow S) \Rightarrow (Q \vee R \Rightarrow S)}}{\to (Q \Rightarrow S) \Rightarrow ((R \Rightarrow S) \Rightarrow (Q \vee R \Rightarrow S))}$$
$$\to P$$

(7) $P = Q \Rightarrow Q \vee R$ construímos la siguiente deducción:

$$\dfrac{\dfrac{\dfrac{Q \to Q}{Q \to Q, R}}{Q \to (Q \vee R)}}{\to Q \Rightarrow (Q \vee R)}$$
$$\to P$$

(8) $P = R \Rightarrow Q \vee R$ es simétrica a la anterior.

(9) $P = \bot \Rightarrow Q$ se sigue debido a que $\bot \to Q$ es un axioma y por lo tanto se sigue $\to \bot \Rightarrow Q$

(10) $P = \forall x\, Q(x) \Rightarrow Q(x/t)$ damos la construcción:

$$\dfrac{\dfrac{\dfrac{Q(x/t) \to Q(x/t)}{\forall x\, Q(x), Q(x/t) \to Q(x/t)}}{\forall x\, Q(x) \to Q(x/t)}}{\to \forall x\, Q(x) \Rightarrow Q(x/t)}$$
$$\to P$$

(11) $P = \forall x (Q \Rightarrow R (x)) \Rightarrow (Q \Rightarrow \forall x R(x))$ construímos la deducción:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{Q \rightarrow Q \qquad\qquad R(x/t) \rightarrow R(x/t)}{(Q \Rightarrow R(x/t)),\ Q\ \forall x (Q \Rightarrow R(x)) \rightarrow Q \ ;\ R(x/t),\ Q\ \forall x (Q \Rightarrow R(x)) \rightarrow R(x/t)}}{(Q \Rightarrow R(x/t)),\ Q\ \forall x (Q \Rightarrow R(x)) \rightarrow R(x/t)}}{(Q \Rightarrow R(x/t)),\ Q\ \forall x (Q \Rightarrow R(x)) \rightarrow \forall x R(x)}}{Q\ \forall x (Q \Rightarrow R(x)) \rightarrow \forall x R(x)}}{\forall x (Q \Rightarrow R(x)) \rightarrow Q \Rightarrow \forall x R(x)}}{\rightarrow \forall x (Q \Rightarrow R(x)) \Rightarrow (Q \Rightarrow \forall x R(x))}}{\rightarrow P}$$

(12) $P = Q(x/t) \Rightarrow \exists x\, Q(x)$ construímos:

$$\dfrac{\dfrac{\dfrac{\dfrac{Q(x/t) \rightarrow Q(x/t)}{Q(x/t) \rightarrow Q(x/t)\ \exists x\, Q(x)}}{Q(x/t) \rightarrow \exists x\, Q(x)}}{\rightarrow Q(x/t) \Rightarrow \exists x\, Q(x)}}{\rightarrow P}$$

(13) $P = \forall x (Q(x) \Rightarrow R) \Rightarrow (\exists x\, Q(x) \Rightarrow R)$ construímos:

$$\dfrac{\dfrac{Q(x/t) \rightarrow Q(x/t)}{Q(x/t)\ (Q(x/t) \Rightarrow R)\ \forall x (Q(x) \Rightarrow R) \rightarrow Q(x/t)}}{(Q(x/t) \Rightarrow R)\ \forall x (Q(x) \Rightarrow R)\ \exists x\, Q(x) \rightarrow Q(x/t)} \qquad (a)$$

Por otra parte:

$$\dfrac{R \rightarrow R}{R\ \forall x (Q(x) \Rightarrow R)\ \exists x\, Q(x) \rightarrow R} \qquad (b)$$

Entonces de (a) y (b) deducimos:

$$\dfrac{\dfrac{\dfrac{\forall x (Q(x) \Rightarrow R)\ (Q(x/t) \Rightarrow R)\ \exists x\, Q(x) \rightarrow R}{\forall x (Q(x) \Rightarrow R)\ \exists x\, Q(x) \rightarrow R}}{\forall x (Q(x) \Rightarrow R) \rightarrow \exists x\, Q(x) \Rightarrow R}}{\rightarrow \forall x (Q(x) \Rightarrow R) \Rightarrow (\exists x\, Q(x) \Rightarrow R)}}{\rightarrow P}$$

De lo anterior tenemos que para axiomas es válida la proposición.

Ahora veamos que es válido si se obtuvo P de una regla de inferencia:

(a) Si se obtuvo por *modus ponens* :

Supongamos que las secuencias $\rightarrow Q$ y $\rightarrow (Q \Rightarrow P)$ se pueden deducir, entonces veamos la siguiente deducción:

$$\dfrac{\dfrac{\dfrac{}{Q \rightarrow Q} \quad \dfrac{}{P \rightarrow P}}{(Q \Rightarrow P)\, Q \rightarrow Q} \quad \dfrac{}{Q\, P \rightarrow P}}{(Q \Rightarrow P)\, Q \rightarrow P} \qquad (a)$$

Entonces (a) es deducible. Ahora bien:

$$\dfrac{\rightarrow (Q \Rightarrow P) \quad ; \quad (Q \Rightarrow P)\, Q \rightarrow P}{Q \rightarrow P} \qquad \text{(aplicando un corte)}$$

$$\dfrac{\rightarrow Q \quad ; \quad Q \rightarrow P}{\rightarrow P} \qquad \text{(aplicando otro corte).}$$

De lo anterior se tiene lo deseado.

(b) Si se obtuvo por *generalización* :

Supongamos que la secuencia $\rightarrow Q$ entonces tenemos:

$$\dfrac{\dfrac{\dfrac{\rightarrow Q}{\rightarrow Q(y)}}{\rightarrow \forall x\, Q}}{\rightarrow P}$$

De todo lo anterior se tiene el resultado.

■

Ahora, con los lemas 3.1.1 - 3.1.8, es facil establecer la segunda parte del teorema 3.1 y terminar la demostración. Veámoslo:

Supongamos que S^{Φ} es deducible en **HPC** . Por inducción con respecto a la construcción de S^{Φ} :
El resultado se tiene por el lema 3.1.8 quitando a todas las deducciones el último paso, entonces se tiene que si S^{Φ} se obtuvo por una regla de inferencia ó es un axioma se obtiene que S es deducible en **GHPC** .
Esto basta para tener el resultado.

■

La remarcable simetría del sistema **GHPC** nos facilita obtener el siguiente resultado en el cálculo de predicados intuicionista:

Proposición *3.2 : Sea P una fórmula atómica. Entonces las fórmulas* $P \vee \neg P$ *y* $\neg\neg P \Rightarrow P$ *no son deducibles en* ***HPC.***

Demostración:

Para la primera, supongamos que $P \vee \neg P$ es deducible en **HPC**, entonces la secuencia $\rightarrow (P \vee \neg P)$ es deducible en **GHPC** , y esta secuencia sólo puede provenir de $\rightarrow P \neg P$ y como $\neg P \equiv P \Rightarrow \perp$, esta sólo puede provenir de $P \rightarrow \perp$ la cual claramente no es deducible en **GHPC** . Por lo tanto $P \vee \neg P$ no puede ser deducible en **HPC** .

Ahora, si suponemos que $\neg\neg P \Rightarrow P$ es deducible en **HPC** sucede algo semejante. La secuencia $\rightarrow \neg\neg P \Rightarrow P$ es deducible en **GHPC**, esta sólo puede provenir de la secuencia $\neg\neg P \rightarrow P$, ahora, como $\neg\neg P \equiv \neg P \Rightarrow \perp$, esta última secuencia sólo puede provenir de $(\neg P \Rightarrow \perp) \rightarrow \neg P$ y de $\perp \rightarrow P$ la cual si es un axioma.
Ahora, si aplicamos la misma regla $(\Rightarrow \rightarrow)$ a $(\neg P \Rightarrow \perp) \rightarrow \neg P$ caemos en algo semejante, por lo tanto sólo pudo provenir de aplicarse la regla $(\rightarrow \Rightarrow)$, con lo cual proviene de $\neg\neg P \; P \rightarrow \perp$. Si seguimos intentando retroceder una deducción nos encontramos con un círculo que proviene de esta última secuencia, y esta no es un axioma. Por lo tanto no es deducible en **GHPC**. Entonces concluímos que $\neg\neg P \Rightarrow P$ no puede ser deducible en **HPC** .

■

CAPITULO 4.

GRUPOS.

El álgebra intuicionista es más complicada que el álgebra clásica en varios sentidos; para empezar, las estructuras algebraicas como regla no conllevan una relación de igualdad decidible. Esta dificultad es en parte evitada al introducir una relación de desigualdad fuerte, la llamada *relación* de *separabilidad.* Además existen varios tipos de subestructuras difíciles de manejar, y por esta razón de estructuras cociente.

En la sección 1 rapidamente trataremos las propiedades básicas de la igualdad, separabilidad y orden.

En la seccion 2 entraremos a la teoría de grupos con separabilidad.

1. IDENTIDAD, SEPARABILIDAD Y ORDEN.

Identidad. En la matemática clásica la relación identidad es completamente neutral ya que, ni influencia ni es influenciada por las propiedades matemáticas. Similarmente su papel en la lógica clásica es modesta: todo lo que podemos hacer es agregar condiciones de cardinalidad.

La situación es completamente diferente en la matemática intuicionista, en donde la naturaleza y construcción de los objetos determina propiedades específicas de la relación identidad.

Por ejemplo la relación identidad en los números naturales es, por su construcción, decidible, y el método de construcción de los números reales conlleva la estabilidad de su relación identidad, así la matemática influencia las propiedades de la relación identidad.

En lo siguiente usaremos *identidad* e *igualdad* como sinónimos.

La mínima teoría de *identidad* tiene los axiomas:

REFL $(x = x)$
SYM $(x = y) \Rightarrow (y = x)$
TRANS $(x = y) \wedge (y = z) \Rightarrow (x = z)$

Y si existen funciones u otras relaciones con $=$ requerimos del axioma de reemplazamiento:

Para toda propiedad *A*:

REPL $(x = y) \Rightarrow (A[z/x] \Rightarrow A[z/y])$

SYM y **TRANS** se siguen de **REFL** en la presencia de **REPL**.

Demostración: Si tomamos $A(x) := (x = t)$, $A(t)$ es verdadera por REFL; así de $A(t) \wedge (t = s) \Rightarrow A(s)$ es decir tenemos $(t = s) \Rightarrow (s = t)$ esto para cualesquiera términos t y s.

También tomando $A(x) := (x = r)$ encontramos que:

$A(r)$ se tiene por **REFL**. Supongamos que $t = r \wedge t = s$

entonces: $t = r \wedge A(r) \Rightarrow A(t)$
$t = s \wedge A(t) \Rightarrow A(s)$ es decir $s = r$

■

Las propiedades más familiares de *identidad* en la práctica matemática son:

Estabilidad $\neg\neg (x = y) \Rightarrow (x = y)$
Decidibilidad $(x = y) \vee (x \neq y)$

La igualdad en **N, Z, Q**, es decidible y en **R** y **C** es estable.

Separabilidad. La segunda relación más importante en matemáticas es la de separabilidad, una fuerte noción de desigualdad. Las propiedades básicas son:

AP1 $\neg (x \# y) \Leftrightarrow (x = y)$
AP2 $(x \# y) \Rightarrow (y \# x)$
AP3 $(x \# y) \Rightarrow (x \# z) \vee (y \# z)$

EJEMPLO: En los números reales se define:

$$x \# y := (x < y) \vee (y < x)$$

Proposición 4.1 *: Sea A un conjunto con una igualdad decidible, entonces la relación* $\neq$ *es una relación de separabilidad.*

Demostración: Supongamos que $(\forall x, y)\ (x = y \vee x \neq y)$ entonces:

$\neg (x \neq y) \Rightarrow (x = y)$ y por otro lado se tiene que $(x = y) \Rightarrow \neg (x \neq y)$ por lo cual se tiene **AP1.**

$(x \neq y) \Rightarrow \neg (x = y) \Rightarrow \neg (y = x) \Rightarrow (y \neq x)$ y por lo tanto se tiene **AP2.**

Para **AP3** supongamos que $(x \neq y)$ y sea $z \in A$ entonces:

a) supongamos $\neg (x \neq z) \Rightarrow (x = z) \Rightarrow \neg (z = y) \Rightarrow (z \neq y)$
b) supongamos $\neg (y \neq z) \Rightarrow (y = z) \Rightarrow \neg (x = z) \Rightarrow (x \neq z)$ por tanto **AP3** se tiene.

■

Por otro lado la relación de separabilidad influencia la relación identidad:

$$\neg\neg (x = y) \Leftrightarrow \neg\neg\neg (x \# y) \Leftrightarrow \neg (x \# y) \Leftrightarrow (x = y)$$

De aquí una estructura con una relación de separabilidad posee una igualdad estable.

En ciertas circunstancias hay un uso para una clase más débil de relación de separabilidad, una con **AP1** reemplazado por $\neg$ (x # x) llamada *preseparabilidad.*

Como fue observado por Fourman, un conjunto con una relación de separabilidad usualmente tiene más de una:

EJEMPLO: Sea A una proposición tal que $\neg\neg A$ sea válida, y definamos: $x \#_A y := ((x \# y) \wedge A)$ entonces $\#_A$ es una relación de separabilidad.

Demostración:

AP1) Supongamos $\neg (x \#_A y)$ es decir $((x \# y) \wedge A)$ ahora si $(x \# y)$ entonces $\neg\neg (x \# y)$ y como $\neg\neg A$ esta dada, se infiere que: $\neg\neg ((x \# y) \wedge A)$, que es una contradicción, así que $\neg (x \# y)$ y por lo tanto $(x = y)$ de **AP1**.

AP2) Supongamos $(x \#_A y)$ entonces $((x \# y) \wedge A)$ como: $(x \# y) \Rightarrow (y \# x)$ se sigue que $((y \# x) \wedge A)$ es decir $(y \#_A x)$

AP3) Supongamos $(x \#_A y)$ y sea z entonces por **AP3** se tiene que $(x \# z \vee y \# z) \wedge A$ por lo tanto $((x \# z) \wedge A) \vee ((y \# z) \wedge A)$ es decir se tiene $(x \#_A z) \vee (y \#_A z)$

■

La relación de separabilidad en X y Y determinan relaciones de separabilidad en el producto cartesiano y en la exponenciación.

Proposición *4.2 :* (i) *Si X y Y son conjuntos con relación de separabilidad $\#_X$ y $\#_Y$ respectivamente entonces $X \times Y$ tiene la relación de separabilidad canónica $\#_{X \times Y}$ dada por:*

$$(x,y) \#_{X \times Y} (x',y') := x \#_X x' \vee y \#_Y y'.$$

(ii) *Si X es un conjunto con relación de separabilidad $\#$ entonces X^Y posee la relación de separabilidad canónica:*

$$f \#' g := (\exists x)(f(x) \# g(x)).$$

Demostración:

(i) Demostremos **AP1**: Supongamos $\neg((x,y) \#_{X\times Y} (x',y'))$ entonces $\neg((x \#_X x') \vee (y \#_Y y'))$ por lo tanto $\neg(x \#_X x') \wedge \neg(y \#_Y y')$ esto implica que $(x = x') \wedge (y = y')$

$$\therefore (x,y) = (x',y').$$

Para demostrar **AP2** supongamos $(x,y) \#_{X\times Y} (x',y')$ entonces $(x \#_X x') \vee (y \#_Y y')$ que implica $(x' \#_X x) \vee (y' \#_Y y)$ por lo tanto se tiene lo deseado.

Para **AP3** supongamos $(x,y) \#_{X\times Y} (x',y')$ y sea (z,z') en $X \times Y$ entonces tenemos que de $(x \#_X x')$ se sigue $(x \#_X z \vee x' \#_X z)$ y de $(y \#_Y y')$ se sigue $(y \#_Y z' \vee y \#_Y z')$ de donde tenemos:

$$(x \#_X z) \vee (y \#_Y z') \vee (x' \#_X z) \vee (y' \#_Y z')$$

$$\therefore (x,y) \#_{X\times Y} (z, z') \vee (x',y') \#_{X\times Y} (z,z').$$

(ii) Para **AP1** supongamos $\neg(f \#' g)$ es decir que:
$\neg(\exists x)(f(x) \# g(x)) \equiv (\forall x) \neg(f(x) \# g(x))$ entonces si tomo x tenemos que :

$$\neg(f(x) \# g(x)) \Leftrightarrow f(x) = g(x) \Rightarrow (\forall x)(f(x) = g(x))$$

$$\therefore f = g.$$

Para **AP2** supongamos que $f \#' g$ es decir $(\exists x)(f(x) \# g(x))$ que implica $(\exists x)(g(x) \# f(x))$

$$\therefore g \#' f.$$

Para **AP3** supongamos que $f \#' g$ y sea $h: Y \to X$ entonces:
$(\exists x)(f(x) \# g(x))$ sea $t \in Y$ tal que $f[x/t] \# g[x/t]$ y tomemos $h[x/t]$ entonces:

$$(f[x/t] \# h[x/t] \vee g[x/t] \# h[x/t])$$
$$\Rightarrow (\exists x)(f(x) \# h(x)) \vee (\exists x)(g(x) \# h(x))$$

$$\therefore f \#' h \vee g \#' h.$$

■

Existe una condición natural en la relación identidad: objetos idénticos tienen las mismas propiedades (Leibniz). ¿Hay también una condición natural con respecto a la relación de separabilidad?
La primera que viene a la mente concierne a las funciones: si una función toma dos objetos a dos objetos que estan apartados entonces ellos debían haber estar apartados en primer lugar. El principio parece muy plausible pero si uno no conoce cuando dos objetos estan apartados, entonces no se puede (hablando extensionalmente) agudamente distinguirlos. Pero entonces uno no podría esperar distinguir agudamente entre sus imagenes.

Definición 4.3: *Una propiedad (o conjunto) A es llamada extensional si* $x = y$ *implica* $A(x) = A(y)$ *(es decir A satisface* **REPL** *).*

En la práctica estamos siempre trabajando con tales entes.

En la matemática clásica uno puede reformular la condición de reemplazamiento como sigue: $B(x) \Rightarrow (x \neq y \vee B(y))$. Esta formulación sugiere la siguiente condición intuicionista. $B(x) \Rightarrow (x \# y \vee B(y))$. Pero no todo conjunto tiene esta propiedad, considere por ejemplo: $B = \{0\} \subseteq \mathbf{R}$; nosotros no tenemos $(\forall y)(0 \# y \vee 0 = y)$.

Definición 4.4: *(i)* X *es fuertemente extensional si :*

$$(\forall x,y)(x \in X \Rightarrow x \# y \vee y \in X).$$

(ii) $f : X \to Y$ *es fuertemente extensional si :*

$$\{(x,y) \mid f(x) \# y\} \text{ lo es.}$$

Por lo tanto un conjunto o una relación *fuertemente extensional* (**FE**) tiene más bien características exclusivas; o estas en él o estas positivamente distinto de todos sus miembros.

EJEMPLOS:

(1) Sea $X = \{x \in \mathbf{R} \mid x \# 0\}$ entonces X es **FE.**
sea $a \in X$ es decir $x \# 0$ entonces $(\forall b)(b \# a \vee b \# 0)$ por **AP3.**

(2) # en X como una propiedad de parejas es FE.

sea $A := \{ (x,y) \in X \times X \mid x \# y \}$ y sea $(x \# y)$ entonces para cualquier (u,v), $(u \# x) \vee (u \# y)$ y por lo tanto $(u \# x \vee u \# v \vee v \# y)$ lo cual nos lleva a:

$$(u,v) \in A \vee (u,v) \# (x,y).$$

(3) La adición en R es FE.

sea $P := \{ (x,y,z) \in R^3 \mid x+y \# z \}$ y sea $(x+y \# z)$ entonces para cualquier (u,v,w), $(u+v,w) \# (x+y,z)$ ó $(u+v \# w)$ aplicando el ejemplo dos.

Ahora $(u+v \# x+y)$ implica $(u \# x \vee v \# y)$ (ver nota abajo), así que $(u+v,w) \# (x+y,z)$ que es equivalente a $(u,v,w) \# (x,y,z)$.

$$\therefore (u,v,w) \# (x,y,z) \vee (u,v,w) \in P.$$

NOTA: Para los números reales se puede demostrar que pasan las siguientes tres propiedades: (i) $(x \# y) \Rightarrow (x + z) \# (y + z)$

(ii) $(x + y \# 0) \Rightarrow (x \# 0) \vee (y \# 0)$

(iii) $(x \cdot y = 1) \Rightarrow (x \# 0) \wedge (y \# 0)$

■

La propiedad FE para funciones puede ser formulado de una manera más adecuada.

Proposición 4.5: *$f \in Y^X$ es FE $\Leftrightarrow$ $(\forall x,x')(f(x) \# f(x') \Rightarrow x \# x')$.*

Demostración:

($\Rightarrow$) Sean $F = \{ (x,y) \mid f(x) \# y \}$ y $f(x) \# f(x')$.
$(x,f(x')) \in F$ así que $(x',f(x')) \in F \vee (x,f(x')) \# (x',f(x'))$ por ser F FE.
entonces de la definición de F se sigue inmediatamente que $x \# x'$ ya que $(x',f(x'))$ no se da.

($\Leftarrow$) Sea F como antes y $(x,y) \in F$ es decir $f(x) \# y$ entonces para cualquier (x',y') tenemos $f(x') \# f(x) \vee f(x') \# y$ ya que $f(x) \# y$ esto nos lleva a que $(x \# x') \vee (f(x') \# y') \vee (y' \# y)$

$$\therefore (x',y') \in F \vee (x,y) \# (x',y').$$

■

Proposición 4.6: *(i) La clase de los conjuntos fuertemente extensionales es cerrado bajo uniones e intersecciones.*

(ii) Sea $f \in A \to B$ fuertemente extensional. Si $X \subseteq B$ es fuertemente extensional, entonces también lo es $f^{-1}[X]$.

Demostración:

(i) (a) Sea Y un conjunto. Tomemos la familia $\cup_{i \in Y}(X_i)$ donde cada X_i es FE. Sean u, w donde $u \in \cup_{i \in Y}(X_i)$.
entonces $u \in X_j$ para alguna $j \in Y$. Entonces $w \in X_j \vee u \# w$ por ser X_j FE.

$$\therefore w \in \cup_{i \in Y}(X_i) \vee u \# w$$

(i) (b) Sea ahora $\cap_{i \in Y}(X_i)$. Y sean u, w con $u \in \cap_{i \in Y}(X_i)$ entonces $u \in X_j$ para toda $j \in Y$. Entonces $u \# w \vee w \in X_j$ para toda $j \in Y$.

$$\therefore u \# w \vee w \in \cap_{i \in Y}(X_i).$$

(ii) Sea $f \in A \to B$ fuertemente extensional y $X \subseteq B$.
Tomemos u, w con $u \in f^{-1}[X]$ entonces $f(u) \in X$.

$$\therefore f(w) \in X \vee f(u) \# f(w) \text{ por ser X FE.}$$

Pero también se tiene $f(u) \# f(w) \Rightarrow u \# w$ por ser f FE.

$$\therefore f(w) \in X \vee u \# w. \text{ Es decir: } w \in f^{-1}[X] \vee u \# w.$$

■

Orden. El tratamiento de las varias nociones de orden difiere del clásico en que, en las matemáticas clásicas, los órdenes *reflexivo* e *irreflexivo* estan interdefinidos. Aquí tenemos que tratarlos por separado.

Definición 4.7: *Un orden parcial* $\leq$ *satisface los siguientes axiomas:*

TRANS $(x \leq y) \wedge (y \leq z) \Rightarrow (x \leq z)$.
ANTIS $(x \leq y) \wedge (y \leq x) \Leftrightarrow (x = y)$.

Para introducir un orden parcial positivo irreflexivo uno debería tener que introducir una relación de separabilidad y entonces poner:

$$x < y := (x \leq y) \wedge (x \# y)$$

En general uno no puede introducir tal relación de orden positivo. Considere por ejemplo el orden parcial de la inclusión de subconjuntos de un conjunto dado: el subconjunto no conlleva una relación de separabilidad, deja solitario un ordenamiento parcial positivo.

La teoría de orden total esta formulada en términos de *menor* más que en *menor o igual*. Debido a que queremos considerar ordenes lineales no solo sobre conjuntos decidibles, nosotros desechamos la tricotomía y la reemplazamos por comparabilidad.

Definición 4.8: *Los axiomas de orden total son:*

1) $(x < y) \wedge (y < z) \Rightarrow (x < z)$ ***TRANS***
2) $\neg ((x < y) \vee (y < z)) \Leftrightarrow (x = y)$ ***ASIM***
3) $(x < y) \Rightarrow (x < z) \vee (z < y)$ ***COMP***

De los axiomas inmediatamente deducimos lo siguiente:

Proposición 4.9: *Para cualquier orden total* $<$ *:*

(i) $\neg (x < x)$
(ii) $(x < y) \vee (y < x)$ *es una relación de separabilidad.*

Demostración:

(i) $(x = x) \Leftrightarrow \neg (x < x \vee x < x) \Rightarrow \neg (x < x) \wedge \neg (x < x)$
$\Rightarrow \neg (x < x)$

(ii) **AP1** se tiene por asimetría.
Para **AP2** $(x<y) \vee (y<x) \Rightarrow (y<x) \vee (x<y)$.
Para **AP3** supongamos que $(x<y) \vee (y<x)$ y sea z entonces aplicando comparabilidad se tiene:
$(x<y) \Rightarrow (x<z) \vee (z<y)$ y $(y<x) \Rightarrow (y<z) \vee (z<x)$ estos implican que:

$$(x<z) \vee (z<y) \vee (y<z) \vee (z<x)$$

■

En el contexto de elementos parciales y el predicado de existencia tenemos que reformular las propiedades de identidad, separabilidad y orden en E-lógica con igualdad.

Cada una de las relaciones básicas $=, \#, <$, se asume que son estrictas, es decir:

$s=t \Rightarrow Es \wedge Et$
$s\#t \Rightarrow Es \wedge Et$
$s<t \Rightarrow Es \wedge Et$

Los axiomas de separabilidad y orden tienen que ser complementados de la manera obvia. Para completar las mencionamos ahora.
$t\#s \Rightarrow s\#t$
$Es \wedge (t\#t') \Rightarrow (s\#t) \vee (s\#t')$
$Es \wedge Et \wedge \neg(s\#t) \Leftrightarrow s=t$
$t<t' \wedge t'<t'' \Rightarrow t<t''$
$Es \wedge Et \wedge \neg(s<t \vee t<s) \Leftrightarrow s=t$
$Es \wedge (t<t') \Rightarrow (t<s) \vee (s<t')$.

2. GRUPOS.

Las operaciones básicas de un grupo, producto e inverso, son ambas totales, es decir $Es \wedge Et \Rightarrow Es\cdot t$ y $Es \Rightarrow Es^{-1}$.

Así, si comenzamos con elementos existentes el producto y el inverso nos darán elementos existentes. Por lo tanto no hay una objeción inmediata en manejar la teoría de grupos con un lenguaje sin predicado de existencia. Sin embargo, los grupos con elementos parciales son perfectamente legítimos; no obstante, dejaremos el predicado de existencia por el momento.

***Definición** 4.10 : Un grupo es una estructura $(A, \cdot, ^{-1}, e)$ que satisface los siguientes axiomas:*

1) $x \cdot e = e \cdot x = x$
2) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
3) $x \cdot x^{-1} = x^{-1} \cdot x = e$

El grupo es abeliano si satisface:

4) $x \cdot y = y \cdot x$

Un grupo con una relación de separabilidad tiene el producto y el inverso estrictamente extensional, es decir que, además de AP1, AP2 y AP3 cumple que:

5) $(x \cdot y) \# (x' \cdot y') \Rightarrow (x \# x') \vee (y \# y')$
6) $x^{-1} \# y^{-1} \Rightarrow x \# y$

De aquí en adelante escribiremos xy en vez de $x \cdot y$ para señalar el producto en el grupo.

***Proposición** 4.11 : En un grupo con una relación de separabilidad tenemos que:*

(i) $xy \# e \Rightarrow (x \# e) \vee (y \# e)$

(ii) $x \# x' \Rightarrow (yx \# yx') \wedge (xy \# x'y)$
(iii) $x \# y \Rightarrow x^{-1} \# y^{-1}$

Demostración:

(i) Supongamos que $xy \# e$ tenemos que $e = ee$ por (1) por lo tanto
$xy \# ee$ y tenemos que $(x \# e) \vee (y \# e)$ por (5).

(ii) Supongamos que $x \# x'$, como $y^{-1}y = e$ tenemos que:
$(yy^{-1})\, x \# (yy^{-1})\, x' \Rightarrow y^{-1}(yx) \# y^{-1}(yx') \Rightarrow (y^{-1} \# y^{-1}) \vee (yx \# yx')$
$\Rightarrow (yx \# yx')$ debido a que $(y^{-1} \# y^{-1})$ no se da.
Analogamente se tiene que $(xy \# x'y)$.

(iii) Tenemos que $(x^{-1})\,(x^{-1})^{-1} = e = (x^{-1})\, x \Rightarrow (x^{-1})^{-1} = x$
entonces tenemos que: $x \# y \Rightarrow (x^{-1})^{-1} \# (y^{-1})^{-1} \Rightarrow x^{-1} \# y^{-1}$.

■

***Lema** 4.12 : En la definición 4.10, (6) se tiene de (5).*

Demostración:

Supongamos $x^{-1} \# y^{-1}$ entonces por el inciso (ii) de la proposición anterior se tiene: $x^{-1} \# y^{-1} \Rightarrow xx^{-1} \# xy^{-1} \Rightarrow e \# xy^{-1} \Rightarrow y \# xy^{-1}y$
$\Rightarrow y \# x \Rightarrow x \# y$.

■

La parte computacional de la teoría de grupos, es decir, la verificación de relaciones entre palabras no presenta ningún nuevo problema cuando se compara con la teoría clásica de los grupos. Hablando matematicamente la teoría de grupos constructiva comienza a diverger considerablemente de su contraparte clásica cuando tomamos en cuenta nociones como la de subgrupo, grupo cociente etc.

Una mayor razón para la divergencia de la matemática intuicionista de la matemática clásica es el comportamiento inusual de conjuntos de objetos en la ausencia del principio del tercer excluído y en las peculiaridades de las sucesiones de elección. En álgebra el primer fenómeno es de considerable importancia. La presencia de subgrupos extraños, aún en grupos finitos nos llevan a dificultades inesperadas.

Uno podría estar tentado a eliminar el aspecto de segundo orden por completo en vez de los conceptos de primer orden, pero esto es más bien un proyecto quimérico en vista de la importancia de homomorfismos, núcleos, etc. Además una parte considerable de las nociones tradicionales y técnicas pueden ser salvadas.

Veámos los siguientes EJEMPLOS:

1) Sea $(\mathbf{Z}^2, \cdot, ^{-1}, 0)$ que es un grupo, y definamos al subgrupo:
$G := \{ (a,b) \mid b = 0 \vee A \}$ donde A es una proposición no decidible. G es un buen subgrupo, pero nosotros no sabemos cuando $G = \mathbf{Z}^2$ o $G \cong \mathbf{Z}$. Note que no tenemos $(\forall x) \in \mathbf{Z}^2 \; (x \in G \vee x \notin G)$ es decir que G no es un subgrupo removible.

2) Para añadir una restricción de removibilidad no es necesario ir tan lejos, como el siguiente ejemplo lo muestra:
$\{ (x,0) \mid x \in \mathbf{R} \}$ es un subgrupo de $\mathbf{R}^2$, pero no es removible. Sin embargo es uno de los ejemplos más naturales en los que podemos pensar.

ANTI-SUBGRUPOS, SUBGRUPOS:

La maquinaria de subgrupos que presentaremos esta dada en una especie de término *dual* en analogía a la relación *separabilidad - igualdad.* Mostramos una noción positiva que nos permita algunos refinamientos no encontrados en la teoría tradicional.

Definición *4.13 : Un anti-subgrupo A de un grupo G en un subconjunto de G con las siguientes propiedades:*

$$(i)\quad \neg e \in A$$
$$(ii)\quad xy \in A \Rightarrow x \in A \vee y \in A$$
$$(iii)\quad x^{-1} \in A \Rightarrow x \in A.$$

El anti-subgrupo es normal si satisface:

$$(iv)\quad xy \in A \Rightarrow yx \in A.$$

El anti-subgrupo es compatible con la separabilidad de G si:

$$(v)\quad a \in A \Rightarrow a \# e.$$

EJEMPLOS:

1) $A := \{ x \in \mathbf{Z} \mid \neg (2 \mid x) \}$ es un anti-subgrupo de Z.
   (i) es evidente que $0 \notin A$.
   (ii) se tiene del hecho de que $\neg (2 \mid (x + y)) \Rightarrow \neg (2 \mid x) \vee \neg (2 \mid y)$.
   (iii) se tiene porque $2 \mid x \Leftrightarrow 2 \mid -x$.

2) $A := \{ x + iy \mid y \# 0 \}$ es un anti-subgrupo del grupo aditivo de C.

3) El subconjunto del grupo de matrices de 2 x 2 de la forma:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

con $c \# 0 \vee b \# 0 \vee a \# d$. Es un anti-subgrupo normal de $GL_2(R)$.

Demostración:

(i) La matriz de ceros no está en A porque:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\neg (0 \# 0) \wedge a \# d \Rightarrow 0 \# a \vee 0 \# d$ por la proposición 4.11 inciso (i).

(ii) Si

$$\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

entonces $(a+a' \# d+d') \vee (c+c' \# 0) \vee (b+b' \# 0)$

$\Downarrow \qquad \Downarrow \qquad \Downarrow$

$a \# d \vee a' \# d' \qquad c \# 0 \wedge c' \# 0 \qquad b \# 0 \wedge b' \# 0$

(por (v) en la definición 4.10) (por la proposición 4.11)

(iii) Si $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ está en A

entonces $-c \# 0 \Rightarrow c \# 0$, $-b \# 0 \Rightarrow b \# 0$ y $-a \# -d \Rightarrow -a + d \# 0$

$\Rightarrow -a \# 0 \wedge d \# 0 \Rightarrow a \# 0 \wedge -d \# 0 \Rightarrow a - d \# 0$

$\Rightarrow a \# d.$

(iv) $xy \in A \Rightarrow yx \in A$ se tiene por la conmutatividad en R.

Proposición *4.14: Sea A un anti-subgrupo de G. A^c satisface:*

(i) $e \in A^c$.
(ii) $x \in A^c \wedge y \in A^c \Rightarrow xy \in A^c$.
(iii) $x \in A^c \Rightarrow x^{-1} \in A^c$.
(iv) $\neg\neg\, x \in A^c \Rightarrow x \in A^c$.

Demostración:

(i) obvio.

(ii) Supongamos que $x \in A \wedge y \in A$. Tenemos que si $xy \in A$ entonces $x \in A$ o $y \in A$. $\therefore \neg (x \in A \vee y \in A) \Rightarrow \neg (xy) \in A$ y esto implica que:

$$(x \in A^c \wedge y \in A^c) \Rightarrow xy \in A^c.$$

(iii) El mismo razonamiento que en (ii).

(iv) $\neg\neg x \in A^c \Rightarrow \neg x \in A \Rightarrow x \in A^c$.

■

OBSERVACION: (i) (ii) y (iii) son exactamente las que definen un subgrupo. Decimos que A^c es el subgrupo determinado por A.

Proposición 4.15: *(i) A es un anti-subgrupo normal*

$$\Leftrightarrow (yxy^{-1} \in A \Rightarrow x \in A)$$
$$\Leftrightarrow (x \in A \Rightarrow yxy^{-1} \in A)$$

(ii) Si A es un anti-subgrupo normal entonces A^c en subgrupo normal es decir $x \in A^c \Rightarrow yxy^{-1} \in A^c$.

Demostración: Sea A un anti-subgrupo normal:

(i)

a) ($\Rightarrow$) Supongamos que $yxy^{-1} \in A \Rightarrow (yx)y^{-1} \in A$
$\Rightarrow y^{-1}(yx) \in A$
$\Rightarrow (y^{-1}y)x \in A$
$\Rightarrow x \in A.$

($\Leftarrow$) Supongamos que $xy \in A \Rightarrow (y^{-1}y)xy \in A$
$\Rightarrow y^{-1}(yx)y \in A$
$\Rightarrow yx \in A.$

b) Se tiene utilizando el mismo método.

(ii) Supongamos que $x \in A^c$ entonces $\neg\, x \in A$
Tenemos por (i) que $(yxy^{-1} \in A \Rightarrow x \in A)$ y esto implica lógicamente que $(\neg\, x \in A \Rightarrow \neg\, yxy^{-1} \in A)$

$$\therefore \neg\, yxy^{-1} \in A \equiv yxy^{-1} \in A^c.$$

■

Nota: Usaremos libremente resultados no problemáticos del álgebra tradicional y conceptos, y se comentará cuando sea necesario en aspectos constructivos.

GRUPOS COCIENTE, HOMOMORFISMOS.

Sea D un subgrupo normal, D define una relación de equivalencia ~ sobre G:

$$a \sim b := a^{-1}b \in D.$$

La clase de equivalencia de a es el conjunto de representantes de la clase $aD = \{ ax \mid x \in D \}$. La multiplicación de clases está definida por medio de sus elementos representantes: $(aD) \cdot (bD) = abD$. la cual como sabemos está bien definida.

Las clases de equivalencia forman un grupo G/ D cuyo elemento neutro es D e inverso $(aD)^{-1} = a^{-1}D$.

En el caso de que D sea un subgrupo normal determinado por un anti-subgrupo normal *A* sabemos más.

Proposición 4.16: *Sea A un anti-subgrupo normal, y $D = A^c$, entonces G / D es un grupo con una relación de separabilidad canónica definida por:*

$$aD \# bD := ab^{-1} \in A.$$

Demostración:

(i) **AP1** se tiene porque: $\neg\, (aD \# bD) \Leftrightarrow \neg\, ab^{-1} \in A \Leftrightarrow ab^{-1} \in D \Leftrightarrow aD = bD.$

(ii) **AP2** se tiene porque: $aD \# bD \Leftrightarrow ab^{-1} \in A \Leftrightarrow ba^{-1} \in A \Leftrightarrow bD \# aD.$

(iii) **AP3** se tiene porque: $aD \# bD \Leftrightarrow ab^{-1} \in A \Leftrightarrow a(cc^{-1})b \in A$
$\Leftrightarrow (ac^{-1})(cb^{-1}) \in A \Rightarrow ac^{-1} \in A \vee cb^{-1} \in A$
$\Leftrightarrow aD \# cD \vee cD \# bD.$

(iv) La extensionalidad fuerte se tiene porque:
$adD \# cdD \Leftrightarrow (ab)^{-1}(cd) \in A \Leftrightarrow b^{-1}a^{-1}cd \in A$
$\Leftrightarrow a^{-1}c\, bd \in A$ (por ser normal) $\Rightarrow a^{-1}c \in A \vee bd \in A$
$\Leftrightarrow aD \# cD \vee bD \# dD.$

■

Definición 4.17: *(i) Un homomorfismo es un mapeo $\sigma: G_1 \to G_2$ tal que:*

$$\sigma(xy) = \sigma(x) \cdot \sigma(y)$$

(ii) σ es un isomorfismo si $\sigma(x) = \sigma(y) \Rightarrow x = y$.
y es un isomorfismo fuerte si además:

$$x \# y \Rightarrow \sigma(x) \# \sigma(y).$$

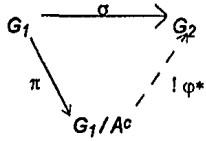
Si G_1 y G_2 tienen relaciones de separabilidad requeriremos que los homomorfismos sean fuertemente extensionales (**FE**).
Observación: (i) La preservación del producto no implica **FE**.

(ii) El mapeo canónico $G \to G/D$ que a un elemento lo manda a su clase es un homomorfismo y si el anti-subgrupo A es compatible con la separabilidad de G, entonces el mapeo canónico $G \to G/A^c$ es **FE**.

Demostración: $aD \# bD \Leftrightarrow ab^{-1} \in A \Leftrightarrow ab^{-1} \# e \Rightarrow a \# b.$

■

Teorema 4.18: *Si G_2 es un grupo con separabilidad y $\sigma: G_1 \to G_2$ es un homomorfismo entonces $A := \{x \in G_1 \,/\, \sigma(x) \# e_2\}$ es un anti-subgrupo normal y existe un único σ^* tal que el diagrama siguiente conmuta:*



Además σ^* es un isomorfismo fuerte sobre un subgrupo de G_2.

Demostración: Primero veamos las propiedades de anti-subgrupo normal.

(i) $e_1 \notin A$ debido a que $\sigma(e_1) = e_2$.

(ii) $ab \in A \Leftrightarrow \sigma(ab) \# e_2 \Leftrightarrow \sigma(a)\sigma(b) \# e_2 \Rightarrow \sigma(a) \# e_2 \vee \sigma(b) \# e_2$
$\Leftrightarrow a \in A \vee b \in A$

(iii) $x^{-1} \in A \Leftrightarrow \sigma(x^{-1}) \# e_2 \Leftrightarrow \sigma(x)^{-1} \# e_2 \Rightarrow \sigma(x) \# e_2 \Leftrightarrow x \in A$.

(iv) $xy \in A \Leftrightarrow \sigma(xy) = \sigma(x)\sigma(y) \# e_2$

Ahora definamos $\sigma^*(aA^c) := \sigma(a)$ entonces σ^* es un homomorfismo porque: $\sigma^*(aA^c\, bA^c) = \sigma^*(abA^c) = \sigma(ab) = \sigma(a)\sigma(b) = \sigma^*(aA^c)\,\sigma^*(bA^c)$

es isomorfismo porque: $\sigma^*(aA^c) = \sigma^*(bA^c) \Leftrightarrow \sigma(a) = \sigma(b)$
$\Leftrightarrow \sigma(a)\sigma(b)^{-1} = e_2 \Leftrightarrow \sigma(a)\sigma(b^{-1}) = e_2$
$\Leftrightarrow \sigma(ab^{-1}) = e_2$
$\therefore ab^{-1} \in A^c$ es decir $aA^c = bA^c$.

y es isomorfismo fuerte porque: si $aA^c \# bA^c$ entonces $ab^{-1} \in A$ así $\sigma(ab^{-1}) \# e_2$
$\therefore \sigma^*(aA^c) = \sigma(a) \# \sigma(b) = \sigma^*(bA^c)$.

La unicidad es debida a la manera en que se definió σ^*.

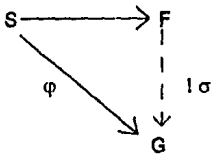
■

GRUPOS ABELIANOS LIBRES.

Ahora nos desviaremos un poco a discutir un tema específico de la teoría de grupos. El tema fue escogido para ilustrar el cuidado extra necesario en el manejo de objetos clásicamente triviales.

Consideremos la noción de grupo abeliano libre. Queremos un grupo libre F con el conjunto generador S que satisfaga la propiedad universal usual: Existe un mapeo canónico de S a F tal que para cada mapeo φ de S a un grupo G existe un único homomorfismo $\sigma : F \to G$.

Tal que el siguiente diagrama conmuta:



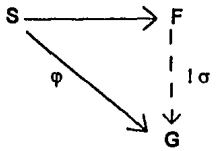
Supongamos por un momento que S es finito por ejemplo $S := \{ 1, \dots , k \}$. ¿Podríamos tomar para F a la suma directa usual $\mathbf{Z} \oplus \dots \oplus \mathbf{Z}$?. Recordemos que la suma directa $A \oplus B$ de dos grupos abelianos está definida como el producto cartesiano con las operaciones coordenada a coordenada. Introduciendo la definición estandard de σ trabaja aquí:

$$\sigma ((n_1, \dots , n_k)) = n_1 \varphi (1) + \dots + n_k \varphi (k).$$

¿Que haremos, sin embargo, cuando S no es un conjunto " *bonito* " ?.

Consideremos, por ejemplo, el conjunto $\{ a,b \}$ donde $a,b \in \mathbf{R}$ para los cuales es desconocido si son iguales o no.

Claramente no podemos definir un mapeo canónico de $\{a,b\}$ a $Z \oplus Z$ ni de $\{a,b\}$ a Z tal que el diagrama siguiente :



pueda ser obtenido.

Para el mapeo canónico deberíamos tener a priori la pregunta de la igualdad acerca de a y b.

En este caso tenemos que recurrir a la vieja construcción de un grupo libre (no necesariamente abeliano).

Sea A un conjunto. Formamos el conjunto A^* de todas las sucesiones finitas de elementos de A ; este es un paso que no tiene problema desde el punto de vista constructivo, incluímos la sucesión vacía ε ($:= <>$) en A^* (ejemplo: la función vacía de $\emptyset$ a A). En el caso de que A sea vacío entonces este es el único elemento de A^*. Como siempre $x * y$ se utiliza para la concatenación de x e y. Intuitivamente pensamos a las sucesiones finitas como elementos de un monoide abeliano sobre A.

Sin embargo como una alternativa a la notación de la adición usual usaremos a las sucesiones por ellas mismas . Normalmente reagrupamos a los elementos de una palabra (por ejemplo: (aabcabbac) en grupos iguales (aaaabbbcc).) pero ya que no podemos decidir igualdad este procedimiento no funciona.

Debido a que la conmutatividad (más asociatividad) nos permiten ignorar el orden de las palabras, la siguiente definición captura la noción abeliano.

Definición 4.19: *Sean* $\bar{a}$ *y* $\bar{a}'$ *palabras de longitudes* n *y* m *respectivamente entonces* $\bar{a} \sim \bar{a}'$ *si y solo si* $n = m$ *y existe una permutación* σ *de* $\{1, \ldots, n\}$ *tal que* $a'_i = a_{\sigma(i)}$ $(i \leq n)$.
Observe que $\varepsilon \sim \bar{a} \Leftrightarrow \bar{a} \equiv \varepsilon$

Lema 4.20 : *$\sim$ es una relación de congruencia con respecto a la concatenación.*

Demostración: Nota: Expresaremos las palabras sin su tilde

(a) Supongamos $a \sim a'$ y $b \sim b'$. Entonces, concatenando tenemos: $a * b$ y $a' * b'$

Si n es la longitud de a y a' y σ su permutación, y m la longitud de b y b' con σ'' su permutación entonces la longitud de $a * b$ y $a' * b'$ es la misma $n + m$ y la permutación que me sirve es σ de $n + m$ elementos tal que las restricciones a los primeros n elementos y a los restantes m, son σ' y σ'' respectivamente.

$\therefore\ a * b \sim a' * b'$

(b) El que $\sim$ sea una relación de equivalencia se tiene tomando:

i) σ como la identidad para ver que $a \sim a$.
ii) σ como σ^{-1} para ver que $a \sim b \Rightarrow b \sim a$
iii) σ como la composición de las permutaciones para ver que: $a \sim b$ y $b \sim c \Rightarrow a \sim c$

■

Recordemos que un monoide es una estructura $(A, \cdot, e)$ con una operación asociativa y un elemento neutral. Denotemos a la operación por $(+)$.

Lema 4.21 : *$A^* / \sim$ es un monoide abeliano libre sobre A.*

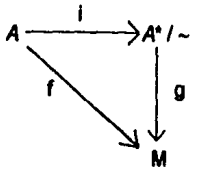
Demostración:

La adición en $A^* / \sim$ esta definida por $(\hat{a} / \sim) + (\hat{a}' / \sim) := (\hat{a} * \hat{a}' / \sim)$ el elemento neutral es $\varepsilon / \sim$. Por definición de $\sim$, la adición es conmutativa. Defina i por $i(a) = a / \sim$ y sea f un mapeo de A en un monoide abeliano M, como se muestra en el diagrama de la siguiente página.

Ahora pongamos $g(a/\sim) := f(a) \quad \forall a \in A$.
Extendemos g canonicamente a elementos arbitrarios de $A^*/\sim$ por:

$$g(<a_1, \ldots, a_n>/\sim) := g(a_1/\sim) \cdot \ldots \cdot g(a_n/\sim) \quad y \quad g(\varepsilon/\sim) := 0.$$

El diagrama conmuta por definición.



Para la unicidad de g, supongamos que h también hace el diagrama conmutativo, entonces:

$$h(i(a)) = f(a) \quad \forall a \in A, \text{ así } h(a/\sim) = f(a) = g(a/\sim).$$

$\therefore h = g$ debido a que h es homomorfismo.

■

Note que la demostración no asume nada de A ; A puede ser cualquier conjunto.

El siguiente paso es mapear al monoide abeliano libre sobre un grupo abeliano libre. El procedimiento es similar al de mapear $\mathbf{N}$ en $\mathbf{Z}$.

***Definición** 4.22 : Para un monoide abeliano libre M definimos:*

$$(u,v) \sim (u',v') := u + v' = u' + v$$

***Lema** 4.23 : $\sim$ es una relación de equivalencia en M^2.*

Demostración:

(i) $(u,v) \sim (u,v)$ ya que $u + v = u + v$.

(ii) $(u,v) \sim (u',v') \Rightarrow u + v' = u' + v \Rightarrow u' + v = u + v' \Rightarrow (u',v') \sim (u,v)$.

Antes de demostrar (iii) veamos que en un monoide abeliano libre es válida la cancelación:

Supongamos que $u/\sim + v/\sim = w/\sim + v/\sim$ entonces las longitudes de u y w son iguales y tomando σ como la restricción de la original a la longitud de u y w se tiene que $u/\sim = w/\sim$.

(iii) $(u,v) \sim (u',v') \Rightarrow u + v' = v + u'$
$(u',v') \sim (u'',v'') \Rightarrow u' + v'' = v' + u''$ entonces tenemos que:

$$u + v'' + v' = u + v' + v'' = v + u' + v'' = v + v' + u'' = v + u'' + v'$$

y como es válida la cancelación tenemos que: $u + v'' = v + u''$.

■

Definición 4.24 : *Sea M un monoide abeliano libre.*
Definimos: $G_M := \langle M^2/\sim, +, -, 0 \rangle$ *mediante las operaciones:*

(i) $(u,v)/\sim + (u',v')/\sim := (u + u', v + v')/\sim$
(ii) $-(u,v)/\sim := (v,u)/\sim$
(iii) $0 := (0,0)/\sim$.

Lema 4.25: *G_M es un grupo abeliano.*

Demostración:

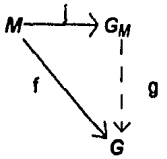
(i) $(0,0) + (u,v) = (0 + u, 0 + v) \sim (u,v)$ porque $0 + u + v = 0 + v + u$.

(ii) $(u,v) - (u,v) = (u,v) + (v,u) = (u + v, v + u) \sim (0,0)$ porque:

$$u + v + 0 = u + v + 0$$

■

Lema 4.26: *Sea $j(m) := (m,0)/\sim$, entonces, para cada f de el monoide abeliano M al grupo abeliano G, existe un único $g: G_M \to G$ tal que el diagrama*



conmuta.

Demostración: Definamos $g((u,v)/\sim) := f(u) - f(v)$. Entonces el diagrama conmuta obviamente porque:

$$g(j(m)) = g((m,0)/\sim) = f(m) - f(0) = f(m).$$

g está bien definida porque: $(u,v) \sim (u',v') \Leftrightarrow u + v' = u' + v \Rightarrow u - v = u' - v'$
$\Rightarrow f(u - v) = f(u' - v') \Leftrightarrow g((u,v)) = g((u',v'))$.

g es un homomorfismo de grupos porque:

$$g((u,v)/\sim + (u',v')/\sim) = g((u+u', v+v')/\sim) = f(u+u') - f(v+v')$$
$$= f(u) + f(u') - f(v) - f(v') = g((u,v)/\sim) + g((u',v')/\sim)$$

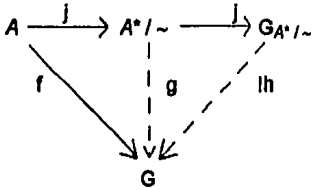
g es única porque: si h hace lo mismo entonces $h((m,0)/\sim) = f(m)$ para que conmute y $h((u,v)/\sim) = h((u,0) + (0,v)) = h((u,0) - (v,0)) = f(u) - f(v)$ que es la definición de g.

■

Ahora combinamos los lemas 4.21 y 4.26 para obtener el deseado grupo abeliano libre sobre el conjunto *A*.

***Teorema** 4.27 : Todo conjunto A genera un grupo abeliano libre F_A.*

Demostración: Aplicando los lemas mencionados obtenemos el siguiente diagrama:



■

CAPITULO 5.

ANILLOS Y MODULOS.

No trataremos la teoría de anillos en su generalidad. Para una demostración de los métodos y problemas en la teoría de anillos constructiva, los anillos conmutativos con elemento unitario y una relación de separabilidad lo harán muy bien.

ANILLOS, DOMINIOS ENTEROS, CAMPOS.

Definición *5.1 : Un anillo conmutativo con elemento unitario y relación de separabilidad, es una estructura:* $R = (R, \#, +, \cdot, -, 0, 1)$ *que satisface los axiomas de separabilidad* ***AP1 - AP3****, y cumple:*

1) $x + 0 = x$
2) $x + y = y + x$
3) $x + (y + z) = (x + y) + z$
4) $x + (-x) = 0$
5) $x \cdot 1 = x$
6) $x \cdot y = y \cdot x$
7) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
8) $x \cdot (y + z) = x \cdot y + x \cdot z$

La fuerte extensionalidad de $+$ y $\cdot$ *(no triviales).*

9) $x + y \# x' + y' \Rightarrow x \# x' \vee y \# y'$
10) $x \cdot y \# x' \cdot y' \Rightarrow x \# x' \vee y \# y'$
11) $0 \# 1$

Un anillo es un dominio entero si satisface.

12) $x \# 0 \wedge y \# 0 \Rightarrow x \cdot y \# 0$

Un anillo es un campo si satisface.

13) $x \# 0 \Rightarrow (\exists y)(x \cdot y = 1)$

Si dejamos fuera los axiomas que envuelven # y añadimos $0 \neq 1$ obtenemos la noción de un anillo. Generalmente será claro del contexto que clase de anillo es considerado.

Si no hay confusión abusaremos de la notación y denotaremos al anillo R por simplemente R. También utilizaremos xy en vez de $x \cdot y$ para el producto.

EJEMPLOS:

1) **Z, Q, R** son anillos con relación de separabilidad (lo mismo dominios enteros y campos respectivamente). La mayoría de las construcciones usuales de la teoría de anillos también producen anillos (anillos de matrices etc.) con relación de separabilidad.

Proposición *5.2 : Si R es un anillo entonces:*

(i) $x + y \# 0 \Rightarrow x \# 0 \vee y \# 0$
(ii) $xy \# 0 \Rightarrow x \# 0 \wedge y \# 0$

Si R es dominio entero:

(iii) $x \neq 0 \wedge xy = 0 \Rightarrow y = 0$
(iv) $x \# y \wedge z \# 0 \Rightarrow xz \# yz$

Si R es un campo:

(v) *R es un dominio entero*
(vi) $x \# 0 \Rightarrow (\exists! y)(xy = 1)$

Demostración:

(i) Se tiene porque $0+0=0$ entonces $x+y\#\,0+0 \Rightarrow x\#0 \vee y\#0$.

(ii) Se tiene porque $y=0\cdot y$ entonces $xy\#\,0y \wedge xy\#x0$

$$\Downarrow \qquad\qquad \Downarrow$$

$$(x\#0 \vee y\#y) \wedge (x\#x \vee y\#0)$$

y $(x\#x)$ así como $(y\#y)$ no pueden ser

$$\therefore\ x\#0 \wedge y\#0$$

(iii) Tenemos que por ser R dominio entero:

$$\begin{aligned}(x\#0 \wedge y\#0 \Rightarrow xy\#0) &\Rightarrow (\neg\neg(x\#0 \wedge y\#0) \Rightarrow \neg\neg(xy\#0))\\ &\Rightarrow (\neg(x\#0 \Rightarrow \neg y\#0) \Rightarrow \neg xy=0)\\ &\Rightarrow (\neg(\neg x\#0 \vee \neg y\#0) \Rightarrow xy\neq 0)\\ &\Rightarrow (\neg(x=0 \vee y=0) \Rightarrow xy\neq 0)\\ &\Rightarrow (\neg x=0 \wedge \neg y=0) \Rightarrow xy\neq 0)\end{aligned}$$

$$\therefore\ x\neq 0 \wedge y\neq 0 \Rightarrow xy\neq 0.$$

Ahora sea $x\neq 0$ y $xy=0$ y supongamos $y\neq 0$ entonces por lo anterior $xy\neq 0$ que es una contradicción

$$\therefore\ \neg\neg y=0$$

y como el anillo tiene separabilidad se tiene que la igualdad es estable

$$\therefore\ y=0$$

(iv) Demostremos primero el siguiente:

Lema 5.2.1: $x\#y \Rightarrow x+z\#y+z$.

Dem.

$x=x+z-z$ entonces $(x+z)-z\#(y+z)-z$

$$\Rightarrow (x+z\#y+z) \vee (-z\#-z)$$

$$\therefore\ x+z\ \#y+z$$

■

Entonces por el Lema se tiene que $x \# y \Rightarrow x - y \# 0$ y por hipótesis se tiene $z \# 0$.

$$\Rightarrow (x - y)z \# 0 \Rightarrow xz - yz \# 0 \Rightarrow xz \# yz.$$

(v) Sean $x \# 0$, $y \# 0$ entonces existen x', y' tales que $xx' = 1$ y $yy' = 1$ que estan separados del cero.

$$\therefore xx'yy' \# 0 \text{ y aplicando (ii) se tiene } xy \# 0 \wedge x'y' \# 0.$$

(vi) Supongamos que existen y, y' que son inversos de x. entonces:

$$xy = 1 = xy' \text{ por lo tanto } xy = xy' \Rightarrow (yx)y = (yx)y' \Rightarrow y = y'.$$

■

Debido a que en un campo el inverso es único lo denotaremos por x^{-1}.

La noción de *homomorfismo*, *isomorfismo*, e *isomorfismo fuerte* se siguen inmediatamente de las definiciones en grupos.

Los homomorfismos entre anillos con separabilidad tienen que ser fuertemente extensionales.

MODULOS Y ESPACIOS VECTORIALES.

Definición *5.3 : Un* Módulo *(con separabilidad) es una estructura de dos clases (R, M, ·) donde R en un anillo y M es un grupo abeliano (con separabilidad) y donde (·) es una función:*

$$de \quad R \times M \rightarrow M,$$

multiplicación por escalar, más las siguientes propiedades: para (r,s ∈ R y a,b ∈ M) se cumple:

1) $(r \cdot s) \cdot a = r \cdot (s \cdot a)$
2) $1 \cdot a = a$
3) $(r + s) \cdot a = r \cdot a + s \cdot a$
4) $r \cdot (a + b) = r \cdot a + r \cdot b$

Y la extensionalidad fuerte:

5) $r \cdot a \# s \cdot b \Rightarrow r \# s \vee a \# b$
6) $r \cdot a \# 0 \Rightarrow r \# 0 \wedge a \# 0$

Un espacio vectorial es un módulo sobre un campo.

Por conveniencia hemos denotado la separabilidad en R y M por el mismo símbolo, en general esto no nos lleva a confusiones.

Eliminando las clausulas que envuelven a # obtenemos un módulo sin separabilidad. En el contexto siempre se hará claro que clase de módulo estamos considerando. Como costumbre tampoco hacemos distinción notacional entre la multiplicación en el anillo y la multiplicación escalar.

Para espacios vectoriales podemos mostrar las siguientes propiedades convenientes de la relación de separabilidad.

***Proposición** 5.4 : En un espacio vectorial lo siguiente es válido:*

(i) $r \# 0 \wedge a \# 0 \Rightarrow ra \# 0$
(ii) $r \# 0 \wedge a \# a' \Rightarrow ra \# ra'$
(iii) $r \# r' \wedge a \# 0 \Rightarrow ra \# r'a.$

Demostración:

(i) Debido a que $r \# 0$, r^{-1} existe. Así que $a \# 0 \Rightarrow r^{-1}(ra) \# 0 \Rightarrow ra \# 0$.

(ii) $r \# 0$ implica que existe $r^{-1} \Rightarrow r^{-1}ra \# r^{-1}ra \Rightarrow r^{-1} \# r^{-1} \vee ra \# ra'$

$$\therefore ra \# ra'$$

(iii) $r \# r' \Rightarrow r - r' \# 0 \Rightarrow (r - r')a \# 0 \Rightarrow ra - r'a \# 0 \Rightarrow ra \# ra'$.

■

IDEALES, ANTI-IDEALES.

Definición 5.5: *Un anti-ideal de un anillo R es un subconjunto A que satisface:*

$(i)\ \ 0 \notin A$
$(ii)\ \ x+y \in A \Rightarrow x \in A \vee y \in A$
$(iii)\ \ xy \in A \Rightarrow x \in A \wedge y \in A$

Un ideal es un subconjunto J de R que satisface:

$(iv)\ \ 0 \in J$
$(v)\ \ x, y \in J \Rightarrow x-y \in J$
$(vi)\ \ x \in R\ e\ y \in J \Rightarrow xy \in J$

EJEMPLOS 5.6:

(i) $A = \{k \in \mathbf{Z} \mid \neg\, n|k\}$ para $n \neq 0$, es un anti-ideal en **Z** (el complemento de **nZ**).

(ii) $A = \{a \in \mathbf{R} \mid a \# 0\}$ es claramente un anti-ideal de **R**.

(iii) $A = \{f \in C(\mathbf{R},\mathbf{R}) \mid |f(0)| > 0\}$ es un anti-ideal en el anillo $C(\mathbf{R},\mathbf{R})$ de las funciones continuas de **R** a **R**. (esto se tiene debido a las propiedades que cumplen los números reales con respecto al *menor que*).

La definición de anti-ideal no requiere que contenga algún elemento del todo, así $\emptyset$ es un perfecto anti-ideal. También, por ejemplo, el conjunto siguiente cumple con las condiciones de ser anti-ideal pero, sin embargo, no es posible mostrar un elemento en él, es decir también es un ejemplo de un conjunto no vacío que no es posible mostrar que es habitado.

(iv) $A = \{n \in \mathbf{Z} \mid (\neg\, 4|n \wedge P) \vee (\neg\, 9|n \wedge \neg P)\}$

Demostración:

(i) $0 \in A$ porque $4|0$ y $9|0$.

(ii) Supongamos que $x+y \in A$ es decir:

$$(\neg 4 | x+y \wedge P) \vee (\neg 9 | x+y \wedge \neg P)$$

Entonces como $\neg 4 | x+y \Rightarrow \neg 4 | x \vee \neg 4 | y$
y $\neg 9 | x+y \Rightarrow \neg 9 | x \vee \neg 9 | y$

Se concluye $x \in A \vee y \in A$.

(iii) Supongamos que $xy \in A$ es decir:

$$(\neg 4 | xy \wedge P) \vee (\neg 9 | xy \wedge \neg P)$$

Entonces como $\neg 4 | xy \Rightarrow \neg 4 | x \wedge \neg 4 | y$
y $\neg 9 | xy \Rightarrow \neg 9 | x \wedge \neg 9 | y$

Se concluye que $x \in A \wedge y \in A$.

Por lo tanto A es un anti-ideal.

■

Los anti-ideales habitados son caracterizados por el hecho de que contienen al 1. Si suponemos que $a \in A$, entonces por (iii) de la definición de anti-ideal se tiene que $a = 1 \cdot a \in A \Rightarrow 1 \in A$.

Como siempre, los ideales pueden ser usados para definir *anillos cociente*, y como en el caso de grupos, los anti-ideales son la herramienta para introducir una relación de separabilidad en el anillo cociente.

***Proposición** 5.7 : (i) Si A es un anti-ideal, entonces A^c es un ideal, y A^c es propio si A es habitado.*

(ii) Sea J un ideal de R, entonces $R/J := \{a + J \mid a \in R\}$ con operaciones: $(a + J) + (b + J) := (a + b) + J$
$(a + J) \cdot (b + J) := (a \cdot b) + J$ es un anillo (cociente), provisto de que $1 \notin J$. (es decir J en un ideal propio).

(iii)Si A es un anti-ideal habitado, entonces R/A^c es un anillo con relación de separabilidad dada por:

$$a + A^c \# b + A^c \Leftrightarrow a - b \in A.$$

Demostración:

(i) 0 está en A^c obviamente.

Supongamos que x e y están en A^c. Entonces si $x - y \in A$ entonces $x \in A \vee -y \in A \Rightarrow y \in A$. que es una contradicción

$$\therefore x - y \notin A \Rightarrow x - y \in A^c$$

Si $x \in R$ e $y \in A^c$ y $xy \in A$ entonces $x \in A$ e $y \in A$ contradicción

$$\therefore xy \notin A \Rightarrow xy \in A^c.$$

(ii) Esta demostración es igual que en el álgebra tradicional así que la omitimos.

(iii) Verifiquemos las propiedades de separabilidad.

(1) $\neg (a + A^c \# b + A^c) \Leftrightarrow a - b \in A^c \Leftrightarrow a + A^c = b + A^c$.

(2) Demostremos primero lo siguiente:

***Lema** 5.7.1 : Si $x \in A^c$ entonces $-x \in A^c$.*

Dem.

supongamos que $\neg -x \in A^c \equiv -x \in A$ entonces:
$-x = -1x \in A \Rightarrow x \in A$ contradicción $\therefore -x \in A^c$.

■

De lo anterior obtenemos que : $x \in A \Rightarrow -x \in A$.

Entonces tenemos que si $a - b \in A \Rightarrow -(a - b) = b - a \in A$.

$$\therefore a + A^c \# b + A^c \Rightarrow b + A^c \# a + A^c.$$

(3) Supongamos $a + A^c \# b + A^c$ es decir $a - b \in A$ entonces se tiene:
$(a - b + c - c) \in A \Rightarrow (a - c) + (c - b) \in A \Rightarrow a - c \in A \vee c - b \in A$
$\Rightarrow a - c \in A \vee b - c \in A$

$\therefore a + A^c \# c + A^c \vee b + A^c \# c + A^c$.

(4) Supongamos $(a + b) + A^c \# (a' + b') + A^c$ es decir:
$(a + b) - (a' + b') \in A \Rightarrow (x - x') + (y - y') \in A \Rightarrow x - x' \in A \vee y - y' \in A$

$\therefore x + A^c \# x' + A^c \vee y + A^c \# y' + A^c$

(5) Supongamos $(ab) + A^c \# (a'b') + A^c$ es decir $(ab) - (a'b') \in A$:
$\Rightarrow ab - a'b' + ab' - ab' \in A \Rightarrow a(b - b') + (a - a')b' \in A$
$\Rightarrow a(b - b') \in A \vee b'(a - a') \in A \Rightarrow b - b' \in A \vee a - a' \in A$

$\therefore a + A^c \# a' + A^c \vee b + A^c \# b' + A^c$.

(6) $1 + A^c \# 0 + A^c$ debido a que $1 - 0 = 1 \in A$ (porque A es habitado).

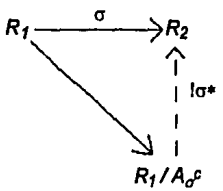
■

A partir de ahora, tacitamente asumiremos que los ideales son propios. La relación entre *homomorfismo* y *anti-ideal* está dada por el siguiente:

***Teorema** 5.8: (i) Para un anti-ideal habitado A el mapeo canónico $j: R \to R/A^c$ es un homomorfismo, y si R tiene una relación de separabilidad compatible con A entonces j es fuertemente extensional como se requirió.*

(ii) Si R_2 es un anillo con separabilidad y $\sigma: R_1 \to R_2$ un homomorfismo, entonces $A_\sigma := \{ a \in R_1 / \sigma(a) \# 0 \}$ es un anti-ideal habitado. Si R_1 es también un anillo con separabilidad, entonces A_σ es compatible con $\#$.

Existe un único isomorfismo fuerte σ^* tal que el diagrama siguiente conmuta:



Demostración:

(i) Sea A un anti-ideal habitado. j así definido es homomorfismo porque:

(a) $j(1) = 1 + A^c$
(b) $j(ab) = ab + A^c = a + A^c \cdot b + A^c = j(a) \cdot j(b)$
$j(a + b) = (a + b) + A^c = (a + A^c) + (b + A^c) = j(a) + j(b)$.

Es fuertemente extensional porque:

$j(a) \# j(b) \Rightarrow a + A^c \# b + A^c \Rightarrow a - b \in A \Rightarrow a - b \# 0 \Rightarrow a \# b.$

(ii) Sea R_2 anillo con separabilidad, $\sigma : R_1 \to R_2$ un homomorfismo de anillos y A_σ como se pidió, entonces:

a) $\sigma(1) = 1 \# 0 \quad \therefore 1 \in A_\sigma$

b) Supongamos que $x + y \; A_\sigma$ entonces:

$$\sigma(x + y) \# 0 \Rightarrow \sigma(x) + \sigma(y) \# 0 \Rightarrow \sigma(x) \# -\sigma(y)$$
$$\Rightarrow \sigma(x) \# 0 \vee -\sigma(y) \# 0 \Rightarrow \sigma(x) \# 0 \vee \sigma(y) \# 0$$

$$\Rightarrow x \in A_\sigma \vee y \in A_\sigma.$$

c) Supongamos que $xy \in A_\sigma$ entonces:

$$\sigma(xy) \# 0 \Rightarrow \sigma(x)\,\sigma(y) \# 0 \Rightarrow \sigma(x) \# 0 \wedge \sigma(y) \# 0$$

$$\Rightarrow x \in A_\sigma \wedge y \in A_\sigma$$

$\therefore$ A_σ es un anti-ideal habitado.

Supongamos que R_1 es un anillo con separabilidad entonces A_σ es compatible con la separabilidad de R_1 porque:

Si ambos anillos tienen separabilidad entonces σ es fuertemente extensional, por lo tanto:

$$a \in A_\sigma \Rightarrow \sigma(a) \# 0 = \sigma(0) \qquad \therefore\ a \# 0.$$

Definamos σ^* mediante: $\sigma^*(x + A_\sigma{}^c) = \sigma(x)$ entonces:

$x + A_\sigma{}^c = x' + A_\sigma{}^c \Leftrightarrow x - x' \in A_\sigma{}^c$ es decir $\neg(x - x') \in A_\sigma$

$\Rightarrow \neg(\sigma(x - x') \# 0) \Rightarrow \neg(\sigma(x) \# \sigma(x')) \Leftrightarrow \sigma(x) = \sigma(y).$

$\therefore$ Está bien definida.

Ahora bien: $\sigma^*(x + A_\sigma{}^c) = \sigma^*(y + A_\sigma{}^c) \Rightarrow \sigma(x) = \sigma(y)$

$\sigma(x - y) = 0 \Rightarrow x - y \in A_\sigma{}^c \Leftrightarrow x + A_\sigma{}^c = y + A_\sigma{}^c.$

Y $\quad x + A_\sigma{}^c \# y + A_\sigma{}^c \Rightarrow x - y \in A_\sigma \Rightarrow \sigma(x - y) \# 0$

$\Rightarrow \sigma(x) \# \sigma(y).$

$\therefore$ Es un isomorfismo fuerte.

Y por como está definido, claramente conmuta el diagrama y se tiene la unicidad.

■

ANTI-IDEALES PRIMOS, ANTI-IDEALES MINIMOS Y MAXIMOS.

Los *anti-ideales primos* juegan un papel muy importante en el álgebra tradicional, pero sus definiciones usuales:

$$J \text{ es primo} \Leftrightarrow (xy \in J \Rightarrow x \in J \vee y \in J).$$
$$J \text{ es primo} \Leftrightarrow (x \notin J \wedge xy \in J \Rightarrow y \in J).$$

son, la primera muy fuerte y la segunda muy débil.

Bajo la primera definición no siempre (X) es un ideal primo de $R[X]$: tome a,b tales que $ab = 0$ pero $a = 0$ o $b = 0$ no sea decidible, y considere a $(X + a)(X + b)$. La segunda definición no es lo suficientemente fuerte para hacer del anillo cociente sobre un ideal primo un dominio entero. Aprovecharemos lo desarrollado por el lado de los anti-ideales; aunque podríamos, sin embargo, utilizar el inciso (i) de la siguiente proposición como definición.

Por exactamente las mismas razones hemos modificado la definición tradicional de dominio entero. El campo R no satisface $xy = 0 \Rightarrow x = 0 \vee y = 0$ así que la definición tradicional es demaciado fuerte.

Definición 5.9: *Sea R un anillo y A un subconjunto de R:*

(i) A es anti-ideal primo de R si:

$$1 \in A,\ x \in A \wedge y \in A \Rightarrow xy \in A.$$

(ii) A es un anti-ideal mínimo si:

$$1 \in A,\ \forall x \in A\ \exists y \in R \text{ tal que } (1 - xy \notin A).$$

Tenemos que usar la noción de anti-ideal mínimo en vez de ideal máximo ya que nos queremos dirigir a los resultados familiares como el que el anillo cociente módulo el complemento de un anti-ideal primo es un campo.

Proposición 5.10: *(i) A es primo si y solo si R/A^c es un dominio entero.*

(ii) A es mínimo si y solo si R/A^c es un campo.

(iii) Un anti-ideal mínimo es primo.

(iv) Si A es mínimo y B es anti-ideal habitado tal que B está contenido en A, entonces B = A.

Demostración:

(i) ($\Rightarrow$) Supongamos que A es primo y sean $x + A^c$, $y + A^c \in R/A^c$ tales que están separados de $0 + A^c$ es decir $x \in A$ e $y \in A$ entonces: $xy \in A$

$$\therefore\ xy + A^c \# 0 + A^c.$$

($\Leftarrow$) Sean $x, y \in A$ entonces $x + A^c \# 0 + A^c$ y $y + A^c \# 0 + A^c$ esto implica que $xy + A^c \# 0 + A^c$ es decir $xy \in A$.

(ii) ($\Rightarrow$) Sea $x + A^c \in R/A^c$ tal que $x + A^c \# 0 + A^c$ es decir $x \in A$ entonces $\exists y \in R$ tal que $(1 - xy) \in A^c$

$$\therefore\ (1 - xy) + A^c = 0 + A^c \Rightarrow (1 + A^c) - (xy + A^c) = 0 + A^c$$

$$\therefore\ 1 + A^c = xy + A^c \text{ es decir}$$

$$y + A^c \text{ es el inverso de } x + A^c.$$

($\Leftarrow$) Sea $x \in A$ entonces $x + A^c \# 0 + A^c$.

$$\therefore\ \exists (y + A^c) \text{ tal que } xy + A^c = 1 + A^c \Rightarrow (1 - xy) + A^c = 0 + A^c$$

$$\therefore\ 1 - xy \in A^c.$$

(iii) A mínimo $\Leftrightarrow$ R/A^c campo $\Rightarrow$ R/A^c dominio entero $\Leftrightarrow$ A primo.

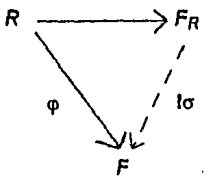
(iv) Sea $x \in A$, entonces $(1 - xy) \notin A$ para alguna $y \in R$. entonces:
$1 = (1 - xy) + xy \in B \Rightarrow (1 - xy) \in B \vee xy \in B$

$\therefore xy \in B$ y en consecuencia $a \in B$.

■

Podemos imitar la construcción tradicional del *campo de fracciones* de un dominio entero donde se introduce adicionalmente una relación de separabilidad.

Teorema 5.11 : *Para cada dominio entero R existe un campo F_R tal que R se mapea mediante un isomorfismo fuerte en F_R y para cada isomorfismo fuerte $\varphi : R \to F$ sobre un campo, existe un único isomorfismo fuerte $\sigma : F_R \to F$ tal que el siguiente diagrama conmuta:*



Demostración: Definamos la relación ~ en $A = \{ (a,b) \mid a \in R,\ b \neq 0 \}$ por:
$(a,b) \sim (a',b') := ab' = a'b$. entonces ~ es una relación de equivalencia:
(i) $ab = ab$ por lo tanto $(a,b) \sim (a,b)$.
(ii) $ab' = a'b \Rightarrow a'b = ab'$ por lo tanto se tiene simetría.
(iii) Para demostrar la transitividad demostremos primero el siguiente:

Lema 5.11.1 : *R dominio entero $\Rightarrow$ en R se vale la cancelación.*

Dem. Supongamos que $a \# 0$.

Tenemos que $a \# 0,\ b \# 0 \Rightarrow ab \# 0$ entonces:
$ab = ac \Rightarrow ab - ac = 0 \Rightarrow \neg (a(b-c) \# 0)$
$\Rightarrow \neg (a \# 0 \wedge (b-c) \# 0) \Rightarrow (a \# 0 \Rightarrow \neg\, b - c \# 0)$
y tenemos por hipótesis que $a \# 0$

$\therefore\ b - c = 0$ es decir $b = c$.

■

Ahora demostrar la transitividad es igual a como ya lo hicimos.

□

Ahora definamos las operaciones del anillo, y la separabilidad en $A / \sim$: (escribiremos [t] en vez de $[t] / \sim$).

$[(a,b)] + [(c,d)] := [(ad + bc, bd)]$
$[(a,b)] - [(c,d)] := [(ad - bc, bd)]$
$[(a,b)] \cdot [(c,d)] := [(ac,bd)]$
$[(a,b)] \# [(c,d)] := ad \# bc$

Es igual que siempre verificar que estas operaciones están bien definidas, que $[(0,1)]$ y $[(1,1)]$ son el cero y el uno.

La estructura es un campo:
Si $a \# 0$ entonces la clase de $(a,b)^{-1} = (b,a)$ porque:
$(a,b) \cdot (b,a) = (ab,ba) \sim (1,1)$ ya que $ab = ba$.

□

Siguiendo la tradición escribimos a / b para $[(a,b)]$. El inverso para a / b con $b \# 0$ es b / a. El isomorfismo fuerte $R \to F_R$ está dado por $a \to a / 1$.

Dem: (i) sup. $f(a) = f(b)$ entonces $(a,1) = (b,1)$

$\Rightarrow a \cdot 1 = b \cdot 1 \Rightarrow a = b$

(ii) sup. $x \# y$ entonces $f(x) = (x,1)$
$f(y) = (y,1)$

y se tiene $(x,1) \# (y,1) \Leftrightarrow x \# y$.

□

Ahora sea $\varphi : R \to F$ un isomorfismo fuerte, definamos:
$\sigma(a/b) = \varphi(a) \cdot \varphi(b)^{-1}$ entonces σ es isomorfismo fuerte.

Dem: (i) sup. $\sigma(a/b) = \sigma(a'/b')$ entonces:
$\varphi(a)\varphi(b)^{-1} = \varphi(a')\varphi(b')^{-1} \Rightarrow \varphi(a)\varphi(b') = \varphi(a')\varphi(b)$
$\Rightarrow \varphi(ab') = \varphi(a'b) \Rightarrow ab' = a'b$. es decir $a/b = a'/b'$.

(ii) sup. $a/b \# a'/b'$ entonces:
$ab' \# a'b \Rightarrow \varphi(ab') = \varphi(a)\varphi(b') \# \varphi(a'b) = \varphi(a')\varphi(b)$
$\Rightarrow \varphi(a)\varphi(b)^{-1} = \varphi(a')\varphi(b')^{-1} \Rightarrow \sigma(a/b) \# \sigma(a'/b')$.

□

Claramente el diagrama conmuta.

Ahora si suponemos que τ hace el diagrama conmutativo entonces $\tau(a/1) = \varphi(a)$, $\tau(b/1) = \varphi(b)$ y por lo tanto:

$\tau(a/b) = \tau((a/1)(1/b)) = \tau((a/1)(b/1)^{-1}) = \tau(a/1)\tau(b/1)^{-1}$
$= \varphi(a)\varphi(b)^{-1} = \sigma(a/b)$.

$\therefore$ σ es único.

■

BIBLIOGRAFIA.

[1] *A. S. Troelstra, D. van Dalen,* **Constructivism in mathematics.** Vol. I Elsevier science publishers B. V. 1988.

[2] *A. S. Troelstra, D. van Dalen,* **Constructivism in mathematics.** Vol II Elsevier science publisher B. V. 1988.

[3] *Dragalin A. G.,* **Mathematical intuitionism. Introduction to proof theory.** (Russian). (Nauka, Moskva). 1979.

[4] A. G. *Hamilton* , **Logic for mathematicians.** Cambridge University Press. 1991.

[5] *Joachim Lambek,* **Rings and modules.**