Teoría de Grupos

Paul Dubreil

EDITORIAL REVERTÉ

Teoría de Grupos

Paul DUBREIL
Professeur à l'Université Paris VI

EDITORIAL
REVERTÉ

Barcelona · Bogotá · Buenos Aires · México

Título de la obra original:
Théorie des groupes

Edición original en lengua francesa publicada por:
Editorial Dunod, París

Edición en papel:
© Editorial Reverté, S. A., 1975
ISBN 978-84-291-5071-1

Edición e-book (PDF):
© Editorial Reverté, S. A., 2021
ISBN 978-84-291-9115-8

Versión española por:
Lucia Yagüe Ena
Licenciada en Ciencias

Revisada por el:
Dr. Rafael Rodríguez Vidal
Catedrático de la Facultad de Ciencias de Zaragoza

Propiedad de:
EDITORIAL REVERTÉ, S. A.
Loreto, 13-15, Local B
08029 Barcelona
reverte@reverte.com
www.reverte.com

#579

Prólogo

Al estar actualmente dividida la enseñanza superior de las Matemáticas en "unidades de valor" consagradas a materias importantes tales como Topología general, Integración, etc., han considerado los matemáticos de la Universidad París VI que la *Teoría de Grupos* debía figurar entre las unidades de valor fundamentales del Algebra.

Desde 1969, estas enseñanzas atraen cada año a cientos de estudiantes que proceden directamente del primer ciclo y que por consiguiente todavía no han estudiado nunca una teoría algebraica en sí misma, con la excepción quizá del álgebra lineal elemental. Está claro, pues, que el presente libro constituye, no un tratado, sino un curso, e incluso un *primer curso* de la Teoría de grupos, un curso *semestral* por otra parte, y por ende inevitablemente incompleto. La selección tanto de las cuestiones a tratar como de la presentación de éstas, ha resultado a menudo difícil. Ha sido el principal objetivo despertar el interés de los estudiantes, proponerles un esfuerzo fructífero pero a su alcance, así como estimular a los mejores de entre ellos por medio del estudio de algunos hermosos teoremas.

Como profesor, no he querido prescindir de mis preferencias personales. Esta es la razón por la que he dedicado el principio del curso a los "primeros principios para el estudio de una estructura algebraica" y especialmente a los homomorfismos. De esta forma la teoría de grupos se encuentra encuadrada en el Algebra general. Después he querido insistir en el estudio de los endomorfismos de un grupo, válidos casi sin necesidad de cambios para las álgebras universales (Capítulo IV, § 1, en especial teorema 3). Dentro del espíritu de Emmy Noether, me he esforzado en evidenciar las propiedades de dualidad de las descomposiciones directas (Capítulo IV, §§ 1 y 2), en ocasiones un poco descuidadas. Me he preocupado en fin de desarrollar un poco las cuestiones referentes a la generación de los grupos, en relación con los problemas universales (Capítulo III, § 3).

Expreso mi profundo agradecimiento a la editorial DUNOD-BORDAS que ha hecho posible la publicación de este curso, considerándolo como una prolongación de las *Lecciones de Algebra Moderna,* escritas en colaboración con Marie Louise Dubreil-Jacotin y publicadas en 1961.* Espero que otros fascículos, dedicados por ejemplo a los Anillos y a los Cuerpos, constituirán prolongaciones análogas.

Constituye para mi un agradable deber el reseñar las excelentes obras que he utilizado principalmente: figuran las mismas en la bibliografía situada inmediatamente a continuación de este prólogo. Recomiendo con insistencia a los estudiantes que se remitan a

* La traducción española de esta obra ha sido publicada por Editorial Reverté (Segunda edición, 1971). N. del T.

ella y, en particular, que comiencen a leer libros de matemáticas escritos en una lengua extranjera.

Es necesario también aconsejarles que hagan ejercicios. El libro de Bigard-Crestey -Grappy que se incluye en la bibliografía contiene dos capítulos dedicados a los grupos. Las soluciones vienen dadas en la misma obra. He añadido, al final de cada capítulo del presente libro, algunas cuestiones que han sido incluidas en exámenes parciales o finales; son de una dificultad realmente moderada.

En lo referente a los conocimientos previos que se suponen, éstos se limitan:

1° A la Aritmética elemental.

2° A los elementos de la Teoría de Conjuntos: partes, conjunto producto, relaciones, aplicaciones.

3° Al Algebra lineal (será conveniente que el lector complete, si procede, sus conocimientos sobre los espacios vectoriales de dimensión infinita).

Paul Dubreil

Bibliografía

a) Tratados de Algebra

Los Capítulos que se indican son los dedicados a la Teoría de grupos.

N. BOURBAKI, *Algebra* (Hermann).
P. DUBREIL y M. L. DUBREIL-JACOTIN, *Lecciones de Algebra Moderna* (Reverté). Caps. II, III, VII. [Citada en este libro A. M. o Algebra Moderna.]
R. GODEMENT *Algebra* (Tecnos), § 7.
N. JACOBSON, *Lectures in abstract Algebra;* vol. 1, Capítulos I y V Conceptos Básicos (Van Nostrand).
A. KUROSH, *Algèbre générale* (Gauthier-Villars, traducción francesa).
S. MAC LANE y G. BIRKHOFF, *Algebra* (MacMillan) (Gauthier-Villars, traducción francesa). Caps. III, XIII.
B. L. VAN DER WAERDEN, *Algebra,* 2 vol (Springer) Caps. II, VII, XIV.
A. BIGARD, M. CRESTEY, J. GRAPPY, *Problemas de Algebra Moderna* (Reverté). Caps. III y IV.
S. LANG *Algebra* (Aguilar).

b) Tratados de Teoría de grupos

MARSHALL HALL, *The Theory of Groups* (MacMillan).
A. KUROSH *The Theory of Groups* (Chelsea Publ. Co.) 2 vol.
J. P. SERRE, *Representaciones lineales de los grupos finitos* (Omega).
H. ZASSENHAUS, *The Theory of Groups* (Chelsea, Publ. Co.)

Para los *grupos abelianos.*

L. FUCHS, *Abelian Groups* (Publ. de la Acad. Húngara de Ciencias).

* En los casos en que nos constaba la existencia de traducción española de la obra citada, hemos puesto la referencia de aquella. N. del T.

Indice analítico

CAPÍTULO I

Nociones fundamentales

CAPÍTULO II

Estudio de los subgrupos. Teoremas de Sylow

CAPÍTULO III

Generación de grupos

CAPÍTULO IV

Productos directos. Descomposiciones directas

CAPÍTULO V

Teoremas generales

CAPÍTULO VI

Representaciones lineales de los grupos finitos y de las álgebras de dimensión finita

capítulo I

Nociones fundamentales

§ 1. *PRIMEROS PRINCIPIOS PARA EL ESTUDIO DE UNA ESTRUCTURA ALGEBRAICA. HOMOMORFISMOS*

Una *estructura algebraica es un conjunto* E provisto de diversas leyes de composición internas o externas, o de leyes con un número cualquiera de variables (aplicaciones de E^n en E). Los grupos, los anillos, los cuerpos, los módulos, los espacios vectoriales son estructuras algebraicas especialmente importantes.

Para estudiar una estructura algebraica, hay que interesarse en primer lugar en las *partes notables* (en particular en los *elementos* notables), en las *relaciones notables,* en las *aplicaciones notables* y en los lazos que existen entre ellas.

Para fijar ideas, consideremos la estructura muy general que se obtiene al proveer a un conjunto no vacío cualquiera E:

1) de una *ley de composición interna:*

$$E \times E \longrightarrow E$$

que denotaremos multiplicativamente: xy designa pues la imagen del par $(x, y) \in E \times E$ diremos entonces que E es un *grupoide multiplicativo;*

2) de una ley de *composición externa por la izquierda:*

$$\Delta \times E \longrightarrow E,$$

siendo Δ un conjunto no vacío cualquiera, llamado *dominio de operadores por la izquierda:* esta ley será denotada también multiplicativamente: αx designa la imagen del par $(\alpha, x) \in \Delta \times E$ (no es de tener confusión alguna, puesto que los operadores, elementos de Δ, vienen representados por letras griegas).

Esta estructura algebraica de *grupoide con operadores* será designada por $E(., \Delta)$ o, más brevemente, por E cuando no haya lugar a precisar más. Los grupos con operadores serán un caso particular de esto.

Partes notables

Una parte S de E es *estable* (para la ley interna) si:

$$(\forall s_1, s_2 \in S)\,, \qquad s_1 s_2 \in S\,.$$

Una parte P de E es *lícita* (para la ley externa) si:

$$(\forall \alpha \in \Delta) \quad \text{y} \quad (\forall p \in P)\,, \qquad \alpha p \in P\,.$$

Observación. La parte vacía, $\varnothing$, posee estas dos propiedades.

Elementos notables

Un elemento a de E es *idempotente* si $a^2 = a$. Por ejemplo, un *elemento neutro por la derecha,* o *elemento unidad por la derecha* e' : $(\forall x \in E)$, $xe' = x$, es un idempotente. Recordemos que un *elemento neutro,* o *elemento unidad bilateral* e viene definido por: $(\forall x \in E)$, $ex = xe = x$, y que tal elemento es necesariamente único.

Relaciones notables

Una relación binaria en un conjunto E se define como una parte $\mathscr{R}$ del producto cartesiano $E^2 = E \times E$. Será cómodo escribir $a \mathscr{R} b$ mejor que $(a, b) \in \mathscr{R}$.

Especialmente importantes son las *relaciones de equivalencia* o, más brevemente, *las equivalencias* (relaciones reflexivas, simétricas y transitivas).

Una relación $\mathscr{R}$ es *compatible* con la ley de composición interna si

$$a \mathscr{R} a' \text{ y } b \mathscr{R} b' \text{ implican } (ab) \mathscr{R} (a' b')\,.$$

$\mathscr{R}$ es *regular por la derecha* si

$$a \mathscr{R} a' \text{ implica } \quad (\forall x \in E) \qquad (ax) \mathscr{R} (a' x)\,,$$

regular por la izquierda si

$$a \mathscr{R} a' \text{ implica } \quad (\forall y \in E) \qquad (ya) \mathscr{R} (ya')\,,$$

y *regular* si posee las dos propiedades procedentes.

En una relación $\mathscr{R}$ *reflexiva,* la compatibilidad implica la regularidad:

$$a \mathscr{R} a' \quad \text{con} \quad x \mathscr{R} x \text{ implican } (ax) \mathscr{R} (a' x)\,,$$

para todo $x \in E$.

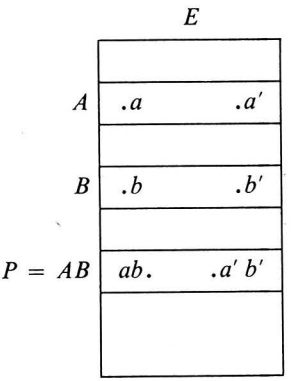
En una relación $\mathscr{R}$ *transitiva,* la regularidad implica la compatibilidad:

$$a \mathscr{R} a' \quad \text{y} \quad b \mathscr{R} b' \quad \text{implican} \quad (ab) \mathscr{R} (a' b) \quad \text{y} \quad (a' b) \mathscr{R} (a' b')$$

en donde $(ab) \mathscr{R} (a' b')$.

En particular, *en una relación de equivalencia, la regularidad y la compatibilidad son ciertas al mismo tiempo.* Pero la regularidad por un solo lado tendrá un interesante papel en la Teoría de Grupos.

Sea $\mathscr{R}$ una equivalencia definida en E y que suponemos *compatible* con la ley interna de E. Consideremos el conjunto cociente $E/\mathscr{R}$, es decir, el conjunto de las clases módulo $\mathscr{R}$ y definamos en este conjunto una ley de composición interna a partir de la de E (diremos que viene *inducida* por la de E). Sean A, B dos clases (distintas o no). Cualesquiera que sean el representante a de A y el representante b de B, el producto ab pertenece a una misma clase P, puesto que $\mathscr{R}$ es compatible con la multiplicación de E: por definición, esta clase P es el producto en $E/\mathscr{R}$ de la clase A por la clase B



$$P = AB\,.$$

Una relación $\mathscr{R}$ definida en E es *lícita* para la ley externa $\Delta \times E \longrightarrow E$ si

$$a\,\mathscr{R}\,a' \quad \text{implica} \quad (\forall \alpha \in \Delta) \qquad (\alpha a)\,\mathscr{R}\,(\alpha a')\,.$$

Si $\mathscr{R}$ es una equivalencia lícita, el conjunto cociente $E/\mathscr{R}$ puede estar provisto de una ley externa por la izquierda $\Delta \times (E/\mathscr{R}) \longrightarrow E/\mathscr{R}$ definida a partir de la de E (ley externa "inducida"). En efecto, dada una clase $A \in E/\mathscr{R}$ y un operador $\alpha \in \Delta$, cualquiera que sea el representante a de la clase A, el producto αa pertenece a una misma clase Q: esta es, por definición, el producto de $\alpha \in \Delta$ por $A \in E/\mathscr{R}$:

$$Q = \alpha A\,.$$

Definición. Toda equivalencia regular y lícita definida en $E(.,\Delta)$ es una *congruencia.* Una equivalencia lícita para Δ se llama también *Δ–equivalencia.*

Aplicaciones notables

Sean E, E' dos conjuntos provistos cada uno de una ley de composición interna, denotada multiplicativamente, y de una ley de composición externa por la izquierda definida por medio del *mismo* dominio de operadores Δ, denotada también multiplicativamente.

Una aplicación h de E en E' es un *homomorfismo* de $E(.,\Delta)$ en $E'(\bullet,\Delta)$ si:

(1) $\qquad (\forall x \text{ y } y \in E) \qquad h(xy) = h(x)\,h(y)\,,$

(2) $\qquad (\forall x \in E) \text{ y } (\forall \alpha \in \Delta) \qquad h(\alpha x) = \alpha h(x)$

Designaremos tal homomorfismo por

$$h : E(.,\Delta) \longrightarrow E'(.,\Delta)$$

o, más brevemente : $h : E \longrightarrow E'$ o también $E \xrightarrow{h} E'$.

El conjunto de los homomorfismos de E en E' se designa Hom (E, E').

Resulta cómodo expresar las eventuales propiedades *inyectiva, suprayectiva, biyectiva,* mediante el empleo de flechas especiales:

$$\begin{array}{ll} h \text{ inyectiva} & E \rightarrowtail E' \\ h \text{ suprayectiva}: & E \twoheadrightarrow E' \\ h \text{ biyectiva} & E \rightarrowtail\!\!\!\!\twoheadrightarrow E'' . \end{array}$$

Si una biyección $f : E \rightarrowtail\!\!\!\!\twoheadrightarrow E'$ es un homomorfismo la biyección recíproca $f^{-1} : E' \rightarrowtail\!\!\!\!\twoheadrightarrow E$ lo es también: en efecto, siendo x' e y' dos elementos cualesquiera de E y x, y sus imágenes recíprocas respectivas en E, la igualdad $f(x)f(y) = f(xy)$, es decir, $x'y' = f(xy)$, implica, tomando las imágenes recíprocas en E, $f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y')$. Igualmente

$$\alpha f(x) = f(\alpha x) \qquad (\alpha \in \Delta)$$

implica $f^{-1}(\alpha x') = \alpha f^{-1}(x')$. Se dice entonces que f es un *isomorfismo de $E(.,\Delta)$ sobre $E'(.,\Delta)$; f^{-1} es el isomorfismo recíproco.* Un isomorfismo de E *sobre sí mismo* $(E' = E)$ es un *automorfismo.*

Un homomorfismo de E *en sí mismo* es un *endomorfismo.*

Consideremos dos homomorfismos:

$$h_1 : E \longrightarrow E' , \qquad h_2 : E' \longrightarrow E'' ,$$

tales que la estructura de llegada del primero sea la de partida del segundo. La aplicación compuesta $h_2 \circ h_1$ viene definida por

$$(\forall x \in E) \qquad (h_2 \circ h_1)(x) = h_2[h_1(x)] \qquad (\in E'') ;$$

(con esta notación, llamada funcional, la composición se hace en sentido inverso de la escritura: puede suprimirse el símbolo $\circ$; se tiene entonces la notación multiplicativa; en algunos autores se encuentran con frecuencia las notaciones xh o x^h en lugar de $h(x)$ y por consiguiente, $h_1 \circ h_2$ en lugar de $h_2 \circ h_1$: la composición se hace entonces en el sentido de la escritura).

Se ve inmediatamente que las condiciones (1) y (2) son respetadas por la composición: *la aplicación compuesta de dos homomorfismos es un homomorfismo* (la misma

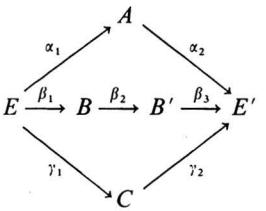
propiedad se verifica para los isomorfismos, para los automorfismos, para los endomorfismos). Por ser asociativa la composición de aplicaciones, puede hablarse del compuesto de n endomorfismos de la forma

$$h_i : E_i \longrightarrow E_{i+1} \qquad (i = 1, \ldots, n) ,$$

tomados en el orden de los índices, y designarlo por $h_n \circ \ldots \circ h_1$, lo que se representa mediante el *diagrama:*

$$E_1 \xrightarrow{h_1} E_2 \xrightarrow{h_2} \ldots E_{n-1} \xrightarrow{h_{n-1}} E_n \xrightarrow{h_n} E_{n+1} .$$

Puede ocurrir que existan varios homomorfismos compuestos de E en E'; se tiene entonces un *diagrama* no lineal tal como:



Si $\alpha_2 \circ \alpha_1 = \beta_3 \circ \beta_2 \circ \beta_1 = \gamma_2 \circ \gamma_1$, se dice que el diagrama anterior es *conmutativo;* con frecuencia expresaremos esta propiedad por medio de las iniciales D.C. colocadas cerca del diagrama.

Para todo homomorfismo $h : E(., \Delta) \to E'(., \Delta)$, tenemos las siguientes propiedades.

Proposición 1. *La imagen* $h(E) = \overline{E}$ *de* E *en* E' *es una parte estable y lícita de* E'.

Si $x', y' \in \overline{E}$, es decir, si $x' = h(x), y' = h(y) (x, y \in E)$, se tiene, según (1):

$$x' y' = h(x)\, h(y) = h(xy) \in \overline{E} ;$$

por lo tanto $\overline{E}$ es parte *estable* de

Análogamente, según (2),

$$(\forall \alpha \in \Delta) , \qquad \alpha x' = \alpha h(x) = h(\alpha x) \in \overline{E} ;$$

$\overline{E}$ es parte *lícita* de E'.

Asociemos al homomorfismo h la relación binaria $\mathcal{R}$ definida en el conjunto de partida E por

(3) $a \mathcal{R} a'$ ssi (= si y sólo si) $h(a) = h(a')$.

Proposición 2. *La relación* $\mathcal{R}$ *que acabamos de definir es una equivalencia regular y lícita y, por lo tanto, una congruencia.*

Evidentemente $\mathscr{R}$ es reflexiva, simétrica y transitiva. Es regular por la derecha (por ejemplo), puesto que la igualdad $h(a)=h(a')$ implica

$$(\forall x \in E) \qquad h(a)\,h(x) = h(a')\,h(x)\,,$$

es decir

$$h(ax) = h(a'\,x)\,.$$

Como la misma igualdad implica también

$$(\forall \alpha \in \Delta) \qquad h(\alpha a) = h(\alpha a')\,,$$

$\mathscr{R}$ es una equivalencia lícita.

Definición. La congruencia $\mathscr{R}$ así definida a partir de un homomorfismo h de $E(.,\Delta)$ en $E'(.,\Delta)$ recibe el nombre de *congruencia nuclear* asociada a h (o congruencia de homomorfismo, equivalencia de homomorfismo).

Consideremos ahora la aplicación canónica γ de E sobre el conjunto cociente $E/\mathscr{R}$, siendo $\mathscr{R}$ la congruencia nuclear de h: para todo elemento x de E, $\gamma(x) = X$ es la clase módulo $\mathscr{R}$ a la cual pertenece x. Evidentemente, esta aplicación γ es suprayectiva. Además, según la definición misma de las leyes de composición interna y externa de $E/\mathscr{R}$, γ es un homomorfismo:

$$\gamma : E \longrightarrow\!\!\!\!\rightarrow E/\mathscr{R}$$

llamado *homomorfismo suprayectivo canónico* de E sobre $E/\mathscr{R}$.

Todos los elementos $x, x', \ldots$, de una clase $X \in E/\mathscr{R}$ tienen la misma imagen $h(x)$ en E': pongamos pues $i(X) = h(x)$. Definimos así una aplicación i de $E/\mathscr{R}$ en $h(E)$ que es *inyectiva* según la definición de $\mathscr{R}$ y evidentemente *suprayectiva*. Además, si x e y son respectivamente representantes de las clases X, Y y α un operador, tenemos:

$$i(XY) = h(xy) = h(x)\,h(y) = i(X)\,i(Y)\,,$$

$$i(\alpha X) = h(\alpha x) = \alpha h(x) = \alpha i(X)\,;$$

y por lo tanto, finalmente, i es un *isomorfismo* del cociente $E/\mathscr{R}$ sobre la imagen $h(E)$: se le llama *isomorfismo canónico asociado* a h.

Finalmente, si j es la *inyección canónica* de $h(E)=\overline{E}$ en E, definida por

$$(\forall x' \in \overline{E}) \qquad j(x') = x' \quad (\in E')\,,$$

tenemos:

$$(\forall x \in E) \qquad (j \circ i \circ \gamma)\,(x) = j[i(X)] = j[h(x)] = h(x)\,,$$

y por lo tanto

$$j \circ i \circ \gamma = h\,. \tag{4}$$

Hemos establecido, para el tipo de estructura algebraica considerada ("grupoide con operadores"), el importante *teorema de homomorfismo:*

Teorema 1. *Para todo homomorfismo* $h : E \longrightarrow E'$,

1) *existe un isomorfismo* i *del cociente* $E/\mathscr{R}$ *de* E *por la congruencia nuclear* $\mathscr{R}$ *de* h, *sobre la imagen* $h(E) = \overline{E}$.

2) h *se descompone en factores por medio del homomorfismo suprayectivo canónico* γ *de* E *sobre* $E/\mathscr{R}$, *del isomorfismo* i *del cociente* $E/\mathscr{R}$ *sobre la imagen* $h(E)$ *y de la inyección canónica* j *de* $h(E)$ *en* E':

$$h = j \circ i \circ \gamma . \tag{5}$$

Este último resultado se expresa mediante el *diagrama conmutativo:*

$$\begin{array}{ccc} E & \xrightarrow{h} & E' \\ {\scriptstyle\gamma}\downarrow & & \uparrow{\scriptstyle j} \\ E/\mathscr{R} & \rightarrowtail & h(E) = \overline{E} \end{array} \qquad \text{DC}.$$

Observación. Haciendo $\beta = j \circ i$, tenemos también la descomposición factorial $h = \beta \circ \gamma$ de h en un homomorfismo suprayectivo γ y un homomorfismo inyectivo β:

$$\begin{array}{ccc} E & \xrightarrow{h} & E' \\ {\scriptstyle\gamma}\downarrow & \nearrow{\scriptstyle\beta} & \\ E/\mathscr{R} & & \end{array} \qquad \text{DC}.$$

Caso particular. Si h es *suprayectivo*, j es la aplicación idéntica de $h(E) = E'$ sobre E'; $\beta = i$ y (4) se escribe:

$$h = i \circ \gamma ; \tag{4'}$$

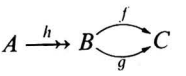
tenemos aquí el diagrama

$$\begin{array}{ccc} E & \xrightarrow{h} & E' \\ {\scriptstyle\gamma}\downarrow & \nearrow{\scriptstyle i} & \\ E/\mathscr{R} & & \end{array} \qquad \text{DC}.$$

Resulta claro que, con la condición de reemplazar los grupoides con operadores por *conjuntos,* los homomorfismos por *aplicaciones,* etc., se tiene, en teoría de conjuntos, un teorema análogo al teorema 1. Inversamente, vamos a dar en forma general referida a conjuntos un teorema que se aplica, en particular, a los homomorfismos.

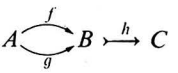
Teorema 2. *En la composición de aplicaciones,*

a) *toda aplicación suprayectiva* $h : A \twoheadrightarrow B$ *es simplificable por la derecha;*



(6) $$f \circ h = g \circ h \quad \textit{implica} \quad f = g \ ;$$

b) *toda aplicación inyectiva* $h : B \rightarrowtail C$ *es simplificable por la izquierda:*



$$h \circ f = h \circ g \quad \textit{implica} \quad f = g \ .$$

La igualdad (6) significa: $(\forall a \in A)$, $f[h(a)] = g[h(a)]$; h suprayectiva, cuando a describe A, $h(a) = b$ describe B. Tenemos pues:

$$(\forall b \in B) \qquad f(b) = g(b) \ ,$$

es decir, $f = g$.

La igualdad (7) significa: $(\forall a \in A), h[f(a)] = h[g(a)]$, de donde, al ser h inyectiva: $(\forall a \in A), f(a) = g(a)$, es decir, $f = g$.

Demos aún un teorema muy general, de nuevo en forma algebraica. En un grupoide multiplicativo E provisto de un dominio de operadores Δ, consideremos dos congruencias $\mathscr{C}$ y $\mathscr{D}$ que verifican $\mathscr{C} \subseteq \mathscr{D}$ ("$\mathscr{C}$ *contenida en* $\mathscr{D}$", o "más fina" que $\mathscr{D}$) lo que significa: $x \mathscr{C} y$ *implica* $x \mathscr{D} y$. Entonces la clase $C = \mathscr{C}(x)$ de los elementos equivalentes a x módulo $\mathscr{C}$ está contenida en la clase $D = \mathscr{D}(x)$ de los elementos equivalentes a x módulo $\mathscr{D}$. Asociando a todo elemento C del conjunto cociente $E/\mathscr{C}$ este elemento D de $E/\mathscr{D}$, definimos una aplicación μ de $E/\mathscr{C}$ en $E/\mathscr{D}$. Además, μ es *suprayectiva* pues si damos una clase $D \in E/\mathscr{D}$ y un representante x de esta clase, tenemos $\mathscr{C}(x) \subseteq D = \mathscr{D}(x)$, y, por lo tanto, $D = \mu(C)$. Finalmente, μ es un homomorfismo: $\mu(CC') = \mu(C)\,\mu(C')$ pues, si x es un representante de C, x' un representante de C', x y x' son también representantes de $D = \mu(C)$ y de $D' = \mu(C')$ y el producto es un representante de CC' y de DD'. Tenemos pues

$$\mu(CC') = DD' = \mu(C)\,\mu(C').$$

Dado esto, puede pasarse de un elemento cualquiera x de E a su clase $\mathscr{D}(x)$ módulo $\mathscr{D}$ asociando en primer lugar a x su clase $C = \mathscr{C}(x)$ módulo $\mathscr{C}$ y después, a ésta, la clase imagen $\mu(C) = D$. Esto significa que el homomorfismo canónico δ de E sobre $E/\mathscr{D}$ es el