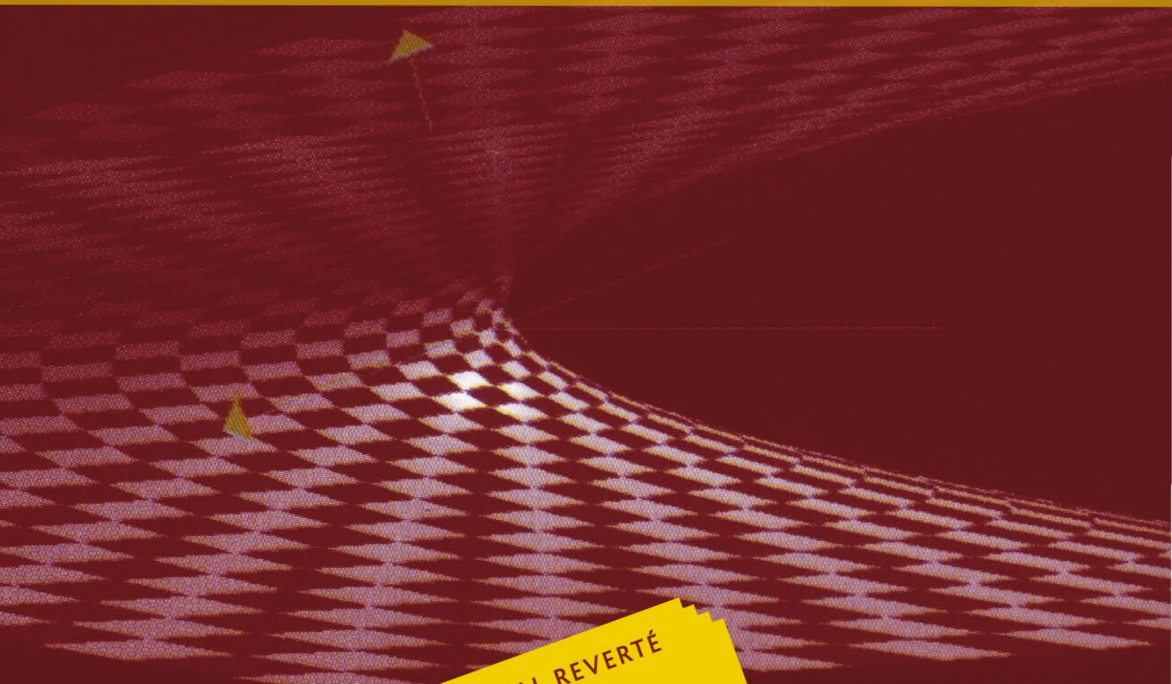


Problemas de álgebra moderna

A. Bigard \ M. Crestey \ J. Grappy



EDITORIAL REVERTÉ

Problemas de **álgebra moderna**

Problemas de álgebra moderna

A. Bigard \ M. Crestey \ J. Grappy



EDITORIAL
REVERTÉ

Barcelona · Bogotá · Buenos Aires · Caracas · México

Título de la obra original:

Problèmes d'Algèbre Générale

Edición original en lengua francesa publicada por

Dunod, Paris

Copyright © Dunod, Paris

Edición en papel:

© Editorial Reverté, S. A., 1975

ISBN: 978-84-291-5030-7

Edición e-book (PDF):

© Editorial Reverté, S. A., 2020

ISBN: 978-84-291-9110-3

Versión española por

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. ESPAÑA

Tel: (34) 93 419 33 36

reverte@reverte.com

www.reverte.com

Reservados todos los derechos. La reproducción total o parcial de esta obra, por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, queda rigurosamente prohibida, salvo excepción prevista en la ley. Asimismo queda prohibida la distribución de ejemplares mediante alquiler o préstamo públicos, la comunicación pública y la transformación de cualquier parte de esta publicación (incluido el diseño de la cubierta) sin la previa autorización de los titulares de la propiedad intelectual y de la Editorial. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (Art. 270 y siguientes del Código Penal). El Centro Español de Derechos Reprográficos (CEDRO) vela por el respeto a los citados derechos.

Prólogo

El incesante incremento del contenido y la enseñanza del Álgebra en estos últimos años, ha provocado un sensible desnivel entre la cota alcanzada por los usuales tratados teóricos, de perfección y altura rápidamente crecientes, y las colecciones de ejercicios y problemas para practicar y afirmar esas teorías. De este modo, bastantes libros de problemas que no hace muchos años ofrecían una interesante novedad, han venido a resultar hoy triviales, o, por lo menos, inadecuados para ilustrar con prácticas los textos utilizados en las clases.

A nuestro juicio, uno de los méritos de este libro, es que contribuye eficazmente a corregir el desnivel antedicho. Los autores de la obra, en su prólogo a la edición original, lo advierten así:

No encontramos hasta ahora, en nuestro idioma, una colección de problemas de Álgebra, con sus soluciones, destinada a los estudiantes del ciclo de especialización, en nuestras Facultades de Ciencias. Esta obra viene a llenar esta laguna. Los ejercicios y problemas que contiene han sido propuestos y resueltos en su mayor parte en las sesiones de trabajos prácticos de la Facultad de Ciencias de París. Otros han sido propuestos en exámenes. Los enunciados se agrupan al comienzo de cada uno de los capítulos del libro, y las soluciones desarrolladas se ofrecen a continuación.

El libro teórico en que éste se apoya, y viene a ilustrar con sus prácticas, es el titulado *Lecciones de Álgebra Moderna*, de P. DUBREIL y M. L. DUBREIL-JACOTIN, cuya traducción española ha publicado recientemente la Editorial REVERTÉ. Los dos textos se complementan, pues, eficazmente, aunque pueden utilizarse independientemente uno del otro, de acuerdo con las indicaciones que vamos a exponer. Los autores de estos *Problemas* han pretendido, con éxito, conservar el espíritu de aquellas lecciones. Sin embargo, en cuanto al modo de ordenar las materias, nos explican :

Nos ha parecido conveniente modificar la separación en capítulos. De este modo, después de un capítulo muy breve de generalidades (Cap. I), hemos reunido en el Cap. II todos los ejercicios referentes a las estructuras ordenadas (axioma de Zorn, retículos, grupos ordenados), y en los capítulos III y IV cuanto se refiere a los grupos, dedicando especialmente el IV a las cuestiones más técnicas (grupos finitos, subgrupos de Sylow, grupos abelianos, grupos libres, grupos resolubles). Del mismo modo, los ejercicios sobre la teoría de anillos se agrupan en los capítulos V y VI, este último dedicado a las intersecciones de ideales primarios y a las descomposiciones noetherianas. En fin, el Capítulo VII se dedica a la teoría de cuerpos y a la teoría de Galois (*).

Las cuestiones de mayor dificultad se han señalado con un asterisco. Este recurso didáctico no está al abrigo de toda crítica, pero por lo pronto tiene la ventaja de recordar al lector, que las cuestiones no están ordenadas en orden creciente de dificultad. Así, en cada etapa de su aprendizaje, no debe desanimarse por la dificultad que una cuestión le presente, en la seguridad de que detrás de ella encontrará otras perfectamente accesibles.

Las referencias a otros puntos del mismo tratado se hacen del modo más natural. Así (Ejercicio V, 26), por ejemplo, significa una llamada al Ejercicio 26 del Capítulo V. En cuanto a las indicaciones del tipo, por ejemplo (texto, IV, 2), señalan la posibilidad de consultar para ese punto la Sección 2 del Capítulo IV del mencionado texto de *Lecciones de Álgebra Moderna*. Pero esto no es una necesidad, y se pone sólo para comodidad del lector que disponga de ese libro, por cuanto los conocimientos implicados son de carácter general, y pueden consultarse (o suponerse sabidos) por el estudioso en cualquier otro texto de análogo nivel.

De todos modos, pensando que el vocabulario algebraico no tiene la universalidad deseable, hemos añadido a esta traducción una Terminología básica, que dará rápida información del significado de las expresiones utilizadas en este libro, y de sus eventuales sinónimos en otros textos. Pensamos que esto puede resultar útil, o al menos cómodo, a bastantes lectores.

R. Rodríguez Vidal

(*) No entra, pues, en el plan de este libro dedicar atención particular a los problemas de Álgebra lineal (*Lecciones de Álgebra Moderna*, Cap. IX. Espacios vectoriales). Al lector interesado en este tema le recomendamos el libro teórico, con muchos ejercicios resueltos, *Lecciones de Álgebra lineal*, de PAIGE-SWIFT (trad. de R. R. V.). Quien se interese de modo particular en la Teoría de matrices y su práctica, puede también consultar con provecho la *Introducción al Análisis matricial*, de L. BELLMAN (trad. de J. J. ETAYO MIQUEO). Ambos libros han sido publicados por la Editorial REVERTÉ.

Terminología y notaciones(*)

El traductor ha respetado disciplinadamente, como debe hacerse, el vocabulario científico de los autores traducidos. Ahora, con el fin de facilitar al lector el manejo de este libro, evitándole tal vez alguna consulta a otros textos teóricos, nos parece útil glosar brevemente el significado que se da aquí a los términos más especializados e indicar eventualmente algunas locuciones sinónimas utilizadas asimismo en la literatura matemática en español.

Por consiguiente, no se ha pretendido ofrecer en esto un riguroso índice alfabético o analítico, por lo que se omite desde luego la mención de muchas expresiones inequívocas de uso universal, que son parte básica del vocabulario usual del Álgebra.

1. Los **conjuntos numéricos** usuales se indican del modo habitual: $\mathbf{N}$ es el semianillo de los naturales; $\mathbf{N}^* = \mathbf{N} - \{0\}$; $\mathbf{Z}$ es el anillo de los enteros relativos; $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ son, respectivamente los cuerpos de los racionales, reales y complejos.

2. Una **aplicación** (sinónimo: *función uniforme*) del conjunto A en el conjunto B , indicada $A \rightarrow B$, se califica así: **suprayectiva** (sinónimos: *de A sobre B*; *exhaustiva*) si cada elemento de B es imagen de al menos uno de A ; **inyectiva** (sinónimos: *uno-a-uno*; *unívoca*; *inequívoca*) si cada elemento de B tiene a lo más un original en A ; **biyectiva** (o *biunívoca*) si es a la vez inyectiva y suprayectiva (es decir, *uno-a-uno y sobre*). [Otros autores llaman aplicación *biunívoca* la que aquí hemos dicho uno-a-uno, por lo que luego deben distinguir entre las aplicaciones biunívocas *en*, y las biunívocas *sobre*].

Cada aplicación $f: A \rightarrow B$ define en A una **equivalencia de aplicación**. Se define: $a \equiv b(f)$ en A , si y sólo si $f(a) = f(b)$ en B .

3. Si en los conjuntos A y B están definidas sendas leyes de composición interna, una aplicación h de A en B que respete esas leyes de composición

(*) N. del T.

(es decir, que sea compatible con ellas) se llama **homomorfismo** de A en B (símbolo: $(h)A \rightarrow B$). Si, además, la aplicación es exhaustiva se llama **epimorfismo** (sinónimo: *homomorfismo sobre*; símbolo: $(h)A \sim B$). Si es biyectiva se llama **isomorfismo** (símbolo: $(h)A \simeq B$). [Ciertos autores llaman isomorfismo al caso correspondiente a una aplicación inyectiva; en tal caso cabe la distinción entre *isomorfismo en* e *isomorfismo sobre*]. Un homomorfismo de E en E se llama **endomorfismo** de E . Un isomorfismo de E sobre E se llama **automorfismo** de E .

Cuando en los conjuntos A y B hay definidas sendas relaciones (por ejemplo, si son conjuntos ordenados) y la aplicación h las respeta, valen las mismas denominaciones anteriores. De este modo cabe hablar, por ejemplo, de un *homomorfismo ordenado* de A en B .

4. Sea E un conjunto con una operación binaria que denotamos con $*$. Para esta ley algunos elementos $a, b, c, \dots$ pueden calificarse como sigue.

Se dice que a es un elemento **simplificable a la izquierda**, si

$$a*x = a*y \Rightarrow x = y, \quad \forall x, y \in E.$$

Lo análogo define un elemento *simplificable a la derecha*. Un elemento se llama **simplificable** (también *cancelable*, o *regular*) cuando es simplificable de ambos modos: a la izquierda y a la derecha. Si todos los elementos tienen esa propiedad, decimos que E es un **conjunto regular**.

Elemento **idempotente** es el a que cumple $a*a = a$. (Si todo a de E es idempotente, se dice que E , y también la ley de composición, son idempotentes.)

Elemento **lícito a la derecha**, es el z que cumple $z*a = z, \forall a \in E$. Lo análogo define un elemento lícito a la izquierda y elemento **lícito**: el que lo es de los dos modos. Si este último existe es único, y en notación multiplicativa suele representarse con 0.

Elemento **neutro a la izquierda**, es el e que cumple $e*x = x, \forall x \in E$. Lo análogo para elemento neutro a la derecha. Es elemento **neutro** el que lo es a los dos lados. Si existe es único. En notación multiplicativa se suele representar con 1. Se le llama también elemento *unidad*, o elemento *idéntico*, para la ley considerada.

En relación a un elemento neutro (al menos a un lado) e , se dice que a' es un **inverso a la derecha** de a si cumple $a*a' = e$. En tal caso diremos que a es *inversible a la derecha*. (Lo análogo a la izquierda.)

En relación al elemento neutro (a los dos lados) e , si para un elemento a existe otro a' con $a*a' = a'*a = e$, se dice que a es **simetrizable** y que a y a' son **simétricos**. (En notación multiplicativa es más usual decir **inversos**, y en notación aditiva es frecuente decir **opuestos**.)

Dos elementos x, y , son **permutables** (o *conmutan*) cuando es $x*y = y*x$.

Un elemento a se dice **central** cuando conmuta con todos los de E . El conjunto C de elementos centrales es el **centro** de E (puede ser $\emptyset$). Si el centro

es $C = E$, la operación se llama *conmutativa*, y el conjunto E se dice **conmutativo** o **abeliano**.

En la igualdad $x*a = m$, se dice que x es el *complemento a la izquierda* (o bien, *cociente a la izquierda*) de m por a .

Un conjunto E verifica la *condición de existencia de cocientes a la izquierda* si cualesquiera sean a, m en E existe al menos un cociente a la izquierda de m por a .

El **axioma de cocientes a la izquierda** en un conjunto E , es la suposición de existencia y unicidad del cociente a la izquierda de m por a , para todo par de elementos a, m en E . En tal caso, la operación que asocia el par (m, a) con el x tal que $x*a = m$, se llama **operación inversa a la izquierda** de la operación considerada.

Análogas son las definiciones *a la derecha*. El **axioma de los cocientes** es la conjunción del axioma de cocientes a la izquierda y el de cocientes a la derecha.

5. Sea E un conjunto con una operación binaria que denotamos multiplicativamente. Indicamos con $a, b, c, \dots$ elementos de E , y con $A, B, C, \dots$ subconjuntos (o **partes**) de E . Ponemos:

$$aA = \{ax; x \in A\} \quad AB = \{ab; a \in A, b \in B\}$$

A es **parte estable** de E , para la operación considerada, si $a \in A$ y $b \in A \Rightarrow ab \in A$. [Otros autores dicen que A es una parte *cerrada*, o *conexa*, para esa operación.]

A es **parte lícita a la derecha** de E , para la operación considerada, si es $Ax = A, \forall x \in E$. (De donde es claro lo que significan parte *lícita a la izquierda* y *parte lícita*.)

U es **parte unitaria a la derecha** de E , si $u \in U$ y $xu \in U \Rightarrow x \in U$. (Como de costumbre es lo que significa parte *unitaria a la izquierda* y *parte unitaria*. Entre todas ellas se incluye el $\emptyset$.)

6. Se llama **orden**, en un conjunto E , a una relación binaria $\mathcal{R}$ que para todos los elementos $a, b, c, \dots$ de E cumple las siguientes relaciones

1. *Reflexiva*: $a\mathcal{R}a$.
2. *Transitiva*: $a\mathcal{R}b$ y $b\mathcal{R}c$ implica $a\mathcal{R}c$.
3. *Antisimétrica* (o *propia*): $a\mathcal{R}b$ y $b\mathcal{R}a$ implica $a = b$.

Diremos que la relación es de **orden total** cuando no hay elementos incomparables, esto es, cuando se añade la siguiente condición.

4. *Alternativa*: si no es $a\mathcal{R}b$, es $b\mathcal{R}a$.

[Otros autores llaman *orden parcial*, o *semiorden*, etc., a la relación definida por 1., 2., 3., que deja la posibilidad en E de elementos incomparables.

En este caso, es claro que ellos llaman *orden* a lo que nosotros hemos llamado *orden total*.]

Un **conjunto ordenado**, u **ordenación**, E , es un conjunto en el que se ha definido una relación de orden. Se llama **cadena** a un conjunto totalmente ordenado, esto es, con una relación de orden total.

De modo general una relación de orden la indicaremos con el signo $\subseteq$. Resulta así claro el significado de los signos $\subset$ e $=$, que en nuestra notación indican relaciones incompatibles: no puede ser simultáneamente $a \subset b$ y $a = b$. Pero pondremos otro signo, $\leq$ ó $\leqslant$, cuando el orden considerado pueda confundirse con un orden de inclusión conjuntista.

[Otros autores emplean el signo $\subset$ con el mismo significado que aquí hemos atribuido al signo $\subseteq$.]

7. Sea E un conjunto ordenado.

Elemento **inferior** (o *elemento nulo*, o *mínimo*) de E es, si existe, el elemento $z \in E$ tal que $z \subseteq a$, $\forall a \in E$. (Si existe es único.)

El elemento **superior** (o *elemento universal*, o *máximo*), u , de E , se define simétricamente al antedicho, por dualidad: $u \in E$ tal que $a \subseteq u$, $\forall a \in E$.

De dos elementos x, y , de E , se dice que x **cubre a** y si es $y \subset x$ y no existe $c \in E$ tal que $y \subset c \subset x$. También se dice entonces que x e y son elementos **contiguos**. Los **átomos** de E son, si existen, los contiguos del elemento inferior de E .

Llamamos **sección inicial** de x , y representamos por $\overset{\leq}{x}$ (también por S_x) el conjunto de los elementos $a \in E$ tales que $a \subseteq x$. Dualmente se define la *sección terminal* de x , indicada por $\overset{\geq}{x}$.

Un subconjunto $A \subset E$, que tenga la propiedad de que $x \in A \Rightarrow \overset{\leq}{x} \subset A$, es decir, que con cada elemento x de E incluye a todos sus anteriores, se llama **parte hereditaria** de E .

8. Sea A una parte del conjunto ordenado E .

Elemento **máximo** de A es, si existe, el $m \in A$ tal que $x \subseteq m$, $\forall x \in A$. Simétricamente a éste se define, por dualidad, el elemento **mínimo** de A .

Elemento **maximal** de A : Es, si existe, todo $m \in A$ tal que $m \not\subset x$, $\forall x \in A$. Dualmente se caracterizan los elementos **minimales** de A .

Elemento **mayorante** (o *cota superior*) de A es, si existe, todo elemento $s \in E$ tal que $x \subseteq s$, $\forall x \in A$. La definición de elemento **minorante** (o *cota inferior*) es dual de la anterior.

El **supremo** de A (sinónimo: *extremo superior* de A) es, si existe el $m \in E$, cota superior mínima de A . Dualmente se define el **ínfimo** de A (o *extremo inferior*, o *cota inferior máxima*).

El subconjunto A se dice **mayorado** (o *acotado superiormente*) si tiene en E alguna cota superior. (Dualmente, se dice **minorado** si tiene cota inferior). Un conjunto A se dice **acotado**, cuando es simultáneamente mayorado y minorado.

El conjunto E se dice **inductivo** cuando toda cadena en E admite un elemento mayorante. Se dice que E es **fuertemente inductivo** cuando toda cadena en E admite una mayorante mínimo.

Axioma de Zorn. *Todo conjunto inductivo admite al menos un elemento maximal.*

Un conjunto ordenado E satisface a la **condición maximal**, si todo subconjunto no vacío de E tiene al menos un elemento maximal. Esto equivale a que toda cadena de E tiene un elemento máximo.

Diremos que E cumple la **condición de cadena ascendente** si toda sucesión estrictamente creciente de elementos de E , $a_1 \subset a_2 \subset \dots$ es finita.

De modo simétrico a lo dicho se definen la **condición minimal** y la de **cadena descendente**.

Se dice que E está **bien ordenado** (o que tiene un **buen orden**) cuando cualquier parte no vacía de E tiene un elemento mínimo.

Axioma de Zermelo. *Todo conjunto E puede ser bien ordenado.*

9. Sean E un conjunto y $\mathcal{P}(E)$ el conjunto de las partes de E . Un subconjunto de $\mathcal{P}(E)$ suele llamarse **familia**.

El conjunto $\mathcal{P}(E)$ se considera ordenado por inclusión.

Axioma de elección. *Para todo E se puede definir una aplicación f de $\mathcal{P}(E)$ en E , con la que a cada $A \in \mathcal{P}(E)$ no vacía se asocia un elemento $a = f(A) \in A$. (Esta f se llama **función de elección**. El $f(A)$ se llama elemento *distinguido* de A , o elemento *elegido*.)*

Llamamos elemento **$\cap$ -irreducible** de una familia $\mathcal{F}$ a todo aquel $F \in \mathcal{F}$ que no es intersección de dos $F_1, F_2 \in \mathcal{F}$ que le contienen estrictamente.

Un **sistema de clausura** (o *familia de Moore*) es una familia $\mathcal{F}$ de partes de E , cuando E pertenece a ella y, además, con cualesquiera partes de E que estén en la familia está su intersección:

1. $E \in \mathcal{F}$; 2. si $\mathcal{F}' \subset \mathcal{F}$, también $\bigcap_{F \in \mathcal{F}'} F \in \mathcal{F}$.

Aplicación de clausura φ relativa a una familia de Moore $\mathcal{F}$, es la que a cada parte A de E asocia la mínima parte $\bar{A} \in \mathcal{F}$ que contiene a A . Las imágenes, $\bar{A}$, se llaman **partes cerradas**, relativamente a φ (o a $\mathcal{F}$). La aplicación de clausura es 1. *extensiva*, $A \subseteq \bar{A}$; 2. *isótoma*, $A \subseteq B \Rightarrow \bar{A} \subseteq \bar{B}$ y 3. *idempotente*, $\bar{\bar{A}} = \bar{A}$. Recíprocamente, en una aplicación φ de $\mathcal{P}(E)$ en sí con estas tres propiedades, el conjunto de imágenes es una familia de Moore.

Equivalencia de clausura, relativa a una $\mathcal{F}$ de Moore dada (o a su φ correspondiente) es la que se define en $\mathcal{P}(E)$ por $A \equiv B$ si y sólo si $\bar{A} = \bar{B}$.

Se llama **filtro** una familia $\mathcal{G}$ de partes de E estables para la intersección, lícitas para la unión y que no contienen al $\emptyset$. O bien, lo que se demuestra equivalente:

1. $F_1 \in \mathcal{G}$ y $F_2 \in \mathcal{G} \Rightarrow F_1 \cap F_2 \in \mathcal{G}$; 2. $F \in \mathcal{G}$ y $X \supset F \Rightarrow X \in \mathcal{G}$; 3. $\emptyset \notin \mathcal{G}$.

Familia $\cup$ -**inductiva** de partes de E , es aquella familia $\mathcal{U}$ tal que si $\mathcal{C}$ es una cadena sacada de $\mathcal{U}$, entonces $X^* = \bigcup_{x \in \mathcal{C}} X$ es un mayorante de los elementos de la cadena. En este caso X^* es mayorante mínimo de $\mathcal{C}$.

Si E es un conjunto ordenado, el conjunto $\mathcal{U}$ de las cadenas $\mathcal{C}$ de E , ordenadas por la inclusión de conjuntos en $\mathcal{P}(E)$ es una familia $\cup$ -inductiva.

Axioma de Hausdorff. En todo conjunto ordenado E existe una cadena maximal.

10. Sea E un conjunto ordenado.

Diremos que E es **filtrante superiormente** cuando todo subconjunto de dos elementos está mayorado:

$$\forall a, b \in E, \exists c \in E, \text{ con } c \supseteq a \text{ y } c \supseteq b.$$

De modo simétrico se define un conjunto **filtrante inferiormente**. [En otros autores se dice *dirigido* en vez de filtrante.] Conjunto **filtrante** es el que lo es de ambos modos: superiormente e inferiormente.

Llamamos **supsemirretículo** (también $\vee$ -*semirretículo*) al conjunto ordenado E donde todo par de elementos $\{a, b\}$ tiene un supremo, designado por $a \vee b$ (también por $a \cup b$). De modo simétrico se define el *infsemirretículo* (o $\wedge$ -*semirretículo*), donde el ínfimo del par de elementos $\{a, b\}$ se indica $a \wedge b$ (también $a \cap b$).

Se dice que un supsemirretículo E es **completo** cuando toda parte de él, $A \subset E$, tiene un supremo. Éste se indica por $\vee A$.

Un **retículo** es un conjunto ordenado T , que es a la vez sup e infsemirretículo. Cabe también definir un retículo como un conjunto T en el que se han definido dos operaciones, indicadas $\vee$ y $\wedge$, que son asociativas, idempotentes, conmutativas, y ligadas por la ley de absorción: $a \vee (a \wedge b) = a$, $a \wedge (a \vee b) = a$.

La correspondencia entre ambas definiciones se establece poniendo:

$$\text{ínfimo de } \{a, b\} = a \wedge b; \text{ supremo de } \{a, b\} = a \vee b.$$

11. Sea T un retículo. Cabe considerar en él diversas propiedades suplementarias, que los califican como sigue (las condiciones son para $\forall a, b, c \in T$).

T distributivo: Cuando

$$1. a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad 2. a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

T modular: Cuando,

$$\text{siempre que sea } a \subset c, \text{ es } a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

T con cotas universales. Son los retículos que tienen un elemento máximo (de ordinario indicado 1, o u) y un elemento mínimo (de ordinario indicado 0, u o).

T complementado. Es un retículo con elementos máximo y mínimo y la propiedad de que para todo elemento $a \in T$ se puede encontrar otro, a^* , con la condición $a \wedge a^* = 0$ y $a \vee a^* = 1$. Se dice que a^* es un **complemento** de a (puede no ser único).

Si un retículo complementado es distributivo, el complemento de cada a es único, y se indica por a' . Un retículo complementado y distributivo se llama **retículo de Boole**.

T completo. Un retículo es completo cuando todo subconjunto de él, $A \subset T$, tiene un supremo y un ínfimo.

Teorema de MacNeille. *Todo conjunto ordenado E puede sumergirse en un retículo completo T de manera que el supremo y el ínfimo se conserven.*

En un retículo completo L , se dice que a es un elemento **compacto** de L si $a \subseteq \bigvee_{j \in J} x_j$, implica la existencia de una parte finita F de J de modo que $a \subseteq \bigvee_{j \in F} x_j$. Un retículo es de *generación compacta* si todos sus elementos son cota superior (finita o infinita) de compactos.

12. Se llama **ideal** de un retículo T (y también de un $\vee$ -semirretículo) toda parte $\mathcal{I} \subset T$ que es 1) hereditaria, 2) estable para $\vee$:

$$1) a \in \mathcal{I} \text{ y } x \subseteq a \Rightarrow x \in \mathcal{I}. \quad 2) a \in \mathcal{I} \text{ y } b \in \mathcal{I} \Rightarrow a \vee b \in \mathcal{I}.$$

Un ideal se llama **maximal** cuando es maximal entre los ideales que no contienen el 1 de T . Se dice **primo** cuando $a \wedge b \in \mathcal{I}$ implica $a \in \mathcal{I}$ ó $b \in \mathcal{I}$. Se dice **irreducible** cuando no puede ser intersección de dos ideales de T que le contengan estrictamente: $\mathcal{I} = \mathcal{J} \cap \mathcal{K} \Rightarrow \mathcal{I} = \mathcal{J}$ ó $\mathcal{I} = \mathcal{K}$. (Aquí $\mathcal{J} \cap \mathcal{K}$ significa el conjunto de $j \wedge k$ con $j \in \mathcal{J}$ y $k \in \mathcal{K}$).

13. En cuanto sigue se trata de **álgebras** asociativas (damos aquí a la palabra *álgebra*, y a *subálgebra*, el significado definido en el enunciado II-8).

Semigrupo es un conjunto S con una ley de composición interna asociativa. Se llama **casigrupo** cuando, además, todo elemento es regular (es decir, si vale la ley de simplificación). [Otros autores llaman *monoide* a lo que nosotros semigrupo, y llaman *semigrupo* a lo que nosotros casigrupo.]

El **semigrupo simétrico** sobre un conjunto E , se define en enunciado I-4. (Un caso particular notable es el de **grupo simétrico** sobre n elementos.)

En correspondencia a cada elemento a de S se define una **traslación a la izquierda** (y a la derecha), como se define en el enunciado I-6.

Los conceptos de **grupo** y **subgrupo** son inequívocos y huelga definirlos aquí. Sea G un grupo, y $a, b, c, \dots$ elementos suyos. Adoptamos notación multiplicativa.

Grupo **monógeno** es el que admite un generador de un solo elemento. Grupo **cíclico** es el monógeno y finito. Grupo **monógeno generalizado**, se define en el enunciado IV-27. Grupo **hipercíclico** se define en el enunciado IV-9.

Grupo **ordenado** (lo mismo para *semigrupo*) es aquel donde hay un orden compatible con la operación. Es decir, la operación es **isótoma**: $a \leq b \Rightarrow ax \leq bx$ y $xa \leq xb$, $\forall x \in G$. El **cono positivo** de un grupo ordenado, se define en el enunciado II-39.

El elemento axa^{-1} se llama **transformado** del x por a . Dos elementos se dicen **conjugados** si uno es un transformado del otro. A cada elemento a de G se asocia una aplicación de G sobre sí definida por $x \rightarrow axa^{-1}$, $\forall x \in G$, que es un automorfismo de G . A éstos se les llama **automorfismos internos** de G .

El subgrupo xHx^{-1} se dice **transformado** del H por x . Los dos subgrupos se dicen **conjugados**.

A cada subgrupo H de G , viene asociada en G una equivalencia $\mathcal{R}$ regular a la derecha con **clases a la derecha** xH y una equivalencia $\mathcal{R}'$ regular a la izquierda con **clases a la izquierda** Hx .

Subgrupo **distinguido** de G es todo H que cumple la condición $xH = Hx$, $\forall x \in G$. [Se les llama también subgrupos *invariantes* de G , o *normales*.]

Subgrupo **casi distinguido** de G se define en III-29.

Subgrupo **conmutador** de G es el engendrado por el conjunto de los *conmutadores* en G , $xyx^{-1}y^{-1}$; se le llama también grupo **derivado** de G , $D(G)$; y el k -ésimo grupo derivado de G , $D^k(G)$, se define por recurrencia, en IV-20.

Subgrupo **denso**, se define en III-28; subgrupo **aislado** se define en III-35.

El **normalizador** y el **centralizador** de una parte A de G , se definen en el enunciado III-31. La **holomorfía** de G se define en la solución de III-33.

Diremos que G es **producto directo** de sus subgrupos A y B si y sólo si: 1) A y B son subgrupos distinguidos de G , 2) $G = AB$ y 3) $A \cap B = \{e\}$. En este caso se escribe $G = A \times B$. El **producto semidirecto** se define en III-36.

En notación aditiva, el grupo abeliano G es **suma directa** de sus subgrupos A y B , si $A + B = G$ y $A \cap B = \{0\}$. En este caso se escribe $G = A \oplus B$.

Grupo abeliano **libre** es el que es suma directa de sus subgrupos monógenos.

Se llama **serie normal** a toda cadena finita que va de G a $E = \{e\}$ (donde e es el elemento unidad del grupo),

$$G_0 = G \supset G_1 \supset G_2 \supset \dots \supset G_K = E,$$

con esta condición suplementaria: todo G_i es subgrupo distinguido de G_{i-1} .

Dos series normales son **isomorfas** cuando tienen la misma longitud, y los grupos cocientes, G_{i-1}/G_i , de ambas se pueden poner en correspondencia biyectiva donde los correspondientes sean isomorfos.

Teorema de Schreier. *Dos series normales cualesquiera de un grupo G , admiten subdivisiones isomorfas.*

Se llama **serie de composición** de un grupo G una serie normal finita maximal de G a E . Esto quiere decir que es (si existe) una serie normal que no admite subdivisiones, lo que equivale a que todo grupo cociente G_{i-1}/G_i sea **simple**, es decir, no tenga ningún subgrupo distinguido propio.

Teorema de Jordan Hölder. Si un grupo G admite diversas series de composición, dos cualesquiera de ellas son isomorfas.

Un grupo **resoluble** es el que admite una serie normal cuyos grupos cociente son abelianos. Si admite una serie de composición, ésta tiene sus grupos cocientes a la vez abelianos y simples, luego cíclicos de orden primo.

La nomenclatura relacionada con los **Teoremas de Sylow** es inequívoca, por lo que no la recordamos aquí.

16. Al referirnos a un **anillo** no le suponemos necesariamente con elemento unidad e . Si lo tiene se llama anillo **unitario**. Al referirnos a un **cuerpo** le sobreentendemos generalmente conmutativo. [Un cuerpo no conmutativo se llama también, en otros autores, *cuerpo oblicuo*, *hemicuerpo*.] **Campo** es sinónimo de cuerpo conmutativo. Por último, *anillo de división* significa un cuerpo sobre cuya conmutatividad o no, nada se presupone.

Sean A un anillo y $a, b, c, \dots$ sus elementos.

Si ni a ni b son cero, pero $ab = 0$ se dice que a es un **divisor de cero** a la izquierda, y que b lo es a la derecha [también se les dice *subceros*]. Un anillo **íntegro** es el que no tiene divisores de 0.

En un A con elemento unidad e , se llaman **unidades** los elementos inversibles. Su conjunto, U , es multiplicativamente el **grupo de las unidades**.

Dominio de integridad es un anillo conmutativo e íntegro [otros autores exigen que también sea unitario].

Anillo de Boole es un anillo conmutativo, idempotente y con elemento unidad.

Característica de un anillo A (en particular, de un cuerpo C) es, si existe, el menor entero positivo m tal que $mx = 0$, $\forall x \in A$. Si no existe se dice que A es de característica **nula** [otros dicen *infinita*, o *sin característica*]. Si A es íntegro y $\neq \{0\}$, la característica o es 0 o es un primo p . Si hay elemento unidad e , este p es el orden del subgrupo aditivo $I' = (e) = (0, e, \dots, (p-1)e)$, que en tal caso constituye el llamado **subcuerpo mínimo** de A .

Cuerpo primo de un cuerpo C , es la intersección $II = \{\bar{e}\}$ de todos los subcuerpos de C . Si es el caso antedicho, coincide con I' .

El **anillo producto** de otros dos A y B , es el conjunto de pares (a, b) con $a \in A$, $b \in B$ y

$$(a, b) + (a', b') = (a + a', b + b'); \quad (a, b)(a', b') = (aa', bb').$$

Ideal a la derecha del anillo A , es un subanillo $\mathfrak{d}$ de A multiplicativamente estable a la derecha: $\mathfrak{d}A = A$. Un ideal bilátero, $\mathfrak{m}$, se llama simplemente **ideal**: $\forall a, b \in A$, $a \in \mathfrak{m}$ y $b \in \mathfrak{m} \Rightarrow a - b \in \mathfrak{m}$; $\mathfrak{m}A = A\mathfrak{m} = \mathfrak{m}$.

Dado un $a \in A$, el conjunto $\mathfrak{d}$ de los elementos $d \in A$ con $ad = 0$ es un ideal a la derecha que se llama **anulador** a la derecha de a . Análogamente a la izquierda, y el **anulador** (bilátero) de a .

La **suma, producto e intersección** (conjuntista) de dos ideales de A , son también ideales, definidos del modo natural:

$$a + b = \{a + b; a \in a, b \in b\} \quad ab = \{ab; a \in a, b \in b\}$$

Residual del ideal a por el b , indicado $a : b$, es el mayor ideal c que multiplicado por b queda contenido en a . Es decir:

$$a : b = c = \{x; x \in A, xb \subseteq a\}$$

17. Sean A un anillo conmutativo, $a, b, \dots$ ideales de A , y $a, b, \dots$ elementos genéricos de A .

Ideal primo es aquel, p , en el que $ab \in p$ y $a \notin p$, implica $b \in p$. Se llama **ideal primario** un ideal q tal que $ab \in q$ y ninguna potencia de a pertenece a q implica $b \in q$.

Diremos que s es ideal **semiprimo** de A cuando todo elemento de A con alguna potencia en s es también elemento de s .

Se llama **radical** de un ideal m , y se indica $\mathcal{R}(m)$, el mínimo ideal semiprimo que contiene a m . Esto es: el conjunto de elementos r del anillo A que tienen alguna de sus potencias en m .

Diremos que un ideal es **p -primario**, si es primario y tiene el ideal primo p como radical.

Un ideal de radical primo se llama **casiprimario**. Si c es casi primario, equivale a decir: $ab \in c$ y ninguna potencia de a pertenece a c , implica que alguna potencia de b pertenece a c .

Ideal **q primario fuerte** en el anillo A , es el que siendo a, b ideales de A , cuando $ab \subseteq q$ y $a \not\subseteq q$, alguna potencia de b está contenida en q .

Todo ideal primo es semiprimo. Todo ideal primo es primario y coincide con su radical. Todo ideal primario fuerte es primario. Todo ideal primario es casiprimario.

18. Una intersección finita de ideales primarios se dice **intersección normada** cuando estos ideales tienen radicales diferentes y ningún ideal es superfluo en la intersección. Tales ideales son los **componentes** de la intersección.

Llamaremos **componente aislado** de la intersección $q_1 \dots q_r$ a toda intersección parcial de ideales primarios q_i tales que sus radicales no incluyan a ninguno de los radicales de los otros ideales primarios.

Diversos conceptos de interés secundario, y por tanto generalmente menos conocidos se definen en los enunciados. Hemos ya citado algunos, y añadiremos: anillo **casi local** (en V-20), anillo **integralmente cerrado** (en VII-13) elementos **idempotentes descomponibles** (en VI-29), elementos **indivisibles** (en VI-28) y, finalmente, **frontera** de un ideal por otro (en VI-24).

En cuanto a la restante terminología relativa a la extensión de cuerpos y teoría de Galois no ofrece posibilidad de confusión, por lo que es innecesario glosarla aquí.

Índice de materias

Terminología y notaciones	IX
CAPÍTULO I. Leyes de composición	1
Enunciados	1
Soluciones.....	6
CAPÍTULO II. Estructuras ordenadas	17
Enunciados	17
Soluciones.....	30
CAPÍTULO III. Grupos. Teoría elemental	59
Enunciados	59
Soluciones	70
CAPÍTULO IV. Grupos (complementos)	97
Enunciados	97
Soluciones.....	108
CAPÍTULO V. Anillos	135
Enunciados	135
Soluciones.....	147
CAPÍTULO VI. Ideales primarios. Anillos nœtherianos	177
Enunciados	177
Soluciones.....	186
CAPÍTULO VII. Cuerpos. Ecuaciones algebraicas	209
Enunciados	209
Soluciones.....	221

Leyes de Composición

Enunciados

1

Si en un semigrupo D existe un elemento a tal que $D = aDa$, hay en D un elemento unidad.

2

Sea D un semigrupo con algún elemento lícito z y elemento unidad e , tal que e y z sean los únicos elementos idempotentes de D . Demostrar que si un producto ab es inversible, ambos elementos a y b son inversibles.

3

Sea D un semigrupo con un número finito de elementos, en el que las igualdades $x = ay$, $y = bx$ implican $x = y$. Demostrar que en D hay al menos un elemento lícito a la izquierda.

4

Siendo E un conjunto cualquiera, llamemos semigrupo simétrico sobre E al conjunto $H(E)$ de las aplicaciones de E en E , con la ley de composición de aplicaciones.

1.º Sea J el conjunto de las $\alpha_a \in H(E)$ definidas por

$$(\forall x \in E) \quad \alpha_a(x) = ax.$$

Demostrar que J es el conjunto de los elementos lícitos a la derecha en $H(E)$, y elemento mínimo del conjunto de partes lícitas a la izquierda de $H(E)$.

2.º Sean ξ, η dos elementos de $H(E)$. Demostrar que la hipótesis

$$(\forall \alpha \in J) \quad \xi \circ \alpha = \eta \circ \alpha$$

implica $\xi = \eta$.

3.° Sea Φ una aplicación de J en J . Demostrar que existe una aplicación única φ de E en E tal que

$$(\forall a \in J) \quad \Phi(a) = \varphi \circ a.$$

Demostrar que la aplicación F de $H(J)$ en $H(E)$ definida por $\varphi = F(\Phi)$ es un isomorfismo de semigrupos.

4.° Sea λ una biyección de J . Demostrar que la aplicación $\mathcal{A}_\lambda$ de $H(E)$ en sí mismo definida por

$$\forall \xi \in H(E), \quad \mathcal{A}_\lambda(\xi) = \lambda \circ \xi \circ \lambda^{-1}, \quad \lambda = F(\lambda)$$

es un automorfismo de $H(E)$ que prolonga λ .

5.° Demostrar que todo automorfismo de $H(E)$ es de la forma $\mathcal{A}_\lambda$ definida en el punto 4.°.

5

Sean E un conjunto cualquiera, $H(E)$ el semigrupo simétrico sobre E (ejercicio precedente). A cada elemento ξ de $H(E)$ se asocian su equivalencia de aplicación $\mathcal{N}_\xi$ y la imagen S_ξ de E por ξ :

$$S_\xi = \{\xi(x), x \in E\}.$$

Si ξ_1 y ξ_2 son dos elementos dados de $H(E)$, establecer los resultados siguientes:

1.° Para que exista $\eta \in H(E)$ tal que $\xi_2 = \eta \circ \xi_1$, es necesario y suficiente que $\mathcal{N}_{\xi_1} \subseteq \mathcal{N}_{\xi_2}$.

2.° Para que exista $\eta \in H(E)$ tal que $\xi_2 = \xi_1 \circ \eta$, es necesario y suficiente que $S_{\xi_1} \subseteq S_{\xi_2}$.

6

Sean D un semigrupo multiplicativo, $S(D)$ el semigrupo simétrico sobre D (ejercicio I, 4). A todo elemento a de D se hace corresponder la traslación a la izquierda asociada, es decir, el elemento γ_a de $S(D)$ definido por

$$(\forall x \in D), \quad \gamma_a(x) = ax.$$

1.° Demostrar que el conjunto de las traslaciones a la izquierda es una parte estable de $S(D)$ y que la aplicación $a \rightarrow \gamma_a$ de D en $S(D)$ es un homomorfismo de semigrupos. Deducir que si D posee un elemento unidad, es isomorfo a un subsemigrupo de $S(D)$.

2.° Se supone que D no tiene elemento unidad. Definir un conjunto D_1 tal que D sea isomorfo a un subsemigrupo del semigrupo simétrico $S(D_1)$.

7

Sea E un conjunto con una ley de composición, indicada por yuxtaposición, que verifica algunos de los axiomas siguientes (siendo a, b, c, d , elementos cualesquiera de E):

1. $(ab)(cd) = (ac)(bd)$;
2. $aa = a$;
3. $a(bc) = (ab)(ac)$;
4. $(ab)c = (ac)(bc)$.

Establecer los siguientes resultados:

- 1.° Los axiomas 1 y 2 implican los axiomas 3 y 4.
- 2.° Cuando se cumple el axioma 1, el conjunto de idempotentes es una parte estable en la que se cumplen los axiomas 3 y 4.
- 3.° Cuando se cumplen los axiomas 3 y 4 el conjunto de idempotentes es una parte lícita.
- 4.° Con la existencia de un elemento unidad bilátera, el axioma 1 implica la conmutatividad y la asociatividad.
- 5.° Con la existencia de un elemento unidad a la derecha, el axioma 3 implica el axioma 2.

8

Sea E un conjunto con una ley de composición indicada por yuxtaposición, que verifica algunos de los axiomas siguientes (en los que a, b, c, d designan elementos cualesquiera de E):

1. $ab = c$ implica $ac = b$;
2. $ab = ba$;
3. $(ab)(cd) = (ac)(bd)$;
4. $(ab)c = a(bc)$ implica $a = c$.

1.° Demostrar que los axiomas 1 y 2 implican la existencia de cocientes y la regla de simplificación.

2.° Demostrar que los axiomas 1, 2 y 3 implican, para elementos a, b, c, d cualesquiera de E , la igualdad $[(ab)c]d = [(ad)c]b$.

3.° Supuesto que se cumplen los axiomas 1, 2, 3 y 4, demostrar los siguientes resultados:

- a) Toda igualdad de la forma $aa = bb$ implica $a = b$;
- b) toda igualdad de la forma $(aa)(bb) = cc$ implica $ab = c$;
- c) si E es un conjunto finito, el número N de sus elementos es impar.

Dar un ejemplo en el que sea $N = 3$.

9

Sea E un conjunto con una ley de composición $(x, y) \rightarrow x \bullet y$ y sean α, β, γ tres biyecciones de E sobre sí mismo. Indicamos por αx , por ejemplo, el transformado de $x \in E$ por α .

Definimos una nueva ley de composición $*$ poniendo, para x, y , cualesquiera, $x * y = \gamma(\alpha x \bullet \beta y)$.

1.º Demostrar que si la ley $\bullet$ posee una de las tres propiedades siguientes:

- a) condición de existencia de cocientes a la izquierda;
- b) condición de existencia y unicidad de cocientes a la izquierda;
- c) regla de simplificación a la derecha;

también la ley $*$ posee esa misma propiedad.

2.º Demostrar que, por el contrario, la existencia de un elemento neutro o lícito a un lado, la asociatividad, la conmutatividad, son propiedades que no se transportan de la operación $\bullet$ a la $*$.

10

Con las mismas notaciones del ejercicio precedente, sea dada la biyección γ .

1.º ¿Se pueden elegir α y β de modo que exista para la ley $*$ un elemento neutro a la izquierda? ¿y un elemento neutro (bilátero)?

2.º ¿Se pueden elegir α y β de modo que exista para la ley $*$ un elemento lícito a la derecha? ¿y un elemento lícito (bilátero)?

11

Conservamos las notaciones del ejercicio I, 9. Suponemos ahora que la ley $*$ es asociativa y que existe para la ley $\bullet$ un elemento e neutro (bilátero). Convenimos en indicar por yuxtaposición la composición de las aplicaciones.

Demostrar que $\beta\gamma\alpha = \alpha\gamma\beta$, y que para elementos cualesquiera x, y , de E , se tiene

$$\begin{aligned}\beta\gamma(x \bullet y) &= \beta\gamma x \bullet y, \\ \alpha\gamma(x \bullet y) &= x \bullet \alpha\gamma y.\end{aligned}$$

Deducir de ello que $\varphi = \beta\gamma\alpha$ es un isomorfismo del semigrupo $(E, *)$ sobre $(E, \bullet)$.

12

Sean a, b dos enteros relativos no nulos. Definimos en el conjunto $\mathbb{Z}$ de los enteros relativos una ley de composición $\top$, poniendo $x \top y = ax + by$.

1.° Demostrar que para todo entero n estrictamente positivo, la relación con congruencia módulo n es compatible con $\top$. Se puede, pues, definir la ley asociada $\overline{\top}$ en el conjunto cociente.

2.° ¿Cómo deben elegirse a , b , n para que la ley $\overline{\top}$ sea asociativa? ¿para que sea conmutativa? ¿para que exista un elemento neutro a la izquierda? ¿a la derecha? ¿bilátero?

13

Sea A un anillo, no necesariamente conmutativo.

1.° Se define en A una nueva ley de composición $*$ poniendo

$$a * b = a + b + ab.$$

a) Verificar que esta ley es asociativa y tiene un elemento neutro. ¿En qué casos existe un elemento lícito?

b) Demostrar que en el caso particular en que el anillo A posee un elemento unidad e , el semigrupo así obtenido es isomorfo al semigrupo multiplicativo del anillo.

2.° Se define en A una nueva ley de composición $\top$ poniendo

$$a \top b = ab - ba.$$

Verificar que esta ley no es generalmente asociativa, que no hay elemento neutro, que la ley $\top$ es distributiva respecto a la adición y que, para a , b , c cualesquiera

$$(1) \quad (a \top b) \top c + (b \top c) \top a + (c \top a) \top b = 0.$$

3.° Definimos en A una nueva ley de composición $\perp$ poniendo

$$a \perp b = ab + ba.$$

Verificar que esta ley es conmutativa, en general no es asociativa, es distributiva respecto a la adición, generalmente no existe elemento neutro y, para a y b cualesquiera,

$$(2) \quad [(a \perp a) \perp b] \perp a = (a \perp a) \perp (b \perp a).$$

Soluciones

1

Sea x un elemento cualquiera de D . Existen en D elementos y, b tales que $x = aya$, $a = aba$. Pongamos $e = ab$, $f = ba$. Se tiene entonces

$$\begin{aligned}ex &= (ab)(aya) = (aba)ya = aya = x, \\xf &= (aya)(ba) = ay(aba) = aya = x.\end{aligned}$$

Resulta de esto, que e es elemento unidad a la izquierda, f es elemento unidad a la derecha, y por tanto $e = f$ es elemento unidad bilátera.

2

Sea c el inverso (único) de ab : $abc = cab = e$. El elemento bc es, pues, inverso de a a la derecha. Para demostrar que también es inverso de a a la izquierda, basta establecer que $bca = e$, y para esto, que bca es idempotente y diferente de z . Ahora bien,

$$(bca)^2 = (bca)(bca) = b(cab)ca = beca = bca.$$

$bca = z$ implicaría $a = (abc)a = a(bca) = az = z$, lo que es imposible porque $abc = e$.

Se tiene, pues, $abc = cab = bca = e$, y los dos elementos a, b son inversibles.

Observación. Un enunciado equivalente es: En un semigrupo con un elemento unidad e y un elemento lícito z como únicos idempotentes, el conjunto de los elementos no inversibles es una parte lícita.

3

Consideremos la relación binaria $\mathcal{R}$ definida por:

$$x\mathcal{R}y \text{ si y sólo si } x = y \text{ ó } x = ay(a \in D).$$

Se comprueba inmediatamente que se trata de una relación de orden. Como el semigrupo D no tiene más que un número finito de elementos, ad-

mite al menos un elemento minimal z . Por la definición de $\mathcal{R}$ tenemos, para todo $x \in D$, $xz \mathcal{R} z$, es decir, puesto que z es minimal, $xz = z$. Por tanto, z es elemento lícito a la izquierda.

Observaciones: 1.° Si D no es conmutativo, este elemento lícito a la izquierda no es necesariamente único (ejercicio 1 de I, 3).

2.° Por el contrario, si D es conmutativo, es z elemento lícito único, por serlo a la derecha y a la izquierda.

4

Convengamos, para aligerar la escritura, en indicar con $\eta\xi$ la aplicación compuesta $\eta \circ \xi$.

1.° Sean $\alpha_a \in J$, $\xi \in H(E)$, $x \in E$.

$$(\alpha_a \xi)(x) = \alpha_a[\xi(x)] = a = \alpha_a(x), \text{ de donde } \alpha_a \xi = \alpha_a.$$

$$(\xi \alpha_a)(x) = \xi(a) = \alpha_b(x), \text{ poniendo } b = \xi(a), \text{ de donde } \xi \alpha_a = \alpha_b.$$

Por tanto todo elemento de J es lícito a la derecha, y J es parte lícita a la izquierda.

Si I es una parte lícita a la izquierda cualquiera, se tiene

$$J = JI \subseteq H(E)I \subseteq I,$$

es decir, $J \subseteq I$, y J es elemento mínimo del conjunto de partes lícitas a la izquierda.

En fin, si α es un elemento lícito a la derecha de $H(E)$, la igualdad $\alpha = \alpha\alpha_a$ implica $\alpha = \alpha_b$, donde $b = \alpha(a)$, luego $\alpha \in J$. Por tanto, J es el conjunto de elementos lícitos a la derecha de $H(E)$.

2.° Por hipótesis, para todo $x \in E$ se tiene $\xi\alpha_x = \eta\alpha_x$, o sea

$$(\forall t \in E) \quad (\xi\alpha_x)(t) = (\eta\alpha_x)(t),$$

o también $\xi(x) = \eta(x)$, es decir $\xi = \eta$.

3.° Sea $\Phi \in H(J)$. Pongamos $\Phi(\alpha_x) = \alpha_y$. Una condición necesaria y suficiente para que $\varphi\alpha_x = \alpha_y$ ($\varphi \in H(E)$), es que

$$(\forall t \in E) \quad (\varphi\alpha_x)(t) = \alpha_y(t),$$

es decir, $\varphi(x) = y$. El dar $\Phi \in H(J)$ determina, pues, $\varphi \in H(E)$ tal que

$$(\forall \alpha \in J) \quad \Phi(\alpha) = \varphi\alpha.$$

Recíprocamente, puesto que J es una parte lícita a la izquierda, el dar φ determina Φ . En fin, si Φ_1 y Φ_2 son dos aplicaciones de J en J , y si

$$\varphi_1 = F(\Phi_1), \varphi_2 = F(\Phi_2),$$

$$(\Phi_1 \Phi_2)(a) = \Phi_1[\Phi_2(a)] = \varphi_1(\varphi_2 a) = (\varphi_1 \varphi_2)a, \text{ para todo } a \in J,$$

lo que implica $F(\Phi_1 \Phi_2) = \varphi_1 \varphi_2 = F(\Phi_1)F(\Phi_2)$ y F es un isomorfismo de $H(J)$ sobre $H(E)$.

4.º Si A es una biyección de J , $\lambda = F(A)$ es, pues, una biyección de E , y se puede definir $\mathcal{A}_\lambda: \xi \rightarrow \lambda \xi \lambda^{-1}$. Es claro que $\mathcal{A}_\lambda$ es un automorfismo de $H(E)$.

Sea $a \in J$; entonces $\mathcal{A}_\lambda(a) = \lambda a \lambda^{-1} = \lambda a = A(a)$, es decir, que A es la restricción de $\mathcal{A}_\lambda$ a J .

5.º Sea $\mathcal{A}$ un automorfismo cualquiera de $H(E)$. La imagen por $\mathcal{A}$ de un elemento lícito a la derecha de $H(E)$ es asimismo un elemento lícito a la derecha de $H(E)$, luego $\mathcal{A}(J) \subseteq J$. Del mismo modo utilizando $\mathcal{A}^{-1}$ se obtiene $\mathcal{A}^{-1}(J) \subseteq J$ de donde $J \subseteq \mathcal{A}(J)$. Se deduce que la restricción A de $\mathcal{A}$ a J existe, y que es una biyección de J . Se pueden entonces definir $\lambda = F(A)$ y el automorfismo $\mathcal{A}_\lambda$. Es claro que $\mathcal{A}^{-1}\mathcal{A}_\lambda$ es un automorfismo de $H(E)$ que deja invariante cada elemento de J . Mostremos que tal automorfismo $\mathcal{B}$ es necesariamente el automorfismo idéntico de $H(E)$, lo que demostrará que $\mathcal{A} = \mathcal{A}_\lambda$.

Si se tiene, para todo $a \in J$, $\mathcal{B}(a) = a$, resulta, para todo $\xi \in H(E)$,

$$\xi a = \mathcal{B}(\xi) \mathcal{B}(a) = \mathcal{B}(\xi)a, \text{ de donde } \mathcal{B}(\xi) = \xi \text{ (2º)}.$$

5

1.º Si $\xi_2 = \eta \circ \xi_1$, es claro que $\xi_1(a) = \xi_1(b)$ implica $\xi_2(a) = \xi_2(b)$; se tiene, pues, $\mathcal{N}_{\xi_1} \subseteq \mathcal{N}_{\xi_2}$.

Recíprocamente, supongamos $\mathcal{N}_{\xi_1} \subseteq \mathcal{N}_{\xi_2}$. Para todo $x \in S_{\xi_1}$ existe al menos un $y \in E$ tal que $x = \xi_1(y)$, y los y que tienen esta propiedad constituyen una clase módulo $\mathcal{N}_{\xi_1}$, contenida en una clase módulo $\mathcal{N}_{\xi_2}$. Luego, si se pone

$$\eta(x) = \xi_2(y),$$

el elemento $\eta(x)$ es independiente de la elección del representante y . Se puede completar la definición de η poniendo, por ejemplo, $\eta(x) = x$ para $x \notin S_{\xi_1}$. Efectivamente η es una aplicación de E en E , y, para todo $z \in E$ se tiene $(\eta \circ \xi_1)(z) = \xi_2(z)$, es decir $\xi_2 = \eta \circ \xi_1$.

2.º Si $\xi_2 = \xi_1 \circ \eta$, es claro que todo elemento de S_{ξ_2} es imagen por ξ_1 de al menos un elemento de E , de donde $S_{\xi_2} \subseteq S_{\xi_1}$.

Recíprocamente, supongamos $S_{\xi_2} \subseteq S_{\xi_1}$. Para cada $x \in E$, $y = \xi_2(x)$ es un elemento de S_{ξ_1} , y existe al menos un $x' \in E$ tal que $y = \xi_1(x')$. Si se elije