PROBLEMAS DE ÁLGEBRA MODERNA

A. Bigard / M. Crestey / J. Grappy

editorial reverté, s.a.

PROBLEMAS DE ÁLGEBRA MODERNA

A. BIGARD M. CRESTEY J. GRAPPY
Profesores en la Facultad de Ciencias de París

PROBLEMAS DE ÁLGEBRA MODERNA

EDITORIAL REVERTÉ, S. A.
BARCELONA - BUENOS AIRES - MÉXICO
MCMLXX

Título de la obra original:
PROBLÈMES D'ALGÈBRE GÉNÉRALE
Editada por Dunod, París

Versión española del
Dr. RODRÍGUEZ VIDAL
Catedrático de la Facultad de Ciencias de Zaragoza

Depósito Legal: B. 15 980 - 1970. Printed in Spain
TALLERES GRÁFICOS IBERO-AMERICANOS, S. A. : PROVENZA, 86, BARCELONA - 15

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: **N** es el semianillo de los naturales; $\mathbf{N}* = \mathbf{N} - \{0\}$; **Z** es el anillo de los enteros relativos; **Q, R, 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 $A \to B$, 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 $f : A \to B$ 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: $(h)A \to B$). 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 $a, b, c, \ldots$ 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 $\varnothing$). 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 $a, b, c, \ldots$ elementos de E, y con $A, B, C, \ldots$ subconjuntos (o **partes**) de E. Ponemos:

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

A es **parte estable** de E, para la operación considerada, si $a \in A$ y $b \in A \Rightarrow$ $\Rightarrow ab \in A$. [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 $\varnothing$.)

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

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

[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, $\leqslant$ 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 $\overset{\leqslant}{x}$ (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 $\overset{\geqslant}{x}$.

Un subconjunto $A \subset E$, que tenga la propiedad de que $x \in A \Rightarrow \overset{\leqslant}{x} \subset A$, 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, $a_1 \subset a_2 \subset \ldots$ 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 $\mathscr{P}(E)$ el conjunto de las partes de E. Un subconjunto de $\mathscr{P}(E)$ suele llamarse **familia.**

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

Axioma de elección. *Para todo E se puede definir una aplicación f de $\mathscr{P}(E)$ en E, con la que a cada $A \in \mathscr{P}(E)$ 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 $\mathscr{F}$ a todo aquel $F \in \mathscr{F}$ que no es intersección de dos $F_1, F_2 \in \mathscr{F}$ que le contienen estrictamente.

Un **sistema de clausura** (o *familia de Moore*) es una familia $\mathscr{F}$ 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. $E \in \mathscr{F}$; 2. si $\mathscr{F}' \subset \mathscr{F}$, también $\bigcap_{F \in \mathscr{F}'} F \in \mathscr{F}$.

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

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

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

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

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

Si E es un conjunto ordenado, el conjunto $\mathscr{U}$ de las cadenas $\mathscr{C}$ de E, ordenadas por la inclusión de conjuntos en $\mathscr{P}(E)$ 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:

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

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 *infsemerrirtículo* (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 infsemerretículo. 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. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ 2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

T **modular:** Cuando,

siempre que sea $a \subset c$, 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 $\mathscr{I} \subset T$ que es 1) hereditaria, 2) estable para $\vee$:

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

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

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 $a, b, c, \ldots$ 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 **isótona:** $a \subseteq b \Rightarrow$ $\Rightarrow ax \subseteq bx$ y $xa \subseteq xb$, $\forall x \in G$. 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 $x \to axa^{-1}$, $\forall x \in G$, 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 $\mathscr{R}$ regular a la derecha con **clases a la derecha** xH y una equivalencia $\mathscr{R}'$ 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),

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

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 $a, b, c, \ldots$ 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 $\Gamma = (e) = (0, e, \ldots, (p-1)e\}$, que en tal caso constituye el llamado **subcuerpo mínimo** de A.

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

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:

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

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

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

17. Sean A un anillo conmutativo, $\mathfrak{a}, \mathfrak{b}, \ldots$ ideales de A, y $a, b, \ldots$ elementos genéricos de A.

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

Diremos que $\mathfrak{s}$ es ideal **semiprimo** de A cuando todo elemento de A con alguna potencia en $\mathfrak{s}$ es también elemento de $\mathfrak{s}$.

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

Diremos que un ideal es $\mathfrak{p}$-**primario,** si es primario y tiene el ideal primo $\mathfrak{p}$ como radical.

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

Ideal $\mathfrak{q}$ **primario fuerte** en el anillo A, es el que siendo $\mathfrak{a}, \mathfrak{b}$ ideales de A, cuando $\mathfrak{ab} \subseteq \mathfrak{q}$ y $\mathfrak{a} \nsubseteq \mathfrak{q}$, alguna potencia de $\mathfrak{b}$ está contenida en $\mathfrak{q}$.

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 $\mathfrak{q}_1 \ldots \mathfrak{q}_r$ a toda intersección parcial de ideales primarios $\mathfrak{q}_i$ 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

CAPITULO I

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.° Sea J el conjunto de las $a_a \in H(E)$ definidas por

$$(\forall x \in E) \quad a_a(x) = a \in E.$$

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

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

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 $\mathscr{A}_\lambda$ de $H(E)$ en sí mismo definida por

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

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

5.° Demostrar que todo automorfismo de $H(E)$ es de la forma $\mathscr{A}_\lambda$ 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 $\mathscr{R}_\xi$ 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 $\mathscr{R}_{\xi_1} \subseteq \mathscr{R}_{\xi_2}$.

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 $a \to \gamma_a$ 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 $(x, y) \to x \bullet y$ 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.° 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.° 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.° ¿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.° ¿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

$$\beta\gamma(x \bullet y) = \beta\gamma x \bullet y,$$
$$\alpha\gamma(x \bullet y) = x \bullet \alpha\gamma y.$$

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 $\mathbf{Z}$ 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

$$(a \top b) \top c + (b \top c) \top a + (c \top a) \top b = 0. \tag{1}$$

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,

$$[(a \perp a) \perp b] \perp a = (a \perp a) \perp (b \perp a). \tag{2}$$

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

$$ex = (ab)(aya) = (aba)ya = aya = x,$$
$$xf = (aya)(ba) = ay(aba) = aya = x.$$

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 $a_a \in J$, $\xi \in H(E)$, $x \in E$.

$$(a_a\xi)(x) = a_a[\xi(x)] = a = a_a(x), \text{ de donde } a_a\xi = a_a.$$
$$(\xi a_a)(x) = \xi(a) = a_b(x), \text{ poniendo } b = \xi(a), \text{ de donde } \xi a_a = a_b.$$

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 $\alpha = \alpha a_a$ implica $\alpha = a_b$, 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 $\xi a_x = \eta a_x$, o sea

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

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

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

$$(\forall t \in E) \quad (\varphi a_x)(t) = a_y(t),$$

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

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

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

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

5.° 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 Λ de $\mathcal{A}$ a J existe, y que es una biyección de J. Se pueden entonces definir $\lambda = F(\Lambda)$ 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 $\alpha \in J$, $\mathcal{B}(\alpha) = \alpha$, resulta, para todo $\xi \in H(E)$,

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

5

1.° 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, $\mathcal{H}_{\xi_1} \subseteq \mathcal{H}_{\xi_2}$.

Recíprocamente, supongamos $\mathcal{H}_{\xi_1} \subseteq \mathcal{H}_{\xi_2}$. 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 $\mathcal{H}_{\xi_1}$, contenida en una clase módulo $\mathcal{H}_{\xi_2}$. 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.° 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

uno de estos x' para cada $x \in E$, y si se pone $x' = \eta(x)$, se define una aplicación η de E en E. Se tiene entonces $\xi_2(x) = y = \xi_1(x') = (\xi_1 \circ \eta)(x)$, es decir, $\xi_2 = \xi_1 \circ \eta$.

6

1.° Para todo $x \in D$, la igualdad $a(bx) = (ab)x$ demuestra que $\gamma_a \circ \gamma_b = \gamma_{ab}$. La aplicación compuesta de dos traslaciones a la izquierda es, pues, una traslación a la izquierda y, además, la aplicación $a \to \gamma_a$ es un homomorfismo de semigrupos.

2.° Si D admite un elemento unidad e, $a \neq b$ implica $\gamma_a(e) = a \neq b = \gamma_b(e)$, de donde $\gamma_a \neq \gamma_b$. El homomorfismo $a \to \gamma_a$ es, pues, inyectivo, y la imagen de D en este homomorfismo, es decir, el subsemigrupo de $S(D)$ constituído por las traslaciones a la izquierda, es isomorfo a D.

Observaciones: 1. Se obtiene la misma conclusión suponiendo solamente la existencia de al menos un elemento simplificable a la derecha.

2. En el caso particular de que D sea un grupo, se reencuentra un resultado conocido (II, 6).

3.° Consideremos el conjunto $D \cup \{e\} = D_1$ donde e es un símbolo cualquiera. Se le puede dar a D_1 una estructura de semigrupo si ponemos $e^2 = e$,

$$ex = xe = x \quad \text{para todo} \quad x \in D,$$

y tomando como producto en D_1 de dos elementos de D su producto en D. La verificación de la asociatividad es inmediata.

Entonces D_1, semigrupo con elemento unidad e, es isomorfo a un subsemigrupo D_1^* del semigrupo simétrico $S(D_1)$. Luego D, subsemigrupo de D_1, es isomorfo a un subsemigrupo D^* de $S(D_1)$.

7

1.° Utilizando el axioma 1 y $ab = aa = a$ si $a = b$, se obtiene

$$a(cd) = (aa)(cd) = (ac)(ad),$$

es decir, el axioma 3. De un modo análogo se verifica el axioma 4.

2.° Si se supone $aa = a$, $bb = b$, es ab idempotente en virtud de

$$ab = (aa)(bb) = (ab)(ab) \text{ (axioma 1).}$$

Si además $cc = c$, se tiene $a(bc) = (aa)(bc) = (ab)(ac)$.

Se verifica de igual modo que $(ab)c = (ac)(bc)$.

3.° Supongamos verificados los axiomas 3 y 4. Sean a un idempotente y b un elemento cualquiera de E. Entonces, $ab = (aa)b = (ab)(ab)$, y ab es idempotente. Análogamente se verifica que es ba idempotente.

4.° Supongamos verificado el axioma 1. Sea e el elemento unidad de E. Entonces,

$$ab = (ea)(be) = (eb)(ae) = ba \quad \text{y} \quad a(bc) = (ae)(bc) = (ab)(ec) = (ab)c.$$

5.° Supongamos verificado el axioma 3. Sea f un elemento unidad a la derecha de E. Entonces, para todo $a \in E$, se tiene

$$a = af = a(ff) = (af)(af) = aa.$$

8

1.° La ley de composición considerada es conmutativa. La existencia de cocientes resulta del axioma 1: en efecto, $ax = b$ equivale a $x = ba$.

Supongamos $ab = ac = d$. El axioma 1 implica $b = ad = c$.

2.° Supongamos verificados los axiomas 1, 2, 3. Sea $x = [(ab)c]d$.

El axioma 1 implica sucesivamente $(ab)c = xd$, luego $c = (ab)(xd)$.
Mediante el axioma 3 se obtiene $c = (xb)(ad)$.
De nuevo el axioma 1 implica $(ad)c = xb$, luego $x = [(ad)c]b$.

3.° Supongamos verificados los axiomas 1, 2, 3, 4.

a) Basta establecer que $aa = bb$ implica $(ac)b = a(cb)$ para un elemento c de E.

Ahora bien, de $aa = bb$ resulta $(aa)b = b$ (axioma 1). Pero $b = c(cb)$, de donde $(aa)b = c(cb)$, luego $[(aa)b]c = cb$.

El resultado del punto 2.° demuestra entonces que $cb = bc = [(ac)b]a$ y, por el axioma 1 $(ac)b = a(bc)$.

b) Supongamos $(aa)(bb) = cc$. Poniendo $x = ab$, el axioma 3 da $cc = (ab)(ab) = xx$, de donde $x = c$, es decir, $ab = c$.

c) Sea a un elemento fijo de E, que suponemos constituido por N elementos. La aplicación de E en E definida por $x \to ax$ es inyectiva, por la regla de simplificación, y suprayectiva, en virtud de la existencia de cocientes. Se trata pues de una biyección, que por axioma 1 coincide con su propia recíproca. Esta aplicación admite un único punto fijo f, pues $ax = x$ equivale a $xx = a$, y la aplicación $x \to xx$ es también biyectiva. Resulta, pues, que N es impar, ya que los elementos distintos de f pueden asociarse por pares cuyo producto es a.

Se verifica fácilmente que la tabla de multiplicación

$\bullet$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

define una ley de composición sobre $\{a, b, c\}$ con la que se cumplen los axiomas 1, 2, 3 y 4.

9

1.° Las propiedades indicadas en el enunciado resultan de las equivalencias

$$x * a = b \Leftrightarrow \alpha x \bullet \beta a = \gamma^{-1} b;$$

$$x * a = y * a \Leftrightarrow \alpha x \bullet \beta a = \alpha y \bullet \beta a \Leftrightarrow \alpha x = \alpha y \Leftrightarrow x = y$$

(suponiendo válida para $\bullet$ la regla de simplificación a la derecha).

2.° Consideremos el semigrupo definido por la tabla de multiplicación

$\bullet$	z	e	a
z	z	z	z
e	z	e	a
a	z	a	e

Se trata efectivamente de un semigrupo, puesto que $\{e, a\}$ es un grupo cíclico de orden 2 y el elemento z es lícito. El elemento unidad es e.

Si definimos α y β por

$$\alpha = \begin{pmatrix} z & e & a \\ e & a & z \end{pmatrix}, \quad \beta = \begin{pmatrix} z & e & a \\ a & z & e \end{pmatrix},$$

y γ es la aplicación idéntica, la tabla de multiplicar para $*$ es

$*$	z	e	a
z	a	z	e
e	e	z	a
a	z	z	z

La ley $*$ no es ni conmutativa ni asociativa, pues

$$(z * z) * z = z \neq z * (z * z) = e.$$

No existen para $*$ elementos lícitos a un lado ni elemento neutro a un lado.

10

Supongamos que e sea el elemento neutro a la izquierda para la ley de composición $*$. Entonces, para todo $x \in E$, $e * x = x$, es decir $\alpha e \bullet \beta x = \gamma^{-1} x$.

Pongamos $b = \alpha e$ y sea λ_b la traslación a la izquierda definida por b:

$$(\forall y \in E) \quad \lambda_b(y) = b \bullet y.$$

Entonces, $$\lambda_b(y) = \gamma^{-1} \beta^{-1} y = (\beta\gamma)^{-1} y.$$

Es, pues, necesario que la traslación a la izquierda λ_b sea una biyección.

Recíprocamente, si una traslación a la izquierda λ_b es una biyección, tomaremos $\beta = (\gamma\lambda_b)^{-1}$, α cualquiera, $e = \alpha^{-1} b$. Se tendrá entonces

$$(\forall x \in E) \quad e * x = \gamma(b \bullet \beta x) = \gamma\lambda_b \lambda_b^{-1} \gamma^{-1} x = x.$$

Lo mismo se demuestra que existe para $*$ un elemento neutro a la derecha, e, si y sólo si, existe un $c \in E$ tal que la traslación a la derecha $\rho_c : y \to y \bullet c$ sea una biyección.

En fin, para que exista un elemento neutro (bilátero), es necesario que existan a la vez una traslación a la izquierda λ_b y una traslación a la derecha ρ_c que sean biyectivas. Recíprocamente, si se cumple tal condición, se tomará

$$\alpha = (\gamma\rho_c)^{-1}, \ \beta = (\gamma\lambda_b)^{-1};$$

con esto se constata que $\beta^{-1} c = \alpha^{-1} b$, y este elemento es efectivamente elemento neutro para $*$.

2.° Supongamos que el elemento z sea lícito a la derecha para $*$. Entonces, para todo $x \in E$, $z * x = z$, de donde $\alpha z \bullet \beta x = \gamma^{-1} z$. Poniendo $\alpha z = b$, vemos que la traslación a la izquierda $\lambda_b : y \to b \bullet y$ da una imagen de E reducida al elemento $p = \gamma^{-1} z$.

Recíprocamente, si existe un $b \in E$, tal que $\lambda_b (E) = \{p\}$, se tiene, tomando α tal que $\alpha\gamma p = b$ y poniendo $z = \alpha^{-1} b$,

$$(\forall x \in E) \quad z * x = \gamma(\alpha z \bullet \beta x) = \gamma(b \bullet \beta x) = \gamma p = \alpha^{-1} b = z.$$

Se demuestra del mismo modo que existe para $*$ un elemento lícito a la izquierda z, si y sólo si, existe un $c \in E$ tal que la traslación a la derecha $\rho_c : y \to y \bullet c$ de una imagen de E reducida a un elemento.

Finalmente, para que exista un elemento lícito (bilátero) es necesario que existan a la vez una traslación a la izquierda λ_b y una traslación a la derecha ρ_c, tales que

$$\lambda_b(E) = \{p\}, \quad \rho_c(E) = \{q\}.$$

Recíprocamente, si esa condición se cumple, tomemos α y β tales que

$$\alpha\gamma p = b, \quad \beta\gamma q = c;$$

se comprueba entonces que $\alpha^{-1} b = \beta^{-1} c$, y que este elemento es efectivamente lícito para $*$.

11

Sean x, y, z, tres elementos cualesquiera de E. La asociatividad de $*$ implica

$$\alpha\gamma(\alpha x \bullet \beta y) \bullet \beta z = \alpha x \bullet \beta\gamma(\alpha y \bullet \beta z). \tag{1}$$

Basta tomar $x = \alpha^{-1} e$, $z = \beta^{-1} e$, para obtener, para todo $y \in E$, $\alpha\gamma(e \bullet \beta y) \bullet e = e \bullet \beta\gamma(\alpha y \bullet e)$, es decir $\alpha\gamma\beta y = \beta\gamma\alpha y$.

Reemplazando en la anterior relación (1) x, y, z, por $\alpha^{-1} e$, $\alpha^{-1} x$, $\beta^{-1} y$, respectivamente, se obtiene

$$\alpha\gamma(e \bullet \beta\alpha^{-1} x) \bullet y = e \bullet \beta\gamma(x \bullet y),$$

es decir,

$$\alpha\gamma\beta\alpha^{-1} x \bullet y = \beta\gamma x \bullet y = \beta\gamma(x \bullet y).$$

De modo análogo se demuestra que $x \bullet \alpha\gamma y = \alpha\gamma(x \bullet y)$.

La aplicación φ compuesta de tres biyecciones es una biyección. Es un isomorfismo, pues para todo par de elementos x, y de E,

$$\varphi(x*y) = \beta\gamma\alpha\gamma(\alpha x \bullet \beta y) = \beta\gamma[\alpha\gamma(\alpha x \bullet \beta y)] = \beta\gamma(\alpha x \bullet \alpha\gamma\beta y) = \\ = \beta\gamma\alpha x \bullet \alpha\gamma\beta y = \varphi x \bullet \varphi y.$$

12

1.° La verificación es inmediata, puesto que de $x \equiv x'\ (n)$ e $y \equiv y'\ (n)$ se deduce

$$ax + by \equiv ax' + by' \quad (n).$$

2.° Para que la ley $\overline{\top}$ sea asociativa, es necesario y suficiente que

$$(\forall x, y, z \in \mathbf{Z}) \quad a(ax + by) + bz \equiv ax + b(ay + bz) \quad (n),$$

es decir, que n divida a $a(a-1)x - b(b-1)z$. Haciendo $x = 1$, $z = 0$, después $x = 0$, $z = -1$, se ve que es necesario que n divida a $a(a-1)$ y $b(b-1)$. Es claro que esta condición es suficiente.

Para que la ley $\overline{\top}$ sea conmutativa, es necesario y suficiente que

$$(\forall x, y \in \mathbf{Z}) \quad ax + by \equiv bx + ay \quad (n),$$

es decir, que n divida a $(a-b)(x-y)$. Es claro que para esto es necesario y suficiente que n divida a $a-b$.

Para que exista un elemento neutro a la izquierda $\overline{e'}$, es necesario y suficiente que exista $e' \in \mathbf{Z}$ tal que

$$(\forall x \in \mathbf{Z}) \quad ae' + bx \equiv x \quad (n),$$

es decir, que n divida a $(b-1)x + ae'$. Dando a x dos valores consecutivos se ve que n debe ser divisor de $b-1$. Inversamente, si n divide a $b-1$, basta tomar e' tal que ae' sea múltiplo de n, para que la clase de e' módulo n sea elemento neutro a la izquierda para $\overline{\top}$.

Se ve del mismo modo que $\overline{\top}$ tiene un elemento neutro a la derecha si y sólo si n divide a $a-1$, luego, tendrá un elemento neutro bilátero si y sólo si n divide a la vez a $a-1$ y a $b-1$. [Se puede observar que en este último caso, $ax + by \equiv x + y\ (n)$, y la ley $\overline{\top}$ no es otra que la clásica ley de grupo aditivo definida en el conjunto de los enteros módulo n.]

13

1.° La verificación de la asociatividad de la ley $*$ es inmediata. Es claro que el elemento nulo 0 del anillo es elemento neutro para $*$, y que un elemento z es lícito a un lado para $*$ si y sólo si, su opuesto es elemento unidad al otro lado para la multiplicación habitual.

Si el anillo tiene un elemento unidad e, la aplicación $x \to e + x$ es visiblemente biyectiva. Además, el transformado de $x * y$ es

$$e + x * y = e + x + y + xy = (e + x)(e + y).$$

Se trata, pues, efectivamente, de un homomorfismo de semigrupos.

2.° Para los elementos a, b de A se tiene

$$a \top a = 0, \quad b \top a = -(a \top b).$$

La verificación de la distributividad respecto a la adición y de la propiedad (1) son inmediatas. No puede existir elemento neutro por ser $a \top a = 0$.

Tomando como anillo A el anillo de las matrices 2×2 de elementos enteros y, por ejemplo,

$$a = \begin{Vmatrix} 1 & 0 \\ 1 & 0 \end{Vmatrix}, \qquad b = \begin{Vmatrix} 1 & 1 \\ 0 & 0 \end{Vmatrix}, \qquad c = \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix},$$

se constata que $a \top b \neq 0$, y $(b \top b) \top c \neq a \top (b \top c)$. La ley de composición $\top$ no es, pues, asociativa.

3.° La conmutatividad de la ley $\perp$ resulta de su definición. La distributividad respecto a la suma y la propiedad (2) se verifican fácilmente.

Volviendo a los elementos a, b, c, del anillo de matrices considerado en el apartado 2.°, se comprueba que $(a \perp b) \perp c \neq a \perp (b \perp c)$, y también se ve que, poniendo

$$e = \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} \quad (x, y, z, t \in \mathbf{Z}),$$

la igualdad $a \perp e = a$ es imposible. La ley $\perp$ no es, por tanto, asociativa y no hay en ella elemento neutro.

CAPÍTULO II

Estructuras ordenadas

Enunciados

Los cuatro ejercicios que siguen consisten en demostrar que la proposición dada en cada uno es equivalente al axioma de Zorn.

1

Si f es una aplicación de un conjunto X en el conjunto de las partes de Y, existe una aplicación g de X en Y tal que $g(x) \in f(x)$ si $f(x) \neq \varnothing$.

2

Si $(E_i)_{i \in I}$ es una familia de conjuntos no vacíos, el producto cartesiano $\prod_{i \in I} E_i$ no es vacío.

3

Si $\mathcal{F}$ es una familia de partes de un conjunto E tal que $X \in \mathcal{F}$ si y sólo si toda parte finita de X pertenece a $\mathcal{F}$, entonces $\mathcal{F}$ admite un elemento maximal.

4

Si E es un conjunto ordenado en el que toda parte bien ordenada está mayorada, E admite un elemento maximal.

5

Estudiar la demostración del hecho que el axioma de Zorn implique el axioma de Zermelo. Aportando algunos afinamientos a esta demostración, establecer — mediante el axioma de Zorn — que todo orden que satisfaga la condición minimal puede sumergirse en un buen orden más fino.

6

Sea E un espacio vectorial sobre un cuerpo K. Para todo subespacio L de E, designaremos por $\mathcal{V}(L)$ el retículo de subespacios de L. Sea $\mathcal{G}$ el conjunto de los pares (L, γ_L) donde γ_L es una aplicación de $\mathcal{V}(L)$ en sí mismo tal que

— $A \subseteq B \Rightarrow \gamma_L(B) \subseteq \gamma_L(A)$.

— Para todo $A \in \mathcal{V}(L)$, $L = A \oplus \gamma_L(A)$.

Se ordena $\mathcal{G}$ poniendo $(L, \gamma_L) \leqslant (N, \gamma_N)$ si $L \subseteq N$ y $\gamma_L(X \cap L) \subseteq \gamma_N(X)$ para todo $X \in \mathcal{V}(N)$.

1.° Demostrar que $\mathcal{G}$ es no vacío e inductivo.

2.° Sea (M, γ_M) un elemento maximal de $\mathcal{G}$. Se supone $a \notin M$. Si

$$X \in \mathcal{V}(M \oplus Ka),$$

se pone $\tau(X) = \gamma_M(X) \oplus Ka$ si $X \subseteq M$, y $\tau(X) = \gamma_M(X \cap M)$ si $X \nsubseteq M$. Mostrar que $(M \oplus Ka, \tau) \in \mathcal{G}$ y que $(M, \gamma_M) < (M \oplus Ka, \tau)$. Concluir que existe una aplicación que a todo subespacio de E asocia un suplementario.

7

Se considera un conjunto ordenado E fuertemente inductivo (es decir, que toda parte totalmente ordenada admite cota superior). Se supone además que en E hay una función de elección φ. Se define sobre E una aplicación f del modo siguiente:

$$f(x) = \begin{cases} \varphi(\overset{>}{x}) & \text{si } x \text{ no es maximal } (*) \\ x, & \text{si } x \text{ es maximal} \end{cases}$$

Dado un $a \in E$ se considera la familia Φ de las partes T de E tales que: $a \in T$; $f(T) \subseteq T$; si $X \subseteq T$ es una cadena, $\sup X \in T$. Nótese que la intersección A de los elementos de Φ pertenece a Φ.

Se pone:

$$B = \{ y \in A \mid x \in A \text{ y } x < y \Rightarrow f(x) \leqslant y \}$$
$$C = \{ z \in A \mid \forall y \in B,\ z \leqslant y \text{ ó } f(y) \leqslant z \}.$$

(*) El símbolo $\overset{>}{x}$ indica el conjunto de elementos superiores a x en un conjunto ordenado E.

1.° Mostrar que $C \in \Phi$.

2.° Mostrar que $B \in \Phi$.

3.° Mostrar que A es bien ordenado. Deducir de aquí, sin apelar al axioma de Zorn, que E admite un elemento maximal.

8*

En todo el problema, llamaremos álgebra un conjunto A con una familia $(o_i)_{i \in I}$ de leyes de composición internas o externas. Se llamará subálgebra a toda parte de A que sea estable para todas las leyes o_i.

1.° Utilizando el axioma de Zorn, demostrar la proposición P1:

(P1). Si A es un álgebra, B una subálgebra, m un elemento de A que no es de B, existe una subálgebra C tal que $B \subseteq C$, $m \notin C$, y es maximal para estas dos propiedades.

2.° Sea $(B_\alpha)_{\alpha \in S}$ la familia de las subálgebras de A. Diremos que B_λ es $\cap$-irreducible, o interirreducible, si

$$B_\lambda = \bigcap_{\alpha \in T} B_\alpha \Rightarrow \exists\, \alpha \in T \quad B_\lambda = B_\alpha.$$

Mostrar que (P1) implica (P2):

(P2). Si A es un álgebra, toda subálgebra es la intersección de las subálgebras interirreducibles que la contienen.

3.° Observar que $(B_\alpha)_{\alpha \in S}$ es una familia de Moore. Sea $R \to \overline{R}$ la clausura asociada. Se llama sistema generador una parte X tal que $\overline{X} = A$, y base un sistema generador minimal. Mostrar que (P1) implica la siguiente proposición:

(P3). Si el álgebra A admite una base finita, toda subálgebra propia está contenida en una subálgebra maximal.

4.° Se llama ideal de un retículo $\mathcal{C}$ a toda parte $\mathcal{I}$ tal que

— $a \in \mathcal{I}$ y $b \in \mathcal{I} \Rightarrow a \vee b \in \mathcal{I}$.

— $a \in \mathcal{I}$ y $x < a \Rightarrow x \in \mathcal{I}$.

Mostrar, utilizando (P3) que en un retículo que admite un elemento máximo, todo ideal propio está contenido en un ideal maximal.

Sea X un conjunto en el que se da un orden no total. Sea Γ el conjunto de sus cadenas. Mostrar que $\Gamma \cup \{X\}$, ordenado por inclusión, es un retículo con elemento máximo. Aplicando lo precedente, establecer que existe en X una cadena maximal. Concluir que si X es inductivo, admite un elemento maximal.

5.° Sean E un conjunto, $\mathcal{P}$ el conjunto de sus partes que tienen más de dos elementos. Consideramos $A = \{(F, x) \mid F \in \mathcal{P},\ x \in F\}$. Para todo $a \in A$ se define una ley interna o_a, como sigue:

$$b o_a c = \begin{cases} a \text{ si } b = (F, x),\ c = (F, y),\ x \neq y; \\ b \text{ en todos los otros casos.} \end{cases}$$

Mostrar que una subálgebra propia de A es una función. Señalando que (P2) implica la existencia en A de una subálgebra propia $\cap$-irreducible, mostrar que existe en E una función de elección.

Concluir que (P1), (P2) y (P3) son equivalentes al axioma de Zorn.

9

1.° Sean E y F dos conjuntos bien ordenados. Se supone que el conjunto $\mathcal{C}$ de las aplicaciones estrictamente crecientes de E en F no es vacío. Mostrar que $\mathcal{C}$ admite un elemento mínimo φ caracterizado por la propiedad

$$\varphi(\overset{<}{x}) = \overset{<}{\varphi(x)}.$$

2.° Sean E y F dos conjuntos bien ordenados. Se supone que no existe ninguna aplicación estrictamente creciente de E en F. Sea Γ el conjunto de las aplicaciones crecientes de E en F. A todo $h \in \Gamma$ se asocia el elemento t_h:

$$t_h = \inf \{x \mid h(x) = h(x')\}.$$

a) Mostrar que existe una aplicación estrictamente creciente mínima de $\overset{\leqslant}{t_h}$ en F. Se la designará por $\widetilde{h}$.

b) Definir una aplicación estrictamente creciente γ de $E' = \bigcup_{h \in \Gamma} \overset{\leqslant}{t_h}$ en F, que prolonga las $\widetilde{h}$.

c) Mostrar que γ es suprayectiva. (Suponiendo que existe $b \in F - \gamma(E')$, prolongar γ en una aplicación creciente de E en F.)

d) Probar que F es isomorfo a un intervalo de E. Concluir que dados dos conjuntos bien ordenados, uno es isomorfo a un intervalo del otro.

3.° Intentar demostrar este resultado por un camino más rápido pero que utiliza el axioma de Zorn.

Advertencia: En un conjunto bien ordenado denotamos:

$$\overset{<}{x} = \{z \mid z < x\}, \qquad x' = \inf \{z \mid x < z\}.$$

10*

1.° Recordemos que un conjunto X se dice infinito cuando existe una aplicación inyectiva (inyección) φ de X en X tal que $\varphi(X) \neq X$.

Demostrar que existen una parte N de X y $a \in N$ tales que:

N es estable para φ; $a \notin \varphi(N)$ y toda parte de N estable para φ y que contiene a a, es igual a N.

2.° Sean N' un conjunto, $a' \in N'$, φ' una inyección de N en N, tales que $a' \notin \varphi'(N')$ y toda parte de N' estable para φ' y conteniendo a a' es igual a N'. Mostrar que existe una biyección f de N sobre N' tal que $f\varphi = \varphi' f$.

3.° Si $x \in N$, se designa por $S(x)$ la menor parte de N estable para φ que contiene a x. Mostrar que, para todo $x \in N$, $x \notin \varphi(S(x))$. Deducir de ello que el par $(S(x), \varphi)$ es isomorfo a (N, φ).

4.° Mostrar que para todo $x \in N$, $S(x) = \{x\} \cup \varphi S(x)$.

Deducir que $\varphi S(x) = S(\varphi(x))$.

5.° Se considera la relación $x \leqslant y \Leftrightarrow y \in S(x)$.

Mostrar que es un orden y que para este orden φ es creciente.

6.° Mostrar que el antedicho es un buen orden para N. (Se hará ver primero que es un orden total.)

11

Sea T un retículo completo y sea a una aplicación creciente de T en sí mismo. Mostrar que existe un punto b tal que $a(b) = b$.

12

Sean E un conjunto ordenado, $x \to \bar{x}$ una aplicación de E en sí mismo. Recordemos que esta aplicación es una clausura de Moore si $x \leqslant \bar{x}$, $\bar{\bar{x}} = \bar{x}$ y si $x \leqslant y$ implica $\bar{x} \leqslant \bar{y}$. Demostrar que se pueden reemplazar estos tres axiomas por los dos siguientes: $x \leqslant \bar{x}$ y si $x \leqslant \bar{y}$, entonces $\bar{x} \leqslant \bar{y}$.

13

Mostrar que un conjunto ordenado puede ser infinito y no admitir más que una sola clausura de Moore (la identidad).

14

Sean u y v dos clausuras de Moore sobre un conjunto ordenado E. Pondremos $u \leqslant v$ si $u(x) \leqslant v(x)$ para todo $x \in E$. Demostrar que $u \leqslant v$, $uv = v$, $vu = v$ y $v(E) \subseteq u(E)$ son equivalentes.

15

Sean E y F dos conjuntos ordenados, π una aplicación de E en F y σ una aplicación de F en E, ambas decrecientes. Se supone, además, que

$$x \leqslant \sigma\pi(x)$$

para todo $x \in E$ y $y \leqslant \pi\sigma(y)$ para todo $y \in F$. Demostrar que $\sigma\pi$ y $\pi\sigma$ son dos clausuras de Moore, admitiendo respectivamente como imágenes $\sigma(F)$ y $\pi(E)$. Mostrar que la restricción de π a $\sigma(F)$ es una biyección de $\sigma(F)$ sobre $\pi(E)$, donde σ es la aplicación recíproca.

16

Sea φ un homomorfismo de un retículo T sobre un retículo T'. Si T cumple la condición maximal, mostrar que lo mismo sucede con T'.

17

Sea E un conjunto ordenado. Mostrar que toda cadena es finita si y sólo si E cumple simultáneamente la condición minimal y la condición maximal.

18*

Se considera un conjunto ordenado E en el cual toda cadena y toda parte trivialmente ordenada son finitas. Mostrar que el propio E es finito.

19

Para un conjunto ordenado E demostrar (utilizando si es necesario el ejercicio anterior), que las dos condiciones siguientes son equivalentes:

A) Cumple la condición minimal y toda parte trivialmente ordenada es finita.

B) Toda parte que cumple la condición maximal es finita.

20

Demostrar que $\mathbf{N}^k$ ordenado por $(a_i) \leqslant (b_i)$ si y sólo si $a_i \leqslant b_i$ para $i < k$, verifica la condición A del ejercicio precedente.

21

Sea T un $\vee$-semirretículo. Se llama ideal T a toda parte hereditaria estable para $\vee$. Sea $\mathcal{I}(T)$ el conjunto de los ideales de T.

1.° Demostrar que $\mathcal{I}(T)$ ordenado por inclusión es un retículo completo. Precisar explícitamente la cota superior. Mostrar que existe un isomorfismo natural de T en $\mathcal{I}(T)$.

Sea L un retículo completo. Se dice que $a \in L$ es compacto si $a \leqslant \bigvee_{j \in J} x_j$ implica $a \leqslant \bigvee_{j \in F} x_j$, donde F es una parte finita de J. Se dice que L es de generación compacta si todo elemento de L es cota superior (finita o infinita) de compactos.

2.° Demostrar que la imagen canónica de T en $\mathcal{I}(T)$ es el conjunto de los compactos de $\mathcal{I}(T)$. Deducir que $\mathcal{I}(T) \simeq \mathcal{I}(T')$ implica $T \simeq T'$.

3.° Demostrar que todo retículo de generación compacta es isomorfo al retículo de los ideales de un semirretículo.

4.° Demostrar que todo subretículo completo de un retículo de generación compacta es también de generación compacta.

22

Sea T un retículo modular. Si a y b son dos elementos de T, mostrar que el segmento $[a \wedge b, a]$ es isomorfo al segmento $[b, a \vee b]$. Deducir que si b cubre a a, $b \vee x$ cubre a $a \vee x$ ó $b \vee x = a \vee x$. (Recordamos que la expresión b cubre a a significa, que b es mayor que a y que no hay ningún elemento comprendido estrictamente entre b y a.)

23

Sea T un retículo modular y sean $a, b \in T$. Si $\overset{\leqslant}{a}$ y $\overset{\leqslant}{b}$ verifican la condición maximal, mostrar que lo mismo ocurre con $(a \overset{\leqslant}{\vee} b)$. Se puede utilizar el ejercicio precedente.

24

Sea T un retículo modular y complementado. Mostrar que todo segmento $[a, b]$ es complementado.

25

Demostrar que un retículo es distributivo si y sólo si, cualesquiera sean a, b, c,

$$(a \vee b) \wedge c \leqslant a \vee (b \wedge c).$$

26

Demostrar que un retículo es distributivo si y sólo si, cualesquiera sean a, b, c

$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c).$$

27

Si T es un retículo distributivo finito, mostrar que existe un isomorfismo de T en el retículo de partes del conjunto

$$K = \{ x \in T \mid x = y \vee z \Rightarrow x = y \text{ ó } x = z \}.$$

28

En un álgebra de Boole demostrar las relaciones:

$(a \vee b)' = a' \wedge b'$ y $(a \wedge b)' = a' \vee b'$ (se indica con x' el complemento de x).

29

En un álgebra de Boole, donde denotamos con 0 el elemento mínimo, mostrar que $a \wedge b' = 0$ si y sólo si $a \leqslant b$.

30

Demostrar que en un álgebra de Boole, si $\bigvee_{i \in I} b_i$ existe, entonces

$$a \wedge (\bigvee b_i) = \bigvee (a \wedge b_i) \quad \text{para todo } a.$$

31*

Sea T un retículo con elementos mínimo y máximo (0 y 1). Sea I un ideal (es decir, una parte hereditaria estable para $\vee$). Se dice que I es maximal

cuando es maximal entre los ideales de T que no contienen a 1. Se dice que I es primo si

$$a \notin I \text{ y } b \notin I \Rightarrow a \wedge b \notin I.$$

Se dice irreducible si $I = J \cap K$ implica $I = J$ ó $I = K$.

1.° Demostrar que en un retículo cualquiera, todo ideal maximal es irreducible y todo ideal primo es irreducible.

Se llama congruencia en un retículo a una relación de equivalencia compatible con las operaciones $\vee$ y $\wedge$. Demostrar que todo ideal primo P es clase de una congruencia de T (considérese la función característica de $T - P$).

2.° Si T es distributivo, mostrar que todo ideal irreducible es primo.

3.° Inversamente, supongamos que todo ideal irreducible es primo. Mostrar entonces que todo ideal es clase de una congruencia. Deducir que $x \wedge y \leqslant a$ implica $a = (a \vee x) \wedge (a \vee y)$, y luego establecer que T es distributivo.

4.° Supongamos T distributivo y complementado. Demostrar que todo ideal primo es maximal.

5.° Recíprocamente, supongamos T distributivo y tal que todo ideal primo sea maximal. Supóngase, para reducir al absurdo, que c no admite complemento. Sea E el filtro engendrado por c y los elementos d verificando la condición $d \vee c = 1$. Demostrará que existen ideales irreducibles P tales que $P \cap E = \varnothing$ y que estos ideales son primos sin ser maximales.

32

Se considera un retículo distributivo T con elemento mínimo 0 y elemento máximo 1, en el que, para todo a, el conjunto $\{ x \mid x \wedge a = 0 \}$ admite un máximo a'.

1.° Mostrar que la aplicación $a \to a''$ es una clausura de Moore. Se denotará por A el conjunto de clausuras o cerrados.

2.° Mostrar que A (ordenado por el orden inducido) es un retículo, con la cota inferior máxima y la cota superior mínima de dos elementos dadas por las fórmulas

$$\inf (a', b') = a' \wedge b' = (a \vee b)', \quad \sup (a', b') = (a' \vee b')'' = (a \wedge b)'.$$

3.° Mostrar igualmente que $a'' \wedge b'' = (a \wedge b)''$; $\sup (a'', b'') = (a \vee b)''$. Deducir que A es un retículo de Boole.

4.° Si existe un elemento u tal que $u' = 0$ y $a \wedge u = b \wedge u$, mostrar que $a' = b'$. Recíproco [tómese $u = (a' \wedge b') \vee (a \wedge b)$].

5.° Demostrar que el retículo T de los abiertos de un espacio topológico satisface a las condiciones del enunciado. ¿Es completo el correspondiente retículo A?

33

Sea A un álgebra de Boole. Se recuerda que una subálgebra es una parte no vacía estable para $\vee$, $\wedge$ y la complementación. Se llama cuantificador una aplicación $\exists$ de A en A tal que

$$\exists 0 = 0, \quad p < \exists p, \quad \exists(p \wedge \exists q) = \exists p \wedge \exists q$$

(cualesquiera sean p y q, elementos de A).

1.° Demostrar que todo cuantificador es una clausura de Moore.

2.° Sea $\exists$ una clausura de Moore que deja invariante el 0. Demostrar la equivalencia de las siguientes propiedades:

— $\exists$ es un cuantificador.

— La imagen de A según $\exists$ es un subálgebra de A.

— Cualquiera sea p, $\exists(\exists p') = (\exists p)'$.

Deducir en consecuencia, que un cuantificador verifica la igualdad: $\exists(p \vee q) = \exists p \vee \exists q$.

3.° Se dice que una subálgebra B de A, es relativamente completa, si, para todo $a \in A$, hay un mínimo de $\overset{\geqslant}{a} \cap B$. Si $\exists$ es un cuantificador, $\exists(A)$ es relativamente completa. Recíprocamente, si B es relativamente completa, existe un cuantificador $\exists$ tal que $\exists(A) = B$.

4.° Sean X un conjunto, A un álgebra de Boole, $\mathcal{F}(X, A)$ el álgebra de Boole de las aplicaciones de X en A. Sea C una subálgebra de $\mathcal{F}(X, A)$ que contiene las constantes y tal que, para toda $f \in C$, hay cota superior de $f(X)$. Mostrar que hay para C un cuantificador.

34

Consideremos un anillo unitario A en el que todo elemento sea idempotente.

1.° Mostrar que dos elementos que engendren el mismo ideal son iguales.

2.° Mostrar que todo ideal primo es maximal.

3.° Para dos elementos distintos, existe un ideal primo que contiene a uno y no contiene al otro.

4.° Si A es nœtheriano, no tiene más que un número finito de ideales primos.

5.° Si A no tiene más que un número finito m de ideales primos, es finito.

6.° Se considera A como un retículo de Boole. En la hipótesis del punto 5.°, mostrar que m es la longitud común de las cadenas maximales de A.

7.° Mostrar que es, igualmente, el número de elementos minimales.

35

Sea T un retículo distributivo con elemento mínimo 0 y verificando la propiedad: si $0 \neq a \not\leqslant b$, entonces existe x tal que $0 < x \leqslant a$ y $x \wedge b = 0$. Se designa por R el conjunto de los elementos minimales de $T - \{0\}$, y se pone $R(x) = R \cap \overset{\leqslant}{x}$.

1.° Si para todo $a \neq 0$, $R(a)$ es no vacío, mostrar que $a = \bigvee_{r \in R(a)} r$ y que la aplicación $a \to R(a)$ es un isomorfismo de T en $\mathcal{P}(R)$.

2.° Suponemos que toda sección $\overset{\leqslant}{x}$ verifica la condición maximal. Deducir que toda sección $\overset{\leqslant}{x}$ es complementada. Mostrar que resultan estas dos propiedades:

α) Todo intervalo $[a, b]$ es complementado.

β) T verifica la condición minimal (ejercicio II, 34).

3.° Si T satisface las condiciones α) y β), mostrar que para todo $a \neq 0$, $R(a)$ es no vacío y finito.

4.° Demostrar que esta última condición implica que toda sección $\overset{\leqslant}{x}$ verifica la condición maximal.

36

Un álgebra de Boole que tenga ley de grupo y el orden habitual ¿es un grupo ordenado?

37

En un grupo reticulado G, mostrar que $a^n \geqslant e$ para un n, implica $a \geqslant e$. Deducir que entonces G es sin torsión y que el elemento $|b| = b \vee b^{-1}$ es positivo con cualquier b.

38

Sea G un grupo ordenado. Demostrar la equivalencia de las dos propiedades siguientes:

1.° Si a y b son ambos inferiores a c y d, existe un m tal que $a \leqslant m \leqslant c$ y $b \leqslant m \leqslant d$.

2.° Si $e \leqslant x \leqslant yz$ con $y \geqslant e$ y $z \geqslant e$, existen y', z', tales que $e \leqslant y' \leqslant y$, $e \leqslant z' \leqslant z$ y $x = y'z'$.

39

Sea G un grupo ordenado. Ponemos

$$P = \{ x \in G \mid x \geqslant e \} \text{ y } P^{-1} = \{ x^{-1} \mid x \in P \}.$$

Llamaremos P al cono positivo de G.

1.° Demostrar que P cumple las condiciones siguientes:

$$PP \subseteq P; \quad \text{para todo } a, \quad aPa^{-1} = P; \quad P \cap P^{-1} = \{ e \}.$$

2.° Recíprocamente, si P es una parte de G que verifica esas tres propiedades, existe un orden sobre G, y sólo uno, para el que P es el cono positivo.

3.° Demostrar que G es filtrante si y sólo si está engendrado por P.

4.° Demostrar que G es totalmente ordenado si y sólo si $G = P \cup P^{-1}$.

40*

Sea G un grupo reticulado. Sea $\mathcal{R}$ el conjunto de sus partes no vacías mayoradas. Si Y es una parte de G se designará por $M(Y)$ el conjunto de sus mayorantes y por $m(Y)$ el conjunto de sus minorantes.

1.° Mostrar que $Y \to Y^* = m(M(Y))$ es una clausura de Moore en $\mathcal{R}$. Denotaremos por $\mathcal{G}$ el conjunto de las clausuras, ordenado por inclusión.

2.° Mostrar que $\mathcal{G}$ es un retículo en el cual toda parte mayorada (respectivamente, minorada) admite una cota superior (resp. inferior).

3.° Si $a \in G$, se denota $a^* = \{ a \}^*$. Mostrar que $a \to a^*$ es una inyección, que

$$\left(\bigvee_{i \in I} a_i \right)^* = \bigvee_{i \in I} a_i^*, \quad \text{y} \quad \left(\bigwedge_i a_i \right)^* = \bigwedge_i a_i^*,$$

cuando existen $\bigvee_i a_i$ ó $\bigwedge_i a_i$.

4.° Si A, $B \in \mathcal{G}$, pondremos $A \circ B = (AB)^*$. Para Y, $Z \in \mathcal{R}$ mostrar que $Y^* \circ Z^* = (YZ)^*$. Deducir que la ley $\circ$ es asociativa y distributiva con relación a V.

5.° Si $A \in \mathcal{G}$, mostrar que $m(A^{-1}) = B \in \mathcal{G}$. Mostrar que $M(AB)$ es un subsemigrupo de G que contiene al cono positivo P (ejercicio II, 39).

6.° Se supone que G satisface la condición (i): Si para todo $n > 0$, $b^n \geqslant a$, entonces $b \geqslant e$. Mostrar que $\mathcal{G}$ es entonces un grupo reticulado.

7.° Recíprocamente, si G es un grupo reticulado que puede sumergirse en un grupo $\mathcal{G}$ reticulado « completo » (en el sentido de la cuestión 2.ª), demostrar que verifica la condición (i).

Soluciones

1

Supongamos dado el axioma de elección, que es equivalente al de Zorn. Sea φ una función de elección sobre Y. Es claro que $g = \varphi f$ responde a la cuestión. Recíprocamente, pretendemos demostrar la existencia de una función de elección sobre un conjunto Y. Tomemos $X = \mathcal{P}(Y) - \{\varnothing\}$, y para f la identidad. Entonces la aplicación cuya existencia se afirma en el enunciado es una función de elección.

2

Recordemos primero que $\prod_{i \in I} E_i$ es el conjunto de las aplicaciones g de I en $\bigcup_{i \in I} E_i = F$, tales que $g(i) \in E_i$ para todo i. Sea φ una función de elección sobre F y sea f la aplicación de I en $\mathcal{P}(F)$ definida por $i \to E_i$. Es claro que $\varphi f \in \prod_{i \in I} E_i$. Recíprocamente, vamos a demostrar la existencia de una función de elección para un conjunto Y. Tomemos $I = \mathcal{P}(Y) - \{\varnothing\}$. Si $i \in I$, tomemos $E_i = i$. Se tiene evidentemente $E_i \neq \varnothing$. Existe, pues, un elemento φ en $\prod E_i$. Éste es una aplicación de I en $\bigcup_{i \in I} E_i = Y$ tal que

$$\varphi(i) \in E_i = i.$$

3

Supongamos válido el axioma de Zorn y consideremos una familia con la propiedad del enunciado. Si $\mathcal{C} \subseteq \mathcal{F}$ es una cadena, consideremos $C = \bigcup_{X \in \mathcal{C}} X$. Sea K una parte finita de C. Para todo $a \in K$, existe $X_a \in \mathcal{C}$ tal que $a \in X_a$. Entonces $K \subseteq \bigcup_{a \in K} X_a \in \mathcal{C}$ luego $K \in \mathcal{F}$. Puesto que esto es cierto para toda parte finita de C, se tiene $C \in \mathcal{F}$. Luego, $\mathcal{F}$ es $\cup$-inductivo y, por consiguiente, admite un elemento maximal.

Recíprocamente, consideremos un conjunto ordenado F, inductivo. Sea $\mathcal{F}$ la familia de las partes de F totalmente ordenadas. X es totalmente

ordenado si y sólo si toda parte finita de X es totalmente ordenada. Por tanto $\mathcal{F}$ admite un elemento maximal M. Sea m un mayorante de M. No puede ser $m < x$, pues $M \cup \{x\}$ sería un elemento de $\mathcal{F}$ mayor que M. Luego m es maximal.

4

El enunciado implica claramente el axioma de Zorn. Demostremos ahora la recíproca. Sea $\mathcal{B}$ el conjunto de las partes bien ordenadas de E. Si B y B' son de $\mathcal{B}$, pondremos $B \leqslant B'$ si B es una parte hereditaria de B'. El conjunto $\mathcal{B}$ ordenado de este modo es inductivo: en efecto, sea $\mathcal{C}$ una cadena de $\mathcal{B}$ y sea $C = \bigcup_{B \in \mathcal{C}} B$. Si $X \subseteq C$ y $X \neq \varnothing$, tomemos $s \in X$. Existe B en $\mathcal{C}$ tal que $s \in B$. Si $t \leqslant s$ y $t \in C$, existe $B' \in \mathcal{C}$ tal que $t \in B'$. $B' \leqslant B$ implica $\leqslant t \in B$ y $B \leqslant B'$ implica también $t \in B$, puesto que B es hereditario en B'. Se tiene pues $s^{\leqslant} \cap X \subseteq B$. El elemento mínimo de $s^{\leqslant} \cap X$ es efectivamente mínimo en X, pues C es con evidencia totalmente ordenado. Esto muestra que $C \in \mathcal{B}$. La demostración ha probado también que C mayora todo elemento de la cadena. Según el axioma de Zorn, $\mathcal{B}$ admite un elemento maximal M. Sea m un mayorante de M. Si se tuviese $m < a$, $M \cup \{a\}$ sería una parte bien ordenada mayorante estrictamente de M, lo que es imposible. Por consiguiente, m es un elemento maximal.

5

Sea E un conjunto con un orden O que satisface a la condición minimal. Se considera el conjunto $(A_i, O_i)_{i \in I}$ de los pares constituidos por una parte A_i de E hereditaria (para el orden O), y de un buen orden O_i sobre A_i que prolonga el orden O. Se ordena este conjunto por la relación $(A_i, O_i) \leqslant (A_j, O_j)$ si A_i es parte hereditaria de A_j (para el orden O_j) y si el orden O_i es la restricción a A_i del orden O_j. El conjunto $(A_i, O_i)_{i \in I}$ no es vacío (basta considerar un elemento minimal de E). Se puede demostrar que es inductivo, reproduciendo la demostración del lema 1.° de (VI, 3). Según el axioma de Zorn, admitirá un elemento maximal (A_μ, O_μ). Veamos que $A_\mu = E$. Si $A_\mu \neq E$, sea a un elemento minimal para el orden O en $E - A_\mu$. Pongamos $A_\lambda = A_\mu \cup \{a\}$. A_λ es hereditario en E para el orden O: si $x < u$ y $u \in A_\lambda$, o bien $u \in A_\mu$ y en este caso $x \in A_\mu$, pues A_μ es hereditario, o bien $u = a$, y entonces $x \in A_\mu$, pues a es minimal.

Consideremos sobre A_λ el orden O_λ cuya restricción a A_μ es O_μ y tal que $x < a(O_\lambda)$ para todo $x \in A_\mu$. Es claro que éste es un buen orden.

Si $u, v \in A_\lambda$ y $u < v(O)$ dos casos se pueden presentar:

— $u, v \in A_\mu$, entonces $u < v(O_\mu)$, luego $u < v(O_\lambda)$.

— $u \in A_\mu$ y $v = a$. Entonces $u < v(O_\lambda)$.

No hay más casos posibles, pues $u = a$ implicaría $a \in A_\mu$, puesto que A_μ es hereditario para O.

Por último, el par (A_λ, O_λ) pertenece al conjunto considerado, y mayora estrictamente (A_μ, O_μ) lo que es una contradicción. Luego O_μ es un buen orden sobre E más fino que O.

6

1.° $\mathcal{J}$ no es vacío, pues $(0, 0) \in \mathcal{J}$. Sea $(L_i, \gamma_i)_{i \in I}$ una cadena de $\mathcal{J}$. Los L_i para $i \in I$ forman una cadena, luego $L = \bigcup_{i \in I} L_i$ es un subespacio. Si $X \in \mathcal{V}(L)$ pondremos

$$\gamma_L(X) = \bigcup_{i \in I} \gamma_i(X \cap L_i).$$

Se tiene $\gamma_L(X) \in \mathcal{V}(L)$, pues las $\gamma_i(X \cap L_i)$ forman una cadena. Además,

$$X \cap \gamma_L(X) = \bigcup_{i \in I} [X \cap \gamma_i(X \cap L_i)] = \bigcup_{i \in I} [X \cap L_i \cap \gamma_i(X \cap L_i)] = 0.$$

Si $a \in L$, existe un i tal que $a \in L_i$. Se tiene, pues, $a = b + c$, con

$$b \in X \cap L_i \subseteq X, \quad \text{y} \quad c \in \gamma_i(X \cap L_i) \subseteq \gamma_L(X).$$

Luego $L = X \oplus \gamma_L(X)$. Si $X \subseteq Y \subseteq L$, se tiene, para todo i,

$$X \cap L_i \subseteq Y \cap L_i, \quad \gamma_i(Y \cap L_i) \subseteq \gamma_i(X \cap L_i), \quad \text{luego} \quad \gamma_L(Y) \subseteq \gamma_L(X).$$

Por consiguiente $(L, \gamma_L) \in \mathcal{J}$ mayora la cadena. $\mathcal{J}$ es, pues, inductivo.

2.° Si $X \subseteq M$, se tiene

$$M \oplus Ka = [X \oplus \gamma_M(X)] \oplus Ka = X \oplus \tau(X).$$

Si $X \nsubseteq M$, observemos primero que

$$X \cap \gamma_M(X \cap M) = X \cap M \cap \gamma_M(X \cap M) = 0.$$

Sea $x \in X - M$. Se tiene $x = m + \lambda a$, con $m \in M$ y $\lambda \neq 0$. Por tanto,

$$a = \lambda^{-1} x - \lambda^{-1} m \in X + M,$$

$$M \oplus Ka \subseteq X + M = X + (X \cap M) + \gamma_M(X \cap M) = X + \gamma_M(X \cap M) = X + \tau(X).$$

Finalmente, en este caso se tiene también $M \oplus Ka = X \oplus \tau(X)$. Supongamos $X \subseteq Y \subseteq M \oplus Ka$:

— si $X \subseteq M$, se tiene $X \subseteq Y \cap M$, luego

$$\tau(Y) \subseteq \gamma_M(Y \cap M) \oplus Ka \subseteq \gamma_M(X) \oplus Ka = \tau(X);$$

— si $X \not\subseteq M$ *a fortiori* $Y \not\subseteq M$, y se tiene

$$\tau(Y) = \gamma_M(Y \cap M) \subseteq \gamma_M(X \cap M) = \tau(X).$$

Luego, tenemos $(M \oplus Ka, \tau) \in \mathcal{J}$ y es un mayorante estricto de (M, γ_M) de donde una contradicción. Luego, en realidad, $M = E$, es decir, que existe una aplicación que, a todo subespacio de E asocia un suplementario, y que es decreciente.

7

1.° Es claro que $\overset{\geq}{a}$ pertenece a Φ. Se tiene, pues, $A \subseteq \overset{\geq}{a}$ y *a fortiori* $B \subseteq \overset{\geq}{a}$. Luego, para todo $y \in B$, $a < y$, lo que implica $a \in C$. Si $z \in C$, $f(z)$ pertenece a C: en efecto, si $y \in B$ se pueden distinguir tres casos

— $f(y) < z$. Entonces $f(y) < f(z)$.

— $z = y$. Entonces $f(y) < f(z)$.

— $z < y$. En este caso $f(z) < y$, puesto que $y \in B$.

Si $X \subseteq C$ es totalmente ordenado, y si z es su cota superior, se sabe ya que $z \in A$. Si $y \in B$ se pueden distinguir dos casos:

— $x < y$ para todo $x \in X$. Entonces $z < y$.

— Existe $x \in X$ tal que $x \not< y$. Como $x \in C$, esto implica $f(y) < x$, luego, *a fortiori* $f(y) < z$.

Se ha demostrado así que $z \in C$. Siendo A minimal se tiene $A = C$.

2.° Como $A \subseteq \overset{\geq}{a}$, $a \in B$ es una verdad evidente.

Si $y \in B$, $f(y) \in B$. En efecto, sea $x \in A$ tal que $x < f(y)$. Como $x \in C$, se tiene $x < y$ ó $f(y) < x$. Pero la segunda eventualidad está excluida. Distingamos entonces dos casos:

— $x = y$. Entonces, evidentemente, $f(x) < f(y)$.

— $x < y$. Como $y \in B$, se tiene entonces $f(x) < y$, luego *a fortiori*

$$f(x) < f(y).$$

Sea $X \subseteq B$. Designemos por y la cota superior de X y demostremos que $y \in B$. Sea $t \in A$, $t < y$. Existe un $x \in X$ tal que $x \not\leqslant t$. Pero $t \in C$ y $x \in B$ implican $t < x$ ó $f(x) \leqslant t$. La segunda eventualidad queda excluida porque exigiría $x \leqslant t$. La primera se reduce a $t < x$ e implica $f(t) \leqslant x$, puesto que $x \in B$. *A fortiori* $f(t) \leqslant y$.

Se tiene, pues, $B \in \Phi$ y, en consecuencia, $B = A$.

3.° Sean y, $z \in A$. Se tiene $z \leqslant y$ ó $f(y) \leqslant z$, lo que implica $y \leqslant z$. Por tanto, A es totalmente ordenado. Existe $m = \sup A$, y como $A \in \Phi$ se tiene $m \in A$. Por la misma razón $f(m) \in A$, luego $f(m) = m$. Esta igualdad no puede cumplirse más que si m es maximal. Se tiene así otra demostración del hecho de que, mediante el axioma de elección, todo conjunto fuertemente inductivo admite un elemento maximal.

En efecto, A es bien ordenado: Sea $X \subseteq A$, $X \neq \varnothing$. El conjunto

$$\{t \mid t \in A \text{ y } t \leqslant x \text{ para todo } x \in X\}$$

no es vacío, puesto que contiene a a. Sea h su cota superior. Se tiene $h \in A$. Si fuese $h \leqslant x$ para todo $x \in X$, resultaría $f(h) \leqslant x$ (pues $x \in B$), luego $f(h) \leqslant h$ y h sería maximal, en contradicción con $h \geqslant X \neq \varnothing$. Luego existe un $x \in X$ tal que $h = x$, es decir, que h es mínimo en X.

8

1.° Sea $\mathcal{C}$ la familia de subálgebras de A conteniendo a B y sin contener a m. Es $B \in \mathcal{C}$, luego $\mathcal{C} \neq \varnothing$. Ordenado $\mathcal{C}$ por inclusión, es inductivo: si $(D_i)_{i \in I}$ es una cadena, es claro que $D = \cup D_i \in \mathcal{C}$. Mediante el axioma de Zorn $\mathcal{C}$ admite un elemento maximal C.

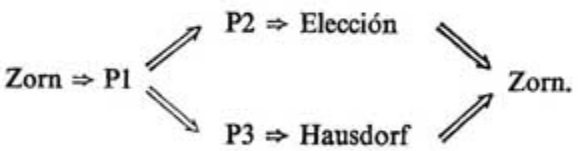
2.° C es $\cap$-irreducible: si $C = \bigcap_{\alpha \in T} B_\alpha$, existe α tal que $m \notin B_\alpha$, luego $B_\alpha \in \mathcal{C}$ y, puesto que C es maximal, $B_\alpha = C$. Por consiguiente m no pertenece a la intersección de las subálgebras $\cap$-irreducibles que contienen a B. Esta intersección es, pues, igual a B.

3.° Sean K una base finita de A y B una subálgebra. Se va a razonar por recurrencia sobre el número n de elementos de la base que no están en B. Si $n = 1$, $K - B = \{a\}$. Según (P1) existe un C maximal para las propiedades $B \subseteq C$ y $a \notin C$. Toda subálgebra mayor contiene a K, luego es A, y C es efectivamente maximal. Si la propiedad es cierta para $n' < n$, sea $a \in K - B$. Sea C maximal para las propiedades $B \subseteq C$ y $a \notin C$. Si C es maximal, todo va bien. Si no, sea $C \subset D \subset A$. D contiene a a, y también a los elementos de K que B contenía ya. Luego en $K - D$ hay menos de n elementos. D está contenida en un subálgebra maximal, y también B, *a fortiori*.

4.° Se puede considerar que en $\mathcal{T}$ se tiene la ley interna $(x, y) \to x \vee y$, y la ley externa $(x, a) \to x \wedge a$ (con el propio $\mathcal{T}$ como dominio de operadores). Esto supuesto, las subálgebras son exactamente los ideales. $\mathcal{T}$ tiene una base finita, reducida al elemento máximo. (P3) afirma que todo ideal propio está contenido en un ideal maximal. $\Gamma \cup \{X\}$ es una familia de Moore, luego es un retículo completo. Si Π es un ideal maximal de este retículo, consideremos $R = \bigcup_{Y \in \Pi} Y$. Sean a, $b \in R$. Existen Y_1, $Y_2 \in \Pi$ tales que $a \in Y_1$, $b \in Y_2$. Luego, a y b pertenecen a $Y_1 \vee Y_2 \in \Pi$. Como $X \notin \Pi$, $Y_1 \vee Y_2 \in \Gamma$, luego a y b son comparables. Luego, $R \in \Gamma$. No existe ninguna cadena mayor que R', pues $\{ Y \in \Gamma \mid Y \subseteq R' \}$ sería un ideal propio conteniendo estrictamente a Π. De este modo se ha demostrado que (P3) implica el axioma de Hausdorf.

5.° Si B es una subálgebra propia, sea $a \notin B$. $(F, x) \in B$ y $(F, y) \in B$, implican $(F, x)\sigma_a(F, y) \in B$, luego $(F, x)\sigma_a(F, y) \neq a$, luego $x = y$. Así, B define una función. Recíprocamente si B es el grafo de una función, y si $(F, x) \in \mathcal{P}$, existe $y \in F$ tal que $y \neq x$ y $(F, y) \notin B$. Cualesquiera sean b y $c \in B$, se tiene siempre $b\sigma_a c = b \in B$, luego B es una subálgebra. La subálgebra vacía es intersección de las subálgebras $\cap$-irreducibles, mediante (P2). Esto exige la existencia de una subálgebra propia $\cap$-irreducible I. Demostremos que para todo $F \in \mathcal{P}$, existe $x \in F$ tal que $(F, x) \in I$.

Para la reducción al absurdo, tomemos dos elementos x e y de F distintos, con $(F, x) \notin I$, y $(F, y) \notin I$. Las subálgebras $I \cup (F, x)$ e $I \cup (F, y)$ son distintas de I, pero admiten I por intersección. Por consiguiente I define una aplicación de $\mathcal{P}$ en E tal que $I(F) = x \in F$. Si, además, a todo conjunto reducido a un elemento se asocia este mismo elemento, se ve que existe en E una función de elección. En resumen



9

1.° Sea $x \in E$. Pondremos $\varphi(x) = \inf_{f \in \mathcal{C}} f(x)$.

Si $x < y$, $f(x) < f(y)$, luego $\varphi(x) < f(y)$ para toda $f \in \mathcal{C}$.

Existe $f \in \mathcal{C}$ tal que $\varphi(y) = f(y)$. Luego $\varphi(x) < \varphi(y)$. Es claro que φ es mínimo en $\mathcal{C}$.

Se tiene, pues, $\overset{<}{\varphi}(x) \subseteq \overset{<}{\varphi}(x)$. Recíprocamente, sea $\mu < \varphi(x)$. Consideremos

$$\{ t \in E \mid \mu < \varphi(t) \}.$$

Este conjunto no es vacío, pues contiene a x. Sea a mínimo en este conjunto. Pondremos

$$\bar{\varphi}(x) = \begin{cases} \varphi(x) & \text{si} \quad x \neq a \\ \mu & \text{si} \quad x = a. \end{cases}$$

Si $y < a$, $\bar{\varphi}(y) = \varphi(y) < \mu = \bar{\varphi}(a)$.

Si $a < y$, $\bar{\varphi}(a) = \mu \leqslant \varphi(a) < \varphi(y) = \bar{\varphi}(y)$.

Luego $\bar{\varphi} \in \mathcal{C}$. Como $\bar{\varphi} \leqslant \varphi$, es $\bar{\varphi} = \varphi$, de donde $\varphi(a) = \mu$, $\mu \in \varphi(\overset{<}{x})$. Se ha demostrado así que $\varphi(\overset{<}{x}) = \varphi(x)$. Si $f \in \mathcal{C}$ tiene también esta propiedad, se tiene $\varphi \leqslant f$. Supongamos $\varphi \neq f$. Sea c mínimo en $\{ x \mid \varphi(x) < f(x) \}$. $\varphi(c) < f(c)$. Existe $d < c$ tal que $f(d) = \varphi(c)$. Pero entonces, $\varphi(d) = f(d) = \varphi(c)$, de donde una contradición. Esta condición significa que $f(E)$ es hereditaria. En efecto, $f(\overset{<}{x}) = f(\overset{<}{x}) \subseteq f(E)$. Recíprocamente, si $y = f(\overset{<}{x})$, existe t tal que $y = f(t)$. Necesariamente, $t < x$, luego $y \in (\overset{<}{x})$. Como se tiene $f(\overset{<}{x}) \subseteq f(\overset{<}{x})$ cuando $f \in \mathcal{C}$, resulta la igualdad.

2.° *a*) Si $y < z \leqslant t_h$, $h(y) < h(y') \leqslant h(z)$, luego h es estrictamente creciente sobre $\overset{\leqslant}{t_h}$. Según 1) existe $\tilde{h}$.

b) Si $t_g \leqslant t_h$ se sabe que la imagen de $\tilde{h}$ es hereditaria. La restricción de $\tilde{h}$ a $\overset{\leqslant}{t_g}$ posee también esta propiedad, luego coincide con $\tilde{g}$. Destaquemos de otra parte que todas las t_h son comparables. Así, pues, se define una aplicación estrictamente creciente de E' en F, si se asocia a todo $x \in E'$ el elemento $\gamma(x) = \tilde{h}(x)$, donde h es un elemento de Γ tal que $x \leqslant t_h$.

c) Observemos primero que E' es hereditaria, como reunión de partes hereditarias. Lo mismo sucede con $\gamma(E') = \cup \tilde{h}(\overset{\leqslant}{t_h})$. Luego, todo $x \notin E'$ mayora todo elemento de E' y b mayora todo elemento de $\gamma(E')$. En consecuencia, poniendo $\tau(x) = \gamma(x)$ si $x \in E'$ y $\tau(x) = b$ si $x \notin E'$, definimos una aplicación creciente. Consideremos $t_\tau \in E'$. Se tiene

$$\tau(t'_\tau) = \tau(t_\tau) = \gamma(t_\tau) \in \gamma(E').$$

Luego $t'_\tau \in E'$. Pero entonces, $\gamma(t'_\tau) = \tau(t'_\tau) = \gamma(t_\tau)$, lo que es absurdo.

d) Sea a mínimo en $E - E'$. Como E' es hereditario se ve inmediatamente que $E' = \overset{<}{a}$. Es, pues, un intervalo. Por ser γ estrictamente creciente, define un isomorfismo de E' sobre F. En conclusión, si E y F son dos conjuntos bien ordenados, o bien existe una aplicación estrictamente creciente

de E en F, en cuyo caso la aplicación φ definida en el apartado 1.° es un isomorfismo de E sobre un intervalo de F, o bien no existe y entonces acabamos de ver que γ^{-1} es un isomorfismo de F sobre un intervalo de E.

3.° Sea $\mathcal{G}$ el conjunto de los pares (H, f) donde H es una parte hereditaria de E y f un isomorfismo de H sobre una parte hereditaria de F. $\mathcal{G}$ no es vacío (considérese la aplicación que a inf E asocia inf F). Lo ordenaremos por la relación

$$(H, f) < (H', f')$$

si y sólo si $H \subseteq H'$ y f' prolonga a f. Se ve fácilmente que $\mathcal{G}$ es inductivo. Por el axioma de Zorn admite, pues, un elemento maximal (H^*, f^*). No puede ser simultáneamente $H^* \neq E$ y $f^*(H) \neq F$, pues se tendría entonces $H^* < a, f^*(H) < b$. La aplicación g definida sobre $H^* \cup \{a\}$ que prolonga f^* y que toma el valor b en a es tal que $(H^*, f^*) < (H^* \cup \{a\}, g)$, lo que es absurdo.

10

1.° Sea $a \notin \varphi(X)$. Sea N la intersección de las partes de X estables para φ que contienen a a. Es claro que N responde a la cuestión.

2.° Consideremos las partes G de $N \times N'$ tales que $(a, a') \in G$ y si $(x, y) \in G$ entonces $(\varphi(x), \varphi'(y)) \in G$. Su intersección F posee evidentemente estas propiedades.

Para todo $x \in N$, existe $y \in N'$ tal que $(x, y) \in F$: esto es cierto para a, puesto que $(a, a') \in F$. Si esto es cierto para x lo es también para $\varphi(x)$, por la segunda condición impuesta. Además, sea K el conjunto de los $x \in N$ tales que $(x, y) \in F$ y $(x, y') \in F$ implica $y = y'$. Se tiene $a \in K$, pues si $(a, y) \in F$ con $y \neq a'$, entonces $G = F - (a, y)$ pertenece a la familia, lo que es absurdo. Si $x \in K$, sea $y \in N'$ con $(x, y) \in F$. Supongamos $(\varphi(x), t) \in F$, con $t \neq \varphi'(y)$. Si $t \notin \varphi'(N')$, entonces $G = F - (\varphi(x), t)$ pertenece a la familia. Si $t = \varphi'(z)$, se tiene $z \neq y$, luego $(x, z) \notin F$ y se obtiene la misma contradicción. Por consiguiente, $\varphi(x) \in K$. En consecuencia $K = N$, lo que significa que F es una función de N en N'. Es biyectiva, pues en la demostración precedente se pueden invertir los papeles de N y N'.

3.° Tenemos $a \notin \varphi S(a)$, puesto que $a \notin \varphi(N)$. Cuando x satisface la relación $x \notin \varphi S(x)$, lo mismo ocurre con $\varphi(x)$:

$\varphi(x) \in \varphi S(\varphi x)$ implicaría $\varphi(x) = \varphi(z)$, con $z \in S(\varphi x)$, $x = z$, pues φ es inyectiva. Pero, por otra parte, $\varphi S(x)$ es estable, pues $\varphi S(x) \subseteq S(x)$ implica $\varphi\varphi S(x) \subseteq \varphi S(x)$. Como $\varphi(x) \in \varphi S(x)$, se tiene, pues, $S\varphi(x) \subseteq \varphi S(x)$ de donde $x \in \varphi(Sx)$, contra la hipótesis.

El par $[S(x), \varphi]$ puede hacer el mismo papel que el par (N', φ') en la segunda cuestión. Es, pues, « isomorfo » a (N, φ).

4.° Consideremos $\{ b \in N \mid b \notin \varphi(N) \text{ y } b \neq a \}$. Su complementario en N es estable para φ y contiene a a. Es, pues, todo N. Luego, a es el único elemento de N que no pertenece a $\varphi(N)$.

$$S(a) = N = \{ a \} \cup \varphi(N) = \{ a \} \cup \varphi S(a).$$

Por otra parte, $a \cup S\varphi(a)$ es una parte estable que contiene a a, luego es N. Como $S\varphi(a) \subseteq \varphi S(a)$, se tiene necesariamente $S\varphi(a) = \varphi S(a)$. Estas dos relaciones se transportan a todo elemento de N, gracias al isomorfismo demostrado en la cuestión 3.ª.

5.° Se tiene, pues, $x < y \Leftrightarrow S(y) \subseteq S(x)$. Esta relación es evidentemente reflexiva y transitiva. Si $x < y$ e $y < x$, se tiene $S(x) = S(y)$. Ahora bien, x es el único elemento de $S(x)$ que no pertenece a $\varphi S(x)$. Se tiene, pues, $x = y$.

Además

$$\begin{aligned} x < y \Leftrightarrow S(y) \subseteq S(x) &\Leftrightarrow \varphi S(y) \subseteq \varphi S(x) \\ &\Leftrightarrow S\varphi(y) \subseteq S\varphi(x) \\ &\Leftrightarrow \varphi(x) < \varphi(y). \end{aligned}$$

6.° Sea $K = \{ x \in N \mid \forall y \in N,\ x < y \text{ ó } y < x \}$.

Se tiene $a < y$ para todo $y \in N$, luego $a \in K$. Supongamos $x \in K$. Como φ es creciente, se tiene $\varphi(x) < \varphi(y)$ ó $\varphi(y) < \varphi(x)$ para todo $y \in N$. Es decir, que $\varphi(x)$ es comparable a todo elemento de $\varphi(N)$. Como es comparable a a, pertenece a K. Se tiene, pues, $K = N$ y el orden es total. Si $x \in N$, sea $I(x)$ su sección inicial.

Si $y < \varphi(x)$, se tiene $y \in I(x)$ ó $x < y$. En este caso, $S\varphi(x) \subseteq S(y) \subseteq S(x)$, lo que implica $S\varphi(x) = S(y)$, luego $y = \varphi(x)$. Finalmente

$$I(\varphi(x)) = I(x) \cup \{ \varphi(x) \}$$

$I(a)$ es, evidentemente, bien ordenado. Si $I(x)$ es bien ordenado, también lo es $I(\varphi x)$, por la relación precedente. Luego toda sección inicial es bien ordenada. El propio N estará bien ordenado, puesto que ya sabemos que el orden es total.

11

Consideremos el conjunto $X = \{ x \in T \mid x < a(x) \}$. X no es vacío, puesto que contiene al menor elemento de T.

Sea $b = \bigvee_{x \in X} x$. Si $x \in X$ se tiene $x < b$, luego $x < a(x) < a(b)$. Por tanto, $a(b)$ es un mayorante de X. Resulta que $b < a(b)$ (luego $b \in X$). Pero la desigualdad precedente implica $a(b) < a(a(b))$ luego $a(b) \in X$ y por tanto $a(b) < b$. Finalmente, vemos que $a(b) = b$.

12

Mostremos que el primer sistema implica el segundo: si $x < \bar{y}$ se tiene $\bar{x} < \bar{\bar{y}}$ y $\bar{\bar{y}} = \bar{y}$, luego $\bar{x} < \bar{y}$.

Recíprocamente, supongamos que se satisface el segundo sistema.

Si $x < y$, como $y < \bar{y}$, se tiene $x < \bar{y}$ y por consiguiente $\bar{x} < \bar{y}$. Por otra parte, $\bar{x} < \bar{x}$, luego $\bar{\bar{x}} < \bar{x}$. El carácter extensivo de la clausura da $\bar{x} < \bar{\bar{x}}$, de donde la igualdad $\bar{x} = \bar{\bar{x}}$.

13

Consideremos $E = \mathbf{N} \times \{0, 1\}$. Se pone $(0, n) < (0, n')$ si y sólo si $n < n'$ y $(0, n) < (1, n + 1)$ para todo n. Se ve fácilmente que la única clausura de Moore es la identidad.

14

Sean u y v dos clausuras de Moore sobre un conjunto ordenado E. Ponemos $u < v$ si $u(x) < v(x)$ para todo x. Vamos a demostrar que $u < v$, $uv = v$, $vu = v$, $v(E) \subseteq u(E)$, son proposiciones equivalentes.

Supongamos $u < v$. Entonces $v(x) < uv(x) < vv(x) = v(x)$, luego $uv = v$. Esta igualdad, $uv = v$, significa que todo elemento de $v(E)$ es invariante para u, es decir, que $v(E) \subseteq u(E)$.

Supongamos $uv = v$. Se tiene

$$v(x) < vu(x) < vuv(x) = vv(x) = v(x),$$

luego $vu = v$. En fin, si $vu = v$, $u(x) < vu(x) = v(x)$, luego $u < v$.

15

Se tiene $\pi(x) < \pi\sigma\pi(x)$. Por otra parte, $x < \sigma\pi x$ implica $\pi\sigma\pi(x) < \pi(x)$ de donde la igualdad $\pi = \pi\sigma\pi$. Se demuestra del mismo modo que $\sigma\pi\sigma = \sigma$.

Si $x < \sigma\pi(y)$, se tiene $\pi(y) = \pi\sigma\pi(y) < \pi(x)$, luego $\sigma\pi(x) < \sigma\pi(y)$. Esto basta para demostrar que $\sigma\pi$ es una clausura de Moore. Si $\sigma(y)$ es un ele-

mento de $\sigma(F)$ se tiene $\sigma\pi\sigma(y) = \sigma(y)$, luego $\sigma(y)$ es invariante para $\sigma\pi$. La recíproca es inmediata.

$\sigma\pi$ restringido a $\sigma(F)$ es, pues, la aplicación idéntica. Del mismo modo, $\pi\sigma$ restringido a $\pi(E)$ es la aplicación idéntica. En consecuencia, π define una biyección de $\sigma(F)$ sobre $\pi(E)$.

16

Sea $X \subseteq T'$ con $X \neq \varnothing$. Puesto que $\varphi^{-1}(X)$ admite un elemento maximal m, no es vacío. Supongamos que $\varphi(m) < x' \in X$. Tomemos x tal que $\varphi(x) = x'$. Entonces,

$$\varphi(x \vee m) = \varphi(x) \vee \varphi(m) = x' \in X, \quad \text{luego} \quad x \vee m \in \varphi^{-1}(X).$$

Pero $x \vee m > m$, luego efectivamente $x \vee m = m$, puesto que m es maximal. Resulta $x' = \varphi(m)$, luego $\varphi(m)$ es maximal en X.

17

Si toda cadena es finita, es evidente que toda sucesión estrictamente creciente o estrictamente decreciente es finita. Si existe una cadena infinita C, y si E satisface la condición minimal, podremos construir una sucesión del siguiente modo. Sea c_1 un elemento minimal (luego mínimo) de C. Se toma c_{n+1} minimal (luego mínimo) en $C \cap \overset{>}{c}_n$. Se tiene así una sucesión estrictamente creciente infinita, y por consiguiente no se cumple la condición maximal.

18

Se sabe ya que E cumple las condiciones maximal y minimal. Vamos a demostrar que la sección terminal $\overset{\geq}{x}$ de todo elemento x es finita. En efecto supongamos, para reducir al absurdo, que el conjunto $X = \{x \in E \mid \overset{\geq}{x} \text{ infinito}\}$, sea no vacío. Sea s maximal en este conjunto. Sea M el conjunto de los elementos minimales de $\overset{>}{s}$. Se tiene $\overset{\geq}{s} = \bigcup_{m \in M} \overset{\geq}{m}$. M es finito porque es una parte trivialmente ordenada y cada $\overset{\geq}{m}$ es finito porque $m \notin X$. Luego $\overset{>}{s}$ es finito, lo que da una contradicción. Por tanto, efectivamente, X es vacío. Si K designa el conjunto de los elementos minimales de E, se tiene $E = \bigcup_{x \in K} \overset{\geq}{x}$. Cada $\overset{\geq}{x}$ es finito, y K es finito, puesto que es una parte trivialmente ordenada, luego E es finito.

19

A implica *B*. En efecto, si X es una parte que verifica la condición maximal, toda cadena de X es finita, puesto que X verifica también la condición minimal. Según el ejercicio precedente, X es finito. Mostremos ahora que *B* implica *A*.

En primer lugar toda sucesión estrictamente decreciente es una parte de E que cumple la condición maximal, luego es finita. Es también evidente que toda parte trivialmente ordenada verifica la condición maximal.

20

La propiedad es evidente para $k = 1$. Vamos, pues, a razonar por inducción sobre K. Escribiremos $\mathbf{N}^k = \mathbf{N}^{k-1} \times \mathbf{N}$.

Sea φ la proyección de $\mathbf{N}^k$ sobre $\mathbf{N}^{k-1}$ y sea σ su proyección sobre N. Desde luego, $\mathbf{N}^k$ verifica la condición minimal, pues toda sección inicial es finita y *a fortiori* toda sucesión estrictamente decreciente es finita. Sea X una parte de $\mathbf{N}^k$ trivialmente ordenada. El conjunto $I = \{ x \in X \mid \varphi(x)$ minimal en $\varphi(X) \}$ es finito. En efecto:

Primeramente, el conjunto de elementos minimales de $\varphi(X)$ es una parte trivialmente ordenada de $\mathbf{N}^{k-1}$, luego es finito. Además, si x e $y \in X$ son tales que $\varphi(x) = \varphi(y)$, se tiene $x = y$, pues si no x e y serían comparables. Sea $a = \bigvee_{x \in I} \sigma(x)$. Si $y \in X$ se puede encontrar $x \in I$ tal que $\varphi(x) < \varphi(y)$. Por consiguiente $\sigma(y) < \sigma(x) < a$, puesto que x e y no son comparables. Se ve que $\sigma(X)$ está contenido en $\overset{<}{a}$, luego es finito. Tomemos $b < a$ y consideremos $K_b = \{ x \in X \mid \sigma(x) = b \}$. Es claro que $\varphi(K_b)$ es trivialmente ordenado, luego finito. Por tanto, el propio K_b es finito.

Resulta de esto que $X = \bigcup_{b<a} K_b$ es finito.

21

1.° Es claro que $\mathcal{S}(T)$ es una familia de Moore, luego un retículo completo. Sea $(C_i)_{i \in I}$ una familia de ideales.

Su cota superior es el conjunto de los x para los que se puede encontrar elementos $x_{i_1}, \ldots, x_{i_n}$ tales que $x < x_{i_1} \vee \ldots \vee x_{i_n}$ y $x_{i_p} \in C_{i_p}$. Si $\overset{<}{a}$ designa la sección inicial de a, se ve inmediatamente que la aplicación $a \to \overset{<}{a}$ es un isomorfismo de T en $\mathcal{S}(T)$. Se tiene, en efecto, $\overset{<}{a} \vee \overset{<}{b} = \overset{<}{(a \vee b)}$.

2.° Mostremos que $\overset{\leqslant}{a}$ es compacto en $\mathcal{S}(T)$. Si $\overset{\leqslant}{a} \subseteq \bigvee_{i \in I} C_i$,

$$a \in \bigvee C_i, \qquad \text{luego} \qquad a < x_{i_1} \vee \ldots \vee x_{i_n} \text{ y } x_{i_p} \in C_{i_p}.$$

Luego, en efecto, $a \in C_{i_1} \vee \ldots \vee C_{i_n}$.

Recíprocamente, sea K un ideal compacto. Se tiene

$$K = \bigvee_{a \in K} \overset{\leqslant}{a}, \quad \text{luego} \quad K = \overset{\leqslant}{a_1} \vee \ldots \vee \overset{\leqslant}{a_n} \quad \text{con} \quad a_i \in K.$$

Si ponemos $a = a_1 \vee \ldots \vee a_n$, resulta $K = \overset{\leqslant}{a}$. Cuando se concoce $\mathcal{S}(T)$, está, pues, determinado T, a menos de un isomorfismo.

3.° Sea L un retículo de generación compacta. Sea T el conjunto de los compactos (distintos del mínimo). Es un $\vee$-semirretículo: Si $a, b \in T$ y $a \vee b \leqslant \bigvee_{i \in I} x_i$ se tiene

$$a \leqslant \bigvee_{i \in I} x_i \quad \text{y} \quad b \leqslant \bigvee_{i \in I} x_i,$$

luego existen partes finitas F y F' de I tales que

$$a \leqslant \bigvee_{i \in F} x_i, \quad b \leqslant \bigvee_{i \in F'} x_i.$$

Por consiguiente

$$a \vee b \leqslant \bigvee_{F \cup F'} x_i.$$

Se define una aplicación de L en $\mathcal{S}(T)$ del modo siguiente:

$$a \to I_a = \overset{\leqslant}{a} \cap T.$$

Es claro que $a = \bigvee_{x \in I_a} x$. Luego $I_a \subseteq I_b \Leftrightarrow a < b$. La aplicación es, pues, inyectiva. Sea I un ideal de T. Pongamos $a = \bigvee_{x \in I} x$. Entonces, evidentemente, $I \subseteq I_a$. Recíprocamente, si $u \in I_a$, $u < a$; como u es compacto $u \leqslant \bigvee_{x \in F} x$, con $F \subseteq I$, finito. Pero $\bigvee_F x \in I$, luego $u \in I$.

La aplicación considerada es un isomorfismo.

4.° Sea L un retículo de generación compacta y sea N un subretículo completo. Toda sección inicial de L es de generación compacta, luego se puede suponer que N y L tiene un mismo máximo, es decir, que N es una familia de Moore en L. Sea $x \to \bar{x}$ la clausura asociada. Si c es compacto, $\bar{c}$ es compacto en N. En efecto

$$\bar{c} \leqslant \bigvee_{i \in I} x_i \quad (x_i \in N) \text{ implica } c \leqslant \bigvee_{i \in I} x_i, \quad \text{luego} \quad c \leqslant \bigvee_{i \in F} x_i.$$

Resulta $\bar{c} \leqslant \bigvee_{i \in F} x_i$, pues $\bigvee_{F} x_i$ pertenece a N. Finalmente, sea $h \in N$. Se tiene $h = \bigvee_{j \in J} c_j$, donde c_j es compacto en L. Es $h \leqslant \bigvee_{j \in J} \bar{c}_j$. Pero, de otra parte, $c_j \leqslant h$ implica $\bar{c}_j \leqslant h$, luego $h = \bigvee_{J} \bar{c}_j$, lo que demuestra que N es de generación compacta.

22

Consideremos la aplicación φ definida sobre $[a \wedge b, a]$ por $\varphi(x) = x \vee b$, y la aplicación ψ definida sobre $[b, a \vee b]$ por $\psi(y) = y \wedge a$. Se ve inmediatamente que estas dos aplicaciones aplican uno sobre otro los dos segmentos dichos, y que ambas son crecientes. Falta hacer ver que son mutuamente recíprocas. Por la condición modular ocurre que

$$\psi\varphi(x) = (x \wedge b) \wedge a = x \vee (b \wedge a) = x,$$
$$\varphi\psi(y) = b \vee (a \wedge y) = (b \vee a) \wedge y = y.$$

Supongamos ahora que b cubra a a. Según lo demostrado,

$$[(a \vee x) \wedge b, b] \simeq [a \vee x, (a \vee x) \vee b] = [a \vee x, b \vee x].$$

Pero se tiene $a \leqslant (a \vee x) \wedge b \leqslant b$, luego $(a \vee x) \wedge b = a$ ó $(a \vee x) \wedge b = b$. En el primer caso, resulta $[a, b] \simeq [a \vee x, b \vee x]$, luego $b \vee x$ cubre a $a \vee x$. En el segundo caso ocurre $a \vee x = b \vee x$.

23

Consideremos una sucesión creciente de elementos

$$x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n \leqslant \cdots \leqslant a \vee b.$$

La sucesión $x_n \wedge b$ es estacionaria desde cierto índice p en adelante, pues b satisface la condición maximal.

Por otra parte, $[a \wedge b, a]$ cumple la condición maximal, luego otro tanto $[b, a \vee b]$ que le es isomorfo. La sucesión $x_n \vee b$ es, pues, estacionaria desde un cierto índice q. Puede tomarse $q > p$. Entonces, si $n > q$, se tiene

$$x_n \wedge b = x_q \wedge b \quad \text{y} \quad x_n \vee b = x_q \vee b.$$

Como $x_q < x_n$, la modularidad implica $x_q = x_n$.

24

Sea $t \in [a, b]$ y sea t' un complemento de t en T.
Es claro que $(t' \vee a) \wedge b \in [a, b]$. Ahora bien, se tiene

$$t \vee [(t' \vee a) \wedge b] = (t \vee t' \vee a) \wedge b = b$$
$$t \wedge [(t' \vee a) \wedge b] = [(t \wedge t') \vee a] \wedge b = a \wedge b = a.$$

Se ve que $(t' \vee a) \wedge b$ es un complemento de t en $[a, b]$.

25

Supongamos el retículo distributivo. Se puede escribir

$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c) < a \vee (b \wedge c).$$

Recíprocamente, si esta condición se cumple,

$$(x \vee y) \wedge (x \vee z) < x \vee [y \wedge (x \vee z)] < x \vee [x \vee (y \wedge z)] = x \vee (y \wedge z)$$

de donde la igualdad, pues la desigualdad recíproca es siempre cierta.

26

Se tiene en todo caso,

$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) < (a \vee b) \wedge (a \vee c) \wedge (b \vee c).$$

Veamos, en un retículo distributivo, la desigualdad inversa,

$$\begin{aligned}(a \vee b) \wedge (a \vee c) \wedge (b \vee c) &= [a \vee (b \wedge c)] \wedge [c \vee (a \wedge b)] < \\ &< [a \vee (b \wedge c) \vee (a \wedge b)] \wedge [c \vee (b \wedge c) \vee (a \wedge b)] < \\ &< (a \wedge c) \vee (b \wedge c) \vee (a \wedge b).\end{aligned}$$

Recíprocamente, se tiene

$$(a \vee b) \wedge c < (a \vee b) \wedge (a \vee c) \wedge (b \vee c) = \\ = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c) < a \vee (b \wedge c).$$

La distributividad se deduce, según el ejercicio precedente.

27

Si $a \in T$ pongamos $\varphi(a) = \{ x \in K \mid x < a \}$. Es claro que

$$\varphi(a \wedge b) = \varphi(a) \cap \varphi(b).$$

Se tiene también $\varphi(a \vee b) = \varphi(a) \cup \varphi(b)$ pues si $x \in K$ y $x < a \vee b$, entonces

$$x = x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b),$$

luego $x = x \wedge a < a$ ó $x = x \wedge b < b$.

Para demostrar que φ es inyectiva, basta mostrar que $a = \bigvee_{x \in \varphi(a)} x$, es decir, que todo elemento de T es cota superior de elementos de K. Si no fuese así, se podría considerar un elemento a minimal entre los que no fuesen cota superior de elementos de K. Entonces $a \notin K$, luego $a = g \vee h$, con $g < a$ y $h < a$. Necesariamente g y h son cotas superiores de elementos de K, de donde la contradicción.

28

Designemos por 0 el elemento mínimo y por 1 el elemento máximo. Se tiene

$$(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = 1 \wedge 1 = 1,$$
$$(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = 0 \vee 0 = 0.$$

Como el complemento de $a \vee b$ es único, $(a \vee b)' = a' \wedge b'$.

29

Si $a \wedge b' = 0$, tenemos

$$b = b \vee (a \wedge b') = (b \vee a) \wedge (b \vee b') = b \vee a > a.$$

Recíprocamente, si $a < b$, tenemos $a \wedge b' < b \wedge b' = 0$.

30

Vamos a utilizar el ejercicio precedente. Notaremos primero que

$$a \wedge b_i \leq a \wedge \left(\bigvee_i b_i\right) \text{ para todo } i.$$

Si $a \wedge b_i \leq x$ para todo i, entonces $a \wedge b_i \wedge x' = 0$, luego $b_i \leq (a \wedge x')'$. Por consiguiente

$$\bigvee_i b_i \leq (a \wedge x')', \quad \text{luego} \quad (\bigvee b_i) \wedge a \wedge x' = 0,$$

de donde, finalmente $a \wedge (\bigvee b_i) \leq x$. Esto demuestra que $a \wedge (\bigvee b_i)$ es la cota superior de los $a \wedge b_i$.

31

1.° Es evidente que todo ideal maximal es irreducible. Sea P primo, con $P = J \cap K$. Si $P \subset J$, sea $a \in J - P$. Para todo $b \in K$ es $a \wedge b \in P$, luego $b \in P$ y se tiene $P = K$. P es, pues, irreducible. Se ve muy fácilmente que la función característica de $T - P$ es un homomorfismo de T sobre el retículo $\{0, 1\}$. Entonces es P la imagen recíproca de 0. Es, pues, una clase, para la congruencia asociada a este homomorfismo.

2.° Sea I irreducible en T distributivo. Supongamos $a \wedge b \in I$. Si

$$x \in (I \overset{\leq}{\nabla} a) \cap (I \overset{\leq}{\vee} b),$$

se tiene $x \leq i \nabla a$ y $x \leq j \vee b$, con $i, j \in I$. Entonces,

$$x \leq [(i \vee j) \vee a] \wedge [(i \nabla j) \vee b] = (i \vee j) \vee (a \wedge b) \in I,$$

luego $x \in I$. De $I = (I \overset{\leq}{\vee} a) \cap (I \overset{\leq}{\vee} b)$ resulta $I = I \overset{\leq}{\vee} a$ ó $I = I \overset{\leq}{\vee} b$, es decir, $a \in I$ ó $b \in I$.

3.° Inversamente, los ideales forman una familia de Moore $\cup$-inductiva, luego todo ideal I es intersección de ideales irreducibles. Aquí tenemos $I = \bigcap_{i \in \Lambda} P_i$ con P_i primo. Sea θ_i la congruencia correspondiente a P_i. Entonces, I es una clase para la congruencia θ definida por $x \equiv y(\theta) \Leftrightarrow \forall_i \; x \equiv y(\theta_i)$. En particular, el ideal $\overset{\leq}{a}$ es clase para una congruencia θ.

Si $x \wedge y \leqslant a$, entonces, $x \wedge y \equiv a(\theta)$. Tomando en los dos miembros la $\vee$ con x, es $x \equiv a \vee x(\theta)$ y, lo mismo, $y \equiv a \vee y$. Por consiguiente,

$$a \equiv x \wedge y \equiv (a \vee x) \wedge (a \vee y), \text{ luego } (a \vee x) \wedge (a \vee y) \leqslant a$$

y como la desigualdad inversa es siempre cierta, $a = (a \vee x) \wedge (a \vee y)$.

Resulta que T es distributivo:

$$t \wedge u \leqslant s \vee (t \wedge u),$$

luego

$$\begin{aligned} s \vee (t \wedge u) &= [s \vee (t \wedge u) \vee t] \wedge [s \vee (t \wedge u) \vee u], \\ &= (s \vee t) \wedge (s \vee u). \end{aligned}$$

4.° Sean P primo, $a \notin P$ y $x \in T$. Sea a' el complemento (único) de a. $a \wedge a' = 0 \in P$ y $a \notin P$, luego $a' \in P$.

$$x = x \wedge (a \vee a') = (x \wedge a) \vee (x \wedge a') \in \overset{\leqslant}{a} \vee P.$$

Luego $T = \overset{\leqslant}{a} \vee P$. P es, efectivamente, maximal.

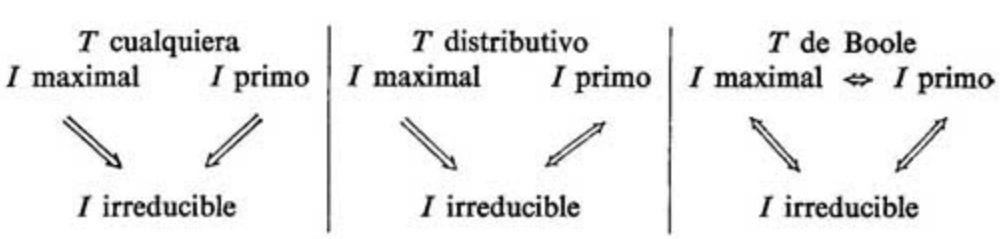
5.° Consideremos $E^* = \{ c \wedge d \mid d \vee c = 1 \}$, con el elemento c fijado. Este conjunto E^* es estable para la intersección: si $d \quad c = 1$ y $d' \quad c = 1$ se tiene

$$(d \wedge d') \vee c = (d \vee c) \wedge (d' \vee c) = 1, \quad \text{luego} \quad c \wedge d \wedge d' \in E^*.$$

Además, $0 \notin E^*$, puesto que c no tiene complemento. Sea P un ideal maximal entre los I que verifican $I \cap E^* = \varnothing$. P es irreducible, pues $P = X \cap Y$ con $P \subset X$ y $P \subset Y$ implicaría $X \cap E^* \neq \varnothing$ y $Y \cap E^* \neq \varnothing$, luego, tomando $x \in X \cap E^*$ e $y \in Y \cap E^*$ se tendría $x \wedge y \in P \cap E^*$. Luego P es primo. No es maximal:

se tiene $P \subset P \vee \overset{\leqslant}{c}$ pues $c \notin P$ y $1 \notin P \vee \overset{\leqslant}{c}$, si no $1 = p \vee c$, con $p \in P$ de donde $p \wedge c \in E^* \cap P$.

Finalmente, obtenemos las configuraciones siguientes, que son características:



32

1.° $a \wedge x = 0$ es equivalente a $x \leq a'$. De $a' \wedge a = 0$ resulta, pues, $a \leq a''$.

Si $a \leq b$ se tiene $b \wedge b' = 0$, luego $a \wedge b' = 0$, $b' \leq a'$.

Por consiguiente, $a \leq b$ implica $a'' \leq b''$.

De $a \leq a''$ resulta $(a'')' \leq a'$. Pero, por otra parte, $a' \leq (a')''$, luego $a' = a'''$. Resulta $a'''' = a''$.

2.° Mostremos que $a' \wedge b' = (a \vee b)'$.

Ante todo $a \leq a \vee b$, luego $(a \vee b)' \leq a'$. Lo mismo, $(a \vee b)' \leq b'$, luego $(a \vee b)' \leq a' \wedge b'$. Se tiene

$$(a' \wedge b') \wedge (a \vee b) = (a' \wedge b' \wedge a) \vee (a' \wedge b' \wedge b) = 0 \vee 0 = 0,$$

de donde $a' \wedge b' \leq (a \vee b)'$, con lo que resulta la igualdad.

Esto muestra que $a' \wedge b' \in A$, luego es necesariamente $\inf(a', b')$.

Mostremos que $\sup(a', b') = (a \wedge b)'$. Se tiene $a \wedge b \leq a$, luego

$$a' \leq (a \wedge b)'$$

y, lo mismo, $b' \leq (a \wedge b)'$.

Si $a', b' \leq c'$, se puede escribir

$$(a \wedge b)' \wedge a \wedge b = 0, \quad (a \wedge b)' \wedge a \leq b' \leq c',$$

luego

$$(a \wedge b)' \wedge a \wedge c = 0, \quad (a \wedge b)' \wedge c \leq a' \leq c',$$

de donde $(a \wedge b)' \wedge c = 0$ y finalmente $(a \wedge b)' \leq c'$.

La fórmula $\sup(a', b') = (a' \vee b')''$ es inmediata.

3.° Se deduce:

$$(a \wedge b)'' = [\sup(a', b')]' = [(a' \vee b')'']' = (a' \vee b')' = a'' \wedge b'',$$
$$\sup(a'', b'') = (a' \wedge b')' = (a \vee b)''.$$

La aplicación $a \to a''$ es, pues, un homomorfismo de T sobre A. Resulta que A es distributivo. Además, $a' \wedge a'' = 0$, es decir,

$$\inf(a', a'') = 0 \text{ y } \sup(a', a'') = (a \wedge a')' = 0' = 1.$$

Por consiguiente A es un retículo de Boole.

4.° Se tiene:

$$a' = \sup(a', u') = (a \wedge u)' = (b \wedge u)' = \sup(b', u') = b'.$$

Inversamente, si tomamos $u = (a' \wedge b') \vee (a \wedge b)$ resulta:

$$u' = (a' \wedge b')' \wedge (a \wedge b)' = (a' \wedge b')' \wedge \sup(a', b').$$

Si $a' = b'$ se obtiene $u' = a'' \wedge a' = 0$. Además

$$a \wedge u = a \wedge [(a' \wedge b') \vee (a \wedge b)] = (a \wedge a' \wedge b') \vee (a \wedge b) = a \wedge b,$$
$$b \wedge u = b \wedge [(a' \wedge b') \vee (a \wedge b)] = (b \wedge a' \wedge b') \vee (a \wedge b) = a \wedge b.$$

5.° Sea E un espacio topológico y sea U un abierto. Para que un abierto V tenga con U una intersección vacía, es necesario y suficiente que esté contenido en el complementario de U, es decir, contenido en el interior de ese complementario. Es, pues, U' el interior de $E - U$. Como T es estable para la reunión infinita, toda parte de A admite una cota superior:

$$\sup V_i' = (\bigcup V_i')''.$$

Como A es un álgebra de Boole se deduce, por dualidad, que toda parte admite una cota inferior, dada por la fórmula

$$\inf_i V_i' = (\sup V_i'')' = (\bigcup V_i'')''' = (\bigcup V_i'')'.$$

33

Sea $\exists$ un cuantificador. Se tiene $p < \exists p$. Si $p < q$ resulta que $p < \exists q$, luego

$$\exists p = \exists(p \wedge \exists q) = \exists p \wedge \exists q,\ \exists p < \exists q.$$

Por tanto

$$\exists\exists q = \exists(\exists q \wedge \exists q) = \exists\exists q \wedge \exists q = \exists q.$$

Es, pues, $\exists$ una clausura de Moore.

2.° Sea $\exists$ una clausura de Moore que deja 0 invariante. Si $\exists A$ es una subálgebra, ésta es estable para la complementación, es decir que $\exists(\exists p)' = (\exists p)'$, cualquiera sea p.

Recíprocamente, si es estable para la complementación, es también estable para $\vee$, pues $p \vee q = (p' \wedge q')'$, y es una subálgebra. En estas condiciones se tiene:

$$\exists p \vee \exists q = \exists(\exists p \vee \exists q) = \exists(p \vee q).$$

Demostremos que $\exists$ es un cuantificador. Para ello basta probar que

$$\exists(p \wedge \exists q) = \exists p \wedge \exists q$$

y para esto vamos a demostrar que $\exists(p \wedge \exists q)$ admite $(\exists p \wedge \exists q)'$ por complemento:

$$\begin{aligned}
\exists(p \wedge \exists q) \wedge (\exists p \wedge \exists q)' &\leqslant (\exists p \wedge \exists\exists q) \wedge (\exists p \wedge \exists q)' = 0 \\
\exists(p \wedge \exists q) \vee (\exists p \wedge \exists q)' &= \exists(p \wedge \exists q) \vee [(\exists p)' \vee (\exists q)'] \\
&= \exists(p \wedge \exists q) \vee \exists(\exists p)' \vee \exists(\exists q)' \\
&= \exists[(p \wedge \exists q) \vee (\exists p)' \vee (\exists q)'] \\
&= \exists[(p \vee (\exists p)' \vee (\exists q)') \wedge (\exists q \vee (\exists p)' \vee (\exists q)')] \\
&= \exists[p \vee (\exists p)' \vee (\exists q)'] \\
&= \exists p \vee \exists(\exists p)' \vee \exists(\exists q)' \\
&= \exists p \vee (\exists p)' \vee (\exists q)' \\
&= 1.
\end{aligned}$$

Recíprocamente: supongamos que $\exists$ sea un cuantificador. Tenemos

$$\exists(\exists p)' \vee \exists p \geqslant (\exists p)' \vee \exists p = 1.$$

Luego, $\exists(\exists p)' \vee \exists p = 1$. Además

$$\exists(\exists p)' \wedge \exists p = \exists((\exists p)' \wedge \exists p) = \exists 0 = 0.$$

Por consiguiente, $\exists(\exists p)' = (\exists p)'$.

3.° Es inmediato que $\exists a$ es mínimo en $\exists A \cap \overset{\leqslant}{a}$. Recíprocamente, sea B una subálgebra relativa completa. La aplicación $a \to \inf B \cap \overset{\leqslant}{a}$ es una clausura de Moore que deja 0 invariante y que admite B por imagen. Según el punto 2.° será un cuantificador.

4.° Sea D la subálgebra de C formada por las funciones constantes. Sea $f \in C$. La aplicación $\exists f \in C$ definida por $\exists f(x) = \vee f(X)$ para $x \in X$, es mínimo entre las aplicaciones constantes superiores a f. Por consiguiente D es relativamente completo y $\exists$ es un cuantificador.

34

1.° Se tiene $Ab = \{ ab \mid a \in A \} = \{ a \wedge b \mid a \in A \} = \overset{\leqslant}{b}$. Luego $Ab = Ac$ si y sólo si $b = c$.

2.° Sea $\mathcal{P}$ primo y $x \notin \mathcal{P}$. Se tiene $x(1 - x) = x - x^2 = 0 \in \mathcal{P}$. Luego

$$1 - x \in \mathcal{P}, \quad 1 \in \mathcal{P} + Ax, \quad \mathcal{P} + Ax = A,$$

que muestra que $\mathcal{P}$ es maximal.

3.° Si I es un ideal, coincide con su radical. En efecto, $x^n \in I$ implica $x \in I$, puesto que $x = x^n$.

Si $b \neq c$ se tiene $Ab \neq Ac$ de donde, por ejemplo, $c \notin Ab$. Puesto que Ab coincide con su radical, es igual a la intersección de los ideales primos que lo contienen. Existe, pues, un ideal primo $\mathcal{P}$ tal que $Ab \subseteq \mathcal{P}$ y $c \notin \mathcal{P}$.

4.° Si A es nœtheriano, se tiene una descomposición de (0) en la forma

$$(0) = Q_1 \cap \ldots \cap Q_n,$$

donde Q_i es $\mathcal{P}_i$-primario. En efecto, aquí $Q_i = \mathcal{P}_i$. Luego

$$\mathcal{P}_1 \mathcal{P}_2 \ldots \mathcal{P}_n = (0).$$

Si $\mathcal{P}$ es un ideal primo cualquiera, contiene a este producto de ideales primos, luego contiene a uno de ellos, sea $\mathcal{P}_1$. Pero siendo $\mathcal{P}_1$ maximal, se tiene $\mathcal{P} = \mathcal{P}_1$. De donde la conclusión.

5.° Sea S el conjunto de los ideales primos. La aplicación φ de A en $\mathcal{P}(S)$ definida por

$$\varphi(a) = \{ \mathcal{P} \mid \mathcal{P} \in S, \quad a \notin \mathcal{P} \}$$

es inyectiva, según el punto 3.°. Si S es finito también lo será $\mathcal{P}(S)$ y por ende lo sera A.

6.° y 7.° Es suficiente mostrar que en este caso φ será un isomorfismo de A sobre $\mathcal{P}(S)$. Mostremos que es una aplicación suprayectiva.

Si $X \subseteq S$, sea $I = \bigcap_{\mathcal{P} \notin X} \mathcal{P}$. Se puede tomar un elemento a maximal en I. Si $x \in I$ se tiene $x \vee a = x + a + xa \subset I$, luego $x \vee a = a$, $x \leqslant a$. Por tanto a es máximo en I y en consecuencia $I = \overset{\leqslant}{a} = Aa$.

Si $a \notin \mathcal{P}'$, se tiene evidentemente $\mathcal{P}' \in X$.

Si $a \in \mathcal{P}'$, se tiene

$$\coprod_{\mathcal{Q} \notin X} \mathcal{P} \subseteq \bigcap_{\mathcal{Q} \notin X} \mathcal{P} \subseteq \mathcal{P}'$$

Luego existe $\mathcal{P} \notin X$ tal que $\mathcal{P} \subseteq \mathcal{P}'$. Pero $\mathcal{P}$ es maximal, luego $\mathcal{P}' = \mathcal{P}$, $\mathcal{P}' \notin X$.

Se tiene, pues, $\varphi(a) = X$. Además,

$$\mathcal{P} \in \varphi(a) \cup \varphi(b) \Leftrightarrow a \notin \mathcal{P} \quad \text{o} \quad b \notin \mathcal{P} \Leftrightarrow a \vee b \notin \mathcal{P} \Leftrightarrow \mathcal{P} \in \varphi(a \vee b),$$

$$\mathcal{P} \in \varphi(a) \cap \varphi(b) \Leftrightarrow a \notin \mathcal{P} \quad \text{y} \quad b \notin \mathcal{P} \Leftrightarrow a \wedge b \notin \mathcal{P} \Leftrightarrow \mathcal{P} \in \varphi(a \wedge b).$$

35

1.° Se tiene evidentemente $r < a$ para todo $r \in R(a)$. Si $r < b$ para todo $r \in R(a)$, mostremos que $a < b$. En caso contrario existiría un x tal que $0 < x < a$ y $x \wedge b = 0$. Sea $r \in R(x)$. Se tiene $r \in R(a)$, luego $r < b$, $r = r \wedge b = 0$, lo que es contradictorio. Luego $a = \bigvee_{r \in R(a)} r$. Por consiguiente, $R(a) = R(c)$ implica

$$a = \bigvee_{r \in R(a)} r = \bigvee_{r \in R(c)} r = c.$$

Por tanto, la aplicación $a \to R(a)$ es inyectiva. Es claro que

$$R(a \wedge b) = R(a) \cap R(b).$$

Si $r \in R(a \wedge b)$, se tiene,

$$r < a \vee b, \qquad r = r \wedge (a \vee b) = (r \wedge a) \vee (r \wedge b)$$

y como $r \wedge a$ y $r \wedge b$ no pueden ser ambos nulos, uno de ellos debe ser igual a r. Resulta que, ó $r \in R(a)$ ó $r \in R(b)$. Se tiene, pues,

$$R(a \vee b) = R(a) \cup R(b)$$

lo que acaba de probar que la aplicación es un isomorfismo.

2.° Supongamos $0 < u < a$. El conjunto $\{x \mid x < a,\ x \wedge u = 0\}$ admite un elemento maximal u'. Se tiene $u \wedge u' = 0$. Para que u' sea un complemento de u en a basta, pues, que $a < u \vee u'$. Si no fuese así, existiría un s tal que $0 < s < a$ y $s \wedge (u \vee u') = 0$. De esto se deduce $s \wedge u = 0$, luego

$$(u' \vee s) \wedge u = (u' \wedge u) \vee (s \wedge u) = 0.$$

Pero u' es maximal, luego $u' = u' \vee s$. Resulta así $s = s \wedge u' = 0$, que es contradictorio.

Es, pues, $\overset{\leqslant}{a}$ un álgebra de Boole que verifica la condición maximal, y por consiguiente finita (ejercicio II, 34). La propiedad β) resulta inmediatamente.

La propiedad α) es una consecuencia del ejercicio II, 24.

3.° Consideremos una sección $\overset{\leqslant}{a}$. Si T verifica α) y β) esta sección es un álgebra de Boole satisfaciendo a la condición minimal y por consiguiente finita (ejercicio II, 34). En particular, ella tiene elementos minimales, en número finito.

4.° Según la primera cuestión, la aplicación $a \to R(a)$ es un isomorfismo de T en el retículo de las partes finitas de R. En este retículo toda sección inicial es finita, luego, asimismo en T.

36

Un álgebra de Boole no es un grupo ordenado. En efecto, todo grupo ordenado que posee un elemento máximo t se reduce al elemento neutro, pues se tiene $e < t$, luego $t < t^2$ lo que da $t = t^2$ y finalmente $t = e$.

37

Se tiene

$$(a \vee e)^n = a^n \vee a^{n-1} \vee \ldots \vee e = a^{n-1} \vee \ldots \vee e = (a \vee e)^{n-1},$$

de donde $a \vee e = e$ y por consiguiente $a \geqslant e$. Si $a^n = e$ se tiene, pues, $a \geqslant e$. Pero también $(a^{-1})^n \geqslant e$, luego $a^{-1} \geqslant e$ y finalmente $a = e$. Luego, G es sin torsión. Se tiene $|d| \geqslant d$ y $|d| \geqslant d^{-1}$, luego $|d|^2 \geqslant dd^{-1} = e$, lo que da $|d| \geqslant e$.

38

Demostremos que lo 1.° implica lo 2.°.

Se tiene $y^{-1}x < z$ e $y^{-1}x < x$. Por otra parte, $e < z$ y $e < x$. Se puede, pues, encontrar z' tal que $y^{-1}x < z' < z$ y $e < z' < x$. Tomemos $y' = x(z')^{-1}$. Se tiene $x = y'z'$ y $e < z' < z$. Además, $e < y'$, pues $z' < x$, e $y' < y$, pues

$$y^{-1}y' = y^{-1}x(z')^{-1} < e.$$

Recíprocamente, demostremos que lo 2.° implica lo 1.°.

Por una traslación conveniente nos podemos referir al caso en que $a = e$. Supongamos, pues, que e y b son inferiores a c y d. Se tiene $e < b^{-1}c < b^{-1}dc$, con $e < b^{-1}d$ y $e < c$; luego $b^{-1}c$ se puede escribir $b^{-1}c = uv$, con $e < u < b^{-1}d$ y $e < v < c$. Tenemos $b < bu < buv = c$. Además, $e = cc^{-1} < cv^{-1} = bu < d$, luego bu es el elemento buscado.

39

1.° Se ve inmediatamente que $PP \subseteq P$ y $P \cap P^{-1} = \{e\}$.

Si $y \in P$, se tiene $xyx^{-1} > xex^{-1} = e$, $xyx^{-1} \in P$, luego, para todo $x \in G$, $xPx^{-1} \subseteq P$. Por consiguiente

$$P \subseteq x^{-1}Px = x^{-1}P(x^{-1})^{-1} \subseteq P,$$

de donde $x^{-1}Px = P$. Se ve que para todo x, $xP = Px$, y, para toda parte A de G, $PA = AP$.

2.° Si P verifica estas condiciones, se define el orden para $x < y$ si y sólo si $x^{-1}y \in P$. Mostremos que esto es efectivamente un orden.

— $x < x$ pues $x^{-1}x = e \in P$.

— $x < y$ e $y < x$ implica $x^{-1}y \in P$ y $(x^{-1}y)^{-1} = y^{-1}x \in P$, luego
$$x^{-1}y \in P \cap P^{-1}, \quad x^{-1}y = e, \quad x = y.$$

— si $x < y$ e $y < z$, se tiene $x^{-1}y \in P$, $y^{-1}z \in P$, de donde

$$x^{-1}z = x^{-1}yy^{-1}z \in PP \subseteq P, \quad x < z.$$

Esta relación hace de G un grupo ordenado:
Si $a < b$,

$$(xa)^{-1}xb = a^{-1}x^{-1}xb = a^{-1}b \in P,$$
$$(ax)^{-1}bx = x^{-1}a^{-1}bx \in x^{-1}Px \subseteq P.$$

Por consiguiente $xa < xb$ y $ax < bx$. Además, $x > e$ equivale a

$$x = e^{-1}x \in P.$$

3.° Supongamos G filtrante. Sea $x \in G$ cualquiera. Sea s un mayorante de x y de e. Se tiene

$$x = ss^{-1}x = s(x^{-1}s)^{-1}.$$

Pero $s \in P$ y $x^{-1}s \in P$, luego x pertenece al subgrupo engendrado por P.

De un modo general, el subgrupo engendrado por P es PP^{-1}. En efecto, $e \in P \subseteq PP^{-1}$. Se tiene

$$(PP^{-1})^{-1} = (P^{-1})^{-1} P^{-1} = PP^{-1} \quad \text{y} \quad (PP^{-1})(PP^{-1}) = PPP^{-1} P^{-1} \subseteq PP^{-1},$$

lo que demuestra que PP^{-1} es un subgrupo.

Supongamos $G = PP^{-1}$. Si $x, y \in G$ se tiene $x = ab^{-1}$ e $y = cd^{-1}$, con $a, b, c, d \in P$. Ocurre entonces,

$$x = xe \leqslant xb = a = ae \leqslant ac.$$

Así se ha visto que G es filtrante superiormente. Si m es un mayorante de x^{-1} e y^{-1}, será m^{-1} un minorante de x y de y. Luego G es también filtrante inferiormente.

40*

1.° $X \subseteq Y$ implica $M(Y) \subseteq M(X)$ y $m(Y) \subseteq m(X)$. Por otra parte, se tiene siempre $Y \subseteq m[M(Y)] = Y^*$ e $Y \subseteq Mm(Y)$.

De esto se deduce: $M(Y^*) \subseteq M(Y)$ y $M(Y) \subseteq Mm[M(Y)] = M(Y^*)$, luego $M(Y) = M(Y^*)$. Resulta,

$$Y^{**} = mM(Y^*) = mM(Y) = Y^*.$$

Si $X \subseteq Y$, tenemos

$$M(Y) \subseteq M(X), \quad X^* = mM(X) \subseteq mM(Y) = Y^*,$$

Y^* es, pues, una clausura de Moore en el conjunto de las partes de G. $\mathcal{R}$ es estable para esta clausura, pues $Y \in \mathcal{R}$ implica $M(Y^*) = M(Y) \neq \varnothing$, luego $Y^* \in \mathcal{R}$.

2.° Si $A \subseteq A_i$ para todo $i \in I$ con A y A_i elementos de $\mathcal{G}$, entonces $\bigcap A_i$ es no vacío y evidentemente mayorado. Se tiene, pues, $\bigcap_i A_i \in \mathcal{R}$. Como $(\bigcap_i A_i)^* = \bigcap_i A_i$, efectivamente es $\bigcap_i A_i \in \mathcal{G}$ y es la cota inferior de las A_i.

Si $A_i \subseteq A$ para todo i, se tiene $\bigcup_i A_i \subseteq A$, luego $\bigcup A_i$ es mayorado. Es un elemento de $\mathcal{R}$. Su clausura $(\bigcup A_i)^* \in \mathcal{G}$ es entonces la cota superior de las A_i.

Tomemos $A, B \in \mathcal{G}$. Sean $a' \in M(A)$, $b' \in M(B)$. Entonces A y B están contenidos en $(a' \vee b')^* \in \mathcal{G}$, luego su cota superior existe. Se demuestra análogamente la existencia de cota inferior de A y B.

3.° Se tiene $a^* = \overset{\leqslant}{a}$, luego $a^* = b^*$ implica $a = b$.
Igualmente resulta

$$\left(\bigwedge_i a_i\right)^* = (\overset{\leqslant}{\bigwedge} a_i) = \bigcap_i \overset{\leqslant}{a_i} = \bigcap a_i^* = \bigwedge a_i^*.$$

$a_i \leqslant \bigvee_i a_i$ implica $a_i^* \subseteq (\bigvee a_i)^*$. Supongamos que se tenga $a_i^* \subseteq A \in \mathcal{G}$ para todo i. Si x es mayorante de A, $a_i \leqslant x$, pues $a_i \in A$. Por consiguiente $\bigvee a_i \leqslant x$. Se tiene, pues

$$\bigvee_i a_i \in mM(A) = A.$$

Luego $(\bigvee a_i)^* \subseteq A$. Esto muestra que $(\bigvee a_i)^* = \bigvee a_i^*$.

4.° Sea $a \in M(XY)$ con $X,\ Y \in \mathcal{R}$. Si $y \in Y$ se tiene $a \geqslant xy$ para todo $x \in X$, luego $ay^{-1} \geqslant x$ y recíprocamente. Se tiene, pues,

$$a \in M(XY) \Leftrightarrow aY^{-1} \subseteq M(X).$$

Se deduce:

$$a \in M(XY) \Leftrightarrow aY^{-1} \subseteq M(X^*) \Leftrightarrow a \in M(X^* Y),$$

de donde

$$(XY)^* = mM(XY) = mM(X^* Y) = (X^* Y)^*.$$

Un razonamiento análogo daría $(XY)^* = (XY^*)^*$. Combinando ambos resultados se obtiene

$$(XY)^* = (X^* Y^*)^* = X^* \circ Y^*.$$

Ahora bien, $\mathcal{R}$ es un semigrupo para la multiplicación de los complejos. La fórmula anterior muestra que $Y \to Y^*$ es compatible con las leyes multiplicativas de $\mathcal{R}$ y $\mathcal{G}$. Este último es, pues, un semigrupo. Se deduce así, para $A,\ B,\ C \in \mathcal{G}$:

$$\begin{aligned} A \circ (B \vee C) &= A^* \circ (B \cup C)^* = [A(B \cup C)]^* = (AB \cup AC)^* \\ &= [(AB)^* \cup (AC)^*]^* = (AB)^* \vee (AC)^* = (A^* \circ B^*) \vee (A^* \circ C^*) \\ &= (A \circ B) \vee (A \circ C). \end{aligned}$$

5.° Se tiene $A^{-1} \subseteq MmA^{-1} = M(B)$, luego $B^* = mM(B) = m(A^{-1}) = B$, de donde $B = B^* \in \mathcal{G}$. De otra parte $B^{-1} = M(A)$, luego

$$x \in M(AB) \quad \Leftrightarrow \quad xB^{-1} \subseteq M(A) \quad \Leftrightarrow \quad xM(A) \subseteq M(A).$$

Si $y \in M(AB)$, se tiene $xyM(A) \subseteq xM(A) \subseteq M(A)$; luego $xy \in M(AB)$. Es claro que $c \in M(AB)$ luego todo elemento positivo está en $M(AB)$.

6.° Sea $c \in AB$. Si $b \in M(AB)$, para todo n, $b^n \in M(AB)$, luego $b^n > c$. Resulta $b \geqslant e$. Se tiene pues

$$M(AB) = P, \quad A \circ B = (AB)^* = mM(AB) = P^{-1} = e^*.$$

Ahora, e^* es elemento neutro de $\mathcal{G}$. Todo elemento de $\mathcal{G}$ tiene, pues, un inverso y por consiguiente $\mathcal{G}$ es un grupo reticulado.

7.° Si $b^n \geqslant c$ para todo $n > 0$, entonces $f = \bigwedge_{n>0} b^n$ existe. Se tiene

$$bf = \bigwedge_{n>1} b^n \geqslant f,$$

de donde $b \geqslant e$.

CAPÍTULO III

Grupos. Teoría elemental

Salvo mención expresa de lo contrario, un grupo será indicado con notación multiplicativa y e designará su elemento neutro.

Enunciados

1

Se considera un conjunto S en el que se da una ley de composición interna $(a, b) \to ab$, verificando, cualesquiera sean a, b, c:

$$a^2 = b^2,$$
$$ab^2 = a,$$
$$a^2(bc) = cb,$$
$$(ac)(bc) = ab.$$

Demostrar que S es un grupo con la operación

$$a \top b = a(b^2 b).$$

Enunciar y demostrar la proposición recíproca.

2

Designamos por $G(\top)$ un conjunto G con una ley de composición interna denotada $\top$. El conjunto G es finito.

1.° Supongamos que $G(\top)$ sea un casigrupo (todo elemento es regular) y que satisface a la condición A) siguiente:

A) Cualesquiera sean a, b, g, existe un elemento c, independiente de g, tal que

$$a \top (b \top g) = c \top g.$$

Demostrar que asociando al par (a, b) la solución c de esa ecuación, y poniendo $a \circ b = c$, se le da a G una ley de grupo. Deducir que $G(\top)$ posee un elemento neutro a la izquierda, designado por e.

2.° Sea Γ el conjunto de traslaciones a la izquierda de $G(\top)$. Dar una condición necesaria y suficiente, referida a Γ, para que el casigrupo $G(\top)$ verifique A). Mostrar que entonces Γ es isomorfo a $G(\circ)$.

3.° Sea $G(\top)$ un casi grupo satisfaciendo A). Sea φ la aplicación de G en G definida por $\varphi(x) = x \top e$. Se pone, $\psi = \varphi^{-1}$ y se define en G la ley de composición

$$x \perp y = \psi(x) \top y.$$

Demostrar que $G(\perp)$ es isomorfo a $G(\circ)$.

3

Demostrar que un grupo no puede ser la unión de dos subgrupos propios.

4

Sea G un grupo. Se supone que existe un entero k tal, que cualesquiera sean a y b en G se tienen las relaciones

$$(ab)^i = a^i b^i \quad \text{para} \quad i \in \{k - 1, k, k + 1\}.$$

Demostrar que G es abeliano.

5

Sean a y b dos elementos de un grupo G cumpliendo

$$a^5 = e, \quad b^4 = e, \quad ab = ba^3.$$

Demostrar que se tiene

$$a^2 b = ba, \quad ab^3 = b^3 a^2.$$

6

Si en G, a y b cumplen las condiciones

$$b^6 = e, \quad ab = b^4 a,$$

demostrar que se tiene $b^3 = e$ y $ab = ba$.

7

Si H y K son dos subgrupos finitos de un grupo G, demostrar la relación

$$\text{Card } (HK) = \frac{\text{Card } (H)\text{Card } (K)}{\text{Card } (H \cap K)}.$$

8

Se considera el conjunto $\mathcal{A}$ de las aplicaciones afines de $\mathbf{R}$, es decir, las aplicaciones $x \to ax + b$, $a \in \mathbf{R}^*$, $b \in \mathbf{R}$. Demostrar que $\mathcal{A}$ es un grupo para la composición de las aplicaciones. Sea $\mathcal{H}$ el conjunto de las aplicaciones $x \to x + b$. Demostrar que $\mathcal{H}$ es un subgrupo distinguido de $\mathcal{A}$ y que $\mathcal{A}/\mathcal{H}$ es isomorfo a $\mathbf{R}^*$.

9

Demostrar que si todos los elementos de un grupo G verifican: $x^2 = e$, entonces G es abeliano. Además, si G es finito su orden es una potencia de 2.

10

Sea D un semigrupo y sea $a \in D$. Se considera el conjunto

$$S = \{ a, a^2, \ldots, a^n, \ldots \}.$$

Demostrar que si S es finito, existen dos enteros m y n, $m < n$, tales que $a^m = a^n$.

Elegido n mínimo en la relación precedente, demostrar que se tiene

$$S = \{ a, a^2, \ldots, a^{n-1} \},$$

y que el conjunto

$$C = \{ a^m, \ldots, a^{n-1} \}$$

es un grupo cíclico.

11

Demostrar que un subgrupo de índice 2 es distinguido.

12

Sea H un subgrupo de un grupo G. Se supone que el producto de dos clases a la izquierda cualesquiera según H, es una clase a la izquierda. Demostrar que H es distinguido en G.

13

Si un elemento a de un grupo G tiene exactamente dos conjugados, entonces G admite un subgrupo distinguido propio.

14

Sea G un grupo monógeno. Demostrar que todo subgrupo de G es invariante para los automorfismos de G.

Deducir que si G es un subgrupo monógeno distinguido en un grupo N, todo subgrupo de G es distinguido en N.

15

Supongamos que existe un entero n tal que la aplicación $x \to x^n$ sea un automorfismo del grupo G. Demostrar que para todo $x \in G$, x^{n-1} pertenece al centro de G.

16

Sea N un subgrupo distinguido de un grupo G. Si $a \in G$ es de orden finito n, demostrar que el menor entero k tal que $a^k \in N$, es divisor de n.

17

Sean a y b dos elementos de un grupo G cumpliendo $ab = ba$. Si a es de orden m, b es de orden n, y si m y n son primos entre sí, demostrar que ab es de orden mn.

18

Sean a y b dos elementos de un grupo G cumpliendo

$$ab = ba \text{ y } (a) \cap (b) = \{e\}.$$

Demostrar que ab es de orden finito si y sólo si a y b son de orden finito, y que el orden de ab es el m.c.m. de los órdenes de a y b.

19

Sea N un subgrupo distinguido de un grupo G. Se supone que el índice de N en G es finito e igual a n. Demostrar que si m es primo con n, la relación $x^m = e$ implica $x \in N$.

20

Sea G un grupo abeliano de orden n. Si k es un entero primo con n, demostrar que cualquiera sea $a \in G$, la ecuación $x^k = a$ admite una solución única en G. (Demostrar que la aplicación $x \to x^k$ es un automorfismo de G.)

Dar otra demostración válida cuando G no sea abeliano.

21

Sean G un grupo abeliano y H un subgrupo de G tal que G/H sea un grupo monógeno infinito. Demostrar que G es isomorfo al grupo-producto $H \times G/H$.

22

Supongamos que en un grupo G se cumple para un entero n

$$(ab)^n = a^n b^n$$

cualesquiera sean a y b. Demostrar que $G^n = \{x^n;\ x \in G\}$ y $G_n = \{x;\ x \in G,\ x^n = e\}$ son subgrupos distinguidos de G. Si G es finito, el orden de G^n es igual al índice de G_n.

23

1.° Sea G un grupo. Demostrar que el conjunto de los enteros relativos k tales que se tenga $x^k = e$, $\forall x \in G$, es un subgrupo $n\mathbf{Z}$ de $\mathbf{Z}$. Demostrar que n es distinto de cero si y sólo si los órdenes de los diferentes elementos de G son finitos y no toman más que un número finito de valores distintos; entonces n es su m.c.d. El entero n se llama exponente de G.

2.° Si G es de exponente $n > 0$, y es $n = mp^{\alpha}$, p primo, $p \nmid m$, demostrar que G tiene algún elemento de orden p^{α}.

Si, además, G es abeliano, tiene algún elemento de orden n.

24

Sea G un grupo cíclico de orden n, denotado aditivamente. Demostrar que el conjunto End (G) de los endomorfismos de G puede tomar una estructura de anillo isomorfo a $\mathbf{Z}/(n)$.

¿Qué puede decirse cuando G sea monógeno infinito?

25

Demostrar que un grupo finito G en el que la ecuación $x^p = e$ admite (cualquiera sea p) a lo más p soluciones, es cíclico. (Si G es de orden n se puede hacer ver que, cualquiera sea p, G no contiene más elementos de orden p que $\mathbf{Z}/(n)$.)

26

Sea H un subgrupo distinguido de un grupo G. Se supone que el orden n de H es primo con el índice m de H en G. Demostrar que H es el único subgrupo de orden n de G.

27

Sea G un grupo cíclico de orden n. Demostrar que el retículo de los subgrupos de G es isomorfo al conjunto de los divisores positivos de n ordenados por la divisibilidad.

Dar una representación análoga del retículo de los subgrupos de un grupo monógeno infinito.

28

Sea G un grupo abeliano. Un subgrupo A de G se dice denso si se tiene $A \cap H \neq \{e\}$ para todo subgrupo $H \neq \{e\}$ de G.

Demostrar que para que un subgrupo A de G sea denso, es necesario y suficiente que

a) G/A sea un grupo con torsión,

b) todo elemento de orden primo de G pertenece a A.

29

Un subgrupo N de un grupo G se dice casi-distinguido si es permutable con todo subgrupo de G.

Demostrar que:

a) Todo subgrupo conjugado de un subgrupo casi-distinguido es casi-distinguido.

b) Un subgrupo casi-distinguido maximal (en el conjunto de los subgrupos casi-distinguidos propios) es distinguido.

30

Sean un grupo G y $\{G_i\}_{i \in I}$ la familia de los subgrupos propios maximales, supuesta no vacía. Pongamos $\Phi = \bigcap_{i \in I} G_i$.

1.° Sea Φ^* el conjunto de elementos x de G tales que para todo sistema generador M de G que contiene a x, también $M - \{x\}$ sea un sistema generador de G. Demostrar que $\Phi^* = \Phi$.

2.° Demostrar que Φ es un subgrupo distinguido de G. Demostrar que los G_i son distinguidos en G si y sólo si Φ contiene el grupo conmutador de G.

31

Sea A una parte no vacía de un grupo G. Se llama normalizador de A el conjunto N de los $x \in G$ tales que $xAx^{-1} = A$. Se llama centralizador de A el conjunto K de los $x \in G$ tales que $xax^{-1} = a$, $\forall a \in A$. Demostrar que N es un subgrupo de G, K un subgrupo distinguido de N. Si A es un subgrupo, N es el mayor subgrupo de G en el cual es distinguido A.

32

Sean Φ el grupo de los automorfismos de un grupo G, A el grupo de los automorfismos internos de G. Demostrar que A es un subgrupo distinguido de Φ. Demostrar que si el centro de G se reduce al elemento neutro, lo mismo sucede con el centralizador (ejercicio III, 31) de A en Φ.

33

Sean G un grupo, $S(G)$ el grupo de biyecciones de G sobre G, Γ (respectivamente, Δ) el grupo de traslaciones a la izquierda (respect., a la dere-

cha) de G. G es isomorfo a Γ. Se indicará por γ_a la traslación a la izquierda definida por $a \in G$.

1.° Mostrar que el grupo Φ de los automorfismos de G es un subgrupo del normalizador Ω de Γ en $S(G)$.

Mostrar que todo automorfismo de Γ es de la forma

$$\gamma_a \to \varphi \circ \gamma_a \circ \varphi^{-1}, \quad \text{donde} \quad \varphi \in \Phi.$$

2.° Mostrar que Δ es el centralizador de Γ en $S(G)$ (ejercicio III, 31).

Deducir que $\Gamma\Delta = \Delta\Gamma$ es un subgrupo de Ω.

Mostrar que $\Gamma \cap \Delta$ es el centro de Γ.

3.° Sea A el grupo de los automorfismos internos de G. Demostrar que se tiene

$$\Gamma\Delta = A\Gamma = \Gamma A.$$

Deducir que : $\Omega = \Phi\Gamma = \Gamma\Phi$ y que $\Phi \cap \Gamma$ se reduce al elemento neutro.

34

Sean G un grupo y H un subgrupo distinguido de G. Sean, A el grupo de automorfismos de H, N el grupo de automorfismos internos de H, $K = \{ x;\ x \in G,\ xh = hx,\ \forall h \in H \}$.

1.° Demostrar que HK y N son subgrupos distinguidos de G y de A, y que existe un isomorfismo de G/HK sobre un subgrupo de A/N.

2.° Demostrar que HK/K es isomorfo a N.

3.° Se supone que H tiene sólo automorfismos internos y que su centro se reduce a $\{ e \}$. Demostrar que G es producto directo de H y K.

35

Recordaremos que un grupo es sin torsión cuando cada uno de sus elementos, excepto e, es de orden infinito.

1.° Sea G un grupo. Un subgrupo H de G se dice aislado si la relación $x^n \in H$, donde $x \in G$ y $n \in \mathbf{Z}$, $n \neq 0$, implica $x \in H$.

a) Demostrar que los subgrupos aislados de G forman una familia de Moore.

b) Sea H un subgrupo distinguido de G. Demostrar que H es aislado si y sólo si G/H es sin torsión.

2.° Se dice que G es un R-grupo si la relación $x^n = y^n$, $n \in \mathbf{Z}$, $n \neq 0$, implica $x = y$.

a) Demostrar que un R-grupo es sin torsión, y que un grupo abeliano sin torsión es un R-grupo.

b) Demostrar que el centralizador (ejercicio III, 31) de una parte M de un R-grupo es un subgrupo aislado. Deducir que el centro de un R-grupo es un subgrupo aislado y que la relación $x^k y^n = y^n x^k$, implica $xy = yx$.

c) Demostrar que G es un R-grupo si y sólo si el centro Z de G y el grupo cociente G/Z son R-grupos.

36

1.° Sea G un grupo del que A y B son subgrupos. Diremos que G es producto semidirecto de A y B si se satisfacen las tres condiciones siguientes:

a) $G = AB$,
b) $A \cap B = \{e\}$,
c) A es distinguido en G.

Demostrar que existe entonces un homomorfismo $b \to \varphi(b) = b$ de B en el grupo de automorfismos de A, tal, que se tiene

$$ba = \tilde{b}(a)b, \quad \text{para todo } a \in A \quad \text{y todo } b \in B.$$

Demostrar que B es isomorfo a G/A.

2.° Sean A y B dos grupos. Suponemos que existe un homomorfismo $b \to \varphi(b) = \tilde{b}$ de B en el grupo de automorfismos de A. Demostrar que el conjunto producto $A \times B$ con la ley de composición interna

$$(a, b)(a', b') = (a\tilde{b}(a'), bb')$$

es un grupo. Mostrar que este grupo es producto semidirecto de dos subgrupos A' y B' isomorfos respectivamente a A y B.

3.° Dar un ejemplo de grupo que sea producto semidirecto de dos subgrupos sin ser su producto directo.

37*

Sean G un grupo finito, N un subgrupo distinguido minimal de G. Demostrar que N es producto directo de subgrupos simples isomorfos entre ellos.

38*

Designamos por $\mathbf{Q}$ el cuerpo de los racionales y por $\mathbf{Z}$ el anillo de los enteros relativos. Sea U el grupo aditivo $\mathbf{Q}/\mathbf{Z}$. Siendo p un número primo se considera el subgrupo U_p de U constituido por los elementos cuyo orden es una potencia de p.

1.° Demostrar que cualesquiera sean $\alpha \in U_p$ y $n \in \mathbf{Z}$, $n \neq 0$, existe $\beta \in U_p$ tal que $\alpha = n\beta$.

2.° Demostrar que todo subgrupo de U_p, distinto de U_p, es cíclico. ¿Cómo es el retículo de los subgrupos de U_p?

3.° Sea G un grupo abeliano que tiene una sucesión creciente de subgrupos

$$G_0 \subset G_1 \subset \cdots \subset G_n \subset \cdots$$

tales que:

a) G_n es cíclico de orden p^n.

b) $G = \bigcup_{n \geqslant 0} G_n$.

Demostrar que existe una sucesión $(x_n)_{n \geqslant 0}$ de elementos de G donde x_n engendra G_n y $x_n = px_{n+1}$, $\forall n > 0$. Deducir que G es isomorfo a U_p.

4.° Sea P el conjunto de los números primos $p > 1$ (*). Demostrar que todo $\alpha \in U$ se escribe de modo único como suma de elementos pertenecientes a ciertos grupos U_p. Deducir un isomorfismo de U sobre un subgrupo del grupo producto $\prod_{p \in P} U_p$.

39

Sea G un grupo. Al escribir sg d queremos indicar subgrupo distinguido.

1.° *a*) Se denota por (a) el sg d engendrado por $a \in G$. ¿Cuáles son los elementos de (a)?

(*) El número 1 no se considera primo (ni compuesto). *N. del T.*

b) Si A y B son dos sg d de G, indicaremos por $[A, B]$ el subgrupo de G engendrado por los conmutadores

$$[a, b] = aba^{-1}b^{-1} \qquad a \in A, \qquad b \in B.$$

Demostrar que $[A, B]$ es un sg d de G contenido en $A \cap B$. Si A_1 y A_2 son dos sg d de G demostrar la relación

$$[A_1 A_2, B] = [A_1, B]\,[A_2, B].$$

2.° *a*) Se dice que un sg d P de G es primo si la relación $[(a), (b)] \subseteq P$ implica $a \in P$ ó $b \in P$. Demostrar que un sg d P es primo si y sólo si la relación $[A, B] \subseteq P$, donde A y B son ambos sg d, implica $A \subseteq P$ ó $B \subseteq P$. Deducir que si los A_i, $1 \leqslant i \leqslant n$ son sg d, la intersección $A_1 \cap \cdots \cap A_n$ está contenida en P si y sólo si uno de los A_i está contenido en P.

b) Un subconjunto M de G se llama m-sistema si, cualesquiera que sean m_1 y m_2 en M, existen $m_1' \in (m_1)$ tales que $[m_1', m_2'] \in M$. El conjunto vacío se considera un m-sistema.

Demostrar que un sg d P es primo si y sólo si su complementario $G - P$ es un m-sistema.

3.° *a*) Sean A un sg d y M un m-sistema disjunto con A. Demostrar que M está contenido en un m-sistema M^* maximal en el conjunto de los m-sistemas disjuntos con A.

b) Con las mismas hipótesis, demostrar que A está contenido en un sg d P^* maximal en el conjunto de los sg d disjuntos con M. Demostrar, además, que P^* es primo.

c) Mostrar que un conjunto P de elementos de G es un sg d primo minimal que contiene a un sg d A si y sólo si $G - P$ es maximal en el conjunto de los m-sistemas disjuntos con A.

4.° Sea A un sg d de G. Se denota por $r(A)$ la intersección de todos los sg d primos que contienen a A. Demostrar que $r(A)$ es la intersección de los sg d primos minimales que contienen a A.

Si B es otro sg d de G demostrar:

$$r([A, B]) = r(A \cap B) = r(A) \cap r(B).$$

Demostrar que $r(A)$ es el conjunto de los $a \in G$ tales que todo m-sistema que contiene a a tiene intersección no vacía con A.

Soluciones

1

En S los cuadrados de todos los elementos son iguales. Sea e este elemento cuadrado único. La segunda igualdad se escribe: $ae = a$. La ley $\top$ se puede definir por

$$a \top b = a(eb).$$

Verifiquemos su asociatividad. Se tiene sucesivamente

$$\begin{aligned}
&(a \top b) \top c = [a(eb)]\,(ec),\\
&a \top (b \top c) = a[e\,\{\,b(ec)\,\}]\\
&\qquad = a[e^2\,\{\,b(ec)\,\}] && \text{porque } e = e^2\\
&\qquad = a[(ec)b] && \text{según la tercera fórmula}\\
&\qquad = [a(eb)]\,[\{\,(ec)b\,\}\,(eb)] && \text{según la cuarta}\\
&\qquad = [a(eb)]\,[(ec)e] && \text{según la cuarta}\\
&\qquad = [a(eb)]\,(ec) && \text{mediante } xe = x.
\end{aligned}$$

El elemento neutro es e:

$$\begin{aligned}
a \top e &= a(ee) = ae = a,\\
e \top a &= e(ea) = e^2(ea) = ae = a.
\end{aligned}$$

El inverso de a para $\top$ es ea:

$$\begin{aligned}
a \top (ea) &= a[e(ea)] = a[ae] = a^2 = e,\\
(ea) \top a &= (ea)\,(ea) = e
\end{aligned}$$

Recíprocamente, si S tiene una ley $\top$ que le haga un grupo, se puede poner

$$ab = a \top b^{-1}.$$

Se comprueban fácilmente las cuatro relaciones, y se tiene:

$$a \top b = a(b^2\,b).$$

2

1.° El elemento c que verifica $a \top (b \top g) = c \top g$ es único, puesto que $G(\top)$ es regular. La ley $\circ$ está, pues, definida sobre G, y se puede escribir:

$$a \top (b \top g) = (a \circ b) \top g, \quad \forall g \in G. \tag{1}$$

La ley $\circ$ es asociativa:

Utilizando la relación (1) obtenemos,

$$[(a \circ b) \circ c] \top g = (a \circ b) \top (c \top g) = a \top (b \top (c \top g)],$$
$$[a \circ (b \circ c)] \top g = a \top [(b \circ c) \top g] = a \top [b \top (c \top g)].$$

La asociatividad resulta de que $G(\top)$ es regular.

Para demostrar que $G(\circ)$ es un grupo, bastará, pues que G es finito, demostrar la regularidad de la ley $\circ$.

Si $a \circ b = a \circ c$, se tiene,

$$(a \circ b) \top g = (a \circ c) \top g,$$

o sea,

$$a \top (b \top g) = a \top (c \top g),$$

de donde $b \top g = c \top g$, luego $b = c$.

Si $a \circ b = c \circ b$, se tiene análogamente,

$$a \top (b \top g) = c \top (b \top g) \quad \text{y} \quad a = c.$$

Sea e el elemento neutro de $G(\circ)$. Cualesquiera sean a y g,

$$a \top (e \top g) = (a \circ e) \top g = a \top g,$$

de donde,

$$e \top g = g.$$

2.° Denotemos por γ_a la traslación a la izquierda definida por $a \in G(\top)$. El axioma A) equivale a lo siguiente:

Cualesquiera sean a y b existe c tal que $\gamma_a \circ \gamma_b = \gamma_c$. El axioma A) se verifica, pues, si y sólo si Γ es una parte estable del conjunto de las aplica-

ciones de G en G, con la composición de aplicaciones, que también indicaremos por $\circ$.

Nótese que la regularidad de $G(\top)$ implica que cada traslación a la izquierda es biyectiva, puesto que G es finito. Γ es una parte estable finita del grupo de biyecciones de G, luego es un subgrupo.

La relación

$$a \top (b \top g) = (a \circ b) \top g, \qquad \forall g \in G$$

se escribe entonces

$$\gamma_a \circ \gamma_b = \gamma_{a \circ b}.$$

La aplicación $x \to \gamma_x$ es, pues, un homomorfismo de $G(\circ)$ sobre $\Gamma(\circ)$. Es inyectiva, puesto que $G(\top)$ es regular. Es, pues, un isomorfismo.

3.° La traslación a la derecha φ es biyectiva, luego $\psi = \varphi^{-1}$ está bien definida. Las relaciones

$$\varphi(x) \perp \varphi(y) = \psi[\varphi(x)] \top \varphi(y) = x \top (y \top e) = (x \circ y) \top e = \varphi(x \circ y)$$

demuestran que $x \to \varphi(x)$ es un isomorfismo de $G(\circ)$ sobre $G(\perp)$.

3

Sean A y B dos subgrupos propios de G.

Si $A \subseteq B$, entonces $A \cup B = B$ y $A \cup B$ es distinto de G; lo mismo ocurre si $B \subseteq A$.

Si no, existen $a \in A$, $a \notin B$ y $b \in B$, $b \notin A$. El producto ab no puede pertenecer a $A \cup B$, pues, si, por ejemplo, $ab \in A$, entonces $b \in A$. Luego $A \cup B$ es distinto de G.

4

Multiplicando a la izquierda por x^{-1} y a la derecha por y^{-1}, la igualdad:

$$(xy)^{k+1} = x^{k+1} y^{k+1},$$

nos da

$$(yx)^k = x^k y^k.$$

Ahora bien, por hipótesis,

$$x^k y^k = (xy)^k.$$

y, finalmente, obtenemos

(1) $$(xy)^k = (yx)^k.$$

Del mismo modo, la igualdad

$$(xy)^k = x^k y^k$$

implica

$$(xy)^{k-1} = (yx)^{k-1},$$

de donde

(2) $$(xy)^{-k+1} = (yx)^{-k+1}.$$

Multiplicando miembro a miembro las relaciones (1) y (2) resulta

$$xy = yx.$$

5

Se tiene, sucesivamente,

$$\begin{aligned} a^2 b &= a(ab) = (ab)\, a^3 = ba^6 = ba. \\ ab^3 &= (ab)\, b^2 = ba^3 b^2 = ba(a^2 b)\, b = b(ab)\, ab \\ &= bba^3 ab = b^2 a^2 a^2 b = b^2 a^2 ba = b^2 baa = b^3 a^2. \end{aligned}$$

6

La última relación se escribe

$$b = a^{-1} b^4 a = (a^{-1} ba)^4.$$

Entonces,

$$b^3 = (a^{-1} ba)^{12} = a^{-1} b^{12} a = e.$$

De esto resulta $b^4 = b$, luego $ab = ba$.

7

Consideremos la aplicación φ de $H \times K$ en HK definida por

$$\varphi(h, k) = hk, \quad h \in H, \quad k \in K.$$

Si R es la equivalencia de aplicación φ, existe correspondencia biyectiva entre $H \times K/R$ y HK.

Sea $(h, k) \in H \times K$. Enumeremos los elementos de su clase de equivalencia.

Si $hk = h'k'$, entonces $h'^{-1}h = k'k^{-1}$ es elemento de $H \cap K$. Dado (h, k), k' debe pertenecer a $(H \cap K)k$, luego puede tener a lo más Card $(H \cap K)$ valores. Cada elemento $k' \in (H \cap K)k$ define de modo único el elemento $h' = hkk'^{-1}$. La clase de (h, k) tiene, pues, Card$(H \cap K)$ elementos, de donde la igualdad que se pide.

8

Denotemos por $f_{a,b}$ la aplicación $x \to ax + b$.
Se comprueba fácilmente

$$f_{a,b} \circ f_{c,d} = f_{ac,ad+b}. \tag{1}$$

Por tanto, en $\mathcal{A}$ queda dada una ley interna. El elemento neutro es $f_{1,0}$, y

$$(f_{a,b})^{-1} = f_{a^{-1},-ba^{-1}}.$$

$\mathcal{N}$ es un subgrupo, pues si $f_{1,b} \circ f_{1,d}$, pertenecen a $\mathcal{N}$, entonces

$$f_{1,b} \circ f_{1,d}^{-1} = f_{1,-d+b} \in \mathcal{N}.$$

El subgrupo $\mathcal{N}$ es distinguido, puesto que

$$f_{a,b} \circ f_{1,d} \circ f_{a,b}^{-1} = f_{1,ad}.$$

Sea φ la aplicación de $\mathcal{A}$ en $\mathbf{R}^*$: $\varphi(f_{a,b}) = a$. La fórmula (1) demuestra que φ es un homomorfismo de $\mathcal{A}$ en el grupo multiplicativo $\mathbf{R}^*$. Este homomorfismo es suprayectivo y su núcleo es $\mathcal{N}$, así que se tiene

$$\mathcal{A}/\mathcal{N} \simeq \mathbf{R}^*.$$

9

La relación $x^2 = e$ implica $x = x^{-1}$. Entonces, cualesquiera sean a y b en G se tiene

$$aba^{-1}\, b^{-1} = abab = (ab)^2 = e$$

y, finalmente,

$$ab = ba.$$

Demostremos, por recurrencia sobre el orden de G, que este orden es una potencia de 2.

La propiedad es cierta para $G = \{ e \}$.

Sea $a \neq e$. El subgrupo engendrado por a : $\{ e, a \} = (a)$ es de orden 2, y es distinguido en G, puesto que G es abeliano. El grupo cociente $G/(a)$ es de orden inferior al de G y todos sus elementos satisfacen $x^2 = e$. Según la hipótesis de recurrencia el orden de $G/(a)$ es igual a 2^n, y el orden de G es entonces 2^{n+1}.

10

La aplicación: $n \to a^n$ de $\mathbf{N}^*$ sobre S no es inyectiva si S es finito. Existen, pues, dos enteros m, n, $m < n$, tales que $a^m = a^n$. Entre estos pares elijamos uno en que n sea mínimo. Pongamos $m = n - d$.

La igualdad

$$a^m = a^{m+d}$$

implica

$$a^{m+d} = a^{m+2d} = \cdots = a^{m+hd}.$$

Sea $k \geqslant m$, $k = m + l$. Dividamos l por d:

$$l = hd + r, \quad 0 \leqslant r < d,$$

Se tiene entonces:

$$a^k = a^{m+hd} a^r = a^m\ a^r = a^{m+r}.$$

De esto resulta $a^k \in C$ y se tiene en efecto

$$S = \{ a, a^2, \ldots, a^{n-1} \}.$$

Todos estos elementos son distintos, pues no puede ser

$$a^k = a^{k'},\ k < k' < n - 1,$$

ya que n se ha elegido mínimo.

Demostremos que C es un grupo isomorfo a $\mathbf{Z}/(d)$.

Se ha visto que C es el conjunto de elementos a^k, $k > m$. Por tanto C es estable para la multiplicación de D.

Además, si $k = m + l$, se tiene $a^k = a^{m+r}$, donde r es el resto de la división de l por d, y todos los elementos a^{m+r}, $0 \leqslant r < d$ son distintos. Luego si a^k y $a^{k'}$ son de C se tiene: $a^k = a^{k'}$ si y sólo si $k \equiv k'(d)$. Se puede entonces definir una aplicación φ de C en $\mathbf{Z}/(d)$

$$a^k \in C : \varphi(a^k) = \bar{k}, \quad \text{donde } \bar{k} \text{ es la clase de } k \text{ en } \mathbf{Z}/(d).$$

Esta aplicación es biyectiva, pues es suprayectiva y C consta de d elementos. Es también un homomorfismo, luego es un isomorfismo. Nótese que un generador de C es a^{m+r}, con $m + r \equiv 1(d)$.

11

Si H es el índice 2 y si $x \notin H$, las dos clases a la izquierda H y xH realizan una partición de G, como asimismo las clases a la derecha H y Hx. Se tiene, pues, necesariamente, $xH = Hx$. Si $x \in H$, también es $xH = Hx(= H)$. Luego, H es distinguido en G.

12

Advirtamos que $a = ae$ pertenece a la clase aH. Entonces ab pertenece a la clase $(aH)(bH)$. Ahora bien, si un complejo es una clase a la izquierda, es la clase a la izquierda de cada uno de sus elementos. Se tiene, pues,

$$(aH)(bH) = abH.$$

Tomando $b = a^{-1}$ resulta

$$(aHa^{-1})H = H,$$

lo que implica

$$aHa^{-1} \subseteq H.$$

13

Sea b el conjugado de a, distinto de a. No puede ser $bab^{-1} = b$, si no $a = b$. Luego $bab^{-1} = a$, y $ab = ba$.

El subgrupo H engendrado por a y b es distinguido en G, puesto que $\{a, b\}$ es estable para los automorfismos internos. Puesto que a y b conmutan, todo elemento de H es de la forma $a^\alpha b^\beta$, $\alpha, \beta \in \mathbf{Z}$. Si $H = G$, sea $x \in G$ tal que $b = xax^{-1}$. Pero x se escribe

$$x = a^\alpha b^\beta, \quad \text{de donde } b = a^\alpha b^\beta a b^{-\beta} a^{-\alpha} = a,$$

lo que es absurdo. Luego H es subgrupo distinguido propio de G.

14

Si $G = (a)$, un subgrupo H de G será de la forma $H = (a^k)$. Sea α un automorfismo de G. Si $\alpha(a) = a^p$, entonces $\alpha(H)$ está engendrado por $\alpha(a^k) = \alpha(a)^k = a^{pk}$ que es elemento de H. Se tiene, pues, $\alpha(H) \subseteq H$. El mismo razonamiento prueba que $\alpha^{-1}(H) \subseteq H$, esto es, $H \subseteq \alpha(H)$. Se tiene, finalmente, $\alpha(H) = H$.

Si G es distinguido en N, para todo $x \in N$ la aplicación: $g \to \alpha(g) = xgx^{-1}$ es un automorfismo de G.

Se tiene pues $\alpha(H) = H$, y H es distinguido en N.

15

Sean x e y elementos de G. Existe $z \in G$ tal que $y = xz$. La aplicación $u \to u^n$ es suprayectiva por lo que existe un $u \in G$ tal que $z = u^n$. Se tiene entonces

$$\begin{aligned} x^{n-1} y &= x^{n-1} xu^n = x^n u^n = (xu)^n = x(ux)^n x^{-1}, \\ &= xu^n x^n x^{-1} = yx^{n-1}. \end{aligned}$$

16

El mismo entero k que satisface $a^k \in N$ es, por definición, el orden de la clase $\bar{a}$ de a en G/N.

Ahora bien, se tiene $\bar{a}^n = \overline{a^n} = \bar{e}$, lo que demuestra que n es un múltiplo del orden k de $\bar{a}$.

17

La relación $ab = ba$ implica

$$(ab)^k = a^k b^k, \quad \text{para todo } k \in \mathbf{Z}.$$

Se tiene entonces

$$(ab)^{m \cdot n} = a^{mn} b^{m \cdot n} = (a^m)^n (b^n)^m = e,$$

que demuestra que el orden q de ab divide a mn. Para demostrar la igualdad, basta probar que m y n dividen a q. Puesto que m y n son primos entre sí, el elemento a^n tiene orden m. Las relaciones

$$(a^n)^q = (ab)^{nq} = [(ab)^q]^n = e$$

muestran que q es múltiplo del orden m de a^n. Del mismo modo se demuestra que n es divisor de q.

18

La relación $(ab)^k = e$ implica $a^k = b^{-k} \in (a) \cap (b)$, de donde $a^k = b^k = e$, y k es múltiplo común de los órdenes de a y b. El orden de ab es, pues, el m.c.m. de los órdenes de a y b.

De esto se deduce una nueva demostración para (ejercicio III, 17), pues con las hipótesis hechas $(a) \cap (b)$ se reduce a $\{ e \}$, puesto que su orden divide a m y n.

19

Sea $\bar{x}$ la clase de x en G/N. Si $x^m = e$, entonces $\bar{x}^m = \bar{e}$. Ahora, G/N es un grupo de orden n y el orden de $\bar{x}$, que debe dividir a m y n simultáneamente es necesariamente igual a 1, es decir, $x \in N$.

20

Sea φ la aplicación de G en G definida por

$$\varphi(x) = x^k.$$

Siendo G abeliano, φ es un homomorfismo. Su núcleo es el conjunto de los elementos de G cuyo orden es divisor de k. Puesto que el orden de todo elemento de G divide a n, y que n y k son primos entre sí, el núcleo de φ se reduce a $\{e\}$. φ es, pues, inyectiva y, siendo G finito, es φ un automorfismo de G. Cualquiera sea $a \in G$ existe por tanto un único elemento b verificando

$$b^k = a.$$

Puesto que k es primo con n, existen u y v tales que $1 = uk + vn$. Se tiene entonces, para todo $x \in G : x = x^{uk} x^{vn} = (x^u)^k$. Sea $a \in G$. Entonces a^u satisface la ecuación $x^k = a$. Si b es una solución de esta ecuación se tendrá $(b^k)^u = b = a^u$. Así, a^u es la única solución. En esta demostración no se utiliza que G sea conmutativo.

21

Sea $a \in G$, del que la clase a engendra G/H. Para todo $g \in G$ existe un entero único k tal que

$$\bar{g} = \bar{a}^k = a^k.$$

Existe pues un único $h \in H$ tal que $g = ha^k$. Pongamos $h = \psi(g)$ y denotemos con φ la aplicación canónica $G \to G/H$.

Definiremos ahora una aplicación F de G en $H \times G/H$, con

$$F(g) = [\psi(g), \varphi(g)].$$

Si $g = ha^k$, $g' = h'a^{k'}$, entonces $gg' = hh'a^{k+k'}$, lo que demuestra que

$$\psi(gg') = \psi(g)\,\psi(g').$$

Como ψ y φ son homomorfismos, F lo es también.

Es inmediato que F es un isomorfismo.

22

La aplicación φ de G en G definida por

$$\varphi(x) = x^n$$

es un homomorfismo. Su imagen G^n es, pues, un subgrupo de G, y su núcleo G_n es un subgrupo distinguido. También G^n es distinguido, pues si $x^n \in G^n$, $y \in G$, entonces, $yx^n y^{-1} = (yxy^{-1})^n \in G^n$.

Se tiene el isomorfismo

$$\varphi(G) = G^n \simeq G/G_n$$

que demuestra, si G es finito, que el orden de G^n es igual al índice de G_n.

23

1.° Es inmediato que el conjunto A de los enteros $k \in \mathbf{Z}$ tales que $x^k = e$, $\forall x \in G$, es un subgrupo $n\mathbf{Z}$ de $\mathbf{Z}$. El entero n es múltiplo del orden de cada uno de los elementos de G. Si $n > 0$ resulta que los órdenes distintos de los elementos de G son en número finito. Si esta condición se satisface, $k \in A$ si y sólo si k es múltiplo del orden de todo elemento de G. Siendo n el menor elemento positivo de A, viene a ser el m.c.m. de todos los órdenes distintos antedichos.

2.° Según lo que se acaba de demostrar, si $n = mp^a$, $p \nmid m$, entonces G contiene algún elemento x de orden hp^a. El elemento x^h es entonces de orden p^a.

Si, además, G es abeliano de orden $p_1^{a_1} \dots p_k^{a_k} = n$, sean $a_1, \dots, a_k$ elementos de orden, respectivamente, $p_1^{a_1}, \dots, p_k^{a_k}$. Entonces el producto $a_1 \dots a_k$ es de orden n (ejercicio III, 17).

24

Se puede definir en el conjunto $\mathrm{End}(G)$ una multiplicación que es la composición de aplicaciones y una adición por

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x).$$

Se comprueba sin dificultad que de este modo se define una estructura de anillo unitario.

Si G está engendrado por a, a todo entero k se le puede asociar el endomorfismo definido por

$$\alpha(x) = kx.$$

Esta aplicación es un homomorfismo del anillo $\mathbf{Z}$ en el anillo $\mathrm{End}(G)$. Es una aplicación suprayectiva, pues si $\alpha \in \mathrm{End}(G)$ y si $\alpha(a) = ka$, entonces, para todo $x \in G$, $x = qa$:

$$\alpha(x) = q\alpha(a) = qka = kx.$$

Su núcleo es manifiestamente el ideal (n). Resulta

$$\mathbf{Z}/(n) \simeq \mathrm{End}(G).$$

Los automorfismos de G aparecen como las unidades del anillo End(G), es decir, en $\mathbf{Z}/(n)$ las clases de los enteros primos con n. Recordemos que si α es un automorfismo $\alpha(a) = ka$ debe engendrar G, lo que ocurre si k es primo con n.

Si G es monógeno infinito el núcleo de la aplicación se reduce a $\{0\}$, y End(G) $\simeq \mathbf{Z}$. Hay aquí solamente dos automorfismos: la aplicación idéntica y α: $\alpha(x) = -x$, correspondientes a las dos unidades 1 y -1 de $\mathbf{Z}$.

25

Para todo entero p denotemos por λ_p (respectivamente, μ_p) el número de elementos de G [resp., $\mathbf{Z}/(n)$] cuyo orden es igual a p. Se tienen las relaciones

$$n = \sum_{p/n} \mu_p = \sum_{p/n} \lambda_p. \tag{1}$$

Sea p un divisor de n. Si $\lambda_p \neq 0$, G contiene un elemento g de orden p. Los p elementos del grupo cíclico (g) son soluciones de la ecuación $x^p = e$ y, según la hipótesis, no hay otras. Luego todos los elementos de G de orden p pertenecen a (g).

En $\mathbf{Z}/(p)$ existe un único subgrupo de orden p, a saber el subgrupo cíclico engendrado por la clase de $\frac{n}{p}$, y él contiene todos los elementos de orden p. Dos grupos cíclicos de orden p son isomorfos, luego se tiene, si $\lambda_p \neq 0$: $\lambda_p = \mu_p$, y en todo caso, $\lambda_p \leq \mu_p$. La igualdad (1) implica $\lambda_p = \mu_p$ y en particular $\lambda_n = \mu_n$.

Puesto que $\mathbf{Z}/(n)$ contiene elementos de orden n, lo mismo sucede para G, por lo que G es un grupo cíclico.

26

Sea n un subgrupo de orden n de G. El grupo cociente HS/H que es subgrupo de G/H tiene orden divisor de m. Según el segundo teorema de isomorfismo se tiene $HS/H \simeq S/S \cap H$, lo que demuestra que el orden de HS/H es divisor del orden n de S. La hipótesis hecha implica que HS/H tenga orden 1, es decir $HS = H$ y $S \subseteq H$. Puesto que ambos subgrupos tienen el mismo orden, se deduce $S = H$.

27

Designemos por $\mathcal{N}$ el conjunto de los divisores positivos del entero n, y sea $G = (a)$ un grupo cíclico de orden n.

Sabemos que todo subgrupo de G es cíclico y tiene un orden divisor de n.

Sea k un divisor de n. El subgrupo engendrado por $a^{\frac{n}{k}}$ es de orden k. Demostremos que es el único. Si a^q engendra un subgrupo de orden k, sabemos que este subgrupo está también engendrado por a^d, donde d es el m.c.d. de q y n.

a^d es, pues, de orden k, y este orden es también $\frac{n}{d}$ ya que d divide a n.

Se tiene, pues, $d = \frac{n}{k}$, y $(a^q) = (a^{\frac{n}{k}})$.

Asociando a cada subgrupo su orden, se define, pues, una biyección entre el conjunto de subgrupos de G y $\mathcal{H}$. Sean $H = (a^{\frac{n}{k}})$, $H' = (a^{\frac{n}{k'}})$. Se tiene $H \subseteq H'$ si y sólo si $a^{\frac{n}{k}} \in (a^{\frac{n}{k'}})$ lo que equivale a : $\frac{n}{k'}$ es divisor de $\frac{n}{k}$ esto es, en fin: k es divisor de k'.

El retículo de los subgrupos de G es, pues, isomorfo al conjunto $\mathcal{H}$ ordenado por la relación de divisibilidad.

En cuanto G sea un grupo monógeno infinito, $G = (a)$, todo subgrupo es monógeno y puede caracterizarse por su generador a^n con $n > 0$. Se tiene $(a^n) \subseteq (a^{n'})$ si y sólo si n' divide a n. Se establece así un isomorfismo entre el retículo de los subgrupos y el conjunto N de los enteros > 0 ordenado en orden opuesto al de la divisibilidad (adviértase que 1 y 0 son respectivamente el elemento mayor y el menor).

28

La condición es necesaria:

a) Sea $x \notin A$. Se tiene $A \cap (x) \neq \{e\}$, luego existe $n > 0$ tal que $x^n \in A$. Entonces la clase $\bar{x}$ de x en G/A verifica $\bar{x}^n = \bar{e}$. Por tanto, G/A es un grupo con torsión.

b) Si $x \notin A$ es de orden primo p, entonces $(x) \cap A \neq \{e\}$ implica $(x) \cap A = (x)$, es decir $(x) \subseteq A$, ya que (x) no admite subgrupos propios.

La condición es suficiente:

Sea H un subgrupo de G, $H \neq \{e\}$. Sea $x \neq e$, $x \in H$. Según *a*) existe algún $n > 0$ tal que $x^n \in A$. Si $x^n \neq e$ entonces $A \cap H \neq \{e\}$. Si no, x es de orden finito. Si p es un divisor primo del orden de x, entonces existe $y \in (x)$ de orden p. Según *b*), $y \in A$ y se tiene $A \cap H \neq \{e\}$.

29

a) Sea N un subgrupo casidistinguido de G. Si H es un subgrupo cualquiera, se tienen las siguientes relaciones

$$(xNx^{-1})\,H = xH(x^{-1}Hx)\,x^{-1} = x(x^{-1}Hx)\,Nx^{-1} = H(xNx^{-1})$$

que demuestra que xNx^{-1} es casidistinguido.

b) Observemos que si N_1 y N_2 son subgrupos casidistinguidos, entonces N_1N_2 es un subgrupo, pues N_1 permuta con N_2, asimismo casidistinguido.

Sea N un subgrupo casidistinguido maximal y sea $x \notin N$.

En tal caso $N(xNx^{-1})$ es casidistinguido y contiene a N. Este subgrupo es distinto de G, porque si no x^{-1} podría escribirse

$x^{-1} = n_1 x n_2 x^{-1}$, $n_1 \in N$, $n_2 \in N$, de donde: $x = n_1^{-1} n_2^{-1}$, que contradice $x \notin N$.

Se tiene, pues, $N(xNx^{-1}) = N$, de donde $xNx^{-1} \subseteq N$, o sea, N es distinguido en G.

30

1.° Veamos que $\Phi \subseteq \Phi^*$. Sea $x \notin \Phi$. Existe $i \in J$ tal que $x \notin G_i$. Entonces $G_i \cup \{x\}$ engendra G, pero G_i no engendra G, luego $x \notin \Phi^*$.

Veamos que $\Phi^* \subseteq \Phi$. Sea $x \notin \Phi^*$. Existe una parte N de G tal que $N \cup \{x\}$ engendra G y N engendra un subgrupo propio de G. El conjunto de los subgrupos propios de G continentes de N, y que no contienen a x, no es, pues, vacío. Este conjunto es inductivo y posee un elemento maximal H. Es H subgrupo propio maximal de G, pues si K contiene estrictamente a H, entonces $x \in K$, ya que K contiene a N, y $N \cup \{x\} \subseteq K$ implica $K = G$. H es, pues, uno de los G_i y $x \notin H$ demuestra que $x \notin \Phi$.

2.° Si φ es un automorfismo de G, $\varphi(G_i)$ es un subgrupo maximal de G, así como $\varphi^{-1}(G_j)$, y, cualquiera sea j: $G_j = \varphi[\varphi^{-1}(G_j)]$. Como φ permuta el conjunto de las G_i se tiene $\varphi(\Phi) = \Phi$. En particular, si Φ es un automorfismo interno vemos que Φ es distinguido.

Si todos los G_i son distinguidos, los grupos cocientes G/G_i no poseen subgrupos propios, pues los G_i son maximales. Son, por consiguiente, grupos cíclicos de orden primo, y por tanto abelianos. Para todo i, G_i contiene, pues, al grupo conmutador, y lo mismo Φ.

Si Φ contiene al grupo conmutador, lo mismo sucede con cada G_i. Ahora bien, vamos a ver que si un subgrupo H contiene al grupo conmutador C, es distinguido.

En efecto, sean $x \in G$ y $h \in H$. Se puede escribir:

$$xhx^{-1} = (xhx^{-1}h^{-1})\,h.$$

Este elemento está en H, pues H contiene al conmutador $xhx^{-1}h^{-1}$. También se puede razonar de este modo:

Si φ es la aplicación $G \to G/C$, puesto que H contiene a C se tiene: $\varphi^{-1}[\varphi(H)] = H$. Ahora bien $\varphi(H)$ es distinguido en G/C (grupo abeliano), y por tanto su imagen recíproca lo es en G.

31

La relación $xAx^{-1} = A$ se escribe también $A = x^{-1}Ax$, que prueba que $x^{-1} \in N$ si $x \in N$. Si x e y están en N, se tiene:

$$(xy)\,A(xy)^{-1} = x(yAy^{-1})\,x^{-1} = xAx^{-1} = A.$$

N es, efectivamente, subgrupo de G. Se tiene $K \subseteq N$ y se ve, lo mismo, que K es un subgrupo de G. Demostremos que K es distinguido en N; si $x \in N$, $y \in A$, para todo $a \in A$ es

$$\begin{aligned}(xyx^{-1})\,a(xyx^{-1})^{-1} &= xy(x^{-1}ax)\,y^{-1}x^{-1}\\ &= x(x^{-1}ax)\,x^{-1}, \text{ puesto que } x^{-1}ax \in t\\ &= a\end{aligned}$$

Si A es un subgrupo de G es evidente que es distinguido en N. Si A es distinguido en un subgrupo H se tiene, para todo $x \in H$, $xAx^{-1} = A$, es decir, $x \in N$ y $H \subseteq N$. Por tanto, N es el mayor subgrupo en el que A es distinguido.

32

Denotemos con α_x al automorfismo interno definido por $x \in G$. Si φ es un automorfismo de G se tiene:

$$\begin{aligned}(\varphi \circ \alpha_x \circ \varphi^{-1})\,(a) = (\varphi \circ \alpha_x)\,[\varphi^{-1}(a)] &= \varphi[x\varphi^{-1}(a)\,x^{-1}]\\ &= \varphi(x)\,a[\varphi(x)]^{-1}.\end{aligned}$$

Se deduce,

$$\varphi \circ \alpha_x \circ \varphi^{-1} = \alpha_{\varphi(x)}$$

que demuestra que A es distinguido en Φ.

Supongamos que el centro de G se reduce a $\{ e \}$, y sea φ un elemento del centralizador de A. Se tiene pues, cualquiera sea $x \in G$,

$$\varphi \circ \alpha_x \circ \varphi^{-1} = \alpha_x$$

es decir: $\alpha_{\varphi(x)} = \alpha_x$.

Cualquiera sea $y \in G$, la relación

$$\varphi(x)\, y[\varphi(x)]^{-1} = xyx^{-1}$$

demuestra que $x^{-1}\varphi(x)$ pertenece al centro de G y, a consecuencia de la hipótesis hecha, $\varphi(x) = x$.

φ es, pues, la aplicación idéntica, y el centralizador de A se reduce al elemento neutro de Φ.

33

La aplicación $a \to \gamma_a$ es un isomorfismo de G sobre Γ, pues se cumple la relación

$$\gamma_a \circ \gamma_b = \gamma_{a.b}.$$

1.° La inclusión $\Phi \subseteq \Omega$ resulta de la igualdad

(1) $$\varphi \circ \gamma_a \circ \varphi^{-1} = \gamma_{\varphi(a)}, \text{ donde } \varphi \in \Phi.$$

Puesto que Γ es isomorfo a G todo automorfismo de Γ es de la forma $\gamma_a \to \gamma_{\varphi(a)}$, donde $\varphi \in \Phi$. Basta aplicar la fórmula (1).

2.° Si σ pertenece al centralizador de Γ en $S(G)$, debe tenerse, para todo $a \in G$

$$\sigma \circ \gamma_a = \gamma_a \circ \sigma.$$

Así resulta

$$(\sigma \circ \gamma_a)(e) = \sigma(ae) = \sigma(a) = (\gamma_a \circ \sigma)(e) = a\sigma(e).$$

Si δ_b designa la traslación a la derecha definida por $b \in G$, se tiene en consecuencia

$$\sigma = \delta_{\sigma(e)}$$

y por tanto $\sigma \in \Delta$.

Recíprocamente, si $\delta_b \in \Delta$, entonces,

$$\delta_b \circ \gamma_a = \gamma_a \circ \delta_b .$$

Δ es, pues, el centralizador de Γ en $S(G)$.

Resulta que Γ y Δ son permutables.
Como Γ es también el centralizador de Δ, $\Delta \cap \Gamma$ es el centro de Γ y de Δ.

3.° Designemos por α_a el automorfismo interno definido por $a \in G$.
La igualdad

$$\delta_b \circ \gamma_a = \gamma_{ab} \circ \alpha_b{}^{-1}$$

demuestra la inclusión

$$\Delta\Gamma \subseteq \Gamma A.$$

Las igualdades pedidas resultan entonces de las relaciones

$$\alpha_a \circ \gamma_b = \gamma_{aba}{}^{-1} \circ \alpha_a = \delta_{a-1} \circ \gamma_{ab}.$$

Sea $\omega \in \Omega$. La aplicación

$$\gamma_a \to \omega \circ \gamma_a \circ \omega^{-1}$$

es un automorfismo de Γ, luego se tiene, por lo 1.°):

$$\omega \circ \gamma_a \circ \omega^{-1} = \varphi \circ \gamma_a \circ \varphi^{-1}, \quad \text{donde} \quad \varphi \in \Phi.$$

Resulta que $\varphi^{-1} \circ \omega$ pertenece al centralizador de Γ, que es Δ. Se tiene pues,

$$\omega \in \Phi\Delta \subseteq \Phi\Delta\Gamma = \Phi A\Gamma = \Phi\Gamma,$$

y

$$\Omega \subseteq \Phi\Gamma.$$

Se verifica la igualdad, puesto que Φ y Γ están contenidos en Ω. Se tiene también $\Phi\Gamma = \Gamma\Phi$ puesto que $\Phi\Gamma$ es un grupo (y porque Γ es distinguido en Ω).

Además $\Phi \cap \Gamma$ se reduce a $\{\varepsilon\}$, pues una traslación a la izquierda no es un isomorfismo más que cuando viene definida por e.

El grupo Ω puede considerarse como una extensión de G, puesto que contiene a Γ isomorfo a G. Todo automorfismo de G puede entonces considerarse como la restricción a G de un automorfismo interno de Ω. Se dice que Ω es la holomorfía de G.

34

1.° K, que es el centralizador de H en G, es un subgrupo de G (ejercicio III, 31). Demostremos que K es distinguido en G. Sean $x \in K$, $g \in G$, $h \in H$. Puesto que H es distinguido, $g^{-1}hg$ pertenece a H y se puede escribir

$$x(g^{-1}hg) = (g^{-1}hg)\,x,$$

de donde resulta

$$(gxg^{-1})\,h = h(gxg^{-1}).$$

El producto HK de dos subgrupos distinguidos es entonces un subgrupo distinguido.

Se han visto ya (ejercicio III, 32) que el grupo de los automorfismos internos de un grupo H es un subgrupo distinguido del grupo de los automorfismos de H.

Se puede razonar más brevemente como sigue.

Para todo $g \in G$, denotemos α_g el automorfismo interno de G definido por g. Puesto que H es distinguido se tiene $\alpha_g(H) = H$, y la restricción α_g/H de α_g a H pertenece a A. Se define un homomorfismo φ de G en A por

$$\varphi(g) = \alpha_g/H.$$

El núcleo de φ es el conjunto de los $g \in G$ tales que $\alpha_g/H = id_H$, es decir $ghg^{-1} = h$, $\forall h \in H$. El núcleo de φ es, pues, K, lo que vuelve a demostrar que K es distinguido en G.

Es evidente que $\varphi(H)$ es igual a N. Siendo N distinguido en G lo es en $\varphi(G)$ y el segundo teorema de isomorfismo nos dice que $\varphi(G)/N$ y $G/\varphi^{-1}(N)$ son isomorfos. Ahora bien, se tiene

$$\varphi^{-1}(N) = \varphi^{-1}[\varphi(H)] = HK.$$

Por tanto, G/HK es isomorfo a $\varphi(G)/N$ que es un subgrupo de A/N.

2.° Sea φ' la restricción de φ a HK. Se tiene,

$$\varphi'(HK) = \varphi(HK) = N.$$

El núcleo de φ' coincide con el de φ puesto que $HK \supseteq K$. Entonces el teorema de homomorfismo afirma

$$HK/K \simeq N.$$

He aquí otra demostración:
Si $Z(H)$ es el centro de H, sabemos que se tiene el isomorfismo

$$H/Z(H) \simeq N.$$

Ahora, aquí es $Z(H) = H \cap K$ y el segundo teorema de isomorfismo nos permite escribir

$$H/H \cap K \simeq HK/K.$$

3.° Puesto que $Z(H) = \{e\}$, se tiene $H \cap K = \{e\}$. Además, A es igual a N, y G/HK se reduce a la clase unidad; es decir, $G = KH$. Por tanto, G es producto directo de H y de K.

35

1.° *a*) La verificación es inmediata.

b) Designemos por $\bar{x}$ la clase de $x \in G$ en G/H. La expresión $x^n \in H$ equivale a $\bar{x}^n = \bar{e}$. Resulta que H es aislado si y sólo si G/H es sin torsión.

2.° *a*) Si G es un R-grupo la relación $x^n = e = e^n$ implica $x = e$, luego G es sin torsión.

Si G es un grupo abeliano sin torsión la relación $x^n = y^n$ se escribe

$$x^n y^{-n} = (xy^{-1})^n = e,$$

de donde resulta $xy^{-1} = e$, o sea $x = y$, luego G es un R-grupo.

b) Sea $C(M)$ el centralizador de $M \subseteq G$. Si $x^n \in C(M)$ la igualdad $yx^n y^{-1} = x^n$ para todo $\forall\, y \in M$, se escribe $(yxy^{-1})^n = x^n$, de donde resulta $yxy^{-1} = x$, que demuestra que x pertenece a $C(M)$. Por tanto, $C(M)$ es un subgrupo aislado. En particular, el centro de G, $Z = C(G)$ es un subgrupo aislado.

La relación $x^k y^n = y^n x^k$ implica $x \in C(y^n)$, equivalente a $y^n \in C(x)$. Por consiguiente $y \in C(x)$, es decir $xy = yx$.

c) Si G es un R-grupo, lo es asimismo todo subgrupo de G. Indicaremos con $\bar{x}$ la clase de $x \in G$ en G/Z. La igualdad $\bar{y}^n = \bar{x}^n$ implica $x^n = zy^n$, donde $z \in Z$. Resulta,

$$x^n y = zy^{n+1} = yzy^n = yx^n.$$

Por 2.° *b*) se tiene entonces $xy = yx$. La igualdad $\bar{x}^n = \bar{y}^n$ se escribe: $(xy^{-1})^n \in Z$ de donde $xy^{-1} \in Z$, puesto que Z es aislado, y finalmente, $\bar{x} = \bar{y}$. Por tanto, G/Z es un R-grupo.

Recíprocamente, si Z y G/Z son R-grupos, la igualdad $x^n = y^n$ implica $\bar{x}^n = \bar{y}^n$, luego $\bar{x} = \bar{y}$, esto es, $y = zx$, donde $z \in Z$. Por consiguiente $y^n = z^n x^n$, de donde $z^n = e$, luego $z = e$, puesto que Z es sin torsión. Se tiene, pues, $x = y$, lo que demuestra que G es un R-grupo.

36

1.° Al ser A distinguido en G, la restricción $\tilde{b}$ a A del automorfismo interno de G definido por $b \in B$, es un automorfismo de A, y se tiene

$$\tilde{b}(a) = bab^{-1}$$

de donde

$$ba = \tilde{b}(a)b.$$

La aplicación $\varphi\colon b \to \varphi(b) = \tilde{b}$ es un homomorfismo.

Todo $g \in G$ se escribe de modo único $g = ab$, $a \in A$, $b \in B$, pues si $ab = a'b'$, se deduce

$$a'\,a^{-1} = b'\,b^{-1} \in A \cap B,$$

de donde $a = a'$ y $b = b'$. Se puede entonces definir una aplicación f de G en B por

$$g = ab, \quad f(g) = b.$$

Esta aplicación f es suprayectiva, pues $b = f(b)$. Si $g = ab$, $g' = a'\,b'$, entonces,

$$gg' = ab\,a'\,b' = a\tilde{b}(a')bb' \quad \text{demuestra que} \quad f(gg') = bb' = f(g)f(g').$$

El núcleo de f es A, y se tiene el isomorfismo $G/A \simeq B$.

2.° Se verifica fácilmente lo asociatividad de la ley. Designando por el mismo símbolo e los elementos neutros de A y B, el elemento neutro para la ley dada es (e, e). El elemento inverso de (a, b) es $[\tilde{b}^{-1}(a^{-1}), b^{-1}]$. Pongamos

$$A' = \{(a, e);\, a \in A\}, \qquad B' = \{(e, b);\, b \in B\}.$$

El lector puede comprobar que el grupo $A \times B$ es el producto semidirecto de A' y B'

3.° El grupo simétrico S_3 es producto semidirecto del grupo alternado A_3, grupo cíclico de orden 3 engendrado por la permutación circular (123) y de un grupo cíclico de orden 2 engendrado por una trasposición.

37

Sea K_0 un subgrupo distinguido minimal de N (minimal en el conjunto de los subgrupos $\neq \{e\}$ distinguidos de N) y sean $K_0, K_1, ..., K_p$ los distintos conjugados de K_0 por los automorfismos internos de G. Puesto que N es distinguido en G, un automorfismo interno de G induce un automorfismo sobre N. Los K_i son, pues, subgrupos distinguidos minimales de N. Los K_i engendran un subgrupo de N, estable para los automorfismos internos de G, y por tanto igual a N, puesto que N es minimal en el conjunto de los subgrupos distinguidos de G.

Se puede suponer, suprimiendo si es necesario algunos K_i, que para todo i

$$K_i' = K_1 ... K_{i-1} K_{i+1} ... K_p$$

es diferente de N, es decir, $K_i \not\subseteq K_i'$. En tal caso $K_i \cap K_i'$, que es un subgrupo distinguido de N, contenido en K_i, es igual a $\{e\}$. Por tanto, N es el producto directo de los K_i.

Queda por demostrar, por ejemplo, que K_1 es simple. Si H es un subgrupo distinguido en K_1, demostremos que lo es también en N. Puesto que $N = K_1 \times K_1'$, todo $x \in N$ se escribe: $x = x_1 x_1'$, $x_1 \in K_1$, $x_1' \in K_1'$, y se tiene

$$xHx^{-1} = x_1 x_1' H x_1'^{-1} x_1^{-1} = H$$

pues x_1 conmuta con todo elemento de K_1, siendo el producto directo. Tenemos, pues $H = \{e\}$ ó $H = K_1$, y K_1 es un grupo simple.

38

Sea $\frac{r}{s} \in Q$. Denotemos con $\left[\frac{r}{s}\right]$ su clase módulo $\mathbf{Z}$. Si $\left[\frac{r}{s}\right]$ es irreducible, $s > 0$, $\left[\frac{r}{s}\right]$ es de orden s. Se puede suponer $0 < r < s$, pues $\left[\frac{r}{s}\right] = \left[\frac{r'}{s}\right]$ si r' es el resto de la división de r por s. Los elementos de U_p pueden, pues, escribirse $\left[\frac{r}{p^k}\right]$, donde $(r, p) = 1$ y $0 < r < p^k$. Pongamos $a_\lambda = \left[\frac{1}{p^k}\right]$. a_λ engendra un subgrupo de orden p^k, a saber, $V_k = \mathbf{Z}a_k$. Si $k < k'$,

$$a_k = p^{k'-k} a_{k'}, \quad \text{y} \quad V_k \subseteq V_{k'}.$$

Además V_k es el conjunto de elementos de U_p de orden $p^{k'}$, $k' \leqslant k$, pues

$$\left[\frac{r}{p^{k'}}\right] = rp^{k-k'}\,a_k.$$

Si $a \in U_p$ es de orden p^k, entonces a engendra V_k, pues $\mathbf{Z}a$ tiene p^k elementos y está contenido en V_k.

1.° Sea $a = \left[\frac{r}{p^{k'}}\right]$, $(r, p) = 1$, y sea $n = n'\,p^l$, $(n', p) = 1$. Los elementos a y $n'\,p^l\,a_{k+l} = \left[\frac{n'}{p^k}\right]$ engendran cada uno V_k. Existe, pues, $m \in \mathbf{Z}$ tal que $a = m(n'\,p^l\,a_{k+l})$. Poniendo $\beta = ma_{k+l}$ se tiene efectivamente $a = n\beta$.

2.° Sea H un subgrupo de U_p. Si, cualquiera sea k, H contiene un elemento de orden $p^{k'}$, $k' \geqslant k$, entonces H contiene a $V_{k'}$, y por tanto a V_k, para todo k. Por consiguiente:

$$H = \bigcup_{k \geqslant 0} V_k = U_p.$$

Si no, existe k tal que todo elemento de H sea de orden menor o igual a p^k, es decir, $H \subseteq V_k$. Si k se ha elegido mínimo, H contiene un elemento de orden p^k, y entonces $H = V_k$.

Los subgrupos de H forman una cadena:

$$V_0 = \{0\} \subset V_1 \subset V_2 \subset \cdots \subset V_k \subset \cdots \subset U_p.$$

3.° Sea a_1 un generador de G_1. Supongamos que existen elementos a_1, a_2, ..., a_k, que engendran respectivamente G_1, G_2, ..., G_k, y tales que $a_i = pa_{i+1}$, $1 \leqslant i \leqslant k-1$; demostremos que existe un generador a_{k+1} de G_{k+1} tal que $a_k = pa_{k+1}$.

La aplicación φ de G_{k+1} en G_{k+1} definida por $\varphi(x) = px$ es un homomorfismo, cuyo núcleo es el conjunto de elementos de G_{k+1} de orden p y el cero. Ahora, por ser G_{k+1} cíclico no posee más que un subgrupo de un orden dado; G_1 es de orden p: contiene, pues, a todos los elementos de orden p. Luego $\varphi(G_{k+1})$ es isomorfo a G_{k+1}/G_1, que es de orden p^k. Se tiene, pues, $\varphi(G_{k+1}) = G_k$, pues G_k es el único subgrupo de orden p^k. Existe entonces $a_{k+1} \in G_{k+1}$ tal que

$$a_k = pa_{k+1},$$

y a_{k+1} es de orden p^{k+1}; este elemento engendra G_{k+1}.

De este modo se construye por recurrencia la sucesión $(a_k)_{k \geqslant 0}$ pedida.

Sea $x \in G = \bigcup_{n \geqslant 0} G_n$. Si $x = qa_m = ra_n$, $n \geqslant m$, entonces,

$$qp^{n-m} a_n = ra_n$$

y p^n divide a $qp^{n-m} - r$. En consecuencia

$$(qp^{n-m} - r)\, a_n = 0. \quad \text{de donde} \quad qa_m = ra_n.$$

Esto permite definir una aplicación f de G en U_p por

$$f(x) = ra_n \quad \text{si} \quad x = ra_n \in G.$$

f es inyectiva, pues $ra_n = 0$ implica $p^n \mid r$, de donde $ra_n = 0$.

f es suprayectiva, pues $a = \left[\frac{r}{p^n}\right] = f(ra_n)$.

f es un homomorfismo pues si $x, y \in G$, existe n tal que $x, y \in G_n$,

$$x = ra_n \quad y = sa_n$$

y se tiene inmediatamente

$$f(x + y) = (r + s)\, a_n = ra_n + sa_n = f(x) + f(y).$$

4.° Sea $a = \left[\frac{r}{s}\right] \in U$. Si $s = p_1^{h_1} \ldots p_n^{h_n}$, es una descomposición de s en factores primos, pongamos $q_i = \frac{s}{p_i^{h_i}}$. Los q_i son primos entre sí en su conjunto. Existen pues (identidad de Bezout), enteros u_i tales que

$$1 = \sum_{i=1}^{n} u_i q_i.$$

Por consiguiente,

$$a = \left[\frac{r}{s}\right] = \sum_{i=1}^{n} ru_i \left[\frac{1}{p_i^{hi}}\right], \quad \text{y} \quad ru_i \left[\frac{1}{p_i^{hi}}\right] \in U_{p_i}.$$

Para demostrar la unicidad es suficiente, por linealidad, demostrar que

$$0 = a_{p_1} + \ldots + a_{p_n} \quad a_{p_i} \in U_{p_i}$$

implica $a_{p_i} = 0$, $\forall i$.

Esa igualdad se escribe también

$$a_{p_i} = -(a_{p_1} + \cdots + a_{p_n}).$$

Si a_{p_i} es de orden $p_i^{h_i}$, se deduce $p_2^{h_2} \cdots p_n^{h_n} a_{p_1} = 0$.

El orden $p_1^{h_1}$ de a_{p_1} es por tanto divisor de $p_2^{h_2} \ldots p_n^{h_n}$, lo que implica $h_1 = 0$ y $a_{p_1} = 0$. Se demuestra lo mismo $a_{p_i} = 0$, $\forall i$.

Se puede entonces definir una aplicación f de U en $\prod_{p \in P} U_p$. Si $a = \sum_{i=1}^{n} a_{p_i}$, $a_{p_i} \in U_{p_i}$, pongamos

$$f(a) = (\gamma_p)_{p \in P}, \quad \text{donde} \begin{cases} \gamma_p = a_{p_i} & \text{si} \quad p = p_i \\ \gamma_p = 0 & \text{en otro caso.} \end{cases}$$

Esto es manifiestamente un isomorfismo de U sobre el subgrupo de $\prod_{p \in P} U_p$ formado por las sucesiones $(\gamma_p)_{p \in P}$ tales que $\gamma_p = 0$ salvo para un número finito de $p \in P$.

39

1.° *a*) Es inmediato que (*a*) es el conjunto de elementos: $\alpha_1(a^{n_1}) \ldots \alpha_k(a^{n_k})$, donde los α_i son automorfismos internos y $n_i \in \mathbf{Z}$.

b) $[A, B]$ es distinguido en G, pues el conjunto de conmutadores $aba^{-1}b^{-1}$ es estable para los automorfismos internos de G. Además,

$$(aba^{-1})\, b^{-1} = a(bab^{-1})$$

está en $A \cap B$, pues A y B son distinguidos. Se tiene, pues, $[A, B] \subseteq A \cap B$.

Señalemos que $[A, B] = [B, A]$, pues

$$bab^{-1}a^{-1} = (aba^{-1}b^{-1})^{-1}.$$

Además, $A \subseteq A'$ implica $[A, B] \subseteq [A', B]$. Por consiguiente

$$[A_i, B] \subseteq [A_1 A_2, B]\ i = 1, 2, \quad \text{de donde} \quad [A_1, B]\,[A_2, B] \subseteq [A_1 A_2, B].$$

Sea $x = a_1 a_2 b a_2^{-1} a_1^{-1} b^{-1}$ un conmutador de $[A_1 A_2, B]$. Se puede escribir

$$x = \{ a_1(a_2 b a_2^{-1}) a_1^{-1} (a_2 b a_2^{-1})^{-1} \} \quad \{ a_2 b a_2^{-1} b^{-1} \} \in [A_1, B]\,[A_2, B],$$

y finalmente

$$[A_1, B]\,[A_2, B] = [A_1 A_2, B].$$

2.° *a*) La condición es evidentemente suficiente. Demostremos que es necesaria y, para ello, que si se tienen dos sg d, A y B, tales que $[A, B] \subseteq P$, $A \nsubseteq P$, $B \nsubseteq P$, entonces P no es primo. Sean $a \in A$, $a \notin P$, $b \in B$, $b \notin P$. Entonces $[(a), (b)] \subseteq [A, B] \subseteq P$, y P no es primo.

Pongamos

$$C(A_1, ..., A_n) = [C(A_1, ..., A_{n-1}), A_n], \qquad C(A_1, A_2) = [A_1, A_2].$$

Se tiene

$$C(A_1, ..., A_n) \subseteq A_1 \cap ... \cap A_n \quad \text{(por recurrencia)}.$$

Si $A_1 \cap ... \cap A_n \subseteq P$, entonces: $A_n \subseteq P$, ó $C(A_1, ..., A_{n-1}) \subseteq P$. Se prueba así, por recurrencia, que existe i con $A_i \subseteq P$.

b) Sea P primo, $M = G - P$. Si $m_1 \in M$, $m_2 \in M$, entonces $[(m_1), (m_2)] \subseteq$ $\subseteq P$; existen, pues, $m_i' \in (m_i)$, $i = 1, 2$, tales que $[m_1', m_2'] \notin P$. Luego M es un m-sistema.

Sea P un sg d tal que $G - P$ sea un m-sistema. Veamos que $a \notin P$, $b \notin P$, implica $[(a), (b)] \subseteq P$. En efecto, existen $a' \in (a)$, $b' \in (b)$ tales que

$$[a', b'] \notin P.$$

Luego, P es primo.

3.° *a*) En efecto, la familia de los m-sistemas que contienen a M y son disjuntos con A es $\cup$-inductiva, lo que es de verificación inmediata.

b) La familia de los sg d que contienen a A y son disjuntos con M es inductiva. Sea P^* un elemento maximal de esta familia. Demostremos que P^* es primo. Sean x e $y \in G - P^*$. $P^*(x)$ y $P^*(y)$ contienen estrictamente a P^*, luego se cortan con M (esto es, dan intersección no vacía, o tienen elementos comunes). Existen $m_1 \in P^*(x) \cap M$ y $m_2 \in P^*(y) \cap M$. Tomemos $m_i' \in (m_i)$, $i = 1, 2$, tales que $[m_1', m_2'] \in M$. Se tiene

$$[m_1', m_2'] \in [P^*(x), P^*(y)], \quad \text{luego} \quad [P^*(x), P^*(y)] \subseteq P^*.$$

Por consiguiente $[(x), (y)] \subseteq P^*$, pues

$$[P^*(x), P^*(y)] = [P^*, P^*]\,[P^*, (x)]\,[P^*, (y)]\,[(x), (y)],$$

mediante la fórmula de 1.° *b*), y los tres primeros corchetes están contenidos en P^*.

c) Sea P una parte que contiene a A y tal que $G - P = M$ sea un m-sistema maximal disjunto con A. Sea P^* un sg d maximal conteniendo a A y disjunto con M. Se ha visto que P^* es primo, luego $G - P^*$ es un m-sistema; ahora bien, $G - P^*$ contiene a M y es disjunto con A. Se tiene, pues, $M = G - P^*$, de donde $P^* = P$, y P es primo.

Recíprocamente, sea P un sg d minimal conteniendo a A. $M = G - P$ es un m-sistema. Sea M' un m-sistema conteniendo a M y disjunto con A.

Según *b*) existe un sg d primo P' que contiene a A y es disjunto con M'. Se tiene entonces

$$P' \subseteq G - M' \subseteq G - M = P.$$

Por consiguiente $P' = P$, luego $M' = M$ y M es maximal.

4.° Puesto que existe siempre un m-sistema disjunto con A, a saber $\varnothing$, todo ideal A está contenido en un sg d primo minimal. Además todo sg d primo P conteniendo a A contiene un sg d primo minimal conteniendo a A (puesto que $G - P$ es un m-sistema). Por consiguiente $r(A)$ es la intersección de los sg d primos minimales que contienen a A.

Manifiestamente $A \subseteq B$ implica $r(A) \subseteq r(B)$. Por tanto se tiene,

$$r([A, B]) \subseteq r(A \cap B) \subseteq r(A) \cap r(B).$$

Para un sg d primo P tendremos:

$$P \supseteq [AB] \Leftrightarrow P \supseteq A \quad \text{o} \quad P \supseteq B,$$

de donde:

$$r([A, B]) = \bigcap_{\substack{P \supseteq A \\ \text{o} \\ P \supseteq B}} P = \left(\bigcap_{P \supseteq A} P\right) \cap \left(\bigcap_{P \supseteq B} P\right) = r(A) \cap r(B).$$

Sean $a \in r(A)$ y M un m-sistema que contiene a a. Si $M \cap A = \varnothing$ existe, según lo 3.°, un sg d primo P contenido en $G - M$, y $a \notin P$, lo que es absurdo. Se tiene, pues, $M \cap A \neq \varnothing$.

Si a cumple la condición, entonces, para todo sg d primo P se tiene $a \in P$; si no, $G - P$ sería un m-sistema conteniendo a a y disjunto con A.

CAPÍTULO IV

Grupos (complementos)

Enunciados

1

Sea G un grupo finito. Demostrar que el número de conjugados distintos de un subgrupo H de G es igual al índice en G del normalizador de H.

Deducir que si $H \neq G$, entonces $G \neq \bigcup_{x \in G} xHx^{-1}$.

Demostrar que el número de p subgrupos de Sylow de G es divisor del orden de G.

2

Sean G un grupo de orden p^n, H un subgrupo distinguido de G. Demostrar que si H no se reduce a $\{e\}$, entonces H contiene un elemento $\neq e$ del centro de G. (Hacer operar a G sobre H por los automorfismos internos.)

3

Sean G un grupo, H un subgrupo propio de G, S el conjunto de clases a la izquierda de G según H. Se considera que G opera sobre S por traslaciones a la izquierda. Demostrar que se define así un homomorfismo de G en el grupo de biyecciones de S, cuyo núcleo es el mayor subgrupo de H distinguido en G.

Deducir que si G es un grupo finito cuyo orden no sea divisor de $i(H)!$, entonces H contiene un subgrupo propio distinguido en G.

4

Sea H un subgrupo distinguido en un grupo G contenido en el centro de G. Demostrar que, si G/H es cíclico, G es abeliano. Deducir que si G es

un grupo no abeliano de orden p^a (p primo), entonces el índice del centro de G es al menos divisible por p^2. ¿Qué se puede decir de los grupos de orden p^2?

5

Demostrar que el centro Z de un grupo de orden p^2 no puede ser de orden p. (Tómese en cuenta el normalizador de $a \notin Z$.)

Deducir que un grupo de orden p^2 es abeliano.

6

Sea G un grupo de orden mp^r (p primo, $p \nmid m$). Consideremos un subgrupo H de orden p^a, $a < r$, y su normalizador N. H opera por automorfismos internos sobre el conjunto $\mathcal{H}$ de sus conjugados. Contando de dos maneras el número de elementos de $\mathcal{H}$, demostrar que la hipótesis $N = H$ conduce a una contradicción.

Deducir que todo subgrupo de orden p^{r-1} de un grupo de orden p^r es distinguido.

Demostrar que todo grupo de orden p^2 que no sea cíclico, es producto directo de dos subgrupos de orden p, y, por tanto, es abeliano.

7

1.° Un grupo finito G se dice p-primario si todo elemento de G tiene por orden una potencia del número primo p. Demostrar que el orden de G es una potencia de p. Demostrar que todo subgrupo distinguido de orden p está contenido en el centro.

2.° Sea G un grupo de orden $m = np^r$, $(p \nmid n)$.

a) Sea K un subgrupo de G. Demostrar que los conjuntos de la forma KgK distintos, $g \in G$, forman una partición de G, y que KgK es una unión de clases a la izquierda de G por K. Sea $\mu(KgK)$ el número de clases a la izquierda contenidas en KgK. Demostrar que $\mu(KgK)$ es igual al índice de $(gKg^{-1}) \cap K$ en K. Demostrar que $\mu(KgK) = 1$ si y sólo si g pertenece al normalizador N de K.

Se supone que el orden de K es p^i, $i < r$. Demostrar que el orden de N/K es divisible por p.

b) Sea G un grupo de orden p^r. Demostrar que todo subgrupo de orden p^i, $i < r$, es distinguido en un subgrupo de orden p^{i+1}, y que todo subgrupo de orden p^{r-1} es distinguido en G.

8

1.° Sea G un grupo finito; si $x \in G$ es de orden mn con m y n primos entre sí, demostrar que existen dos potencias de x, sean y y z, de órdenes respectivos m y n, tales que $x = yz = zy$. Deducir que G es el producto de sus subgrupos de Sylow.

2.° Sea P un subgrupo de Sylow de H y sea N su normalizador. Demostrar que N es su propio normalizador.

3.° Sea G un grupo finito en el que todo subgrupo propio sea distinto de su normalizador. Demostrar que G es el producto directo de sus subgrupos de Sylow.

9

Se llama grupo hipercíclico un grupo finito en el que todos los subgrupos de Sylow son cíclicos. Sea G un grupo hipercíclico.

1.° Demostrar las siguientes propiedades:
Todo subgrupo de G es hipercíclico. Si G es abeliano, entonces es cíclico. Dos subgrupos de G de orden p^n (p primo) son conjugados.

2.° Sean N un subgrupo distinguido de G, H un subgrupo cualquiera. Demostrar que el orden de $N \cap H$ es el m.c.d. de los órdenes de N y H, y que el orden de NH es su m.c.m.

3.° Demostrar que todo subgrupo distinguido N de G es estable para los automorfismos de G.

10

Sean G un grupo finito, p un número primo, S un p-subgrupo de Sylow de G, N un subgrupo distinguido de G.

1.° Demostrar que $N \cap S$ es un p-subgrupo de Sylow de N y que NS/N es un p-subgrupo de Sylow de G/N.

2.° Sea $\mathcal{N}(S)$ el normalizador de S en G.
Demostrar que $\mathcal{N}(S)N/N$ es el normalizador de NS/N en G/N, y que $\mathcal{N}(S)$ está contenido en $\mathcal{N}(S \cap N)$, normalizador de $S \cap N$ en G.
Se tiene el isomorfismo

$$\frac{G}{N} \simeq \frac{\mathcal{N}(S \cap N)}{N \cap \mathcal{N}(S \cap N)}.$$

11*

Sea G un grupo finito y sea p un número primo divisor del orden de G.

1.° Demostrar que la familia de los p-subgrupos distinguidos de G tiene un elemento máximo D que es la intersección de los p-subgrupos de Sylow de G. (Se llama p-subgrupo un subgrupo cuyo orden es una potencia de p.)

2.° Se supone que los p-subgrupos de Sylow de G son abelianos. Nos proponemos demostrar que si P es uno de ellos, existe un conjugado P^* de P tal que $P \cap P^* = D$. Para ello se razonará por recurrencia sobre el orden de G, distinguiendo dos casos:

a) Si $D \neq \{e\}$, aplicar la hipótesis de recurrencia a G/D.

b) Si $D = \{e\}$, demostrar que existen conjugados $P_1, \ldots, P_r$ de P tales que

$$P \cap P_1 \cap \ldots \cap P_r = \{e\}, \quad \text{y, si} \quad r > 1, \quad P \cap P_1 \cap \ldots \cap P_{r-1} = T \neq \{e\}.$$

Sea H el grupo engendrado por $P, P_1, \ldots, P_{r-1}$. Demostrar que T es la intersección de los p-subgrupos de Sylow de H y que $H \neq G$. Aplicando a H la hipótesis de recurrencia, demostrar que existe un p-subgrupo de Sylow R de H, que contiene a $H \cap P_r$, y existe un conjugado R^* de R tales que $R \cap R^* = T$. Demostrar que $R^* \cap P_r = \{e\}$ y deducir que G satisface la propiedad y deducir que en G se cumple la propiedad enunciada.

12

Sean G un grupo, M un sistema generador de G. Sea N el subgrupo distinguido de G engendrado por los conmutadores $m_1 m_2 m_1^{-1} m_2^{-1}$, $m_i \in M$. Demostrar que N es el grupo conmutador de G.

13

Sea G el grupo engendrado por dos elementos a y b ligados por las relaciones de definición:

$$a^4 = e = b^4, \quad a^2 = b^2, \quad aba = b.$$

Demostrar que G consta a lo más de ocho elementos.

Sea G' el subgrupo de S_8 engendrado por

$$a' = (1\ 2\ 3\ 4)\,(5\ 6\ 7\ 8), \quad b' = (1\ 5\ 3\ 7)\,(2\ 8\ 4\ 6).$$

Demostrar que G' es isomorfo a G.
¿Cuáles son los subgrupos G?

14

Sea G un grupo de orden pq, donde p y q son primos, $p > q$.
Demostrar que G tiene un subgrupo distinguido de orden p. Si q no es divisor de $p - 1$, G tiene un subgrupo distinguido de orden q y es un grupo cíclico. (Tener presente el ejercicio IV, 1.) Dar un ejemplo de grupo no abeliano de orden pq. Demostrar que todo grupo abeliano de orden pq es cíclico.

15

1.° Sea G un grupo no abeliano de orden pq, p y q primos, $p > q$. (Tener presente el ejercicio IV, 14.)

Demostrar que G está engendrado por dos elementos a y b satisfaciendo

$$a^p = e, \quad b^q = e, \quad bab^{-1} = a^r, \quad r^q \equiv 1(p), \quad r \not\equiv 1(p), \quad q \mid p - 1.$$

2.° Recíprocamente, sea G el grupo engendrado por a y b ligados por las relaciones de definición precedentes.

Demostrar que todo elemento de G se escribe

$$a^x b^y, \quad 0 \leqslant x < p, \quad 0 \leqslant y < q.$$

Sea Γ el grupo formado por los pares (x, y), $0 \leqslant x < p$, $0 \leqslant y < q$, con la siguiente ley de composición

$$(x, y)\,(x', y') = \begin{cases} (x + r^y x', y + y') & \text{si} \quad y + y' < q \\ (x + r^y x', y + y' - q) & \text{si} \quad y + y' \geqslant q \end{cases}$$

donde la primera coordenada del segundo miembro es una suma módulo p.

Demostrar que Γ es isomorfo a G. Por consiguiente G tiene pq elementos.

16

Sea G un grupo abeliano denotado aditivamente. Se supone que G es suma directa de grupos monógenos infinitos. Demostrar que G es un grupo abeliano libre.

17

Dar un ejemplo de grupo abeliano sin torsión que no sea libre.

18

1.° Encontrar todas las bases del grupo abeliano libre $\mathbf{Z}^2$.

2.° Sea G el grupo abeliano engendrado por dos elementos a y b ligados por la relación de definición

$$ma = nb \quad \text{(notación aditiva).}$$

Se sabe que G es isomorfo a un grupo cociente de $\mathbf{Z}^2$. Repitiendo sobre este ejemplo la demostración del teorema de estructura de grupos abelianos de tipo finito (texto, II, 6) demostrar que G es suma directa de un grupo monógeno infinito y de un grupo cíclico.

19

Sea G un grupo abeliano de tipo finito sin torsión, con notación aditiva. Se considera una parte libre maximal L de G y el subgrupo H engendrado por L. H es un grupo abeliano libre. Demostrar que existe un entero n tal que, cualquiera sea $x \in G$, se tiene $nx \in H$. Deducir que G es isomorfo a un subgrupo de H y que G es un grupo abeliano libre.

¿Es necesariamente $G = H$?

Demostrar directamente que G es un grupo abeliano libre mediante los teoremas relativos a los grupos abelianos de tipo finito.

20

Designamos con $D(G)$ el grupo engendrado por los conmutadores de un grupo G, al que se llama también grupo derivado de G. Se define por recu-

rrencia el k-ésimo grupo derivado de G, designado $D^k(G)$, como igual a $D(D^{k-1}(G))$.

1.° Demostrar que $D^k(G)$ es un subgrupo de G estable para los endomorfismos de G.

Deducir que si H es un subgrupo de G, $D^k(H) \subseteq D^k(G)$. Si H es distinguido se tiene

$$D^k(G/H) = (HD^k(G))/H.$$

2.° Un grupo G se dice resoluble si tiene una sucesión normal cuyos grupos cociente sean abelianos.

Demostrar que G es resoluble si y sólo si existe un entero k tal que

$$D^k(G) = \{e\}.$$

Sea H un subgrupo distinguido de G. Demostrar que G es resoluble si y sólo si H y G/H lo son.

3.° Demostrar que todo grupo de orden p^a, p primo, es resoluble. (Razonar por recurrencia sobre el orden de G, tomando en cuenta el centro.)

21

1.° Se llama sucesión distinguida de un grupo G a una sucesión decreciente, $G_0 = G \supset G_1 \supset \ldots \supset G_n = \{e\}$ de subgrupos distinguidos de G. Una sucesión distinguida es principal si G_{i+1} es maximal en el conjunto de subgrupos distinguidos de G contenidos estrictamente en G_i.

Demostrar que estas sucesiones tienen propiedades análogas a las enunciadas en los teoremas de Schreier y Jordan Hölder.

2.° Sea G un grupo finito resoluble (ejercicio IV, 20). Dar la estructura de los grupos cocientes de una sucesión de composición de G y de una sucesión principal de G. (Utilizar el ejercicio III, 37.)

22*

1.° Sea G un grupo finito resoluble (ejercicios IV, 20 y IV, 21), de orden $N = np^a$, $a > 0$, p primo, $p \nmid n$. Se pretende demostrar que G posee al menos un subgrupo cuyo índice es una potencia de p (distinta de 1). Para esto se razonará por recurrencia sobre N, distinguiendo dos casos:

a) Si existe un subgrupo distinguido $H \neq \{e\}$ de G tal que p sea divisor del orden de G/H, se aplicará a G/H la hipótesis de recurrencia.

b) Si no existe un tal subgrupo, demostrar que G posee un subgrupo distinguido mínimo H diferente de $\{e\}$. ¿Cuál es su orden? Sea un subgrupo distinguido minimal N/H de G/H. Demostrar que su orden es q^β, donde q es un número primo, $q \neq p$. Se designa por C un q-subgrupo de Sylow de N. Demostrar que $CH = N$, $C \cap H = \{e\}$. Deducir que si K es el normalizador de C en G se tiene $KH = G$, y que el índice de K es una potencia de p.

2.° Deducir que un grupo resoluble de orden mn, con m y n primos entre sí, tiene al menos un subgrupo de orden n.

23

Un grupo G se dice completamente reducible si es producto directo de una familia $\{G_i\}_{i \in I}$ de subgrupos distinguidos simples.

1.° Sea H un subgrupo distinguido de un grupo G completamente reducible. Demostrar que H es factor directo de G (es decir, que existe un subgrupo H' tal, que G es producto directo de H y H'). Para esto se puede considerar el conjunto de partes J de I tales, que la intersección de H y del subgrupo engendrado por la familia $\{G_i\}_{i \in J}$ se reduce al elemento neutro; se demostrará que esta familia es inductiva.

Deducir que H es completamente reducible.

2.° Sea G un grupo producto directo de dos familias finitas de subgrupos simples $\{G_i\}_{i \in I}$, $\{H_l\}_{l \in L}$. Demostrar que I y L tienen el mismo número de elementos y que los grupos G_i y H_l son isomorfos dos a dos.

24*

El grupo abeliano G se dice inyectivo si, cualquiera que sea el grupo abeliano H, todo homomorfismo de un subgrupo N de H en G se prolonga en un homomorfismo de H en G.

Todos los grupos que vamos a considerar en lo sucesivo, serán abelianos y con notación aditiva.

1.° *a*) Demostrar que si G es inyectivo, para todo entero $n > 0$ y todo $a \in G$, existe $b \in G$ tal que $a = nb$.

b) Recíprocamente, supongamos que G verifica esta condición. Sean N un subgrupo de un grupo H, f un homomorfismo de N en G. Sea $\mathcal{C}$ el conjunto de pares (N_i, f_i), donde N_i es un subgrupo de H que contiene a N y f_i es un homomorfismo de N_i en G que prolonga f. Se ordena $\mathcal{C}$ por

$$(N_i, f_i) \prec (N_j f_j) \Leftrightarrow N_i \subseteq N_j \quad \text{y} \quad f_j \quad \text{prolonga} \quad f_i.$$

Demostrar que $\mathcal{H}$ admite un elemento maximal. Deducir que G es inyectivo.

c) Sea G un subgrupo inyectivo de un grupo H. Demostrar que existe un subgrupo G' de H tal que H sea suma directa de G y G'.

2.° Sea G un grupo inyectivo. Si $x_0 \in G$ tiene por orden una potencia de un número primo p, se define por recurrencia una sucesión (x_k) de elementos de G,

$$x_k = px_{k+1}, \quad \text{para todo entero } k \geqslant 0.$$

Demostrar que el subgrupo de G engendrado por la sucesión (x_k) es isomorfo al grupo U_p estudiado en el ejercicio III, 38.

3.° Un grupo abeliano se dice indescomponible si no es suma directa de dos subgrupos propios.

Demostrar que un grupo inyectivo indescomponible es isomorfo, sea a $\boldsymbol{Q}$, sea a un grupo U_p.

4.° Demostrar que todo grupo inyectivo es suma directa de subgrupos inyectivos e indescomponibles. (Aplicar el axioma de Zorn a las familias de subgrupos inyectivos indescomponibles cuya suma es directa.)

25

Encontrar todos los grupos abelianos de orden 8. Enumerar todos los elementos de orden 2 en cada uno de estos grupos.

26

Sea G un grupo abeliano de orden p^m. Se supone que G es suma directa de t grupos cíclicos. Demostrar que el subgrupo H de G constituido por 0 y los elementos de orden p, tiene por orden p^t. ¿Cuál es su descomposición en suma directa de grupos cíclicos?

27*

Diremos que un grupo G es un grupo monógeno generalizado si dos elementos cualesquiera de G engendran un subgrupo monógeno.

1.° Demostrar que si G es monógeno generalizado, entonces el retículo $T(G)$ de sus subgrupos es distributivo.

2.° Suponemos que el retículo $T(G)$ de los subgrupos de G es distributivo. Siendo a y b dos elementos de G, consideremos los subgrupos monógenos engendrados por a, por b y por ab. Sean, $A = (a)$, $B = (b)$, $C = (ab)$.

a) Demostrar que $A \cap C$ y $B \cap C$ están engendrados por elementos a^r y b^s, respectivamente, que conmutan.

b) Demostrar que existen enteros m y n tales que $a^{mr-1} = b^{1-ns}$.

c) Deducir que a conmuta con b^s, y también con b.

d) Sea H el grupo engendrado por a y b. H es abeliano y de tipo finito. Por consiguiente se descompone en producto directo de subgrupos monógenos infinitos, o p-primarios (p primo). Demostrar que no pueden existir dos componentes de orden infinito, ni dos componentes p-primarias (con el mismo número primo p). (Razónese por reducción al absurdo, estableciendo que en cada caso resulta que $T(H)$ no es distributivo.) Demostrar que no pueden existir a la vez un componente de orden infinito y otro finito. Deducir que H es monógeno.

28

Sea G el grupo libre engendrado por M. Todo $x \in G$ se escribe

$$x = \prod_{i=1}^{n} m_i^{k_i}, \quad \text{donde} \quad m_i \in M, \quad k_i \in \mathbf{Z}.$$

Dado $a \in M$ se denota por $d_a(x)$ el número entero

$$d_a(x) = \sum_{i, m_i = a} k_i.$$

1.° Se considera la relación R definida en G por

$$xRy \Leftrightarrow d_a(x) \equiv d_a(y)\ (n),$$

donde n es un entero dado.

Demostrar que R es una equivalencia regular en G. Sean E la clase unidad, G' el grupo engendrado por $M - \{a\}$. Demostrar que $G' \subseteq E$. ¿Puede ser $G' = E$? ¿Es G' distinguido en G? ¿De qué naturaleza es el grupo cociente G/E?

2.° Sea φ una aplicación de M en $\mathbf{Z}$. Consideremos la relación S definida en G por

$$xSy \Leftrightarrow \{ \forall a \in M,\ d_a(x) \equiv d_a(y)\ (\varphi(a)) \}.$$

Demostrar que S es una equivalencia regular. ¿De qué naturaleza es el grupo cociente G/S? ¿En qué caso este grupo es finito, o de tipo finito, o abeliano libre?

Soluciones

1

Haremos operar a G sobre el conjunto $\mathcal{H}$ de los conjugados de H por los automorfismos internos. Si H_i es un conjugado de H, pondremos, para $g \in G$:

$$g * H_i = g H_i g^{-1}.$$

G opera transitivamente sobre $\mathcal{H}$. El número de elementos de $\mathcal{H}$ es, pues, el índice en G del estabilizador de H (texto: II, 6. Espacios homogéneos). Ahora bien, el estabilizador de H es aquí su normalizador

$$N = \{ x;\ xHx^{-1} = H \}.$$

Supongamos que H no es distinguido en G.

Si se tuviese $G = \bigcup_{H_i \in \mathcal{H}} H_i$, puesto que los H_i son isomorfos a H, y tienen por lo menos un elemento común, debería tenerse

$$O(G) < O(H)\, i(N) \leqslant O(H)\, i(H) = O(G),$$

lo que es absurdo.

Si H es distinguido en G, entonces

$$\bigcup_{H_i \in \mathcal{H}} H_i = H.$$

Se deduce igualmente del resultado anterior, y de los teoremas de Sylow, que el número de p-subgrupos de Sylow es el índice del normalizador de uno de ellos, luego es divisor del orden de G.

2

Sea Z el centro de G.

G opera sobre H por los automorfismos internos. Consideremos las clases de transitividad. Una clase se reduce a un elemento si y sólo si este elemento pertenece a $H \cap Z$, si no, su cardinal es una potencia de p superior a 1.

Se tiene pues,

$$O(H) = O(H \cap Z) + \sum p^{\alpha l}$$

que demuestra que p divide a $O(H \cap Z)$ y, por lo tanto, $H \cap Z \neq \{e\}$.

Esta demostración es análoga a la que establece que Z es mayor que $\{e\}$ (texto: II, 6. Aplicación 1).

3

Designemos por Γ el grupo de biyecciones de S. Se define una aplicación φ de G en Γ asociando a $x \in G$ la traslación a la izquierda γ_x de S:

$$\gamma_x(aH) = xaH.$$

Se comprueba fácilmente

$$\gamma_x \circ \gamma_y = \gamma_{xy}.$$

φ es, pues, un homomorfismo de G en Γ.

El núcleo N de φ es distinguido en G;

$$N = \{x;\ xaH = aH, \quad \forall a \in G\}.$$

La relación $xaH = aH$ se puede escribir

$$x(aHa^{-1}) = aHa^{-1}$$

y equivale a $x \in aHa^{-1}$.

Se tiene pues

$$N = \bigcap_{a \in G} (aHa^{-1}).$$

N está contenido en H, y si K es un subgrupo de H distinguido en G se tiene

$$K = aKa^{-1} \subseteq aHa^{-1}, \quad \forall a \in G,$$

de donde: $K \subseteq N$.

Por tanto, N es el mayor subgrupo de H distinguido en G.

Supongamos G finito; si H no tiene ningún subgrupo propio distinguido en G, entonces $N = \{ e \}$ y $\varphi(G)$ es isomorfo a G. Luego, el orden de G divide al orden de Γ que es $i(H)!$

4

Si $a \in G$ es un elemento cuya clase engendra G/H, todo elemento $g \in G$ puede escribirse

$$g = a^k h, \quad \text{donde } h \in H.$$

Si $g' = a^k h'$, puesto que h y h' están en el centro, se puede escribir

$$gg' = a^k h\, a^k h' = a^{k+k'} hh',$$
$$g'g = a^{k+k'} h'\, h = a^{k+k'} hh' = gg'.$$

Si G es de orden p^a y no abeliano, su centro Z, que es abeliano, es distinto de G. Si el índice de Z fuese igual a p, el grupo cociente G/Z sería cíclico, pues su orden es p, y según lo que precede G sería abeliano. Luego el índice de Z es por lo menos p^2.

Esto demuestra que un grupo de orden p^2 no abeliano, tiene su centro reducido al elemento neutro. Ahora bien, esto contradice un conocido resultado teórico (texto: II, 6, aplicación 1). Por consiguiente todo grupo de orden p^2 es abeliano.

5

Si G es de orden p^2 su centro es de orden p o p^2. Si Z es de orden p, sea $a \notin Z$. El normalizador $N(a)$ de a, contiene a Z y a, luego es G. Lo mismo, si $a \in Z$, $N(a) = G$. Ahora, $Z = \bigcap_{a \in G} N(a)$ lleva a una contradicción. Por lo tanto $Z = G$, luego G es abeliano.

6

Supongamos $N = H$. El número de conjugados de H, que es el índice de N en G es, pues, mp^{r-a}.

H opera sobre $\mathcal{H}$ por los automorfismos internos. Como H permanece invariante su clase de transitividad se reduce a él mismo. Si $H_i \in \mathcal{H}$, $H_i \neq H$, no permanece H_i invariante, pues si eso fuese su normalizador contendría a H y sería estrictamente mayor que H_i; como H y H_i son conjugados, la

misma propiedad se verificaría con H, contradiciendo $N = H$. La clase de transitividad de H_i no se reduce a H_i luego el número de sus elementos es de la forma p^{α_i}, ya que divide al orden de H.

Sumando el número de elementos de todas las clases resulta

$$mp^{r-\alpha} = 1 + \sum p^{\alpha_i},$$

lo que es absurdo, porque $r - \alpha > 0$, $\alpha_i > 0$. Se tiene, pues, $H \subset N$.

Si G es un grupo de orden p^r, tomando $\alpha = r - 1$ vemos que el normalizador de un subgrupo de orden p^{r-1} es igual a G, y que un subgrupo de orden p^{r-1} es distinguido.

Sea G un grupo de orden p^2. Si existe un elemento de G de orden p^2, G es cíclico, luego abeliano. Si no, todo $x \in G$, $x \neq e$, engendra un subgrupo de orden p que es por tanto distinguido en G. Sean $a \in G$, $a \neq e$ y $b \notin (a)$. Se tiene $(b) \cap (a) = \{ e \}$, pues es un subgrupo de (a) y (b). Además $(b)\,(a)$, producto directo de (b) y (a), tiene p^2 elementos, luego es igual a G. G es abeliano ya que a y b conmutan.

7

1.° Sea q un divisor primo del orden de G. Según los teoremas de Sylow, G tiene un elemento de orden q. Por consiguiente $q = p$ y el orden de G es una potencia de p.

Si K es un subgrupo distinguido de orden p, sea $a \in K$, $a \neq e$. El número de sus conjugados, que es el índice de su normalizador, es una potencia de p. Ahora, sus conjugados están en K y son distintos de e, luego hay como máximo $p - 1$. Finalmente, a no tiene más que un conjugado, y pertenece al centro.

2.° *a*) Se tiene $g \in KgK$, luego $G = \bigcup_{g \in G} KgK$.

Si $a \in KgK$, entonces $KaK \subseteq KgK$. Además, $a = k_1 g k_2$ implica

$$g = k_1^{-1} a k_2^{-1} \in KaK \quad \text{y} \quad KgK = KaK.$$

Por consiguiente, si $a \in (KgK) \cap (KhK)$, entonces

$$KgK = KaK = KhK.$$

Los conjuntos distintos KgK forman, pues, una partición de G. KgK es la unión de clases a la izquierda uK, $u \in Kg$.

Sea $\mathcal{C}$ el conjunto de clases a la izquierda contenidas en KgK. Sea φ la aplicación de K sobre $\mathcal{C}$ definida por: $\varphi(k) = kgK$. La equivalencia $\mathcal{R}$

sobre K asociada a φ, es regular a la izquierda, pues si $\varphi(k_1) = \varphi(k_2)$, entonces $\varphi(kk_1) = \varphi(kk_2)$. Por tanto $\mathcal{E}$, que está en biyección con $K/\mathcal{R}$, tiene un número de elementos igual al índice en K de la clase módulo $\mathcal{R}$ de e. Ahora bien, $k \equiv e(\mathcal{H})$ equivale a $kgK = gK$, que se escribe

$$k(gKg^{-1}) = gKg^{-1},$$

es decir, $k \in gKg^{-1}$; $\mu(KgK)$ es, pues, el índice en K de $(gKg^{-1}) \cap K$.

Entonces son equivalentes las siguientes relaciones:

$$\mu(KgK) = 1, \quad K = K \cap (gKg^{-1}), \quad gKg^{-1} = K, \quad g \in N.$$

Si el orden de K es p^i, $\mu(KgK)$ es una potencia de p igual a 1 si y sólo si $g \in N$. Contando las clases a la izquierda según K obtenemos

$$[G : K] = [N : K] + \sum_{g \notin N} \mu(KgK).$$

Ahora bien $[G : k]$ es divisible por p; por consiguiente $[N : K]$ es divisible por p y $N \neq K$.

b) Si K es de orden p^i, G de orden p^r, $i < r$, N/K cuyo orden es una potencia de p posee un subgrupo T' de orden p. Sea T la imagen recíproca de T' en N; T contiene a K, y su orden es p^{i+1} pues $T' \simeq T/K$. K es distinguido en T, ya que lo es en N.

En particular los grupos con orden expresado por p^{r-1} son distinguidos en G.

8

1.° Sea $x \in G$ de orden mn. Según la identidad de Bezout existen λ y μ tales que $1 = \lambda m + \mu n$. Poniendo $x^{\lambda m} = y$, $x^{\mu n} = z$, se tiene $x = yz = zy$. Designemos por s y t los órdenes de y y de z. Resulta $y^n = x^{\lambda m \cdot n} = e$, luego s es divisor de n; del mismo modo t es divisor de m. Si $s < n$ se tiene $st < mn$ y $x^{st} = (yz)^{st} = e$, lo que es absurdo puesto que el orden de x es mn. Por consiguiente, $s = n$, $t = m$.

Se deduce fácilmente por recurrencia, que un elemento x de orden $p_1^{\alpha_1} \dots p_n^{\alpha_n}$, donde los p_i son primos y distintos, se escribe $x = x_1 \dots x_n$, donde x_i es de orden $p_i^{\alpha_i}$. Por tanto x_i pertenece a un p_i-subgrupo de Sylow. Por consiguiente G es el producto de sus subgrupos de Sylow.

2.° Sean P un subgrupo de Sylow, N el normalizador de P, K el normalizador de N.

Para todo $g \in K$ es

$$gPg^{-1} \subseteq gNg^{-1} = N.$$

gPg^{-1} es un subgrupo de Sylow de N. Como los subgrupos de Sylow de N son conjugados en N, existe $n \in N$ tal que

$$gPg^{-1} = nPn^{-1},$$

de donde

$$(n^{-1}g)\, P(n^{-1}g)^{-1} = P, \quad \text{y} \quad n^{-1}g \in N.$$

Se tiene por tanto $g \in N$, luego $K = N$.

3.° Según lo 2.°, la hipótesis sobre G implica que el normalizador de todo subgrupo de Sylow es igual a G, o dicho de otro modo, estos subgrupos son distinguidos. Para cada número primo p_i divisor del orden de G, hay un único p_i-subgrupo de Sylow, P_i. Tendremos

$$P_i \cap \left(\coprod_{j \neq i} P_j \right) = \{e\}$$

pues los órdenes de los P_i son primos entre sí. G es pues el producto directo de sus subgrupos de Sylow.

9

1.° Sean H un subgrupo de G, K un p-subgrupo de Sylow de H. Según los teoremas de Sylow, K está contenido en un p-subgrupo de Sylow S de G. Por ser S cíclico también lo es K, y H es hipercíclico.

Si el orden de G es $p_1^{a_1} \dots p_k^{a_k} = n$ (donde los p_i son números primos distintos), G tiene al menos un elemento a_i de orden $p_i^{a_i}$, generador de un p_i-subgrupo de Sylow. Si G es abeliano el elemento $a_1 \dots a_k$ es de orden n (ejercicio II, 17) y engendra G, que por tanto es cíclico.

Sean H y H' dos subgrupos de orden p^a. Éstos están respectivamente contenidos en dos p-subgrupos de Sylow S y S' de G. Los subgrupos S y S' son conjugados. El automorfismo interno que transforma S en S' transforma H en un subgrupo de orden p^a de S', que necesariamente debe ser H', pues un grupo cíclico posee un solo subgrupo de un orden dado. H y H' son, pues, conjugados.

2.° Denotaremos con $a \cup b$ y $a \cap b$ respectivamente el m.c.m. y el m.c.d. de dos números enteros a y b.

$O(N \cap H)$ es divisor de $O(H)$ y de $O(N)$, por lo que también será divisor de $O(H) \cap O(N)$.

Si

$$O(H) \cap O(N) = p_1^{a_1} \dots p_k^{a_k},$$

será $p_i^{a_i}$ divisor de $O(H)$ y de $O(N)$. Existen dos subgrupos N' y H' de N y H con orden $p_i^{a_i}$. Ambos serán conjugados, según lo 1.°. Por ser N distinguido, H' está contenido en N, luego también en $N \cap H$, de modo que $p_i^{a_i}$ es divisor de $O(N \cap H)$. Resulta en fin,

$$O(N \cap H) = O(N) \cap O(H).$$

Como N es distinguido se tiene el isomorfismo

$$NH/N \simeq H/N \cap H,$$

de donde

$$O(NH) = \frac{O(N)\,O(H)}{O(N \cap H)} = \frac{O(N)\,O(H)}{O(N) \cap O(H)} = O(N) \cup O(H).$$

3.° Sea α un automorfismo de G. El orden de $\alpha(N)$ es el mismo que el orden de N. Lo visto en el punto 2.° implica que $\alpha(N) \cap N$ tiene el mismo orden que N y, por consiguiente, $\alpha(N) = N$.

10

1.° El orden de $N \cap S$ es una potencia de p. Por tanto, $N \cap S$ está contenido en un p-subgrupo de Sylow S' de N. Como el orden de S' es una potencia de p, está S' contenido en un p-subgrupo de Sylow S'' de G. Por ser conjugados S y S'' existe un $x \in G$ tal que $xS''x^{-1} = S$. Por consiguiente $xS'x^{-1} \subseteq S$. Como N es distinguido se tiene también $xS'x^{-1} \subseteq N$ y por tanto $xS'x^{-1} \subseteq N \cap S$. Ahora bien, $xS'x^{-1}$ es también un p-subgrupo de Sylow de N, pues su orden es igual al de S'. Se tiene pues $N \cap S = xS'x^{-1}$, y $N \cap S$ es un p-subgrupo de Sylow de N.

Pongamos

$$O(G) = mp^r,\ p \nmid m, \qquad O(N) = np^k,\ p \nmid n, \qquad n \mid m,\ k < r.$$

El segundo teorema de isomorfismo nos da

$$NS/N \simeq S/S \cap N.$$

Acabamos de ver que $O(S \cap N) = p^k$, y tenemos

$$O(NS/N) = O(S/S \cap N) = p^{r-k}.$$

Ahora, la más alta potencia de p que divide a $O(G/N)$ es p^{r-k}. Luego NS/N es un p-subgrupo de Sylow de G/N. Advirtamos que es la imagen de S en G/N.

2.° Designemos con φ la aplicación canónica $G \to G/N$. Se trata de demostrar

$$\mathcal{N}(\varphi(S)) = \varphi(\mathcal{N}(S)).$$

Puesto que S es distinguido en $\mathcal{N}(S)$, $\varphi(S)$ lo es en $\varphi(\mathcal{N}(S))$ y se tiene

$$\varphi(\mathcal{N}(S)) \subseteq \mathcal{N}(\varphi(S)) \quad \text{(Ejerc. III, 31).}$$

Sea $\varphi(x) \in \mathcal{N}(\varphi(S))$. Se tiene

$$\varphi(xSx^{-1}) = \varphi(x)\,\varphi(S)\,\varphi(x^{-1}) = \varphi(S)$$

y por consiguiente

$$xSx^{-1} \subseteq \varphi^{-1}(\varphi(S)) = NS.$$

Los dos p-subgrupos de Sylow S y xSx^{-1} son también p-subgrupos de Sylow de NS, y son conjugados en NS. Existen, pues, $n \in N$, $s \in S$, tales que

$$xSx^{-1} = nsSs^{-1}n^{-1} = nSn^{-1}.$$

Se deduce,

$$(n^{-1}x)\,S(n^{-1}x)^{-1} = S, \quad \text{y} \quad n^{-1}x \in \mathcal{N}(S).$$

Entonces,

$$\varphi(x) = \varphi(n^{-1}x) \in \varphi(\mathcal{N}(S)),$$

y se tiene la igualdad buscada.

Demostremos la inclusión

$$\mathcal{N}(S) \subseteq \mathcal{N}(S \cap N).$$

Si $x \in \mathcal{N}(S)$ se tiene $xSx^{-1} = S$, $xNx^{-1} = N$ y en fin, $x(S \cap N)x^{-1} = S \cap N$.

El segundo teorema de isomorfismo permite escribir

$$\frac{\mathcal{N}(S \cap N)}{N \cap \mathcal{N}(S \cap N)} \simeq \frac{N\mathcal{N}(S \cap N)}{N}.$$

Falta demostrar que

$$N\mathcal{N}(S \cap N) = G.$$

Sea $g \in G$; $g(N \cap S)g^{-1}$ es un p-subgrupo de Sylow de N, luego es conjugado en N de $N \cap S$. Existe pues un $n \in N$ tal que

$$N \cap S = ng(N \cap S)g^{-1}n^{-1}.$$

Esta igualdad demuestra que ng pertenece a $\mathcal{N}(N \cap S)$ y $g \in N\mathcal{N}(N \cap S)$.

11

1.° Sea $\{P_i\}_{i \in I}$ el conjunto de los p-subgrupos de Sylow de G. Todo automorfismo interno α de G realiza una biyección de los p-subgrupos de Sylow de G sobre los de $\alpha(G) = G$. Se tiene pues

$$\alpha\left(\bigcap_{i \in I} P_i\right) = \bigcap_{i \in I} \alpha(P_i) = \bigcap_{i \in I} P_i = D.$$

D es pues un subgrupo distinguido de G. Es un p-subgrupo, porque está contenido en cada P_i.

Sea N un p-subgrupo distinguido de G. Según los teoremas de Sylow, existe $i \in I$ tal que $N \subseteq P_i$. Cualquiera sea $j \in I$ existe $g \in G$ tal que

$$gP_i g^{-1} = P_j.$$

Entonces se tiene

$$N = gNg^{-1} \subseteq gP_i g^{-1} = P_j,$$

de donde resulta $N \subseteq D$, y D es efectivamente el mayor p-subgrupo distinguido de G.

2.° Supongamos la propiedad enunciada válida para todo grupo G' cuyo orden sea estrictamente inferior al de G.

a) Si $D \neq \{e\}$, sean $G' = G/D$ y $\varphi : G \to G'$. Se sabe que φ establece una biyección entre los subgrupos de G que contienen a D y los subgrupos

de G'. Si K es un p-subgrupo de G que contiene a D, entonces $\varphi(K) = K/D$ es evidentemente un p-subgrupo de G'. Recíprocamente, si K' es un p-subgrupo de G', entonces $K = \varphi^{-1}(K')$ es tal que $K/D = K'$ y por tanto se tiene: $O(K) = O(K')\,O(D)$, que demuestra que K es un p-subgrupo de G. Por tanto, φ establece un isomorfismo del conjunto ordenado de los p-subgrupos de G que contienen a D, sobre el de los p-subgrupos de G'. Puesto que los p-subgrupos de Sylow de G contienen a D, se corresponden con los p-subgrupos de Sylow de G'.

Resulta de esto que los p-subgrupos de Sylow de G', que son los $\varphi(P_i)$, son abelianos, y G' satisface la hipótesis de recurrencia. Existe, pues, P^* tal que

$$\varphi(P) \cap \varphi(P^*) = \cap\, \varphi(P_i) = \varphi(\cap\, P_i) = \varphi(D),$$

es decir, $P \cap P^* = D$.

b) Si $D = \{e\}$ se pueden encontrar conjugados $P_1, \ldots, P_r$ de P tales que

$$P \cap P_1 \cap \ldots \cap P_r = \{e\}, \quad P \cap \ldots \cap P_{r-1} = T \neq \{e\} \text{ si } r > 1,$$

suprimiendo, si es necesario, algunos P_i.

Es claro que $P, P_1, \ldots, P_{r-1}$, son p-subgrupos de Sylow de H, luego T contiene la intersección de los p-subgrupos de Sylow de H. Si se demuestra que T es distinguido, la igualdad resultará de lo 1.°. Ahora bien, siendo abelianos $P, P_1, \ldots, P_{r-1}$, todo elemento de T permuta con cada uno de sus elementos, luego también con cada elemento del grupo que ellos engendran.

Resulta que $P_r \nsubseteq H$, pues si no la intersección de los p-subgrupos de Sylow de H se reduciría a $\{e\}$ y, por consiguiente, $H \neq G$.

$H \cap P_r$ es un p-subgrupo de H; está contenido en un p-subgrupo de Sylow R de H. La hipótesis de recurrencia prueba que existe un conjugado R^* de R tal que $R \cap R^* = T$.

Puede escribirse

$$R^* \cap P_r = R^* \cap H \cap P_r \subseteq R^* \cap R = T$$

y por consiguiente

$$R^* \cap P_r = R^* \cap P_r \cap T = \{e\}.$$

Existe un automorfismo interno α de H tal que $P_r = \alpha(P)$. Poniendo $P^* = \alpha^{-1}(R^*)$ se tiene inmediatamente

$$P \cap P^* = \{e\}\,.$$

12

Sea C el grupo conmutador de G, es decir, el grupo engendrado por los conmutadores $xyx^{-1}y^{-1}$ donde x e y recorren G. Se tiene desde luego $N \subseteq C$.

El grupo cociente G/N está engendrado por las clases $\overline{m}$ de los elementos $m \in M$. Si m_1 y m_2 están en M, puesto que $m_1 m_2 m_1^{-1} m_2^{-1} \in N$, resulta

$$\overline{m}_1 \overline{m}_2 = \overline{m}_2 \overline{m}_1;$$

Al ser G/N engendrado por elementos que conmutan dos a dos es abeliano y por tanto $C \subseteq N$ (texto: III, 1, Teor. 3) de donde $C = N$.

13

La relación $aba = b$ se escribe

$$ba = a^{-1} b.$$

Resulta fácilmente, por recurrencia sobre el entero k,

$$ba^k = a^{-k} b\,. \tag{1}$$

La relación $a^2 = b^2$ permite escribir

$$b^{2k} = a^{2k} \qquad b^{2k+1} = a^{2k} b.$$

Esto permite poner todo elemento $g \in G$ en la forma

$$g = a^{\alpha_1} b a^{\alpha_2} b \ldots a^{\alpha_n} b^{\beta_n}\,.$$

Razonando por recurrencia sobre n, teniendo en cuenta la relación (1), puede escribirse finalmente,

$$g = a^{\alpha} b^{\beta}, \quad 0 < \alpha < 4, \quad 0 < \beta < 1.$$

Por consiguiente G tiene a lo más 8 elementos distintos

$$e,\ a,\ a^2,\ a^3,\ b,\ ab = ba^3,\ a^2 b = ba^2,\ a^3 b = ba.$$

Pero no sabemos todavía si las relaciones impuestas no implicarán la igualdad de dos de tales elementos. Si logramos construir un grupo G' engendrado por dos elementos a' y b' satisfaciendo a las relaciones dadas, sabe-

mos (teorema de Van Dyck) que G' es imagen homomorfa de G. Nos bastará, pues, encontrar un grupo G' constituido por ocho elementos, pues entonces el homomorfismo sería un isomorfismo, y nuestra duda quedaría resuelta.

Para esto consideremos el subgrupo de S_8 engendrado por las permutaciones

$$a' = (1\ 2\ 3\ 4)\ (5\ 6\ 7\ 8), \quad b' = (1\ 5\ 3\ 7)\ (2\ 8\ 4\ 6).$$

Se verifica sin ninguna dificultad que se cumplen las relaciones

$$a'^4 = b'^4 = e' \quad b'^2 = a'^2 \quad a'\,b'\,a' = b'$$

y que las ocho permutaciones $a'^{\alpha}\,b'^{\beta}$ son distintas.

Busquemos el orden de los diferentes elementos de G.

$a^2 = b^2$ es de orden dos; todos los otros elementos, excepto e, tienen su cuadrado igual a a^2, luego son de orden cuatro.

El único subgrupo de orden dos es $\{ e, a^2 \}$. Por tanto éste es distinguido. Los subgrupos de orden cuatro son cíclicos. Éstos son

$$\{ e, a, a^2, a^3 \},\ \{ e, b, b^2, b^3 = a^2\,b \},\ \{ e, ab, (ab)^2 = a^2, (ab)^3 = a^3\,b \}.$$

Todos ellos contienen a $\{ e, a^2 \}$.

Verifiquemos que son distinguidos: Si $H = (c)$ es uno de ellos, es suficiente verificar que $aca^{-1} \in H$ y $bcb^{-1} \in H$, lo que es inmediato. También se puede utilizar el resultado del ejercicio IV, 6.

El grupo tratado suele llamarse « grupo de los cuaternios ».

14

El número de p-subgrupos de Sylow de G es de la forma $kp + 1$. Es también un divisor del orden pq de G (ejercicio IV, 1). Se tiene, pues, un solo p-subgrupo de Sylow que por tanto es distinguido. Éste es de orden p, luego es cíclico. Llamémosle A, poniendo $A = (a)$.

El número de q-subgrupos de Sylow es de la forma $kq + 1$, y divisor de pq. Si se tuviese $k \neq 0$, $kq + 1$ sería igual a p, y q dividiría a $p - 1$. Se tiene pues un q-subgrupo de Sylow único, luego es distinguido. También es cíclico, y lo indicaremos $B = (b)$.

Puesto que $A \cap B = \{ e \}$, AB es producto directo de A y B. Por consiguiente a y b conmutan, y ab es de orden pq (ejercicio III, 17), luego G es cíclico, engendrado por ab.

El grupo S_3 de permutaciones de 3 elementos es de orden 3×2 y no es abeliano.

Si G es abeliano posee un elemento x de orden p, un elemento y de orden q y el elemento xy es de orden pq; éste engendra a G.

15

1.° Puesto que G no es abeliano, q es divisor de $p - 1$ (ejercicio IV, 14).

Sea A el subgrupo distinguido de orden p, $A = (a)$; sea B un subgrupo de orden q: $B = (b)$. Por ser A distinguido, existe r tal que $bab^{-1} = a^r$. Para todo entero n se puede escribir

$$ba^n b^{-1} = (bab^{-1}) = a^{rn}. \tag{1}$$

Resulta,

$$b^2 a^n b^{-2} = b(ba^n b^{-1}) b^{-1} = ba^{rn} b^{-1} = a^{r^2 n}$$

y se prueba fácilmente, por recurrencia sobre k, que es

$$b^k a^n b^{-k} = a^{r^k n}.$$

Tomando $k = q$, $n = 1$, la relación deviene $a = a^{r^q}$, lo que demuestra $r^q \equiv 1(p)$.

No puede ser $r \equiv 1(p)$; de serlo a y b conmutarían, y G sería cíclico engendrado por ab.

2.° Sea G el grupo engendrado por a y b y sometido a las precedentes relaciones de definición. De esto se deduce la relación (1).

Entonces, $A = (a)$ es distinguido, y se tiene: $G = AB$, $B = (b)$. Todo $g \in G$ puede escribirse $a^x b^y$, donde se puede suponer $0 \leq x < p$, $0 \leq y < q$. Pero *a priori* no se puede afirmar que, por ejemplo, a sea de orden p. Se sabe que $a^p = e$, luego el orden de a divide a p. Las relaciones dadas podrían implicar $a = e$. Por el momento sólo estamos en condiciones de decir que G tiene a lo más pq elementos. Sabemos sin embargo que si un grupo Γ está engendrado por dos elementos α y β satisfaciendo las mismas relaciones dadas, entonces Γ es imagen homomorfa de G. Si hallamos un grupo Γ que tenga pq elementos, entonces el orden de Γ, inferior o igual al orden de G, nos dará, $O(G) = O(\Gamma) = pq$, y Γ será isomorfo a G.

El lector puede verificar que el grupo Γ propuesto en el enunciado está engendrado por $\alpha = (1, 0)$, $\beta = (0, 1)$, que estos elementos cumplen las relaciones $\alpha^p = (0, 0)$, $\beta^q = (0, 0)$, $\beta\alpha\beta^{-1} = \alpha^r$, y que Γ tiene pq elementos. También se ve que la aplicación $(x, y) \to a^x b^y$ es un homomorfismo de Γ sobre G.

Advirtamos que G no es el producto directo de A y B, aunque

$$A \cap B = \{e\},$$

y todo $g \in G$ se escriba de modo único $g = uv$, $u \in A$, $v \in B$. Pero B no es distinguido.

16

Supongamos que $G = \bigoplus_{i \in I} \mathbf{Z}a_i$, $a_i \in G$, y que cada a_i sea de orden infinito.

Sea $\mathcal{C}$ el grupo abeliano libre engendrado por I, que indicaremos aditivamente. Todo elemento $e \in \mathcal{C}$ se escribe de modo único como

$$e = n_1 i_1 + \ldots + n_k i_k,\ n_r \in \mathbf{Z},\ i_r \in I\,.$$

Se verifica fácilmente que la aplicación f de $\mathcal{C}$ en G definida por

$$f(e) = \sum_{i=1}^{k} n_r a_{i_r}$$

es un isomorfismo de $\mathcal{C}$ sobre G.

Indiquemos por $\mathbf{Z}^{[I]}$ el subgrupo aditivo de $\mathbf{Z}^I$ formado por las sucesiones $(n_1, \ldots, n_k, \ldots)$ donde todos los elementos son nulos salvo un número finito. Se comprueba con facilidad que $\mathbf{Z}^{[I]}$ es un subgrupo. Si a_i es la sucesión definida por $n_k = 0$, para $k \neq i$ y $n_i = 1$ se tiene,

$$\mathbf{Z}^{[I]} = \sum \mathbf{Z}a_i.$$

Así, un grupo abeliano libre engendrado por un conjunto I es isomorfo a $\mathbf{Z}^{[I]}$. En particular, todo grupo abeliano libre de rango n es isomorfo al grupo aditivo $\mathbf{Z}^n$.

17

El grupo aditivo $\mathbf{Q}$ es abeliano y sin torsión. Si fuese libre sería suma directa de subgrupos monógenos. Ahora bien, cualesquiera sean $\frac{r}{s}$ y $\frac{m}{n}$ en $\mathbf{Q}$, la intersección $\mathbf{Z}_{\frac{r}{s}} \cap \mathbf{Z}_{\frac{m}{n}}$ no se reduce a cero, puesto que contiene a rm.

18

1.° $\mathbf{Z}^2$ es un grupo abeliano libre de rango dos. Dos elementos $\alpha = (r, s)$ y $\beta = (u, v)$ forman una base si y sólo si engendran $\mathbf{Z}^2$, lo que equivale a la existencia de enteros x, y, z, t tales que

$$(1, 0) = x\alpha + y\beta, \quad (0, 1) = z\alpha + t\beta,$$

es decir,

$$\begin{cases} 1 = xr + yu & (1) \\ 0 = xs + yv & (2) \\ 0 = zr + tu & (3) \\ 1 = zs + tv & (4) \end{cases}$$

La relación (2) muestra que x divide a yv. Según (1), x e y son primos entre sí, luego x divide a v. Un razonamiento parecido demuestra que v divide a x y por consiguiente $x = \varepsilon_1 v$, $\varepsilon_1 = \pm 1$. Del mismo modo se demuestra que $y = -\varepsilon_1 s$. Las relaciones (3) y (4) llevan a $t = \varepsilon_2 r$, $z = -\varepsilon_2 u$. Llevándolas a (1) y (4) se obtiene

$$1 = \varepsilon_1 vr - \varepsilon_1 su, \quad 1 = -\varepsilon_2 us + \varepsilon_2 rv \tag{5}$$

que implican $\varepsilon_1 = \varepsilon_2$.

La relación (5) prueba que r y s son primos entre sí.

Recíprocamente, si r y s son primos entre sí, satisfacen una identidad de Bezout, que se puede escribir en la forma (5), y el elemento (u, v) forma con (r, s) una base de $\mathbf{Z}^2$; basta tomar

$$x = \varepsilon_1 v, \; y = -\varepsilon_1 s, \; t = \varepsilon_1 r, \; z = -\varepsilon_1 u,$$

para verificar las cuatro condiciones.

Por ejemplo $\alpha = (2, 3)$ puede completar una base con $\beta = (4, 3)$; también con $(7, 5)$, etc.

2.° El grupo abeliano engendrado por a y b, con la relación de definición $ma - nb = 0$ es, por definición, el cociente de $\mathbf{Z}^2$ por el subgrupo U engendrado por

$$m(1, 0) - n(0, 1) = (m, -n) = \gamma$$

(siendo a, b las respectivas clases de (1, 0) y (0, 1)). Sea d un m.c.d. de m y $-n$. Sea $m = m'\,d$, $-n = n'\,d$. Existen u y v tales que $1 = vm' - un'$ y hemos visto en lo 1.° que $\alpha = (m', n')$ y $\beta = (u, v)$ forman una base de $\mathbf{Z}^2$ y se tiene $\gamma = d\alpha$. (En este ejemplo volvemos a encontrar un resultado del texto: VIII, 6, teor. 2.) Entonces, $\mathbf{Z}^2/U$ es producto directo de grupos monógenos engendrados por las clases $\bar{\alpha}$ y $\bar{\beta}$, uno de orden d, el otro de orden infinito.

Por tanto G es suma directa de los grupos monógenos

$$\mathbf{Z}(m'\,a + n'\,b) \quad \text{y} \quad \mathbf{Z}(ua + vb).$$

Por ejemplo, si $m = 4$, $n = -6$,

$$G = \mathbf{Z}(2\,a + 3\,b) \oplus \mathbf{Z}(2\,a + b).$$

19

H es un grupo abeliano libre, pues está engendrado por una parte libre L. Sea $x_1, \ldots, x_k$ un sistema generador de G. Si $x_i \notin L$, $L \cup \{x_i\}$ no es libre. Existen, pues, enteros $n_i, \alpha_1, \ldots, \alpha_q$, y elementos $l_1, \ldots, l_q$ de L tales que

$$n_i\,x_i + \alpha_1\,l_1 + \ldots + \alpha_q\,l_q = 0.$$

No puede ser $n_i = 0$, pues L no sería libre. Se tiene pues $n_i\,x_i \in H$. Si $x_i \in H$ tomaremos $n_i = 1$. Si n es el m.c.m. de los n_i, entonces, para todo i, $nx_i \in H$ y, finalmente, $nx \in H$, $\forall x \in G$.

La aplicación $\varphi : \varphi(x) = nx$ es un homomorfismo de G en H. Es inyectiva, pues G es sin torsión. Luego G es isomorfo a un subgrupo de H. Ahora bien, se sabe que todo subgrupo de un grupo abeliano libre es un grupo abeliano libre. Tal es, pues, el caso para G.

No es forzosamente $G = H$, pues tomando $G = \mathbf{Z}$, $L = \{2\}$ es una parte libre maximal y $H = 2\mathbf{Z}$.

Puesto que G es de tipo finito, es suma directa de grupos monógenos, que aquí son infinitos, pues que G es sin torsión. G es pues un grupo abeliano libre, según el ejercicio IV, 16.

20

1.° Sea φ un homomorfismo de G en un grupo G'. La imagen por φ de un conmutador de G es un conmutador de G', y por consiguiente $\varphi(D(G)) \subseteq D(G')$. Si φ es suprayectiva se tiene la igualdad, pues todo conmutador $x'\,y'\,x'^{-1}\,y'^{-1}$ de G' es la imagen de un conmutador de G: $xyx^{-1}\,y^{-1}$, donde $\varphi(x) = x'$, $\varphi(y) = y'$.

Como hipótesis para la recurrencia suponemos que

$$\varphi(D^{k-1}(G)) \subseteq D^{k-1}(G').$$

Así, φ induce un homomorfismo de $D^{k-1}(G)$ en $D^{k-1}(G')$ y el resultado precedente permite escribir

$$\varphi(D^k(G)) = \varphi[D(D^{k-1}(G))] \subseteq D(D^{k-1}(G')) = D^k(G').$$

La igualdad se verifica cuando φ es suprayectiva.

En particular $D^k(G)$ es distinguido en G.

Sea H un subgrupo de G. Indicamos por i la aplicación idéntica $H \to G$. Se puede escribir

$$i(D^k(H)) = D^k(H) \subseteq D^k(G).$$

Si H es distinguido tomemos $G' = G/H$. $\varphi(D^k(G))$ no es otro que $(HD^k(G))/H$, que por tanto es igual a $D^k(G/H)$.

2.° Supongamos G resoluble. Existe una sucesión normal

$$G_0 = G \supset G_1 \supset \ldots \supset G_n = \{e\}$$

tal que G_i/G_{i+1} sea abeliano, es decir, $G_{i+1} \supseteq D(G_i)$. Se tiene sucesivamente

$$G_1 \supseteq D(G), \quad G_2 \supseteq D(G_1) \supseteq D^2(G).$$

Por recurrencia sobre k, se obtiene fácilmente

$$D^k(G) \subseteq G_k$$

y, por último, $D^n(G) = \{e\}$.

Recíprocamente, si existe k tal que $D^k(G) = \{e\}$, la sucesión

$$G \supset D(G) \supset \ldots \supset D^k(G) = \{e\}$$

es una sucesión normal cuyos grupos cocientes son abelianos.

Si H es un subgrupo de G la relación $D^k(H) \subseteq D^k(G)$ demuestra entonces que si G es resoluble, H lo es también. Si además H es distinguido, G/H es también resoluble, porque

$$D^k(G/H) = HD^k(G)/H.$$

Supongamos que H y G/H sean resolubles. Entonces existe n tal que

$$D^n(G/H) = HD^n(G)/H$$

se reduce a la clase unidad, es decir, $D^n(G) \subseteq H$. Existe m tal que

$$D^m(H) = \{e\}.$$

Se tiene entonces,

$$D^{m+n}(G) = D^m(D^n(G)) \subseteq D^m(H) = \{e\}$$

y G es resoluble.

3.° Demostremos por recurrencia sobre α que todo grupo de orden p^α es resoluble.

La propiedad es evidente para $\alpha = 0$.

Sea G un grupo de orden p^α, $\alpha > 0$. Sabemos que el centro Z de G es un subgrupo distinguido, distinto de $\{e\}$.

Si $G = Z$, entonces G es abeliano, luego resoluble.

Si $G \neq Z$, Z y G/Z satisfacen la hipótesis de recurrencia. Éstos son resolubles y por consiguiente G también lo es.

21

1.° Basta considerar G como un Δ-grupo, donde Δ es el conjunto de los automorfismos internos (texto: VIII, 1). Los teoremas de Schreier y Jordan Hölder permanecen válidos al reemplazar sucesión normal (respectivamente, de composición) por sucesión distinguida (resp., principal).

2.° Si G es finito y resoluble posee una sucesión normal (respectivamente, distinguida. A saber: la sucesión de los $D^k(G)$) cuyos grupos cocientes son abelianos. Siendo G finito esta sucesión admite una subdivisión que es una sucesión de composición (resp., principal). Los grupos cociente de esta sucesión son abelianos. En efecto, si G_i/G_{i+1} es abeliano, sean $G_i \supseteq H \supset K \supseteq G_{i+1}$, donde K es distinguido en H. Ahora, G_i/K es imagen homomorfa de G_i/G_{i+1} (recordemos que $G_i/K \simeq G_i/G_{i+1}/K/G_{i+1}$), luego es abeliano, y H/K es un subgrupo de G_i/K.

Cualquier otra serie de composición (respect., principal) tiene esta misma propiedad, según el Teorema de Jordan Hölder.

Si (G_i) es una sucesión de composición, G_i/G_{i+1} será un grupo simple abeliano, por lo que es cíclico de orden primo.

Si (G_i) es una sucesión principal, G_i/G_{i+1} es un grupo abeliano, que además es subgrupo distinguido minimal de G/G_{i+1}. Se ha visto (ejercicio III, 37)

que un grupo tal es producto directo de subgrupos simples, aquí abelianos, todos isomorfos. Luego G_i/G_{i+1} es isomorfo a un grupo del tipo $(Z/p)^k$, donde p es primo.

22

1.° Si G es de orden p la propiedad es evidente. Supongámosla verificada para todo grupo de orden inferior a N y divisible por p.

a) Si existe un subgrupo distinguido $H \neq \{e\}$, tal que p divida al orden de G/H, existe, según la hipótesis de recurrencia, un subgrupo N/H de G/H de índice p^γ, $\gamma > 0$. El índice de N en G es igual a p^γ.

b) Supongamos que no exista un subgrupo tal. Sea H un subgrupo distinguido minimal distinto de $\{e\}$. Existe una sucesión principal pasando por H, y puesto que H es distinguido minimal, $H = H/\{e\}$ es un cociente de esta sucesión. Por consiguiente (ejercicio III, 37) es producto directo de grupos cíclicos de orden r primo, y por tanto su orden es r^γ. Se tiene $p = r$ y $\gamma = \alpha$, pues p no divide al orden de G/H. Es H un p-subgrupo de Sylow de G; es distinguido, luego único. Resulta entonces que H es un subgrupo distinguido mínimo $\neq \{e\}$.

Sea N/H un subgrupo distinguido minimal de G/H. Puesto que G/H es resoluble, es N/H producto directo de grupos cíclicos de orden q primo, y $q \neq p$. El orden de N/H es pues q^β, y el de N es $p^\alpha q^\beta$. Si C es un q-subgrupo de Sylow de N su orden es q^β, de donde resulta $C \cap H = \{e\}$, y el orden de CH es $q^\beta p^\alpha$, es decir, $CH = N$.

Demostremos que $KH = G$. Sea $g \in G$. gCg^{-1} es un q-subgrupo de Sylow de N; es, pues, conjugado de C en N: $gCg^{-1} = nCn^{-1}$, con $n \in N$. Se deduce,

$$n^{-1}g \in K \quad \text{y} \quad g \in KH = KCH = KH.$$

El segundo teorema de isomorfismo

$$G/H = KH/H \simeq K/K \cap H$$

muestra que el índice de K en G es el cociente $O(H) : O(K \cap H)$, igual a una potencia de p. No puede ser $K = G$, si no C sería distinguido y contendría a H, contra la relación $C \cap H = \{e\}$.

2.° Razonaremos por recurrencia sobre el orden de G.

Si p es un número primo divisor de m, existe un subgrupo K de G de índice p^α, $\alpha > 0$. El orden de K es $m'n$ (donde $m = m'p^\alpha$) luego K posee un subgrupo de orden n.

23

1.° Sea G un grupo completamente reducible. Designemos G_J al subgrupo de G engendrado por la familia $\{G_i\}_{i\in J}$. G_J es el producto directo de sus subgrupos y es distinguido en G.

Sea H un subgrupo distinguido de G. Consideremos el conjunto $\mathcal{J}$ de partes $J \subseteq I$ tales que $G_J \cap H = \{e\}$. La familia $\mathcal{J}$ es inductiva pues si $\{J_a\}_{a\in A}$ es una cadena de $\mathcal{J}$, poniendo $J = \bigcup_{a\in A} J_a$ se tiene,

$$\{e\} = \bigcup_a (H \cap G_{J_a}) = H \cap \left(\bigcup_a G_{J_a}\right) = H \cap G_J.$$

Sea entonces J una parte maximal de $\mathcal{J}$. Demostremos que $G = HG_J$, y para esto demostraremos que para todo $i \in I$, $G_i \subset HG_J$. Basta tomar $i \in I - J$. Siendo G_i simple, $G_i \cap (HG_J)$ será, o igual a G_i o igual a $\{e\}$. Supongamos $G_i \cap (HG_J) = \{e\}$, y entonces $(G_iG_J) \cap H = \{e\}$, pues si $x_i x_J \in H$, $x_i \in HG_J$, de donde $x_i = e$ y $x_J = e$, ya que $G_J \cap H = \{e\}$. Resulta que $J \cup \{i\}$ está en $\mathcal{J}$, contradiciendo el que J sea maximal. Se tiene pues $G_i \cap (HG_J) = G_i$, y $G_i \subseteq HG_J$.

G es producto directo de H y G_J. Si $K = I - J$, también es G producto directo de G_K y G_J. Resulta que H es isomorfo a G_K y por consiguiente es completamente reducible.

2.° Supongamos $I = \{1, 2, ..., n\}$, $L = \{1, 2, ..., m\}$. Ponemos

$$G_i' = G_{i+1} \dots G_n \qquad 0 \leq i \leq n-1, \qquad G_n' = \{e\},$$
$$H_l' = H_{l+1} \dots H_m \qquad 0 \leq l \leq m-1, \qquad H_m' = \{e\}.$$

Se obtienen dos sucesiones normales de G, que son sucesiones de composición pues sus factores son isomorfos a los grupos simples G_i, H_l. Según el teorema de Jordan Hölder estas dos sucesiones son isomorfas: se tiene $m = n$ y los grupos G_i, H_l son isomorfos dos a dos.

24

1.° *a*) Sea G un grupo inyectivo. Sean $a \in G$, $n > 0$. Definimos un homomorfismo f de $\mathbf{Z}$ en G por $f(k) = ka$. Sea f^* su prolongación a $\mathbf{Q}$. Si $b = f^*(1/n)$, entonces

$$nb = nf^*\left(\frac{1}{n}\right) = f^*(1) = f(1) = a.$$

b) Sea $(N_i, f_i)_{i \in I}$, una cadena de $\mathcal{U}$. $N' = \bigcup_{i \in I} N_i$ es un subgrupo de H que contiene a N. Sea $x \in N'$; existe $i \in I$ tal que $x \in N_i$ y si $x \in N_j$ se tiene $f_i(x) = f_j(x)$. Pondremos $f'(x) = f_i(x)$. El par (N', f') es un mayorante en $\mathcal{U}$ de la familia (N_i, f_i). Luego $\mathcal{U}$ es inductivo. Ahora, $\mathcal{U}$ no es vacío, puesto que $(N, f) \in \mathcal{U}$, luego existe un elemento maximal $(N_0, f_0) \in \mathcal{U}$.

Si $N_0 \neq H$ sea $a \in H - N_0$. Consideremos $U = \{k,\ k \in \mathbf{Z},\ ka \in N_0\}$. Éste es un subgrupo de $\mathbf{Z}$, de la forma $n\mathbf{Z}$. Si $n \neq 0$ existe $b \in G$ tal que $nb = f_0(na)$. Si $n = 0$ eso es todavía cierto. Sea $x + ma \in N_0 + \mathbf{Z}a$. Si $x + ma = x' + m'a$, con $x,\ x' \in N_0$, se tiene $x - x' = (m' - m)a$, de donde

$$m' - m \in U \quad \text{y} \quad m' - m = kn.$$

Entonces se tiene sucesivamente

$$f_0(x - x') = f_0(kna) = knb = (m' - m)b,$$
$$f_0(x) + mb = f_0(x') + m'b.$$

Podemos, pues, poner

$$g(x + mb) = f_0(x) + mb.$$

Se comprueba fácilmente que g es un homomorfismo cuya restricción a N_0 es f_0. El par $(N_0 + \mathbf{Z}a, g)$ mayora estrictamente a $(N_0 f_0)$ lo que es absurdo.

Se tiene, pues, $N_0 = H$ y G es inyectivo.

c) Sea i la aplicación idéntica de G en G. Puesto que G es inyectivo, i se prolonga en una aplicación $\bar{i}$ de H en G. Sea G' el núcleo de $\bar{i}$.

Si $x \in G \cap G'$ se tiene $0 = \bar{i}(x) = i(x) = x$ y por tanto $G \cap G' = \{0\}$.

Todo elemento $x \in H$ se escribe

$$x = \bar{i}(x) + (x - \bar{i}(x)), \quad \text{donde} \quad \bar{i}(x) \in G \quad \text{y} \quad x - \bar{i}(x) \in G'.$$

Finalmente se tiene

$$H = G \oplus G'.$$

2.° Sea $x_0 \in G$ de orden p^l; entonces x_k es de orden p^{k+1} ya que $x_0 = p^k x_k$. Sea H el subgrupo engendrado por la sucesión (x_k). Consideremos los subgrupos

$$G_0 = (0), \quad G_1 = \mathbf{Z}p^{l-1}x_0, \ldots, G_{l-1} = \mathbf{Z}px_0, G_l = \mathbf{Z}x_0, \ldots, G_n = \mathbf{Z}x_{n-l}, \ldots$$

Estos subgrupos de H forman una sucesión creciente. G_n es de orden p^n y se tiene $H = \bigcup_{n \geqslant 0} G_n$. Mediante los resultados del ejercicio III, 38, vemos que H es isomorfo a U_p.

3.° Señalemos que $\mathbf{Q}$ es inyectivo; también es indescomponible pues dos subgrupos H y H' distintos de $\{0\}$ no tienen nunca la intersección reducida a $\{0\}$:

si $$\frac{r}{s} \in H, \frac{r'}{s'} \in H' \quad \text{entonces} \quad rr' \in H \cap H'.$$

El grupo U_p es inyectivo (ejercicio III, 38, 1.°). Es también indescomponible, puesto que sus subgrupos forman una cadena.

Sea G un grupo inyectivo e indescomponible.

Si G tiene algún elemento de orden finito hay también un elemento cuyo orden es potencia de un número primo p. Entonces, por lo 2.°, G tiene un subgrupo H isomorfo a U_p, luego inyectivo. Según lo 1.° c), H es factor directo de G y, puesto que G es indescomponible, $H = G$.

Si no, todo elemento de G, excepto el 0, es de orden infinito. Sea $x \neq 0$, $x \in G$. Cualquiera sea $\frac{r}{s} \in \mathbf{Q}$, existe $y \in G$ tal que $sy = rx$. Si $\frac{r}{s} = \frac{r'}{s'}$ y $s'y' = r'x$, entonces

$$ss'y = ss'y', \quad \text{de donde} \quad ss'(y - y') = 0,$$

e $y - y' = 0$, puesto que G es sin torsión. La aplicación $\frac{r}{s} \to y$ de $\mathbf{Q}$ en G es inyectiva, pues si $sy = rx$, $s'y = r'x$, entonces

$$r'sy = rs'y = rr'x,$$

de donde

$$rs' = r's \quad \text{y} \quad \frac{r}{s} = \frac{r'}{s'}.$$

Se comprueba fácilmente que es un homomorfismo. La imagen de $\mathbf{Q}$ es un subgrupo inyectivo de G, luego igual a G como antes. Entonces G es isomorfo a $\mathbf{Q}$.

Señalemos que hemos demostrado que todo grupo inyectivo contiene un subgrupo inyectivo indescomponible.

4.° Sea G un grupo inyectivo. Designemos por $\mathcal{M}$ el conjunto de familias de subgrupos inyectivos indescomponibles cuya suma es directa. Demos-

tremos que $\mathcal{H}$, ordenado por inclusión, es inductivo. Sean $\{ H_i \}_{i \in I_a}$ las familias, donde las I_a forman una cadena. Poniendo $I = \bigcup_a I_a$ basta demostrar que la suma de la familia $\{ H_i \}_{i \in I}$ es directa, es decir, que la relación

$$x_{i_1} + x_{i_2} + \ldots + x_{i_k} = 0, \quad \text{donde} \quad x_{i_n} \in H_{i_n}$$

implica

$$x_{i_1} = \ldots = x_{i_k} = 0.$$

Ahora bien, existe a tal que $i_1, \ldots, i_k$ pertenece a I_a y la suma de la familia $\{ H_i \}_{i \in I_a}$ es directa.

Sea $\{ H_i \}_{i \in J}$ una familia maximal en $\mathcal{H}$, $H = \bigoplus_{i \in J} H_i$. Es H inyectivo, puesto que lo es cada H_i. Si $H \neq G$, existe H' tal que $G = H \oplus H'$. Demostremos que H' es inyectivo. Sean $a' \in H'$, $n \in \mathbf{Z}$; existe $y \in G$ tal que $ny = a'$. Si $y = b + b'$, $b \in H$, $b' \in H'$, entonces

$$nb = a' - nb' \in H \cap H', \quad \text{de donde} \quad a' = nb'.$$

Puesto que H' es inyectivo, contiene un subgrupo H_j inyectivo e indescomponible, y la suma de la familia $\{ H_i \}_{i \in I} \cup \{ H_j \}$ es directa, contradiciendo la hipótesis.

Se tiene pues:

$$G = \bigoplus_{i \in I} H_i.$$

25

Todo grupo abeliano de orden 8 es de tipo finito, luego es suma directa de subgrupos monógenos cuyos órdenes son potencias de 2. Distingamos los diversos casos posibles.

1.° $G = \mathbf{Z}a$, a de orden 8. Entonces $4a$ es el único elemento de orden 2.

2.° $G = \mathbf{Z}a \oplus \mathbf{Z}b$, a de orden 4, b de orden 2. Los elementos de orden 2 son $2a$, b, $2a + b$.

3.° $G = \mathbf{Z}a \oplus \mathbf{Z}b \oplus \mathbf{Z}c$, a, b, c de orden 2. Todos los elementos no nulos de G son de orden 2.

26

Se tiene

$$G = \mathbf{Z}a_1 \oplus \ldots \oplus \mathbf{Z}a_t,$$

donde a_i es de orden p^{α_i}, con $\alpha_1 + \ldots + \alpha_t = m$. Todo $x \in G$ se escribe

$$x = \sum_{i=1}^{t} n_i a_i,$$

y el orden de x es el m.c.m. de los órdenes de los elementos $n_i a_i$. Para que x sea nulo, o de orden p, es necesario y suficiente que, para todo i, $n_i a_i$ sea nulo o de orden p. Los únicos elementos de orden p de $\mathbf{Z}a_i$ son los de $\mathbf{Z}a_i'$, donde $a_i' = p^{\alpha_i - 1} a_i$. Así vemos que

$$H = \mathbf{Z}a_1' \oplus \ldots \oplus \mathbf{Z}a_t'.$$

H es pues efectivamente de orden p^t.

27

1.° Si G es monógeno generalizado, es en particular abeliano, y la cota superior mínima de dos subgrupos es su producto. Para demostrar que $T(G)$ es distributivo, basta probar que para tres subgrupos cualesquiera se tiene

$$A \cap (BC) \subseteq (A \cap B)(A \cap C).$$

Sea $a = bc \in A \cap (BC)$, $a \in A$, $b \in B$, $c \in C$. El grupo engendrado por $\{a, b, c\}$ está contenido en un grupo monógeno. Ahora bien, el retículo de los subgrupos de un grupo monógeno es distributivo (ejercicio III, 24). Se tiene pues

$$a = bc \in (a) \cap ((b)(c)) = ((a) \cap (b))((a) \cap (c)) \subseteq (A \cap B)(A \cap C)$$

que concluye la demostración.

2.° Suponemos $T(G)$ distributivo.

a) $A \cap C$ es un subgrupo de A. Es pues monógeno, engendrado por a^r. Lo mismo, $B \cap C$ está engendrado por b^s. Además a^r y b^s están en C, luego conmutan.

b) Se tiene

$$ab \in (A \vee B) \cap C = (A \cap C) \vee (B \cap C) = (A \cap C)(B \cap C)$$

pues $A \cap C$ y $B \cap C$ conmutan, según *a*).

Resulta,

$$ab = (a^r)^m (b^s)^n,$$

y finalmente

$$a^{mr-1} = b^{1-ns}.$$

c) a conmuta con $a^r = b^s$, luego con b^{ns}. Además a es permutable con $a^{mr-1} = b^{1-ns}$, luego con $b = b^{1-ns} b^{ns}$.

d) Falta por demostrar que un grupo abeliano H de tipo finito tal que $T(H)$ sea distributivo es necesariamente monógeno.

Se sabe que un grupo abeliano de tipo finito, en notación multiplicativa, es producto directo de grupos monógenos

$$H = (a_1) \times (a_2) \times \ldots \times (a_n),$$

donde $a_1, \ldots, a_s$ son de órdenes infinitos, $a_{s+1}, \ldots, a_n$ de órdenes finitos, siendo a_i de orden $p_i^{\alpha_i}$, p_i primo.

α) Necesariamente es $s < 1$. Pues si fuesen a_1 y a_2 de orden infinito, resultaría

$$(a_1 a_2) \cap (a_1) = \{ e \} = (a_1 a_2) \cap (a_2),$$
$$(a_1 a_2)(a_1) = (a_1) \times (a_2) = (a_1 a_2)(a_2),$$

que contradice la distributividad de $T(H)$.

β) Con $i \neq j$ no puede ser

$$p_i = p_j \quad (\{ i, j \} \subseteq \{ s+1, \ldots, n \}).$$

Si no, los elementos $b_i = a_i^{p_i^{\alpha_i - 1}}$ y $b_j = a_j^{p_j^{\alpha_j - 1}}$ serían ambos de orden p_i, y entonces

$$(b_i b_j) \cap (b_i) = \{ e \} = (b_i b_j) \cap (b_j)$$
$$(b_i b_j)(b_i) = (b_i) \times (b_i) = (b_i b_j) \bullet (b_j)$$

que contradice la distributividad de $T(H)$.

Puesto que $p_{s+1}^{\alpha_{s+1}}, \ldots, p_n^{\alpha_n}$ son primos entre sí, el elemento $a = a_{s+1} \ldots a_n$ es de orden

$$n = p_{s+1}^{\alpha_{s+1}} \ldots p_n^{\alpha_n}, \quad \text{y} \quad (a_{s+1}) \times \ldots \times (a_n) = (a).$$

γ) Tres son hasta ahora los casos posibles:

$$H = (a_1), \quad H = (a), \quad \text{o } H = (a_1) \times (a).$$

Demostraremos que el último es imposible. En efecto, se tendría entonces

$$[(a_1^n)\,(a)] \cap (a_1) = (a_1) = [(a_1^n)\,(a)] \cap (aa_1),$$
$$[(a_1^n)\,(a)]\,(a_1) = H = [(a_1^n)\,(a)]\,(aa_1),$$

que contradice la distributividad de $T(H)$.

1.° La aplicación $d_a : x \to d_a(x)$ es claramente un homomorfismo de G sobre $\mathbf{Z}$. La imagen recíproca por d_a de la congruencia módulo n es precisamente R, que por consiguiente es una equivalencia regular. Se tiene $d_a(G') = 0$, de donde

$$G' \subseteq d_a^{-1}(0) \subseteq E.$$

Si $b \in M$, $b \neq a$, aba^{-1} está en E, pero no en G', así como a^n, si $n \neq 0$. Luego, si $E = G'$ resulta $n = 0$ y $M = \{ a \}$ y con estas condiciones $G' = \{ e \} = E$ (si convenimos en que el grupo engendrado por la parte vacía es $\{ e \}$). Sólo es G' distinguido cuando $M = \{ a \}$.

El segundo teorema de isomorfismo da

$$G/E \simeq \mathbf{Z}/(n).$$

2.° Denotemos por δ_a la aplicación de G sobre $\mathbf{Z}/\varphi(a)$. Se define un homomorfismo de G en $P = \prod_{a \in M} \mathbf{Z}/(\varphi(a))$, por

$$\delta(x) = (\delta_a(x))_{a \in M}$$

cuya equivalencia asociada es precisamente S. Entonces,

$$G/S \simeq \delta(G).$$

Para todo $x \in G$ se tiene $d_a(x) = 0$, salvo para un número finito de $a \in M$, luego también $\delta_a(x) = 0$.

Si $(\gamma_m)_{m \in M} \in P$, y si $\gamma_m = 0$ salvo para un número finito de $m \in M$, entonces

$$(\gamma_m) = \delta(x) \text{ donde } x = \prod_{\gamma_m \neq 0} m^{k_m},$$

donde k_m es representante de γ_m.

$\delta(G)$ es el subgrupo de P constituido por elementos de soporte finito.

Sea $P_a = \{(\gamma_m),\ \gamma_m = 0,\ \forall m \neq a\}$. Es un subgrupo de P isomorfo a $\mathbf{Z}/(\varphi(a))$, y se tiene

$$\delta(G) = \bigoplus_{a \in M} P_a.$$

Los generadores de P_a no nulos forman un sistema generador minimal de $\delta(G)$. Recordemos que en un grupo de tipo finito, todo sistema generador contiene un sistema generador finito.

Dicho esto, $\delta(G)$ será de tipo finito si y sólo si un número finito de P_a son no nulos, es decir, si $\varphi(a) = 1$, salvo para un número finito de $a \in M$.

Entonces G será finito si, además, $\varphi(a) \neq 0$, $\forall a \in M$.

G será un grupo abeliano libre si $\varphi(a) = 0$ o $\varphi(a) = 1$, para todo $a \in M$.

Se podría haber razonado directamente, señalando que la clase U de e módulo S contiene a los conmutadores. Luego G/S es efectivamente abeliano. Indicando con $\bar{x}$ la clase de x, se ve que $\bar{a}^{\varphi(a)} = \bar{e}$ y G/S es producto directo de subgrupos monógenos $\{(\bar{a})\}_{a \in M}$.

CAPÍTULO V

Anillos

En todo este capítulo los anillos que consideramos no son conmutativos ni tienen elemento unidad, salvo mención expresa de lo contrario.

Enunciados

1

Sea A un anillo no conmutativo.

1.° Consideremos los dos conjuntos, eventualmente vacíos,

$$E' = \{ e',\ e' \in A,\ (\forall x \in A)\ xe' = x \},$$
$$E'' = \{ e'',\ e'' \in A,\ (\forall x \in A)\ e'' x = x \}.$$

Si E' no es vacío, se asocia a cada elemento e' de E' la aplicación $\varphi_{e'}$ de A en A definida por

$$\varphi_{e'}(x) = e' x - x + e'.$$

Demostrar que $\varphi_{e'}(A) \subseteq E'$ y que la restricción de $\varphi_{e'}$ a E' es inyectiva. Estudiar el caso en que E' se reduce a un solo elemento. En el caso en que E' tiene al menos dos elementos, ver que existe un ideal bilátero I tal que E' sea una clase módulo I y que toda imagen homomorfa de A con elemento unidad (bilátera) sea imagen homomorfa del anillo cociente A/I.

2.° Se supone que A posea un elemento unidad e. A todo elemento a de A se asocian dos conjuntos, eventualmente vacíos,

$$S'_a = \{ x',\ x' \in A,\ ax' = e \}, \qquad S''_a = \{ x'',\ x'' \in A,\ x'' a = e \}.$$

Si S'_a no es vacío, se asocia a todo elemento s de S'_a la aplicación ψ_s de S'_a en A definida por

$$\psi_s(x) = xa - e + s.$$

Demostrar que $\psi_s(S'_a) \subseteq S'_a$ y que ψ_s es inyectiva. Estudiar el caso en que S'_a se reduce a un solo elemento. En el caso en que S'_a tiene al menos dos elementos, demostrar que es infinito. Dar un ejemplo.

3.° ¿En qué se convierten los resultados precedentes para un anillo A íntegro?

2

Todo anillo con un número finito de elementos, en el que existan un elemento a que no sea divisor de cero a la izquierda y un elemento b que no sea divisor de cero a la derecha, tiene un elemento unidad.

3

Sea A un anillo con un número finito de elementos. Si A tiene un elemento unidad e, todo elemento no divisor de cero a la izquierda pertenece al grupo de las unidades.

4

Si para todo elemento x de un anillo A el elemento $x^2 - x$ pertenece al centro de A, el anillo es conmutativo.

5

Sea A un anillo de característica no nula N. A cada entero natural m se asocia el conjunto I_m de los elementos x de A tales que $mx = 0$.

1.° Comprobar que I_m es un ideal bilátero de A, y que $I_m = I_d$, donde d es el m.c.d. de m y N.

2.° Suponemos $N = ab$, donde a y b son dos enteros naturales primos entre sí. Demostrar que A es isomorfo al anillo producto (texto: IV, 2) de sus subanillos I_a e I_b.

3.° Suponemos $N = p^\alpha$ (p primo, α entero natural). Demostrar que para todo entero natural β tal que $1 < \beta < \alpha$, existe al menos un elemento x de A que engendra un grupo cíclico aditivo de orden $\nu(x) = p^\beta$.

4.° Volviendo al caso general, donde N es un entero natural cualquiera, mostrar que, para todo divisor δ de N, existe al menos un elemento x de A que engendra un grupo cíclico aditivo de orden $\nu(x) = \delta$.

6

Sea A un anillo tal que para todo $x \in A$ existe un entero natural

$$n = n(x) > 1$$

tal que $x^n = x$. Se demuestra que tal anillo es necesariamente conmutativo.

1.° Verificar que 0 es el único elemento nilpotente de A.

2.° Demostrar que todo $x \in A$ engendra un grupo aditivo finito, cuyo orden $r(x)$ no es divisible por ningún cuadrado distinto de 1.

3.° Demostrar que la existencia de un elemento no divisor de cero implica la existencia de un elemento unidad.

7

Sean p un número primo, A un anillo de característica p.

1.° Demostrar que si A tiene un número finito de elementos, este número es una potencia de p.

2.° Demostrar que si A tiene p elementos y contiene al menos un producto no nulo, A es un cuerpo.

8

Utilizando los resultados de los ejercicios V, 5 y V, 7, demostrar que un anillo A que consta de $n = p_1 p_2 \dots p_k$ elementos ($p_1, \dots, p_k$ son números primos distintos) es conmutativo; y, si además, A tiene elemento unidad, es isomorfo al producto de k cuerpos.

9

Sea A un anillo con elemento unidad e. Suponemos que existe un entero natural $n > 1$ tal que todo elemento x de A satisface la condición $x^n = x$. Sea N la característica del anillo A y sean $p_1, \dots, p_s$ los factores primos de N.

1.° Aplicando los resultados de los ejercicios V, 6 y V, 7 al subanillo de A engendrado por e, demostrar que el entero $n - 1$ es múltiplo de los enteros $p_i - 1$ ($i = 1, 2, \dots, s$).

2.° Demostrar que si n es par, $N = 2$. En particular, demostrar que en el caso $n = 6$, A es un anillo de Boole (texto, V, 7).

10*

Sean A un anillo y σ un endomorfismo no nulo de A. Definimos en el conjunto de series formales sobre el anillo A una ley de composición * poniendo

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) * \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} p_n x^n$$

si

$$p_n = a_0 b_n + a_1 \sigma(b_{n-1}) + \ldots + a_k \sigma^k(b_{n-k}) + \ldots + a_n \sigma^n(b_0)$$

para todo entero natural n.

1.° Demostrar que el conjunto de las series formales sobre A, con la ley de adición habitual y multiplicación *, es un anillo S_σ, y que los polinomios de coeficientes en A constituyen un subanillo P_σ de S_σ.

2.° Suponemos que A tiene un elemento unidad e, invariante para σ. Demostrar que S_σ posee un elemento unidad. ¿Cuáles son los elementos inversibles de S_σ?

3.° Suponemos A íntegro y σ inyectivo. Demostrar que S_σ es íntegro. ¿Qué se puede decir del producto en P_σ de dos polinomios de grados respectivos p y q?

4.° Supongamos que A es un cuerpo. Demostrar que para todo par (f, g) de elementos de P_σ, no siendo nulo g, existe un par único (q, r) de elementos de P_σ tales que

$$f = (q * g) + r, \quad \text{con} \quad r = 0 \quad \text{o} \quad \text{grado de } r < \text{grado de } g.$$

5.° Supongamos que A es un cuerpo y que σ no es suprayectivo. Demostrar que se pueden encontrar en p_σ dos elementos no nulos f, g de los que el único múltiplo a la izquierda común es 0.

11

1.° Sean A un anillo factorial y $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ un polinomio de grado n ($a_n \neq 0$) con coeficientes en A. Suponemos que existe en A un elemento irreducible p, tal, que p divide a los coeficientes $a_0, a_1, \ldots, a_{n-1}$, pero p no divide a a_n, y p^2 no divide a a_0.

Demostrar que $f(x)$ es irreducible en $K[x]$, donde K es el cuerpo de fracciones de A.

2.° Demostrar que si K es un cuerpo conmutativo de característica distinta de 2, $f(x, y) = x^2 + y^2 - 1$ es irreducible en el anillo $K[x, y]$.

12

Sea A un anillo conmutativo con un elemento unidad e. Establecer la equivalencia de las propiedades siguientes:

a) 0 es el único elemento nilpotente de A;

b) todo elemento inversible del anillo de polinomios $A[x]$ es de grado nulo.

13*

Se pretende extender a ciertos anillos no conmutativos la teoría de los anillos euclídeos.

Sea A un anillo íntegro tal que existe una aplicación φ de $A^* = A - \{0\}$ en el conjunto $\mathbf{N}^*$ de los enteros naturales no nulos satisfaciendo a las condiciones

$$(C_1)\ (\forall a, b \in A^*) \quad \varphi(b) \leqslant \varphi(ab),$$
$$(C_2)\ (\forall a, b \in A^*), \quad (\exists q, r \in A) \quad a = qb + r,$$

con

$$r = 0 \quad \text{o} \quad \varphi(r) < \varphi(b).$$

(Si $r = 0$ diremos que b divide a a a la derecha, o que a es un múltiplo a la izquierda de b.)

1.° Demostrar que A admite un elemento unidad 1, y que los elementos inversibles de A están caracterizados por la condición $\varphi(x) = \varphi(1)$. ¿En qué casos la desigualdad que figura en (C_1) es una igualdad?

2.° Demostrar que todo ideal a la izquierda de A, es principal. Estudiar el conjunto de los divisores a la derecha comunes a dos elementos a, b de A^* y el conjunto de múltiplos a la izquierda comunes. Hágase ver claramente que este último conjunto no se reduce al elemento 0.

3.° Se hace la hipótesis suplementaria

$$(C_3)\ (\forall a, b \in A^*, a \neq b) \quad \varphi(a - b) \leqslant \sup\,[\varphi(a), \varphi(b)].$$

Demostrar que el par (q, r) definido por la condición (C_2) es único, para a y b dados, y que la unión del grupo K^* de unidades de A y el elemento 0, es un cuerpo K.

Demostrar que la desigualdad $\varphi(a) < \varphi(b)$, con $a, b \in A^*$, implica

$$\varphi(a - b) = \varphi(b).$$

Supongamos que A no coincida con el cuerpo K. Demostrar que existe al menos un elemento ξ de $A - K$ tal que A sea el conjunto de expresiones polinómicas $a_0 + a_1 \xi + \ldots + a_n \xi^n$ con coeficientes de K.

14*

1.° A cada serie formal no nula de coeficientes enteros

$$U = u_0 + u_1 x + \ldots + u_n x^n + \ldots, \quad u_i \in \mathbf{Z},$$

se hacen corresponder los enteros naturales $\omega(U) = k$, $\varphi(U) = |u_k|$ si es u_k el primer coeficiente no nulo de U.

Demostrar que los elementos del cuerpo K de fracciones del anillo $\mathbf{Z}[[x]]$ que admiten al menos una representación de la forma $\frac{U}{V}$, donde

$$\varphi(V) = 1, \quad U, V \in \mathbf{Z}[[x]],$$

constituyen un subanillo A de K; y demostrar que todo elemento de $A - \mathbf{Z}[[x]]$ puede escribirse $\frac{U}{x^\alpha}$, donde $U \in \mathbf{Z}[[x]]$ y donde α es un entero natural no nulo.

2.° Sean U y V dos elementos de $\mathbf{Z}[[x]]$ con $\omega(V) = 0$.

Demostrar que existe una serie formal con coeficientes racionales

$$W = w_0 + w_1 x + \ldots + w_n x^n + \ldots$$

tal que $U = VW$ en el anillo $\mathbf{Q}[[x]]$.

Suponemos que $W \notin \mathbf{Z}[[x]]$. Sea w_k su primer coeficiente no entero. Demostrar que el producto $\varphi(V)w_k$ es entero. Deducir que existe un polinomio P, de grado a lo sumo k, con coeficientes enteros, y una serie formal T con coeficientes enteros, tales que

$$U = PV + T, \quad \omega(T) = k, \quad \varphi(T) < \varphi(V).$$

3.° Demostrar que el anillo A definido en el punto 1.° es un anillo euclídeo.

15

Sea d un entero relativo sin más divisores cuadrados que el 1

1 ° Si α designa uno de los números complejos de cuadrado igual a d, consideramos el subcuerpo $\mathbf{Q}[\alpha]$ del cuerpo de los números complejos, constituido por los elementos de la forma $x + y\alpha$ ($x, y \in \mathbf{Q}$), y el subanillo $A = \mathbf{Z}[\alpha]$ de $\mathbf{Q}[\alpha]$, constituido por los elementos de la forma $x + y\alpha$ ($x, y \in \mathbf{Z}$).

Si $z = x + y\alpha$, pondremos $N(z) = x^2 - dy^2$.

Verificar que para dos elementos cualesquiera z', z'' de $\mathbf{Q}[\alpha]$ se tiene $N(z'\,z'') = N(z')\,N(z'')$; que $N(z)$ sólo es nulo cuando $z = 0$; y que los elementos inversibles del anillo A se caracterizan por la propiedad $N(z) = \pm 1$.

2.° Supongamos que d es uno de los cuatro números, -2, -1, 2, 3. Demostrar que para todo $z \in \mathbf{Q}[\alpha]$ existe al menos un $z' \in A$ tal que

$$|\, N(z - z')\,| < 1.$$

Deducir que el anillo A es euclídeo.

16

Sea A un anillo sin ningún ideal a la izquierda propio.

1.° Supongamos que exista en A al menos un producto no nulo. Establecer la existencia de un elemento $a \in A$ que no es divisor de cero a la derecha, y la de un idempotente e tal que $ea = a$. Demostrar que e es elemento unidad de A y que A es un cuerpo.

2.° Suponemos que todo producto de elementos de A es nulo, no estando A reducido a su elemento 0. Demostrar que el grupo aditivo de A es cíclico de orden primo.

17

Sea un anillo A en el que toda parte lícita multiplicativamente a la izquierda sea un ideal a la izquierda de A. Demostrar que el conjunto de los ideales a la izquierda de A es totalmente ordenado (por inclusión).

18

Se supone que el conjunto de los ideales a la izquierda principales de un anillo A es totalmente ordenado, por inclusión.

1.° Demostrar que para todo entero natural $n \geqslant 2$ y para todo par (x, y) de elementos de A, el elemento $xy - yx$ pertenece a la potencia n-ésima del ideal A.

2.° Se supone que para todo $x \in A$, $x \in Ax$. Demostrar que toda parte multiplicativamente lícita a la izquierda es un ideal a la izquierda de A.

En el caso particular en que A sea conmutativo, demostrar que A tiene un elemento unidad.

19

Se considera el anillo producto $A = B_1 \times B_2$ de dos anillos B_1 y B_2 (texto: IV, 2): A es el conjunto de pares (x_1, x_2) donde $x_i \in B_i$ $(i = 1, 2)$ y la adición y multiplicación se realizan componente a componente.

1.° Verificar que el conjunto A_1 de pares $(x_1, 0)$ y el conjunto A_2 de pares $(0, x_2)$ son ideales biláteros de A, y que todo ideal a la izquierda, a la derecha o bilátero de A_i $(i = 1, 2)$ es ideal a la izquierda, a la derecha o bilátero de A.

Para todo lo que sigue suponemos que A tiene un elemento unidad e.

2.° Demostrar que todo ideal a la izquierda de A es de la forma $\mathfrak{g} = \mathfrak{g}_1 + \mathfrak{g}_2$, donde $\mathfrak{g}_i$ es un ideal a la izquierda de A_i $(i = 1, 2)$, que esta descomposición es única y que $\mathfrak{g}$ es un ideal a la izquierda principal si y sólo si cada uno de los ideales $\mathfrak{g}_1$, $\mathfrak{g}_2$, es un ideal a la izquierda principal.

3.° Sea $\mathfrak{m} = \mathfrak{m}_1 + \mathfrak{m}_2$ un ideal de A, supuesto A conmutativo, siendo $\mathfrak{m}_i$ ideal de A_i $(i = 1, 2)$. Demostrar que el anillo cociente $A/\mathfrak{m}$ es isomorfo al producto de los anillos cocientes $A/\mathfrak{m}_1$ y $A/\mathfrak{m}_2$.

¿Cómo es preciso elegir $\mathfrak{m}_1$ y $\mathfrak{m}_2$, para que $\mathfrak{m}$ sea maximal? para que $\mathfrak{m}$ sea primo? para que $\mathfrak{m}$ sea primario?

20

Sea A un anillo conmutativo con elemento unidad e.

1.° Establecer la equivalencia de las dos condiciones siguientes:

α) el conjunto de elementos no inversibles de A es un ideal;

β) el conjunto de ideales propios de A admite un elemento máximo.

Cuando se cumplen estas dos condiciones se dice que A es un *anillo casi local*.

2.° Demostrar que si A es casi local no tiene otros elementos idempotentes que el 0 y el e.

3.° Demostrar que si el conjunto de ideales principales de A es totalmente ordenado (por inclusión), A es casi local.

4.° Suponemos que A es casi local, que su ideal propio máximo $\mathfrak{m}$ es principal, y que la intersección de potencias de $\mathfrak{m}$ es el ideal nulo. Demostrar que todo ideal no nulo de A es una potencia de $\mathfrak{m}$.

Si además A es íntegro, demostrar que para todo elemento x no nulo del cuerpo de fracciones de A, uno al menos de los elementos x y x^{-1} pertenece a A. Dar el ejemplo de un anillo A que tenga las propiedades antedichas.

21

Sea A un anillo casi local (véase ejercicio precedente).

1.° Se supone que el retículo de los ideales de A es distributivo. Demostrar que, para todo par (a, b) de elementos de A, existen $u \in (a) \cap (b)$, $v \in A$ tales que $a = u + v(a - b)$, $vb \in (a)$. Deducir que el conjunto de los ideales de A es totalmente ordenado.

2.° Se supone que A es íntegro y que la multiplicación de ideales es distributiva respecto a la intersección. Demostrar que para todo par (a, b) de elementos no nulos de A, existen $x, y \in (a) \cap (b)$ tales que $ab = xa + yb$. Deducir que el conjunto de ideales de A es totalmente ordenado.

22

Sean A un anillo y e un elemento idempotente de A.

1.° Establecer la equivalencia de las propiedades siguientes (se pueden utilizar los resultados del ejercicio V, 1):

a) e pertenece al centro del anillo A;

b) e conmuta con cualquier otro elemento idempotente de A;

c) e es elemento unidad del subanillo $B = eA$;

d) $eA = Ae = eAe$.

2.° Supuesto que se verifican las condiciones anteriores, demostrar que:

α) todo ideal a la izquierda del anillo $B = eA$ es ideal a la izquierda de A;

β) todo elemento de A puede ponerse de modo único en la forma $b + c$, donde $b \in B$ y $ce = ec = 0$.

23

Sean A un anillo conmutativo no íntegro, $f = \sum_{i=0}^{n} a_i x^i$ un elemento del anillo de polinomios $A[x]$, I el ideal anulador de f en $A[x]$. Se supone f de grado $n \geqslant 1$.

Se propone demostrar, por reducción al absurdo, que $I \neq (0)$ implica $I \cap A \neq (0)$. Para ello hágase la hipótesis $I \cap A = (0)$, $I \neq (0)$. Entonces:

1.° Demostrar que el conjunto de los grados de los polinomios no nulos que están en I admite un elemento mínimo $t \geqslant 1$.

2.° Sea $g = \sum_{j=0}^{t} b_j x^j$ un elemento de I de grado t ($b_t \neq 0$). Demostrar que los polinomios $g_i = a_i g$ ($i = 0, 1, ..., n$) no son todos nulos, y que uno de ellos es de grado estrictamente inferior a t. Deducir que la hipótesis propuesta conduce a una contradicción.

24

En un anillo factorial A, el ideal principal (p) es primo si y sólo si el elemento p es irreducible.

25

Sean A un anillo conmutativo, A' la imagen de A por un homomorfismo f, $\mathfrak{n}$ el núcleo de f. Establecer los siguientes resultados:

1.° Si $\mathfrak{a}'$ es un ideal de A' y $\mathfrak{r}'$ su radical, $f^{-1}(\mathfrak{r}')$ es el radical de $f^{-1}(\mathfrak{a}')$. Si $\mathfrak{a}'$ es primo, $f^{-1}(\mathfrak{a}')$ lo es también. Si $\mathfrak{a}'$ es primario, $f^{-1}(\mathfrak{a}')$ lo es también.

2.° Si $\mathfrak{a}$ es un ideal de A que contiene a $\mathfrak{n}$, y es $\mathfrak{r}$ su radical, $f(\mathfrak{r})$ es el radical de $f(\mathfrak{a})$. Si $\mathfrak{a}$ es primo, $f(\mathfrak{a})$ es primo. Si $\mathfrak{a}$ es primario, $f(\mathfrak{a})$ lo es también.

3.° Las propiedades dichas en el punto 2.° pueden no ser verdad si no se supone $\mathfrak{n} \subseteq \mathfrak{a}$.

4.° Si el anillo A es principal e íntegro, la imagen por f de todo ideal primo de A es un ideal primo de A'.

26

A designa un anillo conmutativo.

1.° Sea $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ una familia finita de ideales no comparables dos a dos. Sea $\mathfrak{a}$ un ideal de A que no está contenido en ninguno de los $\mathfrak{p}_i$. Para

cada valor del índice i ($1 < i < n$) se designa por $\mathfrak{a}_i$ la intersección de $\mathfrak{a}$ y las $\mathfrak{p}_j$ distintas de $\mathfrak{p}_i$. Demostrar que $\mathfrak{a}_i$ no está contenido en $\mathfrak{p}_i$. Poniendo $x = \sum_{i=1}^{n} x_i$, donde $x_i \in \mathfrak{a}_i$, $x_j \notin \mathfrak{p}_i$, demostrar que $x \in \mathfrak{a}$ y que x no pertenece a ningún $\mathfrak{p}_i$.

2.° Deducir que si un ideal de A está contenido en una unión finita de ideales primos, está contenido en uno de esos ideales primos.

27

Sea $\mathfrak{m}$ un ideal maximal de un anillo conmutativo A sin elemento unidad. Utilizando el ejercicio V, 16 demostrar que $\mathfrak{m}$ es ideal primario de A. ¿En qué casos es ideal primo?

28

Sean A un anillo conmutativo con elemento unidad e, y $A[x]$ el anillo de los polinomios en una indeterminada con coeficientes en A.

A todo ideal $\mathfrak{a}$ de A, se hace corresponder el ideal $\varphi(\mathfrak{a})$ de $A[x]$ engendrado por $\mathfrak{a}$ en $A[x]$.

1.° Sea $f(x) = \sum_{i=0}^{n} a_i x^i$. Demostrar que para que $f(x) \in \varphi(\mathfrak{a})$ es necesario y suficiente que todos sus coeficientes a_i pertenezcan a $\mathfrak{a}$.

2.° Demostrar que para todo ideal $\mathfrak{a}$ de A, $\mathfrak{a} = \varphi(\mathfrak{a}) \cap A$.

3.° Demostrar que para dos ideales cualesquiera $\mathfrak{a}_1$, $\mathfrak{a}_2$ de A, se tiene

$$\varphi(\mathfrak{a}_1 + \mathfrak{a}_2) = \varphi(\mathfrak{a}_1) + \varphi(\mathfrak{a}_2), \quad \varphi(\mathfrak{a}_1 \mathfrak{a}_2) = \varphi(\mathfrak{a}_1)\varphi(\mathfrak{a}_2),$$
$$\varphi(\mathfrak{a}_1 \cap \mathfrak{a}_2) = \varphi(\mathfrak{a}_1) \cap \varphi(\mathfrak{a}_2).$$

4.° Demostrar que $\mathfrak{a}$ es ideal primo de A si y sólo si, $\varphi(\mathfrak{a})$ es ideal primo de $A[x]$.

29

Sea A un anillo conmutativo con elemento unidad e. Sea $B \neq (0)$ un subanillo de A ($e \notin B$) tal que $A = B[e]$ donde $B[e]$ indica el anillo extensión simple del B por la adjunción del elemento e.

1.° Comparar los ideales principales engendrados en A y en B por un elemento b de B. Deducir que todo ideal de B es también ideal de A.

2.° Sea $\mathfrak{a}$ un ideal de A. Demostrar que si el ideal $\mathfrak{a} \cap B$ del anillo B admite una base $\{b_1, b_2, ..., b_s\}$ de s elementos, $\mathfrak{a}$ admite al menos una base de $s + 1$ elementos.

3.° Suponiendo A íntegro, demostrar que todo ideal primo no nulo de A contiene un ideal primo no nulo de B.

30

Sean A un anillo conmutativo con elemento unidad e, $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales de A. Se dice que $\mathfrak{b}$ cubre a $\mathfrak{a}$ si $\mathfrak{a} \subset \mathfrak{b}$ y si no existe ningún ideal $\mathfrak{c}$ tal que $\mathfrak{a} \subset \mathfrak{c} \subset \mathfrak{b}$.

1.° Supongamos que $\mathfrak{b}$ cubre a $\mathfrak{a}$. Sea x un elemento de $\mathfrak{b}$ que no pertenezca a $\mathfrak{a}$. Demostrar que para todo $a \in A$ tal que $ax \notin \mathfrak{a}$, es

$$\mathfrak{a} + Aax = \mathfrak{a} + Ax = \mathfrak{b},$$

y que $\mathfrak{m} = \mathfrak{a} : Ax$ es un ideal maximal de A, tal que $\mathfrak{a} \subset \mathfrak{a} : \mathfrak{m}$.

2.° Si suponemos que para un ideal $\mathfrak{a}$ existe un ideal maximal $\mathfrak{m}$ tal que $\mathfrak{a} \subset \mathfrak{a} : \mathfrak{m}$, entonces, demostrar que para todo $x \in \mathfrak{a} : \mathfrak{m}$ tal que $x \notin \mathfrak{a}$ se tiene $\mathfrak{m} = \mathfrak{a} : Ax$, y que el ideal $\mathfrak{b} = \mathfrak{a} + Ax$ cubre a $\mathfrak{a}$.

Soluciones

1

1.° Es bien sabido (texto: I, 7) que cuando ni E' ni E'' son vacíos, ambos conjuntos coinciden y se reducen a un solo elemento e, elemento unidad de A.

Sean $e' \in E'$; $x, y \in A$. Entonces $y\varphi_{e'}(x) = y$, de donde

$$\varphi_{e'}(x) \in E' \quad \text{y} \quad \varphi_{e'}(A) \subseteq E'.$$

Para $x, y \in E'$, $\varphi_{e'}(x) = \varphi_{e'}(y)$ implica $e'x - x + e' = e'y - y + e'$, lo que, por ser $e'x = e'y = e'$, nos da $x = y$, de donde la restricción de $\varphi_{e'}$ a E' es inyectiva.

Si E' se reduce a un solo elemento e' se tiene, para todo $x \in A$, $\varphi_{e'}(x) = e'$, es decir $e'x = x$, de donde $e' \in E''$ y $E' = E'' = \{ e' \}$. En tal caso A tiene elemento unidad (único).

Supongamos ahora $e \in E'$, $f \in E'$, $e \neq f$. En tal caso E'' es vacío, según la advertencia inicial.

Consideremos el anulador a la derecha de A,

$$I = \{ y, y \in A, (\forall x \in A)\, xy = 0 \}$$

Éste es un ideal bilátero de A, no nulo ya que $e - f \in I$, diferente de A, pues si fuese $e \in I$, resultaría $x = xe = 0$ para todo $x \in A$. Está claro que para todo $e' \in E'$, $e' - e \in I$. Recíprocamente $e' - e \in I$ implica $e' \in E'$. Por tanto, E' es la clase módulo I que contiene a e.

Sea θ un homomorfismo tal que $\theta(A)$ tenga un elemento unidad $\bar{e}$. Si $a \in I$, $\theta(b) = \bar{e}$, es claro que

$$\theta(a) = \bar{e}\theta(a) = \theta(b)\,\theta(a) = \theta(ba) = 0,$$

luego I está contenido en el núcleo de θ. Resulta entonces, del primer teorema de isomorfismo para anillos (texto: VIII, 1, teor. 5) que $\theta(A)$ es imagen homomorfa de A/I.

Nota. A/I admite elemento unidad. En efecto, si φ es el homomorfismo canónico $A \to A/I$, la relación $xe = x$ muestra que $\varphi(e)$ es elemento unidad

a la derecha de A/I. Además, para todo par (x, y) de elementos de A, se tiene

$$y(ex - x) = (ye)\,x - yx = 0,$$

luego $ex - x \in I$, y $\varphi(e)$ es elemento unidad a la izquierda de A/I. Podemos, pues, enunciar: para que un anillo B, imagen homomorfa de A, admita un elemento unidad, es necesario y suficiente que sea imagen homomorfa de A/I.

2.° Se sabe (texto: II, 1, Teor. 9) que cuando ni S'_a ni S''_a son vacíos, coinciden y se reducen a un solo elemento, inverso bilátero único de a.

Sean x, $s \in S'_a$. Entonces

$$a\psi_s(x) = a(xa - e + s) = e,$$

de donde $\psi_s(S'_a) \subseteq S'_a$.

Sean x, y, $s \in S'_a$. La igualdad $\psi_s(x) = \psi_s(y)$ implica $xa = ya$, de donde $xas = yas$, es decir $x = y$; ψ_s es inyectiva.

Si S'_a se reduce a un único elemento s, $\psi_s(s) = s$ se escribe $sa = e$, de donde $s \in S''_a$. En este caso $S'_a = S''_a = \{s\}$, y s es elemento inverso bilátero único de a.

Supongamos ahora $s \in S'_a$, $t \in S'_a$, $s \neq t$. Si S'_a fuese finito, la inyección ψ_s sería también una suprayección, y existiría $x \in S'_a$ tal que $\psi_s(x) = s$, de donde $xa = e$ y $x \in S''_a$, lo que contradice la observación inicial. Por tanto S'_a es infinito.

Ejemplo. Sea E un espacio vectorial sobre un cuerpo conmutativo, que admite una base numerable $\{a_1, a_2, \ldots, a_n, \ldots\}$. Se sabe que los endomorfismos de E constituyen un anillo y que cada uno de ellos viene definido por el dato de los transformados de los a_i.

Pongamos $f(a_1) = f(a_2) = a_1$ y $f(a_i) = a_{i-2}$ para $i \geq 3$,

$$g_k(a_1) = a_k \qquad (k = 1, 2, 3),$$
$$g_k(a_n) = a_{n+2} \qquad \text{para } n > 2.$$

Entonces se verifica que $f \circ g_1 = f \circ g_2 = f \circ g_3 = e$, donde e es el endomorfismo idéntico de E.

3.° Si A es íntegro, ninguno de los conjuntos E', E'', S'_a, S''_a puede tener más de un elemento. Se tiene pues, o bien $E' = E'' = \varnothing$, o bien $E' = E'' = \{e\}$, donde e es el elemento unidad de A; y, para un a dado, o bien $S'_a = S''_a = \varnothing$, o bien $S'_a = S''_a = \{a^{-1}\}$, donde a^{-1} es inverso bilátero único de a.

2

Las aplicaciones $x \to ax$ y $x \to xb$ son inyectivas, luego también suprayectivas, puesto que el anillo es finito. Resulta que existen e y f tales que $a = ae$, $b = fb$. Se tiene entonces, para todo elemento x del anillo, $ax = aex$, $xb = xfb$, es decir, $x = ex = xf$. Por consiguiente, e es elemento unidad a la izquierda, f es elemento unidad a la derecha, de donde $e = f$, elemento unidad bilátero.

3

Sea a un elemento no divisor de cero a la izquierda. La aplicación $x \to ax$ es entonces inyectiva, luego también suprayectiva, puesto que el anillo es finito. Existe pues un elemento a' y uno solo, tal, que $aa' = e$. Según el ejercicio V, 1, a' es inverso bilátero de a y así a es una unidad.

4

El centro Z de un anillo A es un subanillo conmutativo de A, según se verifica inmediatamente. Sean x, y dos elementos cualesquiera de A. Por hipótesis los elementos

$$x^2 - x,\ y^2 - y,\ (x + y)^2 - (x + y) = (x^2 - x) + (y^2 - y) + xy + yx$$

pertenecen a Z, luego también $xy + yx$, lo que implica

$$x(xy + yx) = (xy + yx)\,x,$$

es decir, $x^2 y = yx^2$. El cuadrado de todo elemento x de A pertenece pues a Z, lo mismo que $x^2 - x$ y por lo tanto también x. Esto quiere decir $Z = A$ y A es conmutativo.

5

1.° Se verifica inmediatamente que I_m es un ideal bilátero de A y que para todo divisor m' de m es $I_{m'} \subseteq I_m$. Se sabe que existen dos enteros relativos u, v tales que $um + vN = d$. Entonces $mx = 0$ implica $dx = 0$, puesto que $Nx = 0$, es decir, $I_m \subseteq I_d$, de donde la igualdad: $I_m = I_d$.

2.° Siendo a y b primos entre sí, existen dos enteros relativos a', b' tales que $a'\,a + b'\,b = 1$. Todo elemento x de A es entonces suma de un

elemento $\lambda = b'bx$ de I_a y un elemento $\mu = a'ax$ de I_b. Esta descomposición es única pues $y \in I_a \cap I_b$ implica $y = a'ay + b'by = 0$. Esto permite definir una biyección φ del conjunto producto $I_a \times I_b$ sobre A, poniendo $\varphi[(\lambda, \mu)] = \lambda + \mu$. Esta biyección φ es un isomorfismo de anillos, en virtud de la definición de anillo producto y del hecho de que $xy = yx = 0$ cuando $x \in I_a$, $y \in I_b$.

Notas: 1. Los elementos $x \in I_a$, $y \in I_b$ engendran dos grupos, de órdenes respectivos, $\nu(x)$, divisor de a, y $\nu(y)$, divisor de b. Por tanto $\nu(x)$ y $\nu(y)$ son primos entre sí. Si φ es una biyección, el conjunto de los $z(x + y)$, donde $z \in \mathbf{Z}$, comprende $\nu(x)\,\nu(y)$ elementos distintos, de donde $\nu(x + y) = \nu(x)\,\nu(y)$. Se trata de un caso particular de un resultado clásico (texto: VIII, 4).

2. Reiterando el razonamiento precedente, vemos que si

$$N = a_1 a_2 \dots a_n,$$

donde los factores a_i son primos entre sí dos a dos, A es isomorfo al anillo producto $I_{a_1} \times I_{a_2} \times \dots \times I_{a_n}$ y que si $x_i \in I_{a_i}$ $(1 \leqslant i \leqslant n)$, se tiene

$$\nu(x_1 + x_2 + \dots + x_n) = \nu(x_1)\,\nu(x_2) \dots \nu(x_n).$$

3.° Se sabe (texto: IV, 4) que cuando x recorre A, el orden $\nu(x)$ toma sólo un número finito de valores $\nu_1, \nu_2, \dots, \nu_k$, y que p^α es el m.c.m. de los ν_i. Cada ν_i es pues una potencia de p y uno de ellos es necesariamente p^α. Existe pues al menos un $x \in A$ tal que $\nu(x) = p^\alpha$. Entonces $\nu(px) = p^{\alpha-1}$ y, sucesivamente,

$$\nu(p^{\alpha-\beta} x) = p^\beta \quad (1 \leqslant \beta \leqslant \alpha).$$

4.° Sean

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}, \quad \delta = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} \quad (0 \leqslant \beta_i \leqslant \alpha_i)$$

las descomposiciones de N y δ en producto de factores primos. Tengamos presente la nota 2 al punto 2.° y el punto 3.°, tomando $a_i = p_i^{\alpha_i}$. La característica del subanillo I_{a_i} es de la forma $p_i^{\gamma_i}$ $(1 \leqslant \gamma_i \leqslant \alpha_i)$ y el conjunto de los órdenes $\nu(x)$ de los elementos de I_{a_i} es exactamente el conjunto de enteros de la forma $p_i^{\lambda_i}$ $(0 \leqslant \lambda_i \leqslant \gamma_i)$. El conjunto de órdenes de elementos de A es entonces (nota 2 de 2.°) el conjunto de enteros de la forma

$$p_1^{\lambda_1} p_2^{\lambda_2} \dots p_n^{\lambda_n} \quad (0 \leqslant \lambda_i \leqslant \gamma_i).$$

Puesto que N es el m.c.m. de estos enteros se tiene necesariamente $\gamma_i = \alpha_i$ para cada valor del índice i. Por consiguiente, el subanillo I_{α_i} es de característica $p_i^{\alpha_i}$ y todo divisor δ de N es efectivamente orden de al menos un elemento de A, obteniendo como suma de elementos $x_i \in I_i$ tales que $v(x_i) = p_i^{\beta_i}$ para $i = 1, 2, ..., n$.

6

1.° Sea A un elemento nilpotente de A. Existe un entero natural α tal que $a^\alpha = 0$. Por otra parte

$$a = a^n = a^{n^2} = ... = a^{n^k} = ...$$

Para k suficientemente grande se tiene

$$n^k > \alpha \quad \text{y} \quad a = a^{n^k} = a^\alpha a^{n^k - \alpha} = 0.$$

2.° Para dos elementos cualesquiera a, b de A existe un entero natural $r > 1$ tal que $a^r = a$, $b^r = b$. Basta tomar r tal que $r - 1$ sea múltiplo común de $n(a) - 1$ y de $n(b) - 1$. La verificación es inmediata.

En particular, para $b = ka$ (k entero natural > 2) obtenemos $(k^r - k)\, a = 0$. El orden $v(a)$ del grupo aditivo engendrado por a es pues finito, y es divisor de $k^r - k$. La descomposición del entero $v(a)$ en factores primos no aporta ningún cuadrado, pues si $k = p$, número primo, $p^r - p$ no puede ser divisible por p^2.

3.° Sea a un elemento no divisor de cero. De $a^n = a$ se sigue, para todo $x \in A$,

$$(xa^{n-1} - x)\, a = a(a^{n-1} x - x) = 0,$$

de donde

$$x = a^{n-1} x = x a^{n-1}.$$

El elemento $e = a^{n-1}$ es, pues, elemento unidad del anillo.

Nota. En un anillo tal, todo elemento no divisor de cero es unidad; en efecto, si $n \neq 2$ es a^{n-2} inverso de a, y si $n = 2$, a es su propio inverso.

7

1.° Para todo entero relativo m y para todo $x \in A$, es $(m + p)\, x = mx$. Poniendo $\overline{m}x = mx$, donde $\overline{m}$ es la clase de m módulo p, se hace de A un espacio vectorial de dimensión finita sobre el cuerpo $\mathbf{Z}/(p)$.

Si $(a_1, a_2, ..., a_s)$ es una base de este espacio vectorial, todo elemento $x \in A$ tiene una representación única

$$x = \sum_{j=1}^{s} x_j \, a_j, \quad x_j \in \mathbf{Z}/(p) .$$

Puesto que cada x_j puede tomar p valores distintos, el número de elementos de A es p^s.

2.° Si A tiene p elementos su grupo aditivo es cíclico, y si a es un generador de ese grupo,

$$A = \{ 0, a, 2a, ..., (p-1)a \}.$$

Existe entonces un entero k $(0 \leqslant k \leqslant p-1)$ tal que $a^2 = ka$.

Si $k = 0$, todo producto de elementos de A es nulo. Si no, k y p son primos entre sí, y existen dos enteros relativos u, v, tales que $uk + vp = 1$. Se puede desde luego suponer $1 \leqslant u \leqslant p-1$. Entonces se comprueba fácilmente que la aplicación f de $\mathbf{Z}/(p)$ en A, definida por $f(\bar{n}) = nua$ es un isomorfismo de anillos. Por consiguiente A es un cuerpo.

8

Al ser el grupo aditivo de A de orden n, se tiene $nx = 0$ para todo $x \in A$. Por tanto la característica N de A es un divisor de n. Se pueden suponer las notaciones elegidas de modo que

$$N = p_1 p_2 ... p_s \quad (1 \leqslant s \leqslant k).$$

Según la cuestión 2.ª del ejercicio V, 5, A es isomorfo al anillo producto

$$I_{p_1} \times I_{p_2} \times ... \times I_{p_s}$$

donde I_{p_λ} es el conjunto de los $x \in A$ tales que $p_\lambda x = 0$, y según el ejercicio V, 7, I_{p_λ} consta de $p_\lambda^{r_\lambda}$ elementos.

La igualdad $n = p_1^{r_1} p_2^{r_2} ... p_s^{r_s}$ implica $s = k$ y $r_1 = r_2 = ... = r_k = 1$.

Resulta que cada I_{p_λ} es, o bien un anillo en el que todo producto es nulo, o bien isomorfo al cuerpo conmutativo $\mathbf{Z}/(p_\lambda)$. Por consiguiente A es conmutativo.

Si A tiene elemento unidad, cada I_{p_λ} tiene también elemento unidad y, por consiguiente, cada I_{p_λ} es un cuerpo.

9

Recordemos que si K es un cuerpo con p elementos y con elemento unidad e, el grupo multiplicativo K^* de K tiene $p-1$ elementos, luego todo $x \in K^*$ satisface $x^{p-1} = e$, y toda igualdad $x^r = e$ implica que $p-1$ sea divisor de r.

1.° El subgrupo aditivo A' engendrado por e es también el subanillo engendrado por e. Se sabe que su orden $v(e)$ es la característica del anillo A y, según ejercicio V, 6, no tiene ningún divisor cuadrado salvo el 1. Luego

$$N = p_1 p_2 \dots p_s.$$

Apliquemos al anillo A' el resultado de ejercicio V, 7, 2.°. Para cada descomposición de N en un producto ab de factores primos entre sí, se obtiene $e = e_a + e_b$, con $e_a \in I_a$, $e_b \in I_b$. La igualdad $ze = ze_a + ze_b$, donde $z \in \mathbf{Z}$, muestra que el ideal I_a de A' es el subanillo engendrado por su elemento unidad e_a. En particular, si a es uno de los p_i, I_a es un subcuerpo de p_i elementos de A', y, para $x \in I_a$, no nulo, de $x^n - x = 0$ significa que $p_i - 1$ es divisor de $n-1$.

2.° Si n es par, $n-1$ es impar. No puede pues existir otro p_i que 2, y $N = 2$.

En el caso $n = 6$ se tiene, teniendo en cuenta las reglas de cálculo válidas cuando la característica es 2,

$$(x+e)^6 = x^6 + x^4 + x^2 + e,$$

de donde

$$x^4 = -x^2, \quad \text{y} \quad x = x^5 = -x^4 = x^2, \quad \text{para todo } x \in A.$$

Por tanto A es un anillo de Boole.

10

1.° Las verificaciones a efectuar son inmediatas, excepto la de la asociatividad de $*$, que requiere un poco de atención. Sean α, β, γ tres series formales sobre A:

$$\alpha = \sum_{n=0}^{\infty} a_n x^n, \quad \beta = \sum_{n=0}^{\infty} b_n x^n, \quad \gamma = \sum_{n=0}^{\infty} c_n x^n.$$

Pondremos,

$$\alpha * \beta = \sum_{n=0}^{\infty} p_n x^n, \qquad \beta * \gamma = \sum_{n=0}^{\infty} q_n x^n.$$

Es cómodo, para facilitar la escritura, poner $\sigma^0(a) = a$, para cualquier elemento a de A. Se tiene entonces

$$p_n = \sum_{\lambda+\mu=n} a_\lambda \sigma^\lambda(b_\mu), \qquad q_n = \sum_{\mu+\nu=n} b_\mu \sigma^\mu(c_\nu).$$

La igualdad

$$a_\lambda \sigma^\lambda(b_\mu)\, \sigma^{\lambda+\mu}(c_\nu) = a_\lambda \sigma^\lambda[b_\mu \sigma^\mu(c_\nu)],$$

donde λ, μ, ν son enteros naturales tales que $\lambda + \mu + \nu = n$, permite obtener, por sumación

$$\sum_{i+\nu=n} p_i \sigma^i(c_\nu) = \sum_{\lambda+j=n} a_\lambda \sigma^\lambda(q_j),$$

es decir, $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$.

2.° Es claro que para todo $\alpha \in S_\sigma$, $e\alpha = \alpha$, y que $\sigma(e) = e$ implica $\alpha e = \alpha$.

Si $\alpha = \sum_{n=0}^{\infty} a_n x^n$ admite en S_σ por inversa $\beta = \sum_{n=0}^{\infty} b_n x^n$, se tiene $\alpha\beta = \beta\alpha = e$, de donde $a_0 b_0 = b_0 a_0 = e$, luego a_0 es inversible en A. Recíprocamente, si a_0 es inversible en A, se puede determinar, por el método de coeficientes indeterminados, una serie formal $\beta = \sum_{n=0}^{\infty} b_n x^n$ tal que $\alpha * \beta = e$, y una serie formal $\gamma = \sum_{n=0}^{\infty} c_n x^n$ tal que $\gamma * \alpha = e$. Los coeficientes se determinan sucesivamente por las relaciones de recurrencia

$$b_0 = c_0 = a_0', \quad \text{inverso de } a_0,$$
$$a_0 b_n + a_1 \sigma(b_{n-1}) + \ldots + a_k \sigma^k(b_{n-k}) + \ldots + a_n \sigma^n(b_0) = 0,$$
$$c_0 a_n + c_1 \sigma(a_{n-1}) + \ldots + c_k \sigma^k(a_{n-k}) + \ldots + c_n \sigma^n(a_0) = 0,$$

[$\sigma^n(a_0)$ es evidentemente inversible, de inverso $\sigma^n(a_0')$].

Se sabe (texto: II, 1, teor. 9) que $\beta = \gamma$, luego α es inversible.

3.° Consideremos dos series formales

$$\alpha = \sum_{n=0}^{\infty} a_n x^n, \qquad \beta = \sum_{n=0}^{\infty} b_n x^n.$$

Si $\alpha \neq 0$ existe un mínimo índice n tal que $a_n \neq 0$. Lo indicaremos por $\omega(\alpha)$. Supongamos también $\beta \neq 0$. Es claro que si ponemos

$$\alpha * \beta = \sum_{n=0}^{\infty} p_n x^n,$$

se tiene $p_n = 0$ para $n < \omega(\alpha) + \omega(\beta)$, y que

$$p_{\omega(\alpha)+\omega(\beta)} = a_{\omega(\alpha)} \sigma^{\omega(\alpha)}[b_{\omega(\beta)}].$$

Supuesto A íntegro, y σ inyectivo, $b_{\omega(\beta)} \neq 0$ implica $\sigma[b_{\omega(\beta)}] \neq 0$, y sucesivamente, por recurrencia,

$$\sigma^{\omega(\alpha)}[b_{\omega(\beta)}] \neq 0.$$

Luego $p_{\omega(\alpha)+\omega(\beta)} \neq 0$, lo que implica

$$\alpha * \beta \neq 0 \quad \text{y} \quad \omega(\alpha * \beta) = \omega(\alpha) + \omega(\beta).$$

Un razonamiento análogo demuestra que si α y β son polinomios no nulos $\alpha * \beta$ es un polinomio no nulo y

$$\text{grado } (\alpha * \beta) = \text{grado } (\alpha) + \text{grado } (\beta).$$

4.° Si A es un cuerpo, el endomorfismo no nulo σ es necesariamente inyectivo (puesto que los cuerpos no tienen ideales propios), y no es necesariamente suprayectivo. (Véase ejercicio VII, 8.)

Basta establecer que si grado $f >$ grado g, es posible encontrar un monomio $\mu = c_r x^r$ tal que, grado $[f - (\mu * g)] <$ grado f. El razonamiento clásico de la teoría de división euclídea subsiste sin modificación.

Sean pues $a_p x^p$, $b_q x^q$ $(a_p b_q \neq 0,\ p > q)$ los monomios de más alto grado de f y g. Es claro que la condición impuesta equivale a

$$a_p = c_r \sigma^r(b_q),$$

lo que determina efectivamente un coeficiente c_r.

5.° No siendo σ suprayectivo, ninguna de sus potencias lo será. Supongamos que cuatro elementos, f, g, u, v de P_σ cuyos monomios de mayor grado sean respectivamente $a_p x^p$, $b_q x^q$, $c_r x^r$, $d_s x^s$, verifiquen la igualdad $f * u = g * v$. Se tiene entonces $p + r = q + s$, y $a_p \sigma^p(c_r) = b_q \sigma^q(d_s)$. Si, por ejemplo, q es superior o igual a p, es suficiente que $b_q^{-1} a_p$ no pertenezca a $\sigma^p(A)$ para que $f * u = g * v$, $fg \neq 0$ implique $u = v = 0$.

11

1.° Supongamos $f(x) = g(x)\,h(x)$ con

$$g(x) = \sum_{j=0}^{r} b_j x^j, \quad h(x) = \sum_{k=0}^{s} c_k x^k, \quad b_j \in A, \quad c_k \in A.$$

Puesto que p no divide a $a_n = b_r\,c_s$, no divide ni a b_r ni a c_s, por lo que existe, de una parte, un entero mínimo λ tal que p no divide a b_λ, y por otra parte, un entero mínimo μ tal que p no divide a c_μ.

No puede ser $\lambda = \mu = 0$, porque entonces p no dividiría a $a_0 = b_0\,c_0$, ni $\lambda > 0$, $\mu > 0$, porque entonces p^2 sería divisor de a_0.

Supongamos, por ejemplo, $\lambda > 0$ y $\mu = 0$. Se tiene entonces

$$a_\lambda = b_\lambda\,c_0 + b_{\lambda-1}\,c_1 + \ldots + b_0\,c_\lambda.$$

Para $j < \lambda$, es p divisor de b_j, luego p es divisor de $a_\lambda - b_\lambda\,c_0$. Como p no divide a $b_\lambda\,c_0$, tampoco divide a a_λ, lo que implica $\lambda = n$, de donde $r = n$ y $s = 0$. Por tanto $h(x)$ es una constante no nula.

Los anillos $A[x]$ y $K[x]$ son factoriales. En estos anillos, f se descompone en producto de factores irreducibles. En $A[x]$ esta descomposición es de la forma $c_0\,g$ ($c_0 \in A$; $g \in A[x]$, irreducible), según los resultados precedentes. En $K[x]$ la descomposición es de la forma $f_1' f_2' \ldots f_m'$. Existe un elemento $u \in A$ tal que cada uf_j' sea un polinomio con coeficientes de A. Se tiene entonces

$$c_0\,u^m g = (uf_1')\,(uf_2')\ldots(uf_m'),$$

de donde se deduce, por ser $A[x]$ factorial, que g es divisor de uno de los uf_j', por ejemplo, uf_1'. Existe, pues, $v \in A$ tal que $vg = uf_1'$, y $f = \dfrac{c_0\,u}{v} f_1'$ es irreducible en $K[x]$.

2.° $f(x, y) = x^2 + y^2 - 1$ (donde 1 indica, evidentemente, el elemento unidad de K) es un polinomio en x con coeficientes en $K[y]$. Ahora bien, $y + 1$ es irreducible en $K[y]$, y es divisor de $y^2 - 1$ sin dividir a 1. Si $(y+1)^2$ fuese divisor de $y^2 - 1$ se tendría necesariamente

$$y^2 - 1 = (y+1)^2, \quad \text{sea} \quad y + y + 1 + 1 = 0,$$

lo que sólo es posible si K es de característica 2. Luego, si la característica de K es distinta de 2, se puede aplicar el resultado 1.°, y $f(x, y)$ es irreducible en $K[x, y]$.

12

Supongamos que 0 es el único elemento nilpotente de A, y que

$$f(x)\, g(x) = e,$$

con

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{j=0}^{n} b_j x^j, \quad a_n \neq 0, \quad b_p \neq 0, \quad n \geqslant p \geqslant 1.$$

Puesto que $a_0 b_0 = e$, se puede suponer, sustituyendo si es necesario $f(x)$ y $g(x)$ por $b_0 f(x)$ y $a_0 g(x)$, que $a_0 = b_0 = e$.

Demostremos por recurrencia que para todo valor del entero k tal que $0 \leqslant k \leqslant p$, se tiene $a_n^{k+1} b_{p-k} = 0$. La igualdad $a_n b_p = 0$ resulta de la definición de producto en $A[x]$. Si se supone establecido que

$$a_n b_p = a_n^2 b_{p-1} = \ldots = a_n^k b_{p-k+1} = 0,$$

la relación

$$a_{n-k} b_p + \ldots + a_{n-k+h} b_{p-h} + \ldots + a_n b_{p-k} = 0$$

implica $a_n^{k+1} b_{p-k} = 0$.

Resulta $a_n^{p+1} b_0 = 0$, es decir, $a_n^{p+1} = 0$, lo que contradice la hipótesis $a_n \neq 0$. Los únicos elementos inversibles de $A[x]$ son, pues, los elementos inversibles de A (considerado como subanillo de $A[x]$).

Recíprocamente, para demostrar que *b*) implica *a*), basta establecer que si existiese en A un elemento nilpotente no nulo a, existirían en $A[x]$ elementos inversibles de grado al menos 1. Supongamos, en efecto, $a^\alpha = 0$, $a^{\alpha-1} \neq 0$. Es claro que

$$(e + a^{\alpha-1} x)(e - a^{\alpha-1} x) = e - a^{2\alpha-2} x^2 = e,$$

lo que concluye la demostración.

13

1.° Sea $a \in A^*$ tal que $\varphi(a)$ sea mínimo. Según (C_2) existen e y r tales que $a = ea + r$, con $r = 0$ o $\varphi(r) < \varphi(a)$. Por ser imposible esta última desigualdad, es $r = 0$ y $a = ea$, lo que implica, para todo $x \in A$, $(x - xe)a = 0$

y, por ser A íntegro, $x = xe$. Luego e es elemento unidad a la derecha y, según ejercicio V, 1, es elemento unidad de A. En lo sucesivo lo indicaremos con 1.

Si x es una unidad existe $x' \in A^*$ tal que $x' x = 1$, de donde

$$\varphi(x) \leqslant \varphi(x' x) = \varphi(1),$$

y $\varphi(x) = \varphi(1)$. Recíprocamente, $\varphi(x) = \varphi(1)$ implica la existencia de un inverso a la izquierda x', pues $1 = qx + r$, con $\varphi(r) < \varphi(x)$, es imposible. Según ejercicio V, 1, x' es inverso de x, y x es una unidad.

Supongamos que para un par (a, b) de elementos de A^* se tenga $\varphi(b) = \varphi(ab)$. Existen entonces q y r tales que $b = qab + r$, con $r = 0$ o $\varphi(r) < \varphi(ab) = \varphi(b)$. No puede ser $r \neq 0$, porque esto implicaría $r = (1 - qa)b$, de donde $\varphi(r) \geqslant \varphi(b)$. Luego $r = 0$, y q es inverso de a.

Recíprocamente, si a es inversible y si $a' a = 1$, las desigualdades

$$\varphi(b) \leqslant \varphi(ab) \quad \text{y} \quad \varphi(b) = \varphi(a' ab) \geqslant \varphi(ab),$$

implican $\varphi(b) = \varphi(ab)$.

2.° Sea I un ideal a la izquierda de A. Si $I = (0)$, $I = A0$. Si $I \neq (0)$, sea c un elemento no nulo de I tal que $\varphi(c)$ sea mínimo. Es claro que $Ac \subseteq I$. Recíprocamente, para todo $x \in I$ existen q y r tales que $x = qc + r$, con $r = 0$ o $\varphi(r) < \varphi(c)$. Puesto que $r = x - qc \in I$, $r \neq 0$ es imposible, de donde $x \in Ac$ e $I = Ac$.

Dados a y b no nulos, existen, pues, d y m tales que

$$Aa + Ab = Ad, \qquad Aa \cap Ab = Am.$$

Entonces se verifica inmediatamente que

α) los divisores a la derecha comunes a a y b son exactamente los divisores a la derecha de d,

β) los múltiplos a la izquierda comunes a a y b, son exactamente los múltiplos a la izquierda de m,

γ) poniendo $a = a_1 d$, $b = b_1 d$ y $d = pa + qb$, se obtiene

$$a_1 qb = (1 - a_1 p)\, a, \qquad b_1 pa = (1 - b_1 q)\, b.$$

Puesto que p y q no son ambos nulos, uno al menos de los elementos $a_1 qb$ y $b_1 pa$ es un múltiplo a la izquierda no nulo de a y b.

3.° Supongamos que $a = bq + r = q' b + r'$, con $r = 0$ o $\varphi(r) < \varphi(b)$, y $r' = 0$ o $\varphi(r') < \varphi(b)$.

Si r y r' son distintos no nulos, $\varphi(r - r') = \varphi[(q' - q)\, b] > \varphi(b)$ contra (C_3). Se tiene un resultado análogo si uno de los elementos r, r' es nulo, de donde, puesto que A es íntegro, $q = q'$.

Sean K^* el grupo de unidades de A, a y b dos elementos distintos de K^*. La condición (C_3) implica $\varphi(a - b) = \varphi(1)$, luego $a - b \in K^*$. Esto demuestra que $K = K^* \cup \{0\}$ es un grupo aditivo, y por consiguiente un cuerpo.

Supongamos ahora que a y b son dos elementos de A^* tales que

$$\varphi(a) < \varphi(b).$$

Entonces, $c = a - b \neq 0$. (C_3) implica $\varphi(c) \leqslant \varphi(b)$. La desigualdad estricta es imposible, en virtud de $b = a - c$ y de (C_3). Se tiene, pues, $\varphi(a - b) = \varphi(b)$.

Puede suceder que $A = K$. Por el contrario, si la función φ, con valores enteros, no es constante sobre A^*, existe al menos un $\xi \in A^*$ tal que

$$\varphi(\xi) > \varphi(1)$$

y que la desigualdad estricta $\varphi(a) < \varphi(\xi)$ implique $\varphi(a) = \varphi(1)$. La sucesión de los $\varphi(\xi^n)$ es entonces estrictamente creciente, luego no acotada. En efecto, $\varphi(\xi^n) \leqslant \varphi(\xi^{n+1})$ por (C_1), y la igualdad para un valor particular de n implicaría $\xi \in K^*$.

Demostremos que A coincide con el conjunto $K[\xi]$ de las expresiones polinómicas de la forma

$$a_0 + a_1 \xi + \ldots + a_n \xi^n \quad (a_i \in K).$$

Es claro que $K[\xi] \subseteq A$ y que

$$\varphi(a_0 + a_1 \xi + \ldots + a_n \xi^n) = \varphi(\xi^n) \text{ si } a_n \neq 0.$$

Para todo $f \in A - K$ existen $f_1 \in A$ y $a_0 \in K$ tales que $f = f_1 \xi + a_0$. Si $f_1 \in K$ se tiene $f \in K[\xi]$. Si no, se vuelve a emprender la operación y se llega, al cabo de un número finito de divisiones, a

$$f = a_0 + a_1 \xi + \ldots + a_n \xi^n + f_{n+1} \xi^{n+1}, \quad a_i \in K.$$

Si $f_{n+1} = 0$, $f \in K[\xi]$. Si no, $\varphi(f) = \varphi(f_{n+1} \xi^{n+1}) \geqslant \varphi(\xi^{n+1})$. Existe, pues, un n_0 tal que $f_{n+1} = 0$ para todo n superior o igual a n_0, y $f \in K[\xi]$. Esto termina de demostrar que $A = K[\xi]$.

Nota. El ejercicio V, 10, proporciona un procedimiento que permite construir anillos que satisfacen las condiciones (C_1), (C_2) y (C_3), y también anillos que no las satisfacen.

14

1.° Es claro que si V' y V'' son dos elementos de $\mathbf{Z}[[x]]$ se tiene

$$\varphi(V'\,V'') = \varphi(V')\,\varphi(V'').$$

Por consiguiente, el conjunto de los $\dfrac{U}{V}$ tales que $\varphi(V) = 1$, es estable para la adición y la multiplicación. Es un subanillo A del cuerpo K de fracciones de $\mathbf{Z}[[x]]$.

Si suponemos $\varphi(V) = 1$ y $\omega(V) = 0$, V se escribe

$$V = \varepsilon(1 + a_1 x + \ldots + a_n x^n + \ldots), \qquad a_i \in \mathbf{Z}, \qquad \varepsilon = \pm 1.$$

Si se supone $\varphi(V) = 1$ y $\omega(V) = \alpha > 0$, V se escribe

$$V = \varepsilon x^{\alpha}(1 + a_1 x + \ldots + a_n x^n + \ldots), \qquad a_i \in \mathbf{Z}, \qquad \varepsilon = \pm 1.$$

La serie formal $1 + a_1 x + \ldots + a_n x^n + \ldots$ es inversible en $\mathbf{Z}[[x]]$ (véase ejercicio V, 10, o el punto 2.°). Resulta que $\dfrac{U}{V}$, donde $\varphi(V) = 1$, puede escribirse $x^{\beta}U_1$, donde $\beta \in \mathbf{Z}$ (con la convención $x^0 = 1$) y $U_1 \in \mathbf{Z}[[x]]$. Si $U \neq 0$, se puede imponer $\omega(U_1) = 0$. La escritura $x^{\beta}\,U_1$ de un elemento no nulo es entonces única, y permite prolongar la función φ al anillo A poniendo

$$\varphi(x^{\beta}\,U_1) = \varphi(U_1).$$

Es claro que en A se conserva la propiedad $\varphi(V'\,V'') = \varphi(V')\,\varphi(V'')$.

2.° Pongamos

$$U = \sum_{n=0}^{\infty} u_n x^n, \qquad V = \sum_{n=0}^{\infty} v_n x^n, \qquad v_0 \neq 0.$$

Las igualdades

$$(1) \qquad \begin{cases} u_0 = v_0 w_0 \\ u_1 = v_0 w_1 + v_1 w_0 \\ \ldots\ldots\ldots\ldots\ldots \\ u_n = v_0 w_n + v_1 w_{n-1} + \ldots + v_k w_{n-k} + \ldots + v_n w_0 \\ \ldots\ldots\ldots\ldots\ldots \end{cases}$$

permiten calcular paso a paso los coeficientes racionales

$$w_0, \ldots, w_n, \ldots$$

tales que la serie formal

$$W = \sum_{n=0}^{\infty} w_n x^n \in \mathbf{Q}[[x]]$$

verifique la igualdad $U = VW$.

(Señalemos que si $v_0 = \pm 1$, es decir, si $\varphi(V) = 1$, los w_n son todos enteros.)

Supongamos $w_0, w_1, \ldots, w_{k-1}$ enteros y w_n no entero. Las igualdades (1) demuestran que el producto $v_0 w_k$ es entero, luego también $\varphi(V)w_k$.

Entonces w_k se puede escribir

$$w_k = w'_k + \frac{h}{\varphi(V)},$$

donde w'_k es la parte entera de w_k y h un entero natural tal que $0 < h < \varphi(V)$.

Pongamos

$$P = w_0 + w_1 x + \ldots + w_{k-1} x^{k-1} + w'_k x^k.$$

La serie formal $T = U - PV$ es de coeficientes enteros, y su primer coeficiente no nulo es $\frac{hv_0}{\varphi(V)}$ (coeficiente de x^k). Se tiene pues $\omega(T) = k$,

$$\varphi(T) < \varphi(V).$$

3.° Sean $U_1 = x^\alpha U$, $V_1 = x^\beta V$ dos elementos de A,

$$(\alpha, \beta \in \mathbf{Z},\ U, V \in \mathbf{Z}[[x]],\ V_1 \neq 0,\ \omega(V) = 0).$$

Entonces son posibles dos casos:

a) Existe $W \in \mathbf{Z}[[x]]$ tal que $U = VW$. Entonces $U_1 = V_1 W_1$ con

$$W_1 = x^{\alpha-\beta} W \in A;$$

b) Existen un polinomio P y una serie formal T de coeficientes enteros tales que

$$U = PV + T, \quad \varphi(T) < \varphi(V).$$

Entonces $U_1 = P_1 V_1 + T_1$, con

$$P_1 = x^{\alpha-\beta} P \in A, \; T_1 = x^{\alpha} T \in A \quad \text{y} \quad \varphi(T_1) = \varphi(T) < \varphi(V) = \varphi(V_1).$$

El anillo A es, pues, euclídeo.

15

1.° La igualdad $x^2 - dy^2 = 0$, donde $x, y \in \mathbf{Q}$, implica $x = y = 0$. En efecto, ella implica, si se supone $y \neq 0$, la existencia de dos números naturales p, q, primos entre sí, tales que $p^2 = dq^2$, y todo factor primo de p figuraría por lo menos al cuadrado, en la descomposición de d en factores primos.

Análogamente, la igualdad $x + y\alpha = 0$ implica $x = y = 0$. En efecto,

$$x^2 - dy^2 = (x + y\alpha)(x - y\alpha).$$

Se verifica inmediatamente que los conjuntos considerados son en efecto subanillos del cuerpo de los complejos, y que todo elemento no nulo de la forma $x + y\alpha$ $(x, y \in \mathbf{Q})$ admite como inverso

$$x' + y'\alpha = \frac{x - y\alpha}{x^2 - dy^2},$$

donde $x', y' \in \mathbf{Q}$.

Si $z' = x' + y'\alpha$, $z'' = x'' + y''\alpha$, son dos elementos de $\mathbf{Q}[\alpha]$, su producto es

$$z' z'' = x' x'' + dy' y'' + (x' y'' + y' x'')\alpha,$$

de donde

$$N(z' z'') = (x' x'' + dy' y'')^2 - d(x' y'' + y' x'')^2 =$$
$$= (x'^2 - dy'^2)(x''^2 - dy''^2) = N(z') N(z'').$$

Si z' y z'' son elementos de A, $N(z')$ y $N(z'')$ son enteros relativos. Una condición necesaria para que z' sea inversible en A es que $N(z')$ divida a $N(1) = 1$, luego $N(z') = \pm 1$. Recíprocamente, si $N(z') = \varepsilon = \pm 1$, el inverso de z' en $\mathbf{Q}[\alpha]$ es $\varepsilon(x' - y'\alpha)$, y z' es inversible en A. Las unidades de A se caracterizan, pues, por $N(z) = \pm 1$.

2.° Sean $z = x + y\alpha$ un elemento de $\mathbf{Q}[\alpha]$, x' e y' dos enteros tales que

$$|x - x'| < \tfrac{1}{2}, \quad |y - y'| < \tfrac{1}{2}.$$

Entonces $z' = x' + y'\alpha$ es un elemento de A, y

$$N(z - z') = (x - x')^2 - d(y - y')^2.$$

Si $d = -1$ o -2, $N(z - z')$ es positivo o nulo, y además

$$N(z - z') < \tfrac{1}{4} + 2 \cdot \tfrac{1}{4} < 1.$$

Si $d = 2$ o 3, $-\tfrac{3}{4} < N(z - z') < \tfrac{1}{4}$, de donde $| N(z - z') | < 1$.

Si $a + b\alpha$ y $u + v\alpha$ son dos elementos de A, el segundo distinto de cero, y si

$$\frac{a + b\alpha}{u + v\alpha} = z \notin A,$$

se tendrá $z = z' + r$, con $| N(r) | < 1$, es decir

$$a + b\alpha = (u + v\alpha)(x' + y'\alpha) + r(u + v\alpha),$$

con $r(u + v\alpha) \in A$ y $| N[r(u + v\alpha)] | < | N(u + v\alpha) |$.

Por tanto el anillo A es un anillo euclídeo.

Nota. Se demuestra que el anillo A es también euclídeo para otros valores de d. Pero no lo es siempre: así, sabemos que no es euclídeo para $d = -5$ (texto: IV, 6).

16

1.° Sea $ba \neq 0$, $a, b \in A$. El conjunto de los x de A tales que $xa = 0$, es un ideal a la izquierda de A, que no contiene a b, luego diferente de A, y por consiguiente reducido al elemento 0. Luego a no puede ser divisor de cero a la derecha.

El ideal a la izquierda Aa no es nulo, pues contiene a ba. Luego $Aa = A$, y existe $e \in A$ tal que $a = ea$, de donde $a = ea = e^2 a$ y $(e - e^2)a = 0$, lo que implica $e = e^2$.

Para todo $x \in A$, es $xa = xea$, de donde $(x - xe)a = 0$, y $x = xe$. Luego e es elemento unidad a la derecha. El conjunto de elementos de la forma $x - ex$ es un ideal a la izquierda L. Si fuese $L = A$, existiría $c \in A$, tal que $e = c - ec$, de donde $e = e^2 = e(c - ec) = 0$, y $a = ea = 0$, en contradicción con $ba \neq 0$. Se tiene pues $L = (0)$ es decir, $x = ex$, de donde e es elemento unidad bilátera.

En fin, todo x no nulo es tal que $x = ex \neq 0$ de donde $Ax = A$. Posee, pues, un inverso a la izquierda. Entonces $A^* = A - \{0\}$ es un grupo (texto: II, 2) y A es un cuerpo.

2.° Si todo producto de elementos de A es nulo, A será conmutativo, y sus ideales serán los subgrupos de su grupo aditivo. Sea $a \neq 0$, $a \in A$. El subgrupo aditivo engendrado por a coincide necesariamente con A, y es finito de orden primo, pues si no contendría subgrupos aditivos propios.

17

Sean I, J dos ideales a la izquierda de A.

Supongamos $I \nsubseteq J$ y $J \nsubseteq I$. Existen entonces elementos i, j de A tales que $i \in I$, $i \notin J$, $j \in J$, $j \notin I$.

La unión de dos partes multiplicativamente lícitas a la izquierda es también una parte multiplicativamente lícita a la izquierda, luego es un ideal a la izquierda. Resulta que $i + j \in I \cup J$. Pero si $i + j \in I$, se llega a la contradicción $j \in I$. Lo mismo, es imposible $i + j \in J$. Luego, uno de los dos ideales a la izquierda I, J contiene al otro.

18

1.° La propiedad es cierta para $n = 2$. Supuesta verdad para $n = k$, sean x e y dos elementos de A. Si, por ejemplo, $(x) \subseteq (y)$, existen $r \in \mathbf{Z}$ y $a \in A$, tales que $x = ry + ay$, de donde

$$xy - yx = (ay - ya)\, y \in A^{k+1}.$$

Una consecuencia interesante es la siguiente: Si el anillo A es nilpotente, es decir, si existe un entero n tal que $A^n = (0)$, y si satisface a la condición del enunciado, el anillo A es conmutativo.

2.° Sea P una parte multiplicativamente lícita a la izquierda de A. Si x, y son dos elementos de P y si, por ejemplo, $Ax \subseteq Ay$, existen dos elementos u, v de A tales que $x = uy$, $y = vy$, de donde $x - y = (u - v)\, y$, luego $x - y \in P$. Por tanto P es un ideal a la izquierda.

Nota. De lo anterior y del ejercicio precedente resulta que si los ideales a la izquierda principales de A constituyen un conjunto totalmente ordenado, y si $x \in Ax$ para todo $x \in A$, entonces los ideales a la izquierda de A constituyen también un conjunto totalmente ordenado.

Supongamos ahora A conmutativo. Para todo elemento no nulo x de A, existe $u \in A$ tal que $x = ux$.

Si y es otro elemento no nulo de A, existe $v \in A$ tal que $y = vx$ o $x = vy$. Si $y = vx$, $yu = vxu = vx = y \neq 0$. Si $x = vy$, $vyu = xu = x \neq 0$. Luego u no es divisor de cero.

Existe $e \in A$ tal que $u = eu$. Se tiene entonces, para todo $t \in A$, $u(et - t) = 0$, de donde $et = t$, y e es elemento unidad de A.

19

1.° Es claro que A_i $(i = 1, 2)$ es un subanillo de A isomorfo a B_i. Es un ideal bilátero de A, pues se tienen las igualdades

$$(y_1, y_2)(x_1, 0) = (y_1 x_1, 0) \in A_1,$$
$$(x_1, 0)(y_1, y_2) = (x_1 y_1, 0) \in A_1,$$

e igualdades análogas concernientes a los elementos de A_2.

Sea $\mathfrak{g}_1$ un ideal a la izquierda de A_1. Es también un ideal a la izquierda de A, pues

$$A\mathfrak{g}_1 = (A_1 + A_2)\mathfrak{g}_1 = A_1\mathfrak{g}_1 \subseteq \mathfrak{g}_1.$$

Se ve del mismo modo que un ideal a la derecha de A_1 es un ideal a la derecha de A. Propiedades análogas tiene A_2.

2.° El elemento unidad de A se escribe $e = \varepsilon_1 + \varepsilon_2$ donde $\varepsilon_i (i = 1, 2)$ es elemento unidad del subanillo A_i.

La existencia de una descomposición $\mathfrak{g} = \mathfrak{g}_1 + \mathfrak{g}_2$, donde $\mathfrak{g}_i$ es ideal a la izquierda de A_i, resulta de la distributividad de la multiplicación de ideales a la izquierda respecto a la adición:

$$\mathfrak{g} = A\mathfrak{g} = (A_1 + A_2)\mathfrak{g} = A_1\mathfrak{g} + A_2\mathfrak{g}.$$

Poniendo $\mathfrak{g}_i = A_i\mathfrak{g}$ $(i = 1, 2)$, $\mathfrak{g}_i$ es efectivamente un ideal a la izquierda de A_i.

La unicidad resulta del hecho de que los productos $A_1 A_2$ y $A_2 A_1$ se reducen al elemento 0: si $\mathfrak{g} = \mathfrak{g}_1' + \mathfrak{g}_2'$ se tiene $\mathfrak{g}_1' = A_1\mathfrak{g}$ y $\mathfrak{g}_2' = A_2\mathfrak{g}$, es decir

$$\mathfrak{g}_1' = \mathfrak{g}_1, \quad \mathfrak{g}_2' = \mathfrak{g}_2.$$

Supongamos $\mathfrak{g} = (a\} = Aa$. Entonces, poniendo $a = a_1 + a_2$ $(a_i \in A_i)$, se tiene

$$\mathfrak{g} = (A_1 + A_2)(a_1 + a_2) = A_1 a_1 + A_2 a_2,$$

es decir, $\mathfrak{g}_i = A_i a_i$, ideal a la izquierda principal. Inversamente, si suponemos $\mathfrak{g}_1 = A_1 a_1$, $\mathfrak{g}_2 = A_2 a_2$, queda claro que $\mathfrak{g}_1 + \mathfrak{g}_2 \subseteq A(a_1 + a_2)$ y que todo elemento de este ideal a la izquierda, al ser de la forma $\beta_1 a_1 + \beta_2 a_2$, pertenece a $\mathfrak{g}_1 + \mathfrak{g}_2$ que por tanto es principal.

3.° Sea f el homomorfismo canónico $A \to A/\mathfrak{m}$.

Todo elemento γ de $f(A)$ es de la forma $\gamma_1 + \gamma_2$, donde $\gamma_i \in f(A_i)$ $(i = 1, 2)$. Esta descomposición es única, pues $0 = f(a_1) + f(a_2)$ implica $a_1 + a_2 \in \mathfrak{m}$, o sea $a_i \in \mathfrak{m}_i$ y $f(a_i) = 0$.

Para dos elementos $\gamma' = \gamma'_1 + \gamma'_2$, $\gamma'' = \gamma''_1 + \gamma''_2$, donde γ'_i, $\gamma''_i \in f(A_i)$ la adición y la multiplicación se realizan componente a componente, pues $\gamma'_1 \gamma''_2$, por ejemplo, es nulo, en virtud de $A_1 A_2 = 0$. Luego $f(A)$ es isomorfo al anillo producto $f(A_1) \times f(A_2)$.

La restricción de f a A_i es un homomorfismo cuyo núcleo es $\mathfrak{m} \cap A_i$, es decir, $\mathfrak{m}_i$. Luego $f(A_i)$ es isomorfo al anillo cociente $A_i/\mathfrak{m}_i$.

Puesto que A es conmutativo y tiene elemento unidad, $\mathfrak{m}$ es un ideal maximal si y sólo si $A/\mathfrak{m}$ es un cuerpo; es un ideal primo si y sólo si $A/\mathfrak{m}$ es íntegro; es un ideal primario si y sólo si $A/\mathfrak{m}$ sólo admite divisores de cero que sean nilpotentes.

Si $\mathfrak{m}_1 \neq A_1$ y $\mathfrak{m}_2 \neq A_2$, las imágenes en $f(A) = A/\mathfrak{m}$ de los idempotentes ε_1 y ε_2 son divisores de cero no nilpotentes, y $\mathfrak{m}$ no puede ser ni primario, ni primo, ni maximal.

Si, por ejemplo, $\mathfrak{m}_2 = A_2$ es claro que $f(A)$ es un anillo isomorfo a $f(A_1)$, es decir, $A/\mathfrak{m} \simeq A_1/\mathfrak{m}_1$. Luego $\mathfrak{m}$ es maximal (respectivamente: primo; primario) si y sólo si uno de sus componentes es un ideal maximal (respect.: primo; primario) siendo el otro el ideal unidad del anillo A_i correspondiente.

20

1.° Sea U el grupo de unidades de A. Todo ideal propio $\mathfrak{a}$ es disjunto de U: en efecto, si $x \in \mathfrak{a} \cap U$, y si x^{-1} es inverso de x, $e = xx^{-1} \in \mathfrak{a}$ y $\mathfrak{a} = A$. Resulta que si el complementario de U en A es un ideal, es el elemento máximo del conjunto de los ideales propios.

Recíprocamente, si A admite un ideal propio máximo $\mathfrak{m}$, y si a no es inversible, el ideal (a) es propio, de donde $(a) \subseteq \mathfrak{m}$, y $a \in \mathfrak{m}$. El conjunto de elementos no inversibles de A es, pues, un ideal.

2.° Supongamos que existe en el anillo casi local A un elemento f tal que

$$f = f^2, \quad f \neq 0, \quad f \neq e.$$

La igualdad $f = f^2$ se escribe $f(e - f) = 0$. Entonces ni f ni $e - f$ son inversibles, ni tampoco su suma, e, lo que contradice la hipótesis. Luego 0 y e son los únicos elementos idempotentes de A.

3.° Supongamos que el conjunto de los ideales principales de A sea totalmente ordenado. Sean a y b dos elementos no inversibles de A y x un elemento cualquiera de A.

xa no es inversible, pues $x'(xa) = e$ significaría que a tiene como inverso x' x.

Si, por ejemplo, $(b) \subseteq (a)$, existe y tal que $b = ya$. Si $a - b$ fuese inversible llegaríamos a una contradicción, pues $t\,(a - b) = e$ significaría

$$t(a - ya) = t(e - y)a = e,$$

de donde a tendría inverso, $t(e - y)$.

Los elementos no inversibles forman, pues, un ideal, y A es casi local.

4.° La hipótesis $\mathfrak{m} = (m)$ implica $\mathfrak{m}^n = (m^n)$ para todo entero natural n. Sea $\mathfrak{a}$ un ideal propio, luego no nulo, de A. Si a es un elemento no nulo de $\mathfrak{a}$, no pertenece a todos los $\mathfrak{m}^n$. Existe pues un entero $\alpha \geqslant 1$ tal que $a \in \mathfrak{m}^\alpha$, $a \notin \mathfrak{m}^{\alpha+1}$, luego existe un $x \in U$ tal que $a = xm^\alpha$. Se tiene entonces $\mathfrak{m}^\alpha = (m^\alpha) = (a) \subseteq \mathfrak{a}$, y $\mathfrak{a}$ es la unión de los $\mathfrak{m}^n$ con los que tiene elementos comunes. Como el conjunto de los $\mathfrak{m}^n$ es una cadena, $\mathfrak{a}$ es una potencia de $\mathfrak{m}$. El anillo A es en este caso un anillo principal (texto: VII, 3).

Supongamos además que A es íntegro, y sea K su cuerpo de fracciones. Si x es un elemento no nulo de K, es $x = \dfrac{a}{b}$, donde $a = a'\,m^\alpha$, $b = b'\,m^\beta$ (a', $b' \in U$; α, β enteros naturales, con la convención $m^0 = e$). Es claro que $\alpha \geqslant \beta$ implica $x \in A$, y que $\alpha \leqslant \beta$ implica $x^{-1} \in A$.

Ejemplo. Sean k un cuerpo conmutativo y $A = k[[x]]$ el anillo de las series formales en una indeterminada x con coeficientes de k.

Si $f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$ es un elemento de A, $f(x)$ es inversible si y sólo si $a_0 \neq 0$ (ejercicio V, 10). El conjunto de elementos no inversibles es pues el ideal (x) y A es casi local.

La intersección de los (x^n) es el ideal nulo, y el anillo A es íntegro, luego son aplicables los resultados del apartado 4.°. En particular, todo ideal no nulo es de la forma (x^k).

21

Si x, y son dos elementos de A que suman e (elemento unidad de A), uno de los dos al menos, es inversible.

1.° La condición distributiva, aplicada a los tres ideales (a), (b), $(a - b)$, implica

$$(a) = (a) \cap [(b) + (a - b)] = [(a) \cap (b)] + [(a) \cap (a - b)].$$

Existen pues $u \in (a) \cap (b)$ y $w \in (a) \cap (a - b)$ tales que $a = u + w$. Se puede escribir $w = v(a - b)$, con $vb \in (a)$.

Si v es inversible, se tiene por ello $b \in (a)$. Si no, $e - v$ es inversible, y

$$a(e - v) = u - bv \in (b)$$

implica $a \in (b)$. Resulta que los ideales principales constituyen un conjunto totalmente ordenado, luego también todos los ideales, según ejercicio V, 18, nota.

2.° Queda claro que

$$ab \in (a)(a, b) \cap (b)(a, b) = [(a) \cap (b)](a, b),$$

lo que demuestra la existencia de $x, y \in (a) \cap (b)$ tales que

$$ab = xa + yb.$$

Existen $x', y' \in A$ tales que $x = bx'$, $y = ay'$, de donde

$$ab(e - x' - y') = 0$$

y puesto que A es íntegro, $x' + y' = e$.

Si x' es inversible, $b \in (x) \subseteq (a)$. Si no, y' es inversible y $a \subseteq (y) \subseteq (b)$. La demostración se termina como en el apartado 1.°.

22

1.° De la definición de centro de un anillo, resulta que *a*) implica *b*).

Para demostrar que *b*) implica *c*), es suficiente (ejercicio V, 1) demostrar que e es único elemento unidad a la izquierda de B. Es claro que para todo $x \in B$, $x = ex$. Si f fuese otro elemento unidad a la izquierda, sería idempotente, de donde,

$$f = ef = fe = e.$$

c) implica *d*) pues, para todo $x \in B$, $x = ex = xe = exe$, de donde $eA \subseteq eAe$. Como $eAe \subseteq eA$, se tiene $B = eAe$. Un cálculo análogo demuestra que

$$B' = Ae = eAe,$$

de donde $eAe = eA = aA$.

En fin, *d*) implica *a*), pues para todo elemento $y \in A$, se tiene $ye \in B$, $ey \in B$, de donde $ey = eye = ye$.

2.° *α*) Si $\mathfrak{g}$ es un ideal a la izquierda de B, la igualdad $e\mathfrak{g} = \mathfrak{g}$ implica

$$A\mathfrak{g} = Ae\mathfrak{g} = B\mathfrak{g} \subseteq \mathfrak{g}$$

y $\mathfrak{g}$ es un ideal a la izquierda de A. Se puede señalar que un resultado análogo se obtiene para un ideal a la derecha o bilátero.

β) Sea $y \in A$. Pongamos $b = ey = eye = ye$, $c = y - b$. Entonces $ec = ce = 0$, lo que prueba la posibilidad de la descomposición. Si se tiene

$$y = b + c = b' + c' \quad (b, b' \in B, ec = ce = ec' = c'e = 0),$$

el elemento $p = b - b' = c' - c$ pertenece a B, de donde $p = ep$ y $e(c' - c) = 0$, lo que demuestra la unicidad de la descomposición.

23

1.° Puesto que I no es el ideal nulo, contiene polinomios no nulos. El conjunto de los grados de estos polinomios es una parte no vacía del conjunto N de enteros naturales, luego admite un elemento mínimo t. Al menos es $t = 1$, puesto que $t = 0$ significaría que $A \cap I$ no es el ideal nulo.

2.° La igualdad $fg = 0$ implica $a_n b_t = 0$. Los productos $a_i b_t (0 \leqslant i < n)$ no son nulos, sino se tendría $b_t f = 0$, es decir $b_t \in A \cap I$. Los polinomios $g_i = a_i g$ $(0 \leqslant i \leqslant n)$ no son, pues, todos nulos. Sea q el mayor de los índices i para los que $g_i \neq 0$.

Está claro que $g_q \in I$. Si $q = n$, el grado de g_q es inferior a t en virtud de $a_n b_t = 0$; si $q < n$, los polinomios $g_{q+1}, \ldots, g_n$ son nulos, y la igualdad

$$0 = fg = (a_0 + a_1 x + \ldots + a_q x^q)\, g + x^{q+1} g_{q+1} + \ldots + x^n g_n$$

implica $a_q b_t = 0$, es decir, que el grado de g_q es todavía inferior a t.

Estos resultados se contradicen con la definición de t. Luego, $I \cap A = (0)$ implica $I = (0)$, es decir, $I \neq (0)$ implica $I \cap A \neq (0)$, lo que se puede enunciar del siguiente modo: si $f \in A[x]$ es divisor de cero, existe un elemento no nulo $c \in A$ tal que $cf = 0$

24

Si p es irreducible, y si $xy \in (p)$, existe $a \in A$ tal que $xy = ap$. Según la condición de Gauss, p divide al menos a uno de los elementos x, y, luego uno al menos de estos elementos pertenece al ideal (p) que por tanto es primo.

Si p no es irreducible, es producto de elementos irreducibles

$$p = p_1 p_2 \dots p_k, \quad k > 2.$$

En este caso, ninguno de los $p_j (j = 1, 2, \dots, k)$ pertenece a (p), mientras que su producto pertenece a (p). Luego (p) no es primo.

25

1.° Si $\mathfrak{r}'$ es el radical del ideal $\mathfrak{a}'$ de A', está claro que se tienen las equivalencias siguientes ($\mathcal{R}$ designa el radical)

$$\begin{aligned} x \in f^{-1}(\mathfrak{r}') &\Leftrightarrow f(x) \in \mathfrak{r}' \Leftrightarrow (\exists n \in \mathbf{N})\, [f(x)]^n \in \mathfrak{a}' \\ &\Leftrightarrow (\exists x \in \mathbf{N})\, f(x^n) \in \mathfrak{a}' \Leftrightarrow (\exists x \in \mathbf{N})\, x^n \in f^{-1}(\mathfrak{a}') \\ &\Leftrightarrow x \in \mathcal{R}\,[f^{-1}(\mathfrak{a}')]. \end{aligned}$$

Por tanto, $f^{-1}(\mathfrak{r}')$ es el radical de $f^{-1}(\mathfrak{a}')$.

Supongamos $\mathfrak{a}'$ primo. Sean $a, b \in A$, tales que $ab \in f^{-1}(\mathfrak{a}')$, $\mathfrak{a} \notin f^{-1}(\mathfrak{a}')$. Entonces

$$f(ab) = f(a) f(b) \in \mathfrak{a}', \quad f(a) \notin \mathfrak{a}',$$

luego $f(b) \in \mathfrak{a}'$ y $b \in f^{-1}(\mathfrak{a}')$; por tanto $f^{-1}(\mathfrak{a}')$ es primo.

Supongamos $\mathfrak{a}'$ primario. Su radical $\mathfrak{r}'$ es primo, y $f^{-1}(\mathfrak{r}')$ es el radical (primo) de $f^{-1}(\mathfrak{a}')$. Sean $a, b \in A$ tales que $ab \in f^{-1}(\mathfrak{a}')$, $a \notin f^{-1}(\mathfrak{r}')$. Entonces

$$f(ab) = f(a) f(b) \in \mathfrak{a}', \quad f(a) \notin \mathfrak{r}',$$

luego $f(b) \in \mathfrak{a}'$ y $b \in f^{-1}(\mathfrak{a}')$; luego $f^{-1}(\mathfrak{a}')$ es primario.

2.° Para cualquier ideal $\mathfrak{i}$ conteniendo a $\mathfrak{n}$, sabemos que

$$f^{-1}[f(\mathfrak{i})] = \mathfrak{i}.$$

Pongamos, para $\mathfrak{a} \supseteq \mathfrak{n}$, $\mathfrak{a}' = f(\mathfrak{a})$, $\mathfrak{r}' = \mathcal{R}(\mathfrak{a}')$. Según hemos visto en 1.°, el radical $\mathfrak{r}$ de $\mathfrak{a} = f^{-1}(\mathfrak{a}')$ es $f^{-1}(\mathfrak{r}')$, luego

$$\mathfrak{r}' = f[f^{-1}(\mathfrak{r}')] = f(\mathfrak{r})$$

y $f(\mathfrak{r})$ es efectivamente el radical de $f(\mathfrak{a})$.

Supongamos $\mathfrak{a}$ primo, y sean a', $b' \in A'$ tales que

$$a'\,b' \in \mathfrak{a}' = f(\mathfrak{a}), \qquad a' \notin \mathfrak{a}'.$$

Existen entonces a, $b \in A$ tales que $a' = f(a)$, $b' = f(b)$.

Las relaciones $a' \notin \mathfrak{a}'$ y $a'\,b' \in \mathfrak{a}'$, implican $a \notin \mathfrak{a}$ y $ab \in \mathfrak{a}$, puesto que $\mathfrak{a} \supseteq \mathfrak{n}$, luego $b \in \mathfrak{a}$ de donde $b' \in \mathfrak{a}'$; por tanto $\mathfrak{a}'$ es primo.

Supongamos $\mathfrak{a}$ (conteniendo a $\mathfrak{n}$) primario. Su radical $\mathfrak{r}$ contiene también a $\mathfrak{n}$, y, según lo precedente, $\mathfrak{r}' = f(\mathfrak{r})$ es el radical de $\mathfrak{a}' = f(\mathfrak{a})$. Además, $\mathfrak{r}'$ es primo. Sean a', b' elementos de A' tales que $a'\,b' \in \mathfrak{a}'$, $a' \notin \mathfrak{r}'$. Existen a, $b \in A$ tales que $a' = f(a)$, $b' = f(b)$. Se tiene entonces

$$a \notin \mathfrak{r}, \qquad ab \in \mathfrak{a}$$

luego $b \in \mathfrak{a}$, lo que implica $b' \in \mathfrak{a}'$; luego $\mathfrak{a}' = f(\mathfrak{a})$ es primario.

3.° Por ser un cuerpo conmutativo un anillo factorial, los anillos $\mathbf{Q}[x]$ y $\mathbf{Q}[x, y]$ son factoriales (texto: IV, 6, teor. 5).

El polinomio $x^2 + y^2 - 1$ es irreducible en $\mathbf{Q}[x, y]$ (ejercicio V, 11). Por tanto el ideal $\mathfrak{p} = (x^2 + y^2 - 1)$ es primo en $\mathbf{Q}[x, y]$ (ejercicio V, 24).

La aplicación de $\mathbf{Q}[x, y]$ en $\mathbf{Q}[x]$ definida por

$$h(x, y) \to h(x, 1)$$

es un homomorfismo suprayectivo de anillos, en el cual la imagen del ideal primo $\mathfrak{p}$ es el ideal $\mathfrak{p}' = (x^2)$, que no es semiprimo.

4.° Sea $\mathfrak{p} = (p)$ un ideal primo del anillo principal e íntegro A. Entonces p es irreducible (ejercicio V, 24). Si $(n) = \mathfrak{n}$, y si $(d) = (n) + (p)$, d es divisor de p, luego es o bien una unidad o bien un elemento asociado a p.

Si d es una unidad, existen u, $v \in A$ tales que $un + vp = e$, elemento unidad de A, de donde $f(v)f(p) = e'$, elemento unidad de A'. Entonces $f(p)$ es inversible y $f(\mathfrak{p}) = A'$ es efectivamente primo.

Si d es asociado a p, es p divisor de n, de donde $\mathfrak{n} \subseteq \mathfrak{p}$ y $f(\mathfrak{p})$ es primo según lo establecido en el punto 2.°.

26

1.° Si el ideal $\mathfrak{a}_i$ estuviese contenido en el $\mathfrak{p}_i$ tendríamos

$$\mathfrak{a} \cdot \Big(\prod_{j \neq i} \mathfrak{p}_j\Big) \subseteq \mathfrak{a} \cap \Big(\bigcap_{j \neq i} \mathfrak{p}_j\Big) = \mathfrak{a}_i \subseteq \mathfrak{p}_i,$$

de donde, puesto que las $\mathfrak{p}_j$ no están contenidas en el ideal primo $\mathfrak{p}_i$, $\mathfrak{a} \subseteq \mathfrak{p}_i$, contra la hipótesis. Luego $\mathfrak{a}_i \nsubseteq \mathfrak{p}_i$.

Para cada i existen pues $x_i \in \mathfrak{a}_i$, $x_i \notin \mathfrak{p}_i$. Puesto que x_i pertenece a todos los $\mathfrak{p}_j$ distintos de $\mathfrak{p}_i$, la suma x no puede pertenecer a ninguno de estos ideales primos. Como $x_i \in \mathfrak{a}$ se tiene $x \in \mathfrak{a}$.

2.° La cuestión precedente demuestra que si $\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, existe al menos un índice i_0 tal que $\mathfrak{a} \subseteq \mathfrak{p}_{i_0}$, dado que dos cualesquiera de los $\mathfrak{p}_i$ no sean comparables.

Pero el caso de una familia finita cualquiera $\mathcal{F}$ de ideales primos de A, se lleva fácilmente el caso particular estudiado en lo 1.°, reduciendo $\mathcal{F}$ a sus elementos maximales.

27

Siendo $\mathfrak{m}$ ideal maximal de A, el anillo cociente $A/\mathfrak{m} = \overline{A}$ no admite ningún ideal propio. Según ejercicio V, 16, son posibles dos casos:

1.° Si se pueden encontrar dos elementos de $\overline{A}$ cuyo producto no sea nulo, es decir, dos elementos de A cuyo producto no esté en $\mathfrak{m}$ ($A^2 \nsubseteq \mathfrak{m}$), entonces $\overline{A}$ es un cuerpo, y por tanto $\mathfrak{m}$ es primo, luego es primario.

2.° Si todo producto es nulo en $\overline{A}$, es decir, si $A^2 \subseteq \mathfrak{m}$, queda claro que $\mathfrak{m}$ es primario ($xy \in \mathfrak{m}$, $x \notin \mathfrak{m}$ implica $y^2 \in \mathfrak{m}$). Siendo A el radical de $\mathfrak{m}$, no es $\mathfrak{m}$ ideal primo.

Luego $\mathfrak{m}$ es primo si y sólo si $A^2 \nsubseteq \mathfrak{m}$.

28

1.° Si $a \in \mathfrak{a}$, todo monomio ax^a pertenece a $\varphi(\mathfrak{a})$, luego todo polinomio con coeficientes tomados en $\mathfrak{a}$ es elemento de $\varphi(\mathfrak{a})$.

Recíprocamente, si $f(x) \in \varphi(\mathfrak{a})$, existe un número finito de elementos $a_1, \ldots, a_s$ de $\mathfrak{a}$ y de polinomios $g_1(x), \ldots, g_s(x)$, de $A[x]$ tales que,

$$f(x) = a_1 g_1(x) + \ldots + a_s g_s(x).$$

Ordenando $f(x)$ según las potencias crecientes de x, por ejemplo, es claro que todos los coeficientes obtenidos serán elementos de $\mathfrak{a}$.

2.° La inclusión $\mathfrak{a} \subseteq \varphi(\mathfrak{a}) \cap A$ es evidente. La inclusión opuesta resulta del punto 1.°. Por tanto vale la igualdad.

3.° Es claro que φ es una aplicación creciente del conjunto de los ideales de A en el conjunto de los ideales de $A[x]$. Se deduce inmediatamente,

$$\varphi(\mathfrak{a}_1) + \varphi(\mathfrak{a}_2) \subseteq \varphi(\mathfrak{a}_1 + \mathfrak{a}_2), \quad \varphi(\mathfrak{a}_1 \mathfrak{a}_2) \subseteq \varphi(\mathfrak{a}_1)\varphi(\mathfrak{a}_2), \text{ o } \varphi(\mathfrak{a}_1 \cap \mathfrak{a}_2) \subseteq \varphi(\mathfrak{a}_1) \cap \varphi(\mathfrak{a}_2).$$

Recíprocamente, supongamos $f(x) \in \varphi(\mathfrak{a}_1 + \mathfrak{a}_2)$. Los coeficientes de $f(x)$ están, pues, en $\mathfrak{a}_1 + \mathfrak{a}_2$, y $f(x)$ es la suma de un polinomio $f_1(x) \in \varphi(\mathfrak{a}_1)$ y un polinomio $f_2(x) \in \varphi(\mathfrak{a}_2)$, de donde la igualdad

$$\varphi(\mathfrak{a}_1) + \varphi(\mathfrak{a}_2) = \varphi(\mathfrak{a}_1 + \mathfrak{a}_2).$$

Supongamos ahora $f(x) \in \varphi(\mathfrak{a}_1)\,\varphi(\mathfrak{a}_2)$; $f(x)$ es una suma finita de productos de la forma $f_1(x) f_2(x)$, donde $f_1(x) \in \varphi(\mathfrak{a}_1)$, $f_2(x) \in \varphi(\mathfrak{a}_2)$; los coeficientes de $f(x)$ son, pues, sumas finitas de productos $a_1 a_2$ donde $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$, de donde

$$f(x) \in \varphi(\mathfrak{a}_1\,\mathfrak{a}_2) \quad \text{y} \quad \varphi(\mathfrak{a}_1\,\mathfrak{a}_2) = \varphi(\mathfrak{a}_1)\,\varphi(\mathfrak{a}_2).$$

Supongamos en fin $f(x) \in \varphi(\mathfrak{a}_1) \cap \varphi(\mathfrak{a}_2)$. Los coeficientes de $f(x)$ están, pues, en $(\mathfrak{a}_1 \cap \mathfrak{a}_2)$, de donde

$$f(x) \in \varphi(\mathfrak{a}_1 \cap \mathfrak{a}_2) \quad \text{y} \quad \varphi(\mathfrak{a}_1 \cap \mathfrak{a}_2) = \varphi(\mathfrak{a}_1) \cap \varphi(\mathfrak{a}_2).$$

4.° Puesto que $\mathfrak{a} \subseteq \varphi(\mathfrak{a})$, queda claro que $\mathfrak{a}$ es primo en cuanto lo sea $\varphi(\mathfrak{a})$. Recíprocamente, supongamos $\mathfrak{a}$ primo,

$$f(x)\,g(x) \in \varphi(\mathfrak{a}), \quad f(x) \notin \varphi(\mathfrak{a}), \quad g(x) \notin \varphi(\mathfrak{a}).$$

Se puede entonces escribir,

$$f(x) = f_0(x) + x^h f_1(x), \quad g(x) = g_0(x) + x^k g_1(x),$$

con

$$f_0(x) \in \varphi(\mathfrak{a}), \quad g_0(x) \in \varphi(\mathfrak{a}), \quad f_1(x) \notin \varphi(\mathfrak{a}), \quad g_1(x) \notin \varphi(\mathfrak{a}),$$

con todos los polinomios escritos ordenados según las potencias crecientes de x, con $f_1(0) \notin \mathfrak{a}$, $g_1(0) \notin \mathfrak{a}$.

Se tiene entonces

$$f(x)\,g(x) = f_0(x)\,g_0(x) + x^h f_1(x)\,g_0(x) + x^k f_0(x)\,g_1(x) + \\ + x^{h+k} f_1(x)\,g_1(x) \in \varphi(\mathfrak{a}),$$

de donde $f_1(x)g_1(x) \in \varphi(\mathfrak{a})$, lo que contradice la definición de $f_1(x)$ y $g_1(x)$. Luego $\varphi(\mathfrak{a})$ es un ideal primo de $A[x]$ si $\mathfrak{a}$ es ideal primo de A.

29

El subgrupo aditivo engendrado por B y e es el conjunto de elementos $ne + b (n \in \mathbf{Z}, b \in B)$. Es un anillo, luego coincide con A. Resulta inmediatamente que B es un ideal de A.

1.° Un elemento b de B engendra en A el ideal principal Ab, conjunto de elementos de A que son de la forma

$$(ne + b')\, b = nb + b'\, b \ (n \in \mathbf{Z}, b' \in B);$$

ideal que por tanto coincide con el ideal principal engendrado por b en B.

Si $\mathfrak{b}$ es un ideal de B, contiene pues al ideal principal engendrado en A por cada uno de sus elementos; $\mathfrak{b}$ es por tanto una parte lícita en A. Como es un subgrupo aditivo, es también un ideal de A.

2.° Si B es un ideal de A, es $\mathfrak{a} \cap B = \mathfrak{a}'$ un ideal de A, luego también es un ideal de B. Supongamos que $\mathfrak{a}'$ admite, como ideal de B, una base $\{ b_1, .. , b_s \}$. Entonces, $\mathfrak{a}' = Ab_1 + ... + Ab_s$.

Sea Φ el conjunto de enteros $n \in \mathbf{Z}$ tales que existe un $b \in B$ para el cual $ne + b \in \mathfrak{a}$. Es claro que Φ es un ideal de $\mathbf{Z} : \Phi = \mathbf{Z}n_0$. Sea $b_0 \in B$ tal que $x_0 = b_0 + n_0\, e \in \mathfrak{a}$.

Para todo $y = ne + b \in \mathfrak{a}$, existe $q \in \mathbf{Z}$ tal que $n = qn_0$, de donde

$$y - qx_0 = ne + b - q(n_0\, e + b_0) = b - qb_0 \in \mathfrak{a}'.$$

Esto demuestra que $\mathfrak{a}$ admite la base $\{ x_0, b_1, ..., b_s \}$.

3.° Si $\mathfrak{p}$ es un ideal primo no nulo de A, $\mathfrak{p}' = B \cap \mathfrak{p}$ es un ideal de B no nulo, pues contiene al producto $B\mathfrak{p} \neq (0)$, ya que $B \neq (0)$, $\mathfrak{p} \neq (0)$, siendo A íntegro. En fin, $\mathfrak{p}'$ es primo, pues con $b_1, b_2 \in B$, $b_1\, b_2 \in \mathfrak{p}'$ implica $b_1\, b_2 \in \mathfrak{p}$, luego $b_1 \in \mathfrak{p}'$ o $b_2 \in \mathfrak{p}'$.

30

1.° Puesto que $x \in \mathfrak{b}$, $x \notin \mathfrak{a}$, se tiene $Ax \subseteq \mathfrak{b}$, $Ax \nsubseteq \mathfrak{b}$, de donde

$$\mathfrak{a} \subset \mathfrak{a} + Ax \subseteq \mathfrak{b},$$

lo que implica $\mathfrak{b} = \mathfrak{a} + Ax$, puesto que $\mathfrak{b}$ cubre a $\mathfrak{a}$.

Lo mismo, $ax \in \mathfrak{b}$, $ax \notin \mathfrak{a}$, implica $\mathfrak{b} = \mathfrak{a} + Aax$.

La definición de $\mathfrak{m}$ implica $\mathfrak{m}x \subseteq \mathfrak{a}$, de donde $x \in \mathfrak{a} : \mathfrak{m}$. La inclusión $\mathfrak{a} \subseteq \mathfrak{a} : \mathfrak{m}$ es en efecto estricta, puesto que $x \notin \mathfrak{a}$.

Demostremos finalmente que el anillo cociente $A/\mathfrak{m}$ es un cuerpo. Sea $\bar{a} \in A/\mathfrak{m}$, no nulo. Sea $a \notin \mathfrak{m}$ un representante de $\bar{a}$. Se tiene entonces $ax \notin \mathfrak{a}$. La igualdad

$$\mathfrak{b} = \mathfrak{a} + Aax$$

implica la existencia de un $a' \in A$ tal que $x - aa'x \in \mathfrak{a}$, es decir, $e - aa' \in \mathfrak{m}$. Resulta que $\bar{a}$ es inversible en $A/\mathfrak{m}$, que es pues un cuerpo, luego $\mathfrak{m}$ es un ideal maximal de A.

2.° La hipótesis $x \in \mathfrak{a} : \mathfrak{m}$ implica $\mathfrak{m}x \subseteq \mathfrak{a}$, de donde $\mathfrak{m}Ax \subseteq \mathfrak{a}$ y

$$\mathfrak{m} \subseteq \mathfrak{a} : Ax.$$

$\mathfrak{a} : Ax$ no puede ser A, porque de serlo se tendría $e \in \mathfrak{a} : Ax$, de donde $Ax \subseteq \mathfrak{a}$ y $x \in \mathfrak{a}$, lo que contradice a la hipótesis. Por tanto, si $\mathfrak{m}$ es maximal se tiene $\mathfrak{m} = \mathfrak{a} : Ax$.

Sea $\mathfrak{c}$ un ideal de A tal que $\mathfrak{a} \subset \mathfrak{c} \subseteq \mathfrak{a} + Ax$. En $\mathfrak{c}$ están los elementos de la forma $ax + b$, donde $a \in A$, $b \in \mathfrak{a}$, $ax \notin \mathfrak{a}$ (de donde $a \notin \mathfrak{m}$).

Puesto que $\mathfrak{m}$ es maximal, $a \notin \mathfrak{m}$ implica $\mathfrak{m} + Aa = A$, y existen $m \in \mathfrak{m}$, $t \in A$ tales que $e = m + ta$. Por consiguiente, $x = mx + tax$, $mx \in \mathfrak{a}$, luego

$$x \in \mathfrak{a} + Aax \subseteq \mathfrak{c}$$

y $\mathfrak{a} + Ax \subseteq \mathfrak{c}$, lo que demuestra que $\mathfrak{a} + Ax$ cubre a $\mathfrak{a}$.

CAPÍTULO VI

Ideales primarios Anillos nœtherianos

Los ejercicios 1 a 11 de este capítulo se refieren esencialmente a las propiedades de los ideales primarios y de las intersecciones de ideales primarios; en ellos no se utiliza la condición nœtheriana.

Enunciados

1

En un anillo conmutativo, se consideran los ideales ligados por las relaciones $I = J \cap X = J' \cap X'$. Si J es P-primario, y si $J' \nsubseteq P$, entonces $I = X \cap X'$.

2

Sea I un ideal del anillo A conmutativo y unitario. Se supone que $I : Ab$ es P-primario y que $b \notin P$. Demostrar que

$$I = (I : Ab) \cap (I + Ab).$$

3

En el anillo $\mathbf{Z}[x]$, demostrar que el ideal $P = (2, x)$ es maximal. Demostrar que el ideal $(4, x)$ es P-primario pero no es una potencia de P.

4

Sean K un cuerpo conmutativo, E un espacio vectorial sobre K de dimensión infinita. Se hace de $A = K \times E$ un anillo, poniendo

$$(a, x)(a', x') = (aa', ax' + a' x).$$

Demostrar que todo ideal distinto de A es primario, pero que A no es nœtheriano.

5

Sea A un dominio de integridad, y sea $d \in A$ tal que $P = Ad$ sea primo. Demostrar que para todo $n \geqslant 1$, Ad^n es P-primario. Para demostrar que el aserto no se sostiene cuando A no es íntegro, se tomará $A = B/I$ con $B = K[x, y]$ y $I = (x^2, xy)$.

6

En el anillo $K[x, y, z]$ encontrar una descomposición normada en ideales primarios de $I = (x, y)(x, z)$.

7

Sea A un anillo conmutativo unitario. Se supone que los ideales primos que contienen a un ideal dado I son en número finito e incomparables. Si P es primo y contiene a I, demostrar que

$$Q = \{ x \mid \exists s \notin P,\ sx \in I \}$$

es P-primario. Deducir que I posee una descomposición normada en primarios única.

8

En el anillo $B = \dfrac{K[x, y, z]}{(z^2 - xy)}$, sean $\bar{x}, \bar{y}, \bar{z}$ las imágenes de x, y, z. Demostrar que $(\bar{x}, \bar{z})^2 = (\bar{x}) \cap (\bar{x}, \bar{y}, \bar{z})^2$ es una descomposición primaria normada de $(\bar{x}, \bar{z})^2$. ¿Cuál es la componente aislada?

9

En el anillo $K[x, y]$ de polinomios de dos variables y con coeficientes en un cuerpo K conmutativo, se consideran los ideales siguientes,

$$\mathcal{A} = (x^2, xy), \quad \mathcal{P}_1 = (x), \quad \mathcal{P} = (x, y), \quad \mathcal{A}_t = (x^2, y + tx),$$

donde $t \in K$.

1.° Demostrar que $\mathcal{P}$ es un ideal maximal y que $\mathcal{A}_t$ es $\mathcal{P}$-primario.

2.° Verificar las relaciones $\mathcal{A} = \mathcal{P}_1 \cap \mathcal{A}_t = \mathcal{P}_1 \mathcal{P}$.

3.° ¿Cuál es la intersección $\mathcal{J}$ de los ideales $\mathcal{A}_t$ cuando $t \in K$? Demostrar que $\mathcal{J}$ es $\mathcal{P}$-primario y que $\mathcal{A} = \mathcal{P}_1 \cap \mathcal{J}$.

10

Sea A un anillo conmutativo unitario. Si $\mathcal{A}$ es un ideal y S una parte multiplicativamente estable (conteniendo al elemento unidad), se escribe

$$\mathcal{A}_s = \{ x; \exists s \in S \quad sx \in \mathcal{A} \}.$$

1.° Suponemos que $\mathcal{A}$ admite una descomposición normada en ideales P_i-primarios, a los que llamamos Q_i : $\mathcal{A} = Q_1 \cap \ldots \cap Q_n$.

Demostrar que si $S \cap P_i = \varnothing$ para $i < m$, y $S \cap P_i \neq \varnothing$ para $i > m$, entonces $\mathcal{A}_s = Q_1 \cap \ldots \cap Q_m$ es un componente aislado.

2.° Recíprocamente, si $Q_1 \cap \ldots \cap Q_m$ constituye un componente aislado de $\mathcal{A}$, demostrar que existe una parte estable S tal que $\mathcal{A}_s = Q_1 \cap \ldots \cap Q_m$. (Utilizar el ejercicio V, 26.)

11*

Sea A un anillo conmutativo unitario.

1.° Sea I un ideal de A, $I \neq A$. Sea P un ideal minimal entre los ideales primos que contienen a I. Demostrar que $I_p = \{ x; \exists u \notin P, xu \in I \}$ es un ideal comprendido entre I y P. Sea $x \in P$, y $S = \{ x^n v; n \in N, v \notin P \}$. Demostrar que S es una parte multiplicativamente estable, y que $S \cap I \neq \varnothing$. Deducir que I_p es P-primario.

2.° Sea $a \in A$, no divisor de cero. Sea P un ideal minimal en el conjunto de los ideales primos que contienen a a. Demostrar que P es también minimal en el conjunto de los ideales primos que contienen a $I = aP$, y que $a \notin I_p$.

Si P no es maximal, sea $y \notin P$ tal que $P + Ay \neq A$. Demostrar que el ideal $Q = I_p + Aay$ tiene por radical P y no es primario.

3.° Se supone que en A, todo ideal de radical primo es primario. Demostrar que todo ideal primo es maximal o primo minimal. (Se puede advertir que la propiedad atribuida a A se transmite a todo anillo cociente.)

12

Sea A un anillo conmutativo íntegro que satisfaga la condición de cadena descendente. Si $A \neq 0$, demostrar que es un cuerpo. Deducir que, en un anillo satisfaciendo la condición de cadena descendente, todo ideal primo es maximal o igual al anillo.

13

Sea A un anillo conmutativo, unitario y nœtheriano. Sean I un ideal cualquiera, P un ideal primo. Se considera $I_p = \{ y;\ \exists t \notin P,\ ty \in I \}$. Demostrar que existe un $b \in P$ tal que $I_p = I : Ab$.

14

Demostrar que el producto $A \times B$ de dos anillos nœtherianos, es también nœtheriano.

15

Se consideran un anillo unitario conmutativo A, y un ideal I del mismo. Sea $a \in A$. Si a pertenece al radical de I, demostrar que para todo elemento $b \notin I$, existe $c \in Ab$ tal que $c \notin I$ y $ac \in I$. Demostrar que la recíproca es verdadera cuando A es nœtheriano. (Se puede advertir previamente que existe un entero n tal que

$$I : a^n = I : a^{n+1}.)$$

16

Sea I un ideal en un anillo conmutativo nœtheriano A. Demostrar que los ideales primos de la forma $I : X$ son en número finito.

17

Sean A un anillo conmutativo íntegro y unitario, y K su cuerpo de fracciones. Siendo P un ideal primo, consideremos el anillo

$$A_p = \left\{ \frac{a}{s};\ a \in A,\quad s \in A - P \right\}.$$

Si A es nœtheriano, demostrar que A_p también lo es.

18*

Sea D un dominio de integridad unitario nœtheriano. Se consideran tres ideales $\mathcal{A}$, $\mathcal{B}$, $\mathcal{V}$ tales que $\mathcal{A}\mathcal{V} = \mathcal{B}\mathcal{V}$ y $\mathcal{V} \neq 0$. Demostrar que $\mathcal{A}$ y $\mathcal{B}$ tienen el mismo radical (comiéncese por elegir una base de $\mathcal{V}$). Deducir que un ideal de D, no trivial, tiene todas sus potencias distintas.

19

Sea D un dominio de integridad, unitario, nœtheriano.

1.° Sea a un elemento no nulo. Sea b un elemento no nulo y no inversible. Demostrar que $\{ n;\ a \in Db^n \}$ es finito.

2.° Designando siempre con b un elemento no inversible, no nulo, sea I un ideal no nulo. Demostrar que $Ib \subset I$ (inclusión estricta).

3.° Si en el anillo D, todo ideal maximal es principal, entonces D es principal.

20

Sean A un anillo conmutativo y Q un ideal primario de radical P. Sea n un entero dado. Se considera $I = \{ x;\ \exists d \notin P,\ dx \in Q^n \}$.

1.° Demostrar que I es un ideal P-primario. Comparar I y Q^n cuando P sea maximal.

2.° Se supone A nœtheriano. Demostrar que uno de los ideales figurando en una representación normada de Q^n es un componente aislado, y es el único. ¿Cuál es?

21

Sea A un anillo conmutativo y unitario.

1.° Sean I un ideal y $b \in A$. Si $I + Ab$ e $I : Ab$ admiten una base finita, demostrar que lo mismo es con I.

2.° Se supone que todo ideal primo de A admite una base finita. Demostrar que A es nœtheriano. (Se puede considerar la familia $\mathcal{F}$ de los ideales que no tienen base finita y demostrar que si $\mathcal{F}$ no es vacío admite un elemento maximal.)

22

Sea A un anillo conmutativo unitario y nœtheriano. Se considera un ideal $\mathcal{B}$ del anillo $A[x]$. Sea $\mathcal{A}_n$ el subconjunto de A constituido por 0 y los elementos que aparecen como coeficiente director de algún polinomio de grado n perteneciente a $\mathcal{B}$.

1.° Demostrar que los $\mathcal{A}_n$ son ideales y que sólo hay un número finito que sean distintos: $\mathcal{A}_0, \ldots, \mathcal{A}_p$.

2.° Para cada $k \leqslant n$ sea $\{a_{ki}\}_i$ una base de $\mathcal{A}_k$. Sea f_{ki} un polinomio de grado k que tiene por coeficiente director a_{ki} y pertenece a $\mathcal{B}$. Demostrar que $\mathcal{B}$ es engendrado por los f_{ki}. Deducir que $A[x]$ es nœtheriano.

23

Sea A un anillo conmutativo unitario nœtheriano. Sean $\mathcal{A}$ un ideal y

$$\mathcal{B} = \bigcap_{n \in N} A^n .$$

1.° Demostrar que $\mathcal{B} \subseteq \mathcal{A}\mathcal{B}$ (tomar una descomposición primaria de $\mathcal{A}\mathcal{B}$).

2.° Demostrar que existe un $a \in \mathcal{A}$ tal que $(1 - a)\,\mathcal{B} = (0)$.
Deducir

$$\mathcal{B} = \{ x; \exists a \in \mathcal{A}, (1 - a)\, x = 0 \} .$$

3.° Encontrar en qué casos $\mathcal{B} = (0)$.

24

Sea A conmutativo nœtheriano. Sean X e I dos ideales. Los ideales $X : I^n$ forman una sucesión creciente, luego existe un k tal que $X : I^k = X : I^{k+1}$. Se llama frontera de X por I el ideal $X_{[I]} = X : I^k$.

1.° Demostrar que X es primario si y sólo si sus únicas fronteras son X y A.

2.° Deducir que las fronteras de X son exactamente las componentes aisladas en una descomposición normada de X en primarios. Comparar esto con el ejercicio VI, 10.

25*

Sea A un anillo conmutativo, unitario, nœtheriano, pero no íntegro. Se supone que (0) es un ideal primario.

1.° Demostrar que el conjunto de los divisores de cero es un ideal primo P.

2.° Demostrar que $(0) : P$ es un ideal P-primario no nulo.

3.° Sea Q un ideal P-primario contenido estrictamente en $(0) : P$. Si $a \in (0) : P$, y $a \notin Q$, demostrar que $Q \cap (a) = (0)$.

4.° Si $C \neq (0)$ demostrar que $[(0) : P] \cap C \neq (0)$. (Puede tomarse un elemento maximal en $\{ (0) : X;\ (0) \neq X \subseteq C \}$.)

5.° Demostrar que (0) es $\cap$-irreducible si y sólo si no existe ideal P-primario comprendido entre (0) y $(0) : P$.

26

Se considera un anillo conmutativo A, nœtheriano o satisfaciendo a la condición minimal. Se dice que $\mathcal{A} : \mathcal{B}$ es un residual propio de $\mathcal{A}$ si $\mathcal{B} \subseteq \mathcal{A}$, siendo $\mathcal{A}$ y $\mathcal{B}$ ideales cualesquiera de A.

1.° Demostrar que $\mathcal{C}$ es un residual propio de $\mathcal{A}$ si y sólo si $\mathcal{A} : (\mathcal{A} : \mathcal{C}) = \mathcal{C}$ y $\mathcal{A} : \mathcal{C} \supset \mathcal{A}$.

2.° Demostrar que los residuales propios de $\mathcal{A}$ verifican la condición maximal.

3.° Demostrar que todo residual propio maximal de $\mathcal{A}$ es primo.

4.° Demostrar que $\mathcal{A}$ contiene un producto de ideales primos. (Se puede considerar un residual propio maximal de $\mathcal{A}$, sea $\mathcal{P}_1$, luego un residual propio de $\mathcal{A} : \mathcal{P}_1$ y proseguir la construcción.)

27*

Se considera un anillo conmutativo unitario A que satisface a una de las dos propiedades siguientes:

α) A es nœtheriano y todo ideal primo es maximal.

β) A verifica la condición minimal.

1.° Mediante los ejercicios VI, 12 y VI, 26, demostrar que (0) es producto de ideales maximales: $(0) = \mathfrak{m}_1 \dots \mathfrak{m}_q$.

2.° Demostrar que $E_i = \dfrac{\mathfrak{m}_1 \dots \mathfrak{m}_{i-1}}{\mathfrak{m}_1 \dots \mathfrak{m}_i}$ es un espacio vectorial sobre $A/\mathfrak{m}_i$.

3.° Demostrar que E_i es de dimensión finita.

4.° Deducir que las condiciones α y β son equivalentes (utilizar el teorema de Jordan-Hölder).

28

Sea A un anillo conmutativo unitario. Un elemento $p \neq 0$ se llama indivisible cuando no es invertible y si $p = xy$ implica $x \in Ap$, o $y \in Ap$. Si A es íntegro, demostrar que esta noción coincide con la noción de elemento irreducible.

Cuando A es nœtheriano, demostrar que todo elemento no nulo es producto de elementos inversibles o indivisibles.

29

Sea A un anillo conmutativo unitario.

1.° Si f y g son dos idempotentes, demostrar que fg y $1 - f$ son igualmente idempotentes.

2.° Un idempotente e se dice descomponible si existen dos idempotentes f y g no nulos, tales que $e = f + g$, y $fg = 0$.

Demostrar que entonces $1 - e = (1 - e)(1 - f)$.

3.° Demostrar que dos idempotentes indescomponibles distintos tienen producto nulo.

4.° Si A es nœtheriano, demostrar que todo idempotente es suma de idempotentes indescomponibles. Deducir que A es isomorfo a un producto de anillos nœtherianos unitarios en los que el elemento unidad es un idempotente indescomponible.

30*

Se recuerda que un anillo principal es un anillo conmutativo unitario en el que todo ideal es engendrado por un elemento. Consideremos un anillo principal con divisores de cero y en el que 1 es un idempotente indescomponible (ejercicio VI, 29).

1.° Demostrar que 0 y 1 son los únicos idempotentes. Si $x^r = ax^{r+1}$, demostrar que $a^r x^r$ es un idempotente. Deducir que x es inversible o también que $x^r = 0$.

2.° Demostrar que existe un elemento p indivisible (ejercicio VI, 28) que es divisor de cero. Demostrar que existe una sucesión $a_i (0 \leqslant i \leqslant m)$ de elementos no nulos, salvo $a_0 = 0$, tales que $a_i = pa_{i+1}$ y $a_m \notin Ap$.

3.° Demostrar que el ideal $\{ y;\ yp^m \in Ap^{m+1} \}$ es idéntico a A. Deducir que $p^m = 0$, luego que $ph = 0$ implica $h \in Ap$, y en fin, que $1 - xp$ es inversible para todo $x \in A$ (considérese $1 - x^m p^m$).

4.° Demostrar que todo elemento que no pertenece a Ap es inversible.

5.° Demostrar que todo elemento indivisible es el producto de p por un elemento inversible. Deducir que los ideales de A son los Ap^k $(0 \leqslant k \leqslant m)$ y que su número es exactamente $m + 1$.

Soluciones

1

Se tiene evidentemente $I \subseteq X \cap X'$. Sea $x \in X \cap X'$. Tomemos $t \in J'$ tal que $t \notin P$. Se tiene $tx \in J' \cap X' = I \subseteq J$. Si J es P-primario resulta $x \in J$, luego $x \in J \cap X = I$.

2

Se tiene evidentemente $I \subseteq (I : Ab) \cap (I + Ab)$. Si $x + \lambda b \in I : Ab$, con $x \in I$, se tiene $xb + \lambda b^2 \in I$, luego $\lambda b^2 \in I$, es decir, $\lambda b \in I : Ab$. Pero $I : Ab$ es P-primario y $b \notin P$, luego $\lambda \in I : Ab$. Por consiguiente $\lambda b \in I$, luego

$$x + \lambda b \in I.$$

3

Consideremos el homomorfismo de $\mathbf{Z}[x]$ sobre $\mathbf{Z}$ que aplica todo polinomio sobre su término constante y el homomorfismo canónico de $\mathbf{Z}$ sobre $\mathbf{Z}/(2)$, que es un cuerpo. Es evidente que $P = (2, x)$ es el núcleo del homomorfismo compuesto, luego es maximal. Se tiene

$$P^2 = (4, x^2, 2x) \subseteq (4, x) \subseteq P.$$

Las inclusiones son estrictas, pues $2 \in P - (4, x)$ y $x \in (4, x)$, $x \notin (4, x^2, 2x)$. El ideal $(4, x)$ tiene por radical P, y es sabido que todo ideal de radical maximal es primario.

4

Demostremos primero que los ideales distintos de A son de la forma

$$I = \{0\} \times V,$$

donde V es un subespacio de E.

En efecto, si un ideal I contiene un elemento (a, x) con $a \neq 0$, entonces para todo $(b, y) \in A$ se tiene

$$(b, y) = (a, x)\,(a^{-1} b,\ a^{-1} y - a^{-2} bx) \in I.$$

Si $(0, x) \in \{0\} \times E$, se tiene $(0, x)^2 = 0$, luego $(0, x)$ pertenece al radical de I. Recíprocamente, si $(a, x) \in \mathcal{R}(I)$, existe un n tal que $(a, x)^n \in I = \{0\} \times V$, lo que implica $a^n = 0$, luego $a = 0$. Así, todo ideal propio tiene por radical $\{0\} \times E$. Si $(a, x)\,(a', x') \in I$, y $(a', x') \notin \{0\} \times E$, se tiene

$$aa' = 0 \quad \text{y} \quad ax' + a'x \in V.$$

Puesto que $a' \neq 0$, sigue $a = 0$ y $a'x \in V$, luego $x = (a')^{-1} a'x \in V$, lo que muestra que $(a, x) \in I$, luego I es primario.

A no es nœtheriano, puesto que sus ideales propios corresponden biyectivamente a los subespacios de E y éstos no pueden verificar una condición de cadena, pues si no E sería de dimensión finita. Se advertirá también que A no tiene más que un ideal primo propio, que es ideal máximo en tanto que ideal propio.

5

Supongamos que $xy \in Ad^n$ y $x \notin Ad$.

Se tiene $xy = ad^n$. Se puede escribir $y = cd^i$ con $i \geqslant 0$ y $c \notin Ad$. Por tanto $xcd^i = ad^n$. No se puede tener $n > i$ pues, simplificando por d^i se obtendría

$$xc = ad^{n-i} \in Ad,$$

contrariamente al hecho que $x \notin Ad$ y $c \notin Ad$. Se tiene, pues, $i \geqslant n$, y por tanto $y \in Ad^n$.

En B el ideal (x) es primo, porque es el núcleo del homomorfismo

$$f(x, y) \to f(0, y)$$

que aplica B sobre el anillo íntegro $K[y]$. Como (x) contiene a I, su imagen $(\bar{x})$ en A es también un ideal primo (ejercicio V, 25). Se tiene $(\bar{x})^2 = (0)$, pues $x^2 \in I$. Demostremos que (0) no es primario en A. Es imposible $\bar{y} \in (\bar{x})$, pues esto llevaría en B a una igualdad de la forma

$$y = ux + vx^2 + wxy.$$

Se tendría, pues, $\bar{x}\bar{y} = 0$; pero $\bar{x} \neq 0$, e $\bar{y} \notin (\bar{x})$, lo que es contradictorio.

6

Demostremos que

$$I = (x^2, xy, xz, yz) = (x^2, xy, xz, yz, y^2, z^2) \cap (x, y) \cap (x, z).$$

Es evidente que I está contenido en esta intersección.

Sea $f(x, y, z)$ un elemento de la intersección. Se puede escribir:

$$f(x, y, z) = a_1 x^2 + a_2 xy + a_3 xz + a_4 yz + a_5 y^2 + a_6 z^2,$$

con $a_i \in K[x, y, z]$.

Pero $f(x, y, z) \in (x, y)$ implica $f(0, 0, z) = 0$, es decir, $a_6(0, 0, z)z^2 = 0$, consiguientemente $a_6(0, 0, z) = 0$. Por tanto $a_6 \in (x, y)$ y $a_6 z^2 \in I$. Del mismo modo $f(x, y, z) \in (x, z)$ implica $a_5 y^2 \in I$.

Finalmente

$$f(x, y, z) \in (x^2, xy, xz, yz).$$

(x, y) es primo, porque es el núcleo del homomorfismo

$$g(x, y, z) \to g(0, 0, z)$$

que aplica $K[x, y, z]$ sobre el anillo íntegro $K[z]$. Del mismo modo (x, z) es primo. $J = (x^2, xy, xz, yz, y^2, z^2) = (x, y, z)^2$ tiene por radical (x, y, z) que es maximal, pues es el núcleo del homomorfismo $g(x, y, z) \to g(0, 0, 0)$ que aplica $K[x, y, z]$ sobre el cuerpo K. Luego J es primario. Es evidente que se ha obtenido una descomposición normada de I.

7

Sean $P_1, \ldots, P_n$ los ideales primos que contienen a I. El radical de I es

$$P_1 \cap \ldots \cap P_n.$$

A cada P_i asociemos $Q_i = \{ x;\ \exists s \notin P_i,\ sx \in I \}$. Se tiene

$$\prod_{j \neq i} P_j \not\subseteq P_i,$$

puesto que no puede ser $P_j \subseteq P_i$ con $j \neq i$.

Sea $s \in \prod_{j \neq i} P_j$ y $s \notin P_i$. Si $a \in P_i$, as pertenece a $\prod_{j=1}^{n} P_j$, y por tanto al radical de I. Existe un k tal que $(as)^k \in I$. Como $s^k \notin P_i$ se tiene $a^k \in Q_i$. Esto muestra que Q_i admite por radical P_i.

Si $xy \in Q_i$ y $x \notin P_i$, sea $s \notin P_i$ tal que $sxy \in I$. Se tiene $sx \notin P_i$, luego $y \in Q_i$. Por tanto Q_i es P_i-primario. Es evidente que $I \subseteq Q_1 \cap \ldots \cap Q$.

Supongamos, para la demostración por reducción al absurdo, que la inclusión es estricta. Sea

$$d \in Q_1 \cap \ldots \cap Q_n$$

y sea $d \notin I$. Se tiene $I : Ad \neq A$ (el anillo es unitario). Luego $I : Ad$ está contenido en un ideal maximal, que es necesariamente uno de los P_i, por ejemplo, P_1. Como $d \in Q_1$, existe $s \notin P_1$ tal que $sd \in I$. Se tiene $s \in I : Ad$, lo que da una contradicción.

Esta descomposición es única, pues cada Q_i constituye un componente aislado.

8

Consideremos primero los ideales siguientes en $A = K[x, y, z]$: el ideal (x, z) es primo, pues $A/(x, z)$ es isomorfo a $K[y]$ que es íntegro. Se tienen las inclusiones

$$(x, z)^2 = (x^2, xz, z^2) \subseteq (x, z^2) \subseteq (x, z).$$

Por tanto (x, z^2) tiene por radical (x, z). Demostremos que es primario.

Supongamos que $PQ \in (x, z^2)$ y $Q \notin (x, z)$. Se tiene $PQ = Ux + Vz^2$. No es restrictivo suponer $V \in K[y, z]$. Puesto que $PQ \in (x, z)$ se tiene $P \in (x, z)$ luego $P = P_1 x + P_2 z$. Asimismo podemos suponer $P_2 \in K[y, z]$. Resulta

$$(P_1 x + P_2 z)\, Q = Ux + Vz^2,$$

lo que implica, haciendo $x = 0$,

$$P_2 z Q(0, y, z) = Vz^2, \quad \text{donde} \quad P_2 Q(0, y, z) = Vz \in (z).$$

Ahora bien, $Q(0, y, z) \in (z)$ implicaría $Q \in (x, z)$, lo que no es. Como (z) es primo, se sigue $P_2 \in (z)$, de donde se deduce

$$P = P_1 x + P_2 z \in (x, z^2).$$

Por otra parte, el ideal (x, y, z) es maximal, pues $A/(x, y, z)$ es isomorfo a K, que es un cuerpo. El ideal $(x, y, z)^2$ es, pues, (x, y, z)-primario. Demostremos que (x^2, xz, xy, z^2) se escribe

$$(x^2, xy, xz, z^2) = (x, z^2) \cap (x^2, y^2, z^2, xy, xz, yz).$$

En efecto, queda claro que está contenido en esa intersección. Si

$$P_1 x + P_2 z^2 = Q_1 x^2 + Q_2 y^2 + Q_3 z^2 + Q_4 xy + Q_5 xz + Q_6 yz,$$

P_1 no puede tener término constante, ya que no hay término en x en el segundo miembro. Luego $P_1 \in (x, y, z)$ y por consiguiente

$$P_1 x \in (x^2, xy, xz) \quad \text{y} \quad P_1 x + P_2 z^2 \in (x^2, xy, xz, z^2).$$

Ahora, el núcleo $(z^2 - xy)$ está contenido en (x^2, xy, xz, z^2) y en todos los ideales que hemos considerado. Podemos utilizar el isomorfismo entre el retículo de los ideales de B y el de los ideales de A que contienen el núcleo (ejercicio V, 25). Teniendo en cuenta que $\bar{x}\bar{y} = \bar{z}^2$, la igualdad antes demostrada deviene

$$(\bar{x}^2, \bar{x}\,\bar{z}, \bar{z}^2) = (\bar{x}) \cap (\bar{x}, \bar{y}, \bar{z})^2.$$

Los radicales asociados a esta descomposición primaria son $(\bar{x}, \bar{z})$ y $(\bar{x}, \bar{y}, \bar{z})$, que son distintos. El menor ofrece la componente aislada $(\bar{x})$.

9

1.° $\mathcal{P}$ es el conjunto de polinomios $p(x, y)$ tales que $p(0, 0) = 0$. El homomorfismo de $K[x, y]$ sobre K que aplica $f(x, y)$ en $f(0, 0)$ tiene por núcleo $\mathcal{P}$. El isomorfismo $K[x, y]/\mathcal{P} \simeq K$, demuestra que $\mathcal{P}$ es maximal.

Demostremos que $\mathcal{P}^2 = (x^2, xy, y^2)$ está contenido en $\mathcal{A}_t$:

$$xy = (y + tx)\,x - tx^2 \in \mathcal{A}_t,$$
$$y^2 = y(y + tx) - txy \in \mathcal{A}_t.$$

Se tiene pues $\mathcal{P}^2 \subseteq \mathcal{A}_t \subseteq \mathcal{P}$. Los ideales $\mathcal{P}^2$ y $\mathcal{P}$ tienen por radical $\mathcal{P}$. Lo mismo ocurre con $\mathcal{A}_t$. Como $\mathcal{P}$ es maximal, $\mathcal{P}^2$ y $\mathcal{A}_t$ son $\mathcal{P}$-primarios.

2.° Se tiene inmediatamente $\mathcal{A} = \mathcal{P}_1 \mathcal{P}$. De $\mathcal{A} \subset \mathcal{P}_1$ y $\mathcal{A} \subset \mathcal{A}_t$ se deduce $\mathcal{A} \subseteq \mathcal{P}_1 \cap \mathcal{A}_t$. Sea $f(x, y) \in \mathcal{P}_1 \cap \mathcal{A}_t$. Se tiene $f(x, y) = xg(x, y)$, pero $g(x, y)$ puede siempre escribirse,

$$g(x, y) = \alpha + g_1(x, y), \text{ con } \alpha \in K \text{ y } g_1(x, y) \in \mathcal{P}$$

(basta con aislar el término constante).

Se tiene,

$$xg_1(x, y) \in \mathcal{P}_1 \mathcal{P} = \mathcal{A}.$$

de donde

$$ax = f(x, y) - xg_1(x, y) \in \mathcal{A}_t.$$

Como $x \notin \mathcal{A}_t$, eso exige $a = 0$. Luego

$$f(x, y) = xg_1(x, y) \in \mathcal{A}.$$

Finalmente, $\mathcal{A} = \mathcal{P}_1 \cap \mathcal{A}_t$.

3.° Se tiene $\mathcal{P}^2 \subseteq \mathcal{J} \subseteq \mathcal{A}_0 \cap \mathcal{A}_1$.
Si $f(x, y) \in \mathcal{A}_0 \cap \mathcal{A}_1$, este polinomio se escribe

$$\begin{aligned} f(x, y) &= a(x + y) + f_1(x, y), \quad \text{donde} \quad a \in K, f_1(x, y) \in \mathcal{P}^2 \\ &= \beta y + f_2(x, y), \quad \text{donde} \quad \beta \in K, f_2(x, y) \in \mathcal{P}^2. \end{aligned}$$

Se deduce

$$ax + (a - \beta) y = f_2(x, y) - f_1(x, y) \in \mathcal{P}^2.$$

El polinomio del segundo miembro es por lo menos de segundo grado (o es nulo). Por consiguiente, esta igualdad sólo es posible si $a = \beta = 0$. Luego, $f \in \mathcal{P}^2$, Así, $\mathcal{J}$ no es otro que $\mathcal{P}^2$. Se tiene $\mathcal{A} \subset \mathcal{P}_1$ y $\mathcal{A} \subset \mathcal{P}^2$, luego

$$\mathcal{A} \subseteq \mathcal{P}_1 \cap \mathcal{P}^2 \subseteq \mathcal{A}_t \cap \mathcal{P}_1 = \mathcal{A}.$$

Resulta así la igualdad del enunciado. De este modo hemos obtenido dos diferentes representaciones de $\mathcal{A}$ en ideales primarios. Los radicales asociados son $\mathcal{P}_1$ y $\mathcal{P}$, y se tiene $\mathcal{P}_1 \subset \mathcal{P}$; $\mathcal{P}_1$ es un componente aislado. Por el contrario $\mathcal{A}_t$ no lo es (y éste es efectivamente variable). Se notará que $\mathcal{P}^2$ es primario sin ser inter-irreducible.

10

1.° Si $x \in \mathcal{A}_s$, existe $s \in S$ tal que $sx \in \mathcal{A}$. Sea $i \leqslant m$. Se tiene $sx \in Q_i$, pero $s \notin P_i$, puesto que $P_i \cap S = \varnothing$. Como Q_i es primario, $x \in Q_i$. Se tiene pues

$$\mathcal{A}_s \subseteq Q_1 \cap \ldots \cap Q_m.$$

Recíprocamente, sea $x \in Q_1 \cap \ldots \cap Q_m$. Tomemos para cada $j > m$ un $s_j \in S \cap P_j$. Existen enteros α_j tales que $s_j^{\alpha_j} \in Q_j$. Pongamos $s = \prod_{j>m} s_j^{\alpha_j}$. Se tiene $s \in S$ y $s \in Q_{m+1} \cap \ldots \cap Q_n$. Por consiguiente

$$xs \in Q_1 \cap \ldots \cap Q_m \cap \ldots \cap Q_n = \mathcal{A}.$$

Por tanto $x \in \mathcal{A}_s$. Es $\mathcal{A}_s$ un componente aislado de $\mathcal{A}$, pues si $i \leqslant m$ y $P_j \subseteq P_i$, se tiene $P_j \cap S = \varnothing$, luego $j \leqslant m$.

2.° Pongamos $S = \bigcap_{i \leqslant m} A - P_i$. Por ser intersección de partes estables, S es una parte estable. Si $i \leqslant m$ se tiene $S \subseteq A - P_i$, luego $S \cap P_i = \varnothing$. Si $j > m$ no puede ser $S \cap P_j = \varnothing$: resultaría $P_j \subseteq \bigcup_{i \leqslant m} P_i$, luego P_j estaría contenido en uno de los P_i con $i \leqslant m$ (ejercicio V, 26). Según lo establecido en 1.°, tenemos,

$$\mathcal{A} = Q_1 \cap \ldots \cap Q_m.$$

11

1.° Sean $x, y \in I_p$. Existen $u, v \notin P$ tales que $ux \in I$ y $vy \in I$. Como P es primo, $uv \notin P$. Se tiene pues

$$uv(x - y) = uvx - uvy \in I, \quad \text{de donde} \quad x - y \in I_p.$$

Es evidente que todo elemento de I es de I_p.

Si $ux \in I$ y $u \notin P$, como también tenemos $ux \in P$, resulta $x \in P$. Se tiene pues $I \subseteq I_p \subseteq P$.

Es claro que S es multiplicativamente estable. Supongamos $S \cap I = \varnothing$. Consideremos el conjunto de ideales X tales que $I \subseteq X$ y $X \cap S = \varnothing$. Esta familia no es vacía, puesto que contiene a I. Se verifica fácilmente que ella es $\cup$-inductiva. Según el axioma de Zorn, tal familia admite un elemento maximal P'. Demostremos que P' es primo. Si $b, c \notin P'$ se tiene

$$P' \subset P' + Ab \quad \text{y} \quad P' \subset P' + Ac.$$

Existen, pues, $s, t \in S$, pertenecientes respectivamente a $P' + Ab$ y $P' + Ac$. Se tiene

$$st \in (P' + Ab)(P' + Ac) = P'^2 + P'b + P'c + Abc.$$

bc no puede pertenecer a P', porque con ello se tendría $st \in P' \cap S$. El complementario de P está contenido en S, luego es disjunto con P'. Se tiene por consiguiente $P' \subset P$, estrictamente puesto que $x \in P - P'$. Pero esto contradice el carácter minimal de P.

Efectivamente se tiene pues $S \cap I \neq \varnothing$, es decir, que existe un n tal que $x^n \in I_p$. Luego P es el radical de I_p. Se puede ahora demostrar que I_p es P-primario. Si $xy \in I_p$ y $x \notin P$, existe un $v \notin P$ tal que $vxy \in I$. Pero $vx \notin P$, luego $y \in I_p$.

2.° Sea P' un ideal primo tal que $aP \subseteq P' \subseteq P$.

Si $a \in P'$, entonces $P' = P$ puesto que P es minimal. Si $a \notin P'$ entonces $P \subseteq P'$ puesto que P' es primo. En los dos casos $P = P'$. Luego P es minimal entre los ideales primos que contienen a I. Si $a \in I_p$, existe $u \notin P$ tal que $ua \in I$, luego $ua = ta$ con $t \in P$. Resulta $(u - t)a = 0$, luego $u = t$, puesto que a no es divisor de cero. Pero esto es evidentemente absurdo, luego $a \notin I_p$.

Q tiene radical P, puesto que está comprendido entre I_p y P, que tienen ambos por radical P. Si $a \in Q$ se tiene $a = b + xay$, con $b \in I_p$ y $x \in A$. Por consiguiente $(1 - xy)\, a = b \in I_p$. Pero $1 - xy \notin P$ (porque si no $P + Ay = A$). Como I_p es P-primario, resulta que $a \in I_p$, y acabamos de ver que esto es imposible. Se tiene pues efectivamente $a \notin Q$. Además $y \notin P$, pero $ay \in Q$. El ideal Q no es primario.

3.° Sea f un homomorfismo de A sobre un anillo B, de núcleo N. Se sabe que existe un isomorfismo entre los retículos de los ideales de B y el de los ideales de A que contienen a N (ejercicio V, 25). En este isomorfismo se corresponden los ideales primos, los radicales y los ideales primarios. Por consiguiente, en B, todo ideal cuyo radical sea primo es un radical primario.

Sea entonces P un ideal primo de A, ni maximal ni primo minimal. Sea R un ideal primo tal que $R \subset P$. Tomemos $B = A/R$. Entonces $P' = f(P)$ es un ideal de B, primo y no nulo. Sea $0 \neq a \in P'$. Se sabe que P' contiene un ideal primo minimal P'' que contiene al elemento a (texto: VI, 2, teor. 2). P' no es maximal en B, de modo que *a fortiori* tampoco P'' lo es. Pero entonces, según la cuestión vista en el 2.° punto, se puede encontrar en B un ideal de radical P'' y no primario, lo que es una contradicción.

12

Tomemos $d \in A$, $d \neq 0$. La sucesión de ideales $(Ad^n)_{n \in N}$ es decreciente, luego es estacionaria a partir de un cierto rango: $Ad^n = Ad^{n+1}$. Sea $x \in A$. Se tiene,

$$xd^n \in Ad^{n+1},$$

luego existe y tal que $xd^n = yd^{n+1}$, lo que da $d^n(x - yd) = 0$. Como A es íntegro se tiene $d^n \neq 0$ y por tanto $x = yd$. Notemos que el semigrupo $A - \{0\}$

satisface al axioma de cocientes, luego es un grupo. En otras palabras, A es un cuerpo.

Si P es un ideal primo de un anillo A que verifica la condición de cadena descendente, A/P es íntegro y verifica la condición de cadena descendente, por cuanto existe entre los ideales de A/P y los ideales de A conteniendo a P una correspondencia biyectiva que respeta las inclusiones. Según lo que precede A/P es un cuerpo, luego P es maximal.

13

Indicaremos dos métodos. El primero consiste en señalar que I_p es un ideal y tomar una base $(y_1, ..., y_n)$ de I_p. Se puede encontrar $t_i \notin P$ tal que $t_i y_i \in I$. Basta entonces tomar $b = t_1 ... t_n$. El otro método consiste en considerar un ideal $I : Ab$ maximal entre los ideales de la forma $I : Ac$, con $c \notin P$. Si $y \in I_p$ se tiene $ty \in I$ con $t \notin P$, luego $bty \in I$ e $y \in I : Abt$. Pero,

$$I : Ab \subseteq I : Abt \quad \text{y} \quad bt \notin P,$$

luego $I : Ab = I : Abt$. Resulta así $I_p = I : Ab$.

14

Señalemos primero que $A \times B/B$ es isomorfo a A, luego, entre los ideales de A y los ideales de $A \times B$ que contienen a B existe una correspondencia biyectiva, que respeta las inclusiones. Por consiguiente, estos últimos verifican la condición de cadena ascendente. Consideremos una sucesión creciente (I_n) de ideales de $A \times B$. Existe un m tal que $I_m + B = I_{m+p} + B$, cualquiera sea p. Por otra parte, los $I_n \cap B$ forman una sucesión creciente. Esta sucesión es estacionaria a partir de un cierto rango k, que podemos suponer superior a m. Sea $x \in I_{k+p}$. Se tiene $x \in I_{k+p} + B = I_k + B$, luego $x = y + b$, con $y \in I_k$ y $b \in B$. Se deduce

$$x - y \in I_{k+p} \cap B = I_k \cap B \subseteq I_k,$$

luego $x \in I_k$. Vemos así que la sucesión I_n es estacionaria a partir de k.

15

Sea $b \notin I$. Existe un m tal que $a^m \in I$, luego *a fortiori* $a^m b \in I$. Sea s el menor entero natural entre los exponentes m tales que $a^m b \notin I$. Si $s = 1$, basta tomar $c = b$. Si $s > 1$, tomemos $c = a^{s-1} b$. Se tiene $a^{s-1} b \notin I$; pero

$a(a^{s-1}b) \in I$. Recíprocamente, supongamos que a verifica esa propiedad y que al anillo es nœtheriano. Los ideales $I : a^m$ constituyen una sucesión creciente, luego estacionaria: $I: a^n = I : a^{n+1}$.

Supongamos, para la reducción al absurdo, que $a^n \notin I$. Entonces existirá $c = ta^n$ tal que $c \notin I$ y $ac \in I$. Se tiene pues $ta^{n+1} = ac \in I$, $t \in I : a^{n+1} = I : a^n$ luego $c = ta^n \in I$, lo que es una contradicción.

16

I admite una descomposición normada en ideales Q_i, P_i-primarios:

$$I = Q_1 \cap \ldots \cap Q_n.$$

Si $\mathcal{P} = I : X$ es primo propio, se tiene $X \notin I$. Se puede suponer $X \notin Q_i$ para $i < r$, y $X \subseteq Q_i$ para $i > r$. En estas condiciones,

$$I : X = (Q_1 : X) \cap \ldots \cap (Q_n : X) = (Q_1 : X) \cap \ldots \cap (Q_r : X).$$

Tomando radicales

$$\mathcal{P} = \mathcal{R}(I : X) = \mathcal{R}(Q_1 : X) \cap \ldots \cap \mathcal{R}(Q_r : X) = P_1 \cap \ldots \cap P_r.$$

Se deduce que el producto $P_1 \ldots P_r$ está contenido en $\mathcal{P}$, luego que uno de los P_i está contenido en $\mathcal{P}$, sea éste P_1. De hecho vemos que $\mathcal{P} = P_1$, a consecuencia de la igualdad precedente.

Es posible demostrar que, recíprocamente, todos los P_i $(1 < i < n)$ son residuales de I. En efecto, consideremos por ejemplo, P_1.

Tomemos $I : X$ maximal en el conjunto

$$\{ I : N \mid I \subset N \subseteq Q_2 \cap \ldots \cap Q_n \}.$$

Demostremos que $I : X$ es primo. Si $YZ \subseteq I : X$ y si $Z \notin I : X$ se tiene $ZX \subseteq I$, luego

$$I \subset I + ZX \subseteq X \subseteq Q_2 \cap \ldots \cap Q_n.$$

Por tanto, $I : X \subseteq I : (I + ZX)$, lo que implica la igualdad

$$I : X = I : (I + ZX) = (I : I) \cap (I : ZX) = I : ZX.$$

Ahora bien, $YZX \subseteq I$, luego $Y \subseteq I : ZX$, es decir $Y \subseteq I : X$. Como $X \neq I$, se tiene $X \notin Q_1$ pero $X \subseteq Q_i$ para $i > 1$. Por consiguiente, según lo antedicho, $I : X = P_1$.

17

Sea I un ideal de A_p. Demostremos que $(I \cap A)A_p = I$. En efecto, de una parte

$$(I \cap A)\, A_p \subseteq IA_p \subseteq I.$$

De otra parte, si $\frac{a}{s} \in I$, se tiene

$$a = s\left(\frac{a}{s}\right) \in I \cap A, \quad \text{luego} \quad \frac{a}{s} = \frac{1}{s}\, a \in (I \cap A)\, A_p.$$

Por consiguiente la aplicación $I \to I \cap A$ es una inyección del retículo de los ideales de A_p en el retículo de los ideales de A. Es claro que esta inyección es un isomorfismo. Por consiguiente, toda sucesión creciente de ideales de A_p es estacionaria.

18

Sea $\{ w_1, \ldots, w_n \}$ una base de $\mathfrak{M}$. Tomemos $a \in \mathfrak{A}$. Para todo $i \leq n$,

$$aw_i \in \mathfrak{A}\mathfrak{M} = \mathfrak{B}\mathfrak{M} = \sum_j \mathfrak{B} w_j .$$

Por tanto,

$$aw_i = \sum_{j=1}^{n} b_{ij}\, w_j, \quad \text{con} \quad b_{ij} \in \mathfrak{B}.$$

Poniendo $c_{ij} = \delta_{ij}\, a - b_{ij}$ (δ_{ij}, símbolo de Kronecker), esto nos da

$$\sum_{j=1}^{n} c_{ij}\, w_j = 0 \quad (1 \leq i \leq n).$$

Estas igualdades pueden mirarse en el cuerpo de fracciones de D. Puesto que el sistema de ecuaciones definido por los c_{ij} admite solución no nula, el determinante de los c_{ij} es nulo. Pero este determinante se presenta en la forma $a^n - b$, con $b \in \mathfrak{B}$. Se tiene pues $a \in \mathfrak{R}(\mathfrak{B})$. Los radicales $\mathfrak{R}(\mathfrak{A})$ y $\mathfrak{R}(\mathfrak{B})$ son iguales.

Sea $\mathcal{J}$ distinto de (0). Supongamos que $\mathcal{J}^n = \mathcal{J}^q$, con $q < n$. Entonces $\mathcal{J}^{n-q}\mathcal{J}^q = D\mathcal{J}^q$. Pero $\mathcal{J}^q \neq 0$, pues D es íntegro. Según lo recién establecido,

$$\mathcal{R}(\mathcal{J}) = \mathcal{R}(\mathcal{J}^{n-q}) = \mathcal{R}(D) = D.$$

Luego $1 \in \mathcal{R}(\mathcal{J})$, lo que evidentemente implica $1 \in \mathcal{J}$ y $\mathcal{J} = D$.

19

1.° Los residuales $Da : b^n$ $(n \in \mathbf{N})$ constituyen una sucesión creciente de ideales. Luego existe un n tal que

$$Da : b^n = Da : b^i \quad (\forall i \geqslant n).$$

Si $i > n$ no puede ser $a \in Db^i$. En efecto, si $a = cb^i$ resulta

$$c \in Da : b^i = Da : b^{i-1}, \quad \text{luego} \quad cb^{i-1} = da = dcb^i.$$

De aquí, $cb^{i-1}(1 - db) = 0$. Como D es íntegro obtenemos $1 - db = 0$, es decir, que b es inversible.

2.° Si tuviésemos $Ib = I$, resultaría $Ib^2 = Ib = I$ y, por recurrencia, $I = Ib^n$ para todo n. Pero entonces un elemento $a \neq 0$ de I sería múltiplo de todas las potencias de b^n. Se tiene, pues, $Ib \subset I$.

3.° Sea J un ideal maximal entre los no principales, suponiendo que exista. Se tiene $J \neq D$ luego J está contenido en un ideal maximal, que es por tanto principal: $J \subset (u)$. Se tiene $u(J : u) \subseteq J$. Si $x \in J$, se tiene $x = du$. Como $d \in J : u$ se ve que $x \in u(J : u)$. Luego, $J = u(J : u)$. Es claro que $J : u$ no es principal, pues si no lo sería J. Pero no siendo u inversible, por lo 2.° tenemos $u(J : u) \subset J : u$. Esto contradice el carácter maximal de J.

20

1.° Se verifica inmediatamente que I es un ideal. Se tiene $Q^n \subseteq I \subseteq P$, luego el radical de I está comprendido entre el de Q^n y el de P. Es necesariamente P. Si $xy \in I$ y $x \notin P$, tomemos d tal que $dxy \in Q^n$. Se tiene $dx \notin P$, luego $y \in I$. Efectivamente, I es P-primario. Si P es maximal, Q^n es primario, pues tiene por radical P. Si $x \in I$, existe $d \notin P$ con $dx \in Q^n$ luego $x \in Q^n$. Como siempre se tiene $Q^n \subseteq I$, resulta la igualdad.

2.° Sea $Q^n = \mathcal{Y}_1 \cap ... \cap \mathcal{Y}_k$ una representación normada de Q^n, con $\mathcal{Y}_i$ primario de radical P_i. El radical de Q^n, es decir P, es la intersección de los radicales

$$P = P_1 \cap ... \cap P_k.$$

Esta intersección contiene al producto $P_1 ... P_k$. Siendo P primo, esto implica, por ejemplo, $P \supseteq P_1$, luego efectivamente $P = P_1$. De este modo, P es elemento mínimo en el conjunto de los P_i. Por consiguiente $\mathcal{Y}_1$ es el único ideal, entre los $\mathcal{Y}_i$, que constituye un componente aislado. Mostremos que $\mathcal{Y}_1 = I$.

Si $x \in I$ existe $d \notin P$ tal que $dx \in Q^n \subseteq \mathcal{Y}_1$. Como $\mathcal{Y}_1$ es P-primario, $x \in \mathcal{Y}_1$.

Recíprocamente, sea $x \in \mathcal{Y}_1$. Se tiene $\prod_{i>1}^{k} \mathcal{Y}_i \nsubseteq P$. En efecto, si no fuese así P contendría uno de los $\mathcal{Y}_i$, luego uno de los P_i, con $i \neq 1$ lo que es imposible (los radicales son todos distintos).

Sea $d \in \prod_{i>1} \mathcal{Y}_i$, con $d \notin P$. Se tiene

$$dx \in \prod_{1}^{k} \mathcal{Y}_i \subseteq \bigcap_{1}^{k} \mathcal{Y}_i = Q^n, \quad \text{luego } x \in I.$$

21

1.° Sea $\{ a'_1, ..., a'_r \}$ una base de $I + Ab$. Se tiene $a'_i = a_i + u_i b$ con $a_i \in I$, luego podemos reemplazar la base dada por $\{ a_1, ..., a_r, b \}$. Sea $\{ c_1, ..., c_s \}$ una base de $I : Ab$. Consideremos el ideal I' engendrado por los a'_i y los bc_j. Como $bc_j \in I$, es evidente que $I' \subseteq I$. Sea $t \in I$. Se tiene

$$t \in I + Ab, \quad \text{luego} \quad t = t_1 a_1 + ... + t_r a_r + t_{r+1} b.$$

Se deduce

$$t_{r+1} b = t - \Sigma t_i a_i \in I.$$

Por tanto $t_{r+1} \in I : Ab$, luego $t_{r+1} = \Sigma w_j c_j$. Finalmente

$$t_{r+1} b = \Sigma w_j bc_j \in I'.$$

luego $t \in I'$, lo que muestra que $I = I'$.

2.° Supongamos $\mathcal{F} \neq \varnothing$ y demostremos que esta familia es $\cup$-inductiva. Sea $\mathcal{C}$ una cadena contenida en $\mathcal{F}$. Consideremos $N = \bigcup_{J \in \mathcal{C}} J$. Si N admite una base finita $\{ b_1, ..., b_n \}$ se pueden encontrar ideales $J_i \in \mathcal{C}$ tales que $b_i \in J_i$.

El mayor de estos ideales contiene todos los b_i, luego coincide con N, lo que es absurdo, puesto que aquél no tiene base finita. Luego efectivamente $N \in \mathcal{F}$ y $\mathcal{F}$ es $\cup$-inductiva.

Según el axioma de Zorn, $\mathcal{F}$ admite un elemento maximal I. No es I primo, puesto que todo ideal primo admite una base finita. Se pueden pues encontrar $a, b \in A$ tales que $ab \in I$ pero $a \notin I$ y $b \notin I$. El ideal $I + Ab$ es estrictamente mayor que I. Lo mismo ocurre con $I : Ab$, puesto que él contiene a a. Como I es maximal, ambos ideales deben admitir una base finita pero, según lo establecido en el punto 1.°, I debería también admitir una base finita, lo cual es absurdo.

22

1.° Sean $a, b \in \mathcal{A}_n$. Existen dos polinomios $f, g \in \mathcal{B}$, ambos de grado n, que tienen respectivamente por coeficientes directores a y b. Si $a - b \neq 0$, es $a - b$ coeficiente director de $f - g \in \mathcal{B}$, luego $a - b \in \mathcal{A}_n$. Si $c \in A$, es ca el coeficiente director de $cf \in \mathcal{B}$, luego $ca \in \mathcal{A}_n$. Por tanto $\mathcal{A}_n$ es un ideal. El polinomio xf es de grado $n + 1$ y tiene coeficiente director a, por lo que vemos que $\mathcal{A}_n \subseteq \mathcal{A}_{n+1}$.

La sucesión de los $\mathcal{A}_j$ es creciente, y como A es nœtheriano, es estacionaria a partir de un cierto rango p.

2.° Sea $\mathcal{B}'$ el ideal engendrado por los f_{kl}. Es evidente que $\mathcal{B}' \subseteq \mathcal{B}$. Para demostrar que todo $f \in \mathcal{B}$ es de $\mathcal{B}'$, vamos a razonar por recurrencia sobre el grado m de f. Sea a el coeficiente director de f. Distingamos dos casos:

Si $m < p$, se tiene $a \in \mathcal{A}_m$ luego $a = \sum u_i a_{mi}$. Entonces el polinomio $f - \sum u_i f_{mi}$ tiene grado estrictamente inferior a m, luego pertenece a $\mathcal{B}'$, y por tanto el propio f está en $\mathcal{B}'$.

Si $m \geqslant p$ se tiene $a \in \mathcal{A}_m = \mathcal{A}_n$, luego $a = \sum u_i a_{ni}$. Entonces el polinomio $f - \sum u_i x^{m-p} f_{ni}$ tiene grado estrictamente inferior a m, luego pertenece a $\mathcal{B}'$ y por consecuencia f es también de $\mathcal{B}'$. Se tiene pues $\mathcal{B} = \mathcal{B}'$. Se ha demostrado así que todo ideal de $A[x]$ admite una base finita, es decir, que $A[x]$ es nœtheriano.

23

1.° Sea $\mathcal{A}\mathcal{B} = Q_1 \cap \ldots \cap Q_n$ una descomposición de $\mathcal{A}\mathcal{B}$ en ideales P_i-primarios. Si $\mathcal{B} \nsubseteq \mathcal{A}\mathcal{B}$, existe un i tal que $\mathcal{B} \nsubseteq Q_i$. Como $\mathcal{B}$ está contenido en todas las potencias de $\mathcal{A}$ ninguna de estas potencias puede estar contenida en Q_i. Ahora, se tiene $\mathcal{A}\mathcal{B} \subseteq Q_i$. Hay pues contradicción, pues Q_i es primario fuerte (texto: VIII, 4, teor. 1).

2.° Sea $\{b_1, ..., b_r\}$ una base de $\mathfrak{B}$. Puesto que $\mathfrak{B} \subseteq \mathfrak{A}\mathfrak{B}$, se puede escribir

$$b_i = \sum_j a_{ij} b_j \quad (1 < i < r),$$

con $a_{ij} \in \mathfrak{A}$.

Pongamos $s_{ij} = \delta_{ij} - a_{ij}$ (δ_{ij} símbolo de Kronecker). Se tiene, para todo $1 < i < r$,

$$\sum_{j=1}^{r} s_{ij} b_j = 0.$$

Sea Δ el determinante de los s_{ij}. Por un cálculo clásico de álgebra lineal (texto: X, 5, pág. 396) se tiene

$$\Delta b_j = 0 \quad (1 < j < r), \quad \text{luego } \Delta\mathfrak{B} = 0.$$

Pero Δ es de la forma $1 - a$, con $a \in \mathfrak{A}$.

Sea $x \in A$. Supongamos que existe un $a \in \mathfrak{A}$ tal que $(1 - a)\, x = 0$. Se tiene entonces $x = ax$, de donde, por recurrencia, $x = a^n x$ para todo entero n. Esto implica que x pertenece a la intersección de los $\mathfrak{A}^n$, es decir a $\mathfrak{B}$.

3.° Si $\mathfrak{A} \neq A$, se tiene $1 - a \neq 0$. Si además se supone que A es íntegro, resulta $\mathfrak{B} = (0)$.

Aunque A no sea íntegro, es posible señalar un caso importante en el que $\mathfrak{B} = (0)$. Es el caso en que $\mathfrak{A}$ está contenido en todos los ideales maximales. Entonces $1 - a$ no puede estar contenido en un ideal maximal $\mathfrak{M}$ (se tendría $a \in \mathfrak{M}$ y $1 - a \in \mathfrak{M}$), luego es inversible. $(1 - a)\,\mathfrak{B} = 0$ implica $\mathfrak{B} = (0)$, multiplicando por el inverso de $1 - a$.

24

1.° Supongamos que X sea P-primario. Si $I \nsubseteq P$ se tiene $I^k \nsubseteq P$; pero $I^k(X : I^k) \subseteq X$, luego $X : I^k \subseteq X$ (X es en efecto primario-fuerte). Como la inclusión inversa es siempre cierta, se tiene $X : I^k = X$.

Si $I \subseteq P$ existe un n tal que $I^n \subseteq X$. Entonces $X : I^n = A$. Pero

$$X : I^n \subseteq X : I^k,$$

luego $X : I^k = A$.

Recíprocamente, supongamos que X y A sean las únicas fronteras de X. Si $IJ \subseteq X$ y $J \subseteq X$, se tiene $J \subseteq X : I$ luego $X : I \neq X$. *A fortiori*, la frontera de X por I es diferente de X, luego es A. Se tiene $X : I^k = A$, o también $I^k \subseteq X$.

2.° Sea $X = Q_1 \cap \ldots \cap Q_n$ una descomposición normada en ideales P_i-primarios. Supongamos $I \nsubseteq P_i$ para $i < m$ e $I \subseteq P_i$ para $i > m$. Como los Q_i son en número finito, es posible encontrar un k tal que $X : I^k = X_{[I]}$, y $Q_i : I^k = Q_{i[I]}$ cualquiera que sea i.

Se tiene entonces

$$\begin{aligned} X_{[I]} = X : I^k &= (Q_1 : I^k) \cap \ldots \cap (Q_n : I^k) \\ &= Q_{1[I]} \cap \ldots \cap Q_{n[I]} \\ &= Q_1 \cap \ldots \cap Q_m. \end{aligned}$$

Esto resulta de la demostración dada en la primera cuestión. Si $i < m$ y $P_j \subseteq P_i$, se tiene $I \nsubseteq P_j$, luego $j < m$; $X_{[I]}$ es pues un componente aislado.

Recíprocamente, sea $Q_1 \cap \ldots \cap Q_m$ un componente aislado.

Pongamos $I = P_{m+1} \ldots P_n$. Se tiene $I \subseteq P_j$ para $j > m$. Pero $I \nsubseteq P_i$ para $i < m$, pues de no ser así se pondría encontrar un $j > m$ tal que $P_j \subseteq P_i$.

Según la primera parte de la demostración, resulta

$$X_{[I]} = Q_1 \cap \ldots \cap Q_m.$$

25

1.° Sea P el radical de (0). Todo elemento de P es nilpotente, luego divisor de cero. Si $xa = 0$ y $x \neq 0$ se tiene $a \in P$, porque (0) es P-primario.

2.° Hemos supuesto A no íntegro, luego $P \neq (0)$. Sea $0 \neq p \in P$. Si $x \in (0) : P$, se tiene $xp = 0$, luego $x \in P$. Las inclusiones $(0) \subseteq (0) : P \subseteq P$ implican que $(0) : P$ admite por radical P. Si $xy \in (0) : P$ e $y \notin (0) : P$, se tiene $xyP = (0)$ e $yP \neq (0)$. Por tanto x es divisor de cero, luego $x \in P$. Esto muestra que $(0) : P$ es P-primario. Como A es nœtheriano, se sabe que existe n tal que $P^n = (0)$. Tomemos n minimal para esta propiedad. Se ha visto que $n > 1$. De $PP^{n-1} = (0)$ sale $P^{n-1} \subseteq (0) : P$. Pero $P^{n-1} \neq (0)$, luego $(0) : P \neq (0)$.

3.° Sea $\lambda a \in Q \cap (a)$. Como $a \notin Q$ se tiene $\lambda \in P$, porque Q es P-primario. Pero $a \in (0) : P$, luego $\lambda a = 0$. Obtenemos efectivamente $Q \cap (a) = (0)$.

4.° Sea $(0) : M$ un elemento maximal en el conjunto

$$\{(0) : X;\ (0) \neq X \subseteq C\}.$$

Este ideal es primo. En efecto, si $IJ \subseteq (0) : M$ y $J \nsubseteq (0) : M$, se tiene $IJM = (0)$; luego $I \subseteq (0) : JM$. Pero $(0) \neq JM \subseteq C$ y además $JM \subseteq M$, luego

$(0) : M \subseteq (0) : JM$. Como $(0) : M$ es maximal, eso implica $(0) : M = (0) : JM$. Luego $I \subseteq (0) : M$.

El ideal primo $(0) : M$ contiene al radical de (0), es decir a P. Luego $P \subseteq (0) : M$, $PM = (0)$, $M \subseteq (0) : P$. Se tiene pues

$$(0) \neq M \subseteq [(0) : P] \cap C.$$

5.° Si (0) es $\cap$-irreducible no hay ningún ideal P-primario comprendido entre (0) y $(0) : P$. Ello es una consecuencia inmediata de lo visto en el punto 3.°.

Si (0) no es $\cap$-irreducible, se puede al menos expresarlo como intersección finita de ideales $\cap$-irreducibles, pues A es nœtheriano: $(0) = C_1 \cap \ldots \cap C_r$. Se puede suponer r minimal. Cada C_i es primario. Todos ellos tienen por radical P, pues se puede encontrar

$$0 \neq x \in \bigcap_{j \neq i} C_j.$$

Así, $xC_i = (0)$ y C_i está contenido en el conjunto de divisores de (0), es decir en P. Como $(0) : P \neq (0)$, existe un i tal que $(0) : P \nsubseteq C_i$. Entonces

$$(0) \neq [(0) : P] \cap C_i \subset (0) : P.$$

(La primera desigualdad resulta del 4.° punto.) $Q = [(0) : P] \cap C_i$ es P-primario, como intersección de dos ideales P-primarios.

26

1.° La condición es desde luego suficiente. Recíprocamente, si $\mathcal{C} = \mathcal{A} : \mathcal{B}$ y $\mathcal{B} \nsubseteq \mathcal{A}$, se tiene $\mathcal{B}\mathcal{C} \subseteq \mathcal{A}$, luego $\mathcal{B} \subseteq \mathcal{A} : \mathcal{C}$. Esto implica de una parte $\mathcal{A} \subset \mathcal{A} : \mathcal{C}$ y de otra parte

$$\mathcal{A} : (\mathcal{A} : \mathcal{C}) \subseteq \mathcal{A} : \mathcal{B} = \mathcal{C}.$$

Pero $(\mathcal{A} : \mathcal{C})\,\mathcal{C} \subseteq \mathcal{A}$, luego $\mathcal{C} \subseteq \mathcal{A} : (\mathcal{A} : \mathcal{C})$ y por tanto se tiene la igualdad

$$\mathcal{C} = \mathcal{A} : (\mathcal{A} : \mathcal{C}).$$

2.° Sea F una familia no vacía de residuales propios de $\mathcal{A}$. Si A es nœtheriano, no hay nada a demostrar. Si A satisface la condición minimal, tomemos un elemento minimal $\mathcal{A} : \mathcal{M}$ en $\{\mathcal{A} : \mathcal{C} \mid \mathcal{C} \in F\}$.

Si $\mathcal{M} \subseteq \mathcal{C} \in F$ se tiene $\mathcal{A} : \mathcal{C} \subseteq \mathcal{A} : \mathcal{M}$ luego $\mathcal{A} : \mathcal{C} = \mathcal{A} : \mathcal{M}$. Resulta

$$\mathcal{C} = \mathcal{A} : (\mathcal{A} : \mathcal{C}) = \mathcal{A} : (\mathcal{A} : \mathcal{M}) = \mathcal{M}.$$

Luego $\mathcal{M}$ es maximal en F.

3.° Sea $\mathcal{A} : \mathcal{B}$ un residual propio maximal de $\mathcal{A}$.

Si $\mathcal{QL} \subseteq \mathcal{A} : \mathcal{B}$ y $\mathcal{L} \nsubseteq \mathcal{A} : \mathcal{B}$, se tiene:

$\mathcal{LB} \nsubseteq \mathcal{A}$, luego $\mathcal{A} : \mathcal{LB}$ es propio.

$\mathcal{LB} \subseteq \mathcal{B}$ implica $\mathcal{A} : \mathcal{B} \subseteq \mathcal{A} : \mathcal{LB}$ luego $\mathcal{A} : \mathcal{B} = \mathcal{A} : \mathcal{LB}$.

Se tiene $\mathcal{QLB} \subseteq \mathcal{A}$ luego $\mathcal{Q} \subseteq \mathcal{A} : \mathcal{LB}$, es decir $\mathcal{Q} \subseteq \mathcal{A} : \mathcal{B}$. Esto demuestra que $\mathcal{A} : \mathcal{B}$ es primo.

4.° Sea $\mathcal{P}_1$ un residual propio maximal de $\mathcal{A}$. Éste existe, según lo 2.° y es primo, según lo 3.°. Además, $\mathcal{A}_1 = \mathcal{A} : \mathcal{P}_1 \supset \mathcal{A}$, también por lo 1.°. Si $\mathcal{A} : \mathcal{P}_1 = A$, se tiene $A\mathcal{P}_1 \subseteq \mathcal{A}$, luego $\mathcal{P}_1^2 \subseteq \mathcal{A}$. Si no, $\mathcal{A}_1$ admite residuales propios y se puede tomar uno maximal $\mathcal{P}_2$. Se tiene, $\mathcal{A}_2 = \mathcal{A}_1 : \mathcal{P}_2 \supset \mathcal{A}_1$. Se definirá $\mathcal{P}_n$ como un residual propio maximal de $\mathcal{A}_{n-1}$ y $\mathcal{A}_n = \mathcal{A}_{n-1} : \mathcal{P}_n = \mathcal{A} : \mathcal{P}_1 \dots \mathcal{P}_n$.

La sucesión de los $\mathcal{A}_n$ alcanza a A, pues si no sería una sucesión estrictamente creciente e infinita de residuales propios de $\mathcal{A}$. Si $\mathcal{A}_n = A$, se tiene pues $\mathcal{A} : \mathcal{P}_1 \dots \mathcal{P}_n = A$, luego $\mathcal{P}_1 \dots \mathcal{P}_n A \subseteq \mathcal{A}$, lo que da $\mathcal{P}_1 \mathcal{P}_2 \dots \mathcal{P}_n^2 \subseteq \mathcal{A}$.

27

1.° Según el problema anterior, (0) es producto de ideales primos $\mathfrak{m}_1 \dots \mathfrak{m}_q$. Si A verifica la condición minimal, todo ideal primo es maximal. Luego en ambos casos los $\mathfrak{m}_i$ son maximales.

2.° Pongamos $\mathfrak{q}_i = \mathfrak{m}_1 \dots \mathfrak{m}_i$. Sea φ el homomorfismo canónico de $\mathfrak{q}_{i-1}$ sobre $\mathfrak{q}_{i-1}/\mathfrak{q}_i = E_i$. Sea h el homomorfismo canónico de A sobre $A/\mathfrak{m}_i$, que es un cuerpo puesto que $\mathfrak{m}_i$ es maximal. Sean $\alpha \in E_i$ y $\pi \in A/\mathfrak{m}_i$. Se puede escribir $\alpha = \varphi(a)$ y $\pi = h(p)$. Pondremos $\pi\alpha = \varphi(pa)$. Se define así una operación externa sobre E_i, pues si $\varphi(a') = \varphi(a)$ y $h(p') = h(p)$ se tiene,

$$\begin{aligned}\varphi(pa) - \varphi(p'a') = \varphi(pa - p'a') &= \varphi((p-p')a + p'(a-a')) \\ &= \varphi((p-p')a) + \varphi(p'(a-a')).\end{aligned}$$

Pero

$$(p-p')a \in \mathfrak{m}_i \mathfrak{q}_{i-1} = \mathfrak{q}_i, \quad \text{luego} \quad \varphi((p-p')a) = 0,$$

y $p'(a-a') \in \mathfrak{q}_i$ puesto que $(a-a') \in \mathfrak{q}_i$ luego $\varphi(p'(a-a')) = 0$. Se tiene, pues, efectivamente,

$$\varphi(pa) = \varphi(p'\,a').$$

Los axiomas de espacio vectorial se verifican sin dificultad.

3.° La aplicación $V \to \varphi^{-1}(V)$ establece una biyección entre los subespacios de E_i y los ideales de A comprendidos entre $\mathfrak{q}_i$ y $\mathfrak{q}_{i-1}$. En efecto, sean $a \in \varphi^{-1}(V)$ y $x \in A$. Se tiene $\varphi(a) \in V$, luego

$$\varphi(xa) = h(x)\,\varphi(a) \in V \quad \text{y} \quad xa \in \varphi^{-1}(V).$$

Recíprocamente, si $\mathcal{J}$ es un ideal comprendido entre $\mathfrak{q}_{i-1}$ y $\mathfrak{q}_i$, si $\varphi(a) \in \varphi(\mathcal{J})$ con $a \in \mathcal{J}$ y si $h(x) \in A/\mathfrak{m}_i$, se tiene

$$h(x)\,\varphi(a) = \varphi(xa) \in \varphi(\mathcal{J}).$$

Resulta que los subespacios de V satisfacen la condición de cadena ascendente o descendente. Si E_i fuese de dimensión infinita sobre $K = A/\mathfrak{m}_i$, se podría encontrar una familia libre $(x_n)_{n \in \mathbf{N}}$. Entonces

$$V_p = \sum_{n \geqslant p} Kx_n \quad \text{y} \quad W_p = \sum_{n \leqslant p} Kx_n$$

constituirían dos sucesiones infinitas, la una estrictamente creciente, la otra estrictamente decreciente.

4.° Puesto que E_i es de dimensión finita k, se puede encontrar una sucesión finita maximal de subespacios $\{V_\lambda^i\}$ tal que

$$(0) = V_0^i \subset V_1^i \subset \ldots V_{k-1}^1 \subset V_k^1 = E_i.$$

Entonces $\{\varphi^{-1}(V_\lambda^i)\}_{\lambda \leqslant k}$ es una sucesión finita maximal de ideales de A, de $\mathfrak{q}_i$ a $\mathfrak{q}_{i-1}$. Por yuxtaposición de las sucesiones obtenidas para los diversos índices $1 \leqslant i \leqslant q$ se obtiene una sucesión de composición en A (considerado como A-módulo). Si L designa la longitud de esta sucesión, se sabe (teorema de Jordan-Hölder) que toda sucesión finita estrictamente creciente de ideales tiene longitud inferior a L.

28

Si A es íntegro, todo indivisible es irreducible: $p = xy$ implica, por ejemplo, $x \in Ap$, luego $x = ap$; $p = pay$, $p(1-ay) = 0$, luego $1 - ay = 0$, puesto que $p \neq 0$, lo que significa que y es inversible. La recíproca es siempre cierta.

Supongamos A nœtheriano. Sea $a \neq 0$. Por reducción al absurdo, supongamos que a no sea producto de elementos inversibles o indivisibles. Al no ser a indivisible puede escribirse $a = a_1 a_1'$, con $a_1' \notin Aa$ y $a_1 \notin Aa$, luego $Aa \subset Aa_1$. Al menos uno de estos dos elementos, por ejemplo, a_1, no es indivisible. Se puede entonces descomponer a_1 en la forma $a_1 = a_2 a_2'$ con $Aa_1 \subset Aa_2$. Se obtiene así una sucesión de ideales Aa_n estrictamente creciente e infinita, lo que contradice la hipótesis.

29

1.° Puesto que A es conmutativo.

$$(fg)^2 = f^2 g^2 = fg, \quad (1-f)(1-f) = 1-f-f+f^2 = 1-f.$$

2.° Se tiene

$$ef = (f+g)f = f^2 + gf = f^2 = f.$$

Por consiguiente

$$(1-e)(1-f) = 1-e-f+ef = 1-e.$$

Se tiene pues,

$$1-e \in A(1-f) \quad \text{o} \quad A(1-e) \subseteq A(1-f).$$

Efectivamente esta inclusión es estricta, pues si fuese $1-f = b(1-e)$, seguiría

$$g = e-f = e-ef = e(1-f) = be(1-e) = b(e-e^2) = 0.$$

3.° Sean g y f indescomponibles. Se puede escribir

$$g = g-fg+fg = (1-f)g+fg.$$

Según la primera cuestión, $(1-f)g$ y fg son idempotentes. Su producto es nulo:

$$(1-f)gfg = (f-f^2)g^2 = 0.$$

Como g es indescomponible, uno de los dos es nulo: $g = fg$, o $0 = fg$. El invertir los papeles de f y g nos conduce a la alternativa: $f = fg$, o $0 = fg$. Pero como f y g son distintos, uno de ellos no es igual a fg, luego $fg = 0$.

4.° Supongamos A nœtheriano. Imaginemos, para reducir al absurdo, que existe un idempotente e que no es suma de indescomponibles. En particular, e no es indescomponible, luego $e = e_1 + e_1'$ con e_1 y e_1' distintos de 0 y $e_1 e_1' = 0$. Uno de los dos, por ejemplo, e_1 no es indescomponible. Por recurrencia se construye una sucesión $\{e_n\}$ que permite definir una sucesión estrictamente creciente de ideales

$$A(1 - e) \subset A(1 - e_1) \subset A(1 - e_2)...$$

(cfr. la cuestión segunda), contra la hipótesis.

En particular, 1 es suma de idempotentes indescomponibles $g_i (1 \leqslant i \leqslant n)$. Se pueden suponer los g_i distintos, pues si g_i apareciese k veces en la suma $1 = \Sigma g_i$, se obtendría, al multiplicar por g_i los dos miembros de la igualdad, $g_i = k g_i^2 = k g_i$, lo que permite reemplazar $k g_i$ por g_i. Consideremos los anillos $A_i = A g_i$. La aplicación $x \to (x g_i)_i$ es un homomorfismo de A en el producto de los anillos A_i. En efecto,

$$x = \sum_{i=1}^{n} x g_i, \qquad y = \Sigma\, y g_j,$$

luego

$$xy = \sum_{i,j} xy g_i\, g_j = \sum_{h} xy g_h$$

puesto que $g_i\, g_j = 0$ si $i \neq j$. La aplicación es inyectiva, pues $x g_i = 0$ para todo i implica $x = \Sigma\, x g_i = 0$. Y es suprayectiva, evidentemente.

30

1.° Sea e un idempotente. Se tiene $1 = 1 - e + e$. Ahora bien, $1 - e$ y e son idempotentes cuyo producto es nulo. Se tiene, pues, $1 - e = 0$, o $e = 0$.

Si $x^r = a x^{r+1} = (ax)\, x^r$, la igualdad $x^r = (ax)^k\, x^r$ es cierta para $k = 1$. Si es cierta para el entero k, se tiene

$$x^r = (ax)^k\, x^r = (ax)^k\, (ax)\, x^r = (ax)^{k+1}\, x^r.$$

Por tanto, la igualdad es cierta para todo k. En particular, $x^r = (ax)^r\, x^r$. Se deduce:

$$(ax)^r = a^r\, x^r = (ax)^r\, (ax)^r.$$

Se tiene, pues, $a^r x^r = 1$, o $a^r x^r = 0$. En el primer caso, x es inversible. En el segundo, $x^r = (ax)^r x^r = 0$.

2.° Sea S el conjunto de los elementos no divisores de cero. Es una parte estable de A. Si no existe ningún elemento indivisible divisor de cero, S contiene los elementos indivisibles y contiene también, evidentemente, los elementos inversibles.

Ahora bien, al ser A nœtheriano, todo elemento no nulo es producto de elementos inversibles o indivisibles (ejercicio VI, 28). Se tiene pues $S = A - \{0\}$, contrariamente a la hipótesis hecha sobre A.

Sea p un elemento indivisible divisor de cero. Se puede escribir $pa_1 = 0$ con $a_1 \neq 0$. Si $a_1 \in Ap$, pongamos $a_1 = pa_2$. Reiterando se define una sucesión a_i con $a_i = a_{i+1} p$. Esta construcción no puede proseguirse indefinidamente, pues se tiene una sucesión de ideales $Aa_1 \subset Aa_2 \subset Aa_3 \ldots$ estrictamente creciente. En efecto, tenemos $p^i a_i = 0$, luego $a_{i+1} \in Aa_i$ implicaría

$$a_1 = a_{i+1} p^i \in Aa_i p^i = (0).$$

Por tanto, esa sucesión termina con $a_m \notin Ap$.

3.° Puesto que el anillo es principal, $\{y; yp^m \in Ap^{m+1}\} = Ab$. Se tiene $p \in Ab$, luego $p = ub$. Como p es indivisible se tiene $b \in Ap$ o $u \in Ap$. La primera eventualidad se excluye, pues se tendría

$$a_m \in Ab \subseteq Ap \text{ (esto resulta de } a_m p^m = 0 \in Ap^{m+1}).$$

Se tiene pues $u = vp$, y, por consiguiente, $p = bvp$, de donde $p^m = bvp^m \in Ap^{m+1}$, lo que significa $1 \in Ab$.

Según lo 1.°, se deduce $p^m = 0$, teniendo en cuenta el hecho de que p no puede ser inversible. Esto muestra que $m > 1$.

Si $ph = 0$ y $h \neq 0$, se puede hacer jugar a h el papel de a_1 en la cuestión precedente. Ahora bien, acabamos de ver que la sucesión no podía detenerse en a_1. Se puede pues afirmar que $h \in Ap$. Por otra parte,

$$1 = 1 - x^m p^m = (1 - xp)(x^{m-1} p^{m-1} + \ldots + 1)$$

muestra que $1 - xp$ es inversible, cualquiera sea x.

4.° Sea $s \notin Ap$. Se tiene $Ap + As = Ad$. Como $p \in Ad$, resulta $p = xd$. Por ser p indivisible, se tiene $d \in Ap$ o $x \in Ap$. El primer caso debe excluirse, pues con él se tendría $s \in Ad \subseteq Ap$. Luego $x = yp$. Por consiguiente $p = ypd$, $p(1 - yd) = 0$. Según la cuestión tercera esto implica $1 - yd \in Ap \subseteq Ad$, luego $1 \in Ad$. Por consiguiente, $1 = up + vs$. Pero $vs = 1 - up$ es inversible según el punto 3.°. También, pues, lo es s.

5.° Sea q indivisible. Como q no es inversible, $q \in Ap$. Luego $q = hp$. No puede ser $h \in Aq$, pues si $h = xq$, $q = xqp$, $q(1 - xp) = 0$, luego $q = 0$, puesto que $1 - xp$ es inversible. Se tiene, pues, $p \in Aq$. Pero entonces $Ap = Aq$, y $h \notin Ap$, lo que demuestra que h es inversible.

Todo elemento no nulo es producto de elementos inversibles o indivisibles, luego puede escribirse bajo la forma hp^k donde h es inversible. Todos los ideales son principales, luego son de la forma Ap^k, y forman una cadena

$$(0) = Ap^m \subset Ap^{m-1} \subset \ldots \subset Ap \subset A.$$

Tenemos $Ap^{k+1} \subset Ap^k$, porque $p^k \in Ap^{k+1}$ implicaría $p^k = 0$, según el apartado 1.°, luego $a_1 = p^k a_{k+1} = 0$.

CAPÍTULO VII

Cuerpos. Ecuaciones algebraicas

Enunciados

1

Sean K un cuerpo conmutativo y $f(x) = f_1(x) f_2(x) \dots f_r(x)$ el producto de r polinomios pertenecientes a $K[x]$, primos entre sí dos a dos. Designamos por $q_j(x)$ el polinomio tal que $f_j(x)\, q_j(x) = f(x)$ $(1 < j < r)$, por I el ideal principal engendrado en $K[x]$ por $f(x)$, por A el anillo cociente $K[x]/I$, y por α la clase de x módulo I.

1.° Demostrar que existen polinomios $p_1(x)$, $p_2(x)$, ..., $p_r(x)$ satisfaciendo a estas dos condiciones:

a) el grado de $p_j(x)$ es estrictamente inferior al de $f_j(x)$;

b) $\sum_{j=1}^{r} p_j(x)\, q_j(x) = e$, elemento unidad de K.

2.° Pondremos

$$e_j = p_j(\alpha)\, q_j(\alpha), \qquad I_j = Ae_j \qquad (1 < j < r).$$

Demostrar que cuando es $j \neq k$, el producto de los elementos e_j, e_k es cero. ¿Qué puede decirse del producto de dos ideales I_j, I_k?

Demostrar que A es suma directa de los ideales I_j, es decir, que todo elemento de A se expresa de modo único en la forma $\sum_{j=1}^{r} \xi_j$ con $\xi_j \in I_j$.

Demostrar que $I_j = K[\alpha e_j]$, y que I_j es isomorfo al anillo cociente de $K[x]$ por el ideal engendrado por $f_j(x)$.

2

Sean K un cuerpo conmutativo, k un subcuerpo de K, A y B dos cuerpos intermedios tales que $(A : k) = p$, $(B : k) = q$. Sea L el menor subcuerpo que contiene a A y a B.

1.° Verificar que $(L : A) \leq q$, $(L : B) \leq p$, $(L : k) \leq pq$.

2.° Caracterizar el caso en que $(L : K) = pq$, mediante una conveniente propiedad de los elementos de una base de A considerado como espacio vectorial sobre k.

3.° Supongamos $(K : k) = 4$, $p = q = 2$, $A = k(\alpha)$, $B = k(\beta)$. Establecer la equivalencia de las propiedades siguientes:

a) $A \neq B$,

b) $L = K$,

c) $\{\varepsilon, \alpha, \beta, \alpha\beta\}$ es una base de L sobre k, siendo ε el elemento unidad del cuerpo k.

3

Sean k un cuerpo conmutativo y K una extensión algebraica finita de k.

1.° Supongamos que K es una extensión algebraica simple $k(\alpha)$ de k. Demostrar que no hay más que un número finito de cuerpos intermedios.

2.° Establecer la recíproca de esa propiedad distinguiendo los dos casos:

a) k es un cuerpo finito;

b) k tiene una infinidad de elementos.

4

Un supercuerpo conmutativo K de un cuerpo conmutativo k, se llama extensión cuadrática de k si es $(K : k) = 2$.

1.° Suponemos k de característica distinta de 2. Demostrar que las extensiones cuadráticas de k, si existen, son los cuerpos de ruptura de los polinomios irreducibles de la forma $f(x) = x^2 - a$, $(a \in k)$.

2.° Suponemos k de características 2. Demostrar que las extensiones cuadráticas de k, si existen, son los cuerpos de ruptura de los polinomios irreducibles de una de las formas

$$f(x) = x^2 - a, \quad g(x) = x^2 - x - a, \quad (a \in k).$$

¿Pueden ser k-isomorfas una extensión L_1 cuadrática del primer tipo y una extensión L_2 cuadrática del segundo tipo?

5

Sean K y k dos cuerpos conmutativos de característica distinta de 2, tales que

$$k \subset K, \quad (K : k) = 4.$$

Establecer los siguientes resultados:

1.° Para que exista un cuerpo intermedio L $(k \subset L \subset K)$, es necesario y suficiente que sea K el cuerpo de ruptura de un polinomio irreducible de la forma

$$f(x) = x^4 + ax^2 + b \in k[x].$$

2.° Si $k(\alpha)$ y $k(\beta)$, donde $\alpha^2 = a \in k$, $\beta^2 = b \in k$, son dos extensiones cuadráticas (ejercicio VII, 4) distintas de k, contenidas en K, existen en total tres de tales extensiones.

3.° Si K es un cuerpo finito, dos extensiones cuadráticas de k contenidas en K no pueden ser distintas.

6

1.° ¿Cómo debemos elegir el número racional r para que el polinomio

$$f(x) = x^4 + r \in \mathbf{Q}[x]$$

sea irreducible?

2.° Si K es un cuerpo de ruptura de ese polinomio, supuesto irreducible, determinar los subcuerpos de K distintos de K y de $\mathbf{Q}$.

7*

Sea k un cuerpo conmutativo de característica $p \neq 0$ y sea Π su cuerpo primo.

1.° Expresar los ceros del polinomio $f(x) = x^p - x - a \in k[x]$, en función de uno de ellos α, elemento de un conveniente supercuerpo K de k.

2.° Suponemos que existe un polinomio $d(x)$ del anillo $k[x]$, de grado $r \geq 2$, irreducible, divisor de $f(x)$. Demostrar que existe en Π un elemento s

tal que $d(x + s) = d(x)$. Mediante la consideración del término de grado $r - 1$ de $d(x)$, demostrar que necesariamente es $r = p$.

3.° Deducir de lo que precede una condición necesaria y suficiente para que $f(x)$ sea irreducible sobre k. Demostrar que si $f(x)$ es irreducible, el polinomio $f_t(x) = x^p - x - ta$, donde $t \in \Pi$, $t \neq 0$, es también irreducible sobre k.

4.° Consideremos los dos polinomios de $k[x]$

$$f(x) = x^p - x - a, \quad g(x) = x^p - x - b,$$

que suponemos irreducibles sobre k.

Demostrar que para que los cuerpos de descomposición de estos polinomios sobre k sean k-isomorfos, es necesario y suficiente que $g(x)$ sea de la forma $f_t(x - c)$, donde $c \in k$, $t \in \pi$, $t \neq 0$.

8

Sean K un cuerpo conmutativo, x una indeterminada, n un entero superior o igual a 2.

1.° Determinar los K-automorfismos del cuerpo $K(x)$.

2.° Demostrar que existe un único endomorfismo φ de $K(x)$ dejando invariante todo elemento de K, tal que $\varphi(x) = x^n$. Este endomorfismo φ es inyectivo y no es suprayectivo.

9

Sean k un cuerpo conmutativo de característica $p \neq 0$, Π su cuerpo primo y n un entero natural. Demostrar que la aplicación σ definida por

$$\sigma(a) = a^{p^n} \quad (a \in k),$$

es un Π-isomorfismo de k sobre uno de sus subcuerpos.

¿Con qué condición es σ un Π-automorfismo de k? ¿Con qué condición es el automorfismo idéntico de k?

10

En el conjunto C_2 de las matrices 2×2 con coeficientes complejos, que es un espacio vectorial de dimensión 8 sobre el cuerpo R de los reales, consideremos el subespacio Q engendrado por las matrices

$$E = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \quad J = \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}, \quad K = \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}, \quad L = \begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix},$$

($i \in \mathbf{C}$, $i^2 = -1$).

1.° Verificar que Q es un cuerpo no conmutativo. ¿Cuál es su centro?

2.° Resolver en Q las siguientes ecuaciones en M:

$$M^2 + E = 0,$$
$$M^2 - 2\lambda M + \sigma E + \alpha J + \beta K + \gamma L = 0,$$
$$M^2 + JM + E - L = 0.$$

11

Sean K un cuerpo no conmutativo, $K[x]$ el anillo de polinomios en una indeterminada x, con coeficientes de K, y

$$f(x) = x^2 + ax + b, \quad b \neq 0,$$

un polinomio de $K[x]$.

1.° Demostrar que para que $f(x)$ admita como divisor a la derecha y a la izquierda $x - c \in K[x]$, es necesario y suficiente que

$$f(c) = 0, \quad ac = ca.$$

Estudiar el caso en que b pertenece al centro de K.

2.° Demostrar por un ejemplo, que, dado $f(x)$, puede no existir ningún elemento $c \in K$ que satisfaga esas condiciones.

12

Sea B un anillo íntegro y conmutativo. Sea A un subanillo de B que contiene el elemento unidad e. Se supone que todo elemento de B es entero algebraico sobre A.

Demostrar que A es un cuerpo si y sólo si B es un cuerpo.

13

Un anillo A íntegro, conmutativo, con elemento unidad e, se dice integralmente cerrado si el conjunto $\overline{A}$ de los elementos de su cuerpo de cocientes K que son enteros algebraicos sobre A, coincide con A.

Demostrar que un anillo factorial es integralmente cerrado.

14

Sea Π un cuerpo primo de característica 0 o $p \neq 2$. Sean, además,

α una raíz primitiva $(2n + 1)$-ésima de la unidad e;

$\beta = -\alpha^n$.

Suponiendo que p no sea divisor de $2n + 1$ (si la característica es p), demostrar que β es una raíz primitiva $(4n + 2)$-ésima de la unidad.

Deducir la igualdad de los cuerpos $\Pi(\alpha)$ y $\Pi(\beta)$.

15

Designamos por Π el cuerpo de dos elementos, por $k = \Pi(u, v)$ el cuerpo de las fracciones racionales en dos indeterminadas, u, v, con coeficientes en Π, por K un cuerpo de descomposición del polinomio $f(x) = (x^2 - u)(y^2 - v)$. Utilizando el ejercicio VII, 2, demostrar que K no es una extensión algebraica simple de k.

16*

Sean K un cuerpo no conmutativo de característica $p \neq 0$, a un elemento de orden finito del grupo multiplicativo $K^* = K - \{0\}$, no perteneciente al centro de K, Π el subcuerpo primo de K.

La extensión simple $k = \Pi(a)$ es entonces un subcuerpo conmutativo de K. Sea $N = p^m$ el número de sus elementos.

Designamos por H el anillo de los endomorfismos de K considerado como espacio vectorial sobre k, por ε el elemento unidad de H y por ω el elemento nulo de H.

1.° Verificar que la aplicación φ de K en K definida por

$$\varphi(x) = xa - ax$$

es un elemento del anillo H, y que

$$\varphi^N - \varphi = \prod_{b \in k} (\varphi - b\varepsilon) = \omega.$$

2.° Demostrar que existe un elemento b_0 no nulo de k, tal que el endomorfismo $\varphi - b_0 \varepsilon$ no sea inyectivo.

Deducir que existen al menos un elemento no nulo $c \in k$ y un entero natural s tales que

$$cac^{-1} = a + b_0 = a^s \neq a.$$

17

Sea K un cuerpo tal que el grupo multiplicativo $K^* = K - \{0\}$ sea un grupo con torsión (o grupo periódico). Demostrar que K es conmutativo, (Puede demostrarse que la característica no es nula y utilizar el ejercicio precedente.)

18

Un cuerpo finito no es nunca algebraicamente cerrado.

19*

Sean K un cuerpo conmutativo, E una clausura algebraica de K, G el grupo de los K-automorfismos de E.

1.° Designamos por $\mathcal{L}$ el conjunto de pares (L, φ), donde L es un cuerpo intermedio entre K y E, y φ es un K-isomorfismo de L en E. Se ordena $\mathcal{L}$ poniendo $(L, \varphi) \leqslant (L', \varphi')$ si y sólo si $L \subseteq L'$ y φ' prolonga a φ.

Demostrar que el conjunto $\mathcal{L}$ es inductivo. Deducir que para todo elemento (L, φ) de $\mathcal{L}$ existe un K-automorfismo de E que prolonga a φ.

2.° Sean a y b dos elementos de E que no pertenezcan a K. Establecer la equivalencia de las dos condiciones

α) existe $\sigma \in G$ tal que $\sigma(a) = b$.

β) a y b tienen el mismo polinomio característico $f(x) \in K[x]$.

20

Sean K un cuerpo conmutativo de característica $p \neq 0$, E una clausura algebraica de K, G el grupo de los K-automorfismos de E, $\overline{K}$ el cuerpo fijo de G (texto: X, 12, teorema 2).

1.° Utilizando los resultados del ejercicio precedente, demostrar que $\overline{K}$

es el conjunto de los elementos a de E para los que existe un entero natural m tal que $a^{p^m} \in K$.

2.° Demostrar que $\bar{K}$ es el mínimo subcuerpo perfecto de E que contiene a K.

3.° Demostrar que si $\bar{K} \neq K$, es $\bar{K}$ extensión algebraica infinita de K.

21

Determinar los ceros sobre el cuerpo **C** de los números complejos del ideal

$$\mathfrak{a} = (x^2 + y^2 - 2x,\ x^2 - xy) \in \mathbf{Q}[x, y]$$

y el mínimo exponente ρ tal que $(x - y)^\rho \in \mathfrak{a}$.

22

Se recuerda que toda ecuación algebraica de grado impar con coeficientes reales, admite al menos una raíz real, y que toda ecuación de segundo grado de coeficientes complejos admite al menos una raíz compleja. Utilizando el teorema fundamental de la teoría de Galois (texto: X, 12, teorema 8) y el primer teorema de Sylow (texto: II, 7) demostrar el teorema de d'Alembert: el cuerpo **C** de los números complejos es algebraicamente cerrado.

23

Sea k un cuerpo conmutativo de característica $p \neq 0$, de elemento unidad e, y sea $f(x) = x^p - x - a$ un polinomio irreducible del anillo $k[x]$. Demostrar, utilizando el ejercicio VII, 7, que el grupo de Galois de la ecuación $f(x) = 0$ es cíclico de orden p.

24*

Sean k un cuerpo conmutativo de característica $p \neq 0$, de elemento unidad e, y K una extensión de Galois de k, tal que el grupo de Galois $G = G_{K:k}$ sea cíclico de orden p. Designamos por σ un generador de G y por ξ un elemento primitivo de K.

1.° Demostrar que los elementos $\xi_j = \sigma^j(\xi)$, $(j = 0, 1, 2, ..., p-1)$ son distintos.

2.° Pondremos, para cada entero n tal que $1 < n < p-1$,

$$S_n = \xi_0^n + \xi_1^n + ... + \xi_{p-1}^n.$$

Demostrar que los S_n no son todos nulos y que $\sigma(S_n) = S_n$.

3.° Si n_0 es un índice n tal que $S_{n_0} \neq 0$, definimos un elemento η de K poniendo

$$S_{n_0}\eta + \sum_{j=1}^{p-1} j\xi_j^{n_0} = 0.$$

Demostrar que $\eta^p - \eta \in k$. Deducir que K es cuerpo de descomposición de un polinomio irreducible de la forma $f(x) = x^p - x - a \in k[x]$.

25

Sean k un cuerpo conmutativo, de elemento unidad e, $L = k(x)$ el cuerpo de las fracciones racionales en una indeterminada x con coeficientes de k, σ y τ los k-automorfismos de L definidos por

$$\sigma(x) = e - x, \quad \tau(x) = \frac{e}{x}.$$

1.° ¿Cuál es el grupo G engendrado por σ y τ?

2.° Sea

$$y = \frac{(x^2 - x + e)^3}{x^2(x-e)^2} \in L.$$

Demostrar que el cuerpo fijo de G es $K = k(y)$.

26

Sean K un cuerpo conmutativo, de elemento unidad e, y L un cuerpo de descomposición del polinomio $f(x) = x^n - e \in K[x]$. Si K es de característica $p \neq 0$, se supone que p no es divisor de n.

Sea ξ una raíz primitiva de la ecuación $f(x) = 0$. Demostrar que a todo K-automorfismo σ de L se puede asociar un número entero s, definido módulo n, tal que $\sigma(\xi) = \xi^s$.

Deducir que el grupo de Galois $G = G_{L:K}$ es conmutativo e isomorfo al grupo de unidades del anillo $\mathbf{Z}/(n)$.

27*

Sean L un cuerpo conmutativo, G un grupo finito de automorfismos de L, K el cuerpo fijo de G.

Se dice que un conjunto $\{x_\sigma\}_{\sigma \in G}$ de elementos no nulos de L es una solución del problema de Nœther si

$$(\forall \sigma, \tau \in G) \quad x_\sigma \sigma(x_\tau) = x_{\sigma\circ\tau}.$$

1.° Demostrar que $\{x_\sigma\}_{\sigma \in G}$ es una solución del problema de Nœther si, y sólo si, existe un elemento no nulo a de L tal que

$$(\forall \sigma \in G) \quad x_\sigma = a^{-1}\sigma(a).$$

2.° Demostrar que existe una biyección entre el conjunto de los homomorfismos de G en el grupo multiplicativo de K y el conjunto de soluciones del problema de Nœther formadas de elementos de K, y demostrar que para una solución tal, los elementos a considerados en el punto 1.° satisfacen una ecuación de la forma $x^r - b = 0$, donde $b \in K$ y r es un entero independiente de a.

28*

Sea K un cuerpo conmutativo con infinitos elementos y cuyo elemento unidad es e. Sean L una extensión finita de Galois de K, y $G = G_{L:K} = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ el grupo de Galois de L sobre K. Se sabe que L puede obtenerse a partir de K por medio de la adjunción de un elemento α: $L = K(\alpha)$. Sea $f(x) \in K[x]$ el polinomio característico de α.

Cada uno de los $\varphi_i (1 \leqslant i \leqslant n)$ puede prolongarse por un K-automorfismo Φ_i del anillo de polinomios $L[x]$. Ponemos,

$$g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)}, \quad g_i(x) = \Phi_i[g(x)], \quad (1 \leqslant i \leqslant n).$$

Establecer los resultados siguientes:

1.° $\sum_{i=1}^{n} g_i(x) = e.$

2.° $f(x)$ es divisor de $g_i(x)\,g_j(x)$ si $i \neq j$, y también lo es de

$$[g_i(x)]^2 - g_i(x).$$

3.° Si $D(x)$ es el determinante de la matriz $M = \| u_{ij} \|$, donde

$$u_{ij} = (\Phi_i \circ \Phi_j)\,[g(x)],$$

$f(x)$ es divisor del polinomio $[D(x)]^2 - e$ y, por consiguiente, el polinomio $D(x)$ no es nulo.

4.° Si a es un elemento de K tal que $D(a) \neq 0$, y si $b = g(a)$, los elementos $\varphi_i(b)$ $(1 \leq i \leq n)$ forman una base del K-espacio vectorial L.

29

Sea L el cuerpo $\mathbf{Q}(\xi)$, donde ξ es una raíz primitiva séptima de la unidad. Utilizando el ejercicio VII, 26, estudiar el grupo de Galois $G = G_{L:\mathbf{Q}}$, determinar sus subgrupos propios y los cuerpos intermedios. Dar un elemento primitivo para cada uno de estos cuerpos intermedios.

30

Sea L el cuerpo $\mathbf{Q}(\xi)$, donde ξ es una raíz primitiva de índice doce de la unidad. Utilizando los ejercicios VII, 5 y 26, estudiar el grupo de Galois $G = G_{L:\mathbf{Q}}$, determinar sus subgrupos propios y los cuerpos intermedios. Dar un elemento primitivo para cada uno de estos cuerpos intermedios.

31

Sea K un cuerpo conmutativo, de elemento unidad e, que contiene una raíz primitiva n-ésima de la unidad. (Si K es de característica $p \neq 0$, suponemos que p no es divisor de n.)

Sea L el cuerpo de descomposición del polinomio

$$f(x) = (x^n - a_1)\,(x^n - a_2) \ldots (x^n - a_r) \quad (a_i \in K).$$

1.° Demostrar que L es extensión de Galois de K.

2.° Demostrar que $G = G_{L:K}$ es conmutativo.

3.° Demostrar que el orden de cualquier elemento de G es divisor de n.

32

Sea K un cuerpo conmutativo de característica distinta de 2 y de 3, y sea

$$f(x) = x^3 + ax + b \in K[x]$$

un polinomio irreducible y separable. Designamos por α un cero de $f(x)$ en una extensión de K, y por e el elemento unidad de K.

1.° Demostrar que para que $K(\alpha)$ sea extensión normal de K es necesario y suficiente que $\Delta = -4a^3 - 27b^2$ sea el cuadrado de un elemento de K.

2.° Demostrar que si $K(\alpha)$ es extensión normal de K, y si la ecuación $x^2 + 3e = 0$ no tiene ninguna raíz en K, existen elementos r, s de K tales que

$$s \neq 0, \quad a = -3(r^2 + 3s^2), \quad b = 2r(r^2 + 3s^2).$$

3.° En el caso particular en que K es el cuerpo $\mathbf{Q}$ de los números racionales, o el cuerpo $\mathbf{R}$ de los números reales, verificar que las condiciones en la cuestión precedente, son suficientes para que $K(\alpha)$ sea extensión normal de K.

Soluciones

1

1.° La existencia y unicidad de los polinomios $p_j(x)$ resulta inmediatamente de la teoría de la descomposición de una fracción racional en elementos simples:

$$\frac{e}{f(x)} = \frac{e}{f_1(x) \dots f_r(x)} = \sum_{j=1}^{r} \frac{p_j(x)}{f_j(x)},$$

de donde

$$e = \sum_{j=1}^{r} p_j(x)\, q_j(x).$$

2.° Haciendo en la igualdad precedente $x = a$, se obtiene

$$e = \sum_{j=1}^{r} e_j,$$

de donde

$$A = Ae = A\left(\sum_{j=1}^{r} e_j\right) \subseteq \sum_{j=1}^{r} Ae_j = \sum_{j=1}^{r} I_j \quad \text{y} \quad A = \sum_{j=1}^{r} I_j,$$

$e_j e_k = f_j(a) f_k(a) p_j(a) p_k(a) = 0$, si $j \neq k$, porque k el segundo miembro contiene al menos una vez todos los factores $f_l(a)$ $(1 \leqslant l \leqslant r)$ cuyo producto es $f(a) = 0$. Resulta entonces $I_j I_k = 0$ para $j \neq k$.

Sea ξ un elemento de A. Por lo menos admite una descomposición de la forma $\xi = \sum_{j=1}^{r} \xi_j$ donde $\xi_j \in I_j$. Entonces se tiene

$$\xi_j = \xi_j e = \xi_j(e_1 + \dots + e_n) = \xi_j e_j = (\xi_1 + \dots + \xi_r) e_j = \xi e_j,$$

lo que demuestra que las componentes ξ_j están determinadas de modo único.

Además, haciendo $\xi = e_j$ la unicidad de ξ_j implica $\xi_j = e_j$, de donde $e_j = e_j^2$. Cada e_j es, pues, idempotente, y por tanto elemento unidad del subanillo I_j.

$ae_j \in I_j$ implica $K[ae_j] \subseteq I_j$. Inversamente, si

$$g(a) = \sum_{i=0}^{m} a_i a^i \in I_j ,$$

se tiene

$$g(a) = g(a)\, e_j = g(ae_j) \in k[ae_j], \quad \text{de donde} \quad I_j = k[ae_j].$$

Consideremos, finalmente, dos elementos de A:

$$\xi = \sum_{j=1}^{r} \xi_j, \quad \eta = \sum_{j=1}^{r} \eta_j.$$

Según los resultados precedentes, la componente de $\xi\eta$ en I_j es $\xi_j \eta_j$.

La aplicación $\xi \to \xi_j$ es pues un homomorfismo suprayectivo de anillos. Por tanto, I_j es imagen de $K[x]$ es un homomorfismo Φ.

Sea $g(x) \in K[x]$. Para que $g(x)$ pertenezca al núcleo de Φ, es necesario y suficiente que $g(a)\, e_j = 0$, lo que equivale a las condiciones sucesivas

$$g(x)\, p_j(x)\, q_j(x) \equiv 0 \pmod{I},$$

$f_j(x)\, q_j(x)$ es divisor de $g(x)\, p_j(x)\, q_j(x)$,

$f_j(x)$ es divisor de $g(x)\, p_j(x)$,

$f_j(x)$ es divisor de $g(x)$ (pues $f_j(x)$ y $p_j(x)$ son primos entre sí).

El núcleo de Φ es pues el ideal $(f_j(x))$ y el anillo I_j es efectivamente isomorfo al anillo cociente de $K[x]$ por ese ideal.

Observación: Si los $f_j(x)$ son irreducibles sobre K, los I_j son, por lo antedicho, cuerpos.

2

1.° Es evidente que

$$L = k(A, B) = k(A)(B) = A(B).$$

Sea $\{ b_1, ..., b_n \}$ una base del k-espacio vectorial B. Los elementos de esta base engendran el A-espacio vectorial L, luego $(L : A) \leq q$. Se ve lo mismo que $(L : B) \leq p$.

Además

$$(L : k) = (L : A)\,(A : k) \leqslant pq.$$

2.° Para que $(L : K) = pq$ es necesario y suficiente que $(L : A) = q$, es decir, según el razonamiento de la cuestión precedente, que los elementos de una base de B, considerado como espacio vectorial sobre k, sean también linealmente independientes sobre A (o que los elementos de una base de A sean también linealmente independientes sobre B).

3.° Con las hipótesis del enunciado $\{\varepsilon, \alpha\}$ es una base de A y $\{\varepsilon, \beta\}$ es una base de B, considerados como k-espacios vectoriales.

La hipótesis $\alpha \in B$ implicaría $A \subseteq B$ y, por consiguiente, $A = B$. Luego, si $A \neq B$, α no pertenece a B. Demostremos que entonces ε y α son linealmente independientes sobre B. Si existiesen

$$b = x + y\beta, \quad b' = x' + y'\beta \quad (x, x', y, y' \in k)$$

tales que

$$x + y\beta + (x' + y'\beta)\,\alpha = 0,$$

la hipótesis $x' + y'\beta = 0$ implicaría $x = x' = y = y' = 0$, y la hipótesis $x' + y'\beta \neq 0$ implicaría

$$\alpha = -(x' + y'\beta)^{-1}(x + y\beta) \in B,$$

lo que contradice $A \neq B$. Luego, según el punto 2.°, se tiene $(L : k) = 4$, o sea $L = K$.

Si $L = K$, puesto que $L = k(\alpha, \beta, \alpha\beta)$ los elementos $\varepsilon, \alpha, \beta, \alpha\beta$ son linealmente independientes sobre k, y forman una base de L.

En fin, si $\{\varepsilon, \alpha, \beta, \alpha\beta\}$ es una base de L sobre k, $\alpha \notin k(\beta)$, $\beta \notin (\alpha)$, luego A y B son distintos.

3

1.° Sea L un cuerpo intermedio: $k \subseteq L \subseteq K$. Si es $K = k(\alpha)$, el elemento α admite en $k[x]$ un polinomio característico

$$f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n, \quad (a_i \in k),$$

y en $L[x]$ un polinomio característico

$$g(x) = b_0 + b_1 x + \ldots + b_{q-1} x^{q-1} + x^q, \quad (b_j \in L).$$

Se sabe que en tal caso $g(x)$ divide a $f(x)$ en $K[x]$ y que $(K : L) = q$.

Consideremos $L' = k(b_0, b_1, ..., b_{q-1})$. Es claro que $L' \subseteq L$ y que $K = L'(\alpha)$. El polinomio $g(x)$, irreducible en $L[x]$ lo es también en $L'[x]$, de donde $(K : L') = q$. Resulta que $L' = L$, y L queda perfectamente determinado por el polinomio $g(x)$. Como $f(x)$ no admite más que un número finito de divisores con coeficiente principal igual a la unidad en $K[x]$, no puede existir más que un número finito de cuerpos intermedios.

2.° Si el cuerpo k es finito, K también es finito, y el resultado a demostrar es consecuencia de las propiedades de los cuerpos finitos (texto: X, 7).

Si k tiene una infinidad de elementos, es suficiente establecer que para cada par de elementos α, β de K existe un elemento γ de K tal que $k(\alpha, \beta) = k(\gamma)$. Para cada $a \in k$ consideremos $\gamma = a\alpha + \beta$ y el cuerpo intermedio $k(\gamma)$. Siendo finito el número de esos cuerpos, existe al menos un par (a_1, a_2) de elementos distintos de k tales que, si $\gamma_1 = a_1\alpha + \beta$, $\gamma_2 = a_2\alpha + \beta$, se tiene $k(\gamma_1) = k(\gamma_2)$. Si es así, γ_1 y γ_2 pertenecen a $k(\alpha, \beta)$, pero también, recíprocamente,

$$\alpha = (a_1 - a_2)^{-1}(\gamma_1 - \gamma_2) \in k(\gamma_1) \quad \text{y} \quad \beta = \gamma_1 - a_1\alpha \in k(\gamma_1),$$

de donde $k(\alpha, \beta) \subseteq k(\gamma_1)$, es decir, $k(\alpha, \beta) = k(\gamma_1)$. El resultado obtenido se extiende en seguida, por recurrencia, al cuerpo $k(\alpha_1, \alpha_2, ..., \alpha_s)$ $(s \geq 3)$.

4

Sea e el elemento unidad común a los cuerpos K y k. Existen bases $\{e, \xi\}$ de K sobre k, y es $K = k(\xi)$. Puesto que $(K : k) = 2$, los elementos e, ξ, ξ^2 de K no son linealmente independientes sobre k, y existen elementos $u, v \in k$ tales que

$$\xi^2 = u\xi + v.$$

1.° Si k no es de característica 2, existe $u' \in k$ tal que $2u' = u$. Poniendo $\alpha = \xi - u'$, $a = v + u'^2$, se tiene $\alpha^2 = a$, y $\{e, \alpha\}$ es todavía una base de K sobre k, de donde $K = k(\xi) = k(\alpha)$. Es K cuerpo de ruptura, y también cuerpo de descomposición, de $f(x) = x^2 - a \in k[x]$.

La recíproca es evidente.

2.° Si k es de característica 2, el mismo razonamiento es válido cuando $u = 0$. Se obtiene así un primer tipo de extensiones cuadráticas de k, que son los cuerpos de ruptura de los polinomios irreducibles $f(x) = x^2 - a$.

Cuando $u \neq 0$, existe α tal que $\xi = u\alpha$. Entonces α verifica la condición

$$\alpha^2 = \alpha + a, \quad \text{con} \quad a = u^{-2}v.$$

Entonces K es cuerpo de ruptura de $f(x) = x^2 - x - a \in k[x]$.

La recíproca es evidente. Se obtiene así un segundo tipo de extensiones cuadráticas de k.

Consideremos $L_1 = k(\alpha)$, $L_2 = k(\beta)$, con $\alpha^2 = a$, $\beta^2 = \beta + b$, siendo los polinomios $x^2 - a$ y $x^2 - x - b$ irreducibles sobre k. Supongamos, para reducir al absurdo, que exista un k-isomorfismo φ de L_2 sobre L_1. Si $\bar{\beta} = \varphi(\beta)$, existen $p, q \in k$ tales que $\bar{\beta} = p + q\alpha$, de donde $\bar{\beta}^2 = p^2 + q^2 a = \bar{\beta} + b$, lo que implica la contradicción $\bar{\beta} \in k$.

Observaciones: 1.° Se puede demostrar análogamente que no existe ningún isomorfismo Ψ de L_2 sobre L_1 dejando a k globalmente invariante [esto es, $\psi(k) = k$].

2.° Puede suceder que L_1 y L_2 sean dos cuerpos isomorfos, aunque, desde luego, no pueden ser k-isomorfos.

5

1.° Por ser $(K : k) = (K : L)(L : k)$, un cuerpo L tal que $k \subset L \subset K$, debe ser necesariamente una extensión cuadrática de k.

La condición indicada es suficiente, pues si $K = k(\xi)$, donde ξ es un cero del polinomio irreducible $f(x) = x^4 + ax^2 + b \in k[x]$, basta tomar $L = k(\xi^2)$ para obtener una extensión cuadrática.

Recíprocamente, sea L un cuerpo intermedio, por tanto extensión cuadrática de k. Entonces, por ejercicio VII, 4, L es de la forma $k(\alpha)$, con $\alpha^2 = a \in k$, $\alpha \notin k$. Es K una extensión cuadrática de L, luego $K = L(\lambda)$, con $\lambda^2 = \beta \in L$, $\lambda \notin L$.

El elemento β de L se escribe $\beta = p\alpha + q$; $p, q \in k$.

Si $p \neq 0$, es λ un cero del polinomio bicuadrado $f(x) = (x^2 - q)^2 - ap^2$.

La igualdad $\alpha = p^{-1}(\lambda^2 - q)$ implica $L = k(\alpha) \subseteq k(\lambda)$, luego $K = L(\lambda) \subseteq k(\lambda)$, y por consiguiente $K = k(\lambda)$. Puesto que $(K : k) = 4$, el polinomio $f(x)$ es irreducible, y K es cuerpo de ruptura de este polinomio sobre k.

Si $p = 0$, pongamos $\lambda = \mu - \alpha$. Es claro que $K = L(\lambda) = L(\mu)$, y que μ es un cero del polinomio bicuadrado

$$g(x) = (x^2 + a - q)^2 - 4ax^2.$$

No pertenece μ a k, pues de pertenecer sería $\lambda = \mu - \alpha$ un elemento de $k(\alpha) = L$. El polinomio característico de μ sobre k es de grado al menos 2, luego de grado 2 o 4, puesto que $k(\mu)$ es K o es un cuerpo intermedio. Ahora bien, una igualdad $\mu^2 = s\mu + t$ $(s, t \in k)$ implicaría $2a\mu + q - a = s\mu + t$, o sea $\mu \in k(\alpha)$, de donde la contradicción $L(\mu) = L$. Finalmente, $g(x)$ es irreducible y $K = k(\mu)$.

2.° Según el ejercicio VII, 2, la condición $k(\alpha) \neq k(\beta)$ implica la independencia sobre k de los elementos e, α, β, $\alpha\beta$, donde e es el elemento unidad de K.

Es evidente que $k(\alpha\beta)$ es una tercera extensión cuadrática de k contenida en K. Sólo falta demostrar que no hay ninguna más.

Un elemento de K tiene la forma

$$\xi = x + y\alpha + z\beta + t\alpha\beta \quad (x, y, z, t \in k).$$

Puesto que toda extensión cuadrática de k es de la forma $k(\xi)$, donde $\xi^2 \in k$, $\xi \notin k$, (cfr. ejerc. VII, 4), el problema propuesto equivale a la resolución en k del sistema

$$\begin{cases} xy + bzt = 0, \\ xz + ayt = 0, \\ yz + xt = 0, \\ y, z, t \text{ no todos son nulos.} \end{cases}$$

Se constata fácilmente que las soluciones para las que $t = 0$ conducen a los dos cuerpos $k(\alpha)$, $k(\beta)$ mientras que las soluciones para las que $t \neq 0$ conducen al cuerpo $k(\alpha\beta)$.

3.° Si K es finito es un campo de Galois, lo mismo que k.

Si k tiene p^q elementos, K deberá tener p^{4q}, y un cuerpo intermedio L tendrá p^{2q}, siendo p la característica común de estos campos.

Se sabe que un subcuerpo de un campo de Galois está determinado unívocamente por el número de sus elementos (texto: X, 7). Por tanto, K admite un único subcuerpo L tal que $(K : L) = 2$. Por lo demás este subcuerpo es el conjunto de raíces de la ecuación

$$x^{p^{2q}} - x = 0.$$

6

1.° Para que $f(x)$ no sea irreducible, es necesario y suficiente que exista un polinomio $g(x) \in \mathbf{Q}[x]$, de grado 1 o 2, que divida a $f(x)$.

Evidentemente, para que exista un tal polinomio de grado 1, es necesario y suficiente que $-r$ sea de la forma a^4, con $a \in \mathbf{Q}$.

Para que $f(x)$ admita un divisor de grado 2, es necesario y suficiente que existan números racionales p, q, p', q', tales que

$$x^4 + r = (x^2 + px + q)(x^2 + p'x + q'),$$

es decir

$$p + p' = 0, \quad q + q' + pp' = 0, \quad pq' + p'q = 0, \quad qq' = r.$$

Se comprueba inmediatamente que tales números existen si y sólo si r satisface una de las dos condiciones siguientes:

α) $-r$ es el cuadrado de un número racional,

β) $4r$ es la cuarta potencia de un número racional.

En resumen, $f(x)$ es irreducible si r no es de ninguna de las formas $-a^2$, $\frac{a^4}{4}$ $(a \in \mathbf{Q})$, y sólo en este caso.

2.° Suponemos $f(x) = x^4 + r$ irreducible. Si ξ es un cero de $f(x)$ en K, se tiene $K = \mathbf{Q}(\xi)$, y todo elemento de K es de la forma

$$\eta = a + b\xi + c\xi^2 + d\xi^3, \quad a, b, c, d \in \mathbf{Q}, \quad \xi^4 = -r \in \mathbf{Q}.$$

Una extensión cuadrática de $\mathbf{Q}$ contenida en K es necesariamente de la forma $\mathbf{Q}(\eta)$ con $\eta^2 \in \mathbf{Q}$, $\eta \notin \mathbf{Q}$ (ejercicio VII, 4). Ahora,

$$\eta^2 = (a^2 - rc^2 - 2rbd) + 2(ab - rcd)\xi + (b^2 - rd^2 + 2ac)\xi^2 + \\ + 2(ad + bc)\xi^3.$$

El problema propuesto es pues equivalente a la resolución en $\mathbf{Q}$ del sistema

$$\begin{cases} ad + bc = 0, \\ ab - rcd = 0, \\ b^2 - rd^2 + 2ac = 0, \\ b, c, d \text{ no todos son nulos.} \end{cases}$$

Una primera solución resulta tomando $a = b = d = 0$, $c \neq 0$; se obtiene

$$\eta = c\xi^2, \quad \text{de donde} \quad \mathbf{Q}(\eta) = \mathbf{Q}(\xi^2).$$

Se constata fácilmente que si r no es un cuadrado en $\mathbf{Q}$, no hay otra solución. Por el contrario, si $r = s^2$, $s \in \mathbf{Q}$, se encuentran otras dos extensiones cuadráticas,

$$L_1 = \mathbf{Q}(-s\xi + \xi^3), \quad L_2 = \mathbf{Q}(s\xi + \xi^3),$$

además de $L = \mathbf{Q}(\xi^2)$.

L, L_1, L_2 son distintas; se verifica inmediatamente que la intersección de dos cualesquiera de estos cuerpos es **Q**.

7

1.° Según el teorema de Fermat (texto: X, 7), los ceros del polinomio $f_0(x) = x^p - x$ son los elementos del cuerpo primo Π.

Si α es un cero de $f(x) = x^p - x - a \in k[x]$ en un supercuerpo K de k, $f(x)$ se escribe

$$(x^p - \alpha^p) - (x - \alpha) = (x - \alpha)^p - (x - \alpha).$$

Para que β sea un cero de $f(x)$ es necesario y suficiente que $f_0(\beta - \alpha) = 0$, es decir, $\beta - \alpha \in \Pi$. Los ceros de $f(x)$ están todos en K. Éstos son,

$$\alpha,\ \alpha + e,\ \alpha + 2e,\ \ldots,\ \alpha + (p-1)e,$$

donde e indica el elemento unidad de k.

2.° Supongamos que exista algún divisor irreducible $d(x)$ de $f(x)$, de grado $r \geqslant 2$, perteneciente a $k[x]$. Si K es un supercuerpo de k que contiene un cero α de $f(x)$, los polinomios $f(x)$ y $d(x)$ se descomponen en factores de primer grado en $K[x]$, según la cuestión precedente. Al ser distintos los ceros de $f(x)$, hay en K al menos dos ceros de $d(x)$. Se puede suponer que éstos son α y $\alpha + s'e$ (s' entero, $1 \leqslant s' \leqslant p-1$).

Pongamos $s'e = s$ ($s \in \Pi$) y $d_1(x) = d(x + s)$. El polinomio $d_1(x)$ es irreducible en $k[x]$ y admite en K un cero α común con $d(x)$. Cada uno de los polinomios $d(x)$, $d_1(x)$ es divisor del otro, luego $d(x) = d_1(x)$.

Ahora, si $d(x) = x^r + \delta_{r-1}x^{r-1} + \ldots + \delta_0$, se tiene

$$d_1(x) = d(x + s) = (x + s)^r + \delta_{r-1}(x + s)^{r-1} + \ldots + \delta_0.$$

El examen de los términos de grado $r - 1$ conduce a la igualdad $\delta_{r-1} = \delta_{r-1} + rs$, de donde $rs = 0$, y, según la elección de s, $r \equiv 0 \pmod{p}$ y finalmente $r = p$.

3.° Según la cuestión precedente, todo factor irreducible de $f(x)$ es de grado 1 o de grado p. En el primer caso, $f(x)$ tiene p ceros distintos en k. En el segundo caso, $f(x)$ es irreducible en k.

Por tanto, $f(x)$ es irreducible si y sólo si ninguno de sus ceros pertenece a k. Si es así, y si $t \in \Pi$, $t \neq 0$, el polinomio

$$f\left(\frac{x}{t}\right) = \frac{x^p}{t^p} - \frac{x}{t} - a = \frac{1}{t}f_t(x)$$

no tiene ningún cero en k; por consiguiente, es irreducible en k.

4.° Sean $A = k(\alpha)$, $B = k(\beta)$ los cuerpos de descomposición sobre k de los polinomios irreducibles $f(x) = x^p - x - a$, $g(x) = x^p - x - b$.

Supongamos que existe un k-isomorfismo φ de B sobre A.

El elemento $\bar{\beta} = \varphi(\beta)$ es un cero, contenido en A, del polinomio $g(x)$, y existen elementos $c_0, c_1, \ldots, c_{p-1}$ no todos nulos de k, tales que

$$\bar{\beta} = c_0 + c_1\alpha + \ldots + c_{p-1}\alpha^{p-1}.$$

Se tiene entonces

$$\bar{\beta}^p = c_0^p + c_1^p\ \alpha^p + \ldots + c_{p-1}^p\alpha^{p(p-1)},$$

y puesto que $\alpha^p = \alpha + a$,

$$\bar{\beta}^p - \bar{\beta} - b = (c_0^p - c_0 - b) + \sum_{j=1}^{p-1}[c_j^p(\alpha + a)^j - c_j\alpha^j] = 0.$$

Sea c_q el último elemento no nulo de la sucesión $c_0, c_1, \ldots, c_{p-1}$.

Si $q \geqslant 1$ se tiene necesariamente $c_q^p = c_q$, puesto que los α^j forman una base de $k(\alpha)$, luego $c_q \in \Pi$.

Otra condición necesaria es, si $q > 2$,

$$c_{q-1}^p - c_{q-1} - qc_q^p\, a = 0.$$

Pero la ecuación $x^p - x - qc_q^p\, a = 0$ no tiene ninguna raíz en k, a menos que $qc_q^p\, a = 0$, lo que implica $c_q = 0$, contrariamente a la definición de c_q.

Puesto que $q = 0$ implicaría $\beta \in k$, se tiene, en fin, $q = 1$, de donde

$$\bar{\beta} = c_0 + c_1\alpha \quad \text{y} \quad b = c_1 a + c_0^p - c_0 (c_0 \in k,\ c_1 \in \Pi,\ c_1 \neq 0),$$

es decir, $g(x) = f_t(x - c)$, con $t = c_1$, $c = c_0$.

Recíprocamente, supongamos $g(x)$ de la forma $f_t(x - c)$. Si α es un cero de $f(x)$ en un supercuerpo K de k, es $\beta = t\alpha + c$ un cero de $g(x)$ y $k(\alpha) = k(\beta)$.

8

1.° Sea σ un K-automorfismo de $K(x)$. Si se designa por y la imagen de x por σ, se tiene entonces $K(x) = K(y)$ de donde $x \in K(y)$.

Siendo y un elemento de $K(x)$ existen dos polinomios $p(x)$, $q(x) \in K[x]$, tales que $y = \dfrac{p(x)}{q(x)}$. Se pueden suponer $p(x)$ y $q(x)$ primos entre sí.

Siendo x un elemento de $K(y)$ existen elementos $r_0, r_1, \ldots, r_t, s_0, s_1, \ldots, s_t$ de K tales que

$$x(s_0 + s_1 y + \ldots + s_t y^t) = r_0 + r_1 y + \ldots + r_t y^t,$$

y se pueden elegir las notaciones de modo tal que s_0 y r_0 no sean los dos nulos y que s_t y r_t, asimismo, no sean los dos nulos. Deducimos,

$$x \sum_{i=0}^{t} s_i [p(x)]^i [q(x)]^{t-i} = \sum_{i=0}^{t} r_i [p(x)]^i [q(x)]^{t-i},$$

lo que implica, en particular

$$(r_0 - s_0 x)[q(x)]^t \equiv 0 \quad (p(x)),$$
$$(r_t - s_t x)[p(x)]^t \equiv 0 \quad (q(x)).$$

Por ser $p(x)$, $q(x)$ primos entre sí, se ve que $p(x)$ debe ser divisor de $r_0 - s_0 x$ y $q(x)$ debe ser divisor de $r_t - s_t x$. Esto no es posible más que si $p(x)$ y $q(x)$ son de primer grado,

$$y = \frac{ax + b}{cx + d}, \quad \text{con} \quad a, b, c, d \in K, \quad ad - bc \neq 0.$$

Es inmediato que, recíprocamente, la igualdad precedente define un K-automorfismo de $K(x)$.

2.° Si un endomorfismo φ satisface las condiciones impuestas, el transformado por φ de $f(x) \in K(x)$ no puede ser más que $g(x) = f(x^n)$. Luego un tal φ, si existe, es único. Recíprocamente, definiendo φ por $\varphi[f(x)] = f(x^n)$ se verifica que φ es un endomorfismo de $K(x)$ que deja invariable cada elemento de K.

Este endomorfismo no es suprayectivo, pues de serlo existirían elementos $r_0, \ldots, r_m, s_0, \ldots, s_m$ de K no todos nulos, tales que

$$x(s_0 + s_1 x^n + \ldots + s_m x^{mn}) = r_0 + r_1 x^n + \ldots + r_m x^{mn},$$

lo que es imposible, ya que x es una indeterminada.

El endomorfismo en cuestión es inyectivo, pues si $f(x) \in K(x)$, sólo es posible $f(x^n) = 0$ cuando $f(x) = 0$.

9

Se sabe que en un anillo conmutativo de característica p,

$$(a + b)^p = a^p + b^p.$$

Se demuestra fácilmente por recurrencia, que

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

La aplicación σ es, pues, un homomorfismo de grupos aditivos. También es un homomorfismo de anillos, pues

$$\sigma(ab) = (ab)^{p^n} = a^{p^n} b^{p^n} = \sigma(a)\,\sigma(b).$$

Es σ inyectiva, pues $a^{p^n} = b^{p^n}$ implica

$$(a - b)^{p^n} = a^{p^n} - b^{p^n} = 0, \quad \text{y} \quad a = b.$$

Se trata de un Π-homomorfismo, pues si $a \in \Pi$, $\sigma(a) = a^{p^n} = a$.

Si σ es un Π-automorfismo es suprayectivo, y todo elemento de k admite una raíz p-ésima, luego k es perfecto. Recíprocamente, si k es perfecto todo elemento de k admite una raíz p-ésima, luego también una raíz (p^n)-ésima, y σ es un Π-automorfismo.

La ecuación $x^{p^n} - x = 0$ no tiene más que un número finito de soluciones, por lo que σ no puede ser el automorfismo idéntico más que si k es un cuerpo finito. Recíprocamente, si k es finito, y tiene p^q elementos, todos sus elementos son solución de la ecuación $x^{p^q} - x = 0$; σ es el automorfismo idéntico si y sólo si n es múltiplo de q.

10

1.° Designando con x, y, z, s números reales cualesquiera,

$$sE + xJ + yK + zL = \begin{Vmatrix} s + zi & x + yi \\ -x + yi & s - zi \end{Vmatrix}.$$

Se deduce que E, J, K, L son elementos de $\mathbf{C}_2$ linealmente independientes sobre $\mathbf{R}$.

Q es por tanto un espacio vectorial de dimensión cuatro sobre $\mathbf{R}$, y E, J, K, L constituyen una base de él.

E es elemento unidad de $\mathbf{C}_2$ considerado como anillo. Se verifica inmediatamente que

$$J^2 = K^2 = L^2 = -E,\ JK = -KJ = L,\ KL = -LK = J,\ LJ = -JL = K.$$

Se deduce que Q es un subanillo de $\mathbf{C}_2$.

Finalmente, si $M = sE + xJ + yK + zL \neq 0$, su inverso es

$$M^{-1} = (s^2 + x^2 + y^2 + z^2)^{-1} (sE - xJ - yK - zL) \in Q,$$

luego Q es un cuerpo, evidentemente no conmutativo, al que se llama cuerpo de los cuaterniones.

Toda matriz sE pertenece al centro de Q. Recíprocamente, una matriz $sE + xJ + yK + zL$ debe necesariamente conmutar con J, K, L si pertenece al centro, de donde las condiciones necesarias $x = y = z = 0$. El centro es, pues, el conjunto de las matrices sE ($s \in \mathbf{R}$); es, pues, un anillo isomorfo a $\mathbf{R}$.

2.° Si $M = sE + xJ + yK + zL$, se verifica que

$$M^2 = (s^2 - x^2 - y^2 - z^2) E + 2sxJ + 2syK + 2szL.$$

Para que $M^2 + E = 0$ es necesario y suficiente que

$$\begin{cases} s^2 - x^2 - y^2 - z^2 + 1 = 0 \\ sx = sy = sz = 0, \end{cases}$$

sistema equivalente al

$$\begin{cases} s = 0 \\ x^2 + y^2 + z^2 = 1. \end{cases}$$

Existe pues una infinidad de soluciones, que se podría expresar en función de dos parámetros reales.

Del mismo modo, $M^2 - 2\lambda M + \sigma E + \alpha J + \beta K + \gamma L = 0$ equivale al sistema

$$\begin{cases} s^2 - x^2 - y^2 - z^2 - 2\lambda s + \sigma = 0 \\ 2x(s - \lambda) + \alpha = 0, \\ 2y(s - \lambda) + \beta = 0, \\ 2z(s - \lambda) + \gamma = 0. \end{cases}$$

Soluciones para las que sea $s = \lambda$ pueden existir solamente si α, β, γ son los tres nulos. Entonces el sistema se reduce a

$$x^2 + y^2 + z^2 = \sigma - \lambda^2.$$

Entonces, soluciones para las que sea $s = \lambda$, no hay ninguna si $\lambda^2 > \sigma$, hay exactamente una si $\lambda^2 = \sigma$, y hay una infinidad si $\lambda^2 < \sigma$.

Supongamos ahora $\alpha^2 + \beta^2 + \gamma^2 \neq 0$. Es cómodo utilizar la incógnita auxiliar $S = s - \lambda$. Se comprueba fácilmente que

$$s = S + \lambda, \quad x = -\frac{\alpha}{2S}, \quad y = -\frac{\beta}{2S}, \quad z = -\frac{\gamma}{2S}$$

es una solución si y sólo si

$$S^2 - \frac{k^2}{S^2} + \mu = 0,$$

donde hemos puesto $\alpha^2 + \beta^2 + \gamma^2 = 4k^2$, $\sigma - \lambda^2 = \mu$.

La ecuación bicuadrada en S que se deduce, admite dos raíces opuestas. Luego, la ecuación estudiada admite dos soluciones.

Finalmente, $M^2 + JM + E - L = 0$ equivale a

$$\begin{cases} s^2 - x^2 - y^2 - z^2 - x + 1 = 0, \\ (2x + 1)s = 0, \\ 2ys - z = 0, \\ 2zs + y - 1 = 0. \end{cases}$$

Este sistema no admite otras soluciones que

$$s = 0,\ x = 0, \quad y = 1,\ z = 0,$$
$$s = 0,\ x = -1,\ y = 1,\ z = 0,$$

lo que lleva a las soluciones $M = K$ y $M = K - J$.

11

1.° Investiguemos las condiciones necesarias. Supongamos

$$x^2 + ax + b = (x - c)(x - d) = (x - d')(x - c), \quad (d, d' \in K).$$

Entonces $-a = c + d = d' + e$, de donde $d = d'$ y $b = cd = dc$.

No puede ser c nulo, y $d = bc^{-1} = c^{-1}b$ muestra que b conmuta con c^{-1}, luego también con c.

$d = -a - c$ implica $b = -(a + c)c = -c(a + c)$, es decir

$$c^2 + ac + b = c^2 + ca + b = 0,$$

y c conmuta también con a.

Recíprocamente, supongamos que $f(c) = 0$, es decir, $c^2 + ac + b = 0$, y $ac = ca$. Entonces

$$f(x) = (x^2 + ax + b) - (c^2 + ac + b) = (x + c)(x - c) + a(x - c)$$

es divisible a la derecha por $x - c$. También lo es a la izquierda, pues

$$(x - c)(x + c + a) = x^2 - c^2 + ax - ca = x^2 + ax + b = f(x).$$

Si b es un elemento no nulo del centro de K, un elemento c tal que

$$c^2 + ac + b = 0$$

no puede ser nulo, de donde

$$c + a + bc^{-1} = 0,$$

lo que implica

$$c^2 + ca + cbc^{-1} = c^2 + ca + b = 0 \quad \text{y} \quad ca = ac.$$

En este caso todo divisor a la derecha de la forma $x - c$ es también a la izquierda de $f(x) = x^2 + ax + b$.

2.° Tomemos para cuerpo K el cuerpo Q del ejercicio precedente, y

$$f(x) = x^2 + Jx + E - L.$$

Los únicos elementos M de Q tales que $f(M) = 0$ son K y $K - J$, que no conmutan con J. No existe, pues, ningún divisor a la derecha y a la izquierda de la forma $x - M$.

12

Supongamos que A sea un cuerpo. Sea b un elemento no nulo de B; satisface b una igualdad de la forma

$$b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0 = 0, \quad (a_j \in A).$$

Si se elige n mínimo, es $a_0 \neq 0$. En efecto, si a_0 fuese nulo, satisfaría b una igualdad de la forma $bP(b) = 0$, de donde $P(b) = 0$, puesto que el anillo B es íntegro, siendo $P(x) \in A[x]$ un polinomio de grado $n - 1$.

b tiene inverso, puesto que

$$-a_0^{-1}(b^{n-1} + a_{n-1}\,b^{n-2} + \ldots + a_2\,b + a_1)\,b = e,$$

lo que demuestra que B es un cuerpo.

Supongamos que B sea un cuerpo y sea c un elemento no nulo de A. Éste admite un inverso c^{-1} en B, y c^{-1} satisface una igualdad de la forma

$$(c^{-1})^n + a_{n-1}(c^{-1})^{n-1} + \ldots + a_1\,c^{-1} + a_0 = 0, \qquad (a_j \in A),$$

de donde

$$c^{-1} = -(a_{n-1} + a_{n-2}\,c + \ldots + a_1\,c^{n-2} + a_0\,c^{n-1}) \in A,$$

lo que demuestra que A es un cuerpo.

13

Sean A un anillo factorial, K el cuerpo de cocientes de A, $\alpha = \dfrac{c}{d}$ un elemento de K entero algebraico sobre A. Los elementos c y $d \neq 0$ de A se pueden suponer primos entre sí. Existen en A elementos $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$, tales que

$$\alpha^n + a_{n-1}\,\alpha^{n-1} + \ldots + a_1\,\alpha + a_0 = 0.$$

de donde

$$c^n + a_{n-1}\,c^{n-1}\,d + \ldots + a_1\,cd^{n-1} + a_0\,d^n = 0.$$

Si d no fuese una unidad de A esta igualdad implicaría una contradicción, puesto que d dividiría a c^n, mientras que al ser primo con c lo es también con c^n.

Por tanto, d es una unidad y $\alpha \in A$.

14

Si Π es de característica p, p no divide a $2n+1$ ni a $4n+2$, y se pueden utilizar las propiedades del cuerpo de las raíces m-ésimas de la unidad sobre Π (texto: X, 6). Es claro que $\beta = -\alpha^n$ implica $\Pi(\beta) \subseteq \Pi(\alpha)$ y

$$\beta^{4n+2} = (-1)^{4n+2}\,\alpha^{2n(2n+1)} = e.$$

Por tanto β es una raíz $(4n+2)$-ésima de la unidad. Para demostrar que se trata de una raíz primitiva, basta demostrar que engendra un grupo multiplicativo de orden $4n+2$.

Supongamos pues $\beta^r = e$, con r entero natural, es decir

$$(-1)^r \alpha^{rn} = e.$$

Ninguna potencia de α es igual a $-e$, luego r es par, $r = 2s$. La igualdad $\alpha^{2sn} = e$ implica entonces, puesto que α es raíz $(2n+1)$-ésima primitiva de e, que $2n+1$ divida a $2sn$, luego que divida a s. Luego r es múltiplo de $4n+2$, lo que termina la demostración.

Toda raíz $(2n+1)$-ésima de e, es raíz $(4n+2)$-ésima, por lo que α es una potencia de la raíz primitiva β, de donde $\Pi(\alpha) \subseteq \Pi(\beta)$, y de aquí la igualdad $\Pi(\alpha) = \Pi(\beta)$.

15

Sean α y β dos elementos en K tales que $\alpha^2 = u$, $\beta^2 = v$; como u y v no son cuadrados de elementos de $k = \Pi(u, v)$ se tiene, poniendo $A = k(\alpha)$, $B = k(\beta)$,

$$(A : k) = (B : k) = 2.$$

A y B son distintos, pues si, por ejemplo, β perteneciese a A, existirían p y q elementos de k tales que $\beta = p + q\alpha$, de donde

$$v = \beta^2 = p^2 + q^2\alpha^2 = p^2 + q^2 u,$$

y existirían polinomios $f(u, v)$, $g(u, v)$, $h(u, v) \in \Pi[u, v]$ tales que

$$f^2(u, v) + ug^2(u, v) + vh^2(u, v) = 0, f(u, v) \neq 0.$$

Ahora, cuando la característica es 2, el cuadrado de un polinomio sólo comporta monomios cuyo exponente es par, por lo que tal igualdad es imposible.

Según el ejercicio VII, 2 el menor subcuerpo de K que contiene a A y B, es decir, el propio K, es de grado 4 sobre k; y una base del k-espacio vectorial K es $\{e, \alpha, \beta, \alpha\beta\}$, designando con e el elemento unidad de Π.

Si ξ es un elemento cualquiera de K, es de la forma

$$\xi = x + y\alpha + z\beta + t\alpha\beta \quad (x, y, z, t \in k),$$

de donde

$$\xi^2 = x^2 + y^2 u + z^2 v + t^2 uv \in k.$$

Se tiene pues, si $\xi \notin k$, $(k(\xi) : k) = 2$, luego $k(\xi) \neq K$. Por tanto K no admite ningún elemento primitivo.

16

Puesto que existe un entero n tal que $a^n = a$, a es algebraico sobre el cuerpo primo Π. Por consiguiente $k = \Pi(a)$ es un cuerpo finito, cuyos N elementos son raíces de la ecuación $x^N - x = 0$. Se tiene pues, en el anillo $k[x]$ la factorización

$$x^N - x = \prod_{b \in k} (x - b).$$

1.° Designemos por γ y δ las aplicaciones de K en K definidas por

$$\gamma(y) = ay, \quad \delta(y) = ya.$$

Puesto que a conmuta con todo elemento de k, γ y δ son endomorfismos del espacio vectorial K, y $\varphi = \delta - \gamma \in H$.

Además, γ y δ conmutan, y se puede calcular φ^p por la fórmula del binomio. Como la característica de k es p, la de H es también p, y $\varphi^p = \delta^p - \gamma^p$. Del mismo modo, $\varphi^N = \delta^N - \gamma^N$.

$\delta^N(y) = a^N y = ay = \delta(y)$ implica $\delta^N = \delta$. También $\gamma^N = \gamma$. Se tiene pues $\varphi^N = \varphi$. Por consiguiente, resulta que

$$\varphi^N - \varphi = \prod_{b \in k} (\varphi - b\varepsilon) = \omega.$$

2.° Por hipótesis, φ no es nulo. Pongamos $\psi = \varphi^{N-1} - \varepsilon$. Existe pues $y_0 \neq 0$ en K, tal que $\psi(y_0) = 0$. Ahora bien, ψ que es el producto de los $\varphi - b\varepsilon$ cuando b recorre $k^* = k - \{0\}$, no es pues inyectivo, y existe al menos un $b_0 \in k^*$ tal que $\varphi - b_0 \varepsilon$ no sea inyectivo.

Existe pues un $c \in K$ tal que $c \neq 0$, $\varphi(c) = b_0 c$, lo que implica

$$cac^{-1} = a + b_0.$$

k^* es un grupo cíclico. Si h es el menor entero positivo tal que $a^h = e$, se tiene también $(cac^{-1})^h = e$, luego cac^{-1} es una potencia de a, lo que concluye la demostración.

17

Sea e el elemento unidad de K. Si K es de característica nula los elementos $ne (n \in \mathbf{Z})$ son todos distintos. Un elemento tal no puede ser de orden multiplicativo finito más que para los valores 0, 1, — 1, de n. Luego si K^* es un grupo con torsión, la característica de K es necesariamente un número primo p.

Supongamos que existe un elemento a de K que no pertenece al centro de K. Entonces, según el ejercicio precedente, existirán también un elemento c no nulo de K y un entero s, tales que

$$cac^{-1} = a^s \neq a.$$

Los supuestos a y c engendran en K^* un grupo finito, en que todo elemento puede ponerse en la forma $a^\lambda c^\mu$, donde λ y μ son enteros tales que $1 \leqslant \lambda \leqslant \alpha$, $1 \leqslant \mu \leqslant \gamma$, designando por α y γ los órdenes de a y c.

El anillo engendrado por a, c y los elementos del cuerpo primo de K es entonces un anillo íntegro (como contenido en K) y finito. Es pues un cuerpo conmutativo, según el teorema de Wedderburn, lo que contradice que

$$cac^{-1} \neq a.$$

No hay, pues, en K elementos que no sean del centro de K, es decir, K es conmutativo.

18

Sea K un cuerpo finito del que e es elemento unidad. Por consiguiente K es conmutativo (texto: X, 9).

Sean $a_1, a_2, \ldots, a_n$ los elementos de K. El polinomio

$$f(x) = e + (x - a_1)(x - a_2) \ldots (x - a_n) \qquad \in K[x]$$

satisface la condición $f(a_i) = e$, $(1 < i < n)$, luego no puede tener ningún cero en K.

19

1.° Se verifica fácilmente que la relación así definida en L es una relación de orden. Sea $\{(L_\lambda, \varphi_\lambda)\}_{\lambda \in A}$ una cadena extraída de $\mathcal{L}$. El conjunto $L^* = \bigcup_{\lambda \in A} L_\lambda$ es un subgrupo aditivo de E, pues el conjunto de subgrupos

aditivos de E es $\cup$-inductivo. Si a y $b \neq 0$ son dos elementos de L^*, existen índices $\lambda, \mu \in \Lambda$ tales que $a \in L_\lambda$, $b \in L_\mu$. Si, por ejemplo, $L_\lambda \subseteq L_\mu$, $ab^{-1} \in L_\mu \subseteq$ $\subseteq L^*$, y L^* es un cuerpo.

Para todo $x \in L^*$ existen $\lambda \in \Lambda$ tales que $x \in L_\lambda$, y $\varphi_\lambda(x)$ es independiente del índice λ, puesto que los L_λ forman una cadena; poniendo $\varphi^*(x) = \varphi_\lambda(x)$ se define pues una aplicación de L^* en E. Se verifica inmediatamente que φ^* es un K-homomorfismo inyectivo. Por tanto $\mathcal{L}$ es un conjunto inductivo.

Todo elemento (L, φ) de $\mathcal{L}$ está pues contenido en un elemento maximal (L_0, φ_0). Es suficiente demostrar que $L_0 = E$ y $\varphi_0 \in G$.

Pongamos $\varphi_0(L_0) = L_1$ y supongamos $L_0 \neq E$. Sea $c \in E$, $c \notin L_0$. Como c es algebraico sobre K lo es también sobre L_0. Sea

$$g(x) = \sum_{i=0}^{n} u_i x^i \in L_0[x]$$

su polinomio característico. El polinomio

$$h(x) = \sum_{i=0}^{n} v_i x^i, \quad \text{donde} \quad v_i = \varphi_0(u_i),$$

es irreducible sobre L_1, puesto que $g(x)$ es irreducible sobre L_0. Tal polinomio admite en E un cero $d \notin L_1$. Se sabe que existe entonces un K-isomorfismo φ_0' de $L_0(c)$ sobre $L_1(d)$ que prolonga φ_0. Pero entonces $(L_0(c), \varphi_0')$ mayora estrictamente (L_0, φ_0) lo que contradice la definición de (L_0, φ_0). Se tiene, pues, $L_0 = E$. De modo análogo se verifica que $L_1 = E$. Resulta efectivamente $\varphi_0 \in G$.

2.° Si a y b tienen el mismo polinomio característico, existe un K-isomorfismo φ de $K(a)$ sobre $K(b)$ tal que $b = \varphi(a)$. Según lo 1.°, φ puede prolongarse por un K-automorfismo σ de E.

Recíprocamente, si $\sigma(a) = b$, con $\sigma \in G$, y si a y b tienen por respectivos polinomios característicos $f(x)$ y $g(x)$, se tienen los isomorfismos siguientes

$$K[x]/(f(x)) \simeq K(a) \simeq K(b) \simeq K[x]/(g(x)),$$

lo que implica $f(x) = g(x)$.

20

1.° Supongamos $a^{p^m} \in K$, y sea φ un elemento de G. La condición $a^{p^m} = \varphi(a^{p^m})$ implica $[\varphi(a) - a]^{p^m} = 0$, o sea, $\varphi(a) = a$, y $a \in \overline{K}$.

Recíprocamente, supongamos $a \in \overline{K}$, $a \notin K$. Y con a algebraico sobre K, sea $f(x)$ su polinomio característico. Para todo cero b de $f(x)$ en E existe,

según el ejercicio precedente, un $\sigma \in G$ tal que $b = \sigma(a)$. Puesto que $a \in \overline{K}$, $\sigma(a) = a$, y todos los ceros de $f(x)$ quedan superpuestos. Como el grado de $f(x)$ es superior a 1, se tiene $f(x) \in K[x^p]$. Más precisamente, existe un entero natural h tal que

$$f(x) \in K[x^{p^h}], \quad f(x) \notin K[x^{p^{h+1}}].$$

Existe pues un polinomio irreducible $g(x) \in K[x]$ tal que

$$f(x) = g(x^{p^h}), \quad g(x) \notin K[x^p].$$

En particular, $g(x)$ es separable. Pero si c es uno de sus ceros, y d es una raíz de la ecuación $x^{p^h} = c$, se tiene $f(d) = g(c) = 0$, luego $d = a$ y $c = a^{p^h}$. Por consiguiente $g(x)$ es de primer grado, $g(x) = x - c$, y $c = a^{p^h} \in K$.

2.° La aplicación τ de E en E, definida por $\tau(a) = a^p$, es un automorfismo de E, pues E es algebraicamente cerrado, luego perfecto (ejercicio VII, 9).

Si K es perfecto, $\tau(K) = K$. Se deduce, para todo entero m, $K = \tau^{-m}(K)$. Según lo visto 1.°, $\overline{K}$ es la unión de todos los $\tau^{-m}(K)$, y $\overline{K} = K$.

Recíprocamente, si $K = \overline{K}$, todo elemento r de K admite en E una raíz p-ésima r'. Por definición de $\overline{K}$, $r' \in \overline{K}$, luego $r' \in K$, y K es perfecto (X, 4, teorema 5 *a*).

E, clausura algebraica de K, es también clausura algebraica de $\overline{K}$. Todo $\overline{K}$-automorfismo de E es un K-automorfismo de E. Por consiguiente, $\overline{K}$ es también el cuerpo fijo de $G_{E:\overline{K}}$, grupo de los $\overline{K}$-automorfismos de E. Según lo precedente, K es por tanto un subcuerpo perfecto de E.

Finalmente, si L es un subcuerpo perfecto de E conteniendo a K, es claro que $\overline{K} \subseteq \overline{L} = L$, siendo $\overline{L}$ el cuerpo fijo del grupo $G_{E:L}$ de los L-automorfismos de E.

3.° Si $\overline{K} \neq K$, K no es perfecto, y K está contenido estrictamente en $\tau^{-1}(K)$. Resulta, para todo m natural, que $\tau^{-m}(K) = L_m$ está contenido estrictamente en $\tau^{-(m+1)}(K) = L_{m+1}$.

Puesto que $(L_{m+1} : L_m) \geq p$, $(\overline{K} : K)$ no puede ser finito.

21

La resolución del sistema de ecuaciones

$$\begin{cases} x^2 + y^2 - 2x = 0, \\ x^2 - xy = 0, \end{cases}$$

muestra que a admite dos ceros sobre **C** (y también sobre **Q** o **R**), que son (0, 0) y (1, 1).

El polinomio $f(x, y) = x - y$ toma el valor cero para cada uno de estos ceros. Por consiguiente, según el teorema de Hilbert (texto: X, 11) existe un exponente ρ tal que $(x - y)^\rho \in \mathfrak{a}$, es decir, que existen dos polinomios $g(x, y)$, $h(x, y) \in \mathbf{Q}[x, y]$ tales que

$$(x - y)^\rho = g(x, y)\,(x^2 + y^2 - 2x) + h(x, y)\,(x^2 - xy).$$

Haciendo $x = 0$ se ve que ρ debe ser necesariamente al menos igual a 2, lo que implica $g(0, 0) = 0$. El segundo miembro no puede contener un monomio en y^2 no nulo, luego $\rho > 3$.

Buscando $g(x, y)$, $h(x, y)$ por el método de los coeficientes indeterminados, se ve que el valor $\rho = 3$ conviene, y que es

$$(x - y)^3 = (x - y)\,(x^2 + y^2 - 2x) + 2(1 - y)\,(x^2 - xy).$$

22

De las propiedades recordadas en el enunciado resulta que no existe ninguna verdadera extensión de grado impar de **R**, ni ninguna extensión de grado 2 de **C**. En efecto, siendo **R** y **C** de característica 0, tales extensiones serían simples (teorema del elemento primitivo) y su existencia contradiría las propiedades citadas.

Sea $f(x)$ un polinomio de coeficientes complejos, supuesto irreducible. Si N es un cuerpo de descomposición sobre **C** de dicho polinomio, pongamos $(N : \mathbf{C}) = 2^r m$, siendo m entero impar. Se tiene entonces $(N : \mathbf{R} = 2^{r+1} m$, y N es una extensión galoisiana de **R** y de **C**.

El grupo de Galois $G_{N:\mathbf{R}}$ admite, según el teorema de Sylow, un subgrupo Γ de orden 2^{r+1}, cuyo cuerpo fijo K verifica $(K : \mathbf{R}) = m$. Esto no es posible a menos que $m = 1$, luego $(N : \mathbf{C}) = 2^r$.

Si r fuese por lo menos igual a 1, el grupo de Galois $G_{N:\mathbf{C}}$ admitiría (teorema de Sylow) un subgrupo Γ' de orden 2^{r-1} cuyo cuerpo fijo K' sería tal que $(K' : \mathbf{C}) = 2$. Esto es imposible, luego $r = 0$, y $N = \mathbf{C}$.

23

Se ha visto en el ejercicio VII, 7 que todo cuerpo de ruptura de $f(x)$ es cuerpo de descomposición. Si K es un cuerpo tal, K es extensión finita, normal y separable de k, y el grupo de Galois $G = G_{K:k}$ es de orden p, luego cíclico.

Es claro que si α es un cero de $f(x)$ en K, existe un k-automorfismo único σ de K tal que $\sigma(\alpha) = \alpha + e$, y que σ es un generador de G.

24

1.° Todo elemento de K es de la forma

$$a = c_0 + c_1 \xi + \ldots + c_{p-1} \xi^{p-1}, \quad c_j \in k,$$

puesto que K es una extensión de Galois de k, con $(K : k) = p$.

Si $\xi_j = \xi_{j'}$ para $0 \leqslant j \leqslant j' \leqslant p - 1$, se tiene $\sigma^j(\xi) = \sigma^{j'}(\xi)$; de donde $\sigma^{j'-j}(\xi) = \xi$, luego, para todo $a \in K$, $\sigma^{j-j'}(a) = a$. Esto implica $j' \equiv j(p)$, es decir, $j' = j$.

2.° De la cuestión precedente resulta que el determinante de Vandermonde de los ξ_j no es nulo:

$$\begin{vmatrix} e & \xi_0 & \xi_0^2 & \ldots & \xi_0^{p-1} \\ e & \xi_1 & \xi_1^2 & \ldots & \xi_1^{p-1} \\ e & \xi_2 & \xi_2^2 & \ldots & \xi_2^{p-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ e & \xi_{p-1} & \xi_{p-1}^2 & \ldots & \xi_{p-1}^{p-1} \end{vmatrix} = \begin{vmatrix} 0 & S_1 & S_2 & \ldots & S_{p-1} \\ e & \xi_1 & \xi_1^2 & \ldots & \xi_1^{p-1} \\ e & \xi_2 & \xi_2^2 & \ldots & \xi_2^{p-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ e & \xi_{p-1} & \xi_{p-1}^2 & \ldots & \xi_{p-1}^{p-1} \end{vmatrix} \neq 0$$

Luego los S_n no son todos nulos.

Además, $\sigma(\xi_j) = \xi_{j+1}$ y $\xi_p = \xi_0$ implican $\sigma(S_n) = S_n$.

3.° Transformando por σ la igualdad que define η y señalando que

$$j\xi_{j+1}^{n_0} = (j+1)\,\xi_{j+1}^{n_0} - \xi_{j+1}^{n_0},$$

se obtiene

$$\sigma(S_{n_0}\,\eta) = S_{n_0}\,\sigma(\eta) = -\sum_{j=0}^{p-1} j\xi_{j+1}^{n_0} = S_{n_0}(\eta + e),$$

es decir, $\sigma(\eta) = \eta + e$. En particular $\eta \notin k$.

Se deduce

$$\sigma(\eta^p - \eta) = (\eta + e)^p - (\eta + e) = \eta^p - \eta,$$

luego $\eta^p - \eta \in k$.

Como $\eta \in K = k(\xi)$, $k(\eta) \subseteq k(\xi)$.

Es $(k(\eta) : k) = p$, pues, según el ejercicio VII, 7 el polinomio

$$f(x) = x^p - x - (\eta^p - \eta)$$

es irreducible en $k[x]$. Por consiguiente, $K = k(\eta) = k(\xi)$ es cuerpo de descomposición de $f(x)$.

25

1.° Designando por ε, α, β, γ los k-automorfismos de L definidos por

$$\varepsilon(x) = x, \quad \alpha(x) = e - \frac{e}{x}, \quad \beta(x) = \frac{e}{e - x}, \quad \gamma(x) = \frac{x}{x - e},$$

se ve fácilmente que $G = \{\varepsilon, \sigma, \tau, \alpha, \beta, \gamma\}$, siendo la tabla de multiplicar

	ε	σ	τ	α	β	γ
ε	ε	σ	τ	α	β	γ
σ	σ	ε	α	τ	γ	β
τ	τ	β	ε	γ	σ	α
α	α	γ	σ	β	ε	γ
β	β	τ	γ	ε	α	σ
γ	γ	α	β	σ	τ	ε

2.° Sea F el cuerpo fijo de G. Se comprueba inmediatamente que $\sigma(y) = y$, $\tau(y) = y$, lo que implica $K = k(y) \subseteq F$. Luego σ y τ y, por tanto, todos los elementos de G, son K-automorfismos de L.

El elemento x satisface la ecuación de sexto grado

$$(x^2 - x - e)^3 - x^2(x - e)^2 y = 0,$$

de coeficientes en K. Se tiene pues $(L : K) \leq 6$.

Como el conjunto de automorfismos considerado es un grupo, y F es su cuerpo fijo, resulta $(L, F) = 6$ (texto: X, 12, teorema 4). Puesto que $k \subset K \subseteq F \subset L$, se tiene en efecto $K = F$.

26

La ecuación $f(x) = 0$ no tiene raíces múltiples. En efecto, $f'(x) = nx^{n-1}$ no es nulo, puesto que, si $p \neq 0$, p no es divisor de n. Las raíces de $f(x) = 0$ son, pues, ξ, ξ^2, ..., ξ^{n-1}, $\xi^n = e$. Todo K-automorfismo σ de L transforma ξ en otra raíz primitiva, luego la transforma en un ξ^s con s entero primo con n.

Si $\tau \in G$, con $\tau(\xi) = \xi^t$, t entero primo con n, se tiene

$$(\tau \circ \sigma)(\xi) = \tau(\xi^s) = \xi^{st} = (\sigma \circ \tau)(\xi).$$

Resulta que G es conmutativo. Además, la aplicación $\sigma \to \bar{s}$, donde $\bar{s}$ es la clase de s módulo n, es un homomorfismo del grupo G en el grupo de las unidades de $\mathbf{Z}/(n)$. Como un K-automorfismo de L está determinado por su efecto sobre ξ, este homomorfismo de grupos es inyectivo. También es suprayectivo puesto que G es un grupo finito.

Observación: Si n es un número primo, $\mathbf{Z}/(n)$ es un cuerpo, su grupo multiplicativo es cíclico y G es cíclico.

27

1.° Si, para todo $\sigma \in G$, $x_\sigma = a^{-1}\sigma(a)$, es evidente que

$$x_\sigma \sigma(x_\tau) = a^{-1}\sigma(a)\,\sigma[a^{-1}\tau(a)] = a^{-1}(\sigma \circ \tau)(a) = x_{\sigma\circ\tau}.$$

Recíprocamente, supongamos que $\{x_\sigma\}_{\sigma \in G}$ constituye una solución del problema de Nœther. Los automorfismos $\sigma \in G$ son distintos, luego son linealmente independientes sobre L (texto: X, 12, teorema 3). Existe pues $b \in L$ tal que

$$c = \sum_{\theta \in G} x_\theta\, \theta(b) \neq 0.$$

Aplicando σ y multiplicando por x_σ se obtiene

$$x_\sigma \sigma(c) = \sum_{\theta \in G} x_\sigma \sigma(x_\theta)(\sigma \circ \theta)(b) = \sum_{\theta \in G} x_{\sigma\circ\theta}(\sigma \circ \theta)(b).$$

Pero $\sigma \circ \theta$ recorre G cuando θ recorre G, de donde

$$x_\sigma \sigma(c) = \sum_{\theta \in G} x_\theta\, \theta(b) = c\,.$$

Es pues suficiente poner $a = c^{-1}$ para obtener $x_\sigma = a^{-1}\sigma(a)$.

2.° Si todos los x_σ son de K, es $\sigma(x_\tau) = x_\tau$ para todo índice τ, y $x_\sigma\, x_\tau = x_{\sigma\circ\tau}$. La aplicación f de G en K definida por $f(\sigma) = x_\sigma$, es pues un homomorfismo de grupos.

Recíprocamente, si f es un tal homomorfismo, y si $f(\sigma) = x_\sigma$ para todo $\sigma \in G$, se tiene

$$x_\sigma\, \sigma(x_\tau) = x_\sigma\, x_\tau = f(\sigma) f(\tau) = f(\sigma \circ \tau) = x_{\sigma\circ\tau}.$$

Es evidente que dos homomorfismos distintos proporcionarán dos soluciones distintas del problema de Nœther, y recíprocamente.

En fin, si r es el m.c.m. de los órdenes de los $\sigma \in G$, y si $x_\sigma = f(\sigma) = a^{-1}\,\sigma(a)$, se tiene

$$a^{-r}\,\sigma(a^r) = x_\sigma^r = f(\sigma^r) = f(\varepsilon) = e$$

(siendo ε y e los elementos unidad de G y de L), de donde $\sigma(a^r) = a^r$ y $a^r \in K$.

28

Se sabe que $f(x)$ es de grado n, y admite en L los n ceros distintos $\alpha_i = \varphi_i(\alpha)$. De otra parte, para todo

$$h(x) = \sum_{l=0}^{r} c_l\, x^l \in L[x],$$

$$\Phi_i[h(x)] = \sum_{l=0}^{r} \varphi_i(c_l)\, x^l.$$

Resulta así que $g_i(x)$ no es otro que

$$\frac{f(x)}{(x - \alpha_i) f'(\alpha_i)},$$

y que $g_i(\alpha_j) = \delta_{ij}$ (símbolo de Kronecker).

1.° $e - \sum_{i=1}^{n} g_i(x)$ es un polinomio de $L[x]$ de grado $n - 1$ a lo sumo. Como toma el valor 0 para los n valores distintos $x = \alpha_j$, es el polinomio nulo.

2.° Del mismo modo, los polinomios $g_i(x)\, g_j(x)$ y $[g_i(x)]^2 - g_i(x)$ toman el valor cero para $x = \alpha_l$ $(1 \leq l \leq n)$. Son, pues, divisibles por $f(x)$.

Observación: Todos los α_i tienen las mismas propiedades, luego todo lo que precede subsiste si se reemplaza $g(x)$ por $g_i(x)$.

3.° Si M' es la traspuesta de M, se sabe que $[D(x)]^2 = \det(MM')$,

$$MM' = \| v_{ij} \|, \quad v_{ij} = \sum_{l=1}^{n} u_{il}\, u_{jl}.$$

Si $i \neq j$

$$v_{ij} = \sum_{l=1}^{n} \Phi_i[g_l(x)]\Phi_j[g_l(x)].$$

Cada uno de los términos de la suma es divisible por $f(x)$, según la observación al fin de lo 2.°, luego también v_{ij}.

Por análoga razón,

$$v_{ii} = \sum_{l=1}^{n} \Phi_i[g_l^2(x)]$$

tiene el mismo resto módulo $f(x)$ que

$$\sum_{l=1}^{n} \Phi_i[g_l(x)] = e.$$

Por tanto, $f(x)$ es divisor de $v_{ii} - e$.

El desarrollo del determinante demuestra ahora que $f(x)$ es divisor de $[D(x)]^2 - e$.

Para $x = a$ se tiene pues $[D(a)]^2 = e$, luego $D(a) \neq 0$, lo que prueba que $D(x)$ no es el polinomio nulo.

4.° $D(x)$ sólo tiene un número finito de ceros en K; siendo K infinito existe un $a \in K$ tal que $D(a) \neq 0$. Poniendo $b = g(a)$, el determinante de los $(\varphi_i \circ \varphi_j)(b)$ no será nulo.

Si los $\varphi_i(b)$ no fuesen independientes sobre K, existirían $x_i \in K$, no todos nulos, tales que

$$\sum_{j=1}^{n} x_j\, \varphi_j(b) = 0,$$

de donde, aplicando φ_i, puesto que $\varphi_i(x_i) = x_j$,

$$\sum_{j=1}^{n} x_j(\varphi_i \circ \varphi_j)(b) = 0, \quad (i, j = 1, 2, \ldots, n),$$

lo que contradice la hipótesis hecha, pues se trata de un sistema de Cramer. Los $\varphi_i(b)$ son pues independientes y constituyen una base de L.

29

L es una extensión finita de Galois de $\mathbf{Q}$. Según el ejercicio VII, 26, $G_{L:\mathbf{Q}}$ es isomorfo al grupo multiplicativo $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ del cuerpo $\mathbf{Z}/(7)$.

Existen pues dos subgrupos propios, evidentemente cíclicos

$$\Gamma_2 = \{\bar{1}, \bar{2}, \bar{4}\}, \quad \Gamma_6 = \{\bar{1}, \bar{6}\}.$$

L es pues una extensión de grado 6 de $\mathbf{Q}$, y existen dos subcuerpos intermedios, L_2 y L_6.

L_2 es el cuerpo fijo del subgrupo cíclico de orden 3 de $G_{L:\mathbf{Q}}$. Es pues una extensión cuadrática de $\mathbf{Q}$, ya que $(L : \mathbf{Q})$ es igual al índice de ese subgrupo. L_2 contiene al elemento $\eta = \xi + \xi^2 + \xi^4$ que satisface la ecuación $x^2 + x + 2 = 0$, irreducible sobre $\mathbf{Q}$. Luego

$$L_2 = \mathbf{Q}(\eta) = \mathbf{Q}(i\sqrt{7}),$$

pues las raíces de esta ecuación son $\frac{1}{2}(-1 + i\sqrt{7})$ y $\frac{1}{2}(-1 - i\sqrt{7})$.

L_6 es el cuerpo fijo del subgrupo cíclico de orden 2 de $G_{L:\mathbf{Q}}$. Es pues una extensión de grado 3 de $\mathbf{Q}$, que contiene al elemento $\zeta = \xi^2 + \xi^5$, y al elemento $\xi^3 + \xi^4 = \zeta^2 - 2$, luego también a ζ^2. En efecto, ζ es invariante en el $\mathbf{Q}$-automorfismo de L definido por $\xi \to \xi^6$. Se verifica fácilmente que ζ es raíz de la ecuación $x^3 + x^2 - 2x - 1 = 0$, y que esta ecuación es irreducible sobre $\mathbf{Q}$. Por tanto, $L_6 = \mathbf{Q}(\zeta)$.

Tomando, por ejemplo, $\xi = \cos\frac{2\pi}{7} + i \operatorname{sen}\frac{2\pi}{7}$, se obtiene

$$\zeta = -2\cos\frac{3\pi}{7}, \quad \text{de donde} \quad L_6 = \mathbf{Q}\left(\cos\frac{3\pi}{7}\right).$$

30

L es una extensión finita de Galois de $\mathbf{Q}$. Según el ejercicio VII, 26, $G = G_{L:\mathbf{Q}}$ es isomorfo al grupo de las unidades $\{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$ del anillo $\mathbf{Z}/(12)$. Existen pues en G tres subgrupos propios, cíclicos de orden 2, cuyas imágenes en $\mathbf{Z}/(12)$ son

$$\Gamma_5 = \{\bar{1}, \bar{5}\}, \quad \Gamma_7 = \{\bar{1}, \bar{7}\}, \quad \Gamma_{11} = \{\bar{1}, \overline{11}\}.$$

L es pues una extensión de grado 4 de $\mathbf{Q}$, y existen tres cuerpos intermedios, extensiones cuadráticas de $\mathbf{Q}$.

Se puede tomar $\xi = \frac{1}{2}(i + \sqrt{3})$. Uno de los cuerpos intermedios es

$$\mathbf{Q}(\xi + \xi^5) = \mathbf{Q}(i),$$

otro

$$\mathbf{Q}(\xi + \xi^{11}) = \mathbf{Q}(\sqrt{3}).$$

y finalmente, según el ejercicio VII, 5, el tercero es $\mathbf{Q}(i\sqrt{3})$.

31

1.° Todo factor irreducible $g(x)$ de $f(x)$ divide uno de los $f_i(x) = x^n - a_i$. Puesto que $f_i'(x) = nx^{n-1} \neq 0$ (al no ser n múltiplo de la característica de K), $f_i(x)$ no puede tener ceros múltiples, y, por tanto, tampoco $g(x)$. Luego $f(x)$ es un polinomio separable y L es extensión de Galois de K.

2.° Sea $\xi \in K$ una raíz primitiva n-ésima de e. Si α_i es una raíz de $f_i(x) = 0$, las raíces de $f(x) = 0$ son los $\xi^j \alpha_i$ $(1 \leq i \leq r,\ 0 \leq j < n)$. Luego

$$L = K(\alpha_1, \ldots, \alpha_r).$$

Sean σ, τ dos elementos de $G = G_{L:K}$. La igualdad $\alpha_i^n = a_i$ implica

$$[\sigma(\alpha_i)]^n = \sigma(\alpha_i^n) = \sigma(a_i) = a_i.$$

Existe pues un entero $\varphi(i)$ tal que $\sigma(\alpha_i) = \xi^{\varphi(i)} \alpha_i$ y, del mismo modo, un entero $\psi(i)$ tal que $\tau(\alpha_i) = \xi^{\psi(i)} \alpha_i$. Se tiene entonces

$$(\sigma \circ \tau)(\alpha_i) = \sigma[\xi^{\psi(i)} \alpha_i] = \xi^{\psi(i)} \xi^{\varphi(i)} \alpha_i.$$

Igualmente,

$$(\tau \circ \sigma)(\alpha_i) = \xi^{\varphi(i)} \xi^{\psi(i)} \alpha_i.$$

Un K-automorfismo de L queda definido por su acción sobre los α_i, así que, efectivamente se tiene $\sigma \circ \tau = \tau \circ \sigma$ y G es conmutativo.

3.° $\xi^{\varphi(i)}$ tiene por orden un divisor n_i de n; evidentemente n_i es el menor entero q_i tal que $\sigma^{q_i}(\alpha_i) = \alpha_i$. Si m es el m.c.m. de $n_1, n_2, \ldots, n_r$, es σ de orden m, y se obtiene el resultado del enunciado.

32

Sea $L \supseteq K$ un cuerpo de descomposición de $f(x) = x^3 + ax + b$, y sean α, β, γ las raíces de la ecuación $f(x) = 0$.

Un cálculo clásico muestra que

$$\Delta = -4a^3 - 27b^2 = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

L es una extensión finita de Galois de K, y el grupo de Galois $G = G_{L:K}$ es isomorfo a un subgrupo Γ del grupo de permutaciones del conjunto $\{\alpha, \beta, \gamma\}$. G es, pues, de orden 3 o 6. Para que $K(\alpha)$ sea extensión normal de K es necesario y suficiente que $K(\alpha) = L$, luego que G sea de orden 3.

1.° Pongamos $\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$. Es evidente que $\delta \neq 0$,

$$\delta \neq -\delta,$$

puesto que K no es de característica 2.

Si $K(\alpha)$ es extensión normal de K, G y Γ son cíclicos de orden 3, luego Γ está formado por las permutaciones pares de $\{\alpha, \beta, \gamma\}$. Por tanto δ es invariante en todos los K-automorfismos $\sigma \in G$, lo que implica $\delta \in K$. Por tanto Δ es el cuadrado de un elemento de K.

Recíprocamente, si Δ es el cuadrado de un elemento de K, se tiene $\delta \in K$. Es pues imposible que Γ contenga ninguna permutación impar de $\{\alpha, \beta, \gamma\}$. Entonces Γ y G son de orden 3, y $L = K(\alpha)$.

2.° En el anillo $K(\alpha)[x]$ el polinomio $f(x)$ admite la descomposición

$$f(x) = (x - \alpha)(x^2 + \alpha x + \alpha^2 + a).$$

Para que $K(\alpha) = L$ es necesario y suficiente que el trinomio de segundo grado

$$x^2 + \alpha x + \alpha^2 + a$$

admita dos ceros en $K(\alpha)$, luego que su discriminante sea el cuadrado de un elemento de $K(\alpha)$. Por tanto, $K(\alpha)$ es extensión normal de K si y sólo si existen elementos u, v, w de K tales que

$$-4a - 3\alpha^2 = (u + v\alpha + w\alpha^2)^2, \tag{1}$$

puesto que $\{e, \alpha, \alpha^2\}$ es una base del K-espacio vectorial $K(\alpha)$.

Teniendo en cuenta que $\alpha^3 = -a\alpha - b$, la anterior relación (1) equivale al sistema

$$\begin{cases} v^2 + 2uw - aw^2 + 3e = 0, \\ 2uv - bw^2 - 2uwa = 0, \\ u^2 - 2vwb + 4a = 0. \end{cases}$$

Se comprueba que ese sistema es equivalente al siguiente:

$$\begin{cases} a = \dfrac{1}{w^2}(v^2 + 2uw + 3e), \\ b = \dfrac{-2v}{w^2}(v^2 + uw + 3e), \\ (2v^2 + uw + 2e)(2v^2 + uw + 6e) = 0. \end{cases}$$

Si elegimos u, v, w tales que $2v^2 + uw + 2e = 0$, el polinomio $w^3 f(x)$ se expresa en la forma

$$(wx + 2v)(wx - v + e)(wx - v - e),$$

y no es irreducible en $K[x]$.

Por el contrario, si se eligen u, v, w tales que $2v^2 + uw + 6e = 0$, y se pone

$$r = \frac{v}{w}, \quad s = \frac{1}{w} \neq 0,$$

obtenemos

$$a = -3(r^2 + 3s^2), \quad b = 2r(r^2 + 3s^2),$$
$$\Delta = -4a^3 - 27b^2 = [18s(r^2 + 3s^2)]^2 \neq 0.$$

En tal caso el polinomio $f(x)$ es separable, y sus tres ceros están en $K(\alpha)$. Pero no es evidente que $\alpha \notin K$.

3.° Ahora bien, cuando K es el cuerpo $\mathbf{Q}$ o el $\mathbf{R}$, la condición $\Delta > 0$ implica que la ecuación $f(x) = 0$ no admite más que una sola raíz real. Es pues imposible que $K(\alpha) = K$, puesto que K debiera en tal caso contener las tres raíces de $f(x) = 0$. Las condiciones: $r \in K$, $s \in K$, $s \neq 0$,

$$a = -3(r^2 + 3s^2), \quad b = 2r(r^2 + 3s^2)$$

son pues suficientes para que el cuerpo de ruptura sobre K de

$$f(x) = x^3 + ax + b$$

sea extensión normal y separable, de grado 3, de K.

PUBLICACIONES CIENTÍFICAS Y DE TECNOLOGÍA APLICADA DE EDITORIAL REVERTÉ, S A.

Michael Spivak

CALCULUS

Un volumen de 840 páginas, de 22 x 16 cm, con numerosas figuras

La idea central que ha estado presente en la confección de cada uno de los detalles de este libro, ha sido la de presentar el Cálculo, no simplemente como un preludio de las matemáticas, sino como el primer encuentro real con las mismas. Puesto que fueron los fundamentos del análisis los que suministraron el material que sirvió de base para el desarrollo de las formas modernas de discurso matemático, debería verse en el Cálculo una ocasión de profundizar en los conceptos básicos de lógica, en vez de tratar de eludirlos. Además de fomentar la intuición de los estudiantes acerca de los hermosos conceptos del análisis, es desde luego igualmente importante convencerlos de que la precisión y el rigor no constituyen ni obstáculos para la intuición ni tampoco fines en sí mismos, sino simplemente el medio natural para formular y tratar las cuestiones matemáticas.

Esta finalidad implica un enfoque de las matemáticas que, en cierto sentido, tratamos de defender a lo largo de todo el libro. Por perfecta que pueda ser la exposición de cada materia en particular, los fines del libro sólo se alcanzarán si tiene éxito en su conjunto. Por ello, de poco serviría hacer una lista de las materias tratadas o mencionar las prácticas pedagógicas y otras innovaciones. Incluso la rápida ojeada que rutinariamente se da a cada nuevo texto de Cálculo, valdrá más que cualquier explicación, y el profesor con criterio formado acerca de cada aspecto particular del Cálculo, sabrá dónde consultar para ver si el libro satisface sus aspiraciones.

Hay, sin embargo, algunos rasgos que requieren un comentario explícito. De los veintinueve capítulos del libro, dos (señalados con asteriscos) son optativos, y los tres capítulos de la parte V se han incluido solamente con vistas a aquellos estudiantes a los que pudiera interesar un examen por cuenta propia de la construcción de los números reales. Los apéndices a los capítulos 3 y 11 contienen también material optativo.

EXTRACTO DEL INDICE

Matemáticas para científicos

Thor A. Bak y Jonas Lichtenberg

EN TRES VOLÚMENES

1 - Vectores, Tensores y grupas 2 - Funciones de una y varias variables
3 - Series ecuaciones diferenciales y funciones complejas

Versión española revisada y dirigida por el Dr. R. RODRÍGUEZ VIDAL,
Catedrático de Matemáticas de la Universidad de Zaragoza

Este libro es una edición revisada y algo más ampliada de la obra **«Videregaende Matematik»**, cuya primera edición se publicó en 1960. La obra danesa fue escrita inicialmente para un curso de un año de duración explicado por los autores para químicos, bioquímicos y doctores en Medicina dedicados a la investigación básica.

Este curso, al cual fue en principio destinado el libro, perseguía el fin específico de proporcionar la base matemática necesaria para posteriores estudios e investigaciones en Física, Química y Biología. Puesto que, de hecho, el libro se ha utilizado en otros cursos, le hemos añadido ahora algunas materias que creemos lo harán útil para finalidades más generales.

El escribir un libro de Matemáticas para científicos plantea siempre el problema de hallar un equilibrio razonable, por un lado entre rigor y comprensibilidad, fundamentalmente, y, por otro, entre inmediata utilidad y cobertura suficiente de material. Hemos tratado de resolver este problema por el siguiente procedimiento: A lo largo del libro formulamos de manera bastante exacta los resultados que se han obtenido, incluso en los casos en que se omiten las demostraciones. Sin embargo, la forma en que exponemos los resultados cambia algo desde el principio del libro, en que utilizamos una formulación más rigurosa, a la última parte, donde nos servimos, en notable medida, de la formulación algo más flexible que se utiliza habitualmente en muchos excelentes libros de texto de Física y Química.

El libro 1 (Capítulos 1 y 2) contiene las materias referentes a vectores, tensores y grupos y puede leerse sin necesidad de ningún conocimiento sobre Cálculos. Nuestra experiencia nos dice que puede explicarse en un curso de un semestre empleando dos horas a la semana. El libro 2 (Capítulos 3 y 4) contiene las materias referentes a funciones de una y varias variables. En él se utiliza con mucha frecuencia el concepto de vector, utilizándose, al final del Capítulo 4, las matrices y el concepto de tensor. Dejando esto aparte, el libro 2 puede leerse con independencia del número 1, y, combinado con una pequeña parte del contenido del Volumen 3, podría constituir la base de un curso semestral de Cálculo, a razón de cuatro horas semanales. El libro 3 (Capítulos 5 a 8) contiene las materias que aparecen incluidas normalmente en libros de Cálculo superiores: series, ecuaciones diferenciales, funciones de variable compleja y métodos numéricos. Este volumen está escrito de tal forma que en gran medida es independiente de las formulaciones específicas dadas en los restantes, pero exige un cierto conocimiento de las matrices, de los problemas de valores propios y funciones de una y varias variables. En nuestro curso inicial de un año de duración, de cuatro horas por semana, explicamos los Capítulos 1, 3, 4 y 5 y parte de los Capítulos 6 y 8.

EXTRACTO DEL ÍNDICE

J. DIEUDONNÉ

FUNDAMENTOS DE ANÁLISIS MODERNO

Un volumen de 368 páginas, de 22 × 16 cm, con numerosos problemas

Este volumen es el desarrollo de un curso proyectado para estudiantes graduados del primer año, o para pregraduados aventajados de los años junior y senior. El propósito del curso fue doble: (a) proporcionar los fundamentos necesarios en todas las ramas de la Matemática moderna relacionadas con el Análisis; (b) adiestrar al estudiante en el uso del instrumento matemático más fundamental de nuestro tiempo: el método axiomático.

El lector se dará cuenta inmediatamente, de que en todas partes se ha puesto de relieve el aspecto conceptual de cada noción, en vez de presentar su aspecto algorítmico, es decir, como un ente de cálculo que era el principal objetivo del Análisis clásico. Esta preocupación se manifiesta no sólo en lo que se refiere al texto, sino también en la mayor parte de los problemas. Se observará que se han incluido gran número de problemas como suplemento del texto y muchos de ellos orientan hacia otros desarrollos interesantes. Los problemas a su vez, proporcionan al estudiante una oportunidad para comprobar si ha comprendido la materia expuesta.

Aunque en este volumen se desarrollan muchas cuestiones tratadas ordinariamente en cursos más elementales (incluidos los de Cálculo) el punto de vista desde el que se las considera es completamente distinto.

Los conceptos fundamentales de la Teoría de funciones y del Cálculo se han presentado dentro del armazón de una teoría que es lo suficientemente general para mostrar la finalidad, la potencia y la naturaleza verdadera de estos conceptos, mucho mejor que bajo las restricciones usuales del «Análisis clásico».

EXTRACTO DEL INDICE

OTRAS PUBLICACIONES DE ESTA EDITORIAL

Algebra. *Libro sobresaliente para cursos de matemáticas en las Escuelas de Ingeniería y Facultades de Ciencias, por* P. K. REES y F. W. SPARKS. Un volumen de 500 páginas, de 23 × 16 cm, con 50 figuras y tablas.

Análisis matemático. *Introducción moderna al cálculo superior,* por T. M. APOSTOL. Un volumen de 500 páginas, de 22 × 16 cm, con 88 figuras.

Trigonometría plana. *Obra que presenta un gran valor pedagógico en la exposición de la materia y en la elección de ejercicios y problemas,* por F. W. SPARKS y P. K. REES. Un volumen de 290 páginas, de 23 × 16 cm, con 72 figuras y numerosas tablas.

Geometría descriptiva. *Compendio de geometría descriptiva para técnicos,* por B. LEIGHTON WELLMAN. Un volumen de 628 páginas, de 22 × 16 cm, con 508 figuras.

Matemáticas elementales. *Nociones de aritmética, geometría, álgebra y trigonometría,* por C. I. PALMER y S. F. BIBB. Cuatro volúmenes de 822 páginas en total, de 19 × 13 cm, con 364 ilustraciones y numerosas tablas.

Geometría analítica y cálculo infinitesimal. *Obra de gran valor pedagógica para la enseñanza combinada de estas dos materias,* por W. R. LONGLEY, P. F. SMITH y W. A. WILSON. Un volumen de 794 páginas, de 23 × 15 cm, con 337 ilustraciones.

Nuevas tablas de logaritmos de cinco decimales. *Obra que abarca la división sexagesimal y la división centesimal,* por C. BOUVART y A. RATINET. Un volumen de 188 páginas, de 22 × 10 cm.

Mecánica. *Volumen 1 del curso de física teórica,* por L. D. LANDAU y E. M. LIFSHITZ. Un volumen de 228 páginas, de 22 × 16 cm, con 54 figuras.

Fenómenos de transporte. *Un estudio sistemático de las leyes básicas del transporte de materia, energía y cantidad de movimiento,* por R. BYRON BIRD, WARREN E. STEWART y EDWIN N. LIGHTFOOT. Un volumen de 850 páginas, de 22 × 16 cm, con 267 ilustraciones y numerosas tablas.

Mecánica. *Libro que presenta una gran colección de problemas que ilustran una amplia aplicación a los distintos campos de la técnica,* por J. L. MERIAM. Tomo I. **Estática.** Un volumen de 400 páginas, de 22 × 16 cm, con 656 ilustraciones. Tomo II. **Dinámica.** Un volumen de 450 páginas, de 22 × 16 cm, con 588 ilustraciones.

EDITORIAL REVERTÉ, S. A.

BARCELONA - BUENOS AIRES - MÉXICO


S
REVERTÉ
A