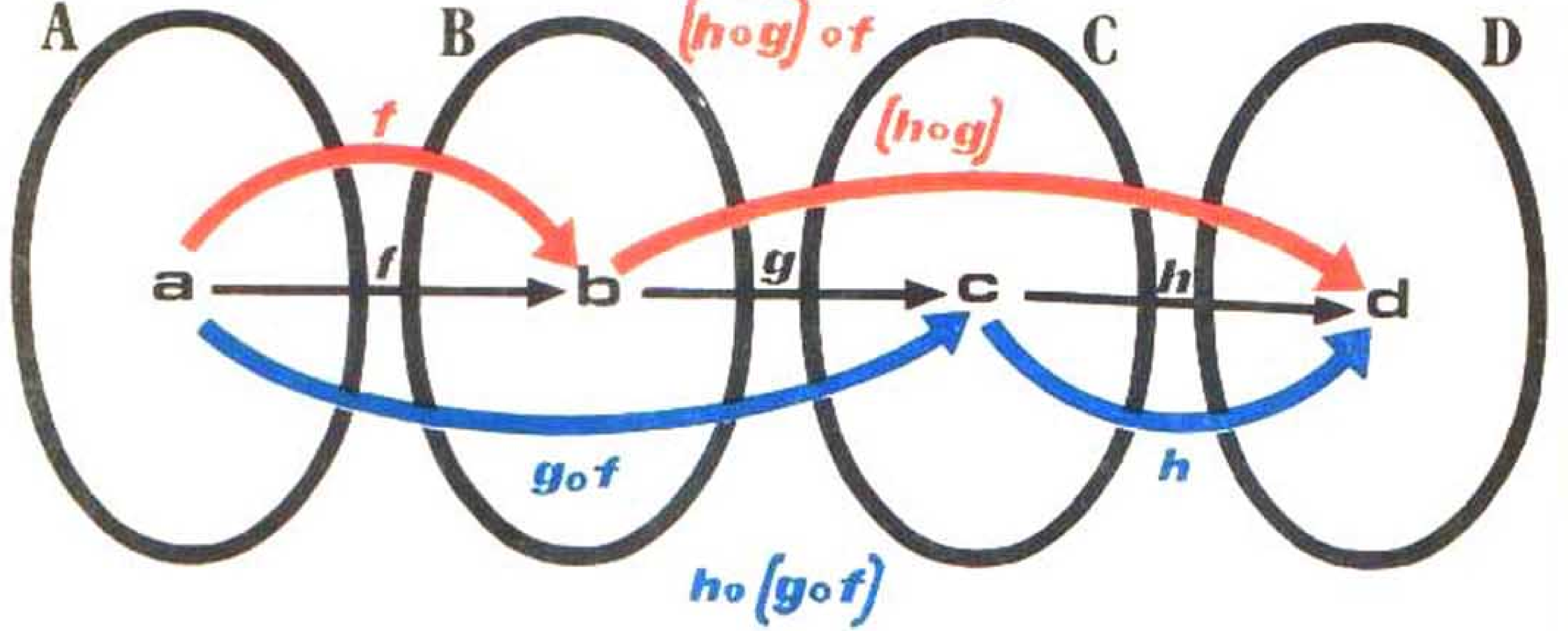
JOSE F. PUERTAS DOMINGO
MANUEL MARQUES PEREZ

MATEMATICA UNIVERSITARIA

ALGEBRA

$$(h\circ g)\circ f\,[a] = (h\circ g)\,[f(a)] =$$
$$= h\circ g\,[b] = h\,[g(b)] = h(c) = d$$



Bello
C.O.U.

MATEMATICA UNIVERSITARIA

A L G E B R A

José Francisco Puertas Domingo
CATEDRATICO MATEMATICAS

Manuel Marqués Pérez
PROFESOR MATEMATICAS

MATEMATICA UNIVERSITARIA

ALGEBRA

BELLO
— VALENCIA —

I.S.B.N. 84-212-0061-5

Depósito Legal: V. 1.563.–1973.

EDITORIAL BELLO - Comedias, 20 - Valencia (España)

Tipografía Artística Puertes, S. L. - Palleter, 47 - Teléfono 25 06 77 - Valencia

PROLOGO

El libro que presentamos —Matemática Universitaria (C.O.U.)— se concibe como un manual a nivel universitario, y es fruto de la docencia realizada por los autores a lo largo de los últimos cinco años en la Universidad de Valencia y Colegio Universitario de Castellón (dependiente de ésta), dictando programas de Matemáticas —Generales, Algebra Lineal y Cálculo Infinitesimal— correspondientes a los primeros cursos de Ciencias y Escuelas Técnicas Superiores.

Consideramos el COU como un curso puente entre la concepción "media" de las Matemáticas y la visión universitaria, caracterizada por un rigor superior en la exposición y un tratamiento más axiomático de los temas. Esto nos ha obligado a redactar un libro que formalmente fuera ya un libro de facultad, y en donde los recortes de materia afectaran en todo caso a la extensión, dejando al margen aspectos considerados secundarios, pero no a lo fundamental de su construcción estructural.

Es indudable que el Plan 1957 y su división del Bachillerato en Ciencias y Letras condiciona el tratamiento del COU por el profesor; sin embargo, este hándicap transitorio que acabará con la implantación del BUP, no debía hacernos incurrir en el error de confeccionar un libro para hoy, sino aportar una experiencia bibliográfica que se aproximara ya a lo que Matemáticas-COU debe contener y significar en el futuro, y tras las experiencias de su implantación. Esta es la razón por la que este libro hoy es utilizable no sólo como libro de orientación universitaria, sino que, por los temas que en él se estudian y la forma en que se tratan, puede ser un libro de consulta para Primero de Ciencias, Escuelas Técnicas Superiores y Ciencias Económicas.

El libro constará de dos volúmenes —"Algebra" y "Análisis y Estadística"— teóricos, y un volumen complementario de Ejercicios y Problemas.

Su contenido será, básicamente:

"Algebra": Lógica. Conjuntos y operaciones con conjuntos. Aplicaciones. Relaciones binarias. Estructuras básicas: Grupo, Anillo, Cuerpo. Espacios vectoriales. Aplicaciones lineales. Aplicaciones multilineales. Sistemas de ecuaciones.

"Análisis y estadística: El número real. Funciones reales de variable real. Continuidad. Derivación. Integral indefinida. Integral definida. Teoría de la probabilidad. Distribuciones. Teoría del muestreo.

El volumen de Ejercicios y Problemas recorrerá el programa teórico con ejemplos resueltos y ejercicios y problemas propuestos.

TEMA 0 | LOGICA

0-1 INTRODUCCION

> *"De manera sumaria, podría decirse que la Lógica Formal tiene por objeto la técnica de la argumentación, y que la validez de la argumentación no depende del contenido de los enunciados, sino sólo de su forma."*
>
> **R. Feys**

> *"El estudio de la Lógica es el estudio de los métodos y principios usados para distinguir un razonamiento correcto de otro incorrecto."*
>
> **I. M. Copi**

Podemos decir que en estas dos definiciones se hallan contenidas las ideas básicas que originan y rigen la Lógica. Por un lado, la Lógica estudia el razonamiento, la argumentación, tratando de estructurar unas formas de razonar cuya validez no depende del significado de

los elementos que en él intervienen, sino solamente de la forma en que éstos se hallen dispuestos en el argumento. Por otro, nos da medios para distinguir en cada caso un razonamiento correcto de otro incorrecto.
De todo esto surgen ya las primeras cuestiones importantes: ¿cuáles son los objetos con los que va a trabajar la Lógica?; ¿qué criterios vamos a establecer para aceptar o rechazar un argumento? La lógica que vamos a tratar será una lógica de dos valores (bivalente), cuyos elementos constitutivos serán las proposiciones.

0-2 PROPOSICION

Llamamos proposición a toda oración de la cual se pueda afirmar que es cierta o es falsa.
Las representaremos por:

$$p, q, r, s, \ldots$$

EJEMPLOS:

"Europa es un continente."
"El número 3 es entero."
"Australia es un cuadrúpedo."

En Lógica, lo importante de una proposición es el hecho de que sea cierta o falsa, y no el significado o el sentido gramatical de la oración. Así, en los ejemplos citados, las dos primeras proposiciones son ciertas, y la última es falsa.

0-3 AXIOMAS

La lógica bivalente que vamos a estudiar quedará establecida con tres axiomas.

1.—Axioma de Identidad

"Toda proposición es igual a sí misma."

2.—Axioma de Contradicción

"Una proposición no puede ser cierta y falsa a la vez."

3.—Axioma de Tercero Excluido

"Toda proposición o es cierta o es falsa."

Esto implica que en lógica bivalente no se puede afirmar que una proposición p es cierta en un 80 %, falsa en un 10 % y otro 10 % de indecisión. Sólo se puede afirmar que una proposición es cierta o falsa, excluyéndose ambas posibilidades y sin ninguna tercera alternativa.
Simbólicamente, expresaremos que una proposición p es cierta diciendo que tiene un *valor lógico 1*, y para indicar que es falsa, la proposición q es falsa, diremos: q tiene un *valor lógico 0*.

0-4 CONEXIONES LOGICAS

Las conexiones lógicas o partículas veritativas, son unos símbolos que al aplicarlos a una o varias proposiciones, cuyo valor lógico es conocido, las transforma en otras cuyo valor lógico depende de la partícula conectiva y de los valores lógicos de las proposiciones originales.
Las partículas conectivas serán ciertas partículas gramaticales que servirán para enlazar oraciones.
Así: Con la proposición "el tres es un número entero", se puede construir una nueva proposición negando la anterior: "el tres NO es un número entero".
También con las proposiciones q = "El cielo está nublado" y r = "Está lloviendo" podemos formar las proposiciones:

p o q = "El cielo está nublado o está lloviendo"
p y q = "El cielo está nublado y está lloviendo"
si p entonces q = "El cielo está nublado entonces está lloviendo"
p sí y sólo si q = "El cielo está nublado sí y sólo si está lloviendo"

y han aparecido a partir de aquellas dos p y q cuatro proposiciones nuevas, que tendrán un valor lógico definido cuando tengamos definidas las partículas conectivas.

Si nos detenemos a observar las proposiciones que nos han salido nos daremos cuenta que todas ellas tienen "sentido". Sin embargo, esto no significa nada, puesto que, por ejemplo, en la proposición: "Si la nieve es blanca entonces el hombre es un árbol" no tiene "sentido" lo que decimos, pero en cambio sí que posee un valor lógico, como veremos en breve.
Las partículas conectivas que vamos a estudiar serán cinco: negación, disyunción, conjunción, implicación, coimplicación.

Negación.—Esta partícula la representaremos por el signo $\neg$ y se leerá "no". La definiremos del siguiente modo: Dada la proposición p, a partir de ella podemos formar $\neg p$, que se leerá "no p" y que tiene valor lógico contrario al de p. Es decir, si p era 1, entonces $\neg p$ será 0, y si p era 0, entonces $\neg p$ será 1.
Esto lo representaremos en las llamadas tablas de verdad del siguiente modo:

p	$\neg p$
1	0
0	1

que significa lo mismo que hemos dicho, cuando p vale 1, $\neg p$ vale 0, y cuando p vale 0, $\neg p$ vale 1.

Disyunción.—Dadas dos proposiciones p y q la disyunción la representaremos por $p \vee q$ (leyendo p o q) y la definiremos como sigue: "La disyunción será cierta cuando lo sea alguna de las proposiciones que la componen y será falsa cuando lo sean las dos simultáneamente".
Esta definición la representaremos en las tablas de verdad, como sigue:

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

lo cual significa: En este caso hay dos proposiciones p y q, por tanto se pueden dar los cuatro casos que hemos escrito: que sea cierta p y cierta q, que sea cierta p y falsa q, que se falsa p y cierta q, y que sean p y q falsas. En cada uno de los cuatro casos posibles hemos colocado a la derecha el valor lógico correspondiente a la disyunción. Entonces, en el ejemplo anterior: "La nieve es blanca o el hombre es un árbol" será cierta, puesto que de las dos proposiciones que la componen hay una que es cierta.

Conjunción.—Dadas dos proposiciones p y q la conjunción la representaremos por $p \wedge q$ (que se leerá p y q) y la definiremos según lo siguiente:
"La conjunción de dos proposiciones será cierta cuando sean ciertas ambas simultáneamente, y será falsa cuando exista una que es falsa".
En las tablas de verdad, esto será:

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

la conjunción de p y q es cierta cuando lo son p y q.

la conjunción es falsa en los restantes tres casos.

Por ejemplo, la proposición "La nieve es blanca y el hombre es un árbol" es falsa, según la definición que hemos dado.

Implicación.—Dadas dos proposiciones p y q, la implicación la representaremos por $p \rightarrow q$ (se lee "p implica q" o "si p entonces q") y se define como "aquella proposición que es cierta siempre que es falsa p o cuando es cierta q, y es falsa sólo en el caso de que siendo cierta p sea falsa q".
En la implicación, a p se le llama antecedente y a q consecuente.
En las tablas de verdad, esto se expresará:

p	q	$p \rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Entonces, la proposición "Si la nieve es blanca entonces el hombre es un árbol", de la cual antes hemos dicho que no tenía "sentido", sí que tiene sentido en lógica, y de acuerdo con lo que hemos visto, como la primera es cierta y la segunda es falsa, la total, que es una implicación, será falsa.

Coimplicación.—La coimplicación de dos proposiciones p y q se representa por $p \leftrightarrow q$ (que se lee "p coimplica q", o "p sí y sólo si q") y la definiremos del siguiente modo:
"Es una proposición que es cierta cuando p y q tienen el mismo valor lógico y falsa cuando p y q poseen valores lógicos distintos".
La tabla de verdad correspondiente, será:

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Del mismo modo que la proposición atravesaba el proceso de ser primero una oración gramatical con un sentido y un valor lógico, a ser, finalmente, un elemento de la lógica (no importa lo que signifique) con un valor lógico, con las partículas conectivas ocurre lo mismo; es decir, que pasan de ser unas partículas gramaticales que sirven para unir oraciones, a ser solo unos elementos de la lógica cuya definición será la tabla de verdad correspondiente, y que sirve para formar nuevas proposiciones que podemos llamar compuestas, porque en ellas intervienen una o varias partículas conectivas. De esta forma llamaremos, pues, proposiciones simples a aquellas que no contienen ninguna partícula conectiva.
Observemos que la certeza o falsedad de una proposición compuesta depende de la certeza o falsedad de las proposiciones simples que la componen, pero también, y esencialmente, de las partículas conectivas. En este sentido, se dice, pues, que las partículas conectivas son funciones veritativas, pues la certeza o falsedad de la proposición compuesta depende (o es función) de la partícula conectiva que se utilice para formarla.

0–5 FORMAS PROPOSICIONALES

Hemos dicho al comenzar el tema que las proposiciones las representaríamos por las letras p, q, r,... Vamos ahora a utilizar unas variables proposicionales A, B, C,... en el sentido de que pueden sustituirse por una proposición concreta cualquiera.
"Llamaremos forma proposicional a las variables proposicionales y al resultado de aplicar a estas las partículas conectivas un número finito de veces".
Así, las A, B, C,... serán formas proposicionales, y también lo serán $\neg A$, $A \vee B$, $A \wedge C$, $A \rightarrow B$, $A \leftrightarrow B$, etcétera.
Para obtener una proposición, reemplazaremos en una forma proposicional las variables proposicionales por proposiciones concretas, siempre que se reemplace la misma variable por la misma proposición en todos los lugares en que aparezca.

EJEMPLO: Una forma proposicional será:

$$(A \wedge \neg B) \rightarrow [A \vee (B \rightarrow C)] \wedge \neg D$$

donde A, B, C y D son variables proposicionales. Ahora obtendremos una proposición, sustituyendo A por p, B por q, C por r y D por s.

$$(p \wedge \neg q) \rightarrow [p \vee (q \rightarrow r)] \wedge \neg s$$

0-5-1 FORMAS PROPOSICIONALES UNIVERSALMENTE VALIDAS

Diremos que una forma proposicional es universalmente válida si es cierta la proposición resultante al reemplazar las variables proposicionales por cualesquiera proposiciones concretas. Es decir, si la certeza de la forma no depende de que sean ciertas o falsas las proposiciones que reemplacen a sus variables.

EJEMPLO:

$$(\neg A \vee B) \rightarrow (A \rightarrow B)$$

Veamos que esta proposición es cierta sea cual sea el reemplazamiento que hagamos de A y B por proposiciones.

	A	B	$\neg A$	$\neg A \vee B$	$A \to B$	$(\neg A \vee B) \to (A \to B)$
1.er caso. . . .	1	1	0	1	1	1
2.° caso. . . .	1	0	0	0	0	1
3.er caso	0	1	1	1	1	1
4.° caso. . . .	0	0	1	1	1	1

Observemos en este ejemplo que al sustituir A y B por distintas proposiciones concretas, como lo único que importa de estas es su valor lógico, se pueden presentar los cuatro casos especificados y en cada uno de los casos la última columna presente el valor lógico 1 para la forma propuesta. Luego ésta es cierta universalmente.

El problema de la validez universal está ligado íntimamente al problema central de la lógica matemática, como apuntaba Feys al comenzar este tema de lógica.
Es evidente que la certeza o falsedad de una forma proporcional sólo depende, por un lado, de su "forma", es decir, del modo en que están unidas las variables por las distintas partículas conectivas que la integran, y de otro, por las proposiciones concretas que reemplacen las variables. Por tanto, si la certeza o falsedad de una forma proposicional no depende de las proposiciones que reemplazan a las variables, como ocurre con las formas proposicionales universalmente válidas, entonces sólo depende de la estructura interna de la misma. Una forma proposicional universalmente válida es cierta en razón de su peculiar estructura lógica, o como decimos comúnmente, es cierta por razones de "lógica".
Cuando reemplazamos las variables proposicionales por proposiciones concretas en una forma universalmente válida, aparecerá siempre una proposición cierta, pero cuya certeza no proviene de las proposiciones que la componen, sino de su estructura lógica. Llamamos *tautologías* a todas las proposiciones que surgen por reemplazamiento en una forma universalmente válida. La negación de una fórmula universalmente válida será, evidentemente, una fórmula universalmente falsa. Llamamos *contradicciones* a la proposición que resulta por reemplazamiento en una fórmula cuya negación es universalmente válida.

EJEMPLOS:

1: $A \vee \neg A$ es una fórmula universalmente válida, puesto que

A	$\neg A$	$A \vee \neg A$
1	0	1
0	1	1

para los dos casos que pueden surgir con cualquier reemplazamiento $A \vee \neg A$ tiene el valor lógico 1.

Si p es una proposición concreta, $p \vee \neg p$ será una tantología.

2: $B \wedge \neg B$ es una fórmula universalmente falsa. Es decir, su negación es universalmente válida.

B	$\neg B$	$B \wedge \neg B$	$\neg(B \wedge \neg B)$
1	0	0	1
0	1	0	1

Si q es una proposición concreta, $q \wedge \neg q$ será una contradicción.

Las formas proposicionales las representaremos por $\alpha\, \beta\, \gamma\, \delta$...

0-5-2 EQUIVALENCIA

Dos formas proposicionales α, β son equivalentes cuando la doble implicación $\alpha \leftrightarrow \beta$ de una a la otra es universalmente válida. Lo representaremos α *eq* β o también $\alpha \Longleftrightarrow \beta$.

La equivalencia entre formas proposicionales posee las propiedades:

a) Reflexiva: Toda forma es equivalente a sí misma $\alpha \Longleftrightarrow \alpha$.

b) Simétrica: Si una forma α es equivalente a otra β, entonces β es equivalente a α.

$$(\alpha \Longleftrightarrow \beta) \rightarrow (\beta \Longleftrightarrow \alpha)$$

c) Transitiva: Si una forma α es equivalente a otra β, y a su vez esta es equivalente a una tercera γ, entonces α es equivalente a γ.

$$[(\alpha \Longleftrightarrow \beta) \wedge (\beta \Longleftrightarrow \gamma)] \rightarrow (\alpha \Longleftrightarrow \gamma)$$

Estudiemos ahora con la ayuda de la equivalencia algunas propiedades de las partículas conectivas:

1) **Negación:** *Idempotencia:* Toda forma α es equivalente a $\neg\neg\alpha$.

α	$\neg\alpha$	$\neg\neg\alpha$	$\alpha \leftrightarrow \neg\neg\alpha$
1	0	1	1
0	1	0	1

como la doble implicación es universalmente válida, ambos son equivalentes.

2) **Conjunción:** *Idempotente:* Toda forma α es equivalente a $\alpha \wedge \alpha$.

α	α	$\alpha \wedge \alpha$	$\alpha \leftrightarrow \alpha \wedge \alpha$
1	1	1	1
0	0	0	1

Conmutativa: $\alpha \wedge \beta \Longleftrightarrow \beta \wedge \alpha$

α	β	$\alpha \wedge \beta$	$\beta \wedge \alpha$	$(\alpha \wedge \beta) \leftrightarrow (\beta \wedge \alpha)$
1	1	1	1	1
1	0	0	0	1
0	1	0	0	1
0	0	0	0	1

Asociativa: $\alpha \wedge (\beta \wedge \gamma) \Longleftrightarrow (\alpha \wedge \beta) \wedge \gamma$.

α	β	γ	$\alpha \wedge \beta$	$\beta \wedge \gamma$	$\alpha \wedge (\beta \wedge \gamma)$	$(\alpha \wedge \beta) \wedge \gamma$	$\alpha \wedge (\beta \wedge \gamma) \leftrightarrow (\alpha \wedge \beta) \wedge \gamma$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	0	0	0	1
0	1	1	0	1	0	0	1
1	0	0	0	0	0	0	1
0	1	0	0	0	0	0	1
0	0	1	0	0	0	0	1
0	0	0	0	0	0	0	1

3) **Disyunción.** Del mismo modo como hemos demostrado las propiedades de la conjunción pueden probarse las siguientes propiedades de la disyunción:

Idempotente: $\alpha \vee \alpha \Longleftrightarrow \alpha$

Conmutativa: $\alpha \vee \beta \Longleftrightarrow \beta > \alpha$

Asociativa: $\alpha \vee (\beta \vee \gamma) \Longleftrightarrow (\alpha \vee \beta) \vee \gamma$

4) **Propiedades distributivas.** Existen dos propiedades distributivas: una de la conjunción respecto de la disyunción, y otra de la disyunción respecto de la conjunción.

a) $\alpha \wedge (\beta \vee \gamma) \Longleftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$

b) $\alpha \vee (\beta \wedge \gamma) \Longleftrightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$

Probemos la primera de ellas:

α	β	γ	$\beta \vee \gamma$	$\alpha \wedge \beta$	$\alpha \wedge \gamma$	$\alpha \wedge (\beta \vee \gamma)$	$(\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$	$\alpha \wedge (\beta \vee \gamma) \leftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$
1	1	1	1	1	1	1	1	1
1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	1	1
0	1	1	1	0	0	0	0	1
1	0	0	0	0	0	0	0	1
0	1	0	1	0	0	0	0	1
0	0	1	1	0	0	0	0	1
0	0	0	0	0	0	0	0	1

Si la doble implicación es universalmente válida, las dos formas son equivalentes.

5) **Leyes de Morgan.** Las llamadas leyes de Morgan son dos equivalencias, de las cuales nosotros probaremos sólo una de ellas por medio de las tablas de verdad y la otra quedará como ejercicio. Estas son:

a) $\neg(\alpha \wedge \beta) \Longleftrightarrow \neg\alpha \vee \neg\beta$ "La negación de la conjunción es la disyunción de las negaciones."

b) $\neg(\alpha \vee \beta) \Longleftrightarrow \neg\alpha \wedge \neg\beta$ "La negación de la disyunción es la conjunción de las negaciones."

Vamos a probar la primera de ellas:

α	β	$\neg\alpha$	$\neg\beta$	$\alpha \wedge \beta$	$\neg\alpha \vee \neg\beta$	$\neg(\alpha \wedge \beta)$	$\neg(\alpha \wedge \beta) \leftrightarrow (\neg\alpha \vee \neg\beta)$
1	1	0	0	1	0	0	1
1	0	0	1	0	1	1	1
0	1	1	0	0	1	1	1
0	0	1	1	0	1	1	1

6) Otras equivalencias que poseen cierta importancia por su uso en la lógica proposicional son las siguientes:

$$(\alpha \rightarrow \beta) \Longleftrightarrow \neg\alpha \vee \beta$$
$$(\alpha \rightarrow \beta) \Longleftrightarrow (\neg\beta \rightarrow \neg\alpha)$$
$$(\alpha \leftrightarrow \beta) \Longleftrightarrow (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$$

El estudio de las equivalencias es fundamental, pues en el cálculo lógico siempre podemos sustituir una forma proposicional por otra equivalente.

0-6 INFERENCIAS LOGICAS

Bajo el nombre de inferencia lógica vamos a estudiar un conjunto de fórmulas universalmente válidas que se utilizan habitualmente en el razonamiento deductivo. En esencia, consisten en reglas que permiten deducir de un conjunto de proposiciones llamadas *premisas* una nueva proposición llamada *conclusión,* siempre del mismo modo, independientemente de cuales sean las premisas. Estas reglas han de ser fórmulas universalmente válidas, a fin de que la conclusión deducida a partir de las premisas sea válida. A estas reglas las llamaremos reglas de inferencia y su estructura lógica es una condicional cuyo antecedente es una conjuntiva de varias *premisas* (o de una sola) y cuyo consecuente es otra proposición que llamamos conclusión.

Esto podemos simbolizarlo del siguiente modo:

$$(p_1 \wedge p_2 \wedge p_3 \cdots \wedge p_n) \rightarrow C$$

(siendo, como hemos dicho, p_1 p_2 - - p_n las premisas y C la conclusión).

Estudiaremos ahora algunas reglas de inferencia particulares:

1) *Ponendo Ponens* (P.P.). Se aplica a una implicación y podemos decir que es "el modo de afirmar el consecuente afirmando el antecedente". El esquema correspondiente al mismo sería:

premisa 1.ª	$A \rightarrow B$
premisa 2.ª	A
conclusión	B

que, desde el punto de vista simbólico, corresponde a la fórmula proposicional

$$[(A \rightarrow B) \wedge A] \rightarrow B$$

Veamos que es una fórmula universalmente válida:

A	B	$A \rightarrow B$	$(A \rightarrow B) \wedge A$	$[(A \rightarrow B) \wedge A] \rightarrow B$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

2) *Tollendo Tollens* (T.T.). Se aplica también a las implicativas, y es "el modo de negar el antecedente negando el consecuente". El esquema del mismo será:

1.ª premisa	$A \rightarrow B$
2.ª premisa	$\neg B$
conclusión	$\neg A$

La fórmula proposicional correspondiente es:

$$[(A \rightarrow B) \wedge \neg B] \rightarrow \neg A$$

Veamos que es también universalmente válida:

A	B	$\neg B$	$A \leftrightarrow B$	$\neg A$	$(A \rightarrow B) \wedge \neg B$	$[(A \rightarrow B) \wedge \neg B] \rightarrow \neg A$
1	1	0	1	0	0	1
1	0	1	0	0	0	1
0	1	0	1	1	0	1
0	0	1	1	1	1	1

lo que nos indica que con esas dos premisas $A \rightarrow B$ y $\neg B$ siempre se puede deducir como conclusión $\neg A$.

3) *Simplificación.* Se aplica a una conjuntiva, y nos afirma que de ella se puede deducir como conclusión cualesquiera de sus componentes:

1.ª premisa	$A \wedge B$
1.ª conclusión	A
2.ª conclusión	B

La fórmula proposicional correspondiente es $(A \wedge B) \rightarrow A$ para la primera conclusión, y $A \wedge B \rightarrow B$ para la segunda.
Veamos que es universalmente válida:

A	B	$A \wedge B$	$A \wedge B \rightarrow A$	$A \wedge B \rightarrow B$
1	1	1	1	1
1	0	0	1	1
0	1	0	1	1
0	0	0	1	1

4) *Tollendo ponens.* Esta regla se aplica a una disyunción y dice: "negando uno de los miembros de la disyunción se afirma el otro miembro".

1.ª premisa	$A \vee B$
2.ª premisa	$\neg B$
conclusión	A

La forma proposicional correspondiente es:

$$[(A \vee B) \wedge \neg B] \rightarrow A$$

A	B	$\neg B$	$A \vee B$	$(A \vee B) \wedge \neg B$	$(A \vee B) \wedge \neg B \rightarrow A$
1	1	0	1	0	1
1	0	1	1	1	1
0	1	0	1	0	1
0	0	1	0	0	1

Es pues, como vemos, una forma universalmente válida.

5) *Silogismo hipotético (S.H.).* Se aplica cuando poseemos como premisas dos condicionales:

1.ª premisa	$A \rightarrow B$
2.ª premisa	$B \rightarrow C$
conclusión	$A \rightarrow C$

Se comprueba, del mismo modo que las anteriores, que la forma proposicional

$$[(A \rightarrow B) \wedge (B \rightarrow C)] \rightarrow (A \rightarrow C)$$

es universalmente válida.

6) *Ley de adición: (L.A.).* Dada la premisa A, si M es una variable proposicional cualquiera, de A se deduce $A \vee M$.

El esquema de la misma es:

1.ª premisa	A
conclusión	$A \vee M$

7) *Silogismo disyuntivo (S.D.).* El silogismo disyuntivo posee tres premisas:

1.ª premisa	$A \vee B$
2.ª premisa	$A \rightarrow C$
3.ª premisa	$B \rightarrow D$
conclusión	$C \vee D$

la forma proposicional correspondiente

$$[(A \vee B) \wedge (A \rightarrow C) \wedge (B \rightarrow D)] \rightarrow C \vee D$$

es universalmente válida, como se puede probar fácilmente con unas tablas de verdad en las que intervendrían 16 filas, correspondientes a todos los valores lógicos posibles a las cuatro variables.

8) *Demostración condicional (D.C.).* En una demostración cualquiera, siempre podemos añadir una premisa más, sea la que sea, en un punto cualquiera de la misma, teniendo bien en cuenta que el resultado obtenido ahora dependerá directamente de la nueva premisa que hemos impuesto. La demostración condicional es la que nos dice de qué modo se realiza esta dependencia. La podemos enunciar del siguiente modo: "Si de un conjunto de premisas y otra premisa que imponemos nueva, N, se deduce una conclusión, C, del conjunto de premisas solo, se deduce la condicional N → C."

El esquema es, pues,
si de:

premisas	P_1 P_2 $\vdots$ P_n
premisa nueva	N
conclusión	C

entonces, de:

premisas	P_1 P_2 P_3 $\vdots$ P_n
conclusión	$N \rightarrow C$

La forma proposicional correspondiente a este tipo de razonamiento será:

$$[((P_1 \wedge P_2 \wedge \ldots \wedge P_n) \wedge N) \rightarrow C] \rightarrow [(P_1 \wedge \quad \wedge P_2 \wedge \ldots \wedge P_n) \rightarrow (N \rightarrow C)]$$

Para probar que es una forma proposicional universalmente válida, llamemos $P = P_1 \wedge P_2 \wedge \ldots \wedge P_n$ a la forma proposicional resultante de la conjuntiva de las *n* formas. Entonces, el problema radica en demostrar

$$[(P \wedge N) \rightarrow C] \rightarrow [P \rightarrow (N \rightarrow C)]$$

En efecto:

P	N	C	$P \wedge N$	$N \rightarrow C$	$(P \wedge N) \rightarrow C$	$P \rightarrow (N \rightarrow C)$	$[(P \wedge N) \rightarrow C] \rightarrow [P \rightarrow (N \rightarrow C)]$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	1	1	1
0	1	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	0	0	0	1	1	1
0	0	1	0	1	1	1	1
0	0	0	0	1	1	1	1

Entonces es ya evidente que la conclusión encontrada dependerá de forma condicional de la premisa N introducida.

9) *Demostración por reducción al absurdo (A.b.).* Esta regla nos dice que si de unas premisas $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ y la proposición R se deduce una contradicción, de la conjuntiva $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ se deduce la proposición $\neg R$.

El esquema nos dice que si

$$\begin{array}{lll} & P_1 & \\ & P_2 & \\ \text{premisas} & \vdots & \\ & P_n & \\ & R & \\ \hline \text{conclusión} & (A \wedge \neg A) & \text{contradicción} \end{array}$$

entonces:

$$\begin{array}{l|l} & P_1 \\ & P_2 \\ \text{premisas} & \vdots \\ & P_n \\ \hline \text{conclusión} & \neg R \end{array}$$

En efecto: llamemos a la conjuntiva P.

$$P = P_1 \wedge P_2 \wedge \ldots \wedge P_n$$

Entonces, por la demostración condicional:

$$\begin{array}{l|c} \text{premisa} & P \\ \text{premisa} & R \\ \hline \text{conclusión} & A \wedge \neg A \end{array} \quad \xrightarrow{\text{(D.C.)}} \quad \begin{array}{l|c} \text{premisa} & P \\ \hline \text{conclusión} & R \rightarrow A \wedge \neg A \end{array}$$

Pero $(R \rightarrow A \wedge \neg A)$ es equivalente a $\neg(A \wedge \neg A) \rightarrow \neg R$. Es decir,

$$(\neg A \vee A) \rightarrow \neg R$$

Aplicando ahora la demostración condicional al revés:

$$\begin{array}{l|c} \text{premisa} & P \\ \hline \text{conclusión} & (\neg A \vee A) \rightarrow \neg R \end{array} \quad \xleftarrow{\text{(C.D.)}} \quad \begin{array}{l|c} \text{premisa} & P \\ \text{premisa} & \neg A \vee A \\ \hline \text{conclusión} & \neg R \end{array}$$

y puesto que $\neg A \vee A$ es universalmente válida, la podemos suprimir, quedando pues que de P solo, se ha deducido $\neg R$.
Entonces, podemos utilizar este tipo de demostración para obtener una conclusión deseada. Para ello seguiremos los tres pasos siguientes:

1) Introduciremos como premisa la negación de la conclusión que se desea obtener.
2) Buscamos una contradicción.
3) Inferiremos la conclusión deseada por demostración por reducción al absurdo.

Podemos aclarar estos tres pasos en un caso general del siguiente modo:

1.—Deseamos demostrar C a partir de P_1, P_2 ... P_n Entonces introducimos como premisa $\neg$ C.

$$\begin{array}{c} P_1 \\ P_2 \\ \vdots \\ P_n \\ \neg C \end{array}$$

2.—Buscamos una contradicción.

$$\begin{array}{|l} P_1 \\ P_2 \\ \vdots \\ P_n \\ \hline \neg C \\ \hline Q \wedge \neg Q \end{array}$$

3.—Se deduce C por Ab.

Utilización de estas reglas de inferencia

La estructura general de un teorema es "hipótesis $\rightarrow$ tesis". Supongamos que se trata de demostrar un teorema cuya hipótesis sea una conjuntiva de varias premisas $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ y cuya tesis sea una condicional $A \rightarrow B$. Veamos cómo lo haríamos por demostración *condicional* y por reducción al *absurdo.*

a) Por demostración condicional:
Partiremos como hipótesis de $P_1 \wedge P_2 \wedge P_n \wedge A$, y trataremos de deducir de ella la proposición B.

$$\left(P_1 \quad P_2 \wedge \ldots \wedge P_n \wedge A\right) \rightarrow B$$

entonces, por demostración condicional del conjunto de premisas solo, se deduce $A \rightarrow B$.

$$\left(P_1 \wedge P_2 \wedge \ldots \wedge P_n\right) \rightarrow (A \rightarrow B)$$

b) Por reducción al absurdo:

1.—Introducimos la negación de la tesis como una premisa más. La negación de la tesis es $\neg (A \rightarrow B)$. Teniendo en cuenta ahora la equivalencia $(A \rightarrow B) \Longleftrightarrow (\neg A \vee B)$. Luego $\neg (A \rightarrow B) \Longleftrightarrow \neg (\neg A \vee B)$, y por leyes de Morgan, $\neg (A \rightarrow B) \Longleftrightarrow A \wedge \neg B$.
Luego añadimos como hipótesis $A \wedge \neg B$.

$$P_1 \wedge P_2 \wedge \ldots \wedge P_n \wedge A \wedge \neg B$$

2.—Con estas premisas buscamos una contradicción $Q \wedge \neg Q$.

$$\left(P_1 \wedge P_2 \wedge \ldots \wedge P_n \wedge A \wedge \neg B\right) \rightarrow (Q \wedge \neg Q)$$

3.—Por reducción al absurdo queda demostrado el teorema.
En esta demostración por reducción al absurdo, lo más importante es que se toman como premisas ciertas el antecedente y la negación del consecuente de la condicional que tratamos de demostrar.

0-7 CALCULO CUANTIFICADOR ELEMENTAL

Dada una función proposicional $p(x)$, en el caso en que existe por lo menos un objeto a tal que $p(a)$ sea cierta, esto lo representaremos:

$$\exists x,\ x = a \text{ tal que } p(x) \text{ es cierto}$$

El símbolo $\exists$ lo llamaremos cuantificador existencial, y su presencia nos asegura que podemos sustituir la vairable (o variables) de una función proposicional por alguna constante y ser cierta la proposición resultante.
En el caso particular de que exista uno y solo un objeto $\underline{a}$ que haga cierta $p(x)$, representaremos el existencial por

$$\exists^* \text{ ó } \exists!$$

A partir de $\exists$ vamos a definir un nuevo cuantificador.
Consideremos la expresión

$$\neg (\exists\, x \mid \neg\, p(x))$$

es decir, no existe ningún x tal que haga cierta la negación de $p(x)$.
A este cuantificador lo representaremos

$$\forall$$

que se lee, "para todo x, $p(x)$", y se llama cuantificador universal.
Los enunciados con cuantificadores se resisten a ser tratados con el cálculo proposicional establecido y es necesario concretar algunas reglas que se desprenden de las definiciones de los cuantificadores y de las conexiones lógicas:

1 $$\forall x\,[p(x) \wedge q(x)] \Longleftrightarrow [\forall\, x, p(x)] \wedge [\forall\, x, q(x)]$$

2 $$\forall\, x\,[p(x) \vee q(x)] \not\Leftrightarrow [\forall\, x, p(x)] \vee [\forall\, x, q(x)]$$

3 $$\exists x\,[p(x) \wedge q(x)] \Rightarrow [\exists x, p(x)] \wedge [\exists x, q(x)]$$

4 $$\exists x\,[p(x) \vee q(x)] \Longleftrightarrow [\exists x, p(x)] \vee [\exists x, q(x)]$$

Cuando el universo del discurso está limitado a un número finito de objetos $a, b, c, \ldots h$, el cuantificador existencial equivale a un desarrollo en disyunciones:

$$\exists x\; p(x) \Longleftrightarrow p(a) \vee p(b) \vee p(c) \vee \ldots \vee p(h)$$

y el cuantificador universal a un desarrollo en conjunciones:

$$\forall x\,[p(x) \Rightarrow q(x)] \Longleftrightarrow [p(a) \Rightarrow q(a)] \wedge [p(b) \Rightarrow q(b)] \wedge \ldots \wedge [p(h) \Rightarrow q(h)]$$

Nota: Con el símbolo $\not\Leftrightarrow$ indicamos "no equivale".

La negación de los cuantificados se rige por:

5 $$\neg\,[\exists x, p(x)] \Longleftrightarrow \forall\, x\,[\neg\, p(x)]$$

La negación de "la existencia de x que cumplan p" es equivalente a que "todo x cumple $\neg\, p$".

6 $$\neg\,[\forall\, x, p(x)] \Longleftrightarrow \exists x\,[\neg\, p(x)]$$

y esto se deriva de las leyes de Morgan, en efecto, para el primer caso (5) será

$$\neg\,[\exists x\ p(x)] \iff \neg\,[p(a) \vee p(b) \vee p(c) \vee \ldots \vee p(h)] \iff$$
$$\iff [\neg\, p(a)] \wedge [\neg\, p(b)] \wedge [\neg\, p(c)] \wedge \ldots \wedge [\neg\, p(h)] \iff$$
$$\iff \forall x\ [\neg\, p(x)]$$

y en el segundo caso (propiedad 6)

$$\neg\,[\forall x\ p(x)] \iff \neg\,[p(a) \wedge p(b) \wedge p(c) \wedge \ldots \wedge p(h)] \iff$$
$$\iff [\neg\, p(a)] \vee [\neg\, p(b)] \vee \ldots \vee [\neg\, p(h)] \iff$$
$$\iff \exists x\ [\neg\, p(x)]$$

0-8 EL METODO DEDUCTIVO

El estudio de una determinada ciencia exige el conocimiento del método que se emplea para construirla, pues sólo en este caso seremos capaces de llegar a entenderla de una manera creadora.
A continuación intentaremos exponer los principios fundamentales que constituyen el método deductivo aplicado en lógica y matemáticas.
Al construir una determinada disciplina matemática, podemos distinguir entre:

A) **Los términos:**

A. 1.—*Los términos primitivos o indefinibles.*

Serán un pequeño número de expresiones que nos parezcan inmediatamente comprensibles.

Ejemplo: punto:

Los emplearemos sin explicitar su significado. Cualquier otro término utilizado sólo podrá serlo si queda perfectamente establecido su significado a partir de estos términos primitivos.

A. 2.—*Los términos definidos.*

A partir de los términos primitivos o indefinibles podremos establecer otros de significado preciso.
La proposición utilizada para establecer los términos definidos a partir de los primitivos se llama *Definición.*

Ejemplo (a partir de punto): establecer el término recta.

B) **Enunciados:**

Procederemos con los enunciados de un modo análogo a como hemos hecho con los términos.

B. 1.—*Enunciados primitivos o axiomas.*

Son proposiciones que aceptaremos como ciertas sin establecer su validez de ningún modo.

Ejemplo (en Geometría Euclídea):

"En un plano, por un punto exterior a una recta, pasa una y sólo una recta paralela a aquella".

B. 2.—*Enunciados demostrados o teoremas.*

Son todos aquellos enunciados cuya validez haya sido establecida utilizando solo axiomas, definiciones y términos primitivos.

El proceso por el cual se establecen los teoremas se llama *Demostración.*

La lógica matemática es una disciplina construida de acuerdo con todos estos supuestos. Cualquier otra disciplina, construida de acuerdo con ésto, debe presuponer la lógica, aunque algunos necesitan presuponer varias disciplinas, llamadas *Disciplinas Precedentes,* para poder construirse. Por tanto, antes de comenzar la construcción de una disciplina dada, deben enumerarse las disciplinas precedentes.
El método de construcción de una teoría basado en los principios que acabamos de exponer exclusivamente, se llama *Método Deductivo* y a la teoría correspondiente, *Teoría Deductiva.*

0-8-1 MODELOS

Consideremos una teoría deductiva basada en un sistema de términos primitivos y de axiomas. Supongamos que la única *Disciplina Precedente* sea la lógica. Es decir, que la construcción de la teoría sólo presupone la lógica. Entonces, en ésta existirán unos variables proposicionales y unas fórmulas proposicionales. Los axiomas de la teoría son formas proposicionales en las que están contenidas las variables, ya citadas, que pueden reemplazarse, como sabemos, por los términos primitivos de una teoría concreta que son las proposiciones. Dados ahora unos ciertos objetos, podemos determinar si satisfacen todas las axiomas de la teoría, es decir, todas las formas proposicionales. Si ocurre esto, decimos que los objetos considerados constituyen un

Modelo o una *realización del sistema de axiomas* de nuestra teoría deductiva.

Puesto que los objetos satisfacen el sistema de axiomas de la teoría, el modelo satisfacerá todos los teoremas de la teoría; sin embargo, cuando pensamos en un teorema deducido de los axiomas, no lo relacionamos con ninguna propiedad concreta del modelo. En otras palabras, que para un sistema de axiomas de una teoría existen muchos modelos y ninguno de ellos es fundamental en la construcción de nuestra teoría. De esto podemos enunciar, pues:

"Todo teorema de una teoría deductiva dada es satisfecho por cualquier modelo del sistema de axiomas y, además, a todo teorema de la teoría corresponde una forma proposicional universalmente válida, demostrada por medio de la lógica, y que pone de manifiesto el hecho de que el teorema es cierto para cualquier substitución de sus variables por los objetos de cualquier modelo."

0-8-2 PROPIEDADES DEL SISTEMA DE AXIOMAS

a) *Independencia.*—Dos sistemas de proposiciones se llaman equivalentes, cuando toda proposición del primero puede deducirse de los del segundo; y recíprocamente, toda proposición del segundo puede derivarse del primero. Entonces, es evidente que trataremos de que nuestro sistema de axiomas sea independiente, es decir, que ninguno de los axiomas del mismo pueda deducirse de los demás, puesto que si esto ocurriese para algún axioma, este podría incluirse entre el conjunto de teoremas deducidos de la teoría.

b) *Consistencia.*—El sistema de axiomas se llama consistente, o no contradictorio, cuando de él no pueden deducirse dos proposiciones contradictorias. O, también, cuando dadas dos proposiciones contradictorias cualesquiera, una al menos no puede demostrarse a partir del sistema de axioma elegido.

c) *Completo.*—Un sistema de axiomas es completo si de todo par de enunciados contradictorios expresados en términos de la teoría y de las teorías precedentes, uno al menos puede ser demostrado. Se dice que un enunciado puede ser *refutado* en una teoría dada si se puede demostrar en ella el contradictorio del mismo.

Para una teoría deductiva cualquiera, nosotros buscaremos siempre sistemas de axiomas que reúnan las tres condiciones arriba expresadas.

TEMA 1 | CONJUNTOS OPERACIONES CON CONJUNTOS

1-1 CONJUNTO

El concepto de conjunto es en sí indefinible y tendremos que hacer referencia a la noción de pertenencia para poder establecerlo. En matemáticas hablamos de conjunto de elementos si existe una condición de pertenencia de los elementos al conjunto; o bien cuando se han enumerado todos los elementos del conjunto.
Así, un conjunto quedará establecido:

1) Por comprensión: Cuando se dé un *criterio de pertenencia,* propiedad que cumplen todos sus elementos.

$$A = \left\{ x \mid P(x) \right\}$$

Ejemplo: El conjunto de los números pares.

2) Por extensión: Cuando se enuncien todos los elementos del conjunto.

Ejemplo: El conjunto de las letras a, b, c, d.

Se utilizan, en general, letras mayúsculas para expresar los conjuntos: A, E, P(E), etcétera; y las letras minúsculas (latinas o griegas) para expresar los elementos: a, b, c, d - $\alpha, \beta, \gamma, \delta$.
Para formular la pertenencia o no pertenencia de los elementos a los conjuntos, se escribe:

"$x \in A$", que se lee: "el elemento x pertenece al conjunto A".
"$x \notin A$", que se lee: "el elemento x no pertenece al conjunto A".

En general, en matemáticas se utilizan símbolos que economicen la escritura y faciliten su comprensión. Dichos símbolos tienen un valor universal con independencia del idioma en que se exprese el matemático. Así:

$\forall$ "para todo"
$\exists$ "existe al menos uno"
$\exists!$, $\exists^*$ "existe uno y uno solo"
$|$ "tal que" "es tal que"
$\Rightarrow$ "implica"
$\Longleftrightarrow$ "equivale"

Definamos así en conjunto. Ejemplo, los múltiplos de 5 positivos:

$$E = \left\{ \forall\ x \mid x = 5n;\, n \in N \right\}$$

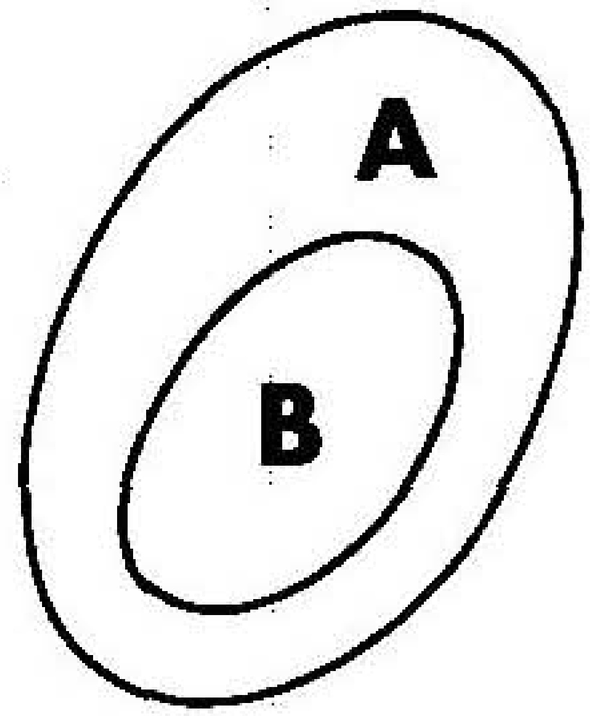
que se leería: "el conjunto E lo forman todos los elementos x tales que son de la forma $5n$, donde n recorre el conjunto de los números naturales.

1-2 SUBCONJUNTOS. RELACION DE INCLUSION

Un conjunto B es subconjunto de otro conjunto A, si todos los elementos de B. lo son de A.

Es decir, "B subconjunto de A" $\Longleftrightarrow \{\forall b \;\; b \in B \mid b \in A\}$

En diagramas de Venn-Euler se representaría:



Simbólicamente escribiremos:

$B \subset A$, que leeremos "B incluido en A"

Es evidente que:

$$\text{Si } (A \subset B \wedge B \subset C) \Rightarrow A \subset C$$

<u>Conjuntos Iguales:</u>
Si podemos formar

$A \subset B$ "todo elemento de A lo es de B"
$B \subset A$ "todo elemento de B lo es de A"

A y B tendrán los mismos elementos:

$$A = B$$

A será igual a B

1-3 CONJUNTO DE UN ELEMENTO

Dado un elemento a existe un solo conjunto $\{a\}$ definido

$$\{a\} = \{x \mid x = a\}$$

que es equivalente a decir

$x \in \{a\} \Longleftrightarrow x = a$

Este conjunto se llama conjunto de un solo elemento.
Será condición necesaria y suficiente para que un conjunto A sea de un solo elemento que A tenga elementos y que

$\forall x \in A \quad \forall y \in A \quad x = y$

1-4 CONJUNTO DE DOS ELEMENTOS

Dados dos elementos matemáticos *a* y *b* distintos existe un solo conjunto definido

$$\{a, b\} = \{x \mid x = a \vee x = b\}$$

que es equivalente a decir

$$z \in \{a\ b\} \Longleftrightarrow (z = a \vee z = b)$$

1-5 CONJUNTOS FINITOS

De igual forma a como hemos hecho para un elemento, y dos elementos, podríamos hacer para tres, cuatro, cinco, etcétera; los conjuntos así generados se llaman conjuntos finitos, los demás conjuntos se llaman infinitos.

1-6 OPERACIONES CON CONJUNTOS

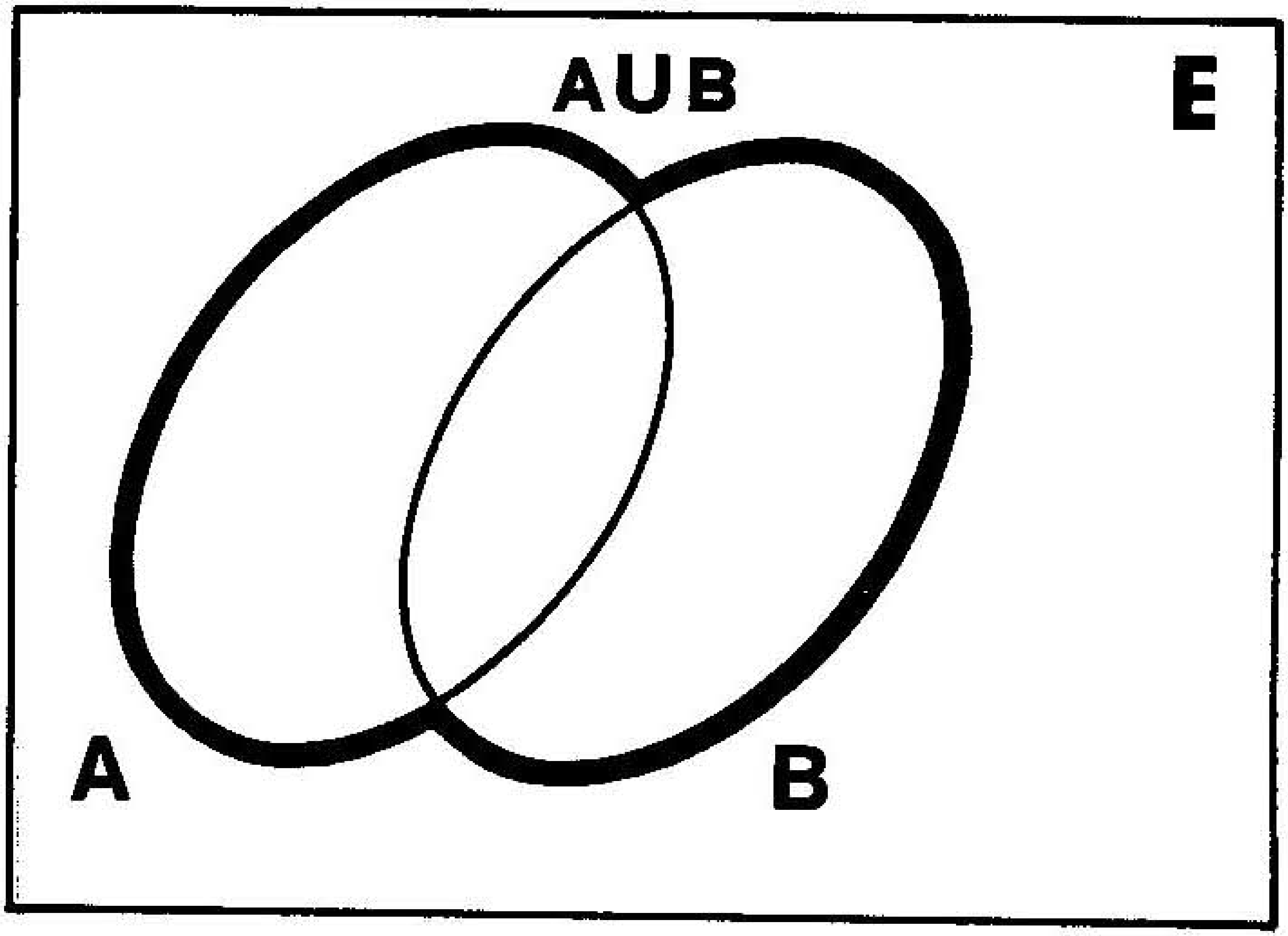
1) Reunión:

"Dados dos conjuntos A, B, llamaremos conjunto "reunión" de A y B, y lo representaremos A ∪ B, al conjunto formado por todos los elementos que lo son de A o de B."
O sea:

$$A \cup B = \{\forall x \mid x \in A \vee x \in B\}$$

Evidentemente:

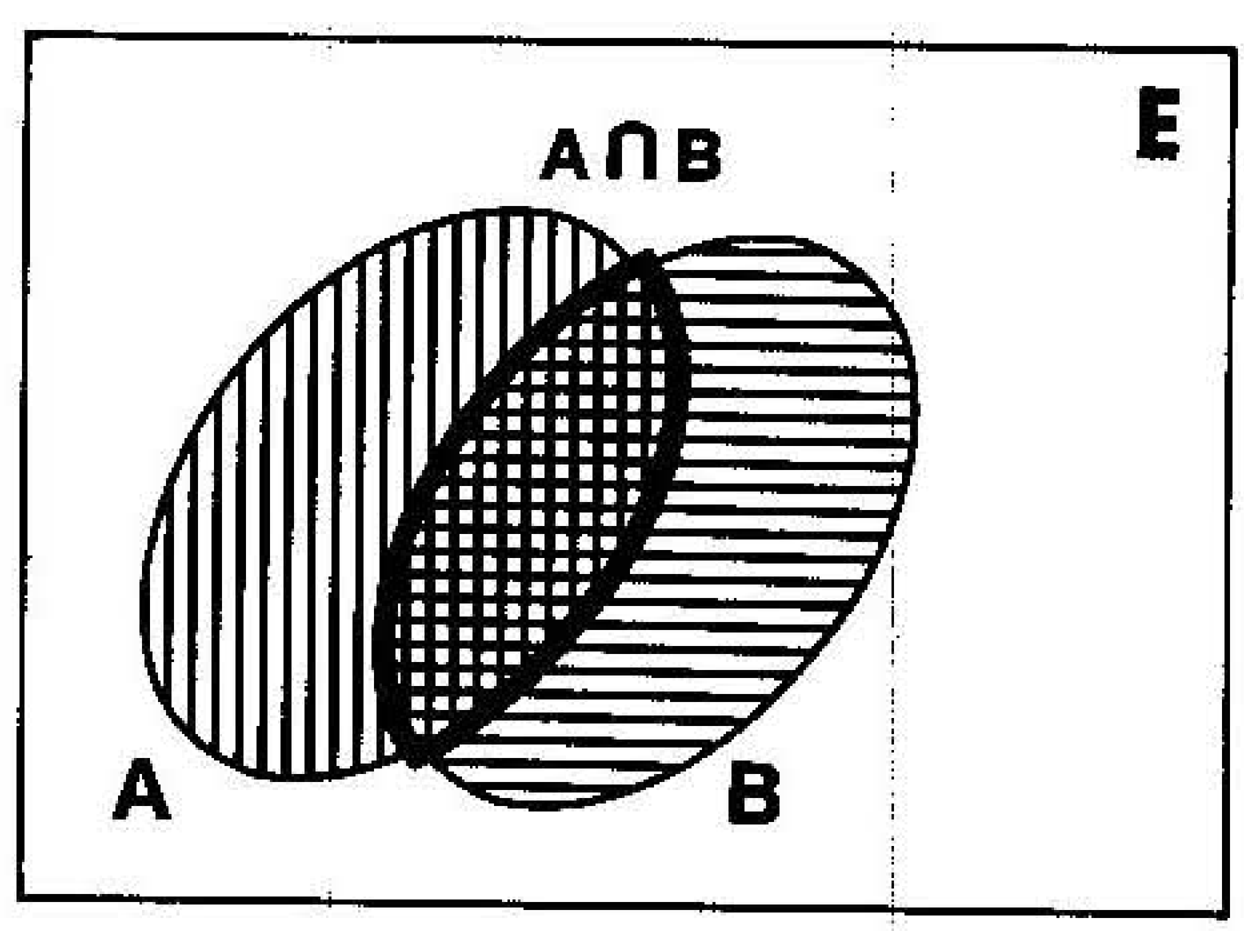
a) $A \cup B \subset E$
b) $A \subset A \cup B \quad B \subset A \cup B$



2) Intersección:

"Dados dos conjuntos A, B, llamaremos conjunto "intersección" de A y B, y lo representaremos $A \cap B$, al conjunto formado por todos los elementos que son al mismo tiempo de A y B."
Es decir: $A \cap B$ está formado por los elementos comunes de A y B

$$A \cap B = \left\{ \forall x \mid x \in A \text{ y } x \in B \right\}$$



Evidentemente:

a) $A \cap B \subset E$
b) $A \cap B \subset A \quad A \cap B \subset B$

1-7 PROPIEDADES DE LA REUNION Y LA INTERSECCION

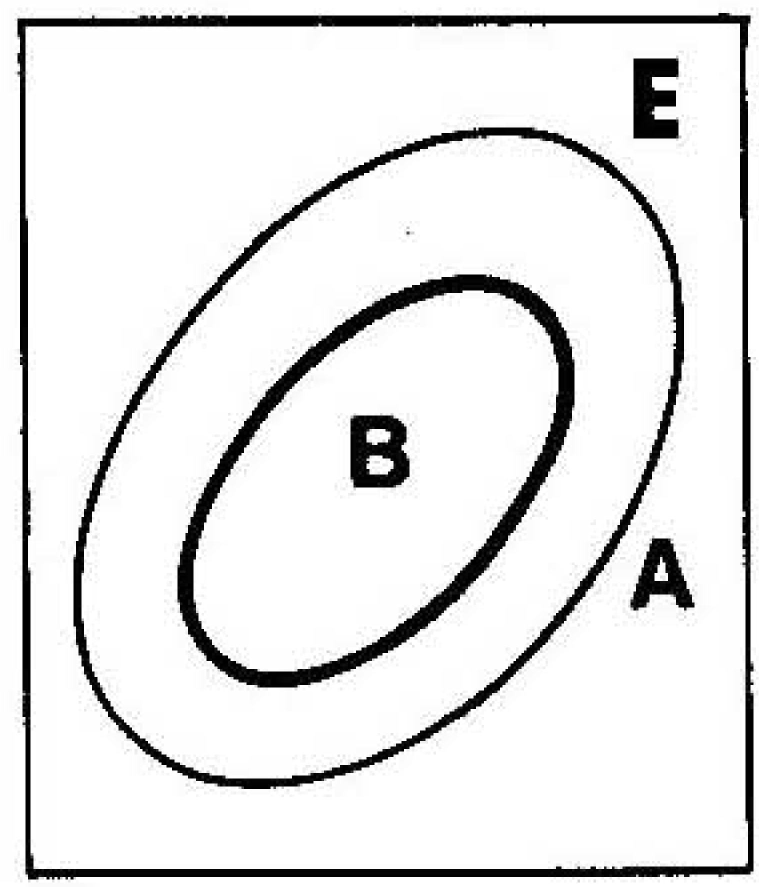
Siendo A, B, C subconjuntos de E.

P_1 : Idempotencia $\quad A \cup A = A \quad\quad A \cap A = A$

P_2 : Conmutativa $\quad A \cup B = B \cup A \quad\quad A \cap B = B \cap A$

P_3 : Asociativa $\quad A \cup (B \cup C) = (A \cup B) \cup C \quad\quad A \cap (B \cap C) = (A \cap B) \cap C$

P_4 : Absorción. Si $\quad B \subset A : A \cup B = A \quad\quad A \cap B = B$

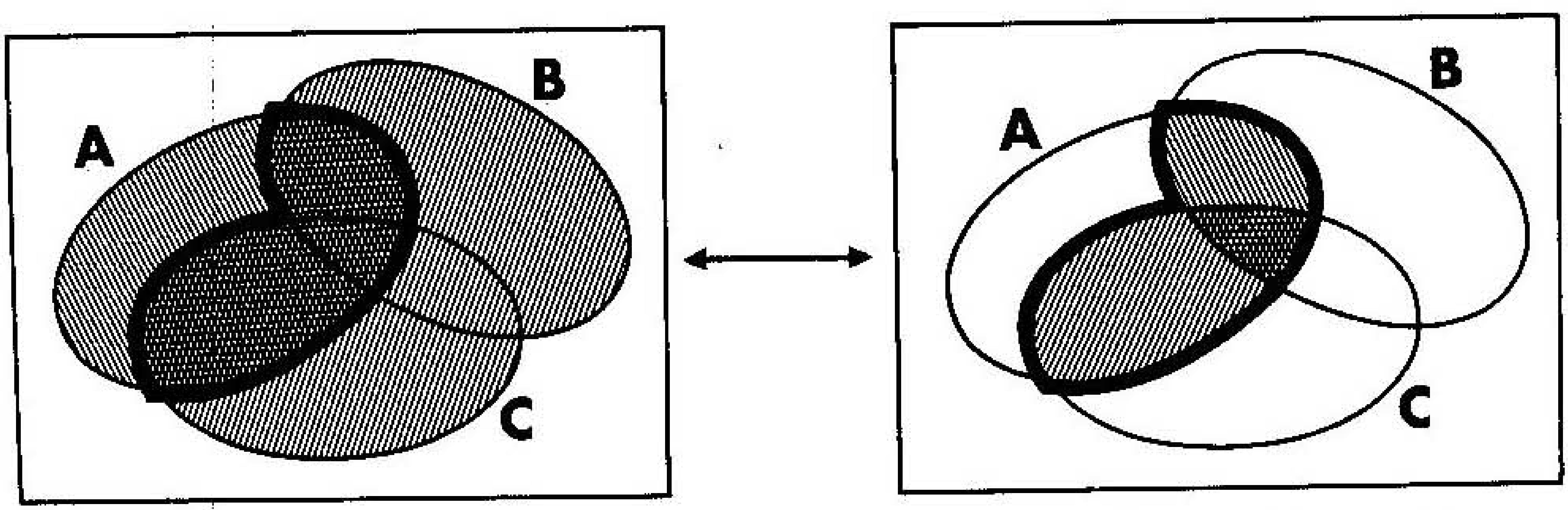


Estas propiedades son triviales.

P_5 : Distributividad:

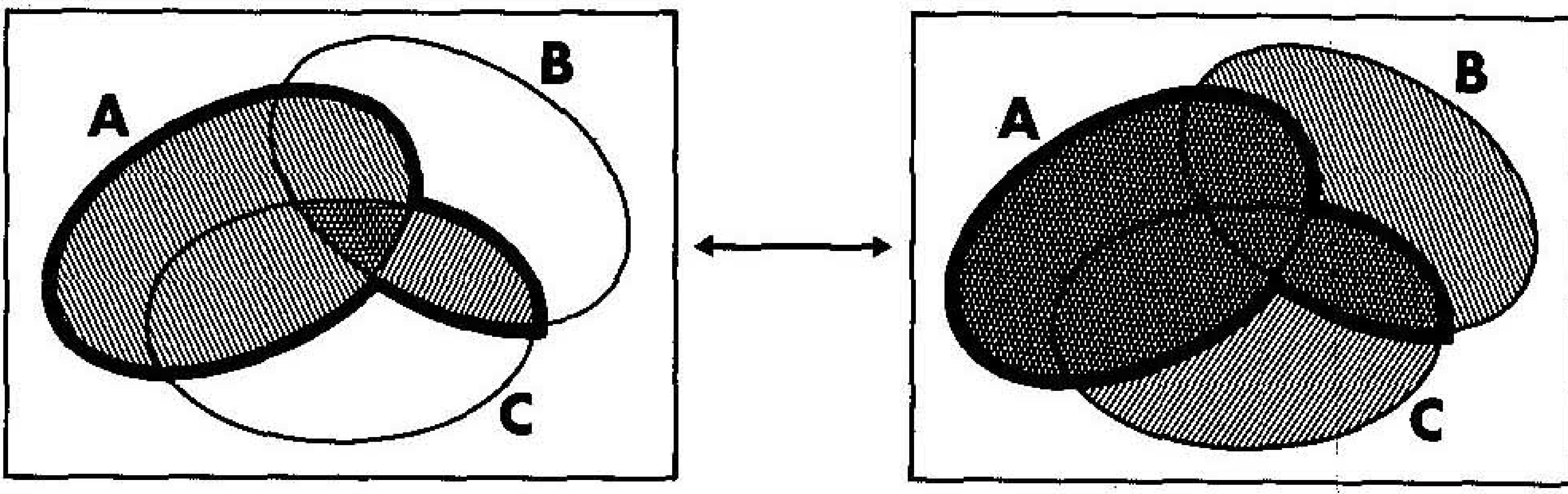
a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Vamos a demostrarlo con diagramas de Venn-Euler.



$A \cap (B \cup C) \longleftrightarrow (A \cap B) \cup (A \cup C)$

b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$



$A \cup \; (B \cap C) \longleftrightarrow (A \cup B) \; \cap \; (A \cup C)$

Podemos también demostrarlo sin recurrir a los diagramas.
En efecto:

a)

(1) Si $x \in A \cap (B \cup C) \Rightarrow \big(x \in A \wedge (x \in B \vee x \in C)\big)$

(2) Si $x \in (A \cap B) \cup (A \cap C) \Rightarrow \big((x \in A \wedge x \in B) \vee (x \in A \wedge x \in B)\big)$

y según vimos, por álgebra de proposiciones (distributiva de $\wedge$ respecto a $\vee$), son equivalentes las proposiciones (1) y (2).

o sea:

$$\{x \in A \cap (B \cup C)\} \Longleftrightarrow \{x \in (A \cap B) \cup (A \cap C)\}$$

luego, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

b) de idéntica forma:

Si $x \in A \cup (B \cap C) \Rightarrow \big(x \in A \vee (x \in B \wedge x \in C)\big)$

Si $x \in (A \cup B) \cap (A \cup C) \Rightarrow \Big((x \in A \vee x \in B) \wedge (x \in A \vee x \in C)\Big)$

que por la propiedad distributiva de $\vee$ respecto de $\wedge$ en álgebra de proposiciones, se puede escribir:

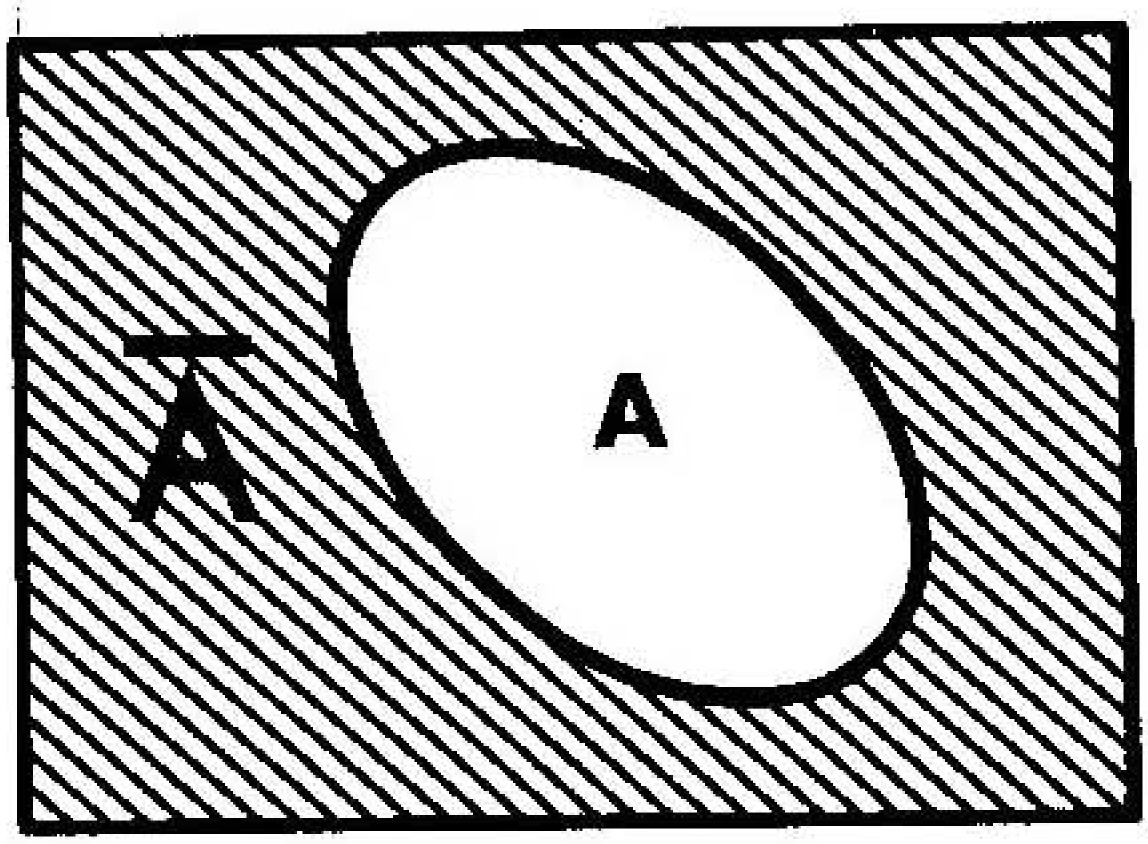
$$x \in A \vee (x \in B \wedge x \in B \wedge x \in C)$$

luego son equivalentes las proposiciones:

$$\{x \in A \cup (B \cap C)\} \Longleftrightarrow \{x \in (A \cup B) \cap (A \cup C)\}$$

de donde:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$



1-8 CONJUNTO COMPLEMENTARIO

Dado un conjunto E y un subconjunto A de E, $A \subset E$ llamaremos complementario de A con relación a E, C^A_E o bien A, o bien A′, al conjunto de todos los elementos de E que no son de A.

O sea:

$$C^A_E = \overline{A} = \left\{ x \mid x \in E \ \text{ y } \ x \notin A \right\}$$

Evidentemente, si $A \not\subset E$, no tiene ningun sentido hablar de C^A_E

EJEMPLO:

Sea Z el conjunto de los enteros,
$Z^+ \cup \{o\}$ el conjunto de los enteros positivos y el cero

$$\complement_Z (Z^+ \cup \{o\}) = Z^-$$

será el conjunto de los enteros negativos.

1-9 CONJUNTO VACIO

Por definición llamaremos conjunto vacío y lo representaremos ϕ al complementario de E respecto de E.

$$\complement_E E = \phi$$

es decir:

$$\phi = \{x \mid x \in E \quad y \quad x \notin E\}$$

Evidentemente el conjunto vacío carece de elementos porque ($x \in E$ y $x \notin E$) es una contradicción y no hay ningún elemento que haga cierta esa contradicción.

Es trivial que

1) $\phi \subset E$ $\quad \forall$ E (es subconjunto de cualquier conjunto)
2) $\forall$ A $\quad A \cup \phi = A$
3) $\forall$ A $\quad A \cap \phi = \phi$

Llamaremos *conjuntos disjuntos* a dos conjuntos A,B tales que $A \cap B = \phi$

1-10 PROPIEDADES DEL CONJUNTO COMPLEMENTARIO

1) Complementariedad

$$A \cup A' = E$$
$$A \cap A' = \phi$$

2) Involución

$$(\overline{\overline{A}}) = A$$

El complementario del complementario de A es el propio A
En efecto:

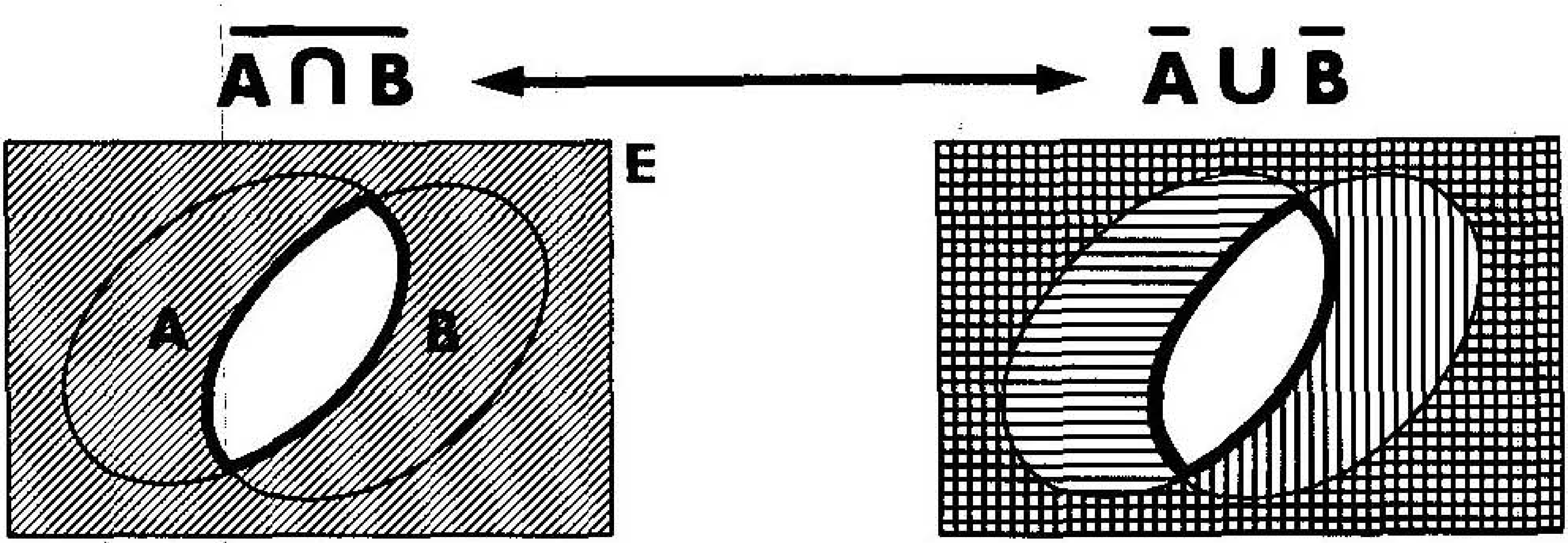
$$(\overline{\overline{A}}) = \left\{ x \mid x \in E \wedge x \notin \overline{A} \right\} = \left\{ x \mid x \in E \wedge x \in A \right\} = A$$

3) Leyes de Morgan.

1.ª Ley: $\overline{A \cap B} = \overline{A} \cup \overline{B}$

"El conjunto complementario de la intersección de dos conjuntos es la reunión de sus complementarios."

En efecto: Por los diagramas de Venn-Euler



Asimismo, se puede demostrar:

$x \in \overline{A} \cup \overline{B} \Longleftrightarrow (x \in \overline{A} \vee x \in \overline{B})$ por definición de reunión

y $(x \in \overline{A} \vee x \in \overline{B}) \Longleftrightarrow (x \notin A \vee x \notin B)$ por definición de complementario

y $(x \notin A \vee x \notin B) \Longleftrightarrow (x \notin A \wedge B)$ por álgebra proposicional y $(x \notin A \wedge B) \Longleftrightarrow (x \notin A \cap B)$ por definición de intersección

y $(x \notin \overline{A} \cap \overline{B}) \Longleftrightarrow (x \in \overline{A \cap B}$ por definición de complementario.

Luego

$$(x \in \overline{A} \cup \overline{B}) \Longleftrightarrow (x \in \overline{A \cap B})$$

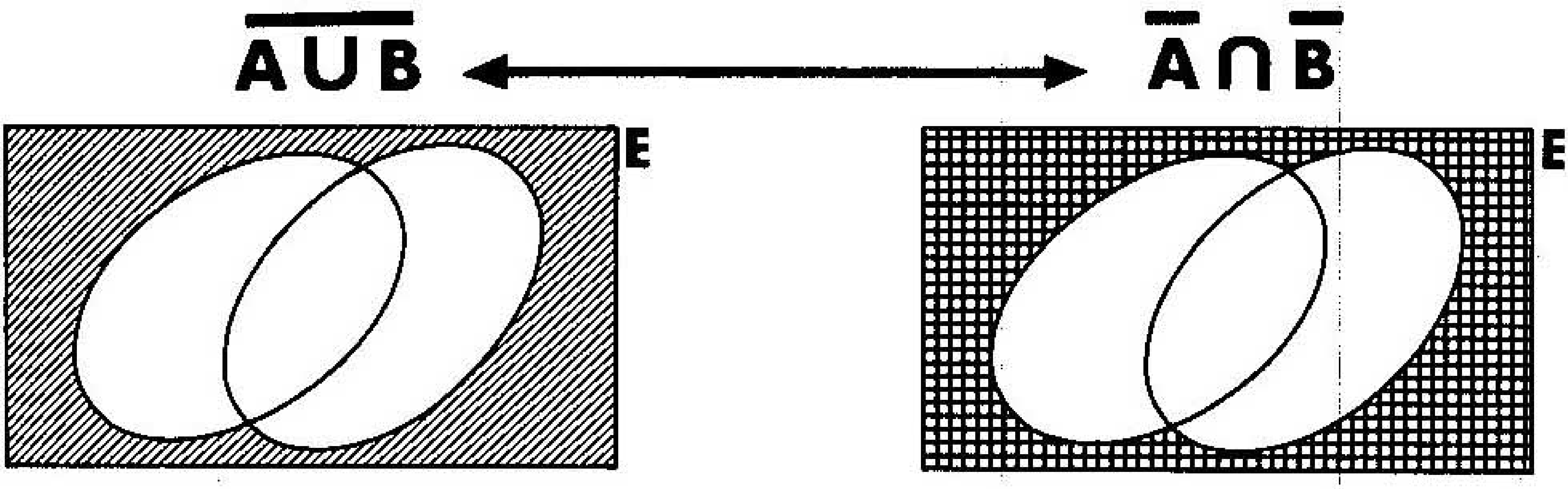
o sea:

$$\overline{A} \cup \overline{B} = \overline{A \cap B} \quad \text{c.q.d.}$$

2.ª Ley: $\overline{A \cup B} = \overline{A} \cap \overline{B}$

"El conjunto complementario de la reunión de dos conjuntos es la intersección de sus complementarios."

En efecto: Por diagramas de Venn-Euler



Y también se puede demostrar

$x \in \overline{A} \cap \overline{B} \Longleftrightarrow (x \in \overline{A} \wedge x \in \overline{B})$ por definición de intersección

$(x \in \overline{A} \wedge x \in \overline{B}) \Longleftrightarrow (x \notin A \wedge x \notin B)$ por definición de complementario

$(x \notin A \wedge x \notin B) \Longleftrightarrow x \notin (A \vee B)$ por álgebra proposicional

$(x \notin (A \vee B)) \Longleftrightarrow (x \notin A \cup B)$ por definición de reunión

$(x \notin A \cup B) \Longleftrightarrow (x \in \overline{A \cup B})$ por definición de complementario.

Luego

$$(x \in \overline{A} \cap \overline{B}) \iff (x \in \overline{A \cup B})$$

o sea:

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \qquad \text{c.q.d.}$$

1-11 PARTICION NUMERABLE DE UN CONJUNTO E

Dado un conjunto E, diremos que hemos establecido una partición de E si se determinan subconjuntos no vacíos de E: $A_1\ A_2 \ldots A_n$, disjuntos entre sí, y tales que reunidos dan E.
Es decir, tendremos una partición si:

a) $A_i \subset E \quad \forall i \in I \quad I = \{1, \ldots, n\}$ (I conjunto de indices)

b) $A_1 \cup A_2 \cup \ldots \cup A_n = E$

c) $A_i \cap A_j = \phi \quad \text{si } i \neq j$

1-12 CONJUNTO DE LAS PARTES DE E: P (E)

Dado un conjunto E, llamaremos conjunto de las partes de E al conjunto formado por todos los subconjuntos posibles de E. Lo representaremos P (E)

$$P(E) = \{A \mid A \subset E\}$$

Es obvio que:

a) $\phi \in P(E)$ y $E \in P(E)$

Si se tratara de un conjunto E finito, por ejemplo $E = \{a, b, c, d\}$, el conjunto P(E) estaría formado por todos los subconjuntos que pudiéramos formar de 4,3,2,1,0 elementos. Es decir:

$$P(E) = \{\phi, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\},$$
$$\{c,d\}, \{a,b,c\}, \{a,b,d\}, \{b,c,d\}, \{a,c,d\}, \{a,b,c,d\}\}$$

o sea, el número total de elementos que P(E) será

$$\sum_{i=0}^{i=4} \binom{4}{i}$$

que es el desarrollo de $(1+1)^4 = 2^4$

En general, si E es finito, de n elementos, los elementos de P(E) vendrán dados por 2^n.

1-13 ESTRUCTURA DEL CONJUNTO P(E)

Consideremos las operaciones anteriormente definidas:

- $\cup$ = reunión
- $\cap$ = intersección
- $\complement$ = complementación

en el conjunto P(E).

Es evidente que:

a) $\forall\ A \in P(E)$ y $\forall\ B \in P(E) \quad A \cup B \in P(E)$

pues $A \subset E \quad B \subset E \Rightarrow A \cup B \subset E$ y por definición de Parte, $A \cup B \in P(E)$.

b) $\forall\ A \in P(E)$ y $\forall\ B \in P(E) \quad A \cap B \in P(E)$

ya que $A \subset E$ y $B \subset E \Rightarrow A \cap B \subset E$, y por definición de Parte, $A \cap B \in P(E)$

c) $\forall\ A \in P(E) \quad \complement_E^A \in P(E)$

En efecto, ya que $A \subset E \Rightarrow \complement_E^A \subset E$; luego, $\complement_E^A \in P(E)$

lo que establece que estas operaciones definidas en P(E) dan para cualesquiera elementos de P(E) resultados que también son elementos P(E). Esto sugiere una generalización del Algebra Elemental en la Teoría de Conjuntos.

En general, una operación definida en un conjunto, si éste es finito, se puede expresar por una tabla con el conjunto P(E); siendo $E = \{a\ b\ c\}$, vamos a construir las tablas para $\cup$ $\cap$ y $\complement$:

$$P(E) = \{\phi\ \{a\}\ \{b\}\ \{c\}\ \{a\,b\}\ \{a\,c\}\ \{b\,c\}\ \{a\,b\,c\}\}$$

Operación reunión

$\cup$	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{ab\}$	$\{a\,c\}$	$\{bc\}$	$\{a\,b\,c\}$
ϕ	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{ab\}$	$\{ac\}$	$\{bc\}$	$\{abc\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{ab\}$	$\{ac\}$	$\{ab\}$	$\{ac\}$	$\{abc\}$	$\{abc\}$
$\{b\}$	$\{b\}$	$\{ab\}$	$\{b\}$	$\{bc\}$	$\{ab\}$	$\{abc\}$	$\{bc\}$	$\{abc\}$
$\{c\}$	$\{c\}$	$\{ac\}$	$\{bc\}$	$\{c\}$	$\{abc\}$	$\{ac\}$	$\{bc\}$	$\{abc\}$
$\{ab\}$	$\{ab\}$	$\{ab\}$	$\{ab\}$	$\{abc\}$	$\{ab\}$	$\{abc\}$	$\{abc\}$	$\{abc\}$
$\{ac\}$	$\{ac\}$	$\{ac\}$	$\{abc\}$	$\{ac\}$	$\{abc\}$	$\{ac\}$	$\{abc\}$	$\{abc\}$
$\{bc\}$	$\{bc\}$	$\{abc\}$	$\{bc\}$	$\{bc\}$	$\{abc\}$	$\{abc\}$	$\{bc\}$	$\{abc\}$
$\{abc\}$	$\{abc\}$	$\{abc\}$	$\{abc\}$	$\{abc\}$	$\{abc\}$	$\{abc\}$	$\{abc\}$	$\{abc\}$

Operación intersección

$\cap$	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{ab\}$	$\{ac\}$	$\{bc\}$	$\{abc\}$
ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ
$\{a\}$	ϕ	$\{a\}$	ϕ	ϕ	$\{a\}$	$\{a\}$	ϕ	$\{a\}$
$\{b\}$	ϕ	ϕ	$\{b\}$	ϕ	$\{b\}$	ϕ	$\{b\}$	$\{b\}$
$\{c\}$	ϕ	ϕ	ϕ	$\{c\}$	ϕ	$\{c\}$	$\{c\}$	$\{c\}$
$\{ab\}$	ϕ	$\{a\}$	$\{b\}$	ϕ	$\{ab\}$	$\{a\}$	$\{b\}$	$\{ab\}$
$\{ac\}$	ϕ	$\{a\}$	ϕ	$\{c\}$	$\{a\}$	$\{ac\}$	$\{c\}$	$\{ac\}$
$\{bc\}$	ϕ	ϕ	$\{b\}$	$\{c\}$	$\{b\}$	$\{c\}$	$\{bc\}$	$\{bc\}$
$\{abc\}$	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{ab\}$	$\{ac\}$	$\{bc\}$	$\{abc\}$

Operación complementación

A	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{ab\}$	$\{ac\}$	$\{bc\}$	$\{abc\}$
C_E^A	$\{abc\}$	bc	$\{ac\}$	$\{ab\}$	$\{c\}$	$\{b\}$	$\{a\}$	ϕ

1-14 ALGEBRA DE BOOLE

En general, se denomina álgebra de Boole a una estructura algebráica defininida sobre un conjunto sobre el que se definen tres operaciones $\wedge, \vee, -$, establecidas con las propiedades siguientes:

A) Para $\wedge, \vee$

- *a)* indempotencia
- *b)* asociatividad
- *c)* conmutatividad
- *d)* absorción
- *e)* doble distributividad (de $\wedge$ respecto de $\vee$ y de $\vee$ respecto de $\wedge$).

B) Para $\wedge, \vee, -$

a) complementariedad
b) dualidad (leyes de Morgan)

Luego [P (E),∪,∩,∁] constituye el álgebra de Boole del conjunto Partes de E. Esta álgebra de Boole se denomina CONCRETA.
Si el conjunto E lo formara un solo elemento $E = \{x\}$, entonces $P(E) = \{\phi\ E\}$ tendría dos elementos. En este caso el álgebra de Boole concreta se reduce a las tablas

∪	E	ϕ
E	E	E
ϕ	E	ϕ

∩	E	ϕ
E	E	ϕ
ϕ	ϕ	ϕ

A	E	ϕ
C_E^A	ϕ	E

Esta álgebra de Boole (del tipo —todo o nada—) es de sumo interés para el estudio de redes eléctricas en las calculadoras [donde pasa o no pasa corriente por una conexión].
Estudiaremos también un álgebra de Boole cuando hablemos de sucesos estocásticos.

TEMA 2 | PRODUCTO DE CONJUNTOS APLICACIONES APLICACIONES ENTRE CONJUNTOS FINITOS COMBINATORIA

2-0 DEFINICION DE PAR

Dados dos objetos matemáticos x, y, llamaremos par a un nuevo objeto (x, y) en el que es fundamental el orden en que están dados, y tal que $(x, y) = (u, v) \iff (x = u \wedge y = v)$.

Generalizando, llamaremos terna a tres objetos dados (x, y, z) y, como antes, se tendrá que cumplir $(x, y, z) = (u, y, w) \Longleftrightarrow (x = u, y = v, z = w)$.

2-1 DEFINICION DE PRODUCTO CARTESIANO DE DOS CONJUNTOS

Dados los conjuntos A y B, llamaremos conjunto producto de A por B y lo representaremos A x B al conjunto formado por todos los pares formados por un elemento de A y otro de B.

$$A \times B = \left\{ \forall\ (a, b) \mid a \in A \wedge b \in B \right\}$$

o también

$$z \in A \times B \Longleftrightarrow \left(\exists x \in A \wedge \exists y \in B \mid z = (x, y) \right)$$

2-1-1 PROPIEDADES

$$a)\ A \times B = \phi \Longleftrightarrow (A = \phi \vee B = \phi)$$

"Si A x B es igual a ϕ, esto es equivalente a $A = \phi$ o $B = \phi$."

$\Rightarrow$ En efecto, si $A \times B$ es el conjunto ϕ, no existe ninguna pareja $(x\ y)$ que pertenezca a $A \times B$, lo que implica o bien no existe ninguna x que pertenece a A o ninguna y que pertenezca a B.

$\Leftarrow$ También si $A = \phi$ o $B = \phi$, no se podrá formar ninguna pareja $(x\ y)$ donde $x \in A$ e $y \in B$, luego $A \times B = \phi$.

$$b)\ A' \times B' \subset A \times B \Longleftrightarrow A' \subset A \text{ y } B' \subset B$$

En efecto:

$\Rightarrow$ Para cualquier $(x\ y) \in A' \times B'$ se cumplirá $(x\ y) \in A \times B$

pero

$$(x\ y) \in A' \times B' \Rightarrow x \in A' \wedge y \in B'$$

y

$$(x\ y) \in A \times B \Rightarrow x \in A \wedge y \in B$$

luego

$$\forall\ X \in A' \Rightarrow x \in A \Rightarrow A' \subset A$$

$$\forall\ y \in B' \Rightarrow y \in B \Rightarrow B' \subset B$$

$\Leftarrow$ Si $A' \subset A$ y $B' \subset B$ entonces para cualquier pareja $(x\ y) \in A' \times B'$ se cumplirá

$$(x\ y) \in A' \times B' \Rightarrow x \in A', \text{ pero como } A' \subset A \Rightarrow x \in A$$

$$(x\ y) \in A' \times B' \Rightarrow y \in B', \text{ y como } B' \subset B \Rightarrow x \in B$$

Luego para toda $(x\ y) \in A' \times B', x \in A \wedge y \in B$

luego

$$A' \times B' \subset A \times B$$

c) Es evidente que $A \times B \neq B \times A$. Es decir, el producto cartesiano no es conmutativo.

2-1-2 PRODUCTO DE VARIOS CONJUNTOS

Dados los conjuntos $A_1\ A_2\ A_3 \ldots A_n$, llamaremos conjunto producto de $A_1 \times A_2 \times A_3 \times \ldots \times A_n$ al conjunto formado por todos los elementos $z = (a_1\ a_2\ \ldots\ a_n)$, donde $a_1 \in A_1\ a_2 \in A_2 \ldots a_n \in A_n$.

$$A_1 \times A_2 \times A_3 \times \ldots \times A_n = \left\{(a_1\ a_2\ a_3 \ldots a_n) \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge \ldots \wedge a_n \in A_n\right\}$$

Si se tratara de conjuntos iguales podríamos escribir:

$$A \times A = A^2 \qquad A \times A \times A = A^3 \quad \text{etc.}$$

2-2 DEFINICION DE GRAFO

Llamaremos grafo G a todo conjunto cuyos elementos sean parejas.

$$G = \left\{(x\ y)\right\}$$

Dada una pareja, llamaremos primera proyección de ella:

$pr_1\ (x\ y) = x$ a su primer elemento

y segunda proyección:

$pr_2\ (x\ y) = y$ a su segundo elemento.

Al conjunto de las primeras proyecciones de G le llamaremos *conjunto de definición X*

$$X = \{ pr_1\ (x\ y) \quad \forall\ (x\ y) \in G \}$$

Y al conjunto de las segundas proyecciones de G, *conjunto de valores Y*

$$Y = \{ pr_2\ (x\ y)\ \forall\ (x\ y) \in G \}$$

Es evidente que:

$$G \subset X \times Y$$

es decir, que G es un subconjunto del producto cartesiano de su conjunto de definición por su conjunto de valores.

EJEMPLO:

$$G = \{ (a\ 1)\ (a\ 2)\ (b\ 3)\ (c\ 2)\ (c\ 4) \}$$

Conjunto de definición $X = \{ a\ b\ c \}$

Conjunto de valores $Y = \{ 1\ 2\ 3\ 4 \}$

Conjunto producto $X \times Y$

luego $G \subset X \times Y$

XxY	a	b	c
1	a1	b1	c1
2	a2	b2	c2
3	a3	b3	c3
4	a4	b4	c4

G

2-3 CORRESPONDENCIA

Dados dos conjuntos A y B, llamaremos correspondencia entre A y B a la terna C = (G,A,B), donde G es un grafo subconjunto del producto de A × B

$$\text{G grafo de C} \quad G = \left\{ (x\ y) \mid x \in A < x \in B \right\}$$

Es decir, la correspondencia estará definida por un subconjunto de A × B.

Al conjunto A le llamaremos conjunto inicial o dominio de C.

Al conjunto B le llamaremos conjunto final o codominio de C.

Por definición de grafo:

$$\left\{ pr_1\ G \right\} \subset A$$

$$\left\{ pr_2\ G \right\} \subset B$$

Decir que:

$(x, y) \in G$, será equivalente a decir:

"a x le corresponde y por la correspondencia C = (G A B)"

o bien:

"y es imagen de x por la correspondencia C = (G A B)"

2-4 CORRESPONDENCIA INVERSA

Dada la correspondencia (G, A, B), llamaremos correspondencia inversa de ella y la representaremos (G^{-1}, B, A) a una correspondencia cuyo grafo G^{-1} esté formado por las mismas parejas de G, pero con el orden invertido.

Es decir:

$$G^{-1} = \left\{ (y\ x) \mid (x\ y) \in G \right\}$$

Por lo tanto:

$$pr_1\ G^{-1} \subset B$$

$$pr_2\ G^{-1} \subset A$$

Es evidente que si "*y* es la imagen de *x*" por el grafo G, "*x* es la imagen de *y*" por el grafo G^{-1}. A esta imagen se le llama imagen por medio de la correspondencia inversa.
Por definición de G^{-1} se tendrá que:

$$pr_1\ G = pr_2\ G^{-1}$$

$$pr_2\ G = pr_1\ G^{-1}$$

2-5 APLICACION

"Sea la correspondencia $f = (G,A,B)$, diremos que es una aplicación si para todo elemento de A existe una y una sola imagen en B".
Es decir:

$$\forall a,\ \ a \in A\ \exists^* b,\ \ b \in B \mid (a\ b) \in G$$

Un grafo de este tipo se llama grafo funcional, y en él por definición

$\{ pr_1\ G \} = A$ *"La primera proyección de G coincide con el dominio"*

aunque esta condición es necesaria, pero no suficiente.

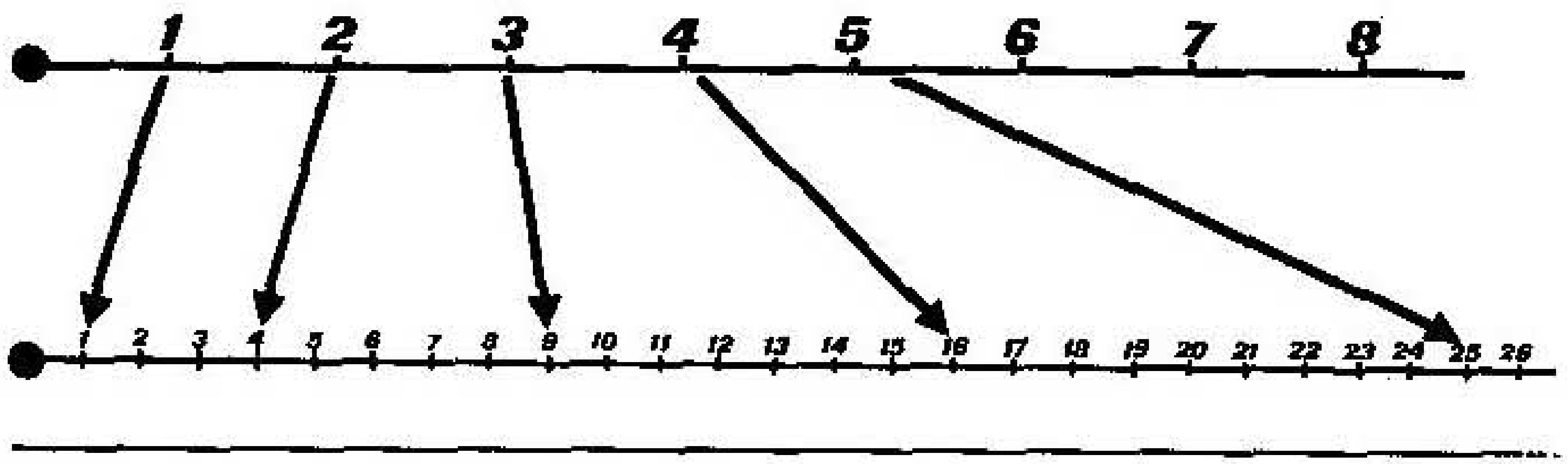
EJEMPLO:

$$\text{Sea } A = N \qquad B = N$$

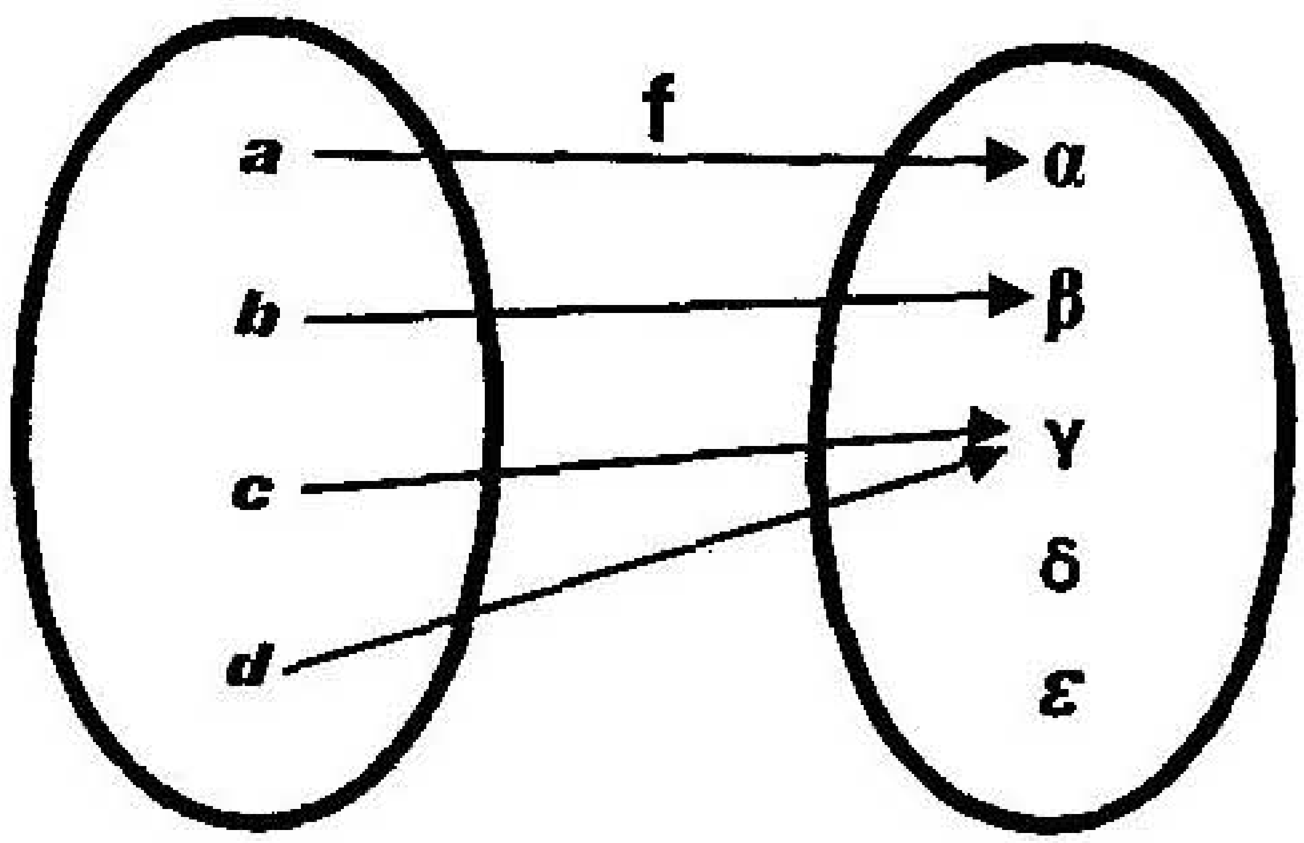
Establezcamos el grafo G cuyos elementos sean:

$$G = \left\{ (n,\ n^2) \mid n \in N \right\}$$

Es evidente que es una aplicación entre los naturales, pues:
— para cada natural existe otro natural que es cuadrado
— y, además, es único.



Las aplicaciones se pueden representar con flechas



donde f simboliza la aplicación.

Si $f = (G,A,B)$ es una aplicación, entonces $(x\ y) \in G$ se suele escribir simbólicamente $y = f(x)$, que se lee "y es la imagen por f de x".
Esta simbolización se utiliza también para conjuntos, así:
Si $A' \subset A$, entonces todo elemento de A' tendra imagen en B.
Al subconjunto de B que contiene a todas las imágenes de A' lo indicaremos $f(A')$.

$$f(A') \subset B$$

En general, pues, $f(A) \subset B$. De igual forma, dado un subconjunto $B' \subset B$, llamaremos imagen recíproca del B' al subconjunto de elementos de A cuyas imágenes están contenidas en B', y lo representaremos $f^*(B') \subset A$.

Una aplicación $f = (G, A, B)$ la expresaremos de forma simbólica:

$$f: A \to B, \text{ o bien } A \xrightarrow{f} B,$$

2-5-1 CLASIFICACION DE LAS APLICACIONES

a) Aplicación inyectiva: Dada una aplicación $f = (G,A,B)$ entre los conjuntos A y B, que simbolizamos $A \xrightarrow{f} B$, diremos que es inyectiva si para cada par de elementos distintos de A corresponden imágenes distintas en B. Es decir:

Si $a \in A$, y $b \in A$ y tal que $a \neq b$, entonces, $f(a) \in B$ y $f(b) \in B$; siendo:

$$f(a) \neq f(b)$$

Es decir, que cada elemento de B puede ser imagen, a lo sumo, de un elemento de A, o también

$$\forall x \quad x \in f(A) \quad \exists^* a \in A \mid x = f(a)$$

b) Aplicación exhaustiva (también llamada suprayectiva o "sobre"): Una aplicación $f = (G,A,B)$ entre A y B, es exhaustiva si el conjunto de las imágenes de A, $f(A)$ [que, en general, es un subconjunto de B] coincide con B.

$$f(A) = B$$

Es decir, todos los elementos de B son imagen de uno o varios elementos de A.

$$\forall x \quad x \in B \; \exists a \quad a \in A \mid x = f(a)$$

De este hecho proviene la nominación de *sobre*, ya que la aplicación cubre todo B.
De la combinación de estos dos tipos de aplicaciones surgen 4 clases de aplicaciones:

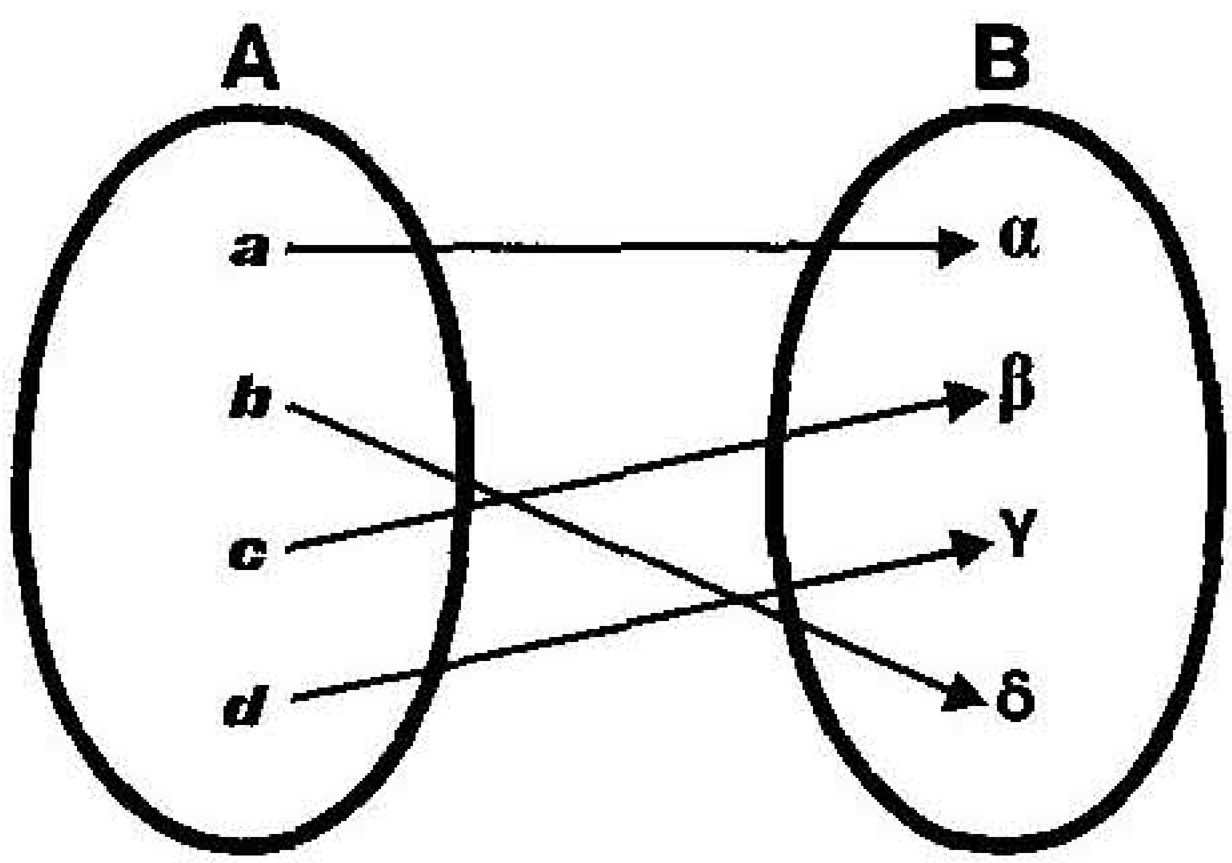
1) Inyectiva-exhaustiva
2) Inyectiva-no exhaustiva

NOTA: Indistintamente se utilizará "sobre" o "exhaustiva".

3) No inyectiva-exhaustiva
4) No inyectiva-no exhaustiva

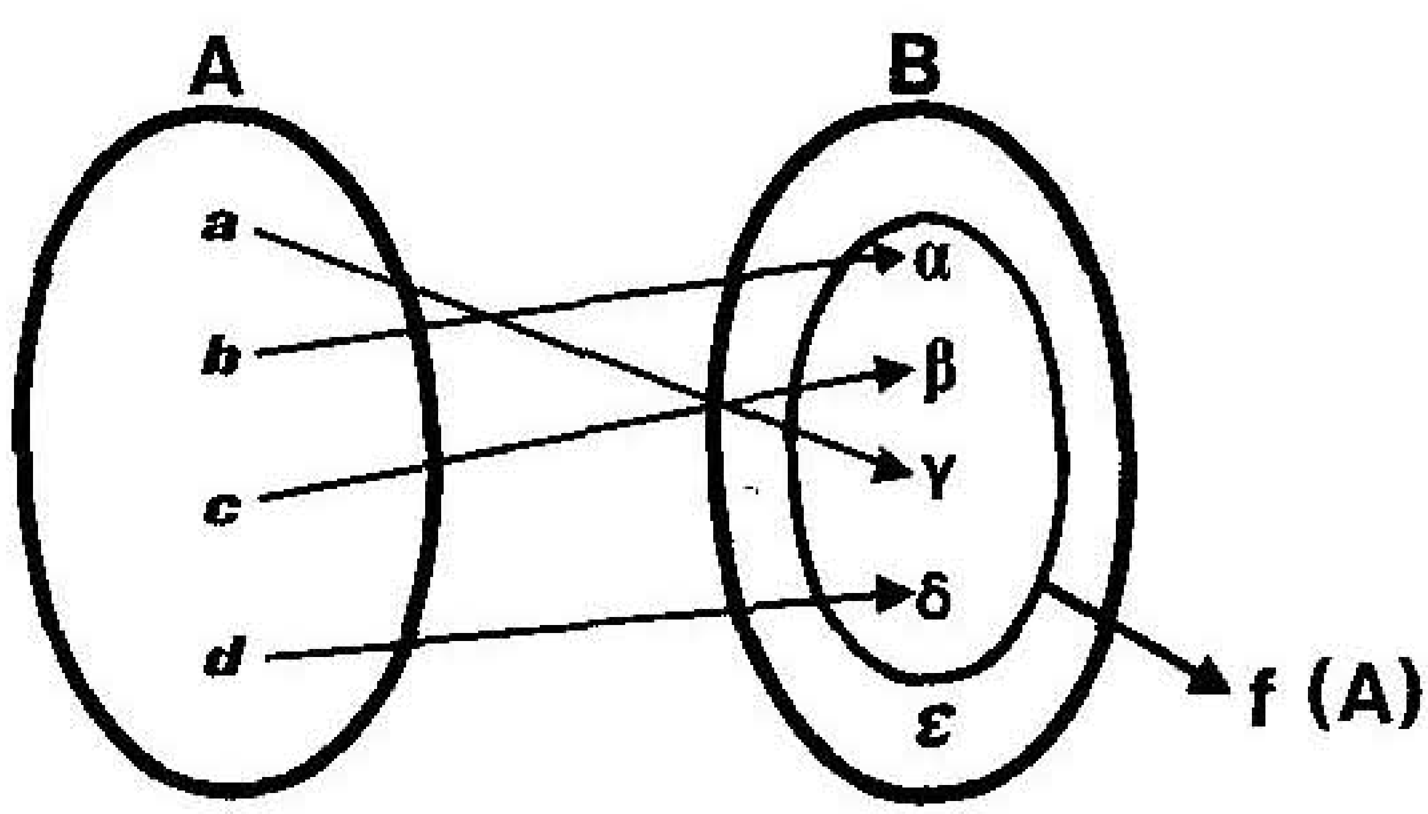
Inyectiva-exhaustiva

"A distintos elementos de A imágenes distintas en B"
$f(A) = B$.
A estas aplicaciones, que son del tipo "uno a uno",
se les llama biunívocas o biyectivas.



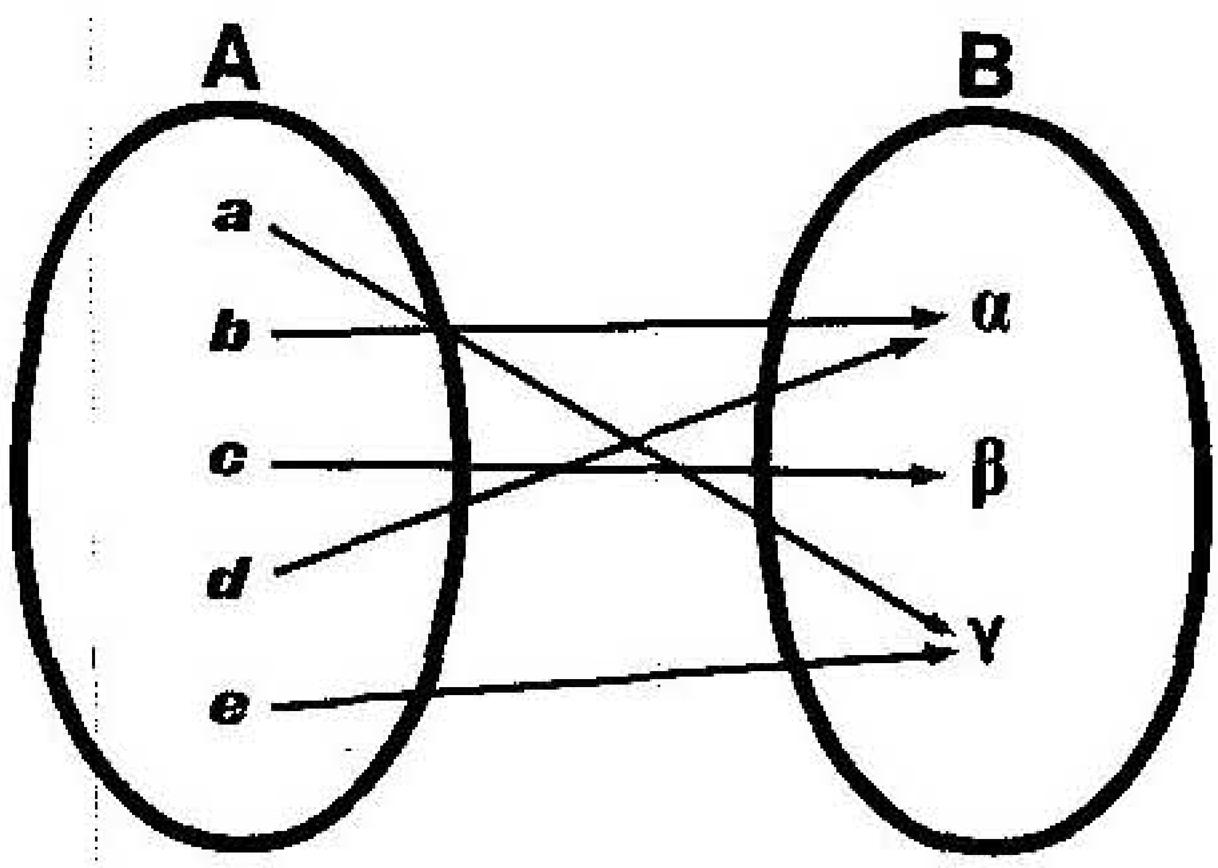
Inyectiva-no exhaustiva

"A cada elemento de A, distinta imagen de B",
pero $f(A) \neq B$
aunque $f(A) \subset B$

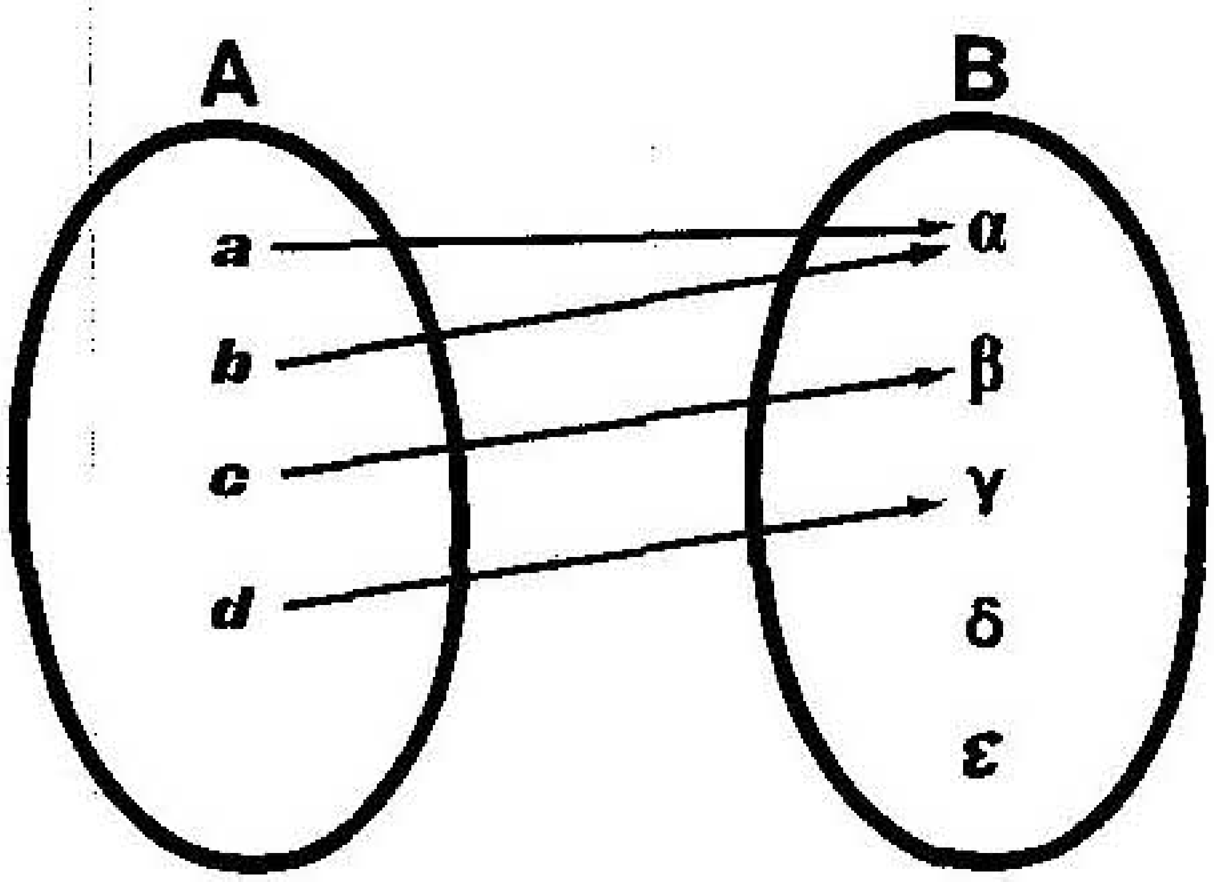


No inyectiva-exhaustiva

$a \neq e$, pero $f(a) = f(a) = f(e) = \gamma$
$f(A) = B$



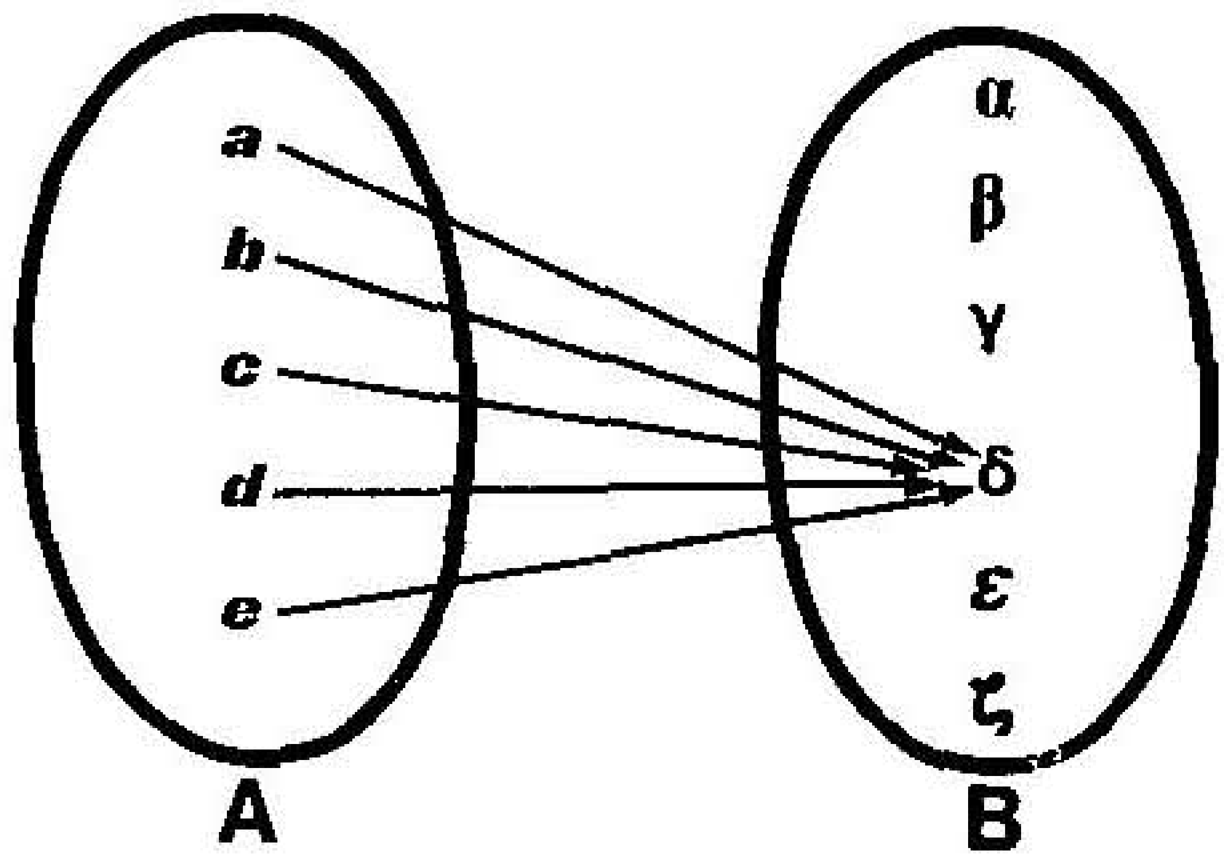
No inyectiva-no exhaustiva



Aplicación constante: En el caso particular de que $f(A)$ sea un conjunto de 1 elemento, es decir, que todos los elementos de A tienen la misma imagen

$$\forall\, a \in A\ \exists^*\, x \in B \mid x = f(a)$$

la aplicación se llama constante.



Aplicación idéntica: Una aplicación $f = (G,A,A)$ de A sobre A, tal que

$$\forall\, a \in A, f(a) = a$$

se llama aplicación idéntica de A y la representaremos $\mathcal{E}_A$.

2-6 COMPOSICION DE APLICACIONES

Dadas las aplicaciones:

$$f_1 = (G_1, A, B)$$
$$f_2 = (G_2, B, C)$$

donde el conjunto inicial de f_2 coincide con el final de f_1.
Por definición de aplicación:

por f_1) $\forall\, a \in A\ \exists^*\, b \in B \mid b = f_1\ (a)$, es decir, $(a\ b) \in G_1$

por f_2) $\forall\, b \in B\ \exists^*\, c \in C \mid c = f_2\ (b)$, es decir, $(b\ c) \in G_2$

debido a que las aplicaciones son correspondencias en que para todos los elementos del conjunto inicial existe una sola imagen en el final, podremos construir el siguiente grafo G:

$$G = \left\{ (a\ c) \mid \exists^*\, b \in B\ (a\ b) \in G_1 \text{ y } (b\ c) \in G_2 \right\}$$

en el que para cada elemento $a \in$ A existirá un único b y un único c; es decir, en G habrá una sola pareja que contenga a a: luego G define una aplicación entre A y C, que representaremos por:

$$f = (G,A,C)$$

y que llamaremos aplicación producto de f_1 y f_2

En notación más simple:

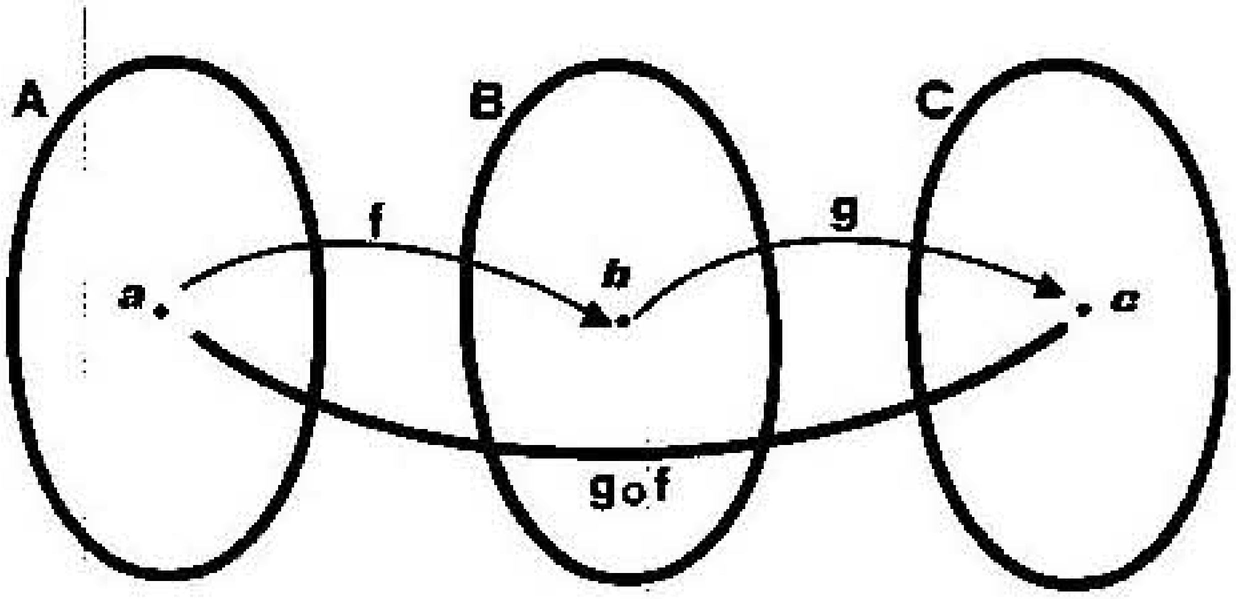
$$f: A \to B$$
$$g: B \to C$$

La aplicación producto la expresaremos $g{\cdot}f$ (en orden inverso al que actúan)

$$g \cdot f : A \to C$$

y para un elemento $a \in$ A su imagen se expresará

$$g \cdot f\,(a) = g[f(a)] = g(b) = c$$



TEOREMA: La composición de aplicaciones es asociativa:

Sean

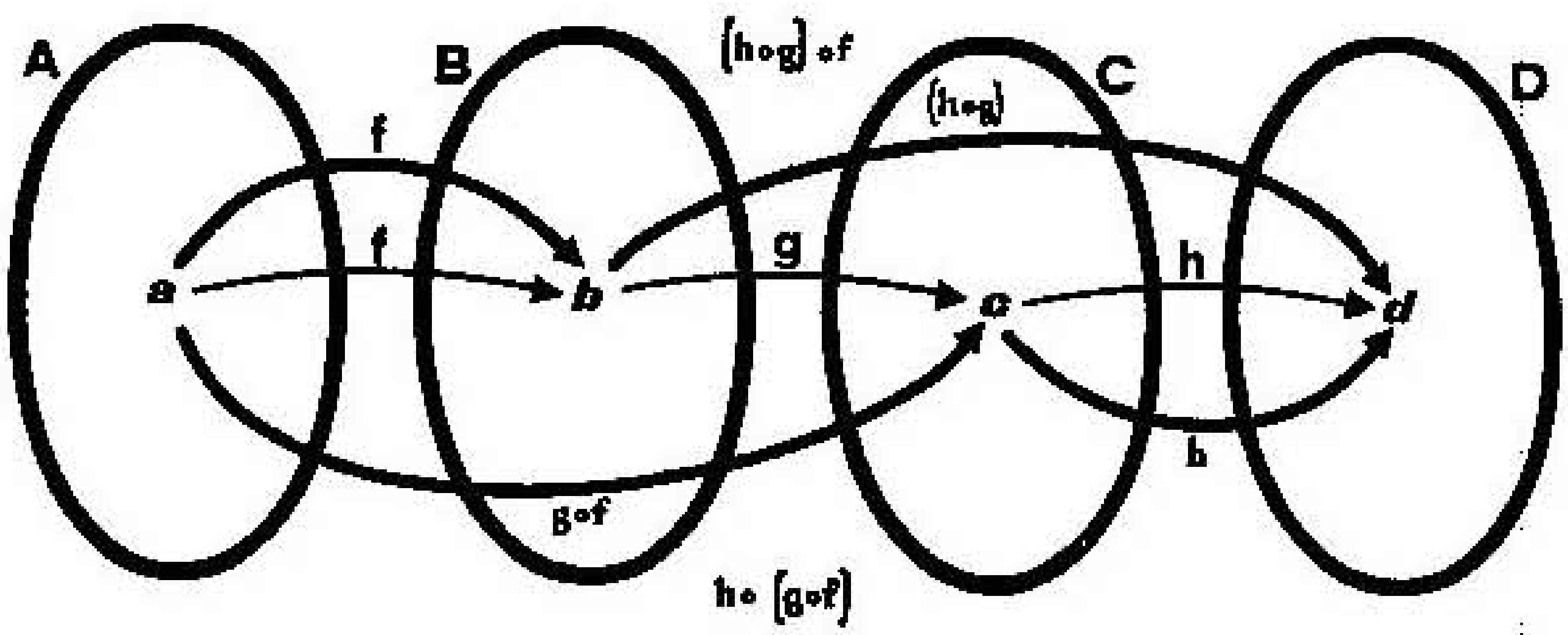
$$f: A \to B$$
$$g: B \to C$$
$$h: C \to D$$

Vamos a probar que $h \cdot (g \cdot f) = (h \cdot g) \cdot f$

En efecto: por composición de aplicaciones, para un elemento a de A:

(1) $h \cdot (g \cdot f)\,[a] = h \cdot [(g \cdot f)\,(a)] = h \cdot [g\,(f(a))] = h\,[g\,(b)] = h\,(c) = d$

(2) $(h \cdot g)\,f[a] = (h \cdot g)\,[f(a)] = h \cdot g\,[b] = h\,[g(b)] = h\,(c) = d$



y esto sucederá para todo $a \in$ A.

TEOREMA:

Composición de aplicaciones inyectivas

La composición de dos aplicaciones inyectivas es una aplicación inyectiva.

En efecto: sean $f_1 = (G_1\ A\ B)$, y $f_2\ (G_2\ B\ C)$ inyectivas que representaremos:

$$f\colon A \to B \qquad \text{y} \qquad g\colon B \to C$$

por lo tanto:

$$\forall\ c \in g\,(B) \qquad \exists^*\ b \in B \mid g(b) = c$$

$$\forall\ b \in f\,(A) \qquad \exists^*\ a \in A \mid f(a) = b$$

de ambas queda:

$$\forall\ c \in g \cdot f\,(A) \quad \exists^*\ a \in A \mid (g \cdot f)\,(a) = c$$

con lo que:

$$g \cdot f \text{ será inyectiva}$$

COROLARIO

De igual forma, el producto de dos aplicaciones biyectivas será biyectiva.
En efecto, por ser biyectivas, serán inyectivas, y por el teorema anterior, la aplicación producto será inyectiva, pero además, por definición de producto la imagen de A por el producto será todo C, luego será biyectiva.

2-7 APLICACION INVERSA

Dada la aplicación $f = (G,A,B)$, en tanto que correspondencia tendrá una correspondencia inversa (G^{-1},B,A) que se obtendrá invirtiendo el orden de los pares de G; ahora bien, esta correspondencia (G^{-1},B,A) en general no será una aplicación (es decir, podrán haber elementos de B que no aparezcan en ningún par de G^{-1} y otros que aparezcan más de una vez). Nuestro problema será establecer en qué caso la correspondencia inversa de una aplicación dada es también aplicación.

EJEMPLO:

En la aplicación $F = (G,N,N)$ tal que $G = \{(n,n^3) \mid n \in N\}$ (a cada número natural le corresponde su cubo), su correspondencia inversa (G^{-1},N,N), $G^{-1} = \{(n^3\ n) \mid n \in N\}$ no será aplicación; por ejemplo, 15, que es natural, no tiene imagen, pues no es cubo de ningún natural.

TEOREMA:

La condición necesaria y suficiente para que una aplicación tenga inversa es que sea biunívoca.

⇒ En efecto, es condición necesaria:

Ya que si la correspondencia $(G^{-1}\ B\ A)$ es una aplicación, entonces

$$\forall\, b \in B \quad \exists^*\, a \in A \mid (b\ a) \in G^{-1}$$

pero esto es equivalente por la definición de correspondencia inversa a que $(a\ b) \in G$, luego

$$\forall\, b \in B \quad \exists^*\, a \in A \mid (a\ b) \in G$$

que es la condición para que $F = (G,A,B)$ sea biunívoca.

$\Leftarrow$ Es condición suficiente:

Pues si $F = (G,A,B)$ es biunívoca, entonces

$$\forall\, b \in B \quad \exists^*\, a \in A \mid b = f(a) \text{ o sea } (a\ b) \in G$$

por lo tanto, todos los elementos de b están en una sola pareja de G, luego el grafo G^{-1} inverso de G definirá una función, es decir, la correspondencia inversa será función inversa.
A la función inversa de una dada $F = (G,A,B)$ $f\colon A \to B$, la representaremos $f^{-1} : B \to A$.

COROLARIOS

1) La composición de $f^{-1}\ f = \mathcal{E}_A$ es la identidad de A.

En efecto:

$$\text{sea: } f\colon A \to B$$
$$\text{y su inversa: } f^{-1} : B \to A$$

$$\forall\, a \in A, f(a) = b$$

y por ser f^{-1} inversa de f, entonces:

$$\forall\, b \in B\ f^{-1}\ (b) = a$$

luego: $\forall\, a, (f^{-1} \cdot f)\ [a] = f^{-1}\ [f(a)] = f^{-1}\ (b) = a$

luego:

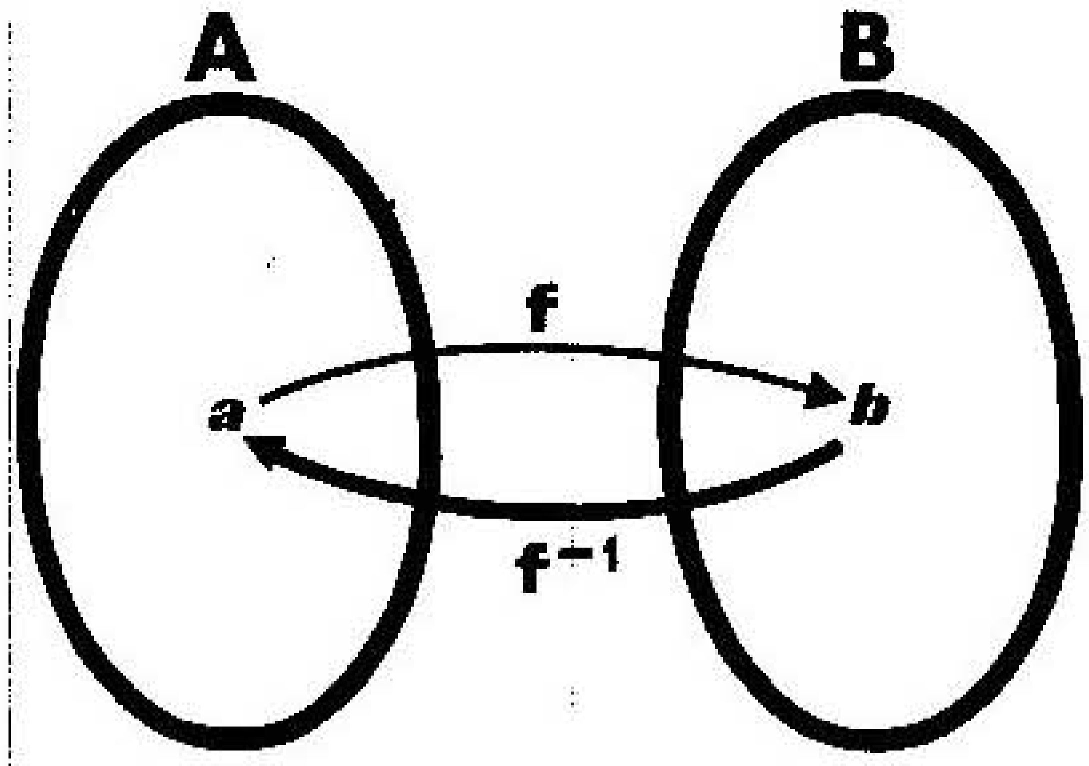
$$f^{-1} \cdot f = \mathcal{E}_A$$

2) La composición de $f \cdot f^{-1} = \mathcal{E}_B$ es la identidad de B.
En efecto: de igual forma

$$\forall\, b \in B \ (f \cdot f^{-1})(b) = f \cdot [f^{-1}\ (b)] = b$$

luego:

$$f \cdot f^{-1} = \mathcal{E}_B$$



2-8 PARTE ESTABLE PARA UNA APLICACION

Dada una aplicación $F = (G,A,A)$ de A en sí misma $f: A \to A$, llamaremos parte estable para F a todo subconjunto $X \subset A$, de A tal que:

$$f(X) \subset X$$

sus imágenes por f están contenidas en X.

2-9 RESTRICCION Y PROLONGACION DE APLICACIONES

1.—*Restricción:*

Dada la aplicación $F = (G,A,B)$, tomemos un subconjunto $X \subset A$ y consideremos el grafo G' subconjunto de G tal que

$$\left\{ pr_1\ G. \right\} = X$$

A la aplicación de X en B

$$F' = (G',X,B)$$

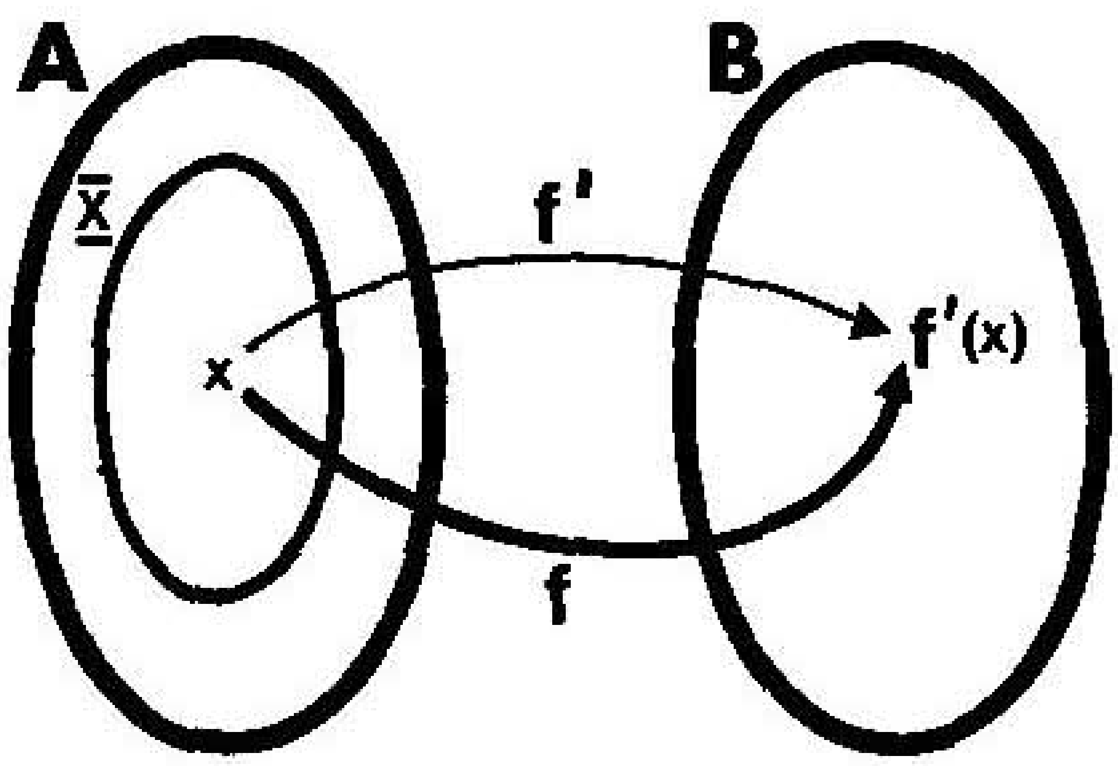
la llamaremos restricción de F a X.

Es evidente que

$$\forall\, x \in X \quad f(x) = f'(x)$$

ya que el grafo de F' está contenido en el grafo de F, y

$$[x, f'(x)] \in G \quad \Rightarrow \quad [x, f'(x)] = [x, f(x)]$$



2.—*Prolongación:*

Una aplicación F = (G,A,B) que tenga una restricción F' = (G' X B) se llamará prolongación de su restricción.

F' restricción de F
F prolongación de F'

2-10 SUCESIONES

Sea el conjunto N de los números naturales. Dado un conjunto X, llamaremos sucesión de elementos de X a toda aplicación

$$F = (G,N,X)$$

Esta aplicación se suele representar:

siendo $i \in N$, su imagen por $F = (G,N,X)$ será un x tal que

$$(i,x) \in G$$

y este par se indica x_i

APLICACIONES ENTRE CONJUNTOS FINITOS. COMBINATORIA.

2-11 NUMERO DE APLICACIONES ENTRE DOS CONJUNTOS FINITOS

Dados dos conjuntos finitos E y E′ de n y n' elementos, respectivamente, consideraremos el conjunto $F = \{ f \mid : E \to E' \}$ de todas las aplicaciones que se puedan establecer entre ellos. Vamos a probar que el conjunto F tiene $(n')^n$ elementos.

En efecto:

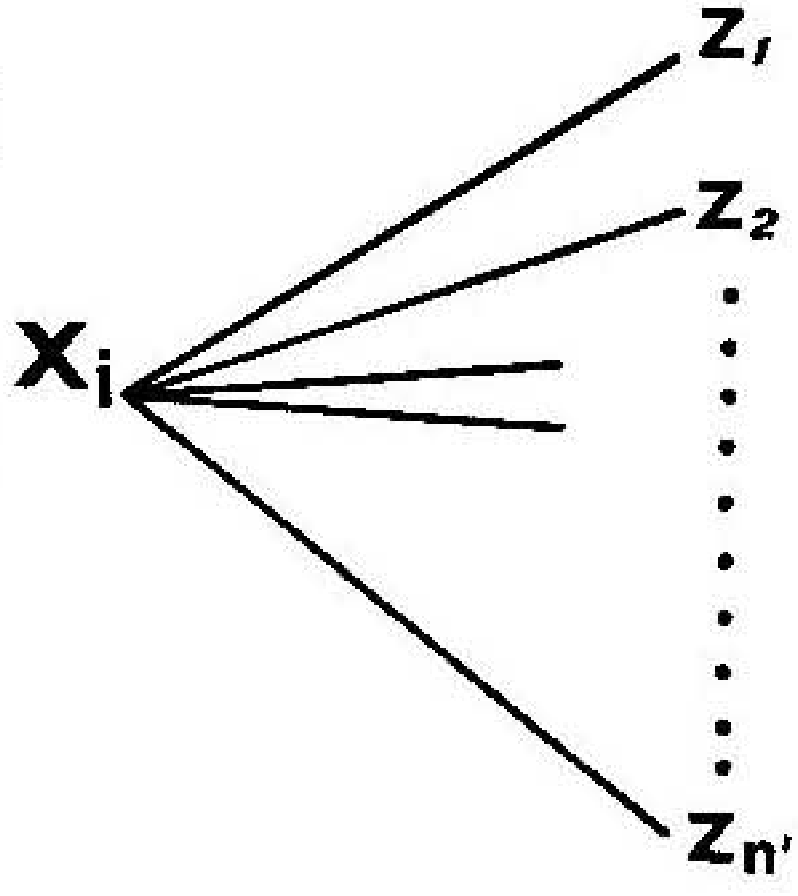
Por definición de aplicación, si consideramos

$$E = \{ x_1, x_2 \ldots x_n \}$$

y

$$E' = \{ z_1, z_2 \ldots z_n \}$$

a cada elemento de E le corresponderá uno y uno solo de E′ (uno cualquiera), luego cada uno de los elementos de E le puede corresponder uno de los n' z_i.



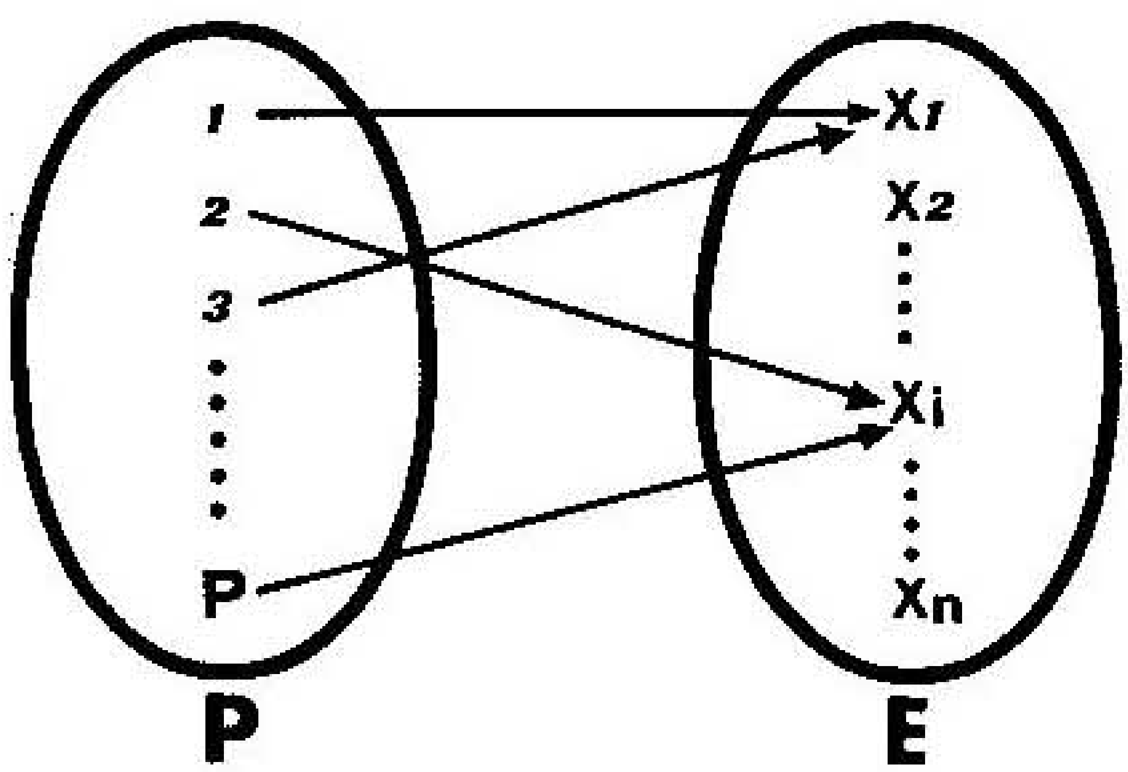
Una vez elegida la imagen de uno de los x_i, siguiendo el proceso a otro x_i le pueden corresponder una cualquiera de las n', z_i (incluso la misma que antes), luego a cada x_i le pueden corresponder n' z_i; el número total de posibilidades será el producto de todas ellas.

$$\underbrace{n'}_{x_1} \cdot \underbrace{n'}_{x_2} \cdot \underbrace{n'}_{x_3} \cdots\cdots\cdots \underbrace{n'}_{x_n} = (n')^n$$

Variaciones con repetición: Consideremos el conjunto finito $E = \{x_i \mid i \in [1 \dots n]\}$ de n elementos; vamos a llamar variaciones con repetición de los elementos de E tomados de p en p a cualquier sucesión de p elementos de E idénticos o distintos.
Es decir, dos variaciones serán distintas si difieren en algún elemento o en el *orden* en que están colocados.
Las variaciones con repetición las representaremos $V'n,p$ (que se leerá variaciones con repetición de n elementos tomados de p en p).

Teorema:

Llamando P al conjunto $P = \{1\ 2\ 3 \dots p\}$, vamos a probar que el número $V'n\ p$ es igual al número de aplicaciones f que se pueden establecer entre P y E. $f: P \rightarrow E$.
En efecto, cada variación será una posible aplicación, pues cada una de éstas ordenadamente hará corresponder a todo elemento de P uno y uno sólo E igual o distinto.



Luego el número $V'n,p$ es igual a n^p.

$$\boxed{V'\,n,p = n^p}$$

2-12 NUMERO DE APLICACIONES INYECTIVAS ENTRE DOS CONJUNTOS FINITOS

Dados los conjuntos E y E' de n y n' elementos, respectivamente, y considerando que en una aplicación inyectiva a elementos distintos de E corresponden elementos distintos de E', necesariamente E' tendrá como mínimo igual número de elementos que E.

$$n' \geqslant n$$

Llamemos I al conjunto de aplicaciones inyectivas entre E y E'

$$I = \left\{ f_i \mid f_i : E \to E' \right\}$$

y vamos a probar que el número de elementos de I es

$$n' (n' - 1) (n' - 2) \ldots \left((n' - (n - 1) \right)$$

En efecto:

Por definición de aplicación a cada elemento de E le corresponderá uno y uno solo de E' (uno cualquiera), pero por ser inyectiva, una vez un elemento de E' es imagen de alguno de E, ya no lo puede ser de otro.

Sea
$$E = \left\{ x_1 \ldots x_n \right\}$$
$$E' = \left\{ z_1 \ldots z_{n'} \right\}$$

Empezando ordenadamente por cualquier elemento de E:

- a x_1 le pueden corresponder como imagen una cualquiera de las n' z_i.
- a x_2 le pueden corresponder una cualquiera de las $n' - 1$ z_i (descontando la que le correspondió a x_1), y razonando así sucesivamente cada uno de los elementos de E tiene una posibilidad menos que el anterior. Y el número total será el producto de todas ellas.

$$\underbrace{n'}_{x_1} \quad \underbrace{(n' - 1)}_{x_2} \quad \underbrace{(n' - 2)}_{x_3} \ldots\ldots\ldots \underbrace{[n' - (n - 1)]}_{x_n}$$

O sea:

$$n' (n' - 1) (n' - 2) \dots (n' - n + 1)$$

Apréciese:

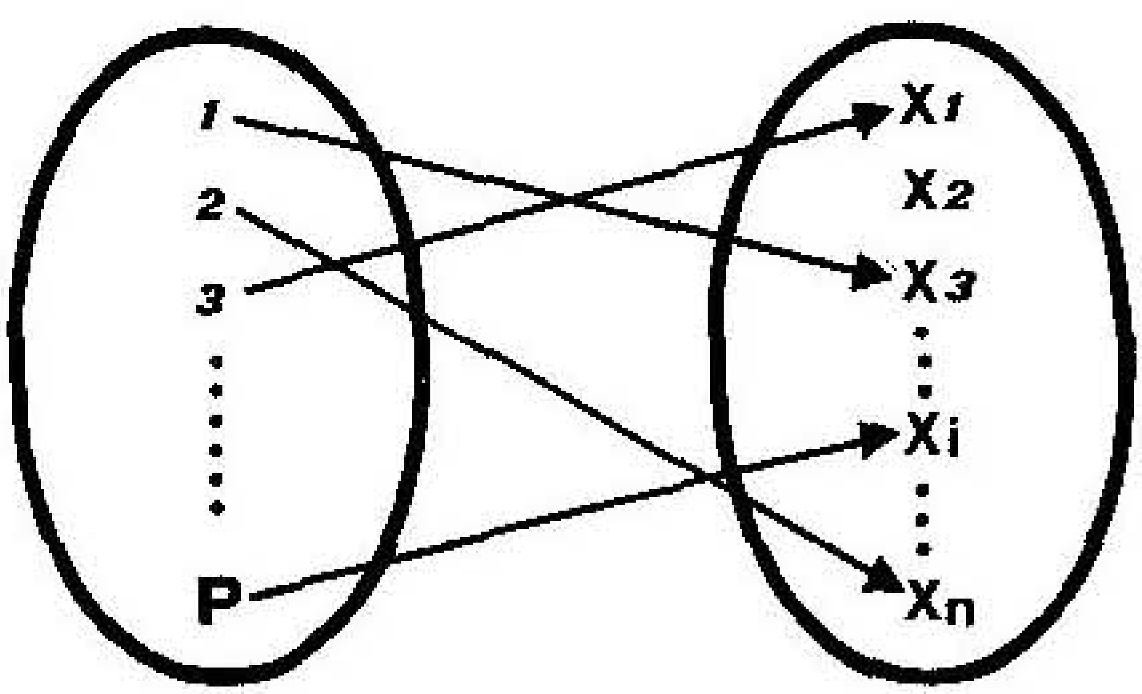
— Que el número de factores coincide con n.
— Que cada factor es una unidad menos que el anterior.

VARIACIONES SIN REPETICION

Consideramos el conjunto $E = \{x_i \mid i \in E\,(1 \dots n)\}$ de n elementos. Vamos a llamar variaciones sin repetición de los elementos E tomados de p en p a cualquier serie de p elementos de E distintos.
Es decir, en unas variaciones no podrá aparecer dos veces el mismo x_i y dos variaciones serán distintas si el orden en que aparecen los elementos de E es distinto.
Las variaciones sin repetición las representaremos V n,p, que se leerá variaciones de n elementos tomados de p en p.

Teorema:

Llamando P al conjunto $P = \{1, 2, \dots p\}$, vamos a probar que el número V $n\,p$ es igual al número de aplicaciones inyectivas f_i que se pueden establecer entre P y E.
En efecto; cada variación corresponde a una serie de p elementos x_i de E en un cierto orden, sin repetirse ninguno, y cada aplicación inyectiva asigna ordenadamente a cada uno de los p elementos de P un elemento distinto de E.



$$\begin{array}{ccccc} 1, & 2, & 3, & \dots\dots & P \\ \downarrow & \downarrow & \downarrow & & \downarrow \\ x_3, & x_n, & x_1 & \dots\dots & x_i \end{array}$$

siendo necesario que $p \leqslant n$

Luego:

$V\,n,p = n\,(n-1)\,(n-2)\,...\,(n-(p-1)) = n\,(n-1)\,(n-2)\,...\,(n-p+1)$

Notación:

Llamando $m! = m\,(m-1)\;\;(m-2)\;\;(m-3)\;\;....1$ a un producto indicado que va de m a 1 descendiendo de unidad en unidad y que llamaremos "factorial de m" las variaciones $V\,n,p$ se podrán expresar multiplicando y dividiendo por la misma expresión $(n-p)$!

$$V\,n\,p = n\,(n-1)\,(n-2)\,...\,(n-p+1)\cdot\frac{(n-p)\,(n-p-1)\,(n-p-2)\,...\,1}{(n-p)\,(n-p-1)\,(n-p-2)\,...\,1} = \frac{n!}{(n-p)!}$$

$$V\,n\,p = \frac{n!}{(n-p)!}$$

2-13 NUMERO DE APLICACIONES BIUNIVOCAS ENTRE DOS CONJUNTOS FINITOS

Una aplicación biyectiva ya vimos que era una aplicación inyectiva que además era exhaustiva; luego entre conjuntos finitos, para que dados dos conjuntos E y E′ entre ellos se pueda establecer una aplicación biunívoca, será necesario que tenga el mismo número de elementos n. Pues cada uno de los elementos de E′ es imagen de uno y uno solo de E y, además, todos los elementos de E′ son imagen de alguno de los elementos de E.

Llamemos B al conjunto de aplicaciones biunívocas entre

$$\}E = x_1 \ldots x_n\{ \text{ y } E' = \}z_1 \ldots z_n\{,\ B = \}f_b \mid f_b : E \to E'\{$$

y vamos a probar que el número de elementos de B es

$$n\,(n-1)\,(n-2)\,(n-3)\,...\,1 = n!$$

En efecto; como las aplicaciones biunívocas son aplicaciones inyectivas en que $n = n'$, sustituyendo ésto en la expresión de las inyectivas queda:

$$n\,(n-1)\,(n-2)\,...\,(n-n'+1) = n\,(n-1)\,(n-2)\,...\,(n-n+1) = n!$$

Permutaciones.—Consideremos el conjunto $E = \{ x_i \mid i \in [1 \ldots n] \}$ de n elementos.
Llamaremos permutaciones de los elementos de E a las variaciones de los elementos x_i tomados de n en n. Es decir, llamándolo P_n.

$$P_n = V\,n{,}n \quad \text{o sea, } P_n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

pues por definición $0! = 1$

Es trivial que a cada aplicación biunívoca corresponde una permutación y el número de aplicaciones biunívocas entre E y E′ de n elementos será igual a P_n.

2-14 COMBINACIONES

Consideremos el conjunto $E = \{ x_i \mid i \in [1\ 2 \ldots n] \}$ de n elemento. Llamaremos combinaciones sin repetición de los n elementos tomados de p en p a las sucesiones de p elementos de E, tales que deben ser todos los elementos distintos, y además dos series con los mismos elementos tomados en distinto orden se considerarán la misma combinación.
Las combinaciones las representaremos $C\,n{,}p$ y, evidentemente, $p \leqslant n$.

Vamos a probar que:

$$C\,n{,}p = \frac{V\,n{,}p}{p!}$$

En efecto; dada una combinación cualquiera de los x_i tomados de p en p

$$\underbrace{x_2\ x_3\ x_1\ \ldots\ x_i}_{p \text{ términos}}$$

como variaciones podríamos obtener permutando todos los elementos que la forman $p!$ series distintas que, sin embargo, como combinaciones serían la misma, pues sólo habría cambiado el orden de las componentes. Luego cada combinación da origen a $p!$ variaciones distintas, es decir, al recorrer todas las posibles combinaciones $\mathbf{C}\, n,p$ reproduciremos las Vn,p variaciones, es decir:

$$\mathbf{C}\, n,p \cdot p! = Vn,p$$

Expresándolo en forma de factoriales quedaría:

$$\mathbf{C}\, n,p = \frac{Vn,p}{p!} = \frac{\dfrac{n!}{(n-p)!}}{p!} = \frac{n!}{(n-p)!\,p!}$$

al número representado por $\mathbf{C}\, n\, p$ se le llama número combinatorio y se representa $\binom{n}{p}$ que se lee *"n sobre p"*

2-14-1 PROPIEDADES DE LOS NUMEROS COMBINATORIOS

1) $\binom{n}{o} = 1 \quad \forall n$

En efecto:

$$\binom{n}{o} = \frac{n!}{0!\ (n-o)!} = \frac{n!}{n!} = 1$$

2) $\binom{n}{n} = 1 \quad \forall n$

En efecto:

$$\binom{n}{n} = \frac{n!}{n!\ (n-n)!} = \frac{n!}{n!\ o!} = \frac{n!}{n!} = 1$$

3) $\binom{n}{p} = \binom{n}{n-p}$

"Dos números combinatorios que tienen igual el índice superior y que sumados los inferiores dan el superior son iguales."
En efecto:

$$\text{por definición} \quad \binom{n}{p} = \frac{n!}{p!\ (n-p)!}$$

$$\text{pero} \quad \binom{n}{n-p} = \frac{n!}{(n-p)!\ [n-(n-p)]!} = \frac{n!}{(n-p)!\ p!}$$

que, evidentemente, es lo mismo.

4) $\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$

"La suma de dos números combinatorios de igual índice superior y de índices inferiores consecutivos es igual a otro número combinatorio de índices iguales al de los menores incrementados en una unidad."
En efecto; hagamos simplemente el cálculo teniendo en cuenta:

$$(p+1)! = (p+1)\cdot p! \qquad y \qquad (n-p-1)! = \frac{(n-p)!}{(n-p)}$$

que es evidente por definición de factorial

$$\binom{n}{p} + \binom{n}{p+1} = \frac{n!}{p!\ (n-p)!} + \frac{n!}{(p+1)!\ (n-p-1)!} = \frac{n!}{p!\ (n-p)!} +$$

$$+ \frac{n!}{(p+1)!\ \dfrac{(n-p)!}{(n-p)}} =$$

sacando factor común queda:

$$\binom{n}{p} + \binom{n}{p+1} = \frac{n!}{p!\ (n-p)!} \left[1 + \frac{n-p}{p+1}\right] = \frac{n!}{p!\ (n-p)!} \cdot \frac{p+1+n-p}{p+1} =$$

$$= \frac{n!\ (n+1)}{p!\ (n-p)!\ (p+1)} = \frac{(n+1)!}{(p+1)!\ (n-p)!}$$

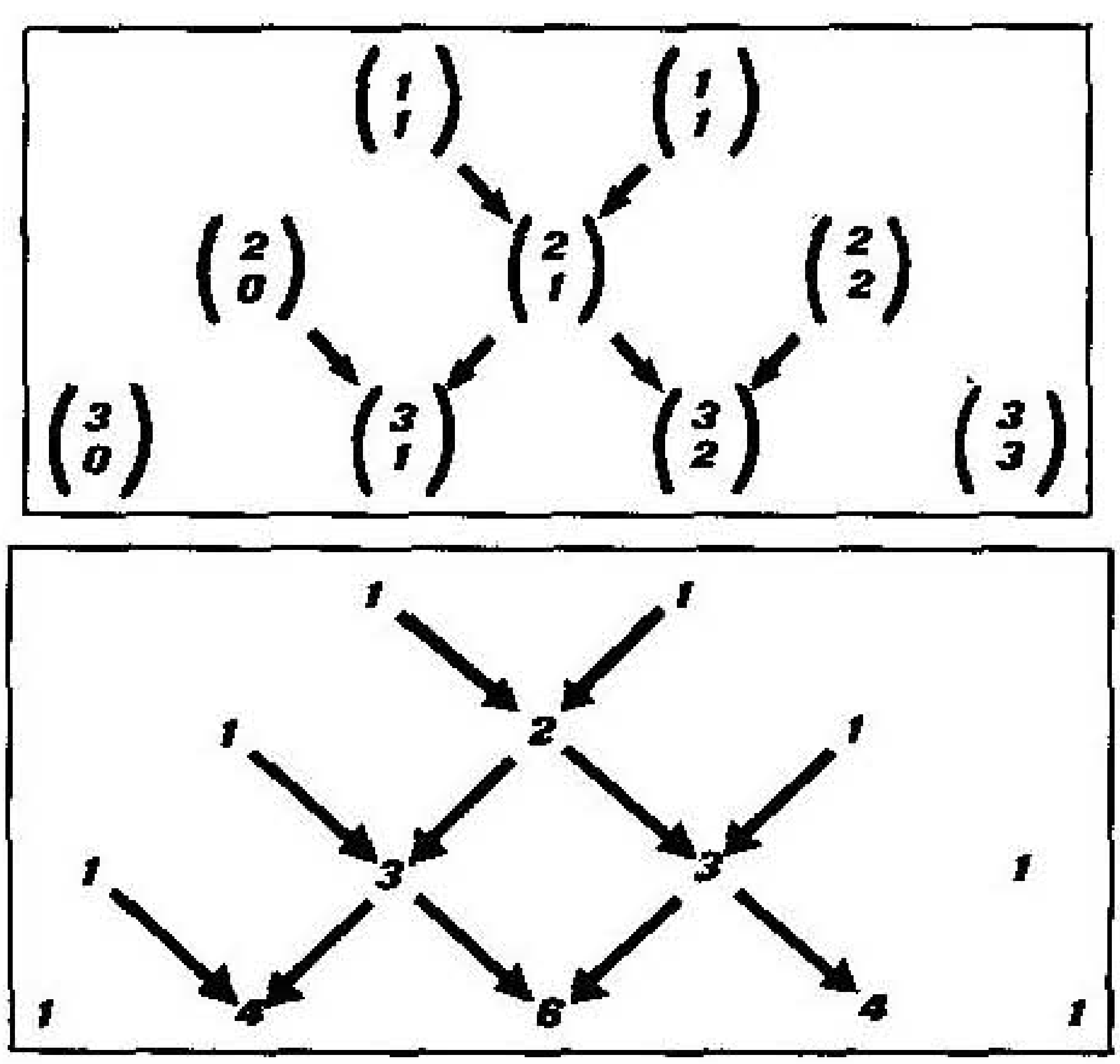
que es precisamente:

$$\binom{n+1}{p+1} = \frac{(n+1)!}{(p+1)!\ (n+1-p-1)} = \frac{(n+1)!}{(p+1)!\ (n-p)!}$$

luego:

$$\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$$

La concurrencia de las 4 propiedades permite construir triángulo de Tartaglia.



Donde todas las filas son simétricas, empiezan por 1 y cada elemento interior es igual a la suma de los dos inmediatos superiores.

Definición de familia de elementos de un conjunto.

Sean X y Λ dos conjuntos.
Establezcamos una aplicación $\Lambda \to$ X tal que

$$\forall \lambda \in \Lambda \ \exists^* x \in X \mid \lambda \xrightarrow{f} x$$

al par (λ, x) que pertenece al grafo de la aplicación f, lo representaremos por notación de índices

$$(\lambda, x) \Longleftrightarrow x_\lambda$$

De tal manera que el conjunto de las imágenes de λ por f se expresará

$$f(\lambda) = \{x_\lambda\}_{\lambda \in \Lambda} \subset X$$

y más simplemente si λ es conocido

$$(x_\lambda) \subset X$$

Al conjunto (x_λ) le llamaremos "familia" de elementos de X, teniendo Λ como conjunto de índices".
Si el conjunto Λ fuera el conjunto vacío ϕ, la familia (x_λ) carecería de elementos, pues no existiría ningún índice

$$(x_\lambda) = \phi$$

esta familia se llama "familia vacía".

Cuando el conjunto Λ es un subconjunto de los números naturales $\Lambda \subset N$ la familia de elementos de X se llama sucesión.

$$(x_n)_{n \in N}$$

que será finita o infinita según:

$$(\lambda \subset N) \text{ (finito) o } (\lambda = N \text{ o } \lambda \subset N) \text{ (infinito)}$$

El propio X puede considerarse como una familia de elementos sin más que considerar la aplicación idéntica $X \to X \ \forall x \in X \ x \to x$ en la que X hará también de conjunto de índices.

Definición de familias de conjuntos de un conjunto.

Dados dos conjuntos X, Λ
Consideremos la aplicación que a cada elemento $\lambda \in \Lambda$ le haga corresponder un subconjunto de X que notaremos indicialmente X_λ

$$\{\lambda \to X_\lambda \subset X\}$$

Al conjunto de subconjuntos de X

$$X_\lambda \mid \lambda \in \Lambda$$

le llamaremos "familia de partes de X" y lo representaremos $(X_\lambda)_{\lambda \in \Lambda}$

Para una familia de conjuntos (X_λ) podremos definir una reunión y una intersección de conjuntos, X_λ.

Reunión

$$\bigcup_{\lambda \in \Lambda} X_\lambda = \{x \mid x \in X_\lambda \text{ para al menos un } \lambda \in \Lambda\}$$

Intersección

$$\bigcap_{\lambda \in \Lambda} X_\lambda = \{x \mid x \in X_\lambda \quad \forall \lambda \in \Lambda\}$$

Si Λ = N se escribiría

$$\bigcup_{M \in N} X_n \qquad \bigcap_{M \in N} X_n$$

Esta reunión e intersección cumplen las propiedades establecidas, en general, para las operaciones de conjuntos.

TEMA 3 RELACIONES BINARIAS EN UN CONJUNTO

3-1 RELACION DE EQUIVALENCIA EN UN CONJUNTO E

Dado un conjunto E, establezcamos una correspondencia R (G,E,E) cuyo conjunto inicial y final sea E. Diremos que R es una relación de equivalencia si como correspondencia cumple

$$1\text{— } R \cdot R = R$$

$$2\text{— } R = R^{-1}$$

Es decir, el producto de la correspondencia R por sí misma es R y la correspondencia R coincide con su correspondencia inversa.

Consecuencias:

a) de 1. Por producto de correspondencias y como $R \cdot R = R$, entonces:

Si $((x,y) \in G \wedge (y,z) \in G) \Rightarrow (x,z) \in G$ *propiedad transitiva*

b) de 2.

$$\forall (x,y) \in G \Rightarrow (y,x) \in G^{-1},$$

pero como $G = G^{-1}$, entonces $(y,x) \in G$ *propiedad simétrica*

c) de 1 y 2.

$\forall (x,y) \in G \Rightarrow (y,x) \in G$ por simetría
pero $((x,y) \in G \wedge (y,x) \in G) \Rightarrow (x,x) \in G$ por transitividad
luego $\forall x \in E\ (x,x) \in G$ *propiedad reflexiva*

o lo que es lo mismo: son idénticas las proposiciones

$$x \in E \Longleftrightarrow (x,x) \in G$$

Luego también podemos definir una relación de equivalencia en un conjunto E como una correspondencia tal que cumple las propiedades

1) Reflexiva $\quad \forall x \in E \Longleftrightarrow (x,x) \in G$

2) Simétrica $\quad (x,y) \in G \Longleftrightarrow (y,x) \in G$

3) Transitiva $\quad \left.\begin{array}{l}(x,y) \in G \\ (y,z) \in G\end{array}\right\} \Rightarrow (x,z) \in G$

Si $(x\ y) \in G$ escribiremos $x\ R\ y$ y leeremos "x relacionado con y".
Si $(x\ y) \notin G$ escribiremos $x\ \bar{R}\ y$ y leeremos "x no está relacionado con y".

A veces se utilizan símbolos especiales:

$=$ igualdad
$\|$ paralelismo
$\equiv_{(R}$ equivalencia o congruencia respecto de R

EJEMPLOS:

1.—Sea:

$$E = \{a, b, c\}$$

Su producto cartesiano E X E será

ExE	a	b	c
a	aa	ab	ac
b	ba	bb	bc
c	ca	cb	cc

Consideramos el grafo G.

La correspondencia R = (G,E,E) define una relación de equivalencia.

En efecto:

Por contener la diagonal

$$\forall\, x \in E \qquad (x\ x) \in E \times E \qquad xRx \begin{cases} aRa \\ bRb \\ cRc \end{cases} \qquad \text{reflexiva}$$

Además:

$$\forall\, (x\ y) \in G \Rightarrow (y\ x) \in G \begin{cases} aRa \rightarrow aRa \\ bRb \rightarrow bRb \\ cRc \rightarrow cRc \\ aRc \rightarrow cRa \end{cases} \qquad \text{simétrica}$$

Su transitividad es inmediata, observando el grafo.

2.—Si el grafo solo contuviera la diagonal de E X E, la relación de equivalencia se llama igualdad en E.

3.—Sea E el conjunto de las rectas del plano. El paralelismo constituye una relación de equivalencia.

En efecto:

$$r \parallel r \qquad \forall\, r \in \mathrm{E}$$

$$r_1 \parallel r_2 \Rightarrow r_2 \parallel r_1$$

$$\left.\begin{array}{l} r_1 \parallel r_2 \\ r_2 \parallel r_3 \end{array}\right\} \Rightarrow r_1 \parallel r_3$$

En definitiva, desde un punto de vista formal, toda relación de equivalencia R (G,E,E) generaliza las propiedades de la igualdad en E. Y retomando, aunque matizado, el concepto de restricción, la igualdad en E aparece como una *contracción* de cualquier equivalencia en E.

Proposición: Toda función $f : \mathrm{A} \to \mathrm{B}$ entre A y B induce una relación de equivalencia en A llamada "equivalencia de aplicación", definida de la siguiente forma:

$$x \in \mathrm{A},\, y \in \mathrm{A},\, x\mathrm{R}y \iff f(x) = f(y)$$

En efecto:

Reflexiva.—$x\mathrm{R}x$, pues $f(x) = f(x) \quad \forall\, x \in \mathrm{A}$

—Si $x\mathrm{R}y \Rightarrow f(x) = f(y)$, que por simetría de la igualdad en B $f(y) = f(x)$, o sea, $y\mathrm{R}x$

Transitiva.—Si $x\mathrm{R}y \Rightarrow f(x) = f(y)$ y si $y\mathrm{R}z \Rightarrow f(z)$

y por la transitividad de la igualdad en B $f(x) = f(z)$, o sea, $x\mathrm{R}z$.

En definitiva:
Toda función $f : \mathrm{A} \to \mathrm{B} \Rightarrow$ relación binaria en A definida por f.

3-2 CLASE DE EQUIVALENCIA. CONJUNTO COCIENTE

Sea un conjunto E y una relación de equivalencia definida en E,R

Dado un elemento $x \in E$ llamaremos clase de equivalencia definida por el elemento x, que representaremos por $C(x)$, al conjunto de elementos de E equivalentes por R a x

$$C(x) = \{ y \in E \mid x \, R y \}$$

Consecuencias:

1.—Toda clase de equivalencia es no vacía, pues al menos contiene a x.

2.—Dos elementos cualesquiera de $C(x)$ son equivalentes entre sí.

En efecto:

$$\left.\begin{array}{l} \text{Si } a \in C(x) \Rightarrow x R a \text{ y por simetría } a R x \\ \text{Si } b \in C(x) \Rightarrow x R b \end{array}\right\}$$

luego $(a \, R \, x \wedge x \, R \, b)$ por transitividad $a \, R \, b$.

3.—Un elemento cualquiera de la clase se le llama representante de la clase.
Pues:

$$\forall y \in R(x) \Rightarrow x R y$$

que por simetría

$$y R x \Rightarrow x \in C(y)$$

4.—Dos clases que tengan un elemento común son idénticas:

En efecto: sea

$$\begin{array}{l} a \in C(x) \\ a \in C(y) \end{array} \quad \text{siendo en principio } C(x) \neq C(y)$$

$$\left.\begin{array}{l} \text{pero } a \in C(x) \Rightarrow x R a \\ \text{y} \quad a \in C(y) \Rightarrow y R a \text{ y por simetría} \quad a R y \end{array}\right\}$$

luego por transitividad $x R y$, o lo que es lo mismo, por simetría $y R x$

O sea:

$$\forall\ z \in C\,(x) \Rightarrow x R z;\ \text{y como } y R x \Rightarrow y R z,\ \text{o sea, } C\,(x) \subset C(y)$$

pero

$$\forall\ z' \in C\,(y) \Rightarrow y R z';\ \text{y como } x R y \Rightarrow x R z',\ \text{o sea, } C\,(y) \subset C\,(x)$$

y por definición de igualdad de conjuntos

$$C\,(x) = C\,(y)$$

Al conjunto de las clases de equivalencia definidas por R se le llama conjunto cociente de E respecto de R y se representa E/R

EJEMPLO:

Las congruencias aritméticas.

Sea el conjunto Z de los números enteros. Dado un entero m fijo, llamaremos congruencia módulo m a la relación definida:

$$x \equiv y_{(m} \quad \text{si y solamente si} \qquad x - y = k \cdot m, \quad k \in z$$

Es evidente que las clases de equivalencia las definen los posibles restos que se puedan obtener al dividir los enteros por m, es decir:

$C\,(0) = \{ \ldots -3m, -2m, -m, 0, m, 2m, 3m \ldots \}$

$C\,(1) = \{ \ldots -3m{+}1, -2m{+}1, -m{+}1, 1, m{+}1, 2m{+}1, 3m{+}1 \ldots \}$

$\vdots$

$C\,(m-1) = \{ \ldots -3m+(m-1), -2m+(m-1), -m+(m-1), m-1, m+(m-1) \ldots \}$

Con lo que el conjunto cociente

$$Z/R = \left\{ \{\dot{m}\}, \{\dot{m} + 1\}, \{\dot{m} + 2\} \ldots \{\dot{m}, + m-1\} \right\}$$

En el caso de que

$$m = 5 \qquad Z/5 = \left\{ \{\dot{5}\} \{\dot{5} + 1\}, \{\dot{5} + 2\}, \{\dot{5} + 3\}, \{\dot{5} + 4\} \right\}$$

$$m = 6 \qquad Z/6 = \left\{ \{\dot{6}\}, \{\dot{6} + 1\}, \{\dot{6} + 2\}, \{\dot{6} + 3\}, \{\dot{6} + 4\}, \{\dot{6} + 5\} \right\}$$

Las clases de equivalencia definen una partición en E, pues

a) Por 1.—Toda clase es no vacía

b) Por 4.—Dos clases cualesquiera son disjuntas

c) por definición de relación de equivalencia y por la conclusión 1:

$\forall\ x, x \in$ E pertenece a alguna clase, luego reunidas nos dan E.

Es decir:

Relación de equivalencia en E $\Rightarrow$ partición de E.

De igual forma:

Partición de E $\Rightarrow$ relación de equivalencia en E, pues basta definir R de tal manera que $(x R y) \iff$ (x e y pertenecen a la misma parte de E).

Luego:

$$\boxed{\text{R. Equivalencia en E} \iff \text{, partición en E.}}$$

3-3 APLICACION CANONICA DE E SOBRE E/R

a) Llamaremos así a una aplicación $f: E \to E/R$, tal que $\not> x \in E$ $\forall\ x \in E\ \forall\ x \in E\ f(x) = C(x)$ "su imagen es su clase de equivalencia".

Es evidente que, como

$$C(x) \subset E \quad f(C(x)) = C(x)$$

es decir, todos los elementos de una clase tienen como imagen su clase.

Esta aplicación es exhaustiva, ya que

$$\forall\ C(x) \in {}^{E}/_{R}, \quad \exists x \in E \mid f(x) = C(x)$$

3-4 DESCOMPOSICION DE UNA APLICACION

Toda función entre A y B, $f: A \to B$ se puede descomponer en producto de otras dos: una suprayectiva y otra inyectiva.

En efecto:

Por la proposición de 3-1, f establece una relación de equivalencia en A que notaremos R_f definida.

$$\text{Si } x \in A \quad y \in A, \quad xRy \quad \text{si} \quad f(x) = f(y)$$

Consideremos el conjunto cociente A/R_f de A respecto de R_f

Por definición de aplicación canónica

$$p_f : A \to A/R_f \text{ será exhaustiva.}$$

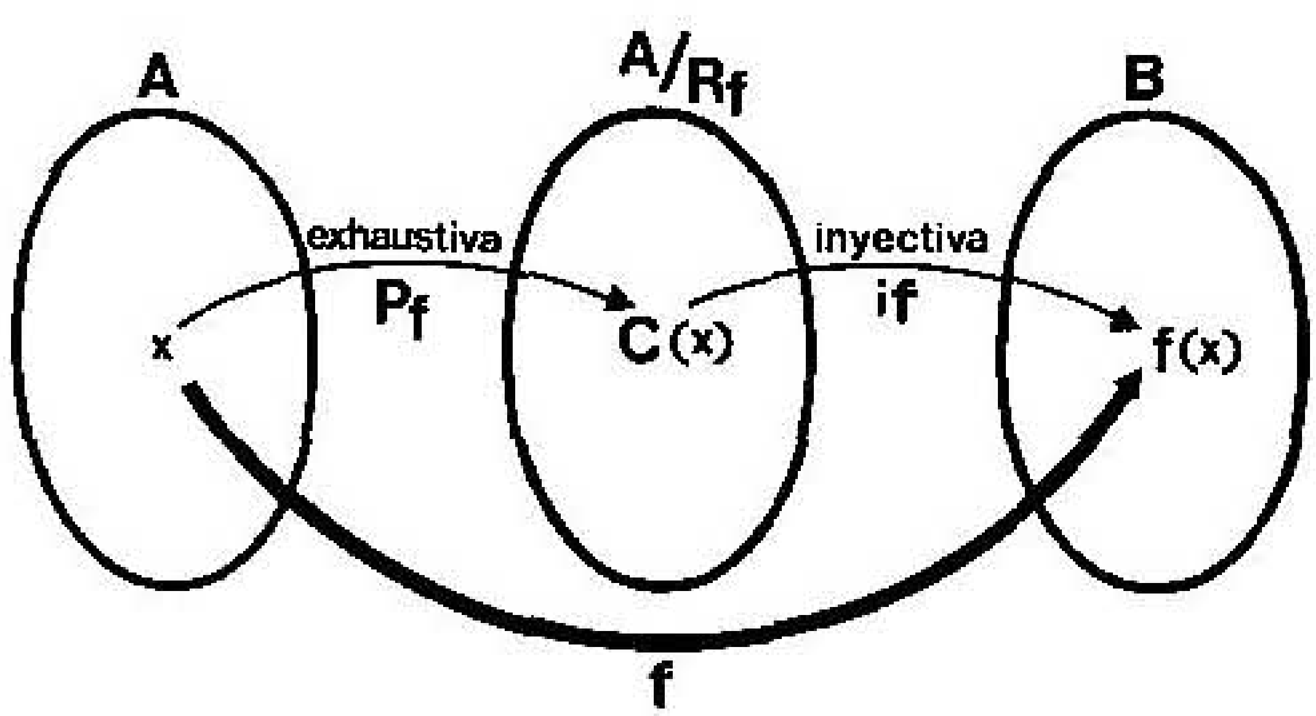
Definamos una nueva aplicación i_f

$$i_f : A/R_f \to B$$

tal que $i_f\ (C\ (x)) = f\ (x)$, que evidentemente será inyectiva, pues por la definición de R_f y las propiedades de las clases

$$\text{si } C\ (x) \neq C\ (y) \text{ entonces } f\ (x) \neq f\ (y)$$

Es decir:



$$f = i_f \cdot p_f$$

esto también se representa

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "P_f"'] & B \\ A/R_f \arrow[ur, "if"'] & \end{tikzcd}$$

la descomposición se hace a través del conjunto cociente A/R

3-5 EQUIVALENCIA S CONTENIDA EN OTRA R

Sea el conjunto E y en él definidas dos relaciones de equivalencia S y R. Diremos que la relación S está contenida en R si

$$xSy \Rightarrow xRy \qquad \forall\, x, y \in E$$

se dirá que S es más fina que R.

Luego toda clase de equivalencia de S estará contenida en una clase de R

$$C_S\,(x) \subset C_R\,(x)$$

Existen relaciones que no son comparables, es decir:

ni S es más fina que R
ni R más fina que S

— La igualdad en E está contenida en toda relación de equivalencia definida en E.
— Toda relación R definida en E está contenida en una relación universal V_E, cuya única clase de equivalencia es el propio E.

EJEMPLO:

Sea el conjunto Z de los enteros y consideremos las congruencias aritméticas Z/2, Z/4, evidentemente, Z/4 es más firme que Z/2.

$$Z/2 = \{\{\dot{2}\},\ \{\dot{2}+1\}\}$$
$$Z/4 = \{\{\dot{4}\},\ \{\dot{4}+1\},\ \{\dot{4}+2\},\ \{\dot{4}+3\}\}$$

y se cumple

$$\{\dot{4}\} \subset \{\dot{2}\} \qquad \{\dot{4}+1\} \subset \{\dot{2}+1\}$$

$$\{\dot{4}+2\} \subset \{\dot{2}\} \qquad \{\dot{4}+3\} \subset \{\dot{2}+1\}$$

Es decir, $C_{Z/4} \subset C_{Z/2}$; las clases de Z/4 están incluidas en las de Z/2.

3-6 RELACIONES DE ORDEN

Dado un conjunto E, establezcamos una correspondencia R_o (G,E,E) cuyo conjunto inicial y final sea E. Diremos que R_o es una relación de orden si como correspondencia cumple

1. $R_o \cdot R_o = R_o$
2. $R_o \cap R_o^{-1} = \Delta$ siendo Δ la diagonal principal de E $\times$ E.

Es decir, si el producto de la correspondencia por sí misma coincide con R_o y si la intersección con su correspondencia inversa nos da la diagonal principal de E $\times$ E; dicha correspondencia definirá una relación de orden.

Consecuencias:

a) De 1.—*Por definición de producto de correspondencias.*
Si $((x,y) \in G \wedge (y,z) \in G) \Rightarrow (x,z) \in G$ *propiedad transitiva.*

b) De 2.—Si $\left.\begin{array}{r}(x,y) \in G \\ (x,y) \in G^{-1}\end{array}\right\}$ $(x,y) \in G \cap G^{-1} = \Delta$, luego $x = y$, *propiedad antisimétrica.*

c) De 2.—Por intersección: $G \cap G^{-1} = \Delta \Rightarrow (\Delta \subset G \wedge \Delta \subset G^{-1}) \Rightarrow$
$\forall x \quad x \in E \quad (x,x) \in G \Rightarrow$ *propiedad reflexiva.*

O sea, son equivalentes

$$x \in E \iff (x,x) \in G$$

Es decir, podríamos definir una relación de orden en un conjunto E como una relación binaria que cumple las propiedades:

1) Reflexiva $\forall x \in E \; (x,x) \in G$

2) Antisimétrica $\left.\begin{array}{l}(x,y) \in G \\ (y,x) \in G\end{array}\right\} \Rightarrow x = y$

3) Transitiva $\left.\begin{array}{l}(x,y) \in G \\ (y,z) \in G\end{array}\right\} \Rightarrow (x,z) \in G$

Notación: Cuando en un conjunto E, definimos una relación de orden R_o (G,E,E), indicaremos $x \leqslant y$ como equivalente a $(x,y) \in G$ y leeremos "x anterior a y".

De igual forma $y \geqslant x$ se leerá "y posterior a x".
En el caso en que con seguridad $x \neq y$ se indicará:
$x < y$ "x estrictamente anterior a y".
$x > y$ "x estrictamente posterior a y".

Relación de orden inducida sobre un subconjunto A de E.
Sea un conjunto E y en él definida una relación de orden R_o (G,E,E), si consideramos un subconjunto A de E, podemos establecer el grafo G'

$$G' = A \times A \cap G$$

que definiría otra relación que también sería de orden R'_o (G',A,A) inducida por G' en A, pues:

a) $G' \subset A \times A$

b) $G' \subset G$

y por tanto, cumpliría para A las mismas propiedades que G para E.

3-7 ORDEN TOTAL Y ORDEN PARCIAL

Orden total.—Una relación de orden R_o definida en un conjunto E diremos que es de orden total si:

$$\forall x \in E, \; \forall y \in E \quad \text{se cumple } (x \leqslant y) \vee (y \leqslant x)$$

es decir, para cualquier para de elementos de E, o bien $(x,y) \in G$ o $(y,x) \in G$.
"Cualquier par de elementos es comparable."

Un conjunto se llama *totalmente ordenado* si se ha definido en él un orden total.
Orden parcial.—Diremos que una relación de orden R_o definida en E es de orden parcial cuando:

$\exists x \in E, \exists y \in E$ tales que: $x \not\leqslant y \wedge y \not\leqslant x$

Es decir:

$\exists (x,y) \in E \times E \,/\, ((x,y) \notin G \wedge (y,x) \notin G)$

O sea, podamos encontrar pares de elementos de E no comparables por R_o

---

EJEMPLOS:

1.—El orden natural en N es un orden total.
2.—Dado un conjunto E, consideremos el conjunto P(E) partes de E.
La relación de inclusión en P(E) constituye un orden parcial.
En efecto:

$\forall A, A \in P(E) \quad A \subset A$ reflexiva.

$\left.\begin{array}{l} A \subset B \\ B \subset A \end{array}\right\} \Rightarrow A = B$ antisimétrica

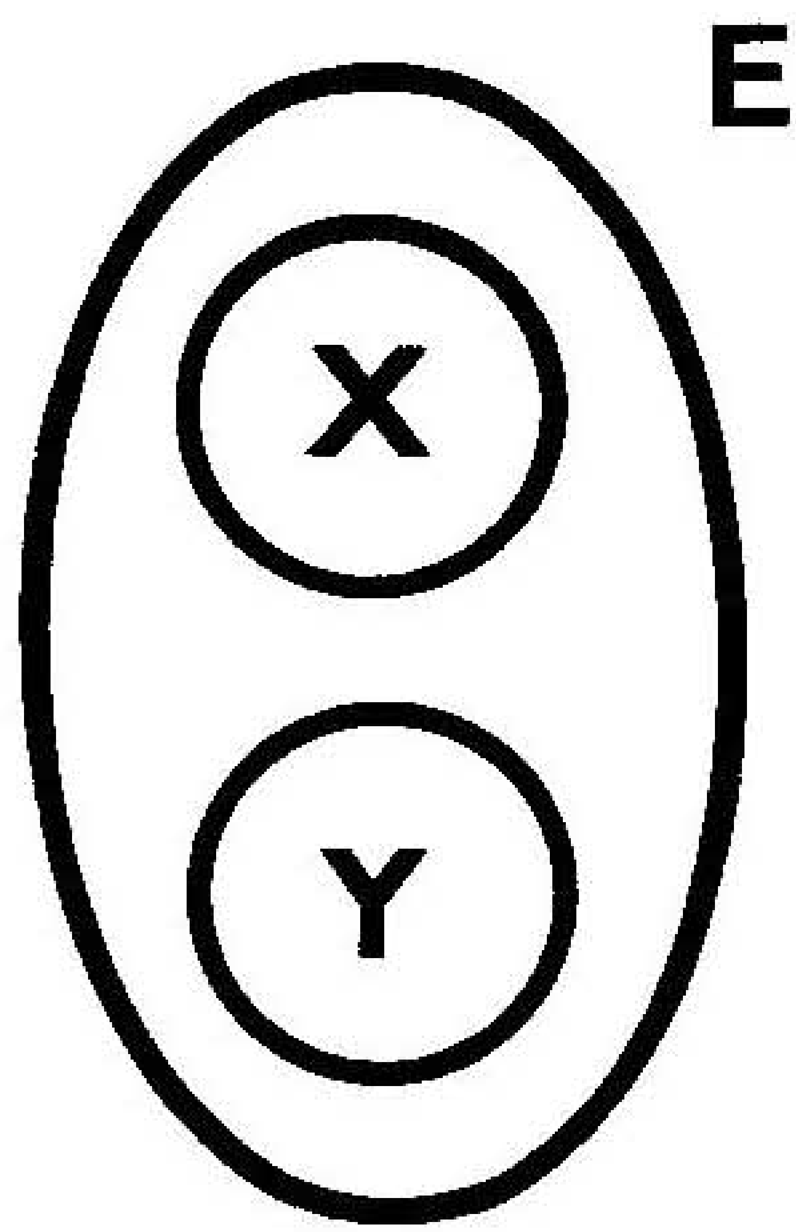
$\left.\begin{array}{l} A \subset B \\ B \subset C \end{array}\right\} \Rightarrow A \subset C$ transitiva

Sin embargo, podemos encontrarnos con:

$X \in P(E)$
$Y \in P(E)$

pero:

$X \not\subset Y$ y $Y \not\subset X$ que no fueran comparables.



3-8 APLICACIONES CRECIENTES Y DECRECIENTES

Dados dos conjuntos E y E' ordenados diremos:

a) que una aplicación f es estrictamente creciente, $f: E \rightarrow E'$, si

$$x < y \Rightarrow f(x) < f(y)$$

a') que es creciente si

$$x \leqslant y \Rightarrow f(x) \leqslant f(y)$$

b) que es estrictamente decreciente si

$$x < y \Rightarrow f(x) > f(y)$$

b') que es decreciente si

$$x \leqslant y \Rightarrow f(x) \geqslant f(y)$$

En general, diremos que una aplicación es monótona si es creciente o decreciente.

3-9 ELEMENTOS MAXIMAL Y MINIMAL

a) Sea el conjunto E y en él definida una relación de orden R_o, si existe un elemento $a \in E$ y tal que $\forall x \in E$, $a \leqslant x \Rightarrow a = x$, este elemento a se le llama elemento maximal de E. Es decir, en E no existe ningún elemento estrictamente mayor que a.

b) Dado un conjunto E y en él definida una relación de orden R_o, si existe un elemento $a \in E$ y tal que $\forall x \in E$, $x \leqslant a \Rightarrow x = a$, este elemento a le llamaremos elemento minimal de E. Es decir, en E no existe ningún elemento estrictamente menor que a.

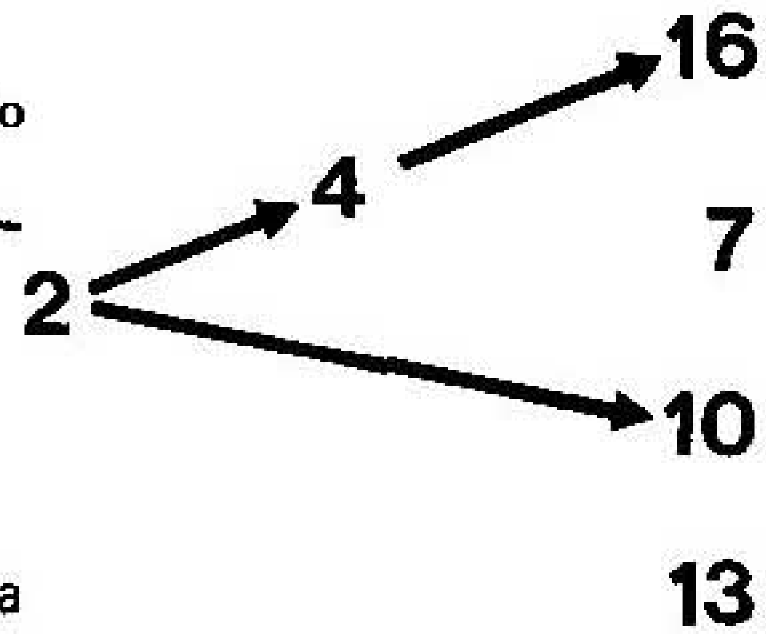
EJEMPLO:

Sea $E = \{2, 4, 7, 10, 13, 16\}$

y definamos $x \leqslant y \Longleftrightarrow y = \dot{x}$

Es decir: y mayor que x si y es múltiplo de x.

Que representándola gráficamente:



2 será elemento minimal, y 7, 10, 13, 16 serán los elementos maximales; siendo el 7 y el 13, a la vez, maximales y minimales.

3-10 ELEMENTOS MAXIMO Y MINIMO

a) Elemento máximo.

En un conjunto E ordenado, llamaremos elemento máximo $a \in E$ a un elemento tal que $\forall x \in E \quad x \leqslant a$.

b) Elemento mínimo.

En un conjunto E ordenado, llamaremos elemento mínimo $a \in E$ a un elemento tal que $\forall x \in E \quad a \leqslant x$,

TEOREMA

En un conjunto ordenado, si existe elemento máximo (mínimo) es único.

En efecto, supongamos que no, que existen dos elementos a y a' máximos, distintos.

$$\left.\begin{array}{l} \text{Por ser } a \text{ máximo } \forall x \in E \quad x \leqslant a \text{ y como } a' \in E \quad a' \leqslant a \\ \text{Por ser } a' \text{ máximo } \forall x \in E \quad x \leqslant a' \text{ y como } a \in E \quad a \leqslant a' \end{array}\right\}$$

Luego por la propiedad antisimétrica

$$a = a'$$

Idem para mínimo.

EJEMPLO:

Sea $E = \{a\ b\ c\}$ y sea $P(E) = \{\phi, \{a\}, \{b\}, \{c\}, \{a\ b\}, \{a\ c\}\ \{b\ c\}\ \{a\ b\ c\}\}$

Tomemos $\quad A \subset P(E)\ A = \{\{a\}\ \{b\}\ \{a\,b\}\ \{a\,b\,c\}\}$

Representando la relación de inclusión en A por flechas:

$$\begin{tikzcd}[row sep=small] \{a\} \arrow[dr] & & \\ & \{a\,b\} \arrow[r] & \{a\,b\,c\} \\ \{b\} \arrow[ur] & & \end{tikzcd}$$

El máximo será $\{a\ b\ c\}$, pues todo elemento de A es anterior (en la inclusión) a él.
No existirá mínimo.

3-11 CONJUNTO BIEN ORDENADO

Un conjunto se llama bien ordenado cuando todo subconjunto de él, considerado como conjunto ordenado, tiene un elemento mínimo.

3-12 CONJUNTOS ACOTADOS

Dado un conjunto E ordenado, llamaremos "cota inferior" o minorante de un subconjunto X de E, $X \subset E$ a todo elemento $c \in E$, tal que

$$\forall x \in X \quad c \leqslant x$$

Análogamente, de un conjunto E ordenado, llamaremos "cota superior" o mayorante de un subconjunto $X \subset E$ a todo elemento $c \in E$, tal que

$$\forall x \in X \quad x \leqslant c$$

Es evidente que si c es cota inferior de X y $c' < c$, c' también es cota inferior.
Y si c es cota superior de X y $c' > c$, entonces c' es también cota superior. Si un conjunto X posee cota superior se llama acotado superiormente; si posee cota inferior, acotado inferiormente, y si posee ambas, conjunto acotado.

3-13 EXTREMO SUPERIOR Y EXTREMO INFERIOR

Dado un conjunto E ordenado y un subconjunto $X \subset E$, acotado:

a) llamemos M al conjunto de las cotas superiores de X, evidentemente $M \subset E$; al elemento mínimo —cuando exista— de M le llamaremos *extremo superior* de X *(a la menor de las cotas superiores).*

b) Llamemos *m* al conjunto de las cotas inferiores de X, $m \subset E$ al elemento máximo de *m* (cuando exista) se le llama *extremo inferior* de X *(a la mayor de las cotas inferiores).*

Por el teorema anterior es inmediato, que si existe extremo superior (o inferior) será único.

Es evidente que:

– Si E ordenado y $A \subset E$ admiten extremo superior e inferior

$$\text{inf. } A \leqslant \text{sup. } A$$

– Si $A \subset E$ y $B \subset E$ admiten extremo superior (o inferior), entonces si $A \subset B$

$$\text{inf. } B \leqslant \text{inf. } A$$
$$\text{sup. } A \leqslant \text{sup. } B$$

3-14 CONJUNTOS FILTRANTES

Un conjunto ordenado E se llama filtrante decreciente cuando dados dos elementos cualesquiera *x y* de E, existe otro $z \in E$ tal que

$$z \leqslant X \wedge z \leqslant y$$

Análogamente se define el filtrante creciente cuando para dos elementos cualesquiera de E, x, y existe un $z \in E$, tal que:

$$z \geqslant x \quad \wedge \quad z \geqslant y$$

3-15 INTERVALOS

Sea un conjunto E totalmente ordenado y dos elementos $a \in E$ $b \in E$ tales que $a \leqslant b$ llamaremos intervalo de origen a y extremo b:

a) Intervalo cerrado

$$[a\ b] = \{ x \in E \mid a \leqslant x \leqslant b \}$$

b) Intervalo semiabierto a la izquierda

$$]a\ b] = \{ x \in E \mid a < x \leqslant b \}$$

c) Intervalo semiabierto a la derecha

$$[a\ b[= \{ x \in E \mid a \leqslant x < b \}$$

d) Intervalo abierto

$$]a\ b[= \{ x \in E \mid a < x < b \}$$

Existen tipos de intervalos ilimitados:

a) De origen a ilimitado a la derecha

cerrado $[a \rightarrow [= \{ x \in E \mid a \leqslant x \}$
abierto $]a \rightarrow [= \{ x \in E \mid a < x \}$

b) De extremo b, ilimitado a la izquierda

cerrado $] \leftarrow b] = \{ x \in E \mid b \geqslant x \}$
abierto $] \leftarrow b [= \{ x \in E \mid b > x \}$

El conjunto E, el mismo, es del tipo doblemente ilimitado

$$] \leftarrow , \rightarrow [$$

3-16 PRINCIPIO DE INDUCCION TRANSFINITA (PRINCIPIO DE RECURRENCIA)

Sea E un conjunto bien ordenado y $P(x)$ una función proposicional que establece una propiedad P para los elementos x de E.

"Si para cualquier $x \in$ E se tiene que los elementos de E anteriores a x cumplen la propiedad P y esto implica que x también la cumple, entonces todos los elementos de E cumplen la propiedad P".
Es decir:

Hipótesis

$$[(x \in E \wedge y \in E \mid y < x) \Rightarrow P(y)] \Rightarrow P(x)$$

Tesis

$$P(x) \qquad \forall x \in E$$

En efecto: Supongamos que existe $A \subset E$ subconjunto de E tal que sus elementos no cumplen P

$$A = \{ z \mid \neg P(z) \} \quad A, \subset E$$

por ser E bien ordenado, A tendrá un elemento mínimo $z_0 . \in A$ anterior a todos los elementos de A. Analicemos este elemento z_0.

1) Por ser $z_0 \in A$, $\neg P(z_0)$ *no cumplirá* la propiedad P.
2) Pero consideremos el conjunto $B \subset E, B = \{ y \mid y < z_0 \}$ como $\forall y \in B \Rightarrow y \notin A$, entonces $\forall y \in B$ se cumplirá la propiedad $P(y)$, y como por hipótesis

$$\text{si } [(\forall y \in E, y < z_0)\, P(y)] \Rightarrow P(z_0)$$

se llega a la conclusión que z_0 *sí cumple* la propiedad P, luego es contradictorio que z_0 cumpla y no cumpla P, luego no puede existir el conjunto A.

3-17 TEOREMA DE ZERMELO

Todo conjunto puede ser bien ordenado (sobre todo conjunto se puede definir una buena ordenación).

3-18 CONJUNTO INDUCTIVO

Se dice que un conjunto ordenado E es inductivo si todo subconjunto totalmente ordenado de él tiene al menos una cota superior en E.

TEMA 4 | ESTRUCTURAS ALGEBRAICAS: GRUPOS

4-1 LEYES DE COMPOSICION. DEFINICION

Consideremos un conjunto E cualquiera. Llamamos ley de composición interna (l.c.i.) definida sobre E a una aplicación

$$f : E \times E \to E$$

Siendo $E \times E$ el producto cartesiano de E por E.

Por definición, pues, de aplicación:

$$\forall\, (x,y), (x,y) \in E \times E, \quad \exists\,!\ \ z, z \in E \mid f\,(x,y) = z$$

Luego a cada par (x,y) de elementos de E queda asociado uno y sólo un elemento z de E. Esto podríamos pues indicarlo sin más así:

$$(x,y) \to z$$

Omitiendo ya la f que sólo indica "corresponde uno y sólo uno", lo cual viene ahora indicado por la flecha.

También, puesto que a cada par (x,y) va asociada una imagen y sola una, $f(x,y)$, la podemos representar por

$$f(x,y) = x \perp y$$

donde $\perp$ es un signo convencional que por sí solo no indica nada.
La proposición "$x \perp y$" es equivalente a: "$x \perp y$ es imagen por medio de f del par $(x\ y)$".
Puesto que una aplicación entre dos conjuntos dados viene definida por las imágenes que da de cada elemento del primer conjunto, y las imágenes las escribimos con el símbolo $\perp$, podemos, pues, decir simbólicamente que $\perp$ es la ley de composición definida sobre el conjunto E.
La ley de composición $\perp$ definida sobre E, por ser una aplicación, posee un grafo G cuya primera proyección es el dominio:

$$\text{proy } G_1 = E \times E$$

y cuya proyección segunda es un subconjunto de E:

$$\text{proy}_2\ G \subset E$$

En la práctica se utiliza para designar las leyes de composición los símbolos (+), (·), (X), etcétera.

EJEMPLOS:

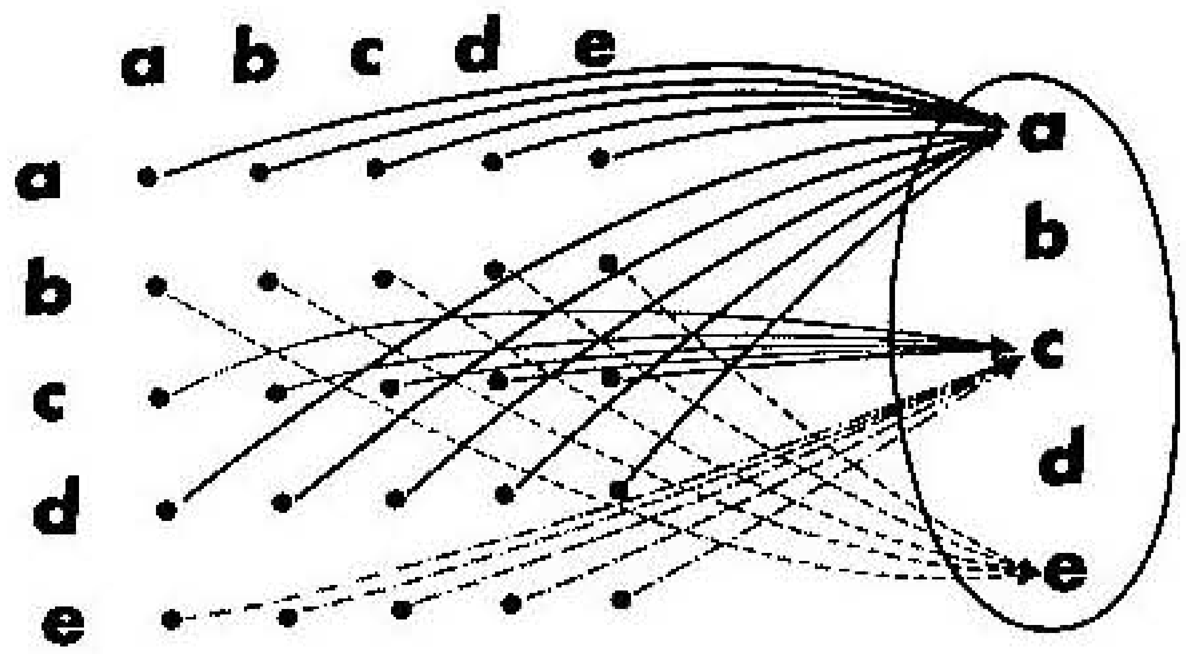
1) Supongamos que el conjunto E sea finito y sus elementos sean:

$$E = \{a, b, c, d, e\}$$

Entonces el producto cartesiano E X E es un conjunto que podemos representar por:

E×E	a	b	c	d	e
a	(a,a)	(b,a)	(c,a)	(d,a)	(e,a)
b	(a,b)	(b,b)	(c,b)	(d,b)	(e,b)
c	(a,c)	(b,c)	(c,c)	(d,c)	(e,c)
d	(a,d)	(b,d)	(c,d)	(d,d)	(e,d)
e	(a,e)	(b,e)	(c,e)	(d,e)	(e,e)

Consideremos la aplicación $f: E \times E \to$ definida como indica la figura:



Entonces esta aplicación es una ley de composición interna que podemos representar por la tabla:

$\perp$	a	b	c	d	e
a	a	a	a	a	a
b	e	e	e	e	e
c	c	c	c	c	c
d	a	a	a	a	a
e	c	c	c	c	c

diciendo $a \perp a = a$

" $c \perp b = c$

" $d \perp e = a$

2) Sea ahora E el conjunto $E = \{x_1\ x_2\ x_3\ x_4\}$ y definimos en él la ley de composición $\forall\, a,b \in E \quad a \perp b = a$. Entonces la tabla de esta ley será:

$\perp$	x_1	x_2	x_3	x_4
x_1	x_1	x_1	x_1	x_1
x_2	x_2	x_2	x_2	x_2
x_3	x_3	x_3	x_3	x_3
x_4	x_4	x_4	x_4	x_4

$\perp$ es la aplicación que $\forall (a\ b),\ (a\ b) \in E \times E \to f(a\ b) = a$. A cada par le asocia su primera componente.

4-2 PARTE ESTABLE DE UN CONJUNTO PARA UNA L.C.I.

Sea E un conjunto cualquiera y $A \subset E$ un subconjunto de él.

Supongamos que se tiene definida sobre E una ley de composición $\perp$ tal que

$$\forall\ (a,b),\ (a,b) \in E \times E \rightarrow a \perp b \in E$$

Decimos entonces que A es una parte estable para dicha ley de composición si

$$\forall\ x,\ \forall\ y,\ x \in A,\ y \in A,\ x \perp y \in A$$

lo que podemos enunciar diciendo: "Los elementos que se obtienen al operar la ley de composición interna sobre los pares de elementos de A son elementos de A."

EJEMPLO:

Consideremos el conjunto Z^+ de los números enteros positivos:

$$Z^+ = \{1, 2, 3...\}$$

Definimos en él una ley de composición interna que llamamos producto y que representamos por:

$$\forall\ x, \forall\ y\quad x \in Z^+\quad y \in Z^+\quad (x\ y) \rightarrow x\ .\ y \in Z^+$$

Tomemos ahora un subconjunto de Z^+. El conjunto de los múltiples de 2.

$$A \subset Z^+\quad A = \{a \mid a \in Z^+ \wedge a = \dot{2}\}$$

Entonces: $\forall\ a,a' \in A\quad (a\ a') \rightarrow a \cdot a' = \dot{2} \cdot \dot{2} = \dot{2}$

Luego: $a \cdot a' \in A$

Se dice, pues, que A es parte estable del conjunto de los enteros positivos para la multiplicación.

4-3 PROPIEDADES DE LAS LEYES DE COMPOSICION

Estudiaremos ahora como propiedades de las leyes de composición la asociativa y conmutativa.

a) *Asociativa.*—Dado un conjunto E, sea $\perp$ la ley de composición definida sobre él. Se dice que esta ley es asociativa si

$$\forall\ x,y,z \in E \qquad x \perp (y \perp z) = (x \perp y) \perp z$$

Entonces si la ley es asociativa, podemos aliminar los paréntesis, teniendo sentido escribir la composición de tres elementos de E, por ejemplo, así:

$$x \perp y \perp z \qquad \forall\ x,y,z \in E$$

puesto que

$$x \perp y \perp z \to (x \perp y) \perp z$$

donde $x \perp y$ es un elemento de E que podemos llamarle c, y $c \perp z$ es otro elemento de E que le llamaremos d. Y así aunque fuera un número mayor de elementos.
Se puede utilizar para representar la ley el símbolo $(\cdot)$ notación multiplicativa. En este caso acordaremos llamar al elemento imagen del par $(x,x) \to x^2$

$$(x,x) \to x \cdot x = x^2$$

Cuando la ley $(\cdot)$ es asociativa, esta notación se puede generalizar:

$$(x \cdot x) \cdot x = x \cdot (x \cdot x) = x^3$$

y, en general:

$$\underbrace{x \cdot x \cdot x \ldots x}_{n \text{ veces}} = x^n$$

Si utilizamos la notación aditiva $(+)$ y la ley es asociativa, entonces, al elemento que corresponde al par (x,x) se le puede representar por

$$(x,x) \to x + x = 2x$$

y en general

$$\underbrace{x + x + x \ldots + x}_{n \text{ veces}} = n \cdot x$$

b) *Conmutativa.*—Sea E un conjunto dado y sea $\perp$ una ley de composición definida en él. Se dice que dicha ley es conmutativa si:

$$\forall\, x, y \in \mathrm{E} \qquad x \perp y = y \perp x$$

EJEMPLO

Consideremos un conjunto A y sea $\mathrm{E} = \mathrm{P(A)}$. Definimos $*$ en E la ley de composición del siguiente modo:

$$\forall\, x, y \in \mathrm{E} \qquad x * y = x \cap y$$

$x \cap y \in \mathrm{P(A)}$, puesto que la intersección de dos subconjuntos de A es otro subconjunto de A.

La ley $(*)$ así definida es asociativa:

$$\forall\, x,y,z \in \mathrm{E} \qquad \begin{aligned} (x * y) * z &= (x \cap y) \cap z \\ x * (y * z) &= x \cap (y \cap z) \end{aligned}$$

y como la intersección es asociativa

$$\boxed{(x *) * z = x * (y * z)}$$

La ley $(*)$ es conmutativa:

$$\forall\, x,y \in \mathrm{E} \qquad \begin{aligned} (x * y) &= x \cap y \\ (y * x) &= y \cap x \end{aligned}$$

y puesto que la intersección es conmutativa:

$$\boxed{x * y = y * x}$$

4-4 CONJUNTOS CON UNA L.C.I.

Supongamos un conjunto E sobre el que se ha definido una l.c.i. $\perp$.

1) Elemento regular.—En un conjunto E con una l.c.i. cualquiera, en general *no es cierto* que

$$\forall\, x \in \mathrm{E} \qquad x \perp a = x \perp \quad \Longrightarrow a = b$$

$$\forall\, y \in \mathrm{E} \qquad c \perp y = d \perp \quad \Longrightarrow c = d$$

Sin embargo, hay algunos elementos particulares en el conjunto para los que sí es cierto.
Llamamos *elemento regular* de un conjunto E, con una ley $\perp$ a un $a \in$ E, tal que:

$$\forall x \in E \left\{ \begin{array}{l} a \perp x = a \perp y \Rightarrow x = y \\ x \perp a = y \perp a \Rightarrow x = y \end{array} \right.$$

en este sentido, se dice que al elemento regular se le puede aplicar la *regla de simplificación*

2) *Elemento neutro.*—Se llama así a un elemento $e \in$ E, si existe, tal que

$$\forall x \in E \quad e \perp x = x \perp e = x \quad (1)$$

Teorema 1: Dado un conjunto E con una ley $\perp$, si existe elemento neutro e, éste es único.
Para demostrarlo lo haremos por reducción al absurdo.
Supongamos que existen dos elementos neutros distintos:

$$e' \in E \quad y \quad e'' \in E \quad e' \neq e''.$$

Entonces, por definición de neutro e':

$$\forall x \in E \quad e' \perp x = x \perp e' = x \quad (2)$$

y por definición de e'':

$$\forall x \in E \quad e'' \perp x = x \perp e'' = x \quad (3)$$

$$\left.\begin{array}{ll} \text{Particularicemos la ecuación (2) para } x = e'' & : e' \perp e'' = e'' \perp e' = e'' \\ \text{Particularicemos la ecuación (3) para } x = e' & : e'' \perp e' = e' \perp e'' = e' \end{array}\right\} e' = e''$$

contrariamente a la hipótesis de que eran distintos, luego el neutro es único.

Ejemplo 1: En el conjunto de los enteros Z, si definimos en él la multiplicación (·), el $1 \in Z$ es elemento neutro, pues

$$\forall x \in Z \quad x \cdot 1 = 1 \cdot x = x$$

Ejemplo 2: En el conjunto $E = P(A)$, visto anteriormente con la ley

$$\forall x,y \in E \quad x \perp y = x \cap y$$

el elemento neutro es el conjunto $A \in P(A)$, puesto que:

$$\forall x \in E \quad x \cap A = x$$

Ejemplo 3: En el conjunto $E = P(A)$, si definimos la ley (*) como

$$\forall x,y \in E \quad x * y = x \cup y$$

el elemento neutro es el conjunto vacío $\phi \in E$, puesto que

$$\forall x \in E \quad x \cup \phi = x$$

3) *Elemento simétrico.*— Supongamos que el conjunto E admite un elemento neutro $e \in E$ para la ley $\perp$.

Llamamos *simétrico a la izquierda* de un elemento $x \in E$, a todo elemento $x' \in E$ tal que

$$x' \perp x = e$$

Y se dice que $x'' \in E$ es un *simétrico a la derecha* del elemento $x \in E$, si

$$x \perp x'' = e$$

Dado el elemento $x \in E$ se llama *simétrico* simplemente a todo elemento $x' \in E$ tal que

$$x \perp x' = x' \perp x = e$$

Ejemplo 1: Sea el conjunto $E = Q - \{0\}$ (los racionales distintos de cero) y consideramos la ley producto (·) definida en él. En este conjunto todos los elementos tienen simétrico (que lo es a su vez a la derecha y a la izquierda), que por ser la ley multiplicativa se le denomina "inverso" y se le representa por $x^{-1} = \frac{1}{x}$

$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$

Ejemplo 2: En el conjunto de los racionales Q con ley (+) todos los elementos tienen simétrico, que, ahora, por ser la ley aditiva se llaman "opuesto" y se representan por $(-x)$

$$\forall x \in Q \quad x + (-x) = (-x) + x = 0$$

Teorema 2.—Sea E un conjunto con una ley de composición $\perp$ definida en él. "La condición necesaria y suficiente para que un elemento $x \in E$ tenga un simétrico $x' \in E$, es que exista algún simétrico x'_i a la izquierda de x y algún simétrico de x a la derecha x'_d. Además, este elemento simétrico x' es único.

En efecto: Para ello supongamos, como dice el enunciado, que x posee algún simétrico a la izquierda y algún simétrico a la derecha. Como estos simétricos podrían no ser únicos, para mayor generalidad supondremos que x posee un conjunto de simétricos a la izquierda $\{S_i\}$, y un conjunto de simétricos a la derecha $\{S_d\}$.

Los elementos de S_i cumplen, en virtud de su propia definición, que:

$$\forall x'_i, x'_i \in S_i \qquad x'_i \perp x = e \quad (4)$$

Y los de S_d:

$$\forall x'_d, x'_d \in S_d \qquad x \perp x'_d = e \quad (5)$$

Tomemos ahora un elemento $a'_i \in S_i$ fijo. Entonces por definición de neutro

$$a'_i = a'_i \perp e$$

Teniendo en cuenta (5)

$$a'_i = a'_i \perp (x \perp x'_d) \qquad \forall x'_d, x'_d \in S_d$$

Y por la propiedad asociativa:

$$a'_i \perp (x \perp x'_d) = (a'_i \perp x) \perp x'_d$$

Aplicando ahora el segundo miembro la expresión (4) queda

$$a'_i = a'_i \perp (x \perp x'_d) = (a'_i \perp x) \perp x'_d = e \perp x'_d = x'_d$$

Luego

$$\forall x'_d, \quad x'_d \in S_d \Rightarrow x'_d = a'_i.$$

Es decir, que el conjunto S_d es el conjunto de un elemento $S_d = \{a'_i\}$. Del mismo modo, tomando ahora al único elemento $a'_i \in S_d$ y teniendo en cuenta (4) y (5).

$$a'_i = e \perp a'_i = (x'_i \perp x) \perp a'_i = x'_i \perp (x \perp a'_i) = x'_i \perp e = x'_i \quad \forall x'_i, x'_i \in S_i$$

Luego S_i es también el conjunto de un elemento

$$S_i = \{a'_i\} = S_d$$

El elemento a'_i cumple pues

$$x \perp a'_i = a'_i \perp x = e$$

Luego a'_i es el único simétrico de x, y le representaremos por x'.

Inversamente: Si un $x \in E$ viene por simétrico x', por definición $x \perp x' = x' \perp x = e$. Luego x' es a la vez simétrico a la izquierda y a la derecha.

Teorema 3.—Si $x \in E$ tiene como simétrico a $x' \in E$, entonces $x' \in E$ tiene como simétrico a x. Es decir:

$$(x')' = x$$

En efecto, si existe algún simétrico de x', habrá de cumplir

$$(x')' \perp x' = x' \perp (x')' = e$$

y por la última expresión del teorema anterior vemos que el elemento x cumple estas igualdades, luego es el único simétrico de x'

$$(x')' = x$$

4-5 GRUPO

Llamamos grupo al par $(G, \perp)$ formado por un conjunto G y una l.c.i. definida sobre él, que cumple las propiedades siguientes:

0) Por definición de l.c.i. sobre G:

$$\forall\, a, b \in G \qquad a \perp b \in G$$

1) Asociativa

$$\forall\, a, b, c \in G \qquad a \perp (b \perp c) = (a \perp b) \perp c$$

2) Existe elemento neutro

$$\exists!\; e \in G \mid \forall\, a \in G \qquad e \perp a = a \perp e = a$$

3) Existe elemento simétrico para cada $a \in G$

$$\forall\, a \in G \qquad \exists!\; a' \mid \qquad a \perp a' = a' \perp a = e$$

Teorema 1.—En todo grupo $(G \perp)$ para todo par de elementos a y b de G existe uno y solo un elemento $x \in G$, que resuelve la ecuación:

$$(1) \qquad a \perp x = b$$

En efecto, por ser a un elemento de G tiene un simétrico $a' \in G$ tal que

$$a \perp a' = a' \perp a = e$$

En la ecuación (1) operamos a la izquierda con a'

$$a' \perp (a \perp x) = a' \perp b$$

en virtud de la propiedad asociativa:

$$(a' \perp a) \perp x = a' \perp b$$

es decir:

$$e \perp x = a' \perp b \Longrightarrow x = a' \perp b$$

Como $a' \in$ G y $b \in$ G, entonces $a' \perp b \in$ G y por definición de $\perp$, es único.

Teorema 2.—En todo grupo (G,$\perp$) para todo par de elementos $a,b, \in$ G existe también un único elemento $y, y \in$ G que resuelve la ecuación.

$$y \perp a = b$$

En efecto: como $a \in$ G tiene simétrico $a' \in$ G luego:

$$(y \perp a) \perp a' = b \perp a'$$

por asociatividad

$$y \perp (a \perp a) = b \perp a'$$
$$y \perp e = b \perp a' \Longrightarrow y = b \perp a'$$

4-6 GRUPO ABELIANO

Se llama *grupo abeliano* a un grupo cuya ley es además conmutativa. Si (M,$*$) es un grupo abeliano, la ley $*$ además de cumplir (0), (1), (2), (3), debe cumplir

4) $\forall\, x,y \in$ M $\quad x * y = y * x$

En un grupo abeliano, los elementos x e y de los teoremas (1) y (2) anteriores son iguales.

Teorema 3.— Si x e $y \in$ G tienen unos simétricos $x', y' \in$ G, $x \perp y$ tiene como simétrico: $y' \perp x'$

$$(x \perp y)' = y' \perp x'$$

En efecto, vamos a ver que este elemento es simétrico de $x \perp y$:

a) $(x \perp y) \perp (y' \perp x') = x \perp (y \perp y) \perp x' = x \perp e \perp x' = x \perp x' = e$

b) $(y' \perp x') \perp (x \perp y) = y' \perp (x' \perp x) \perp y = y' \perp e \perp y = y' \perp y = e$

(como queríamos demostrar), luego $y' \perp x'$ compuesto con $x \perp y$ por la derecha y la izquierda da el neutro, o sea, es su simétrico.

Ejemplo 1.—Consideremos el conjunto de los enteros Z con la ley + definida en él. Entonces (Z, +) es un grupo abeliano, porque cumple las propiedades:

0)

0) $\forall\ x,y \in Z\ \exists!\ z \in Z \mid x + y = z$

1) $\forall\ x,y,z \quad x + (y + z) = (x + y) + z$

2) $\exists\ 0 \in Z \mid \forall\ x \in Z \quad 0 + x = x + 0 = x$

3) $\forall\ x \in Z\ \exists!\ (-x) \mid x + (-x) = (-x) + (x) = 0$

4) $\forall\ x,y \in Z \quad x + y = y + x$

También el conjunto de los números racionales definiendo en ellos una ley + constituyen un grupo abeliano.
El conjunto de los racionales no nulos con una ley (·) definida en ellos constituyen un grupo abeliano multiplicativo.

Hemos visto al principio del tema, que cuando un conjunto tiene un número finito de elementos, la ley de composición definida sobre él puede representarse por una tabla. Por otra parte, se ha definido que un grupo es un par (conjunto, ley) con unas determinadas propiedades. Ahora bien, si la ley cumple estas propiedades, vendrán reflejadas en la tabla. Por tanto, un grupo con un número finito de elementos se puede representar por la tabla correspondiente a su ley de composición interna.
Así, consideremos el conjunto finito: $G = \{a_0\ a_1\ a_2\ a_3\}$ y la ley $\perp$ dada por la tabla:

$\perp$	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_1	a_0	a_1
a_3	a_3	a_0	a_1	a_2

G

G

Se trata de ver si el conjunto G puede tener estructura de grupo con esta ley.

— En primer lugar observamos que posee elemento neutro a_0 pues $\forall a_i \in G \quad a_i \perp a_0 = a_0 \perp a_i = a_i$. Luego podemos decir que el elemento neutro se caracteriza en la tabla porque en su fila y columna correspondientes se repiten los elementos de G en el mismo orden.

— Todos los elementos tienen simétrico. El simétrico del neutro a_0 es el mismo a_0. El simétrico de a_1 es a_3. En la tabla $a_1 \cdot a_3 = a_3 \cdot a_1 = a_0$. El de a_2 es a_2, como se observa en la tabla, pues $a_2 \cdot a_2 = a_0$, y por supuesto, el de a_3 es a_1. Es decir, en todas las filas y columnas aparecerá una vez el a_0.

Sin embargo, hay un detalle importante, y es que dados dos elementos $a_0 \in G$ y $a_2 \in G$, la ecuación

$$x \perp a_1 = a.$$

no tiene solución única, pues:

$$\left.\begin{array}{l} x = a_0 \\ x = a_2 \end{array}\right\}$$

y esto es imposible en la estructura de grupo.

Luego podemos generalizar diciendo que para que una tabla corresponda a un grupo, no se debe repetir ningún elemento en ninguna fila ni en ninguna columna.

Será grupo, por tanto, el conjunto G con una ley $\perp$ que venga dada por la tabla.

$\perp$	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

$a_1 \perp a_2$ = ***Imagen de*** (a_1, a_2)

$a_2 \perp a_1$ = ***Imagen de*** $(a_2\ a_1)$

Compruebe el lector las propiedades de $\perp$.

Cuando el grupo es abeliano, la tabla es simétrica repecto a la diagonal principal, ya que esto significa que la imagen, por ejemplo, del $(a_1\ a_2)$ es la misma que la imagen del elemento $(a_2\ a_1)$.

Vamos a ver ahora un problema inverso de éste. Consideremos tres elementos $x_1\ x_2\ x_3$ cualesquiera. La pregunta es ahora: ¿Cuántos grupos se pueden formar con tres elementos cualesquiera? Evidentemente tantos como leyes de composición que cumplan (1), (2) y (3) podamos definir. Vamos a hallar estos grupos.

a) En primer lugar un grupo debe tener elemento neutro. Sea $x_1 = e$, puesto que los tres elementos son cualesquiera. Esto quiere decir ya que:

$$x_2 \perp x_1 = x_1 \perp x_2 = x_2$$

$$x_3 \perp x_1 = x_1 \perp x_3 = x_3$$

b) Cada elemento del grupo debe tener simétrico dentro del grupo. Entonces como x_1 ya es el neutro, sólo caben dos posibilidades:

$$1)\ \left.\begin{aligned} x'_2 &= x_2 \\ x'_3 &= x_3 \end{aligned}\right\}$$

$$2)\ \left.\begin{aligned} x'_2 &= x_3 \\ x'_3 &= x_2 \end{aligned}\right\}$$

Veamos si en cada una de estas dos posibilidades se obtiene un grupo.

1)

$\perp$	x_1	x_2	x_3
x_1	x_1	x_2	x_3
x_2	x_2	x_1	
x_3	x_3		x_1

$\rightarrow x_2 \perp x_3$

$x_3 \perp x_2$

$x_2 \perp x_3$ puede ser igual, en principio, a x_1 o x_2 o x_3

$$\left.\begin{array}{l} \text{Si } x_2 \perp x_3 = x_2 \Rightarrow x_3 \text{ neutro} \\ \text{Si } x_2 \perp x_3 = x_3 \Rightarrow x_2 \text{ neutro} \end{array}\right\} \text{ no es posible, pues el neutro es } x_1.$$

Por el mismo razonamiento se llega a que $x_3 \perp x_2 = x_1$, quedando la tabla del hipotético grupo como:

$\perp$	x_1	x_2	x_3
x_1	x_1	x_2	x_3
x_2	x_2	x_1	x_1
x_3	x_3	x_1	x_1

Se repiten elementos en filas y columnas, luego se está violando el teorema 1 de grupos. Es decir, esta posibilidad 1) no puede llevarnos a un grupo.

2) $x_2 = x_3$
$x_3 = x_2$

$\perp$	x_1	x_2	x_3
x_1	x_1	x_2	x_3
x_2	x_2		x_1
x_3	x_3	x_1	

$\rightarrow x_2 \perp x_2$

$\rightarrow x_3 \perp x_3$

$x_2 \perp x_2$ puede ser x_1 o x_2 o x_3. Si fuese x_1 esto querría decir que x_2 es simétrico de él mismo, lo cual es falso por hipótesis. Si $x_2 \perp x_2 = x_2$ significaría que x_2 es el neutro, contrariamente a la hipótesis de que el neutro es x_1. Luego necesariamente $x_2 \perp x_2 = x_3$. Razonando del mismo modo obtenemos $x_3 \perp x_3 = x_2$.

Quedando la tabla:

$\perp$	a_0	a_2
a_0	a_0	a_2
a_2	a_2	a_0

en la que se comprueba fácilmente que se cumple la propiedad asociativa y conmutativa. Luego el conjunto $x_1\ x_2\ x_3$, con esta ley es un grupo abeliano.
Este resultado lo podemos enunciar diciendo: "Sólo puede existir una estructura de grupo con tres elementos".

4-7 SUBGRUPOS

Dado un grupo G con una ley $\perp$, decimos que un subconjunto H de G es un subgrupo de G si es una parte estable de G para la ley $\perp$ y además cumple las dos condiciones:

1) El elemento neutro e de G pertenece a H; $e \in$ H.
2) El simétrico de todo elemento de H está también en H.

(Y, también, puesto que una *l.c.i.* de G es una aplicación como vimos, $\perp : G \times G \to G$, esto es tanto como decir que H sea grupo para la restricción de $\perp$ a $H \times H$, $\perp' : H \times H \to H$.)
Las condiciones para que un subconjunto de un grupo sea subgrupo se pueden reunir todas en una sola en el siguiente teorema:
Teorema 1.—Dado un grupo G y un subconjunto de él $H \subset G$, la condición necesaria y suficiente para que H sea subgrupo de G es que

$$\forall\, a,b \in H \quad a \perp b' \in H.$$

Demostremos primero que es condición necesaria:
Si H es subgrupo, por (2) si $b \in H \Rightarrow b' \in H$ y ahora por ser parte estable de G, si $a \in H$ y $b' \in H \Rightarrow a \perp b' \in H$.
Es condición suficiente:

1) La asociativa se cumple por ser H un subconjunto de G.

2) Considerando el caso $a = b$, $a \in H \Rightarrow a \perp a' \in H$, pero $a \perp a' = e$. Luego el neutro pertenece a H.

3) Tomemos el neutro $e \in H$ y $\forall\, b \in H$, $e \perp b' \in H$, pero $e \perp b' = b'$.

Luego el simétrico de cualquier elemento $b \in H$ pertenece también a H. Con lo cual queda demostrado que se es subgrupo.

EJEMPLO:

1) Los números racionales son un grupo para la adición y los números enteros constituyen un subgrupo de los racionales para la adición, puesto que $Z \subset Q$.
2) En la tabla de la fig. 34, que corresponde a un grupo G, los elementos $\}a_0\ a_2\{$ constituyen un subgrupo con la restricción de la ley L. Es decir:

$\perp$	x_1	x_2	x_3
x_1	x_1	x_2	x_3
x_2	x_2	x_3	x_1
x_3	x_3	x_1	x_2

Teorema 2.—Sea un grupo G. La intersección de dos subgrupos $H_1 \subset G$ y $H_2 \subset G$ del mismo grupo es otro grupo.
En efecto: Si $H_1 \subset G$ y $H_2 \subset G$, entonces, evidentemente, $H_1 \cap H_2 \subset G$. Luego basta con probar lo que dice el teorema anterior. Es decir, hay que demostrar que

$$\forall\, x,y \in H_1 \cap H_2 \qquad x \perp y' \in H_1 \cap H_2 .$$

Por ser H_1 subgrupo si $y \in H_1 \Rightarrow y' \in H_1$ y a su vez si $x \in H_1$

$$\Rightarrow x \perp y' \in H_1 \cdot$$

Y como H_2 es subgrupo si $y \in H_2 \Rightarrow y' \in H_2$ y a su vez si $x \in H_2 \Rightarrow$

$$\Rightarrow x \perp y' \in H_2.$$

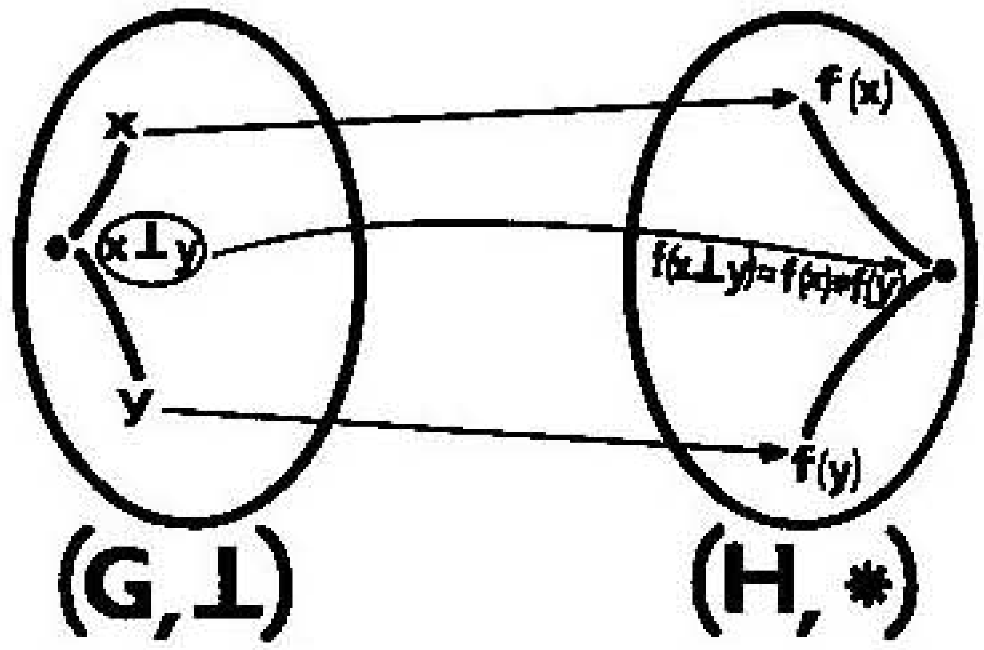
Luego $x \perp y' \in H_1 \cap H_2$, que es lo que queríamos demostrar.

4-8 HOMOMORFISMOS ENTRE GRUPOS

Sean dos grupos $(G, \perp)$ y $(H, *)$. Llamemos al neutro de G, $e_\perp$, y al neutro de H, e_*.
Por definición llamaremos homomorfismo entre el grupo G y el H, a toda aplicación que cumpla:

$$\forall\, x,y \in G \qquad f(x \perp y) = f(x) * f(y)$$

O sea, tal que la imagen de la composición de dos elementos de G es la composición de sus imágenes como elementos de H.



EJEMPLO:

Sea $(G,\perp) = (Z,+)$ y $(H,*) = (R-\{0\},.)$

Es decir, los enteros aditivos y los reales (salvo el cero) con la ley multiplicación.

Definamos la aplicación

$$f : Z \to R-\{0\}$$

del siguiente modo:

$$\forall x \in Z \longrightarrow e^x \in R - \{0\}$$

siendo e la base de los logaritmos nepperianos.

Entonces,

$$\text{para } a \in Z \to e^a = f(a)$$
$$b \in Z \to e^b = f(b)$$

y también

$$a + b \in Z \to e^{a+b} = f(a + b)$$

Cumpliéndose que $f(a + b) = f(a) \cdot f(b)$, luego f, así definida, es un homomorfismo entre grupos, pues $f(a) \cdot f(b) = e^a \cdot e^b = e^{a+b} = f(a + b)$.

Teorema 1.—$f(e_\perp) = e_*$: La imagen del neutro de G es el neutro de H.

Teorema 2.—$\forall a \in G \; f(a') = [f(a)]'$: La imagen del simétrico es igual al simétrico de la imagen.

Demostremos: 1.—Por definición de $e_\perp$, $\forall a \in G \quad a \perp e_\perp = e_\perp \perp a = a$.

Luego

$$f(a \perp e) = f(a) \qquad (1)$$

Por definición de homomorfismo,

$$f(a \perp e) = f(a) * f(e) \qquad (2)$$

Comparando (1) y (2) queda: $f(a) * f(e_\perp) = f(a)$, que por definición de neutro implicará

$$\boxed{f(e_\perp) = e_*}$$

Demostremos: 2.—Por definición de a' $: a' \perp a = a \perp a' = e_\perp$.

Luego

$$f(a' \perp a) = f(e_\perp) = e_* \Rightarrow f(a') * f(a) = e_*$$
$$f(a \perp a') = f(e_\perp) = e_* \Rightarrow f(a) * f(a') = e_*$$

y esto nos dice que el simétrico de $f(a)$ es $f(a')$. Pero el simétrico de $f(a)$ es $[f(a)]'$, luego $[f(a)]' = f(a')$.

4-9 CLASIFICACION DE LOS HOMOMORFISMOS

Los homomorfismos los clasificaremos por la tipo de aplicación que los determina.

EPIMORFISMOS: Si la aplicación $f: G \to H$ es sobre (exhaustiva).

ISOMORFISMOS: Cuando la aplicación f es biyectiva.

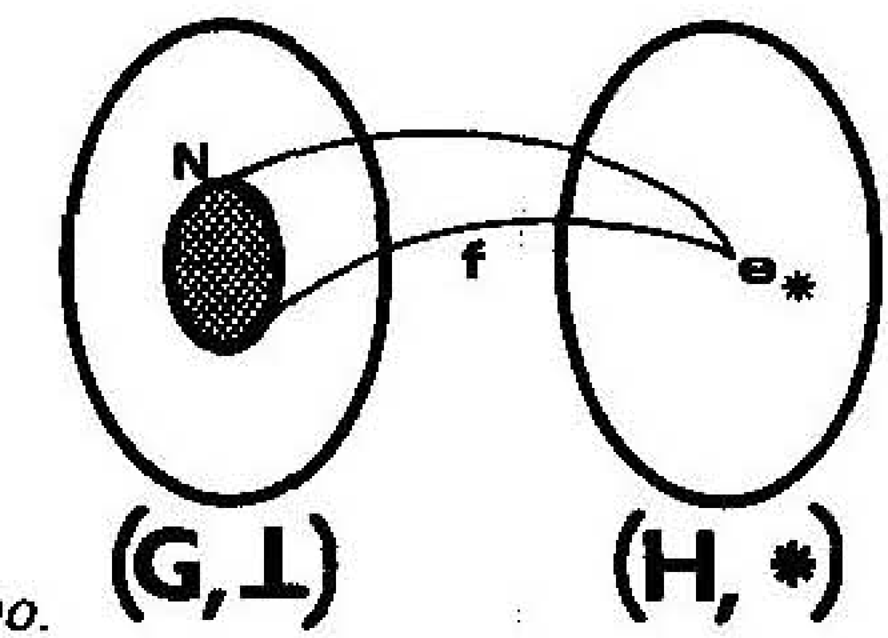
ENDOMORFISMOS: Cuando se trate de un homomorfismo de un grupo en sí mismo $f: G \to G$.

AUTOMORFISMO: Es un endomorfismo cuando la aplicación es biyectiva, o bien un isomorfismo de G sobre G.

Por supuesto, si $f: G \to H$ es un isomorfismo, existe el isomorfismo recíproco $f^{-1}: H \to G$. Consecuencia que se desprende de la definición de aplicación biyectiva.
La aplicación idéntica de un grupo en sí mismo $I_G: G \to G$ es un automorfismo.

4-10 NUCLEO DE UN HOMOMORFISMO

Dado el homomorfismo $f: G \to H$, llamamos núcleo al conjunto N de elementos de G que tienen por imagen el neutro de H.



$$N = \{ x \mid x \in G \mid f(x) = e_* \}$$

TEOREMA: El núcleo es un subgrupo de G.
Demostremos que el núcleo de un homomorfismo es un subgrupo.

En primer lugar $N \subset G$, luego basta probar el teorema 1 de subgrupos que dice que $\forall\, a,b \in N \; a \perp b' \in N$

En efecto:

si $a \in N \Rightarrow f(a) = e_*$
si $b \in N \Rightarrow f(b) = e_* \Rightarrow f(b') = (e_*)' = e_* \Rightarrow b' \in N$

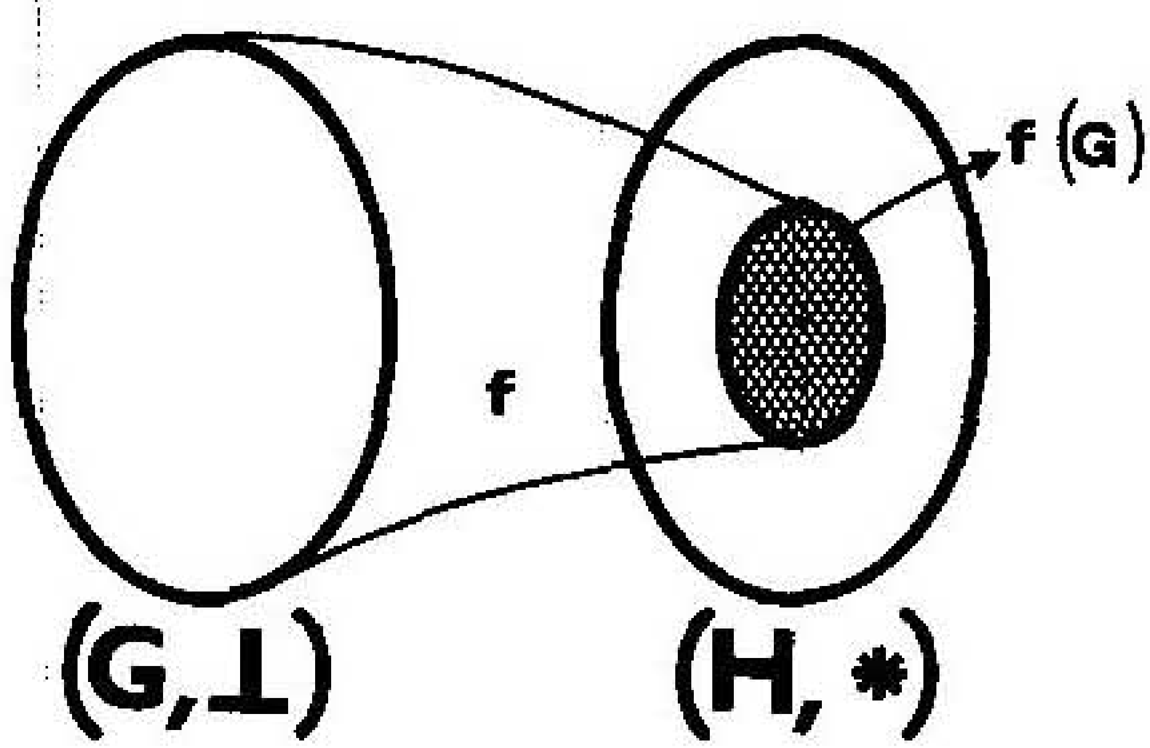
Luego

$$f(a \perp b') = f(a) * f(b') = e_* * e_* = e_*$$

Por tanto, por definición de núcleo $a \perp b' \in N$ y el núcleo es un subgrupo de G como queríamos demostrar.

4-11 IMAGEN HOMOMORFA DE UN GRUPO

Dado el homomorfismo $f: G \to H$, llamamos imagen homomorfa de G al subconjunto $f(G) \subset H$ de H de las imágenes de G por medio de f.



TEOREMA: La imagen homomorfa de un grupo es un subgrupo de H.
En efecto: $f(G) \subset H$. Probemos, pues, el teorema 3.

$$\text{si } x \in f(G) \Rightarrow \exists\, a \in H \mid f(a) = \alpha$$
$$\text{si } \beta \in f(G) \Rightarrow \exists\, b \in H \mid f(b) = \beta$$

Como hemos visto antes, $\beta' = [f(b)]' = f(b')$ *como* $b' \in G \quad f(b') = \beta'$ luego $\beta' \in f(G)$.

Entonces:

Entonces: $x * \beta' = f(a) * (b') = f(a \perp b')$

Y ahora $a \perp b' \in G$ por definición de grupo. Luego $f(a \perp b') \in f(G)$.

Entonces $x * \beta' \in f(G)$, y por tanto, $f(G)$ es un subgrupo.

TEMA 5 | GRUPO SIMETRICO

5-1 DEFINICION DE PERMUTACION

Llamamos permutación p de un conjunto cualquiera X a toda aplicación biyectiva de X en sí mismo.

EJEMPLO:

Si el conjunto X es, por ejemplo, el $X = \{1,2,3\}$, entonces todas las permutaciones posibles de los elementos de este conjunto serán, de acuerdo con lo que sabemos, las siguientes:

$$(1,2,3),(2,3,1),(3,1,2),(1,3,2),(3,2,1),(2,1,3)$$

Según esta forma de representar las permutaciones, damos a los elementos del conjunto original un orden (1,2,3) y sobre él las distintas aplicaciones biyectivas lo van alterando.

Llamemos a estas seis permutaciones P_1 P_2 P_3 P_4 P_5 P_6. Puesto que son aplicaciones, las podemos definir por su grafo (es decir, indicando la imagen que dan de cada elemento), ya que es conocido el conjunto X de partida, y el de llegada, el mismo X.

Según esto:

$$P_1\begin{cases}1\to 1\\2\to 2\\3\to 3\end{cases}\quad P_2\begin{cases}1\to 2\\2\to 3\\3\to 1\end{cases}\quad P_3\begin{cases}1\to 3\\2\to 1\\3\to 2\end{cases}\quad P_4\begin{cases}1\to 1\\2\to 3\\3\to 2\end{cases}\quad P_5\begin{cases}1\to 3\\2\to 2\\3\to 1\end{cases}\quad P_6\begin{cases}1\to 2\\2\to 1\\3\to 3\end{cases}$$

Vemos que una de ellas, P_1, es la aplicación idéntica.
En este conjunto de permutaciones, que llamaremos P(X), tenemos definida una ley de composición interna, la composición de aplicaciones, y de acuerdo con ella podemos construir la tabla de operación:

$\cdot$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_3	P_1	P_6	P_4	P_5
P_3	P_3	P_1	P_2	P_5	P_6	P_4
P_4	P_4	P_5	P_6	P_1	P_2	P_3
P_5	P_5	P_6	P_4	P_3	P_1	P_2
P_6	P_6	P_4	P_5	P_2	P_3	P_1

La primera fila y la primera columna de la tabla son inmediatas teniendo en cuenta la propia definición de aplicación idéntica.

Para efectuar los demás productos, escribiremos los elementos de P(X) así:

$$P_1 = \begin{pmatrix}123\\123\end{pmatrix} \quad P_2 = \begin{pmatrix}123\\231\end{pmatrix} \quad P_3 = \begin{pmatrix}123\\312\end{pmatrix} \quad P_4 = \begin{pmatrix}123\\132\end{pmatrix} \quad P_5 = \begin{pmatrix}123\\321\end{pmatrix} \quad P_6 = \begin{pmatrix}123\\213\end{pmatrix}$$

donde en la primera fila se coloca el conjunto original, y en la segunda las imágenes que corresponden a cada elemento por medio de la permutación correspondiente.
Con esta notación hallemos $P_3 \cdot P_5$, por ejemplo:

$$P_3 \cdot P_5 = \begin{pmatrix}123\\312\end{pmatrix} \cdot \begin{pmatrix}123\\321\end{pmatrix} = \begin{pmatrix}123\\213\end{pmatrix} = P_6$$

buscamos primero la imagen del 1 en P_5 y esta es 3, y luego buscamos la imagen del 3 en P_3 que es el 2. Entonces la permutación producto hace corresponder al 1 el 2, etcétera... Procediendo así completamos la tabla.
Se observa inmediatamente que, según lo que hemos visto en teoría de grupos, la tabla de permutaciones corresponde a un grupo.

5-2 GRUPO SIMETRICO

Considerando el conjunto $E_n = \{1, 2, 3, \ldots n\}$ representamos por S_n el conjunto de todas las permutaciones de E_n. Los elementos de

S_n para la composición de aplicaciones cumplen la propiedad asociativa; existe elemento neutro; la aplicación idéntica; y por ser las aplicaciones biyectivas, todos poseen su aplicación recíproca, que será otra permutación. Por tanto $(S_n, .)$ es, pues, un grupo que llamaremos grupo simétrico.
Vamos a definir ahora algunos tipos especiales de permutaciones.

5-3 DEFINICION DE CICLO

Llamaremos ciclo y lo representaremos por el símbolo $(i_1 i_2 \dots i_k)$ con $i_r \in E_n$, $1 \leqslant r \leqslant k$, a una permutación sobre los n elementos de E_n, que al i_1 le hace corresponder el i_2, al i_2 el $i_3 \dots$ al i_{k-1} el i_k y, al i_k el i_1, y que a todos los demás $n - k$ elementos de E_n los transforma en sí mismos (permanecen invariantes). En particular, cuando el ciclo es de dos elementos $i,j \in E_n$ (i,j) se llama *trasposición.* La trasposición intercambia i por j, y j por i, y deja los demás elementos invariantes.

EJEMPLO:

En S_3, P_2 es, por ejemplo, un ciclo, puesto que $P(1) = 2$, $P(2) = 3$ y $P(3) = 1$. y lo representamos por $(1,2,3)$.
La permutación $P_4 \in S_3$ es una trasposición $(2,3)$, puesto que cambia el 2 por el 3 y deja el 1 invariante.

Proposición 1.—Las trasposiciones $(i, j) = t_{ij}$ cumplen que $t_{ij}^2 = I$, siendo I la permutación idéntica.

En efecto: sea

$$t_{ij} = (i,j) = \begin{pmatrix} 12 \dots i \dots j \dots n \\ 12 \dots j \dots i \dots n \end{pmatrix} \qquad \text{y } I = \begin{pmatrix} 123 \dots n \\ 123 \dots n \end{pmatrix}$$

Entonces,

$$\forall x, x \in E_n \quad x \neq i \wedge x \neq j \quad t_{ij}(x) = x$$

y por lo tanto,

$$t_{ij}^2(x) = t_{ij}[t_{ij}(x)] = t_{ij}(x) = x$$

Si $x = i$ $\quad t_{ij}^2(i) = t_{ij}\,[t_{ij}(i)] = t_{ij}(j) = i$

Si $x = j$ $\quad t_{ij}^2(j) = t_{ij}\,[t_{ij}(j)] = t_{ij}(i) = j$

Luego $t_{ij} \in S_n$ es tal que $\forall\, x \in E_n$ $t_{ij}^2(x) = x$, es decir, $t_{ij}^2 = \mathbf{I}$.

Proposición 2.—El número de trasposiciones de S_n es $\frac{1}{2}n(n-1)$. Puesto que cada trasposición cambia dos elementos, por cada par de elementos (i,j) de E_n, habrá una trasposición. Ahora bien, como $(i,j) = (j,i)$ trivialmente, basta calcular las parejas que forma cada elemento con los que le quedan detrás:

n.° de trasposiciones:

$$S_n = (n-1) + (n-2) + \dots + 2 + 1 = \frac{(n-1)+1}{2}(n-1) = \frac{1}{2}(n-1)n$$

Teorema 1.—Toda permutación de S_n es un producto finito de ciclos disjuntos entre sí. Vamos a demostrarlo por inducción.

Para $n = 1$ y $n = 2$ es evidente.

Supongamos que se cumple para permutaciones de S_m con $m < n$, y sea σ una permutación sobre los n elementos. $\sigma \in S_n$.

Consideremos el conjunto $\sigma(1)$, $\sigma^2(1)$, $\sigma^3(1)$,... Si aplicamos repetidas veces σ, existirán finalmente enteros p y q, $p < q$ tales que $\sigma^p(1) = \sigma^q(1) \Rightarrow \sigma^{q-p}(1) = 1$. Existe entonces, al menos, un $h = q - p$, $h \in \mathbb{N}$, tal que $\sigma^h(1) = 1$. Sea s el menor número h que cumpla esto, $\sigma^s(1) = 1$.

Entonces los elementos: 1, $\sigma(1)$, $\sigma^2(1)$,..., $\sigma^{(s-1)}(1)$ son todos distintos, ya que si existieran t y r, $0 \leq t < r \leq (s-1)$, tales que $\sigma^t(1) = \sigma^r(1) \to \sigma^{r-t}(1) = 1$ con $(r-t) < s$, lo cual es imposible por la propia definición de s.

Consideremos ahora el ciclo: $\tau_1 = [1, \sigma(1), \sigma^2(1), \dots, \sigma^{s-1}(1)]$

(es decir; la imagen del 1 es $\sigma(1)$, la de $\sigma(1)$ es $\sigma^2(1)$... y la de $\sigma^{s-1}(1)$ es el 1. $\forall a$, $a \in E_n$, $a \neq 1, \sigma(1), \dots, \sigma^{s-1}(1)$, $\tau_1(a) = a$)

El recíproco de este, τ^{-1}, será:

$$\tau_1^{-1} = (\sigma^{s-1}(1), \dots, \sigma(1), 1)$$

(es decir, la imagen de $\sigma^{s-1}(1)$ es $\sigma^{s-2}(1)$, así sucesivamente hasta imagen de 1 es $\sigma^{s-1}(1)$, $\forall a$ $a \in E_m$ $a \neq 1, \sigma(1), \dots, \sigma^{s-1}(1)$, $\tau_1^{-1}(a) = a$)

Tomemos ahora la permutación σ' producto de σ por τ_1^{-1}.

$$\sigma' = \sigma \cdot \tau_1^{-1}$$

Veamos qué imágenes da σ' para cada uno de los elementos del conjunto

$$\{1, \sigma(1), \sigma^2(1), \dots, \sigma^{s-1}(1)\} \subset E_n.$$

$$\sigma'(1) = \sigma \cdot \tau_1^{-1}(1) = \sigma \cdot \sigma^{s-1}(1) = \sigma^s(1) = 1$$

$$\text{y } \forall k,\ 1 \leqslant k \leqslant s-1 \quad \text{en general:}$$

$$\sigma'(\sigma^k(1)) = \sigma \cdot \tau_1^{-1}(\sigma^k(1)) = \sigma[\tau_1^{-1}(\sigma^k(1))] = \sigma[\sigma^{k-1}(1)] = \sigma^k(1)$$

Esto significa que σ' deja los elementos del conjunto $\{1, \sigma(1), \sigma^2(1), \dots, \sigma^{s-1}(1)\}$ invariantes y permuta los demás elementos entre ellos. Puesto que σ' deja inalterados a estos s elementos de E_n, puede considerarse como una permutación sobre los demás $n - s$ elementos de E_n.

Teniendo ahora en cuenta que todas las permutaciones de m elementos $m < n$ se pueden expresar como producto finito de ciclos, cada dos de los cuales no poseen elementos comunes, σ' se podrá escribir como producto de un cierto número de estos ciclos $\tau_2 \cdot \tau_3 \dots \tau_k$ por ejemplo:

$$\sigma' = \tau_k\, \tau_{k-1} \dots \tau_2$$

Entonces $\sigma = \sigma' \cdot \tau_1 = \tau_k\, \tau_{k-1} \dots \tau_2\, \tau_1$

Luego $\forall\, \sigma \in S_n$ la hemos expresado en producto de ciclos sin elementos comunes cada dos de ellos entre sí, como queríamos demostrar.

Teorema 2.—Todo ciclo es un producto de trasposiciones.

En efecto, ya que dado un ciclo cualquiera $(1,2,3..r) = \sigma$ se comprueba inmediatamente que:

$$\sigma = (1,r) \cdot (1,r-1) \cdot (1,r-2) \dots (1,3) \cdot (1,2)$$

Consecuencia: Toda permutación es un producto de trasposiciones.

Sin embargo, la representación de las permutaciones como producto de trasposiciones no es única, ya que por ejemplo:

$$(1,2) = (1,2)\ (3,4)\ (4,3) = (1,2)\ (5,6)\ (6,5).$$

EJEMPLO:

En el conjunto S_3 hay tres trasposiciones: $P_4 = t_{23}$; $P_5 = t_{13}$; $P_6 = t_{12}$. Si observamos la tabla de S_3 se deduce inmediatamente que:

$$\begin{array}{ll} P_1 = P_4 \cdot P_4 = P_5 \cdot P_5 = P_6 \cdot P_6 & P_4 = P_4 \\ P_2 = P_4 \cdot P_5 = P_5 \cdot P_6 = P_6 \cdot P_4 & P_5 = P_5 \\ P_3 = P_4 \cdot P_6 = P_5 \cdot P_4 = P_6 \cdot P_5 & P_6 = P_6 \end{array}$$

Así, pues, el conjunto de los $\frac{1}{2}n(n-1)$ trasposiciones posibles constituyen un sistema de generadores de S_n.

5-4 PARIDAD DE UNA PERMUTACION

Definición 1.—Diremos que un par de elementos (i,j) cualesquiera son una inversión de la permutación $P \in S_n$, cuando $i < j$ y $P(i) > P(j)$.

O lo que es lo mismo, cuando:

$$\frac{P(i) - P(j)}{i - j} < 0$$

EJEMPLO:

Para P_2 en S_3, son inversiones los pares (1,3) y (2,3) porque:

$$P_2(1) = 2 \quad P_2(2) = 3 \quad P_2(3) = 1$$

siendo, pues, $1 < 3, P_2(1) > P_2(3)$ y $2 < 3, P_2(2) > P_2(3)$.

Definición 2.—Llamaremos signatura de la permutación P al número de inversiones de la misma; y la representaremos por $sgn(P)$. En el ejemplo anterior $sgn(P_2) = 2$.

Definición 3.—Diremos que $P \in S_n$ es par, o que posee paridad positiva si $(-1)^{sgn\ P} = +1$, y diremos que es impar o que posee paridad negativa si $(-1)^{sgn\ P} = -1$.
Es decir, que una permutación será par si tiene un número par de inversiones, y será impar si tiene un número impar de inversiones. De esto se deduce inmediatamente que toda trasposición es impar.

Definición 4.—Llamamos conjunto "bueno" a un subconjunto $A \subset E_n \times E_n$, tal que no contiene ningún par cuyo primer y segundo elementos sean iguales (i,i) y que de cada par i,j de elementos de E_n, $i \neq j$, contiene uno y sólo uno de los pares (i,j) o (j,i).
En E_3, por ejemplo, será conjunto bueno $A = \{(1,2),(1,3),(2,3)\} \subset E_3 \times E_3$.

Definición 5.—Sea A un conjunto bueno y $P \in S_n$ una permutación. Llamamos imagen de A por medio de la permutación P, y lo representamos por P(A) al conjunto:

$$P(A) = \left\{ [P(i),P(j)],\ \forall\ (i,j) \in A \right\}$$

Teorema 3.—La imagen de un conjunto bueno por una permutación es otro conjunto bueno. Además, si P y $P' \in S_n$, se cumple que $(P \cdot P')(A) = P(P'(A))$. En efecto: Sea A un conjunto bueno y $P \in S_n$.

1) En P(A) no puede existir ningún par de la forma (a,a), ya que esto querría decir que existiría algún par (i,j) de A, con $i \neq j$, tal que $P(i) = a$ y $P(j) = a$, lo cual es imposible, puesto que P es una aplicación biyectiva. Entonces, por ser biyectiva es inyectiva y $P(i) = P(j) \Rightarrow i = j$, lo cual no es posible por ser (i,j) un elemento del conjunto bueno A.
2) En P(A) no puede haber dos pares (a,b) y (b,a), puesto que ello indicaría que habrían pares (i,j) y (k,l) pertenecientes a A, tales que $P(i) = a$, $P(j) = b$, $P(k) = b$ y $P(l) = a$, lo cual es imposible por ser P biyectiva y $P(i) = P(l) \Rightarrow c = l \not> P(j) = P(k) \Rightarrow j = k$

Demostraremos ahora la segunda parte. Por la misma definición de aplicación compuesta de otras dos:

$$(P \cdot P')(A) = \left\{ [(P \cdot P')(i),(P \cdot P')(j)]\ \forall\ (i,j) \in A \right\} = \left\{ [P(P'(i)),P(P'(j))]\ \forall\ (i,j) \in A \right\} = P(P'(A)).$$

Definición 6.—Decimos que un par $(i,j) \in E_n \times E_n$ es "propio" si $i<j$. Al número de pares propios de un conjunto bueno A lo representaremos por $b(A)$". Y representaremos también por $|A|$ el número:

$$|A| = (-1)^{b(A)}$$

Teorema 4.—Si P es una permutación de S_n y A es un conjunto bueno $A \subset E_n \times E_n$, se cumple:

$$|P(A)| = (-1)^{sgn\, P}\, |A|$$

En efecto: Por cada inversión que posee P, *sgn* P aumenta en una unidad. Y pueden haber dos casos:

1) Sea (i,j) una inversión de P tal que $i<j$, $P(i) > P(j)$. Entonces A contiene al par propio (i,j) y P(A) contiene al par impropio $[P(i), P(j)]$. Luego para una inversión:

$$sgn(P) = 1 \quad b(A) = 1 \quad b(P(A)) = 0$$

Por tanto $[b(P(A)) - b(A)] - sgn(P) = -1 - 1 = -2 = \dot{2}$

2) Sea ahora $i > j$, $P(i) < P(j)$. A contiene al par impropio (i,j) y P(A) contiene al par propio $[P(i),P(j)]$. Para una inversión, pues:

$$sgn(P) = 1 \quad b(A) = 0 \quad b(P(A)) = 1$$

Luego: $[b(P(A)) - b(A)] - sgn(P) = (1-0) - 1 = 0 = \dot{2}$
Entonces en todos los casos:

$$[b(P(A)) - b(A)] = sgn(P) + \dot{2}$$

Es decir:

$$(-1)^{[b(P(A)) - b(A)]} = (-1)^{sgn(P) + \dot{2}} = (-1)^{sgn(P)}\,(-1)^{\dot{2}} = (-1)^{sgn(P)}$$

Teniendo ahora en cuenta las definiciones de $|P(A)|$ y $|(A)|$:

$$|P(A)| \cdot |A|^{-1} = (-1)^{sgn(P)} \rightarrow |P(A)| = (-1)^{sgn(P)}\, |A| \qquad c.q.d.$$

Teorema 5.—La paridad de un producto de permutaciones es positiva o par si las paridades de ambas son positivas o ambas nega-

tivas; y es negativa si la paridad de una de ellas es positiva y la de la otra es negativa o impar.
Si A es un conjunto bueno y $P,P' \in S_n$ $P \cdot P' \in S_n$. Luego por el teorema 4:

$$|(P \cdot P')(A)| = (-1)^{sgn(P \cdot P')}|A| \quad \text{pero:}$$

pero:

$$|(P \cdot P')(A)| = |P(P'(A))| = (-1)^{sgn(P)}|P'(A)| = (-1)^{sgn(P)}(-1)^{sgn(P')}|A|$$

Comparando ahora queda:

$$(-1)^{sgn(P \cdot P')}|A| = (-1)^{sgn(P)}(-1)^{sgn(P')}|A|$$

Es decir:

$$(-1)^{sgn(P \cdot P')} = (-1)^{sgn(P)} \cdot (-1)^{sgn(P')}$$

Y recordando ahora la definición de paridad queda:

paridad de $(P \cdot P')$ = paridad de (P) x paridad de (P').

Consecuencias:

1) Puesto que toda trasposición es impar por poseer una sola inversión, el producto de 2 trasposiciones será par.
2) Una permutación par será siempre producto de un número par de trasposiciones, y una impar será producto de un número impar de trasposiciones.
3) Toda permutación se puede escribir de muchos modos como un producto de trasposiciones a condición de que permanezca inalterada la paridad.
4) Existe un homomorfismo entre S_n y el grupo multiplicativo $\{-1, +1\}$, como se ve fácilmente a partir de los teoremas 4 y 5.

TEMA 6 ESTRUCTURAS ALGEBRAICAS: ANILLOS Y CUERPOS

6-1 DEFINICION DE ANILLO

Llamamos anillo a la terna $(A, *, \perp)$ formada por un conjunto A y dos leyes de composición interna $(*)$, $(\perp)$, que cumplen los axiomas siguientes:

A_1) El par $(A_1 *)$ es un grupo abeliano.

A_2) La *l.c.i.* $(\perp)$ es asociativa.

A_3) La *l.c.i.* $(\perp)$ es distributiva a derecha y a izquierda respecto a la ley $(*)$.

Todas estas condiciones las podemos establecer explícitamente del siguiente modo:

1) $(*)$ es ley de composición interna sobre A. Esto quiere decir que existe una aplicación $\tau: A \times A \to A$ que $\forall (x,y) \in A$ le hace corresponder un y solo un elemento $\tau\ (x,y)$ de A que lo representamos así: $(x * y) \in A$.

2) Esta ley es asociativa. Es decir:

$$\forall x,y,z \in A \quad x * (y * z) = (x * y) * z.$$

3) Es conmutativa:

$$\forall x,y \in A \quad x * y = y * x$$

4) Existe elemento neutro en A para la ley $(*)$

$$\exists!\ e \in A \mid \forall x \in A \quad e * x = x * e = x$$

5) Todo elemento en A posee simétrico para $(*)$

$$\forall x \in A \mid \exists!\ x' \quad x * x' = x' * x = e$$

6) $(\perp)$ es una ley de composición interna sobre A. Es decir: existe una aplicación $\mathcal{H} : A \times A \to A$ que $\forall\ (x,y) \in A$ le hace corresponder $\mathcal{H}\ (x,y) \in A$ y que representaremos por $x \perp y$.

7) La ley $(\perp)$ es asociativa en A.

$$\forall\ x,y,z \in A \qquad x \perp (y \perp z) = (x \perp y) \perp z$$

8) La ley $(\perp)$ es distributiva a izquierda y derecha respectivamente respecto a la ley $(*)$ en A.

$$\forall\ x,y,z \in A \quad \begin{aligned} (x * y) \perp z &= (x \perp z) * (y \perp z) \\ x \perp (y * z) &= (x \perp y) * (x \perp z) \end{aligned}$$

Cuando sobre un conjunto A, hay definidas dos leyes de composición interna que cumplan estas ocho condiciones, se dice también que "A es un anillo" o que "A forma un anillo para esas dos leyes".

Consecuencias: De la definición de anillo deducimos inmediatamente las siguientes consecuencias:

a) $\forall x \in A$

$$x \perp e = e \perp x = e$$

b) $\forall\ x,y \in A$

$$x \perp y' = (x \perp y)'$$

c) $\forall\ x,y \in A$

$$x' \perp y = (x \perp y)'$$

d) $\forall\ x,y \in A$

$$x' \perp y' = (x \perp y)$$

Veamos que efectivamente se cumplen:

a) Por definición de neutro
$\forall a, a \in A$

$$e * a = a * e = a$$

luego $\forall x \in A$

$$a \perp x = (a * e) \perp x = (a \perp x) * (e \perp x)$$

O sea: $(a \perp x) = (a \perp x) * (e \perp x)$

es decir:

$$\boxed{e \perp x = e}$$

Razón por la cual al neutro de la primera ley, e, se le llama elemento absorbente para la segunda ley $\perp$.

b) Demostremos que $x \perp y' = (x \perp y)'$. Por definición de simétrico (') de $x \perp y$, lo que hay que probar, pues, es que:

$$(x \perp y') * (x \perp y) = e$$
$$(x \perp y) * (x \perp y') = e$$

En virtud de 8:

$$(x \perp y') * (x \perp y) = x \perp (y' * y) = x \perp e = e$$
$$(x \perp y) * (x \perp y') = x \perp (y * y') = x \perp e = e$$

c) Por un procedimiento igual al anterior:

$$(x' \perp y) * (x \perp y) = (x' * x) \perp y = e \perp y = e$$
$$(x \perp y) * (x' \perp y) = (x * x') \perp y = e \perp y = e$$

d) Llamemos $c = y'$

$$(x' \perp c) = (x \perp c)' = (x \perp y')' = [(x \perp y)']' = (x \perp y)$$

pues $(x \perp y') = (x \perp y)'$ por el teorema *b)*

EJEMPLOS:

a) La terna $(z,+,\cdot)$ constituye un anillo. En efecto, puesto que sabemos que los enteros tienen definida sobre ellos una suma y un producto y que este segundo es distributivo respecto a la suma. Sabemos que la suma es asociativa y conmutativa, que su elemento neutro es el 0, y que para cada $a \in z$ su simétrico se representa por $(-a)$.
Atendiendo a esto quizá, en nuestros próximos razonamientos la primera ley de un anillo A cualquiera la representaremos por el símbolo (+) y la segunda por $(\cdot)$. También el neutro $e \in A$ de la primera ley lo representaremos por 0 y el simétrico anteponiendo al elemento el signo (−).
Con esta nueva notación las consecuencias anteriores para el anillo $(A,+,\cdot)$ serán:

a) $\forall x \in A \quad 0 \cdot x = x \cdot 0 = 0$
b) $\forall x,y \in A \quad x \cdot (-y) = -(x \cdot y)$
c) $\forall x\, y \in A \quad (-x) \cdot y = -(x \cdot y)$
d) $\forall x\, y \in A \quad (-x) \cdot (-y) = x \cdot y$

El *anillo se llama unitario* cuando posee elemento neutro para la segunda ley. Es decir, cuando hay un elemento $u \in A$ tal que

$$\forall x \in A \quad x \perp u = u \perp x = x$$

a este elemento neutro u se le llama elemento unidad y lo representaremos por el símbolo 1, que es el que corresponde al elemento unidad en el anillo Z.
Se dice que un *anillo es conmutativo* si lo es para la segunda ley. O sea, si:

$$\forall x\, y \in A \quad x \perp y = y \perp x$$

6-2 SUBANILLO. DEFINICION

Sea $(A,+,\cdot)$ un anillo con notación aditiva y multiplicativa. Se llama subanillo a todo subconjunto $B \subset A$ que cumpla las dos condiciones:

1) Ser subgrupo de A para la primera ley.
2) Ser parte estable de A para la segunda ley.

Si B es un subanillo de A, las leyes (+) y $(\cdot)$ del B serán verdaderas restricciones en el sentido que definimos para aplicaciones de las

Teorema: Por la condición necesaria y suficiente de subgrupo, podemos decir que una parte B del anillo A será subanillo de A si cumple:

1) $\forall x,y \in B \quad x + (-y) \in B$
2) $\forall x,y \in B \quad x \cdot y \in B$

De demostración inmediata.

6-3 DIVISORES DE CERO *Dominio de integridad.–*

Se dice que dos elementos $a,b \in A$ son divisores de cero, si son distintos de cero y su producto *es igual al neutro de la primera ley.* Esto es:

$$a \neq 0 \wedge b \neq 0 \quad a \cdot b = 0$$

EJEMPLO:

Consideremos el conjunto $Z/\{\dot{6}\}$. En él podemos definir una ley (+) y una ley (·) del siguiente modo:

Se comprueba inmediatamente que el conjunto forma grupo abeliano para la primera ley y que la segunda es asociativa, y distributiva respecto a la primera. El conjunto $Z/\{\dot{6}\}$ es, pues, un anillo para las leyes (+) y (·) definidos más arriba. En él, el elemento neutro para la ley (+) es el $\{\dot{6}\}$.
El anillo $Z/\{\dot{6}\}$ posee divisores de cero, pues siendo así que $\{\dot{6}+2\} \neq \{\dot{6}\}$ y que $\{\dot{6}+3\} \neq \{\dot{6}\}$, su producto es:

$$\{\dot{6}+2\} \cdot \{\dot{6}+3\} = \{\dot{6}+6\} = \{\dot{6}\}$$

luego estos dos elementos son divisores de cero.

Un anillo que no tiene divisores de cero se llama *anillo de integridad.* Llamamos *dominio de integridad* a un anillo de integridad que tiene elemento unidad. Es decir, elemento neutro para la segunda ley.

EJEMPLO:

El conjunto $Z/\{\dot{5}\}$ con las dos leyes $(+)$ y $(\cdot)$ es un dominio de integridad:

a) $\left(Z/\{\dot{5}\},+,\cdot\right)$ es un anillo cuyo elemento neutro para $(+)$ es el $\{\dot{5}\}$ y cuyo elemento unidad es $\{\dot{5}+1\}$.

En efecto:

$$\{\dot{5}+i\}\cdot\{\dot{5}+1\}=\{\dot{5}+i\}=\{\dot{5}+1\}\cdot\{\dot{5}+i\}$$

$\forall\{\dot{5}+i\}\in Z/\{\dot{5}\}$

b) No tiene divisores de cero como se comprueba rápidamente en la tabla de multiplicación.

Teorema: En un anillo de integridad A (y por tanto en un dominio), dados dos elementos, $a, b \in A$, la ecuación $a \cdot x = b$ tiene una solución única.

En efecto: Supongamos que esto no se cumpla. Es decir, que existen dos soluciones distintas $x \neq y$, $x, y \in A$ para esta ecuación.

Entonces:

$$\left.\begin{array}{l} a \cdot x = b \\ a \cdot y = b \end{array}\right\} a \cdot x = a \cdot y$$

luego,

$$a \cdot x + (-a \cdot y) = 0 \Rightarrow a \cdot x + a \cdot (-y) = 0$$

y por la distributiva:

$$a \cdot (x + (-y)) = 0 \Rightarrow a\,(x - y) = 0$$

donde:

$a \in A$ y $a \neq 0$ y $x - y \in A$ y $x - y \neq 0 \Longrightarrow$ que $\underline{a}$ y $\underline{(x-y)}$ sean divisores de cero en A, lo cual no es posible por hipótesis (anillo de integridad). Luego no puede ser $x - y \neq 0$, o sea, $x - y = 0 \Rightarrow$ $\Rightarrow x = y$, *como queríamos demostrar.*

6-4 ELEMENTOS INVERSIBLES. CUERPO

Dado un anillo $(A,+,\cdot)$ unitario, se dice que un elemento $a \in A$ $a \neq O$ es inversible, si existe algún $b \in A$ tal que:

$$a \cdot b = b \cdot a = 1$$

al elemento b se le representa entonces por a^{-1}, quedando, pues, establecido que a es inservible en A.

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

A un elemento inversible de un anillo también se le llama "unidad", pero procuremos no utilizar esta terminología para no confundir con el 1 al que hemos llamado elemento unidad.
Llamaremos *cuerpo* a un anillo unitario $(A + \cdot)$ en cual todos los elementos distintos del 0 sean inversibles. Es decir, posean simétrico para la segunda ley.
Si $(A,+,\cdot)$ es un cuerpo, entonces se cumple:

1) El par $(A,+)$ es un grupo abeliano.

2) El par $(A - \{0\} \cdot)$ es un grupo, con lo cual se está diciendo implícitamente que el $1 \neq 0$. Es decir, que un cuerpo posee al menos dos elementos.

3) La ley $(\cdot)$ es distributiva respecto a la ley $(+)$ en A.

Si la segunda ley $(\cdot)$ del cuerpo es conmutativa, al cuerpo se le llama conmutativo.
En un cuerpo $(A,+,\cdot)$, dados dos elementos $c,d \in A$, la ecuación $c \cdot x = d$ posee una solución única, puesto que existe un inverso de c, el c^{-1}:

$$c^{-1} \cdot (c \cdot x) = c^{-1} \cdot d$$

$$(c^{-1} \cdot c) \cdot x = c^{-1} \cdot d \Rightarrow 1 \cdot x = c^{-1} \cdot d \Rightarrow \boxed{x = c^{-1} \cdot d}$$

$c^{-1} \cdot d$ es un elemento único de A por definición de ley $(\cdot)$ en A.

EJEMPLO:

El conjunto $Z/\{\dot{5}\}$ con las leyes + y, es un cuerpo:

a) Forma grupo abeliano para (+).

+	$\{\dot{5}\}$	$\{\dot{5}+1\}$	$\{\dot{5}+2\}$	$\{\dot{5}+3\}$	$\{\dot{5}+4\}$
$\{\dot{5}\}$	$\dot{5}$	$\dot{5}+1$	$\dot{5}+2$	$\dot{5}+3$	$\dot{5}+4$
$\{\dot{5}+1\}$	$\dot{5}+1$	$\dot{5}+2$	$\dot{5}+3$	$\dot{5}+4$	$\dot{5}$
$\{\dot{5}+2\}$	$\dot{5}+2$	$\dot{5}+3$	$\dot{5}+4$	$\dot{5}$	$\dot{5}+1$
$\{\dot{5}+3\}$	$\dot{5}+3$	$\dot{5}+4$	$\dot{5}$	$\dot{5}+1$	$\dot{5}+2$
$\{\dot{5}+4\}$	$\dot{5}+4$	$\dot{5}$	$\dot{5}+1$	$\dot{5}+2$	$\dot{5}+3$

b) $Z/\{5\} - \{5 + 0\}$ forma grupo abeliano para $(\cdot)$.

c) La ley $(\cdot)$ es distributiva respecto a la ley $(+)$

$\bullet$	$(\dot{5}+1)$	$(\dot{5}+2)$	$(\dot{5}+3)$	$(\dot{5}+4)$
$(\dot{5}+1)$	$\dot{5}+1$	$\dot{5}+2$	$\dot{5}+3$	$\dot{5}+4$
$(\dot{5}+2)$	$\dot{5}+2$	$\dot{5}+4$	$\dot{5}+1$	$\dot{5}+3$
$(\dot{5}+3)$	$\dot{5}+3$	$\dot{5}+1$	$\dot{5}+4$	$\dot{5}+2$
$(\dot{5}+4)$	$\dot{5}+4$	$\dot{5}+3$	$\dot{5}+2$	$\dot{5}+1$

6-5 HOMOMORFISMO ENTRE ANILLOS

Sean: $(A,+,\cdot)$ y $(B,+,\cdot)$ dos anillos, y sea $f: A \to B$ una aplicación definida entre ellos. Decimos que f es un homomorfismo, si:

1) $\forall x,y \in A \quad f(x + y) = f(x) + f(y)$
2) $\forall x,y \in A \quad f(x \cdot y) = f(x) \cdot f(y)$

Consecuencias:

1) Si el $0 \in A$ es el neutro de A y representamos por 0 también el neutro de B, $f(0) = 0$.
2) $\forall x \in A \quad f(-x) = -f(x)$.
3) El núcleo del homomorfismo es un grupo para la ley + de A.
4) La imagen del homorfismo $f(A)$ es un subanillo de B.

Demostremos:

1) Por definición de neutro:

$$\forall x \in A \quad x + 0 = x$$

Luego:

$$f(x + 0) = f(x) \Longrightarrow f(x) + f(0) = f(x) \Longrightarrow f(0) = 0$$

2) Por definición de simétrico:

$$\forall x \in A \quad \exists! \ (-x) \mid x + (-x) = 0$$

$$f[x + (-x)] = f(0) \Longrightarrow f(x) + f(-x) = 0 \Longrightarrow f(-x) = -f(x)$$

3) El núcleo N A definido como:

$$N_f = \{x, x \in A \mid f(x) = 0\}$$

es un subgrupo del grupo abeliano $(A,+)$ como vimos en homomorfismo entre grupos.

4) $f(A) = \{y, y \in B \mid \exists x \in A \mid y = f(x)\}$

a) $\forall y \in f(A) \Rightarrow \exists a \in A \mid y = f(a)$

$\forall z \in f(A) \Rightarrow \exists b \in A \mid z = f(b)$ y en virtud de la consecuencia (2) $-z = f(-b)$. Luego:

$y - z = f(a) + f(-b) = f(a - b) \in f(A)$

Luego $f(A)$ es subgrupo abeliano para la ley $+$.

b) Tomando la $y, z \in f(A)$ como en *(a)*

$y \cdot z = f(a) \cdot f(b) = f(a \cdot b) \in f(A)$

luego $f(A)$ es parte estable para la ley $(\cdot)$. Decimos, pues, que es subanillo de B.
La clasificación es idéntica a la de los homomorfismos entre grupos.

6-6 IDEALES DE UN ANILLO

Consideremos un anillo $(A, +, \cdot)$; decimos que un subconjunto $I \subset A$ es un ideal de A a *la izquierda* si cumple las dos condiciones:

1) Es subgrupo de A para la ley $+$.
2) $\forall x \in A \quad \forall i \in I \quad x \cdot i \in I$

Análogamente, decimos que $I \subset A$ es ideal a *la derecha,* si cumple 1) y

3) $\forall x \in A \quad \forall i \in I \quad i \cdot x \in I$

Un ideal $I \subset A$ se llama *bilátero* si cumple las condiciones 1), 2) y 3).

EJEMPLO:

1) Consideremos el anillo $(Z, +, \cdot)$ y en él un subconjunto $I = \{x, x, \in Z \mid x = \dot{5}\}$. Este conjunto es un ideal bilátero, pues:

1) I es subgrupo para la ley $(+)$.
2) $\forall P \in Z \quad P \cdot \dot{5} = \dot{5} \cdot P = \dot{5} \in I$

2) Sean $(A, +, \cdot)$ y $(B, +, \cdot)$ dos anillos y $f: A \to B$ un homomorfismo entre anillos. El núcleo N_f de este homomorfismo es un ideal bilátero.

En efecto, pues N_f es subgrupo de A como hemos visto antes. Y además $\forall x \in A \wedge \forall n \in N_f$ veamos si $x \cdot n$ y $n \cdot x$ pertenecen a N_f.

$$f(x \cdot u) = f(x) \cdot f(u) = f(x) \cdot 0 = 0 \Rightarrow x \cdot u \in N_f$$
$$f(u \cdot x) = f(u) \cdot f(x) = 0 \cdot f(x) = 0 \Rightarrow u \cdot x \in N_f$$

Luego, efectivamente, el núcleo de un homomorfismo entre anillos es ideal bilátero.

6-7 GENERACION DE IDEALES

Sea el anillo conmutativo $[A,+,\cdot]$. Recordemos que para la notación aditiva establecimos:

$$\underbrace{x + x + x + \ldots + x}_{n} = n \cdot x \quad \text{siendo } n \in Z$$

Consideremos un subconjunto $S \subset A$. $S = [x_1, x_2, x_3, \ldots, x_r]$. Vamos a demostrar que el conjunto

$$I = \left\{ \sum_{i=1}^{r} y_i x_i + \sum_{i=1}^{r} n_i x_i \mid x_i \in S, y_i \in A, n_i \in Z \right\}$$

es un ideal de A. En efecto:

1) Si $\alpha \in I$, $\beta \in I \Rightarrow \alpha + \beta \in I$

pues si $\alpha = \sum^{r} y_i x_i + \sum^{r} n_i x_i$

y $\beta = \sum^{r} y'_i x_i + \sum^{r} n'_i x_i$

Sumando

$\alpha + \beta = \sum^{r} y_i x_i + \sum^{r} n_i x_i + \sum^{r} y'_i x_i + \sum^{r} n'_i x_i =$ por distributividad
$= \sum^{r} (y_i + y'_i) x_i + \sum^{r} (n_i + n'_i) x_i$

pero $y_i + y'_i \in A$
y $n_i + n'_i \in Z$

luego
$\alpha + \beta \in I$

2) Si $\alpha \in I$ y $k \in A \Rightarrow k \cdot \alpha \in I$

pues si

$$\alpha = \sum^{r} y_i x_i + \sum^{r} n_i x_i$$

$$k \cdot \alpha = k \sum^{r} y_i x_i + k \cdot \sum^{r} n_i x_i = \sum^{r} k y_i \cdot x_i + \sum^{r} k n_i x_i$$

pero $k \cdot y_i \in A$
y $\quad n k \in A$

luego $k \cdot \alpha \in I$

O sea, que el conjunto I es un ideal del anillo A.

Conclusión: Al conjunto $S = \{x_i \dots x_r\}$ se le llama conjunto de generadores del ideal I. En particular el conjunto $S_1 = \{x_1\}$ generaría el ideal
$I_1 = \{kx_1 + nx_1 \mid k \in A, x_1 \in S, n \in Z\}$
El ideal se llama principal cuando tiene un solo generador.

EJEMPLO:

Sea el anillo $[Z,+,x]$. Consideremos el número $a \in Z$ y el conjunto de sus múltiplos $\dot{a} = \{a \cdot z \mid z \in Z\}$ este conjunto constituye un ideal principal de generador *a*.
En efecto:
$\forall k \in Z \quad k \cdot a = \dot{a}$ múltiplo de *a*
$\forall a_1 \in \dot{a}$ y $a_2 \in \dot{a} \quad a_1 + a_2 = \dot{a}$

Existen dos ideales destacables:

1) El ideal cuyo generador es el 1, neutro, unitario de la 2.ª ley, que es el propio del anillo A.

$$I_1 = A$$

En efecto:
$\forall k \in A \quad k \cdot 1 = k \in I \Rightarrow A \subset I$
pero $\forall \kappa \in I \quad R \cdot 1 = \kappa \in A \Rightarrow I \subset A$

O sea: $A = I$

2) El ideal cuyo generador es el 0. Neutro de la 1.ª ley del anillo. Este ideal es un conjunto de un solo elemento.

$$I_o = \} 0 \{$$

En efecto. Por ser 0 absorbente para la 2.ª ley.

$$\forall k \in A \quad k \cdot 0 = 0 \in I$$

O sea, $I_o = \} 0 \{$

TEMA 7 | ESPACIOS VECTORIALES

ESPACIOS VECTORIALES

7-1 DEFINICION DE ESPACIO VECTORIAL

La estructura de espacio vectorial queda definida por los siguientes elementos:

a) Un grupo abeliano (E,+) cuyos elementos se llamarán vectores y representaremos por las letras latinas *a, b, c,...* que podrán venir afectadas de subíndices o superíndices, así x_1, x_2,...
El elemento neutro de este grupo lo representaremos por 0 y el simétrico de un elemento dado $x \in E$ por $-x$.

b) Un cuerpo conmutativo (K,+,·) cuyos elementos denominaremos escalares y vendrán representados por letras griegas $\alpha, \beta, \gamma, \ldots$, que también podrán aparecer con índices.
El elemento neutro de la primera ley del cuerpo lo representaremos

por 0 y el simétrico de un elemento dado $\alpha \in K$ para esta ley por $-\alpha$ El neutro de la segunda ley lo representaremos por 1 y el simétrico de $\alpha \in K$ para esta ley por α^{-1}.

c) Una ley de composición externa $(\cdot)$ definida entre K y E

$$(\cdot): K \times E \to E$$

tal que para cada par de elementos (α,x) de $K \times E$, les asocia un elemento de E que representaremos por $\alpha \cdot x$.

$$(\alpha,x) \to \alpha \cdot x \in E$$

Esta ley externa cumplirá los siguientes cuatro axiomas:

A_1) $\forall x,y \in E, \ , \ \forall \alpha \in K$

$$\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$$

A_2) $\forall x \in E, \ , \ \forall \alpha, \beta \in K$

$$(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$$

A_3) $\forall x \in E, \ , \ \forall \alpha,\beta \in K$

$$(\alpha \cdot \beta) \cdot x = \alpha \cdot (\beta \cdot x)$$

A_4) $\forall x \in E$

$$1 \cdot x = x$$

De este modo queda, pues, globalmente definida la estructura de espacio vectorial con los tres elementos señalados $(E,+),(K,+,\cdot)$ y $(\cdot)$ con la verificación de los cuatro axiomas indicados.
Por ello, el espacio vectorial podremos representarlo por:

$$[(E,+),(K,+,\cdot), \cdot\ ]$$

Muchas veces, por necesidad de simplificar el lenguaje, diremos que E es un espacio vectorial, cuando se conozcan perfectamente el cuerpo de escalares y la ley externa.

Nota.—En adelante, por razones de simplificar el lenguaje, diremos siempre cuerpo (o un cuerpo cualquiera), a pesar de que nos referimos siempre a cuerpos conmutativos.

7-1-1 CASOS DESTACADOS

1) Consideremos un cuerpo cualquiera $(K,+,\cdot)$. Por definición del cuerpo $(K,+)$ es un grupo abeliano. Tomemos como ley de composición externa la segunda ley del cuerpo y vamos a probar que la terna $[(K,+),(K,+,\cdot),\cdot]$ es un espacio vectorial. Es decir, probemos que verifica los cuatro axiomas:

A_1) $\forall \alpha,\beta \in K, \forall \gamma \in K$

$$\gamma \cdot (\alpha + \beta) = \gamma \cdot \alpha + \gamma \cdot \beta$$

Que se cumple, puesto que la segunda ley del cuerpo es distributiva a derecha respecto de la primera.

A_2) $\forall \alpha \in K, \forall \beta,\gamma \in K$

$$(\beta + \gamma) \cdot \alpha = \beta \cdot \alpha + \gamma \cdot \alpha$$

También la segunda ley del cuerpo es distributiva a izquierda respecto de la primera.

A_3) $\forall \alpha \in K, \forall \beta,\gamma \in K$

$$(\beta \cdot \gamma) \cdot \alpha = \beta \cdot (\gamma \cdot \alpha)$$

La segunda ley del cuerpo es asociativa, pues para esta ley, K es grupo.

A_4) $\forall \alpha \in K$

$$1 \cdot \alpha = \alpha$$

Evidente, pues 1 es neutro de la ley $(\cdot)$ del cuerpo K.

Nota.—Por razones de simplificar la exposición del tema, no hemos diferenciado la notación de las leyes del grupo, las del cuerpo y la ley externa. Pero es evidente que aunque la primera ley del cuerpo y la ley del grupo las representemos ambas por +, son esencialmente distintas, una compone (suma) escalares, es de la forma $K \times K \to K$ y la otra compone (suma) vectores y es la de forma $E \times E \to E$. Igualmente indicar los elementos neutros por 0 y 1 para todas las leyes es por razón de simplificar aunque según la ley de que se trate será distinto lo representado, bien el vector o escalar nulo, bien el escalar unitario o el elemento neutro de la ley externa. Así observamos el axioma A_3

$$(\alpha \cdot \beta) \cdot x = \alpha \cdot (\beta \cdot x)$$

el primer punto representa la ley multiplicativa del cuerpo, sin embargo, el segundo representa la ley externa y en el segundo miembro de la igualdad ambos puntos son ley externa, pues $(\alpha \cdot x)$ es ya un vector.

2) Consideremos, como en el caso anterior, un cuerpo cualquiera $(K,+,\cdot)$. El conjunto producto cartesiano $K \times K \times K ... = K^n$ tiene estructura de grupo abeliano (fácilmente comprobable) para la ley + definida:

$$\forall \ (\alpha_1, \alpha_2, ..., \alpha_n), (\beta_1, \beta_2, ...) \in K^n$$

$$(\alpha_1, \alpha_2, ... \alpha_n) + (\beta_1, \beta_2, ... \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, ... \alpha_n + \beta_n)$$

Definamos la ley externa

$$(\cdot): K \times K^n \rightarrow K^n$$

en función de la segunda ley del cuerpo de la siguiente forma

$$\forall \alpha \in K \quad \forall (\beta_1, \beta_2, ... \beta_n) \in K^n$$

$$\alpha \cdot (\beta_1, \beta_2, \beta_3 ... \beta_n) = (\alpha \cdot \beta_1, \alpha \cdot \beta_2, ... \alpha \cdot \beta_n)$$

Vamos a demostrar que la terna $[(K,^n +), (K, +, \cdot) \cdot]$ es un espacio vectorial.
En efecto: Por las propiedades de las leyes del cuerpo:

A_1) $\forall (\alpha_1, \alpha_2, ... \alpha_n), (\beta_1, \beta_2, ..., \beta_n) \in K^n, \ \forall \gamma \in K$

$$\begin{aligned}
&\gamma \cdot [(\alpha_1, \alpha_2, ..., \alpha_n) + (\beta_1, \beta_2, ..., \beta_n)] = \\
&= \gamma \cdot [(\alpha_1 + \beta_1, \alpha_2 + \beta_2, ..., \alpha_n + \beta_n)] = \\
&= [\gamma \cdot (\alpha_1 + \beta_1), \gamma \cdot (\alpha_2 + \beta_2), ..., \gamma \cdot (\alpha_n + \beta_n)] = \\
&= [(\gamma \cdot \alpha_1 + \gamma \cdot \beta_1), (\gamma \cdot \alpha_2 + \gamma \cdot \beta_2), ..., (\gamma \cdot \alpha_n + \gamma \cdot \beta_n)] = \\
&= [\gamma \cdot \alpha_1, \gamma \cdot \alpha_2, ..., \gamma \cdot \alpha_n] + [\gamma \cdot \beta_1, \gamma \cdot \beta_2, ..., \gamma \cdot \beta_n] = \\
&= \gamma \cdot [\alpha_1, \alpha_2, ..., \alpha_n] + \gamma \cdot [\beta_1, \beta_2, ..., \beta_n]
\end{aligned}$$

c.q.d.

A_2) $\forall\ \alpha, \beta \in K \quad \forall\ (\gamma_1, \gamma_2, ..., \gamma_n) \in K^n$

$$\begin{aligned}
&(\alpha + \beta) \cdot [\gamma_1, \gamma_2, ..., \gamma_n] = \\
&= [(\alpha + \beta) \cdot \gamma_1, (\alpha + \beta) \cdot \gamma_2, ..., (\alpha + \beta) \cdot \gamma_n] = \\
&= [(\alpha \cdot \gamma_1 + \beta \cdot \gamma), (\alpha \cdot \gamma_2 + \beta \cdot \gamma_2), ..., (\alpha \cdot \gamma_n + \beta \cdot \gamma_n)] = \\
&= (\alpha \cdot \gamma_1, \alpha \cdot \gamma_2, ..., \alpha \cdot \gamma_n) + (\beta \cdot \gamma_1, \beta \cdot \gamma_2, ..., \beta \cdot \gamma_n) = \\
&= \alpha \cdot (\gamma_1, \gamma_2, ..., \gamma_n) + \beta \cdot (\gamma_1, \gamma_2, ..., \gamma_n)
\end{aligned}$$

c.q.d.

A_3) $\forall\ \alpha, \beta \in K \quad \forall\ (\gamma_1, \gamma_2, ..., \gamma_n) \in K^n$

$$\begin{aligned}
&(\alpha \cdot \beta) \cdot [\gamma_1, \gamma_2, ..., \gamma_n] = \\
&= [(\alpha \cdot \beta) \cdot \gamma_1, (\alpha \cdot \beta) \cdot \gamma_2, ..., (\alpha \cdot \beta) \cdot \gamma_n] = \\
&= [\alpha \cdot (\beta \cdot \gamma_1), \alpha \cdot (\beta \cdot \gamma_2), ..., \alpha \cdot (\beta \cdot \gamma_n)] = \\
&= \alpha \cdot (\beta \cdot \gamma_1, \beta \cdot \gamma_2, ..., \beta \cdot \gamma_n) = \alpha \cdot [\beta \cdot (\gamma_1, \gamma_2, ..., \gamma_n)]
\end{aligned}$$

c.q.d.

A_4) $\forall\ (\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n) \in K^n$

$$1 \cdot (\alpha_1, \alpha_2, ..., \alpha_n) = (1 \cdot \alpha_1, 1 \cdot \alpha_2, ..., 1 \cdot \alpha_n) = (\alpha_1, \alpha_2, ..., \alpha_n)$$

c.q.d.

Por tanto, K^n es un espacio vectorial.

7-1-2 CONSECUENCIAS Y TEOREMAS INMEDIATOS

1) $\forall\ x \in E \quad 0 \cdot x = 0$

(Obsérvese que el 0 del primer miembro es el neutro de los escalares para la ley +; que se trata de la ley externa y que el 0 del segundo miembro es el vector nulo.

En efecto, de la definición de $0 \in K$:

$$\forall\ \alpha \in K, \quad (0 + \alpha) \cdot x = \alpha \cdot x$$

Teniendo en cuenta A_2 :

$$(0+\alpha)\cdot x = 0\cdot x + \alpha\cdot x$$

luego:

$$\alpha\cdot x = 0\cdot x + \alpha\cdot x$$

los tres son elementos de un grupo abeliano, y por tanto, $\alpha\cdot x$ es simplificable, quedando:

$$0 = 0\cdot x$$

c.q.d.

2) $\forall\,\alpha\in K$ y $0\in E$, $\alpha\cdot 0 = 0$

En efecto, por definición de $0\in E$:

$$\forall\, x\in E \quad \alpha\cdot x = \alpha\cdot(0+x)$$

y teniendo en cuenta A_1 :

$$\alpha\cdot(0+x) = \alpha\cdot 0 + \alpha\cdot x$$

luego:

$$\alpha\cdot x = \alpha\cdot 0 + \alpha\cdot x$$

Simplificando, queda:

$$0 = \alpha\cdot 0$$

Obsérvese que ahora $0\in E$, es el vector nulo.

c.q.d.

3) $\forall\, x\in E \quad \forall\,\alpha\in K$, $(-\alpha)\cdot x = -(\alpha\cdot x)$
Probemos que $(-\alpha)\cdot x$ es el simétrico de $(\alpha\cdot x)$. En efecto, teniendo en cuenta A_2 y el teorema 1:

$$(-\alpha)\cdot x + \alpha\cdot x = (-\alpha+\alpha)\cdot x = 0\cdot x = 0$$

Luego $(-\alpha) \cdot x$ es el simétrico de $\alpha \cdot x$; o sea:

$$(-\alpha) \cdot x = -(\alpha \cdot x)$$

c.q.d.

4) $\forall x \in E \quad \forall \alpha \in K, \quad \alpha \cdot (-x) = -(\alpha \cdot x)$

Probemos que $\alpha \cdot (-x)$ es el simétrico de $\alpha \cdot x$. En efecto, teniendo en cuenta A_1 y el teorema 2:

$$\alpha \cdot (-x) + \alpha \cdot x = \alpha \cdot (-x + x) = \alpha \cdot 0 = 0$$

Luego $\alpha \cdot (-x)$ es simétrico de $\alpha \cdot x$, es decir,

$$\alpha \cdot (-x) = -(\alpha \cdot x)$$

c.q.d.

5) $\forall x \in E, \forall \alpha \in K, \alpha \cdot x = 0 \Rightarrow (\alpha = 0 \wedge x = 0)$

Demostrémoslo por reducción al absurdo.

Supongamos que $\exists x \in E \mid x \neq 0 \wedge \exists \alpha \in K \mid \alpha \neq 0 \wedge \alpha \cdot x = 0$

Entonces, por ser $\alpha \neq 0$, $\exists \alpha^{-1} \in K$. Operando a la izquierda de la expresión $\alpha \cdot x = 0$ con α^{-1} queda:

$$\alpha^{-1} \cdot (\alpha \cdot x) = \alpha^{-1} \cdot 0 = 0$$

teniendo en cuenta A_3:

$$(\alpha^{-1} \cdot \alpha) \cdot x = 0$$

de donde

$$1 \cdot x = x = 0$$

Hemos obtenido, pues, la contradicción $x \neq 0 \wedge x = 0$, luego queda demostrado que, o bien el escalar, o bien el vector, tiene que ser nulo.

6) $\forall\ x,y \in E, \forall\ \alpha \in K \wedge \alpha \neq 0, \alpha \cdot x = \alpha \cdot y \Rightarrow x = y$

En efecto, operando a la izquierda con α^{-1} :

$$\alpha^{-1} \cdot (\alpha \cdot x) = \alpha^{-1} \cdot (\alpha \cdot y)$$

teniendo en cuenta A_3 :

$$(\alpha^{-1} \cdot \alpha) \cdot x = (\alpha^{-1} \cdot \alpha) \cdot y$$

por tanto

$$x = y$$

c.q.d.

7) $\forall\ x \in E \wedge x \neq 0 \quad \forall\ \alpha, \beta \in K \quad \alpha \cdot x = \beta \cdot x \Rightarrow \alpha = \beta$

Vamos a operar a la izquierda con $-(\alpha \cdot x) \in E$
$-(\alpha \cdot x) + (\alpha \cdot x) = -(\alpha \cdot x) + (\beta \cdot x)$

teniendo en cuenta el teorema 3:

$0 = -(\alpha) \cdot x + \beta \cdot x$ y según A_2 $\quad 0 = (-\alpha + \beta) \cdot x$

y por la consecuencia 5), puesto que $x \neq 0$, necesariamente ha de ser $(-\alpha + \beta) = 0$

Luego: $\alpha = \beta$

c.q.d.

7-2 SUBESPACIOS VECTORALES. DEFINICION

Dado un espacio vectorial E sobre un cuerpo K, llamamos subespacio vectorial de E a un subconjunto $V \subset E$ tal que él mismo es espacio vectorial sobre el cuerpo K.
Esto significa que el subconjunto V de E ha de ser:

a) Grupo abeliano para la restricción de la ley + de E a V; por tanto, subgrupo de E, es decir:

$$\forall\, x,y \in V, \qquad x + (-y) \in V$$

b) La restricción de la ley externa a V ha de estar definida en él.

$$\forall\, x \in V, \quad \forall\, \alpha \in K, \quad ,\alpha \cdot x \in V$$

de todo esto se desprende, pues, el siguiente:

Teorema 1: La condición necesaria y suficiente para que un subconjunto V de un espacio vectorial E sea subespacio vectorial, es que:

$$\forall\, x,y \in V \wedge \forall\, \alpha, \beta \in K \quad \alpha \cdot x + \beta \cdot y \in V$$

En efecto, veamos que es condición necesaria. Si V es subespacio vectorial, entonces $\alpha \cdot x \in V \wedge \beta \cdot y \in V$ por la condición b) y por ser grupo abeliano $\alpha \cdot x + \beta \cdot y \in V$.
Demostremos que es también condición suficiente. Para ello, basta con ver que se cumplen las condiciones a) y b) de la definición.
En efecto, $\forall\, x,y \in V$, tomemos $\alpha = 1, \beta = -1$.
Entonces:
$x - y \in V$; por lo tanto se cumple a) y ahora $\forall\; x, y \in\; V$, tomando $\beta = 0$, queda $\alpha \cdot x \in V$, que establece la condición b).

c.q.d.

EJEMPLOS:

1) El subconjunto de E que contiene solo al vector nulo $\}0\{ \subset E$, es un subespacio vectorial, pues

$$\forall\, \alpha, \beta \in K \quad \alpha \cdot 0 + \beta \cdot 0 = 0 \in \}0\{$$

2) El conjunto V de vectores $\alpha \cdot x$, $\forall\, \alpha \in K$ y siendo x un vector dado de E, es también un subespacio vectorial.

$$\forall\, \beta, \delta \in K, \forall\, \alpha_1 \cdot x, \alpha_2 \cdot x \in V$$
$$\beta \cdot (\alpha_1 \cdot x) + \delta \cdot (\alpha_2 \cdot x) = (\beta \cdot \alpha_1) \cdot x + (\delta \cdot \alpha_2) \cdot x$$
que será también un elemento de V.

3) En el espacio vectorial K^3 sobre K, el conjunto V de ternas que tienen los tres elementos iguales (α, α, α) $\forall \alpha \in K$, es un subespacio vectorial de K^3.
En efecto: $\forall \beta, \delta \in K$, $\forall (\alpha_1, \alpha_1, \alpha_1), (\alpha_2, \alpha_2, \alpha_2) \in K^3$
$\beta \cdot (\alpha_1, \alpha_1, \alpha_1) + \delta \cdot (\alpha_2, \alpha_2, \alpha_2) = (\beta \cdot \alpha_1, \beta \cdot \alpha_1, \beta \cdot \alpha_1) +$
$+ (\delta \cdot \alpha_2, \delta \cdot \alpha_2, \delta \cdot \alpha_2) = (\beta \alpha_1 + \delta \alpha_2, \beta \alpha_1 + \delta \alpha_2, \beta \cdot \alpha_1 + \delta \alpha_2)$

que pertenece también a V por tener los tres elementos iguales.

Teorema 2: La intersección de dos subespacios V_1 y V_2 de E, es otro subespacio de E.
En efecto: $\forall \alpha, \beta \in K, \quad \forall x,y \in V_1 \cap V_2$:

$x,y \in V_1 \cap V_2 \Rightarrow x,y \in V_1 \Rightarrow \alpha \cdot x + \beta \cdot y \in V_1$
$x,y \in V_1 \cap V_2 \Rightarrow x,y \in V_2 \Rightarrow \alpha \cdot x + \beta \cdot y \in V_2$

luego:

$\alpha \cdot x + \beta \cdot y \in V_1 \cap V_2$, y por tanto, $V_1 \cap V_2$ es un subespacio de E.

c.q.d.

7-3 COMBINACIONES LINEALES. DEFINICION

Dada una familia finita de q vectores $x_1, x_2 \dots x_q$ del espacio vectorial E, llamamos combinación lineal de esos vectores a todo vector $v \in E$ tal que cumple la relación:

$$v = \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \dots + \alpha_q \cdot x_q$$

siendo $\alpha_1, \alpha_2, \dots, \alpha_q$ escalares determinados de K.

EJEMPLOS:

1) El vector nulo, 0, es combinación lineal de cualquier familia finita de vectores.

En efecto, ya que dada una familia finita cualquiera de vectores $\{x_1, x_2, \dots x_q\}$ se puede escribir.

$$0 = 0 \cdot x_1 + 0 \cdot x_2 + \dots + 0 \cdot x_q$$

2) Todo vector x, $x \in E$ es combinación lineal de cualquier familia finita que lo contenga.
Sea por ejemplo la familia $\{x, x_1, x_2 \dots x_q\}$. Basta con escribir:

$$x = 1 \cdot x + 0 \cdot x_1 + \cdots + 0 \cdot x_q$$

3) En el espacio vectorial K^2 sobre el cuerpo K, consideremos la familia de vectores $\{e_1, e_2\}$, siendo $e_1 = (1,0)$ y $e_2 = (0,1)$.
Entonces, cualquier vector de K^2 es combinación lineal de e_1 y e_2, ya que $\forall (\alpha,\beta) \in K^2, (\alpha,\beta) = \alpha \cdot (1,0) + \beta \cdot (0,1)$.

Teorema 3: Dada una familia finita $\{x_1, x_2 \dots x_q\}$ de vectores de E, el conjunto de todas las combinaciones lineales de estos vectores, V, es un subespacio vectorial de E. Además, es el menor subespacio que contiene a dicha familia.

Demostremos que el conjunto de todas las combinaciones lineales es un subespacio. Para ello, basta con probar que se cumple la condición necesaria y suficiente expresada en el teorema 1:

$$v \in V,\ \exists\, \alpha_1, \alpha_2 \dots \alpha_q \in K \mid v = \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \dots + \alpha_q \cdot x_q$$

$$w \in V,\ \exists\, \beta_1, \beta_2, \dots \beta_q \in K \mid w = \beta_1 \cdot x_1 + \beta_2 \cdot x_2 + \dots + \beta_q \cdot x_q$$

$\forall\, \gamma, \delta \in K$:

$$\gamma \cdot v + \delta \cdot w = \gamma \cdot (\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \dots + \alpha_q x_q) + $$
$$+ \delta \cdot (\beta_1 \cdot x_1 + \dots + \beta_q \cdot x_q)$$

operando y agrupando queda:

$$= (\gamma \cdot \alpha_1 + \delta \cdot \beta_1) \cdot x_1 + (\gamma \cdot \alpha_2 + \delta \cdot \beta_2) \cdot x_2 + \dots + (\gamma \cdot \alpha_q + \delta \cdot \beta_q) \cdot x_q$$

y como la composición de escalares es un escalar, el resultado de escalar por vector será un vector. Luego $\gamma \cdot v + \delta \cdot w \in V$.
O sea, V es un subespacio.
Demostremos ahora que es el menor subespacio que contiene a esa familia.
Cualquier otro subespacio L que contenga a esa familia habrá de contener, según expresa la condición necesaria de T_1, todas las combinaciones lineales de esa familia y, por tanto, contendrá a V; es decir:

$$V \subset L$$

Y así, llamaremos subespacio engendrado por una familia finita de vectores $\{x_1, x_2, \dots x_q\}$ al conjunto de todas las combinaciones lineales de los mismos con escalares del cuerpo. Lo representaremos por $\& \{x_1, \dots x_q\}$

$$\& \{x_1, \dots x_q\} = \{v,\ v \in E \mid v = \alpha_1 x_1 + \cdots + \alpha_q \cdot x_q\}$$

Al subespacio $\& \{x_1 \dots x_q\}$ también se le llama variedad lineal engendrada.
A los vectores de la familia que engendra dicho subespacio vectorial se les llama *generadores,* y a la familia, por tanto, *familia de generadores.*

EJEMPLO:

En el espacio vectorial K^3 sobre K, se ha demostrado que el conjunto de vectores $(\alpha, \alpha, \alpha)\ \forall \alpha \in K$ es un subespacio vectorial V. Este subespacio vectorial está engendrado por la familia de un solo elemento $x = (1,1,1)$, puesto que

$$\forall (\alpha,\alpha,\alpha) \in V \quad (\alpha,\alpha,\alpha) = \alpha \cdot (1,1,1)$$

x es, pues, el generador de este subespacio vectorial que puede representarse, por $\& (x) = \& \{(1,1,1)\}$.

DEPENDENCIA LINEAL

7-4 FAMILIA DEPENDIENTE O LIGADA DE VECTORES

Dada una familia finita de p vectores $\{x_1, x_2, ..., x_p\}$ de un espacio vectorial E, decimos que es dependiente o ligada si existe algún conjunto de p escalares $\alpha_1, ..., \alpha_p$ *no todos nulos*, tales que dan una combinación lineal nula de aquellos vectores.

$$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + ..., + \alpha_p \cdot x_p = 0$$

Teorema 4: La condición necesaria y suficiente para que una familia finita de vectores $\{x_1, x_2, ..., x_p\}$ sea ligada, es que uno cualquiera de sus vectores se pueda escribir como combinación lineal de los otros $p - 1$.
Es condición necesaria. En efecto, si $\{x_1, ... x_p\}$ es una familia ligada, $\exists\ \alpha_1, ..., \alpha_p$ no todos nulos, tales que:

$$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + ... + \alpha_p \cdot x_p = 0$$

Supongamos que uno de los escalares que no son nulos sea $\alpha_i \neq 0$,

$1 \leqslant i \leqslant p$ Entonces $\exists\ \alpha_i^{-1} \in K$; por tanto

$$\alpha_i x_i = - \alpha_1 x_1 - \alpha_2 x_2 - ... - \alpha_{i-1} x_{i-1} - \alpha_{i+1} x_{i+1} - ... - \alpha_p x_p$$

operando a la izquierda con α_i^{-1}

$$\alpha_i^{-1} \cdot (\alpha_i \cdot x_i) = \alpha_i^{-1} (- \alpha_1 x_1) + \alpha_i^{-1} (- \alpha_2 \cdot x_2) + ... + \alpha^{-1} (- \alpha_p \cdot x_p)$$

o sea $x_i = [\alpha^{-1} \cdot (- \alpha_1)] \cdot x_1 + [\alpha_i^{-1} \cdot (- \alpha_2)] \cdot x_2 + ... + [\alpha_i^{-1} \cdot (- \alpha_p)] \cdot x_p$

como todos los productos son escalares, queda finalmente lo que queríamos demostrar, que x_i es combinación lineal de los demás

$$x_i = \text{C L} \{x_1, x_2, ..., x_{i-1}, x_{i+1}, ... x_p\}$$

Es condición suficiente:
Supongamos que uno de ellos cualquiera, x_j $1 \leqslant j \leqslant p$, por ejemplo, es combinación lineal de los otros:

$$x_j = \text{C L} \{x_1, x_2, ... x_{j-1}, x_{j+1}, ... x_p\}$$

esto significa que existen unos escalares $\beta_1, \beta_2, \dots \beta_{j-1}, \beta_{j+1} \dots \beta_p$ tales que

$$x_j = \beta_1 \, x_1 + \dots + \beta_{j-1} \cdot x_{j-1} + \beta_{j+1} \, x_{j+1} + \dots + \beta_p \cdot x_p$$

pasando x_j al segundo miembro, queda:

$$0 = -1 \cdot x_j + \beta_1 \, x_1 + \dots + \beta_{j-1} \, x_{j-1} + \beta_{j+1} \cdot x_{j+1} + \dots + \beta_p \cdot x_p$$

Hemos obtenido, pues, una combinación lineal nula de los vectores de la familia donde no todos los escalares $-1, \beta_1, \dots \beta_p$ son nulos, luego según la definición es un sistema ligado.
Podemos concluir, pues, que una familia es ligada o dependiente cuando uno o más de sus vectores es combinación lineal de los demás. Es decir, cuando pertenece al subespacio engendrado por los otros $p - 1$ vectores.

EJEMPLOS:

1) Una familia finita cualquiera $\{0_1 \, x_1, x_2, \dots x_p\}$ contiene el vector nulo, es ligada, puesto que podemos tomar un conjunto de escalares $\alpha, \alpha_1, \alpha_2, \dots, \alpha_p$ tales que $\alpha \neq 0$ y $\alpha_1 = \alpha_2 = \dots = \alpha_p = 0$ que da una combinación lineal nula

$$\alpha \cdot 0 + 0 \cdot x_1 + 0 \cdot x_2 + \dots + 0 \cdot x_p = 0$$

y que no son todos nulos, puesto que $\alpha \neq 0$

2) Dados en el espacio vectorial K^3 sobre el cuerpo K la familia $\{V_1, V_2, V_3\}$

$$V_1 = (1,0,1)$$
$$V_2 = (1,0,0)$$
$$V_3 = (0,0,1)$$

es una familia ligada, puesto que

$$(1,0,1) = (1,0,0) + (0,0,1)$$

que cumple la condición suficiente del teorema 4.

$$V_1 = 1 \cdot V_2 + 1 \cdot V_3$$

7-5 FAMILIA LIBRE O INDEPENDIENTE

Dada una familia finita de vectores $\{x_1, x_2, \ldots x_p\}$, decimos que es libre si los únicos escalares de K que pueden dar una combinación lineal nula de esos vectores son todos nulos.

$$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \ldots + \alpha_p \cdot x_p = 0 \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_p = 0$$

EJEMPLOS:

1) La familia constituida por un vector $\{x\}$ no nulo cualquiera de E, es una familia libre.
En efecto, ya que si $x \neq 0$, en la ecuación

$$\alpha \cdot x = 0$$

que forma la combinación lineal nula, ha de ser necesariamente $\alpha = 0$, según se demostró en la consecuencia 5 de 7-1-2. Por tanto, la única combinación lineal nula es con todos los escalares nulos. Es decir, $\{x\}$, $x \neq 0$ es una familia libre.

2) En el espacio vectorial K^3 sea la familia e_1, e_2, e_3

$$e_1 = (1,0,0)$$
$$e_2 = (0,1,0)$$
$$e_3 = (0,0,1)$$

esta familia es libre, puesto que toda combinación lineal nula

$$\alpha_1 \cdot e_1 + \alpha_2 \cdot e_2 + \alpha_3 \cdot e_3 = 0$$

exige que los escalares sean todos nulos. En efecto:

$$\alpha_1 \cdot (1,0,0) + \alpha_2 \cdot (0,1,0) + \alpha_3 \cdot (0,0,1) = (0,0,0)$$

operando

$$(\alpha_1,0,0) + (0,\alpha_2,0) + (0,0,\alpha_3) = (0,0,0)$$

O sea:

$$(\alpha_1,\alpha_2,\alpha_3) = (0,0,0,) \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$$

Teorema 5.—Dadas dos familias finitas F y F' de vectores de E, tales que $F \subset F'$ se cumple:

a) Si F es ligada, F' es ligada.
b) Si F' es libre, F es libre.

Vamos a demostrarlo:
En efecto: sea $F = \{x_1, x_2 \dots x_p\}$
y $F' = \{x_1, x_2 \dots x_p, x_{p+1} \dots x_q\}$

a) Supongamos F ligada. Entonces, $\exists\, \alpha_1, \alpha_2 \dots \alpha_p \in K$ entre los que hay algún $\alpha_i \neq 0 \quad 1 \leqslant i \leqslant p$, tales que:

$$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_p x_p = 0$$

y podemos tomar unos escalares $\alpha_{p+1} = \alpha_{p+2} = \dots = \alpha_q = 0$ y escribir
$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_p \cdot x_p + \alpha_{p+1} x_{p+1} + \dots \alpha_q \cdot x_q = 0$

y hemos obtenido una combinación lineal nula de los vectores de la familia F' en la que hay, por hipótesis, algún $\alpha_i \neq 0$. Luego F' es ligada.

b) Vamos a demostrarlo por reducción al absurdo. Supongamos que F' sea libre, y que F sea ligada.
Entonces, $\exists\, \alpha_1, \alpha_2 \dots \alpha_p$ no todos nulos, tales que

$$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_p x_p = 0$$

añadiendo $\alpha_{p+1} \cdot x_{p+1} + \dots + \alpha_q x_q$ con $\alpha_{p+1} = \alpha_{p+2} = \dots = \alpha_q = 0$

queda:

$$\alpha_1 x_1 + \dots + \alpha_p x_p + \dots + \alpha_q x_q = 0$$

combinación lineal nula, donde no todos los coeficientes $\alpha_1, \alpha_2, \dots \alpha_p \dots \alpha_q$ son nulos. Es decir, F' sería una familia ligada. Hemos llegado, pues, a la contradicción (F' libre $\wedge$ F' ligada), por tanto, queda demostrado el teorema.

Teorema 6.—Sea una familia finita de vectores $\{x_1, x_2, \dots, x_p\}$ de un espacio vectorial E. Toda familia libre de vectores $\{y_1, y_2, \dots, y_m\}$

del subespacio $\& \{x_1, \ldots, x_p\}$ engendrado por esta familia tiene un número de vectores $m \leqslant p$.
Vamos a demostrarlo por reducción al absurdo. Sea, pues,
$\{y_1, y_2, \ldots, y_m\} \subset \& \{x_1 \ldots, x_p\}$, y supongamos que $m > p$.

Por ser $y_1 \in \& \{x_1, \ldots, x_p\}$, se cumple que

$$\& \{y_1, x_1, \ldots, x_p\} = \& \{x_1, \ldots, x_p\} \qquad (1)$$

además, la familia $\{y_1, x_1, \ldots, x_p\}$ es ligada, por ser $y_1 \in \& \{x_1, \ldots, x_p\}$. Entonces deben existir unos escalares $\beta_1, \alpha_1, \ldots, \alpha_p$ no todos nulos, tales que

$$\beta_1 y_1 + \alpha_1 x_1 + \ldots + \alpha_p x_p = 0 \qquad (2)$$

y no todos los $\alpha_1, \ldots, \alpha_p$ pueden ser nulos, porque si esto ocurriese habría de ser $\beta_1 = 0$, y la anterior ecuación quedaría:

$$\beta_1 \cdot y_1 = 0 \qquad (3)$$

que implicaría $y_1 = 0$ por la consecuencia 5. Pero y_1 no puede ser igual a cero, pues entonces la familia $\{y_1, \ldots, y_m\}$ sería ligada contra la hipótesis. Luego $\exists\, \alpha_i \neq 0 \quad 1 \leqslant i \leqslant p$.
Supongamos que un $\alpha_i \neq 0$ sea, por ejemplo, α_1. Entonces debe existir $\alpha_1^{-1} \in K$, y operando con él en la combinación lineal anterior, queda, despejando x_1,

$$x_1 = -(\beta_1 \cdot \alpha_1^{-1}) y_1 - (\alpha_2 \cdot \alpha_1^{-1}) x_2 - \ldots - (\alpha_p \alpha_1^{-1}) x_p \qquad (4)$$

y así, x_1 es combinación lineal de $\{y_1, x_2, \ldots, x_p\}$, por tanto pertenece al subespacio engendrado por éstos:

$$x_1 \in \& \{y_1, x_2, \ldots, x_p\}$$

siendo evidente, por otra parte:

$$\& \{y_1, x_2, \ldots, x_p\} = \& \{x_1, \ldots, x_p\} \qquad (5)$$

Es evidente que se cumple también:

$$\& \{y_1, y_2, x_2, \ldots, x_p\} = \& \{y_1, x_2, \ldots, x_p\} \qquad (6)$$

Por otra parte, la familia $\{y_1, y_2, x_2, \dots, x_p\}$ es ligada, ya que $y_2 \in \& \{y_1, x_2, \dots, x_p\}$, luego $\exists\, \beta_1, \beta_2, \alpha_2, \dots, \alpha_p$ no todos nulos, tales que:

$$\beta_1 y_1 + \beta_2 y_2 + \alpha_2 x_2 + \dots + \alpha_p x_p = 0 \qquad (7)$$

pero en (7) no pueden ser todos los $\alpha_2, \dots, \alpha_p$ nulos, puesto que de ser así, quedaría:

$$\beta_1 y_1 + \beta_2 y_2 = 0$$

con $\beta_1 \neq 0$ ó $\beta_2 \neq 0$, lo cual no es posible, porque esto indicaría que la familia y_1, y_2 es ligada, y, por tanto, también lo sería la familia $y_1, \dots, y_m$ por la consecuencia 5, contrariamente a la hipótesis de que eran una familia libre.
Ha de haber, pues, $\exists\, \alpha_i \neq 0,\ 2 \leqslant i \leqslant p$. Supongamos que sea $\alpha_2 \neq 0$. Existe, pues, $\alpha_2^{-1} \in k$ y podemos despejar x_2 en (7):

$$x_2 = -(\beta_1 \cdot \alpha_2^{-1})y_1 - (\beta_2\, \alpha_2^{-1})y_2 - (\alpha_3 \cdot \alpha_2^{-1})x_3 - \dots - (\alpha_p\, \alpha_2^{-1})x_p$$

mostrando de este modo que x_2 es combinación lineal de $\{y_1, y_2, x_3, \dots, x_p\}$ y que por lo tanto se cumple:

$$\& \{y_1, y_2, x_3, \dots, x_p\} = \& \{y_1, x_2, \dots, x_p\} = \& \{x_1, x_2, \dots, x_p\}$$

Es decir, hemos sustituido dos vectores de la familia inicial por otros dos del sistema libre, y el subespacio engendrado por la nueva familia es el mismo que el inicial. Este proceso podemos repetirlo hasta p veces, puesto que $m > p$, y sustituir todos los vectores x por los p primeros vectores y, verificándose que:

$$\& \{y_1, \dots, y_p\} = \& \{x_1, \dots, x_p\}$$

En la familia de vectores libres han quedado todavía $\{y_{p+1}, y_{p+2}, \dots, y_m\}$, que son por hipótesis vectores del subespacio $\& \{x_1, \dots, x_p\}$ y por tanto del subespacio $\& \{y_1, \dots, y_p\}$. Esto significa que cada uno de los y_i $p + 1 \leqslant i \leqslant m$ es combinación lineal de la familia $\{y_1, \dots, y_p\}$, lo cual indica que la familia $\{y_1, y_2, \dots, y_p, \dots, y_m\}$ es una familia ligada, contrariamente a la hipótesis del teorema, y por tanto queda demostrado que m no puede ser mayor que p.

7-6 BASE DE UN ESPACIO VECTORIAL. DEFINICION

Llamamos base de un espacio vectorial E a toda familia libre de E que lo engendra.

EJEMPLO:

En el espacio vectorial K^3 sobre el cuerpo K, la familia e_1, e_2, e_3 siendo:

$$e_1 = (1, 0, 0)$$
$$e_2 = (0, 1, 0)$$
$$e_3 = (0, 0, 1)$$

es una base del mismo, puesto que por un lado es un sistema generador, ya que todo vector $(\alpha_1, \alpha_2, \alpha_3)$ de K^3 se puede expresar como combinación lineal de ellos, siendo:

$$(\alpha_1, \alpha_2, \alpha_3) = \alpha_1 \cdot (1, 0, 0) + \alpha_2 \cdot (0, 1, 0) + \alpha_3 \cdot (0, 0, 1)$$

y por otro lado es un sistema libre, como vimos ya al hablar de independencia lineal.

7-6-1 ESPACIOS VECTORIALES DE DIMENSION FINITA

Se denominan así todos aquellos que están engendrados por una familia finita de generadores.

EJEMPLO:

Es espacio vectorial de dimensión finita el K^3 sobre K del ejemplo anterior, puesto que le hemos establecido un sistema generador con tres vectores.
También lo es K^2 sobre K, y, en general, K^n sobre K con n finito por la misma razón.

En adelante, vamos a circunscribir nuestro estudio a los espacios vectoriales de dimensión finita, y a demostrar en ellos la existencia de bases finitas.

Teorema 7.—En todo espacio vectorial de dimensión finita E existe una base al menos.
En efecto, por ser de dimensión finita posee una familia de generadores finita. Sea ésta $\{x_1, ..., x_n\}$. Por tanto:

$$E = \mathcal{E} \{x_1, ..., x_n\}$$

Esta familia puede ser libre o ligada. Si es libre sería una base y quedaría demostrado el teorema. Si es ligada, esto significa que existe alguno de esos vectores que es combinación lineal de los demás. Supongamos que sea x_1, por ejemplo, combinación lineal de $\{x_2, ..., x_n\}$. Entonces, la familia $\{x_2, ..., x_n\}$, seguiría engendrando E.

$$E = \mathcal{E} \{x_2, ..., x_n\}$$

Ahora puede ocurrir otra vez uno de los dos casos: que la familia $\{x_2, ..., x_n\}$ sea libre o ligada. En el primer caso sería base y quedaría demostrado el teorema. En el segundo habría un vector que sería combinación lineal de los demás. Podemos entonces suprimirlo y el sistema resultante seguirá engendrando E. Supongamos que x_2 sea combinación lineal de los otros. Entonces:

$$E = \mathcal{E} \{x_3, ..., x_n\}$$

Procediendo de este modo, llegará un momento en que ocurrirá *que el sistema generador de E resultante de esas operaciones SERA LIBRE,* pues de lo contrario llegaríamos, tras realizar la operación $n - 1$ veces, a un sistema que contendría un solo vector y que sería ligado, lo cual significaría que dicho vector es el vector nulo, y que el espacio vectorial engendrado por él sería el trivial $E = \{0\}$.
Conclusión: Sabemos, pues, con este teorema que todos los espacios vectoriales de dimensión finita poseen alguna base, y que ésta se halla tomando un sistema de generadores cualquiera, y eliminando de él los vectores que sean combinación lineal de los demás, hasta obtener un sistema libre.

EJEMPLO:

Dado el sistema de generadores $\{x_1, x_2, x_3, x_4, x_5\}$ de K^4 sobre K

$$\begin{aligned} x_1 &= (1,1,1,0) \\ x_2 &= (0,1,0,0) \\ x_3 &= (1,1,0,0) \\ x_4 &= (0,0,1,1) \\ x_5 &= (0,0,0,1) \end{aligned}$$

determinemos una base de este espacio vectorial. Para ello busquemos si hay alguna combinación lineal entre ellos, es decir, veamos si existen unos valores distintos de cero para los escalares $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$, que cumplan:

$$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \alpha_3 \cdot x_3 + \alpha_4 \cdot x_4 + \alpha_5 \cdot x_5 = 0 \ (^*)$$

Sustituyamos los vectores por sus componentes y operando quedará:

$$\alpha_1 \cdot (1,1,1,0) + \alpha_2 \cdot (0,1,0,0) + \alpha_3 \cdot (1,1,0,0) + \alpha_4 \cdot (0,0,1,1) + \alpha_5 \cdot (0,0,0,1) = (0,0,0,0)$$

Es decir:

$$(\alpha_1, \alpha_1, \alpha_1, 0) + (0, \alpha_2, 0,0) + (\alpha_3, \alpha_3, 0,0) + (0,0, \alpha_4, \alpha_4) + (0,0,0, \alpha_5) = (0,0,0,0)$$

Sumando y agrupando queda:

$$(\alpha_1 + \alpha_3, \alpha_1 + \alpha_2 + \alpha_3, \alpha_1 + \alpha_4, \alpha_4 + \alpha_5) = (0, 0, 0, 0)$$

E igualando, queda el sistema:

$$\begin{aligned} &\alpha_1 + \alpha_3 = 0 \\ &\alpha_1 + \alpha_2 + \alpha_3 = 0 \\ &\alpha_1 + \alpha_4 = 0 \\ &\alpha_4 + \alpha_5 = 0 \end{aligned}$$

en el que fácilmente se aprecia:

$$\alpha_2 = 0 \quad \text{y} \quad \alpha_1 = -\alpha_3 = -\alpha_4 = \alpha_5$$

(*) 0 indica el vector nulo de K^4 sobre K, es decir, $0 = (0,0,0,0)$

Y sustituyendo ésto en la ecuación inicial queda:

$$\alpha_1 \cdot (x_1 - x_3 - x_4 + x_5) = 0$$

Y como esta ecuación es válida para $\forall\ \alpha_1 \in K$ queda:

$$x_1 - x_3 - x_4 + x_5 = 0$$

de donde se puede despejar, por ejemplo, x_1:

$$x_1 = x_3 + x_4 - x_5$$

como x_1 es combinación lineal de los demás, podemos eliminarlo y queda el sistema generador reducido a: $\{x_2, x_3, x_4, x_5\}$
Veamos ahora si este sistema es libre:

$$\beta_2 \cdot x_2 + \beta_3 \cdot x_3 + \beta_4 \cdot x_4 + \beta_5 \cdot x_5 = 0$$

Operando como antes:
$(0, \beta_2, 0, 0) + (\beta_3, \beta_3, 0, 0) + (0, 0, \beta_4, \beta_4) + (0, 0, 0, \beta_5) = (o, 0, 0, 0)$

Sumando y agrupando:

$$(\beta_3, \beta_2 + \beta_3, \beta_4, \beta_4 + \beta_5) = (0, 0, 0, 0)$$

Es decir:

$$\begin{aligned} \beta_3 &= 0 \\ \beta_2 + \beta_3 &= 0 \\ \beta_4 &= 0 \\ \beta_4 + \beta_5 &= 0 \end{aligned}$$

Que resolviendo da $\beta_2 = \beta_3 = \beta_4 = \beta_5 = 0$
Y por lo tanto, los cuatro vectores $\{x_2, x_3, x_4, x_5\}$ son independientes, y por tanto, constituyen una base.
Acabamos de ver que de una familia de generadores siempre podemos encontrar una base contenida en ella. Veamos ahora que a partir de una familia libre podemos formar también una base.

Teorema 8.—Dada la familia libre F, siempre existe una base que la contiene.
En efecto, puesto que nos estamos refiriendo a espacios vectoriales

de dimensión finita, existe siempre una familia finita de generadores G de ese espacio vectorial. Entonces, la reunión

$$R = G \cup F$$

es también una familia de generadores.
Consideremos ahora el conjunto de todas las partes de R libres que contienen a F. Llamemos a este conjunto H

$$H = \{ X, X \subset R \mid X \text{ es libre} \wedge F \subset X \}$$

H no es vacío, puesto que contiene, al menos, a F.
Observemos ahora el número de elementos que tienen los $X \in H$, y supongamos que $p \in N$ sea el máximo número de elementos que poseen.
Tomemos, pues, un $Y \in H$ que posea p elementos $Y = \{y_1, ..., y_p\}$
Entonces, se cumple que:

$$F \subset Y \subset R$$

Y pueden suceder dos casos:

1) Que p = n.° de elementos de R, con lo cual Y = R y R sería libre y generador y por tanto base, quedando demostrado el teorema.
2) Que $p <$ n.° de elementos de R.

Entonces: $\forall\ x, x \in R - F$, la familia formada por $\{x, y_1, ... y_p\}$ sería ligada, pues de lo contrario tendríamos una familia libre que contiene a F con $p + 1$ elementos, contrariamente a lo que hemos dicho más arriba, de que el máximo número de elementos de estas familias que contienen a F es p.

Si $\{x, y_1, ... y_p\}$ es ligado, $\exists\ \alpha; \beta_1, \beta_2, ... \beta_p \in K$ no todos nulos, tales que:

$$\alpha \cdot x + \beta_1 \cdot y_1 + \beta_2 \cdot y_2 + ... + \beta_p \cdot y_p = 0$$

donde, además, no puede ser nulo α puesto que ello implicaría que Y es un sistema ligado; y por tanto $\exists\ \alpha^{-1} \in K$.
Despejando x queda:

$$x = -(\alpha^{-1} \cdot \beta_1) \cdot y_1 - ...... - (\alpha^{-1} \cdot \beta_p) \cdot y_p$$

Luego $\forall\, x \in R - F$ es combinación lineal de los vectores de la familia Y, y $F \subset Y$, luego todo $x \in R$ es combinación lineal de la familia libre Y, y como R es una familia de generadores, Y también lo es, por tanto Y es base.
Luego vemos que siempre podemos completar una familia libre cualquiera con los vectores libres que hagan falta, basta obtener con ella una base.

Teorema 9.—En un espacio vectorial E de dimensión finita, todas las bases tienen el mismo número finito de vectores.
En efecto, el número de vectores de una base cualquiera es finito, puesto que una base es una familia de generadores y por definición de espacio vectorial de dimensión finita, ha de tener un número finito de elementos.
Veamos que todas las bases tienen el mismo número de vectores. Para ello consideremos dos bases distintas B y B′ del espacio vectorial E, y sean

$$\text{Card}\ (B) = n$$
$$\text{Card}\ (B') = n'$$

teniendo en cuenta que B es una base y por tanto una familia de generadores y que B′ es una familia libre y aplicando el teorema 6:

$$n' \leqslant n$$

y a la inversa, teniendo en cuenta ahora que B′ es la base y por tanto familia de generadores y B es una familia libre del espacio E engendrado por B′, por el teorema 6 tenemos

$$n \leqslant n'$$

de estas dos desigualdades se deduce finalmente

$$n = n'$$

7-6-2 DIMENSION DE UN ESPACIO VECTORIAL

Llamamos dimensión de un espacio vectorial de dimensión finita E, al número de vectores de una base B, de él.

El teorema 9 nos asegura que la dimensión puede hallarse a partir de una base cualquiera, puesto que todas tienen el mismo número de vectores.

EJEMPLO:

Hemos encontrado que (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1) forman una base de K^4 y que también lo son (0,1,0,0), (1,1,0,0), (0,0,1,1), (0,0,0,1), luego la dimensión de K^4 es 4. Podemos igualmente decir que la dimensión de K^n es n.

Teorema 10.—Sea $\{x_1, \ldots\ldots x_p\}$ una familia de p vectores libres de un espacio vectorial E. Todo vector $\vec{y}$ perteneciente al subespacio $\&\ \{x_1, \ldots\ldots x_p\}$ engendrado por estos vectores puede expresarse de una forma única como combinación lineal de los vectores de dicha familia. Es decir, que los p escalares $\alpha_1, \ldots, \alpha_p \in K$ tales que:

$$y = \alpha_1 \cdot x_1 + \ldots\ldots + \alpha_p \cdot x_p$$

son únicos.

En efecto, supongamos que para un vector $v \in \&\ \{x_1, \ldots\ldots x_p\}$ existan dos conjuntos de escalares distintos $\beta_1 \ldots\ldots \beta_p$ y $\delta_1 \ldots\ldots \delta_p$ tales que:

$$v = \beta_1 \cdot x_1 + \ldots\ldots + \beta_p \cdot x_p$$
$$v = \delta_1 \cdot x_1 + \ldots\ldots + \delta_p \cdot x_p$$

igualando tenemos:

$$\beta_1\, x_1 + \ldots\ldots + \beta_p\, x_p = \delta_1 \cdot x_1 + \ldots\ldots + \delta_p \cdot x_p$$

o sea: $\quad (\beta_1 - \delta_1) \cdot x_1 + \ldots\ldots + (\beta_p \cdot \delta_p) \cdot x_p = 0$

Ahora bien, como $\{x_1, \ldots\ldots x_p\}$ es un sistema libre, todos los escalares que aparecen en esta combinación lineal han de ser nulos, luego:

$$\begin{array}{ccc} \beta_1 - \delta_1 = 0 & \Rightarrow & \beta_1 = \delta_1 \\ \vdots & & \vdots \\ \beta_p - \delta_p = 0 & \Rightarrow & \beta_p = \delta_p \end{array}$$

lo cual es contrario a la hipótesis de que ambos conjuntos de escalares eran distintos, y por tanto queda demostrado el teorema.

Consecuencia: Dado un espacio vectorial E de dimensión n y una base de él, $B = \{e_1, \ldots\ldots e_n\}$ todo vector de E puede expresarse de una forma única como combinación lineal de los vectores de la base $\{e_1, \ldots\ldots e_n\}$

Esta consecuencia es evidente a partir del teorema, supuesto que en este caso $E = \mathcal{E}\, \{e_1, \ldots\ldots e_n\}$ y $\{e_1, \ldots\ldots e_n\}$ es una familia libre.

Esta consecuencia nos permite asignar en el espacio vectorial E de n dimensiones definido sobre K a cada vector x un conjunto de n escalares $(\alpha_1, \ldots\ldots \alpha_n)$ único

Así, pues, a cada $x \in E$ se le puede asignar, conocida una base de E, un vector y solo uno del espacio vectorial K^n sobre K. Es decir, que conocida una base de E, las operaciones con un conjunto de vectores de E se convierten en operaciones con un conjunto de vectores de K^n, y el conocimiento y manejo de E se convierte en el conocimiento y manejo de K^n. De ahí la importancia de este último.

7-7 COORDENADAS DE UN VECTOR

Llamamos coordenadas de un vector $x \in E$ en una base $B = \{e_1, \ldots\ldots e_n\}$ del espacio vectorial E, al conjunto de escalares $\alpha_1, \ldots\ldots \alpha_n \in K$; con los que se expresa x como combinación lineal de los vectores de B.

$$x = \alpha_1 \cdot e_1 + \ldots\ldots + \alpha_n \cdot e_n$$

EJEMPLO:

En el espacio vectorial K^4 sobre K, la base constituida por $\{e_1, e_2, e_3, e_4\}$

$$e_1 = (1,0,0,0)$$
$$e_2 = (0,1,0,0)$$
$$e_3 = (0,0,1,0)$$
$$e_4 = (0,0,0,1)$$

se llama base "canónica" o "standard". En ella todo vector $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ de K^4 tiene por coordenadas los cuatro mismos escalares que lo definen, ya que:

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha_1 \cdot (1,0,0,0) + \alpha_2 \cdot (0,1,0,0) + \alpha_3 \cdot (0,0,1,0) + \alpha_4 \cdot (0,0,0,1)$$

y las coordenadas serán, pues, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$
Particularicemos ahora el cuerpo K a los reales K =. R, con lo que K^n será R^n
Tomemos ahora otra base cualquiera; la de un ejemplo anterior: $B' = \{u_1, u_2, u_3, u_4\}$

$$\begin{aligned} u_1 &= (0,1,0,0) \\ u_2 &= (1,1,0,0) \\ u_3 &= (0,0,1,1) \\ u_4 &= (0,0,0,1) \end{aligned}$$

El vector $(2, 3, -1, -2)$ que en la base canónica tiene unas coordenadas $2, 3, -1, -2$, en la base B′ tendrá unas coordenadas $\beta_1, \beta_2, \beta_3, \beta_4$ que vamos a determinar:

$$\begin{aligned}(2, 3, -1, -2) = \beta_1 \cdot (0,1,0,0) + \beta_2 \cdot (1,1,0,0) + \beta_3 \cdot (0,0,1,1) \\ + \beta_4 \cdot (0,0,0,1)\end{aligned}$$

operando y agrupando queda:

$$(2, 3, -1, -2) = (\beta_2, \beta_1 + \beta_2, \beta_3, \beta_3 + \beta_4)$$

e igualando: $\beta_1 = 1, \quad \beta_2 = 2, \quad \beta_3 = -1, \quad \beta_4 = -1$

luego en la nueva base B′ tiene unas coordenadas $2, 1, -1, -1$ que son distintas de las que poseía en la base canónica, y es que las coordenadas son solo los escalares de la combinación lineal de los vectores de la base que nos da el vector deseado y que variarán al variar la base en que se expresa un vector dado.

Así, pues, un vector tendrá coordenadas distintas según que se exprese en una base o en otra, y se impone por tanto el arbitrar el paso de las coordenadas $(\alpha_1, \ldots\ldots \alpha_n)$ de un vector $x \in E$ en una base B, a las coordenadas $(\beta_1, \ldots\ldots \beta_n)$ del mismo vector x en otra base distinta B′ de E.
En el espacio vectorial K^n sobre K, el problema de cambio de base podemos resolverlo de momento del siguiente modo: Supongamos un vector $x \in K^n$, que posee unas coordenadas conocidas $(\alpha_1, \ldots\ldots \alpha_n)$

respecto a una base $B = \{v_1, \ldots\ldots v_n\}$ y deseamos hallar sus coordenadas respecto a otra base $B' = \{u_1, \ldots\ldots u_n\}$. Consideremos para ello que los n incógnitas $\beta_1, \ldots\ldots \beta_n$ son las coordenadas respecto a B' que deseamos hallar. Por definición de base el vector x se expresará:

en la base B $\quad x = \alpha_1 \cdot v_1 + \ldots\ldots + \alpha_n \cdot v_n$

en la base B' $\quad x = \beta_1 \cdot u_1 + \ldots\ldots + \beta_n \cdot u_n$

Igualando ambas expresiones, pues se trata del mismo vector x:

$$\alpha_1 \cdot v_1 + \ldots\ldots + \alpha_n \cdot v_n = \beta_1 \cdot u_1 + \ldots\ldots + \beta_n \cdot v_n$$

y de esta igualdad, aparece a la izquierda un vector, que por ser un elemento de K^n es un conjunto ordenado de n escalares, y a la derecha, otro vector que es otro conjunto ordenado de n escalares. Para que ambos sean iguales, por definición de conjunto ordenado de n elementos, han de ser iguales cada uno de sus escalares respectivos. El 1.° de la izquierda igual al 1.° de la derecha. El 2.° al 2.°, y así sucesivamente, el en-esimo de la izquierda al en-esimo de la derecha, con lo que aparecen n ecuaciones, con los n incógnitas $\beta_1, \ldots\ldots \beta_n$. De la resolución de este sistema de ecuaciones, obtendremos las coordenadas que buscábamos.

EJEMPLO:

Consideremos en el espacio vectorial R^3 sobre R el vector x, que en la base $B = \{v_1, v_2, v_3\}$ tiene por coordenadas 2, -1, 1, siendo:

$$v_1 = (1, 1, 0)$$
$$v_2 = (0, 1, 1)$$
$$v_3 = (1, 0, 1)$$

y busquemos sus coordenadas en la base: $B' = \{u_1, u_2, u_3\}$, siendo

$$u_1 = (1, 2, 3)$$
$$u_2 = (0, 2, -1)$$
$$u_3 = (-3, 0, 0)$$

siguiendo nuestra explicación anterior:

$$x = 2 \cdot (1, 1, 0) - 1 \cdot (0, 1, 1) + 1 \cdot (1,0,1)$$
$$x = \beta_1 \cdot (1, 2, 3) + \beta_2 \cdot (0, 2, -1) + \beta_3 \cdot (-3, 0, 0)$$

Igualando:

$$2 \cdot (1, 1, 0) - 1 \cdot (0, 1, 1) + 1 \cdot (1, 0, 1) = \beta_1 \cdot (1, 2, 3) + \beta_2 \cdot (0, 2, -1) + \beta_3 \cdot (-3, 0, 0)$$

Operando los escalares con los vectores y agrupando queda:

$$(3, 1, 0) = (\beta_1 - 3\beta_3, 2\beta_1 + 2\beta_2, 3\beta_1 - \beta_2)$$

O sea:

$$\left.\begin{aligned} 3 &= \beta_1 - 3\beta_3 \\ 1 &= 2\beta_1 + 2\beta_2 \\ 0 &= 3\beta_1 - \beta_2 \end{aligned}\right\} \text{ y resolviendo } \beta_1 = \frac{1}{8},\ \beta_2 = -\frac{3}{8}, \beta_3 = -\frac{23}{24}$$

Por tanto, las coordenadas de x en B' son $\frac{1}{8}, -\frac{3}{8}, -\frac{23}{24}$

7-8 DIMENSION DE UN SUBESPACIO

Teorema 11.—Todo subespacio vectorial V de un espacio vectorial E sobre K de dimensión finita n, es de dimensión finita y se cumple además

$$\dim V \leqslant n$$

En efecto: Si el subespacio es $V = \{0\}$ el teorema es trivial. Supongamos que $V \neq \{0\}$. Entonces tomemos un vector $v_1 \in V$ $v_1 \neq 0$ y construyamos $\mathcal{L}\{v_1\}$. Si $V = \mathcal{L}\{v_1\}$ el teorema está demostrado, pues la dimensión de V sería 1. Supongamos que $V \neq \mathcal{L}\{v_1\}$. Tomemos otro vector $v_2 \in V - \mathcal{L}\{v_1\}$, $v_2 \neq 0$, entonces v_2 es linealmente independiente con v_1 y por tanto la familia $\{v_1, v_2\}$ es libre, y formemos el subespacio $\mathcal{L}\{v_1, v_2\}$. Si $V = \mathcal{L}\{v_1, v_2\}$ el teorema estaría demostrado, pues v_1 y v_2 son linealmente independientes (ya que $v_2 \notin \mathcal{L}\{v_1\}$) y $\dim V = 2$. Si $V \neq \mathcal{L}\{v_1, v_2\}$

tomemos otro vector $v_3 \in V - \& \{v_1, v_2\}$, siendo por construcción la familia $\{v_1, v_2, v_3\}$ libre, y así procedemos sucesivamente. Supongamos que se ha realizado este proceso n veces sin haber encontrado un caso que demuestre el enunciado y que se sigue cumpliendo que $V \neq \& \{v_1, \ldots\ldots, v_n\}$. Entonces $\exists\, v_{n+1} \in V - \& \{v_1, \ldots\ldots, v_n\}$, lo cual significaría que la familia $\{v_1, \ldots\ldots, v_n, v_{n+1}\}$ es una familia libre con $n + 1$ vectores, que evidentemente es imposible, ya que

$$\{v_1, \ldots\ldots, v_n, v_{n+1}\} \subset V \subset E$$

y según el teorema 6, como la base (familia de generadores) de E tiene n vectores, cualquier familia libre de E ha de tener un número de vectores menor o igual a n y, en consecuencia, no es posible que exista algún $v_{n+1} \in V - \& \{v_1, \ldots\ldots, v_n\}$; luego, como máximo $V = \& \{v_1, \ldots\ldots, v_n\}$ siendo $\{v_1, \ldots\ldots, v_n\}$ una familia libre. Ahora bien, una familia libre con n vectores de E engendra todo el espacio vectorial E, luego en este caso límite $V = E$.
Hemos demostrado, pues, que la dimensión de V es, $\dim V \leqslant n$.

7-9 SUMA DE DOS SUBESPACIOS

Sea el espacio vectorial de n dimensiones E sobre K. Dados dos subespacios V y W de E, llamamos suma de los dos y lo representaremos por V + W a un subconjunto de E, definido del siguiente modo:

$$L = V + W = \{x + y;\ \forall\, x \in V \ \wedge\ \forall\, y \in W\}$$

La suma de los dos subespacios se forma, pues, sumando a cada vector del primer subespacio V con cada uno de los vectores del segundo W.

Demostremos que la suma de dos subespacios L = V + W, definida de este modo, es un subespacio.

En efecto, vamos a ver que se cumple el teorema 1, y que por tanto L es un subespacio vectorial.

$$\forall\, z_1, z_2 \in L,\ \exists\, x_1, x_2 \in V \ \wedge\ \exists\, y_1, y_2 \in W \mid z_1 = x_1 + y_1 \ \wedge\ z_2 = x_2 + y_2$$

$\forall \alpha_1, \alpha_2 \in K,$

$\alpha_1 \cdot z_1 + \alpha_2 \cdot z_2 = \alpha_1 \cdot (x_1 + y_1) + \alpha_2 \cdot (x_2 + y_2) = \alpha_1 \cdot x_1 + \alpha_1 \cdot y_1 +$

$+ \alpha_2 \cdot x_2 + \alpha_2 \cdot y_2 = (\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) + (\alpha_1 \cdot y_1 + \alpha_2 \cdot y_2)$

y como V y W son subespacios vectoriales,

$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 \in V \quad \wedge \quad \alpha_1 \cdot y_1 + \alpha_2 \cdot y_2 \in W$

Luego $\alpha_1 \cdot z_1 + \alpha_2 \cdot z_2 \in L$

L es, pues, un subespacio vectorial.

Teorema 12.—El subespacio suma L de dos subespacios V, W de E, es el menor subespacio vectorial que contiene a la reunión $V \cup W$.
En efecto, si tomamos el vector $0 \in V$ y le vamos sumando cada vector de W, se obtiene el subespacio vectorial W.
Luego $W \subset L$

Si ahora tomamos el $0 \in W$ y le sumamos cada vector de V, obtenemos el subespacio V, luego por definición de L:

$$V \subset L$$

entonces $V \cup W \subset L$

Por otro lado, cualquier subespacio S de E que contenga $V \cup W$ cumplirá: $(\forall\ x \in V \Rightarrow x \in S) \wedge (\forall\ y \in W \Rightarrow y \in S)$, luego por definición de subespacio, también, $x + y \in S$, y por tanto $L \subset S$.
Queda demostrado, pues, que el subespacio suma L está incluido en cualquier subespacio S que contenga a $V \cup W$ y por tanto L es el menor subespacio que contiene a esta reunión.

7-9-1 DIMENSION DEL SUBESPACIO SUMA

El subespacio suma L de V y W tiene una dimensión finita, puesto que es un subespacio de E, y E tiene dimensión n. Vamos a establecer la relación existente entre la dimensión del subespacio suma y las dimensiones de V y W.

Teorema 13.—Si dim $V = r$ y $B_v = \{ v_1, ..., v_r \}$ y dim $W = s$ y $B_w = \{ w_1, ..., w_s \}$ entonces el conjunto $\{ v_1, ..., v_r, w_1, ..., w_s \}$ es generador del subespacio suma L.

En efecto, $\forall\ z \in L \quad \exists x \in V \ \wedge \ \exists y \in W \mid z = x + y$
pero, por ser $x \in V \quad x = \alpha_1 \cdot v_1 + ... + \alpha_r \cdot v_r$
y por ser $y \in W \quad y = \beta_1 \cdot w_1 + ... + \beta_s \cdot w_s$

Luego:

$$z = x + y = \alpha_1 \cdot v_1 + ... + \alpha_r \cdot v_r + \beta_1 \cdot w_1 + ... + \beta_s \cdot w_s$$

por tanto $z \in L$ es combinación lineal de $\{ v_1, ..., v_r, w_1, ..., w_s \}$
Luego este conjunto es generador del subespacio L.

Teorema 14.—Dados los subespacios V y W de un espacio vectorial E de dimensión n se verifica:

$$\dim (V + W) + \dim (V \cap W) = \dim V + \dim W$$

En efecto: Supongamos que dim $V = r$, dim $W = s$, dim $(V \cap \cap W) = m$.
Sea $B_I = \{ e_1, ..., e_m \}$ una base del subespacio intersección.
La familia libre B_I cumple:

$$\{ e_1, ..., e_m \} \subset V$$
$$\{ e_1, ..., e_m \} \subset W$$

En virtud del teorema 8 la familia libre B_I puede ampliarse con vectores libres de $V - (V \cap W)$ hasta lograr una base de V.

$$B_v = \{ e_1, ..., e_m, v_{m+1}, v_{m+2}, ..., v_r \}$$

y de igual modo se consigue una base de W:

$$B_w = \{ e_1, ..., e_m, w_{m+1}, w_{m+2}, ..., w_s \}$$

Teniendo ahora en cuenta el teorema 13, el conjunto:

$$S = \{ e_1, ..., e_m, v_{m+1}, ..., v_r, w_{m+1}, ..., w_s \}$$

engendrará el subespacio suma V + W. Entonces, de este conjunto generador se podrá deducir una familia libre que engendra el subespacio.
Vamos a demostrar que todos los vectores de S son libres, y por consiguiente, S es la base del subespacio suma. Supongamos que exista alguna combinación lineal, de coeficientes no todos nulos, entre los vectores de S y probemos que ésto no es posible:

$$\gamma_1 \cdot e_1 + ..., + \gamma_m \cdot e_m + \alpha_{m+1} \cdot v_{m+1} + ..., + \alpha_r \cdot v_r + ..., + \beta_{m+1} \cdot w_{m+1} + ..., + \beta_s \cdot w_s = 0$$

También se puede escribir como:

$$-\alpha_{m+1} \cdot v_{m+1} - ... - \alpha_r \cdot v_r = \gamma_1 \cdot e_1 + ... + \gamma_m \cdot e_m + \beta_{m+1} \cdot w_{m+1} + ... + \beta_s \cdot w_s$$

El vector del primer miembro de la igualdad es un vector de V por ser combinación lineal de vectores de la base B_v y no puede pertenecer a la intersección (puesto que, por definición: $v_{m+1}, ..., v_r \notin V \cap W$), salvo que la combinación lineal de las v sea nula y sea, por tanto, el vector 0, que pertenece a todos los subespacios y, por consiguiente, a $V \cap W$. (1)
El vector del segundo miembro es suma de un vector del subespacio intersección $u = \gamma_1 \cdot e_1 + ..., + \gamma_m \cdot e_m \in V \cap W$ (y por definición de subespacio intersección $u \in V \wedge u \in W$), y de un vector que pertenece sólo a W: $\beta_{m+1} \cdot W_{m+1} + ... + \beta_s \cdot W_s$ (por ser $W_{m+1}, ..., W_s \in W - (V \cap W)$). Luego, definitivamente, en el segundo miembro hay un vector que pertenece a W.
Entonces, como el primer miembro es igual al segundo, tenemos un vector que pertenece a V (1.^{er} miembro) y que pertenece a W (2.° miembro). Es decir, un vector que pertenece a $V \cap W$, que por lo dicho en (1), sólo puede ser el vector nulo.
Luego todos los coeficientes serán nulos:

$$\gamma_1 = ... = \gamma_m = \alpha_{m+1} = ... = \alpha_r = \beta_{m+1} = \cdots = \beta_s = 0$$

Es decir, la única combinación lineal existente de los vectores de S es aquella en que los escalares son todos nulos, por tanto, es un sistema libre y base de V + W.
La dimensión de V + W será el número de vectores de la base S del mismo. Es decir:

$$\dim (V + W) = m + (r - m) + (s - m) = r + s - m$$

y como r, s y m son las dimensiones de V, W y $V \cap W$, queda: $\dim (V + W) = \dim V + \dim W - \dim (V \cap W)$,

como queríamos demostrar.

7-10 SUMA DIRECTA

Consideremos como en los casos anteriores dos subespacios V y W de un espacio vectorial E de n dimensiones. El subespacio suma de ambos será:

$$L = V + W = \{z = x + y; \forall\, x \in V \wedge \forall\, y \in W\}$$

Ahora bien, el hecho de que cada vector del subespacio suma se haya obtenido sumando uno de V y otro de W, no significa recíprocamente que dado un vector $z \in L$, existan dos elementos únicos $x_1 \in V \wedge y_1 \in W$ tales que $z = x_1 + y_1$. En principio podrían existir otros dos vectores $x_2 \in V \wedge y_2 \in W$ tales que $z = x_2 + y_2$

Si esto sucede, igualando ambas expresiones

$$x_1 + y_1 = x_2 + y_2$$

pasando x_2 al primer miembro e y_1, al segundo queda:

$$x_1 - x_2 = y_2 - y_1 \qquad (1)$$

y por ser $x_1, x_2 \in V \Rightarrow x_1 - x_2 \in V$

y también: $y_1, y_2 \in W \Rightarrow y_2 - y_1 \in W$

luego el vector de (1) es del subespacio intersección $V \cap W$

$$x_1 - x_2 = y_2 - y_1 \in V \cap W$$

Entonces, es evidente que dado un vector $z \in L$, su descomposición como suma $z = x_1 + y_1$ de un $x_1 \in V$ y otro $y_1 \in W$ no es única si $V \cap W \neq 0$, puesto que tomando un vector cualquiera $v \neq 0$ $v \in V \cap W$ se tiene:

$$z = (x_1 + v) + (y_1 - v)$$

y ahora, el vector $x_1 + v = x_2$ es un vector distinto de x_1, siendo $x_2 \in V$ (por pertenecer v a la intersección), y el $y_1 + v = y_2$ es otro vector distinto de y_1 y además $y_2 \in W$.
Podemos entonces enunciar el siguiente teorema:

Teorema 15.—La condición necesaria y suficiente para que un vector $z \in V + W$ se pueda descomponer de una forma única como suma de un $x_1 \in W$ y otro $y_1 \in W$ es que $V \cap W = \{0\}$.
Es condición necesaria. En efecto, $\forall\ v \in V \cap W$ se cumplirá

$$z = x_1 + y_1 = (x_1 + v) + (y_1 - v)$$

y como la descomposición es única, se ha de cumplir:

$$\left.\begin{array}{l} x_1 + v = x_1 \\ y_1 - v = y_1 \end{array}\right\} \Rightarrow v = 0$$

y por lo tanto $V \cap W = \{0\}$
También es condición suficiente. Supongamos, para demostrarlo, que hubiese dos expresiones distintas:

$$z = x_1 + y_1 = x_2 + y_2 \qquad \text{con } x_1, x_2 \in V \quad x_1 \neq x_2 \ \text{ y } \ y_1, y_2 \in W \qquad \text{con } y_1 \neq y_2$$

Entonces:

$$x_1 - x_2 = y_2 - y_1 \quad \in V \cap W$$

y como por hipótesis $V \cap W = \{0\}$

$$\begin{array}{l} x_1 - x_2 = 0 \ \Rightarrow \ x_1 = x_2 \\ y_2 - y_1 = 0 \ \Rightarrow \ y_1 = y_2 \end{array}$$

que demostraría la condición suficiente por reducción al absurdo por contradicción con la hipótesis de la misma.

Conclusión: Cuando dos subespacios V y W cumplen que $V \cap W = \{0\}$ se dice que son *independientes*, y entonces la suma de ambos se llama *suma directa*, y se representa por $V \oplus W$.

7-11 SUBESPACIOS SUPLEMENTARIOS

Dos subespacios V y W de un espacio vectorial E de n dimensiones, se dice que son suplementarios cuando cumplen las dos condiciones siguientes:

1) Son independientes: $V \cap W = \{0\}$
2) Su suma es E: $V + W = E$

Es decir, *la suma directa* de V y W es E

$$V \oplus W = E$$

En este caso, como se desprende ya intuitivamente, todos los vectores de E que no están en V lo estarán en W y recíprocamente.
En cuanto a la dimensión de los mismos, podemos aplicar el teorema 14 de la dimensión:

$$\dim (V \oplus W) + \dim (V \cap W) = \dim V + \dim W$$

En virtud de la condición 1.ª, $\dim (V \cap W) = 0$, y en virtud de la 2.ª, $\dim (V \oplus W) = n$. Luego:

$$\boxed{\dim V + \dim W = n}$$

Entonces, dada una base del espacio vectorial E: $B = \{e_1, \ldots\ldots e_n\}$ los vectores de la misma habrán de ser o bien de V o de W. Si suponemos que V tiene dimensión $\dim V = n_1$, entonces $\dim W = n - n_1$, y habrá n_1 vectores de B que pertenecerán a V y constituirán una base de V, y los demás n-n_1 formarán una base de W.
Inversamente, dadas dos bases $B_v = \{v_1, \ldots\ldots v_{n1}\}$ y $B_w = \{w_1, \ldots\ldots w_{n-n1}$ respectivamente, el conjunto de vectores $v_1, \ldots\ldots, v_{n1}, w_1, \ldots\ldots, w_{n-n1}\}$ es una base del espacio vectorial E, como se ve fácilmente a partir del teorema 13 y de la condición primera de subespacios suplementarios.

EJEMPLO:

En K^3 sobre K, el subespacio V engendrado por $\{(1, 0, 0), (0, 1, 0)\}$ y el W engendrado por $\{(0, 0, 1)\}$ son suplementarios, pues cumplen las dos condiciones:

1.ª Son independientes: En efecto, supongamos que no, que $\exists z \in V \cap W$

a) Por ser $z \in V$ $z = \alpha \cdot (1, 0, 0) + \beta \cdot (0, 1, 0) = (\alpha, \beta, 0)$

b) Por ser $z \in W$ $z = \gamma \cdot (0, 0, 1) = (0, 0, \gamma)$

Igualando:

$$(\alpha, \beta, 0) = (0, 0, \gamma) \Rightarrow \alpha = \beta = \gamma = 0$$

o sea $z = (0, 0, 0)$

por tanto $V \cap W = \{0\}$

2.ª Su suma es K^3.

En efecto $\forall_v \in K^3$
$v = (\alpha, \beta, \gamma)$, sabemos que
$v = (\alpha, \beta, 0) + (0, 0, \gamma)$, y ahora
$(\alpha, \beta, 0) = \alpha\,(1, 0, 0) + \beta\,(0, 1, 0) \in V$
$(0, 0, \gamma) = \gamma\,(0, 0, 1) \in W$

Luego:

$$K^3 = V \oplus W$$

se tiene también que $(1, 0, 0)\ (0, 1, 0)\ (0, 0, 1)$ es una base de K^3 como ya sabíamos

---

7-12 ECUACIONES DE UN SUBESPACIO

Un subespacio vectorial podemos, en general, caracterizarlo dando un sistema de generadores del mismo o, en particular, una base. Sin embargo, podemos utilizar otros modos para representarlo que quizá serán particularmente útiles en el estudio de la geometría.

EJEMPLO:

Consideremos el subespacio V de R^4 que hemos visto anteriormente, engendrado por $\{v_1, v_2, v_3\}$

$$v_1 = (1, 1, -1, 0)$$
$$v_2 = (0, 1, 0, 1)$$
$$v_3 = (-1, 0, 0, 1)$$

Entonces, todo vector $x = (\delta_1, \delta_2, \delta_3, \delta_4) \in V$ será combinación lineal de ellos:

$$x = \alpha \cdot v_1 + \beta \cdot v_2 + \gamma \cdot v_3$$

es decir:

$$(\delta_1, \delta_2, \delta_3, \delta_4) = \alpha \cdot (1, 1, -1, 0) + \beta \cdot (0, 1, 0, 1) + \gamma \cdot (-1, 0, 0, 1)$$

y operando $(\delta_1, \delta_2, \delta_3, \delta_4) = (\alpha - \gamma, \alpha + \beta, -\alpha, \beta + \gamma)$

luego:

$$\left.\begin{array}{ll} (1) & \delta_1 = \alpha - \gamma \\ (2) & \delta_2 = \alpha + \beta \\ (3) & \delta_3 = -\alpha \\ (4) & \delta_4 = \beta + \gamma \end{array}\right\}$$

hemos obtenido unas ecuaciones que nos expresan los escalares $\delta_1, \delta_2, \delta_3, \delta_4$ que definen el vector x de V y que son también sus coordenadas en la base canónica, en función de tres parámetros α, β, γ. Estas ecuaciones se llaman *ecuaciones paramétricas* del subespacio V.

De estas ecuaciones, se pueden eliminar los parámetros.

En (3) tenemos: $\alpha = -\delta_3$. Sustituyendo en (1), (2) y (4):

$$\begin{array}{ll} (1') & \delta_1 = -\delta_3 - \gamma \\ (2') & \delta_2 = -\delta_3 + \beta \\ (3') & \delta_4 = \beta + \gamma \end{array}$$

Es decir:

$$\begin{array}{l} \gamma = -\delta_1 - \delta_3 \\ \beta = \delta_2 + \delta_3 \end{array}$$

Sustituyendo en (4') queda:

$$\delta_4 = \delta_2 + \delta_3 - \delta_1 - \delta_3$$

que finalmente da:

$$\boxed{\delta_1 - \delta_2 + \delta_4 = 0}$$

que es una ecuación que relaciona las coordenadas en la base canónica de un vector x del subespacio V entre sí. Estas ecuaciones se llaman *ecuaciones no paramétricas* del subespacio.

Un subespacio vectorial puede venir caracterizado, pues,

(1) Por una base del mismo.
(2) Por sus ecuaciones paramétricas.
(3) Por sus ecuaciones no paramétricas.

EJEMPLO:

Hallemos el subespacio V de R^4 que tiene por ecuaciones paramétricas

$$\left.\begin{array}{l}\delta_1 = 0\\ \delta_2 = \alpha + 2\beta\\ \delta_3 = \alpha - \beta\\ \delta_4 = 2\beta\end{array}\right\}$$

$\forall x \in V,\ x = \delta_1 \cdot e_1 + \delta_2 \cdot e_2 + \delta_3 \cdot e_3 + \delta_4 \cdot e_4$, siendo $\{e_1, e_2, e_3, e_4\}$ la base canónica.

Luego:

$x = 0 \cdot e_1 + (\alpha + 2\beta) \cdot e_2 + (\alpha - \beta) \cdot e_3 + 2\beta \cdot e_4$

es decir:

$x = \alpha \cdot e_2 + 2\beta \cdot e_2 + \alpha \cdot e_3 - \beta \cdot e_3 + 2\beta \cdot e_4$

O sea:

$x = \alpha \cdot (e_2 + e_3) + \beta \cdot (2e_2 - e_3 + 2e_4)$

Sustituyendo los vectores de la base por su expresión en R^4

$x = \alpha \cdot [(0,1,0,0) + (0,0,1,0)] + \beta \cdot [2 \cdot (0,1,0,0) - (0,0,1,0) + 2 \cdot (0,0,0,1)]$

Sumando los vectores

$x = \alpha \cdot (0,1,1,0) + \beta \cdot (0,2,-1,2)$

donde α y β son dos elementos de R.

Todo vector, pues, $x \in V$ puede escribirse como combinación lineal de los dos vectores (0, 1, 1, 0) y (0, 2, −1, 2) que además son linealmente independientes. Luego esto significa que (0, 1, 1, 0) y (0, 2, −1, 2) son una base del subespacio vectorial V.

Hemos conseguido, pues, obtener la base dadas las ecuaciones paramétricas.

---

4) Vamos a hallar ahora el subespacio W de R^4 dado por las siguientes *ecuaciones no paramétricas:*

$$\left.\begin{aligned} \delta_1 + 2\,\delta_2 - \delta_3 &= 0 \\ \delta_1 - \delta_2 &= 0 \end{aligned}\right\}$$

Entonces todo sector $x \in W$ tiene unas coordenadas en la base canónica $(\delta_1, \delta_2, \delta_3, \delta_4)$. Es decir:

$$x = \delta_1 \cdot e_1 + \delta_2 \cdot e_2 + \delta_3 \cdot e_3 + \delta_4 \cdot e_4$$

Sin embargo, las cuatro coordenadas no son independientes entre sí, sino que verifican las dos ecuaciones no paramétricas del subespacio. Despejemos, pues, de aquellas ecuaciones dos coordenadas en función de las otras dos:

De la segunda ecuación: $\delta_1 = \delta_2$

y sustituyendo en la primera: $\delta_3 = 2\,\delta_2$

Llevando esto a la expresión de *x:*

$x = \delta_2 \cdot e_1 + \delta_2 \cdot e_2 + 3\,\delta_2 \cdot e_3 + \delta_4 \cdot e_4$

$x = \delta_2\,(e_1 + e_2 + 3\,e_3) + \delta_4 \cdot e_4$

es decir:

$x = \delta_2\,[(1,0,0,0) + (0,1,0,0) + 3\,(0,0,1,0)] + \delta_4 \cdot (0,0,0,1)$

$x = \delta_2\,(1,1,3,0) + \delta_4 \cdot (0,0,0,1)$

Como δ_2 y δ_4 son dos elementos cualesquiera de R, esto significa que (1, 1, 3, 0) y (0, 0, 0, 1) son una base de W y dim W = *2.*

Hemos pasado, pues, de la representación del subespacio por sus ecuaciones no paramétricas, a su representación dando base del mismo.

TEMA 8 APLICACIONES LINEALES

8-1 APLICACION LINEAL

Definición: Sean dos espacios vectoriales E y F definidos sobre el mismo cuerpo conmutativo K. Una aplicación $f : E \to F$ entre estos dos espacios vectoriales se dice que es lineal, o que es un homomorfismo entre ellos, si cumple las condiciones siguientes:

I) $\forall\, x,y \in E \quad f(x+y) = f(x) + f(y)$

II) $\forall\, \alpha \in K,\ \forall\, x \in E \quad f(\alpha \cdot x) = \alpha \cdot f(x)$

Estas dos condiciones pueden ser combinadas, obteniendo una sola del siguiente modo: Una aplicación $f : E \to F$ es lineal si y solo sí:

III) $\forall\, \alpha, \beta \in K, \forall\, x,y \in E \quad f(\alpha \cdot x + \beta \cdot y) = \alpha \cdot f(x) + \beta \cdot f(y)$

Veamos que en efecto esta condición es equivalente a las dos anteriores.

$\Rightarrow$ Si la aplicación cumple I) y II), entonces tenemos: $\forall\, \alpha$, $\beta \in K$, $\forall\, x,y \in E$

en virtud de I): $f(\alpha \cdot x + \beta \cdot y) = f(\alpha \cdot x) + f(\beta \cdot y)$
y finalmente, por II): $f(\alpha \cdot x + \beta \cdot y) = \alpha \cdot f(x) + \beta \cdot f(y)$

$\Leftarrow$ Si la aplicación cumple la condición III), entonces, tomando $\alpha = \beta = 1$

$f(x + y) = f(x) + f(y)$ que es la condición I)

y ahora, tomando $\beta = 0$

$f(\alpha \cdot x + 0 \cdot y) = f(\alpha \cdot x) = \alpha \cdot f(x)$ que es la condición II)

luego las condiciones I) y II) son equivalentes a la III)

EJEMPLOS:

1) Dado un espacio vectorial cualquiera E definido sobre el cuerpo K, definimos una aplicación idéntica

$$f : E \rightarrow E$$
$$\forall x \in E, \; f(x) = x$$

Esta aplicación es lineal. En efecto:

$$\forall \alpha, \beta \in K, \quad \forall x, y \in E$$

$$f(\alpha \cdot x + \beta \cdot y) = \alpha \cdot x + \beta \cdot y$$

por definición. Pero $x = f(x)$ e $y = f(y)$; por tanto:

$$f(\alpha \cdot x + \beta \cdot y) = \alpha \cdot f(x) + \beta \cdot f(y)$$

2) Podemos generalizar este ejemplo, tomando un escalar $\delta \in K$, fijo cualquiera, y definir la aplicación $f : E \rightarrow E$

$$\forall x \in E \quad f(x) = \delta \cdot x$$

Esta aplicación es también lineal, puesto que

$$\forall \alpha, \beta \in K, \forall x, y \in E$$
$$f(\alpha \cdot x + \beta \cdot y) = \delta \cdot (\alpha \cdot x + \beta \cdot y) = \delta \cdot (\alpha \cdot x) + \delta \cdot (\beta \cdot y)$$

como δ, α, β son elementos de K, que es conmutativo:

$$f(\alpha \cdot x + \beta \cdot y) = \alpha \cdot (\delta \cdot x) + \beta \cdot (\delta \cdot y)$$

y teniendo en cuenta que $\delta \cdot x = f(x)$ y $\delta \cdot y = f(y)$ queda

$$f(\alpha \cdot x + \beta \cdot y) = \alpha \cdot f(x) + \beta \cdot f(y)$$

3) Considerando los espacios vectoriales K^n sobre K y K sobre K, podemos definir la aplicación

$$f : K^n \to K$$

como:

$$\forall (\alpha_1, ..., \alpha_n) \in K^n \quad f(\alpha_1, ..., \alpha_n) = \alpha_1$$

Veamos que es lineal.

$$\forall \gamma, \delta \in K, \quad \forall (\alpha_1, ..., \alpha_n), (\beta_1, ..., \beta_n) \in K^n$$

tendremos

$$f(\gamma \cdot (\alpha_1, ..., \alpha_n) + \delta \cdot (\beta_1, ..., \beta_n)) = f(\gamma \alpha_1 + \delta \beta_1, ..., \gamma \alpha_n + \delta \beta_n)$$

y por definición de la aplicación f:

$$f(\gamma \alpha_1 + \delta \beta_1, ..., \gamma \alpha_n + \delta \beta_n) = \gamma \cdot \alpha_1 + \delta \beta_1$$

pero $\quad f(\alpha_1, ..., \alpha_n) = \alpha_1 \quad$ y $\quad f(\beta_1, ..., \beta_n) = \beta_1$

Luego queda que la imagen final es:

$$\gamma \cdot f(\alpha_1, ..., \alpha_n) + \delta \cdot f(\beta_1, ..., \beta_n)$$

es decir, es lineal.

Consecuencias:

a) Sea una familia finita de vectores de E, $\{x_1, ..., x_p\}$. Sea también $v = \alpha_1 \cdot x_1 +, ..., + \alpha_p \cdot x_p$ una combinación lineal cualquiera de estos vectores. La imagen por medio de la aplicación lineal $f : E \to F$ será:

$$f(v) = \alpha_1 \cdot f(x_1) +, ..., + \alpha_p \cdot f(x_p) \qquad (1)$$

lo cual es evidente, pues se deduce de aplicar p veces la condición III) de linealidad de f.
En adelante, para las combinaciones lineales de una familia finita de vectores, utilizaremos a menudo el signo sumatorio

$$\alpha_1 \cdot x_1 +, ..., + \alpha_p \cdot x_p = \sum_{i=1}^{p} \alpha_i \cdot x_i$$

quedando de este modo la consecuencia a) como:

$$f\left(\sum_{i=1}^{p} \alpha_i \cdot x_i\right) = \sum_{i=1}^{p} \alpha_i \cdot f(x_i) \qquad (2)$$

b) La imagen del vector nulo de E es el vector nulo de F

$$f(0) = 0$$

que es evidente, puesto que f es un homomormismo entre los grupos (E, +) y (F, +) (Condición I) y ya quedó probado en teoría de grupos.

c) La imagen del simétrico de un vector $x \in E$, es igual al simétrico de la imagen de dicho vector.

$$f(-x) = -f(x)$$

que no es necesario demostrar por la misma razón que b)

d) La imagen de una familia ligada de vectores $\{x_1, ..., x_p\}$ de E es otra familia ligada de vectores de F.
En efecto, si la familia es ligada $\exists\ \alpha_1, ..., \alpha_p \in K$ no todos nulos, tales que

$$\alpha_1 \cdot x_1 +, ..., + \alpha_p \cdot x_p = 0$$

tomando la imagen por f tendremos:

$$f(\alpha_1 \cdot x_1 +, ..., + \alpha_p \cdot x_p) = f(0)$$

pero teniendo en cuenta las consecuencias a) y b), queda:

$$\alpha_1 \cdot f(x_1) +, ..., + \alpha_p \cdot f(x_p) = 0$$

con $\alpha_1, ..., \alpha_p$ no todos nulos; luego la familia $f(x_1), ..., f(x_p)$ *de F es ligada.*

e) Si $\{x_1, ..., x_p\}$ es una familia de vectores del espacio E y la familia constituida por sus imágenes $\{f(x_1), ..., f(x_p)\} \subset$ F es libre, entonces la familia $\{x_1, ..., x_p\}$ es libre también.
En efecto: esta proposición está demostrada, puesto que es la forma "tollendo tollens" de la proposición d). Veamos como ejercicio que es así.

Si las proposiciones A y B son:
A = "El sistema $\{x_1, ..., x_p\}$ es ligado"
B = "El sistema $\{f(x_1), ..., f(x_p)\}$ es ligado"

la condición d) se anuncia, pues, como: A → B. Entonces, por "tollendo tollens" se cumple también $\neg$ B → $\neg$ A

Pero:

$\neg$ B = "El sistema $\{f(x_1), ..., f(x_p)\}$ es libre"
$\neg$ A = "El sistema $\{x_1, ..., x_p\}$ es libre"

Queda, pues, visto el enunciado.

8-2 EXISTENCIA Y UNICIDAD DE LA APLICACION

En general, para definir unívocamente una aplicación entre dos conjuntos E y F, es necesario dar las imágenes de cada elemento de E es decir dar el grafo de dicha aplicación. Sin embargo, cuando estos dos conjuntos, entre los que está definida la aplicación, son dos espacios vectoriales y la aplicación es lineal, no es necesario dar las imágenes de todos los vectores de E, sino que basta con dar las imágenes de los vectores de una base B del mismo, como demostraremos a continuación.

Teorema 1.—Sea $B = \{e_1, ..., e_n\}$ una base del espacio vectorial E, y sea $\{u_1, ..., u_n\}$ una familia cualquiera con *n* vectores de F. Existe una y una sola aplicación lineal $f : E \to F$, tal que:

$$f(e_1) = u_1, ..., f(e_n) = u_n \qquad (5)$$

Demostremos primero que existe, al menos, una aplicación definida así y que esta es lineal.
En efecto, todo $x \in E$ tiene unas coordenadas únicas $\alpha_1, ..., \alpha_n \in K$, con los que se expresa como combinación lineal de B.

$$x = \alpha_1 \cdot e_1 +, ..., + \alpha_n \cdot e_n$$

La imagen de *x*, $f(x)$ la definimos del siguiente modo:

$$f(x) = \alpha_1 \cdot u_1 +, ..., + \alpha_n \cdot u_n \qquad (6)$$

con lo que evidentemente todos los $x \in E$ tienen imagen en F, ya que una combinación lineal de vectores de F es otro vector de F. Y además la imagen es única, puesto que una combinación lineal determinada de *n* vectores define un solo vector.
Y es evidente que esta aplicación $f : E \to F$ así definida, es lineal.

Demostremos, en segundo lugar, que la aplicación lineal $f : E \to F$, definida de este modo, es única. En efecto, supongamos que existe otra aplicación lineal $g : E \to F$ definida como se ha expresado en (5)

$$g(e_1) = u_1, ..., g(e_n) = u_n$$

a cada vector $x \in E$

$$x = \alpha_1 \cdot e_1 +, ..., + \alpha_n \cdot e_n$$

le hace corresponder en virtud de la linealidad

$$g(x) = \alpha_1 \cdot g(e_1) +, ..., + \alpha_n \cdot g(e_n)$$

es decir:

$$g(x) = \alpha_1 \cdot u_1 +, \ldots, + \alpha_n \cdot u_n$$

y comparando este resultado con (6),

$$f(x) = g(x) \quad \forall\, x \in E \qquad (7)$$

Tenemos, pues, dos aplicaciones con el mismo conjunto de partida E, con el mismo conjunto de llegada F y con el mismo grafo como indica (7), luego son iguales.

$$f = g$$

Hemos demostrado, pues, que para definir unívocamente una aplicación lineal entre dos espacios vectoriales, basta con conocer solamente las imágenes de los vectores de una base.

EJEMPLO:

Tomando el ejemplo anterior $f: K^n \to K$, podemos definir la aplicación dando las imágenes de la base canónica de K^n.

$$\begin{aligned} f(e_1) &= f(1, 0, 0, \ldots, 0) = 1 \\ f(e_2) &= f(0, 1, 0, \ldots, 0) = 0 \\ &\vdots \\ f(e_n) &= f(0, 0, 0, \ldots, 1) = 0 \end{aligned}$$

Entonces:

$$\forall\, (\alpha_1, \alpha_2, \ldots, \alpha_n) \in K^n : (\alpha_1, \ldots, \alpha_n) = \alpha_1 \cdot e_1 +, \ldots, + \alpha_n \cdot e_n$$

Tomando la imagen

$$f(\alpha_1, \ldots, \alpha_n) = \alpha_1 \cdot f(e_1) +, \ldots, + \alpha_n \cdot f(e_n)$$

Es decir:

$$f(\alpha_1, \ldots, \alpha_n) = \alpha_1 \cdot 1 + \alpha_2 \cdot 0 +, \ldots, + \alpha_n \cdot 0 = \alpha_1$$

8-3 IMAGEN DE UN SUBESPACIO

Consideremos los espacios vectoriales E y F, y sea V un subespacio vectorial de E. La imagen de este subespacio en tanto que subconjunto de E por la aplicación lineal $f : E \to F$, será el conjunto de las imágenes de los vectores de V:

$$f(V) = \{ y,\, y \in F \mid \exists x,\, x \in V \wedge y = f(x) \}$$

Ahora bien, $f(V)$ va a cumplir unas condiciones peculiares por el hecho de que V es subespacio y f es lineal, como demuestra el teorema siguiente:

Teorema 2.—La imagen de un subespacio V de E por la aplicación lineal *f*, es un subespacio vectorial de F.
En efecto:

$$\forall y_1, y_2 \in f(V) \quad \exists x_1, x_2 \in V \mid y_1 = f(x_1) \wedge y_2 = f(x_2)$$

Entonces, si multiplicamos estas igualdades por dos escalares cualesquiera y las sumamos:

$$\alpha_1 \cdot y_1 + \alpha_2 \cdot y_2 = \alpha_1 \cdot f(x_1) + \alpha_2 \cdot f(x_2)$$

pero f es lineal, luego:

$$\alpha_1\, y_1 + \alpha_2 \cdot y_2 = f(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2)$$

como V es un subespacio, $\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 \in V$, y por tanto, $f(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) \in f(V)$

luego:

$$\alpha_1 \cdot y_1 + \alpha_2 \cdot y_2 \in f(V)$$

con lo que queda demostrado que $f(V)$ es subespacio de F.

Subespacio imagen.—Se llama así y se representa por $I_m(f)$ a la imagen $f(E)$ de todo el espacio vectorial. Según hemos visto en el teorema 2, será un subespacio de F. Para caracterizarlo, pues, podemos utilizar uno de los tres medios que se expusieron en el tema de espacios vectoriales; es decir: sus ecuaciones paramétricas, no paramétricas, o dar sencillamente una familia de generadores del mismo. Dadas las ecuaciones paramétricas o las no paramétricas, inmediatamente está determinada una familia de generadores de f (E); sin embargo, debemos estudiar como se determina una de estas familias directamente.

Teorema 3.—Sea V un subespacio vectorial de E, y sea M una familia de generadores de V. La imagen de esta familia f (M) por la aplicación lineal $f : E \rightarrow F$ es una familia de generadores del subespacio $f(V) \subset F$.

En efecto: sea $M = \{ v_1, \ldots, v_p \}$ y por tanto

$$f(M) = \{ f(v_1), \ldots, f(v_p) \}$$

Por definición de f (V)

$$\forall\, y \in f(V) \quad \exists\, x \in V \mid y = f(x)$$

pero:

$$x = \alpha_1 \cdot v_1 +, \ldots, + \alpha_p \cdot v_p \quad \text{con} \quad \alpha_1, \ldots, \alpha_p \in K$$

luego:

$$y = f(x) = f(\alpha_1 \cdot v_1 +, \ldots, + \alpha_p \cdot v_p)$$

por ser f lineal:

$$y = \alpha_1 \cdot f(v_1) +, \ldots, + \alpha_p \cdot f(v_p)$$

luego, como queríamos demostrar, todo vector y del subespacio f (V) se puede expresar como combinación lineal de la familia f (M); es decir, f (M) engendra f (V).

Consecuencia.—Si B es una base del espacio vectorial E, f (B) será una familia de generadores del subespacio imagen $I_m\ (f)$.

Con esto hemos resuelto el problema que planteábamos más arriba, porque para tener una familia de generadores del subespacio imagen, basta con tomar la formada por las imágenes de los vectores de una base de E.

EJEMPLOS:

Consideremos la aplicación $f: K^4 \to K^3$, definida del siguiente modo:

$$\forall\ (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in K^4 \qquad f(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\alpha_1, 0, \alpha_3)$$

y vamos a determinar el subespacio imagen.
Tomemos en primer lugar una base de K^4, por ejemplo la base canónica $B = \{ e_1, e_2, e_3, e_4 \}$

$$e_1 = (1, 0, 0, 0) \qquad e_3 = (0, 0, 1, 0)$$
$$e_2 = (0, 1, 0, 0) \qquad e_4 = (0, 0, 0, 1)$$

Las imágenes de estos vectores serán un sistema generador de $f(K^4)$

$$f(e_1) = (1, 0, 0)$$
$$f(e_2) = (0, 0, 0)$$
$$f(e_3) = (0, 0, 1)$$
$$f(e_4) = (0, 0, 0)$$

luego:

$$f(B) = \{ (1, 0, 0), (0, 0, 0), (0, 0, 1) \}$$

de $f(B)$ deducimos inmediatamente una base del subespacio imagen eliminando el vector $(0, 0, 0)$ que es linealmente dependiente.
La base B' del subespacio imagen es, pues:

$$B' = \{ (1, 0, 0), (0, 0, 1) \}$$

podemos hallar sus ecuaciones paramétricas:

$$\forall\ (\alpha_1, \alpha_2, \alpha_3) \in f(K^4)$$

Por definición de base:

$$(\alpha_1, \alpha_2, \alpha_3) = \delta\ (1, 0, 0) + \gamma \cdot (0, 0, 1)$$

de donde:

$$\alpha_1 = \delta$$
$$\alpha_2 = 0$$
$$\alpha_3 = \gamma$$

ecuaciones paramétricas del subespacio imagen. Las ecuaciones no paramétricas, que las obtenemos eliminando los parámetros, son:

$$\alpha_2 = 0$$

8-4 IMAGEN RECIPROCA DE UN SUBESPACIO

Sea $f : E \to F$ una aplicación lineal entre los espacios E y F, y sea W un subespacio vectorial de F. Puesto que $W \subset F$, se puede hablar de la imagen recíproca $\overset{-1}{f}(W)$ como conjunto de elementos de E que tienen su imagen por f en W.

$$\overset{-1}{f}(W) = \{ x, x \in E \mid f(x) \in W \}$$

A este subconjunto de E, el hecho de ser f lineal y E y F espacios vectoriales le confieren estructura de subespacio vectorial, como demostraremos.

Teorema 4.—La imagen recíproca $\overset{-1}{f}(W)$ de un subespacio vectorial de F por una aplicación lineal, es otro subespacio vectorial.
En efecto:

$$\forall\, x_1, x_2 \in \overset{-1}{f}(W) \;\; \exists\, y_1, y_2 \in W \mid y_1 = f(x_1) \wedge y_2 = f(x_2)$$

Para ver si $\overset{-1}{f}(W)$ es un subespacio, hay que demostrar que $\forall\, \alpha_1, \alpha_2 \in K$, $\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 \in \overset{-1}{f}(W)$, es decir, que su imagen por f pertenezca a W. Hablemos, pues, de su imagen:

$$f(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) = \alpha_1 \cdot f(x_1) + \alpha_2 \cdot f(x_2)$$

Ahora bien, teniendo en cuenta que f es lineal y que W es un subespacio, resulta que toda combinación lineal de dos elementos es otro elemento de él; luego, $\alpha_1 \cdot f(x_1) + \alpha_2 \cdot f(x_2) \in W$. Por tanto:

$$f(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) \in W$$

es decir, que queda demostrado que $\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 \in {}^{-1}f(W)$, y de ahí que ${}^{-1}f(W)$ es un subespacio.

8-5 NUCLEO DE UNA APLICACION LINEAL

Llamamos núcleo de f y lo representaremos por Ker (f), a la imagen recíproca del vector nulo de F.

$$\text{Ker}\,(f) = \{x, x \in E \mid f(x) = 0\}$$

Puesto que el $\{0\}$ es un subespacio de F (subespacio nulo, trivial), el núcleo es también un subespacio de E.
En el núcleo, por ser un subespacio, podemos también determinar una base (o caracterizarlo por sus ecuaciones paramétricas o no paramétricas).

Teorema 5.—Sean E y F dos espacios vectoriales de dimensión finita sobre el mismo cuerpo K y sea $f : E \to F$ una aplicación lineal entre ellos. Entonces:

$$\dim \text{Ker}\,(f) + \dim I_m\,(f) = \dim E$$

En efecto: supongamos que dim (E) = n y que dim Ker $(f) = s$.
Tomemos pues una base $B_1 = \{e_1, \ldots, e_s\}$ del núcleo. Si la ampliamos con n-s vectores linealmente independientes entre ellos y con estos *"s"*, conseguimos una base B del espacio E. Sea esta:

$$B = \{e_1, e_2, \ldots, e_s, e_{s+1}, \ldots, e_n\}$$

Hallemos la imagen de B y con ello habremos obtenido una familia de generadores de $I_m\,(f)$.

$$f(B) = \{f(e_1), \ldots, f(e_s), f(e_{s+1}), \ldots, f(e_n)\}$$

Por ser $e_1, \ldots, e_s$ elementos del núcleo, se cumple:

$$f(e_1) = f(e_2) = \ldots = f(e_s) = 0$$

luego queda, eliminando el 0 por ser linealmente dependiente:

$$S = \{ f(e_{s+1}), \ldots, f(e_n) \}$$

Demostramos que esta familia de generadores de I_m *(f)* es una familia libre, con lo cual será base.
En efecto; si existe alguna combinación lineal nula:

$$\alpha_{s+1} \cdot f(e_{s+1}) +, \ldots, + \alpha_n \cdot f(e_n) = 0$$

como *f* es lineal:

$$f(\alpha_{s+1} \cdot e_{s+1} +, \ldots, + \alpha_n \cdot e_n) = 0$$

lo cual significa que:

$$\alpha_{s+1} \cdot e_{s+1} +, \ldots, + \alpha_n \cdot e_n \in \mathrm{Ker}\,(f)$$

si esto es un vector del núcleo de *f*, se podrá escribir como combinación lineal de B′. Sea esta:

$$\alpha_{s+1} \cdot e_{s+1} +, \ldots, + \alpha_n \cdot e_n = \alpha_1 \cdot e_1 +, \ldots, + \alpha_s \cdot e_s$$

siendo $\alpha_1, \ldots, \alpha_n$ elementos de K.

como $\{ e_1, \ldots, e_s, \ldots, e_n \}$ es una base, es una familia libre, y esto implica, por tanto, que todos los escalares han de ser nulos.

$$\alpha_1 = \ldots = \alpha_s = \ldots = \alpha_n = 0$$

Teniendo en cuenta esto y la ecuación (8), queda finalmente que *f* (S) es libre y por tanto base de I_m *(f)*.
Luego: dim I_m *(f)* = n-s = dim E − dim Ker *(f)*
O sea: dim Ker *(f)* + dim I_m (f) = dim E

c.q.d.

EJEMPLOS:

Hallemos el núcleo de la aplicación lineal $f: K^4 \to K^3$ que hemos considerado en otro ejemplo anteriormente:

$$\forall (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in K^4 \quad f(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\alpha_1, 0, \alpha_3)$$

El Ker *(f)* será, pues, el conjunto de elementos $x \in K^4 \quad x = (\beta_1, \beta_2, \beta_3, \beta_4)$, tales que $f(x) = (0, 0, 0) = (\beta_1, 0, \beta_3)$

luego:

$$\begin{aligned} \beta_1 &= 0 \\ \beta_3 &= 0 \end{aligned}$$

Por tanto:

$$\text{Ker } (f) = \{ (0, \beta_2, 0, \beta_4) \ \forall \beta_2, \beta_4 \in K \}$$

Hallemos una base de Ker *(f)*

$$\forall (0, \beta_2, 0, \beta_4) \in \text{Ker } (f)$$

$$(0, \beta_2, 0, \beta_4) = 0 \cdot (1, 0, 0, 0) + \beta_2 (0, 1, 0, 0) + 0 \cdot (0, 0, 1, 0) + \beta_4 (0, 0, 0, 1)$$

Como todos los elementos del núcleo se pueden escribir como combinación lineal de $\{(0, 1, 0, 0)$ y $(0, 0, 0, 1)\}$, esta es, pues, una base del núcleo. A partir de ella se determinan fácilmente las ecuaciones paramétricas y no paramétricas. La verificación del teorema 5 en este caso es inmediato:

$$\begin{aligned} &\dim \text{Ker } (f) = 2 \\ &\dim I_m (f) = 2 \\ &\dim K^4 = 4 \end{aligned}$$

luego, efectivamente:

$$\dim K^4 = \dim \text{Ker } (f) + \dim I_m(f)$$

8-6 CLASIFICACION DE LAS APLICACIONES LINEALES

La clasificación de las aplicaciones lineales entre espacios vectoriales es la misma que ya hicimos al hablar de ello en teoría de grupos, y conservamos los mismos nombres que allí en cada caso. Así, diremos que f es un *isomorfismo* entre dos espacios vectoriales E y F si es *sobre e* inyectiva. Cuando $E =$ F a f le llamaremos *endomorfismo* y si además es biyectiva, la denominaremos *automorfismo.*
Además de estos conceptos, expuestos por el hecho de que f es lineal y de que E y F son espacios vectoriales, aparecen algunas propiedades cuando f es sobre o inyectiva que son dignas de un particular estudio.

Teorema 6.—La condición necesaria y suficiente para que una aplicación $f: E \to F$ sea inyectiva es que el núcleo se reduzca al vector nulo $\operatorname{Ker}(f) = \{0\}$

$\Rightarrow$ Es condición necesaria. En efecto, supongamos que $f(x_1) = f(x_2)$ para algún par de elementos $x_1, x_2 \in E$. Entonces, pasando $f(x_2)$ al primer miembro y teniendo en cuenta que f es lineal $f(x_1 - x_2) = 0$, lo que significa que $x_1 - x_2 \in \operatorname{Ker}(f)$. Ahora bien, como $\operatorname{Ker}(f) =$ $= \{0\}$ por hipótesis, entonces $x_1 = x_2$ y f es, por tanto, inyectiva.
$\Leftarrow$ Es condición suficiente, ya que $\forall\, x_1, x_2 \in \operatorname{Ker}(f)$, $f(x_1) =$ $= f(x_2) = 0$. Como f es inyectiva, esto significa que $x_1 = x_2$. Si todos los elementos del núcleo son iguales, esto significa que el núcleo sólo tiene un elemento y como el $0 \in \operatorname{Ker}(f)$, el 0 es el único elemento del núcleo. Por tanto, tenemos $\operatorname{Ker}(f) = \{0\}$ como queremos demostrar.

Teorema 7.—Sea $f: E \to F$ una aplicación lineal inyectiva. Entonces, la imagen de toda familia libre de vectores de E es una familia libre de vectores de F.
En efecto, sea $M = \{v_1, ..., v_p\}$ una familia libre de vectores de E. La imagen será $f(M) = \{f(v_1), ..., f(v_p)\}$.
Cualquier combinación lineal nula que exista entre estos será:

$$\alpha_1 \cdot f(v_1) +, ..., + \alpha_p \cdot f(v_p) = 0 \quad \alpha_1, ..., \alpha_p \in K \quad (10)$$

luego:

$$f(\alpha_1 \cdot v_1 +, ..., + \alpha_p \cdot v_p) = 0$$

por tanto:

$$\alpha_1 \cdot v_1 +, ..., + \alpha_p \cdot v_p \in \text{Ker}\,(f)$$

Como por hipótesis f es inyectivo, por el teorema 6, Ker $(f) = \{0\}$, y por tanto:

$$\alpha_1 \cdot v_1 +, ..., + \alpha_p \cdot v_p = 0$$

pero como M era una familia libre, esto implica que:

$$\alpha_1 = \alpha_2 = ... = \alpha_p = 0$$

luego, volviendo a (10), f (M) es también una familia libre como queríamos demostrar.

Consecuencia.—Del teorema anterior se desprende que cuando f sea inyectiva, el subespacio imagen tendrá la misma dimensión que E. dim I_m (f) = dim E, ya que, como se ha visto, la imagen de una base de E es una familia de generadores de I_m (f) (consecuencia de T3) y como esta familia es libre (por T7), es una base de Im (f).
También podemos ver este mismo resultado en el teorema 5, que dice:

$$\text{dim Im}\,(f) + \text{dim Ker}\,(f) = \text{dim E}$$

Si f es inyectiva, por T6, Ker $(f) = \{0\}$ y de ello dim Ker $(f) = 0$ y queda:

$$\text{dim Im}\,(f) = \text{dim E}$$

Teorema 8.—Sean E y F dos espacios vectoriales de dimensión finita. La condición necesaria y suficiente para que una aplicación lineal $f : E \rightarrow F$ sea sobre, es que la imagen de una base cualquiera B de E sea una familia de generadores de F.
En efecto, sea B = $\{e_1, ..., e_n\}$ una base de E. La imagen será: f (B) = $\{f(e_1), ..., f(e_n)\}$.

⇒ Veamos que es condición necesaria: Si f es sobre, entonces:

$$\forall\, y \in F \quad \exists\, x \in E \mid y = f(x)$$

pero:

$$\forall x \in E \quad \exists \alpha_1, ..., \alpha_n \in K \mid x = \alpha_1 \cdot e_1 +, ..., + \alpha_n \cdot e_n$$

luego:

$$y = f(\alpha_1 \cdot x_1 +, ..., + \alpha_n \cdot x_n)$$

por ser f lineal:

$$y = \alpha_1 \cdot f(e_1) +, ..., + \alpha_n \cdot f(e_n)$$

luego $\forall\, y \in F$ se puede expresar como combinación lineal de la familia f (B).

⇐ Demostramos que es condición suficiente: supongamos que f (B) engendra F.
Entonces: $\forall\, y \in F \quad \exists\, \beta_1, ..., \beta_n \in K$, tales que

$$y = \beta_1\, f(e_1) +, ..., + \beta_n \cdot f(e_n)$$

de donde:

$$y = f(\beta_1 \cdot e_1 +, ..., + \beta_n \cdot e_n)$$

pero:

$$\beta_1 \cdot e_1 +, ..., + \beta_n \cdot e_n = z \in E$$

luego:

$$\forall\, y \in F \quad y = f(z) \quad z \in E$$

es decir, que f es sobre.

Consecuencia.—Como consecuencia de los teoremas anteriores, hemos obtenido unos criterios prácticos para saber cuándo la aplicación lineal es inyectiva, cuándo es suprayectiva y cuándo será biyectiva, conociendo la dimensión de $I_m\ (f)$
Según la consecuencia del teorema 7, será inyectiva cuando dim $I_m\ (f)$ = dim E.

Por el teorema 8, será suprayectiva cuando $\dim I_m (f) = \dim F$.
Y será, finalmente, biyectiva cuando $\dim I_m (f) = \dim E = \dim F$.

EJEMPLOS:

1) Sea la $g : R^4 \rightarrow R^3$, tal que:

$$\forall\ (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in R^4 \qquad g\ (\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\alpha_1 + \alpha_3 + \alpha_4, \alpha_1 + \alpha_2, \alpha_1 - \alpha_2 + 2\alpha_3 + 2\alpha_4)$$

en este caso es fácil ver que:

$$\dim \mathrm{Im}\ (g) = 2$$

luego:

$$\dim \mathrm{Im}\ (g) \neq \dim R^4$$
$$\dim \mathrm{Im}\ (g) \neq \dim R^3$$

por tanto, g no es ni inyectiva ni sobre, es un homomorfismo en general.

2) Sea $f : R^3 \rightarrow R^4$ definida por:

$$\forall\ (\alpha_1, \alpha_2, \alpha_3) \in R^3 \quad f\ (\alpha_1, \alpha_2, \alpha_3) = (\alpha_1, \alpha_2, \alpha_3, \alpha_1 + \alpha_2 + \alpha_3)$$

Las imágenes de la base canónica de R^3 serán:

$$f\ (1, 0, 0) = (1, 0, 0, 1)$$
$$f\ (0, 1, 0) = (0, 1, 0, 1)$$
$$f\ (0, 0, 1) = (0, 0, 1, 1)$$

La familia $\{(1, 0, 0, 1), (0, 1, 0, 1), (0, 0, 1, 1)\}$ es, pues, un sistema generador de Im (f) por ser imagen de la base canónica de R^3. Hallemos la dimensión de Im (f).

$$\beta_1 \cdot (1, 0, 0, 1) + \beta_2 \cdot (0, 1, 0, 1) + \beta_3 \cdot (0,0, 1, 1) = (0, 0, 0, 0)$$

operando:

$$(\beta_1, \beta_2, \beta_3, \beta_1 + \beta_2 + \beta_3) = (0, 0, 0, 0)$$

luego:

$$\beta_1 = \beta_2 = \beta_3 = 0$$

Lo cual significa que son una familia libre, y que por tanto:

$$\dim \operatorname{Im} (f) = 3$$

Podemos decir, pues, que f es una aplicación inyectiva, pues:

$$\dim \operatorname{Im} (f) = \dim R^3 = 3$$

No es "sobre", puesto que: $\dim R^4 = 4 \neq \dim \operatorname{Im} (f)$.

Teorema 9.—Sean E y F dos espacios vectoriales, ambos de dimensión n sobre el mismo cuerpo K, y sea f:E → F una aplicación lineal. Entonces, las tres proposiciones siguientes son equivalentes:

a) f es inyectiva.

b) f es sobre.

c) f es biyectiva.

Veamos que: 1) *a)* ⇒ *b)*. En efecto, si f es inyectiva, dim Ker $(f) = 0$, y según el teorema 5, dim Im (f) = dim E, pero dim E = dim F = n, o sea, dim Im (f) = dim F. Por tanto, según lo que acabamos de ver, f es sobre. Entonces, como f es inyectiva y sobre es biyectiva; de donde *a)* ⇒ *c)*.

2) *b)* ⇒ *a)*. En efecto: si f es sobre dim Im (f) = dim E = dim F. Entonces, según teorema 5, dim Ker $(f) = 0$, luego f es inyectiva. Igualmente, por ser f sobre e inyectiva es biyectiva y si se tiene *b)* ⇒ *c)*.

3) *(c ⇒ a)* ∧ *(c ⇒ b)*. Si f es biyectiva, por definición es inyectiva y sobre.

8-7 RANGO DE UNA APLICACION

Llamamos rango de una aplicación lineal a la dimensión del subespacio imagen.

$$\text{rango } (f) = \dim \operatorname{Im} (f)$$

Con esta notación, el teorema 5 puede reformularse escribiendo:

$$\text{rango } (f) + \dim \text{Ker } (f) = \dim \text{E}$$

8-8 INTERPRETACION DE LA NOCION DE BASE

Según lo que hemos estudiado en el presente tema, dados dos espacios vectoriales de la misma dimensión E y F definidos sobre el mismo cuerpo K, siempre puede definirse entre ellos un isomorfismo $i: \text{E} \to \text{F}$. Esto es evidente, pues supongamos que $\text{B} = \{e_1, ..., e_n\}$ sea una base de E, y $\text{B}' = \{u_1, ..., u_n\}$ sea una base de F. Entonces, según el teorema 1, que nos señala la existencia y unicidad de una aplicación lineal, podemos definir $i: \text{E} \to \text{F}$ del siguiente modo:

$$i(e_i) = u_i \quad \forall_i \in [1, ..., n]$$

Como $\{u_1, ..., u_n\}$ engendran Im (i), serán base del mismo, y por tanto, Im $(i) =$ F. De esto se deduce que es sobre, y

$$\dim \text{Im } (i) = \dim \text{F} = \dim \text{E}$$

Luego:

$$\dim \text{Ker } (i) = 0$$

e i es inyectiva. Entonces f es biyectiva.

En particular, dado el espacio vectorial E de n dimensiones sobre K, se puede definir, al menos, un isomorfismo $i: \text{K}^n \to \text{E}$, ya que ambos K^n y E tienen la misma dimensión.
Recordemos ahora que al dar una base $\{e_1, ..., e_n\}$ en un espacio vectorial E, cada vector $x \in \text{E}$ poseía un conjunto de n coordenadas únicas $(\alpha_1, ..., \alpha_n) \in \text{K}^n$, tales que:

$$x = \alpha_1 \cdot x_1 + ..., + \alpha_n \cdot x_n \qquad (9)$$

Inversamente, dado un elemento $(\alpha_1, ..., \alpha_n) \in \text{K}^n$ y fijada una base $\{e_1, ..., e_n\}$ de E, existe un solo vector x que cumple (9). Por tanto, al fijar una base de E, estamos definiendo una aplicación biyectiva Φ entre K^n y E, que por ser lineal es un isomorfismo.

Pero veamos también qué vectores corresponden en E por este isomorfismo a los elementos de la base canónica de K^n.

$$\Phi\,(1, 0, \ldots, 0) = z_1 \mid z_1 = 1 \cdot e_1 + 0 \cdot e_2 + \ldots, + 0 \cdot e_n = e_1$$
$$\Phi\,(0, 1, \ldots, 0) = z_2 \mid z_2 = 0 \cdot e_1 + 1 \cdot e_2 + \ldots, + 0 \cdot e_n = e_2$$
$$\vdots \qquad\qquad \vdots$$
$$\Phi\,(0, 0, \ldots, 1) = z_n \mid z_n = 0 \cdot e_1 + 0 \cdot e_2 + \ldots, + 1 \cdot e_n = e_n$$

luego las imágenes de la base canónica de K^n son los vectores de la base de E.

Entonces podemos concluir, que dar una base en un espacio vectorial E, y, por tanto, unas coordenadas a cada vector de E, es establecer un isomorfismo $i: K^n \to E$, que a cada vector de la base canónica $\{\mathcal{E}_1, \ldots, \mathcal{E}_n\}$ de K^n le hace corresponder un vector de una base cualquiera de E, $\{e_1, \ldots, e_n\}$

$$i\,(\mathcal{E}_i) = e_i$$

A esta base de E que se ha hecho corresponder biyectivamente con la base canónica de K^n se le llama, por ello, "base canónica o standard" de E.

Podemos entonces decir a la vista de lo que acabamos de exponer, que existe una aplicación biyectiva entre el conjunto de las bases de E y el conjunto de los isomorfismos $i: K^n \to E$, es decir, a una base corresponde un y sólo un isomorfismo, y a un isomorfismo corresponde una y sólo una base.

8-9 ESPACIO VECTORIAL DE LAS APLICACIONES LINEALES DE E EN F

Sean dos espacios vectoriales E y F definidos sobre el mismo cuerpo K y consideremos el conjunto de todas las aplicaciones lineales de E en F, que representaremos por L(E, F). Vamos a definir en este conjunto una ley de composición interna + para la que L(E, F) sea grupo abeliano y una ley de composición externa · que cumpla los cuatro axiomas del espacio vectorial.

1) *Suma de dos aplicaciones lineales:*

a) *Definición:* $\forall f, g \in L(E, F)$, definimos una aplicación $h \in L(E, F)$ que se llamará suma de f y g y se representará por $f + g = h$ del siguiente modo:

$$\forall x \in E \quad h(x) = f(x) + g(x)$$

Puesto que $f(x) \in F$ y $g(x) \in F$, su suma $f(x) + g(x)$ es vector único de F. Luego h es una aplicación de E en F. Veamos que es lineal.

$$\forall \alpha_1, \alpha_2 \in K, \ \forall x_1, \ x_2 \in E$$
$$h(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) = f(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) + g(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2)$$

es decir, por ser f y g lineales:

$$h(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) = \alpha_1 \cdot f(x_1) + \alpha_2 \cdot f(x_2) + \alpha_1 \cdot g(x_1) + \alpha_2 \cdot g(x_2) = \alpha_1 \cdot (f(x_1) + g(x_1)) + \alpha_2 \cdot (f(x_2) + g(x_2))$$

teniendo en cuenta la definición de $h = f + g$

$$f(x_1) + g(x_1) = h(x_1)$$
$$f(x_2) + g(x_2) = h(x_2)$$

sustituyendo,

$$h(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) = \alpha_1 \cdot h(x_1) + \alpha_2 \cdot h(x_2)$$

luego h es lineal y, por tanto, $h \in L(E, F)$

b) *Propiedad asociativa:* Demostremos que $\forall f, g, h \in L(E, F)$

$$f + (g + h) = (f + g) + h$$

En efecto:

$$\forall x \in E \quad [f + (g + h)](x) = f(x) + (g + h)(x) = f(x) + (g(x) + h(x))$$

pero como $f(x), g(x), h(x) \in F$, y por tanto, cumplen la asociatividad de la suma de F

$$f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x) = (f + g)(x) + h(x) = [(f + g) + h] (x)$$

Luego queda demostrado, pues las dos aplicaciones $f + (g + h)$ y $(f + g) + h$ tienen el mismo conjunto de partida E, el mismo conjunto de llegada F, y ahora acabamos de ver que tienen el mismo grafo. Por tanto, son iguales.

c) *Conmutativa:* Veamos que

$$\forall f, g \in L(E, F) \qquad f + g = g + f$$

En efecto:

$$\forall x \in E \quad (f + g)(x) = f(x) + g(x)$$

como $f(x)$ y $g(x)$ son elementos de F, cumplen por ello, la conmutatividad de la suma de F,
luego:

$$f(x) + g(x) = g(x) + f(x) = (g + f)(x)$$

y, por tanto,

$$(f + g) = (g + f)$$

d) *Elemento neutro:* Hay una aplicación de L(E, F) que es elemento neutro para la suma. La representaremos por $0 \in L(E, F)$, y se define:

$$\forall x \in E \quad 0(x) = 0 \quad \text{donde } 0 \in F \text{ neutro de } F$$

Veamos que es elemento neutro:

$$\forall f \in L(E, F)$$
$$(0 + f)(x) = 0(x) + f(x) = 0 + f(x) = f(x)$$
$$(f + 0)(x) = f(x) + 0(x) = f(x) + 0 = f(x)$$

A esta aplicación se le llama *aplicación nula.*

e) *Elemento simétrico:* Para toda $f \in L(E, F)$ existe una aplicación que llamaremos *opuesta* de f y representaremos por $(-f)$, que cumple

$$f + (-f) = (-f) + f = 0$$

Esta aplicación opuesta la definimos así:

$$\forall x \in E \quad (-f)(x) = -f(x)$$

que, en efecto, cumple la propiedad de ser opuesta

$$\forall x \in E, \quad (f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = 0(x)$$
$$((-f) + f)(x) = (-f)(x) + f(x) = -f(x) + f(x) = 0 = 0(x)$$

Luego [L (E, F), +] es, pues, un *grupo abeliano.*

2) *Ley de composición externa:*
Sea k el cuerpo de los espacios vectoriales E y F. Definamos el conjunto K x L(E, F) formado por todas las parejas (α, f).

$$K \; x \; L(E, F) = \{(\alpha, f) \mid \forall \alpha \in K, \forall f \in L(E, f)\}$$

La ley de composición externa $(\cdot)$: Kx L(E, F) $\rightarrow$ L(E, F) queda establecida haciendo corresponder a cada pareja $(\alpha, f) \in k \; x$ L(E, F) la aplicación $\alpha \cdot f$ definida:

$$(\alpha, f) \rightarrow \alpha \cdot f$$

$$\forall x \in E \quad (\alpha \cdot f)(x) = \alpha \cdot f(x).$$

Esto es una aplicación, pues $f(x) \in F$, $\alpha \in K$, y por la ley externa del espacio vectorial F, $\alpha \cdot f(x) \in F$.
Demostremos que la ley $(\cdot)$ así definida cumple los 4 axiomas de la ley externa de espacios vectoriales.

A_1) Hemos de demostrar que $\forall f, g \in L(E, F) \; \forall \alpha \in K$

$$\alpha \cdot (f + g) = \alpha \cdot f + \alpha \cdot g$$

En efecto:

$$\forall x \in E, \; [\alpha \cdot (f + g)](x) = \alpha \cdot (f + g)(x) = \alpha \cdot [f(x) + g(x)]$$

pero, $f(x), g(x) \in F$, luego

$$\alpha \cdot [f(x) + g(x)] = \alpha \cdot f(x) + \alpha \cdot g(x) = [\alpha \cdot f + \alpha \cdot g](x)$$

por definición de ley externa $(\cdot)$, luego

$$\alpha \cdot (f + g) = \alpha \cdot f + \alpha \cdot g \quad \forall\, x \in E$$

A_2) Demostramos que $\forall\, \alpha_1, \alpha_2 \in K$, $\forall\, f \in L(E, F)$

$$(\alpha_1 + \alpha_2) \cdot f = \alpha_1 \cdot f + \alpha_2 \cdot f$$

En efecto,

$$\forall\, x \in E \quad [(\alpha_1 + \alpha_2) \cdot f](x) = (\alpha_1 + \alpha_2) \cdot f(x)$$

Como $f(x) \in F$ y F cumple A_2:

$$(\alpha_1 + \alpha_2) \cdot f(x) = \alpha_1 \cdot f(x) + \alpha_2 \cdot f(x)$$

y por definición de ley externa:

$$\alpha_1 \cdot f(x) + \alpha_2 \cdot f(x) = (\alpha_1 \cdot f)(x) + (\alpha_2 \cdot f)(x)$$

o sea: $(\alpha_1 + \alpha_2) \cdot f = \alpha_1 \cdot f + \alpha_2 \cdot f \quad \forall x \in E$

A_3) $\forall\, \alpha_1, \alpha_2 \in K$, $\forall\, f \in L\,(E, F)$

$$(\alpha_1 \cdot \alpha_2) \cdot f = \alpha_1 \cdot (\alpha_2 \cdot f)$$

En efecto,

$$\forall\, x \in E \quad [(\alpha_1 \cdot \alpha_2) \cdot f]\,(x) = (\alpha_1 \cdot \alpha_2) \cdot f(x)$$

pero $f(x) \in F$ y como F cumple A_3):

$$(\alpha_1 \cdot \alpha_2) \cdot f(x) = \alpha_1 \cdot (\alpha_2 \cdot f(x))$$

Y por definición de ley externa:

$$\alpha_1 \cdot (\alpha_2 \cdot f(x) = [\alpha_1 \cdot (\alpha_2 \cdot f)](x) \qquad \text{c.q.d.}$$

A_4) $\forall f \in L(E, F)$ $\quad 1 \in K$ elemento unidad de K

$$1 \cdot f = f$$

En efecto:

$$\forall x \in E \quad (1 \cdot f)(x) = 1 \cdot f(x) = f(x)$$

Luego se cumplen los cuatro axiomas; por lo tanto, $[(L(E, F), +), (K, + \cdot), \cdot]$ es un espacio vectorial llamado espacio vectorial de las aplicaciones lineales o de los homomorfismos entre espacios vectoriales.

8-10 PRODUCTO DE DOS APLICACIONES LINEALES

Sean E, F y G tres espacios vectoriales sobre el mismo cuerpo K, y sean $f \in L(E, F)$, $g \in L(F, G)$ dos aplicaciones lineales. A la aplicación compuesta de $g \cdot f = h$ la llamaremos producto de f por g y demostraremos asimismo que h es lineal, y que por tanto, $h \in L(E, G)$

Definimos h del siguiente modo:

$$\forall x \in E \quad h(x) = (g \cdot f)(x) = g[f(x)]$$

$$\begin{tikzcd} E \arrow[rr, "h = g \cdot f"] \arrow[dr, "f"'] & & G \\ & F \arrow[ur, "g"'] & \end{tikzcd}$$

Demostremos que h: E → G definida así es una aplicación linial. En efecto:

$$\forall \alpha_1, \alpha_2 \in K \quad \forall x_1, x_2 \in E$$

$$h(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) = g[f(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2)] =$$

teniendo en cuenta que g y f son lineales:

$$= g[\alpha_1 \cdot f(x_1) + \alpha_2 \cdot f(x_2)] = \alpha_1 \cdot g[f(x_1)] + \alpha_2 \cdot g[f(x_2)]$$

por definición de h, $\; g[f(x_1)] = h(x_1)$ y $g[f(x_2)] = h(x_2)$

luego: $\quad h(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) = \alpha_1 \cdot h(x_1) + \alpha_2 \cdot h(x_2)$

por consiguiente, h es lineal, y $h \in L(E, G)$

8-11 ANILLO DE LOS ENDOMORFISMOS

Consideremos el conjunto de todas las aplicaciones lineales de E en E, que representaremos por L(E, E). Este conjunto, con la ley + y la ley externa que hemos definido en el apartado anterior es un espacio vectorial sobre K. Definamos ahora en L (E,E) una ley de composición interna, producto que representaremos $\cdot$, que con la ley interna + le conferirá una estructura de anillo.

1) *Ley producto* (Interna):

a) *Definición.*—Para todo par de endomorfismos $f,g \in$ L (E, E) definimos un $h \in$ L (E, E), que se llamará producto de f y g y que se representará $h = g \cdot f$ del siguiente modo:

$$\forall\, x \in E \quad h(x) = g[f(x)]$$

Como hemos visto al hablar de producto de dos aplicaciones lineales, h es lineal y por consiguiente $h \in$ L (E, E). Luego la ley $(\cdot)$ es de composición interna en L (E, E). Esto es posible, ya que el espacio vectorial de partida y llegada es el mismo E.

b) *Asociativa.*—La composición de aplicaciones es asociativa, como vimos al hablar de ellas.

c) *Elemento unidad.*—Existe una aplicación que llamaremos *aplicación idéntica,* que es elemento unidad para la ley producto. La *representaremos por I, y se define del siguiente modo:*

$$\forall\, x \in E \qquad I(x) = x$$

de acuerdo con su definición, $\forall\, x \in E \quad \forall\, f \in$ L (E, E)

$$(I \cdot f)(x) = I[f(x)] = f(x)$$
$$(f \cdot I)(x) = f[I(x)] = f(x)$$

por consiguiente, cumple las dos condiciones:

$$I \cdot f = f \cdot I = f$$

luego es elemento neutro.

2) *Distributiva.*—Demostremos que la ley producto es distributiva respecto a la ley +. Es decir, que:

$\forall f, g, h \in L(E, E)$

$$f \cdot (g + h) = f \cdot g + f \cdot h$$

En efecto,

$\forall x \in E$
$[f \cdot (g + h)](x) = f \cdot [(g + h)(x)] = f[g(x) + h(x)] =$

como f es lineal

$$= f[g(x)] + f[h(x)]$$

teniendo en cuenta la definición de ley producto:

$f[g(x)] = (f \cdot g)(x)$ y $f[h(x)] = (f \cdot h)(x)$; luego,

$$f \cdot (g + h) = f \cdot g + f \cdot h$$

c.q.d.

Entonces, según lo que acabamos de ver, $[L(E, E), +, \cdot]$ es un anillo unitario, llamado *anillo de los endomorfismos de E*.

8-12 GRUPO DE LOS AUTOMORFISMOS

Vamos a demostrar que el conjunto de los automorfismos de E constituye un grupo para la ley producto, también llamado grupo lineal. Representaremos el conjunto de los automorfismos de E por $L_A(E, E)$.

a) *Asociativa.*—Ya hemos visto que la composición de aplicaciones es asociativa.

b) *Elemento unidad.*—La aplicación I es un automorfismo y, por tanto, es el elemento neutro de $L_A(E, E)$ para la ley $(\cdot)$.

c) *Elemento inverso.*—Como vimos en el tema de teoría de conjuntos correspondiente, toda aplicación biyectiva $f \in L_A(E, E)$

posee una inversa f^{-1} que es también biyectiva, que cumple, por tanto,

$$f \cdot f^{-1} = f^{-1} \cdot f = I$$

Veamos que f^{-1} es lineal y que, por consiguiente, $f^{-1} \in L_A\ (E, E)$.

En efecto:

$$\forall\ y_1, y_2 \in E \quad \exists\, x_1, x_2 \in E \mid y_1 = f(x_1) \quad y_2 = f(x_2)$$

Entonces:

$$\forall\ \alpha_1, \alpha_2 \in K \quad \forall\ y_1, y_2 \in E$$

$$f^{-1}\ (\alpha_1 \cdot y_1 + \alpha_2 \cdot y_2) = f^{-1}\ (\alpha_1 \cdot f(x_1) + \alpha_2 \cdot f(x_2)) =$$

y como f es lineal:

$$= f^{-1}\ (f(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2)) = \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2$$

pero $x_1 = f^{-1}\ (y_1)$ y $x_2 = f^{-1}\ (y_2)$

Por tanto:

$$f^{-1}\ (\alpha_1 \cdot y_1 + \alpha_2 \cdot y_2) = \alpha_1 \cdot f^{-1}\ (y_1) + \alpha_2 \cdot f^{-1}\ (y_2)$$

entonces, $f^{-1} \in L_A\ (E, E)$ y $[L_A\ (E, E), \cdot]$ constituye el llamado *grupo lineal*.

TEMA 9 | MATRICES

9-1 DEFINICION

Sea K un cuerpo. Llamamos matriz M de p filas y q columnas, a un conjunto de $p \times q$ escalares distribuidos en p filas y q columnas como sigue:

$$M = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots\cdots & \alpha_{1q} \\ \alpha_{21} & \alpha_{22} & \cdots\cdots & \alpha_{2q} \\ \vdots & & & \\ \alpha_{p1} & \alpha_{p2} & \cdots\cdots & \alpha_{pq} \end{bmatrix}$$

donde, como hemos dicho, $\alpha_{ij} \in K \quad \forall_{i,j} \quad 1 \leqslant i \leqslant p, \; 1 \leqslant j \leqslant q$. En general, para abreviar podemos representar la matriz M por:

$$M = [\alpha_{ij}]$$

Al primero de los dos índices, i, se le llama índice de fila, puesto que indica a qué fila pertenece el elemento correspondiente. Al segundo índice, j, se le da el nombre de índice de columna, porque indica la

columna a la que pertenece el elemento en cuestión. Así, α_{58} significa que este elemento está situado en la fila 5.ª y en la columna 8.ª.
Cuando una matriz posee p filas y q columnas, se dice que es una matriz $(p \times q)$, o que es de orden $p \times q$.

9-1-1 MATRIZ DE UN VECTOR

Sea K^n un espacio vectorial de n dimensiones sobre K.
Cualquier vector $z = (\alpha_1, \ldots, \alpha_n) \in K^n$, por el hecho de estar constituido por estos n escalares, podría venir representado por una matriz

$$[z] = [\alpha_1, \alpha_2, \ldots, \alpha_n]$$

de orden $1 \times n$, llamada *matriz fila*, o también por una

$$[z] = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

de orden $n \times 1$ llamada *matriz columna*, pues tanto en uno como en otro caso, los n escalares que definen el vector z no han perdido el orden.
En general, utilizaremos más a menudo en el texto las matrices columna de orden $n \times 1$ para representar un vector de K^n
Vamos a ver si también es posible representar un vector x de un espacio vectorial cualquiera E, por medio de una matriz.
Recordemos del capítulo anterior que siempre que tenemos un espacio vectorial E de n dimensiones se puede establecer un isomorfismo entre K^n y él. Para ello basta establecer una base $B = \{u_1, \ldots, u_n\}$ de E.

Entonces:

$$\Phi : K^n \to E$$

se define como:

$$\Phi(e_i) = u_i$$

siendo $\{e_1, \ldots, e_n\}$ la base canónica de K^n

El vector $x \in E$ en la base B tiene unas coordenadas únicas $\alpha_1, \ldots, \alpha_n \in K$, tales que:

$$x = \alpha_1 \cdot u_1 +, \ldots, + \alpha_u \cdot u_n$$

Luego el isomorfismo Φ, lo que hará será hacer corresponder a cada conjunto de n escalares $(\alpha_1, \ldots, \alpha_n) \in K^n$, la combinación lineal de los vectores de B que dan estos escalares.

$$\Phi\ (\alpha_1, \ldots, \alpha_n) = x$$

O lo que es lo mismo, el isomorfismo recíproco $\Phi^{-1} : E \to K^n$ hace corresponder a cada vector x de E el conjunto de sus n coordenadas en la base B:

$$\Phi^{-1}\ (x) = (\alpha_1, \ldots, \alpha_n)$$

Podemos entonces resumir diciendo:

Dada una base de E $\Longleftrightarrow$, existe un isomorfismo Φ: $K^n \to E \Longleftrightarrow$
$\Longleftrightarrow \left[\begin{array}{l}\text{a cada vector } x \in E \text{ le corresponde uno y solo uno } (\alpha_1, \ldots, \alpha_n) \in K^n \\ \text{a cada vector } (\alpha_1, \ldots, \alpha_n) \in K^n \text{ le corresponde uno y solo uno } x \in E\end{array}\right.$

Y esto significa que cualquier operación con vectores de E es una operación con vectores de K^n, y viceversa.
Por todo esto, podemos representar cada vector $x \in E$ por una matriz columna:

$$\{x\}_\Phi = \begin{Bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{Bmatrix}$$

que hemos indicado por $\{x\}_{\Phi}$., entendiendo con ello que evidentemente, esta matriz depende de la base B que se ha elegido en E, o lo que es lo mismo, del isomorfismo que esa base induce.

9-1-2 MATRIZ DE UNA FAMILIA DE VECTORES

Sea E un espacio vectorial sobre K de n dimensiones y sea $B = \{u_1, ..., u_n\}$, una base de él. Consideremos una familia cualquiera de vectores de E: $N = \{x_1, ..., x_q\}$. Estos vectores tendrán unas coordenadas en aquella base:

$$\begin{array}{l} x_1 = \alpha_{11}\, u_1 + \alpha_{21}\, u_2 +, \ldots\ldots, + \alpha_{n1}\, u_n \\ x_2 = \alpha_{12}\, u_1 + \alpha_{22}\, u_2 +, \ldots\ldots, + \alpha_{n2}\, u_n \\ \vdots \\ x_i = \alpha_{1i}\, u_1 + \alpha_{2i}\, u_2 +, \ldots\ldots, + \alpha_{ni}\, u_n \\ \vdots \\ x_q = \alpha_{1q}\, u_1 + \alpha_{2q}\, u_2 +, \ldots\ldots, + \alpha_{nq}\, u_n \end{array}$$

que expresado en forma de sumatorio sería:

$$x_i = \sum_{j=1}^{m} \alpha_{ji}\, u_j \qquad \forall i \qquad 1 \leqslant i \leqslant q$$

entonces cada vector de aquella familia tiene asociada una matriz columna:

$$\{x_i\}_\Phi = \begin{Bmatrix} \alpha_{1i} \\ \alpha_{2i} \\ \vdots \\ \alpha_{ni} \end{Bmatrix}$$

siendo Φ el isomorfismo $\Phi : K^n \to E$ que corresponde a la base B.
Podemos, pues, representar la familia N por la matriz:

$$[N]_\Phi = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots\ldots & \alpha_{1q} \\ \alpha_{21} & \alpha_{22} & \ldots\ldots & \alpha_{2q} \\ \vdots & & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \ldots\ldots & \alpha_{nq} \end{bmatrix}$$

de orden $(n \times q)$ cuyas columnas son los vectores (conjunto de los n escalares que corresponden en K^n, a cada vector x_i de la familia a través de Φ.)
Esta representación de una familia de vectores por medio de la matriz

es unívoca, pues dada B solo hay en E "q" vectores $\{x_1, ..., x_q\}$ a los que correspondan por coordenadas los conjuntos de n escalares que constituyen las columnas de la matriz.

9-1-3 MATRIZ DE UN HOMOMORFISMO $h \in L(K^n, K^m)$

Un homomorfismo $h : K^n \to K^m$ queda unívocamente definido, como vimos en el tema 8, cuando se conocen las imágenes de los vectores de una base de K^n por medio de h.
Sea $B = \{e_1, ..., e_n\}$ la base canónica de K^n y sea $B' = \{e'_1, ..., e'_m\}$ la base canónica de K^m. Supongamos entonces que la aplicación h viene dada por las imágenes de B:

$$h(B) = \{h(e_1), ..., h(e_n)\}$$

Ahora bien, $h(e_i) \in K^m \quad \forall i \quad 1 \leqslant i \leqslant n$. Por tanto, se pueden expresar como combinación lineal de la base canónica B'

$$h(e_i) = \sum_{j=1}^{m} \alpha_{ji}\, e'_j \qquad 1 \leqslant i \leqslant n$$

Luego el sistema de vectores h (B) puede representarse uniívocamente por la matriz

$$[h(B)] = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots\cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots\cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots\cdots & \alpha_{mn} \end{bmatrix}$$

de orden $(m \times n)$, cuyas columnas son las coordenadas de los vectores de la base canónica de K^n transformados por h. (No olvidemos que en K^m las coordenadas de un vector en la base canónica coinciden con los escalares que definen dicho vector. Así, $h(e_i) = (\alpha_{1i}, ..., \alpha_{mi})$

coinciden con $h(e_i) = \sum\limits_{j=1}^{m} \alpha_{ji}\, e'_i$.)

Puesto que h (B) define unívocamente el homomorfismo h y dado que la matriz del sistema h (B) representa unívocamente a h (B), podemos considerar la matriz $[h\ (B)]$ como matriz que define el homomorfismo h.

$$[h] = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots\ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots\ldots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \ldots\ldots & \alpha_{mn} \end{bmatrix}$$

Que, como conclusión, establece que para determinar la matriz de una aplicación lineal $h : K^n \to K^m$ basta con poner en columna los transformados de los vectores de la base canónica de K^n,
Recíprocamente, dada una matriz $(m \times n)$ de elementos de K

$$[\alpha_{ij}]$$

existe una y solo una aplicación lineal $h : K^n \to K^m$, tal que

$$h\ (e_1) = (\alpha_{11}, \ldots\ldots, \alpha_{m1})$$
$$h\ (e_2) = (\alpha_{12}, \ldots\ldots, \alpha_{m2})$$
$$\vdots$$
$$h\ (e_n) = (\alpha_{1n}, \ldots\ldots, \alpha_{mn})$$

siendo $B = \{e_1, \ldots, e_n\}$ la base canónica de K^n.

Teorema 1.—Existe una aplicación biyectiva entre el conjunto de matrices $(m \times n)$ de elementos de K, $M^k_{m \times n}$ y el conjunto de las aplicaciones lineales $L\ (K^n, K^m)$.

9-1-4 MATRIZ DE UNA APLICACION LINEAL $f \in L\ (E,F)$

Sean E y F dos espacios vectoriales de dimensiones n y m respectivamente sobre K. Sea $B_E = \{v_1, \ldots, v_n\}$ una base de E y $B_F = \{u_1, \ldots, u_m\}$ una base de F a las que están asociados los isomorfismos $\Phi_E : K^n \to E$ y $\varphi_F : K^m \to F$.
Sea $f : E \to F$ una aplicación lineal definida por las imágenes de la base B de E:

$$\{f\ (v_1), \ldots, f\ (v_n)\} \subset F$$

Estos vectores pueden expresarse como combinación lineal de la base B_F como

$$f(v_1) = \sum_{j=1}^{m} \alpha_{j1}\, u_j$$

$$\vdots$$

$$f(v_n) = \sum_{j=1}^{m} \alpha_{jn}\, u_j$$

en general, decimos:

$$f(v_i) = \sum_{j=1}^{m} \alpha_{ji}\, u_j \qquad 1 \leqslant i \leqslant n$$

Podemos, de acuerdo con esto, construir el siguiente esquema:

$$\begin{tikzcd} E \arrow[r, "f"] & F \arrow[d, "\varphi_F^{-1}"] \\ k^n \arrow[u, "\Phi_E"] \arrow[r, "\varphi_F^{-1}\cdot f\cdot \Phi_E"'] & k^m \end{tikzcd}$$

con lo que un homomorfismo $f: E \to F$ lo hemos convertido en el producto de aplicaciones:

$$\varphi_F^{-1} \cdot f \cdot \Phi_E : K_n \to K_m$$

En virtud de lo que hemos visto en el apartado anterior, este homomorfismo $\Psi = \varphi_F^{-1} \cdot f \cdot \Phi_E$, $\Psi \in L(K^n, K^m)$ se puede representar por una matriz única, constituida por los transformados de los vectores de la base canónica de K^n colocados en columna. Hallemos la matriz que le corresponde.

Sea $B_n = \{\&_1, \ldots, \&_n\}$ la base canónica de K^n y $B'_m = \{\&'_1, \ldots, \&'_m\}$ la base canónica de K^m. Entonces: $\forall i \quad 1 \leqslant i \leqslant n$

$$\Psi(\&_i) = \varphi_F^{-1} \cdot f \cdot \Phi_E\ (\&_i)$$

y teniendo en cuenta la definición de producto de aplicaciones, así como las definiciones dadas de los homomorfismos φ_F, f y Φ_E queda,

$$\Psi(\&_i) = (\varphi_F^{-1} \cdot f)\,(\Phi(\&_i)) = (\varphi_F^{-1} \cdot f)\,(v_i) =$$
$$= \varphi_F^{-1} \cdot (f(v_i)) = \varphi_F^{-1}\,\Big(\sum_{j=1}^{m} \alpha_{ji} \cdot u_j\Big) =$$

y por ser φ_F^{-1} lineal:

$$= \sum_{j=1}^{m} \alpha_{ji} \cdot \varphi_F^{-1} \ (u_j)$$

pero $\varphi_F^{-1} \ (u_j) = \mathcal{E}'_j$ y queda:

$$\Psi \ (\mathcal{E}_i) = \sum_{j=1}^{m} \alpha_{ji} \ \mathcal{E}'_j$$

Luego la matriz que definirá el homomorfismo $\Psi \ : K^n \to K^m$ será:

$$[\Psi] = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots\dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots\dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots\dots & \alpha_{mn} \end{bmatrix}$$

Observemos, entonces, globalmente el proceso: dados una base de E, B_E y otra de F, B_F (o lo que es igual, los isomorfismos que definen Φ_E φ_F), tenemos:

$$\boxed{\begin{array}{c} f \in L(E,F) \\ B_E \rightarrow \Phi_E \\ B_F \rightarrow \varphi_F \end{array}} \Longleftrightarrow \boxed{\begin{array}{c} \exists^* \Psi \in L(K^n, K^m) \\ \Psi = \varphi_F^{-1} \cdot f \cdot \Phi_E \end{array}} \Longleftrightarrow \boxed{\exists^* [\Psi] \in M_{m \times n}^{K}}$$

Por tanto, podemos representar la aplicación lineal $f \in L \ (E,F)$ por la matriz $[\Psi]$, que ahora, para mejor representación, denominaremos $[f]_{\Phi_E \ \varphi_F}$.

La matriz, pues, de una aplicación lineal $f \in L \ (E,F)$, fijadas unas bases B_E, B_F se obtiene colocando en columna las coordenadas, de los transformados de B_E por f, en la base B_F.

En general, cuando las bases E y F sean suficientemente conocidas, la matriz de $f \in L \ (E,F)$ la representaremos sencillamente por $[f]$, o bien por $[\alpha_{ij}]$, siendo α_{ij} el elemento de $[f]$ situado en la fila i, columna j de la misma:

$$
\begin{array}{cc}
 & \text{columna } j \\
 & \downarrow \\
\text{fila } i \rightarrow &
\begin{bmatrix}
\alpha_{11}, & \cdots\cdots & \cdots & \cdots\cdots, & \alpha_{1n} \\
\vdots & & \vdots & & \vdots \\
\cdots & \cdots & \alpha_{ij} & \cdots & \cdots \\
\vdots & & \vdots & & \vdots \\
\alpha_{m1} & \cdots\cdots & \cdots & \cdots\cdots, & \alpha_{mn}
\end{bmatrix}
\end{array}
$$

EJEMPLOS:

1) Dado el espacio vectorial R^4, la matriz correspondiente al vector $v = (1, 2, 3, -1) \in R^4$, será, según lo que hemos dicho:

$$
[v] = \begin{pmatrix} 1 \\ 2 \\ 3 \\ -1 \end{pmatrix}
$$

y la matriz que corresponde a la familia de vectores: $N = \{v_1, v_2, v_3\}$

$$
\begin{aligned}
v_1 &= (1, 0, 1, -1) \\
v_2 &= (1, 2, 0, 1) \\
v_3 &= (0, 0, 1, -3)
\end{aligned}
$$

será

$$
[N] = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \\ -1 & 1 & -3 \end{bmatrix}
$$

2) Sea una aplicación lineal $h : R^4 \to R^4$ definida del siguiente modo:

$\forall (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in R^4$

$h(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\alpha_1 - 2\alpha_2, \alpha_2 + \alpha_3 + \alpha_4, \alpha_1 + \alpha_3, \alpha_2 - 3\alpha_3 + \alpha_4)$

Para hallar la matriz de h, basta con encontrar los transformados de los vectores de la base canónica:

$$h(\&_1) = h(1,0,0,0) = (1,0,1,0)$$
$$h(\&_2) = h(0,1,0,0) = (-2,1,0,1)$$
$$h(\&_3) = h(0,0,1,0) = (0,1,1,-3)$$
$$h(\&_4) = h(0,0,0,1) = (0,1,0,1)$$

luego:

$$[h] = \begin{bmatrix} 1 & -2 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & -3 & 1 \end{bmatrix}$$

3) Consideremos dos espacios vectoriales E y F definidos sobre el cuerpo de los números reales, tales que dim E = 3, dim F = 4. Consideremos dos bases cualesquiera $B_E = \{v_1, v_2, v_3\}$ y $B_F = \{u_1, u_2, u_3, u_4\}$ de E y F respectivamente, definidos por sus isomorfismos Φ_E y φ_F.
Sea la aplicación lineal $f \in L(E,F)$ definida por:

$$f(v_1) = 2u_1 + u_3 - u_4$$
$$f(v_2) = u_1 + u_2 - u_3 + u_4$$
$$f(v_3) = u_2 - u_4$$

y entonces podemos escribir, según lo dicho, la matriz de esta aplicación lineal en aquellas bases:

$$[f]_{\Phi_E, \varphi_F} = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & -1 & 0 \\ -1 & 1 & -1 \end{bmatrix}$$

Teorema 2.—Fijados dos bases B_E y B_F de los espacios vectoriales E y F definidos sobre el mismo K "existe una aplicación biyectiva entre el conjunto de aplicaciones lineales $f \in L(E,F)$ y el conjunto de matrices $M^K_{(m \times n)}$".

9-2 ESTRUCTURA DEL CONJUNTO $M^K_{(m \times n)}$

9-2-1 ESPACIO VECTORIAL DE LAS MATRICES $(m \times n)$

Vamos a definir en el conjunto $M^K_{(m \times n)}$ una ley de composición interna aditiva y una ley externa que cumplan los cuatro axiomas necesarios para tener una estructura de espacio vectorial. Para definir estas leyes utilizaremos el teorema 1, que nos asegura que a cada matriz $(m \times n)$ corresponde un y solo un homomorfismo entre K^n y K^m y a cada homomorfismo de $L(K^n, K^m)$ corresponde una y sola una matriz de orden $(m \times n)$. Operando con esta aplicación biyectiva conseguiremos que las leyes interna y externa del espacio vectorial $L(K^n, K^m)$ induzcan unas leyes aditiva y producto por un escalar que proporcionen estructura de espacio vectorial a $M^k_{(m \times n)}$ y conviertan dicha aplicación biyectiva en un isomorfismo entre los espacios $L(K^n, K^m)$ y $M^k_{(m \times n)}$

1) *Ley de composición interna. Suma de matrices:* Para todo par de matrices A y B pertenecientes a $M^k_{(m \times n)}$ les asociamos $C \in M^k_{(m \times n)}$, que llamaremos suma de A y B y representaremos por $C = A + B$, definida como sigue:

$$\forall\ A \in M^k_{(m \times n)} \overset{T_1}{\rightarrow} \exists^* f \in L(K^n, K^m) \mid A = [f]$$

$$\forall\ B \in M^k_{(m \times n)} \overset{T_1}{\rightarrow} \exists^* g \in L(K^n, K^m) \mid B = [g]$$

Supongamos que las bases canónicas de K^n y K^m sean respectivamente $B_n = \{v_1, ..., v_n\}$ y $B_m = \{u_1, ..., u_m\}$. Entonces g y f vienen dados por:

$$f(v_i) = \sum_{j=1}^{m} \alpha_{ji}\, u_j, \quad \forall_i \quad 1 \leqslant i \leqslant n$$

$$g(v_i) = \sum_{j=1}^{m} \beta_{ji}\, u_j, \quad \forall_i \quad 1 \leqslant i \leqslant n$$

luego:

$$A = [f] = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots\cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots\cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots\cdots & \alpha_{mn} \end{bmatrix} \qquad B = [g] = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots\cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots\cdots & \beta_{2n} \\ \vdots & \vdots & & \vdots \\ \beta_{m1} & \beta_{m2} & \cdots\cdots & \beta_{mn} \end{bmatrix}$$

Definimos entonces $C = A + B$ como la matriz que corresponde a la aplicación suma $(f + g) \in L\ (K^n,\ K^m)$. Teniendo en cuenta la definición de aplicación suma:

$$(f + g)\ (v_i) = \sum_{j=1}^{m} \alpha_{ji}\, u_j + \sum_{j=1}^{m} \beta_{ji}\, u_j = \sum_{j=1}^{m} (\alpha_{ji} + \beta_{ji})\, u_j$$

de donde:

$$C = [f + g] = \begin{bmatrix} (\alpha_{11} + \beta_{11}) & \ldots\ldots & (\alpha_{1n} + \beta_{1n}) \\ \vdots & & \vdots \\ (\alpha_{m1} + \beta_{m1}) & \ldots\ldots & (\alpha_{mn} + \beta_{mn}) \end{bmatrix}$$

De esto podemos, pues, deducir la regla práctica para sumar matrices: "Para sumar dos matrices del mismo orden $(m \times n)$ de elementos de K, se suman elemento a elemento los que ocupan la misma fila y la misma columna en cada una de ellos". Si a los elementos de C les representamos por γ_{ij}. lo que acabamos de decir se representaría por $\gamma_{ij} = \alpha_{ij} + \beta_{ij}$. El elemento que ocupa la fila i y columna j de C se obtiene sumando el que ocupa la fila i columna j de A con el que ocupa el mismo lugar en B.

1*a*) *Asociativa.*—Como la suma de matrices se ha reducido a la suma de los escalares respectivos de aquella se desprende de la asociativa de la ley + de escalares.

1*b*) *Conmutativa.*—Igual que la asociativa se desprende de la conmutativa de los escalares de K.

1*c*) *Elemento neutro. Matriz nula.*—El elemento neutro para esta ley suma de matrices que acabamos de definir, es la matriz de la aplicación nula $0 \in L\ (K^n, K^m)$.

La aplicación nula está definida por:

$$0\ (v_i) = 0 \qquad \forall\ v_i \in B_n$$

por tanto, la matriz de la aplicación 0 que llamaremos *matriz nula* y representaremos por [0] será:

$$[0] = \underbrace{\begin{bmatrix} 0 & 0 & \ldots\ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots\ldots & 0 \end{bmatrix}}_{n} \Big\updownarrow m$$

1*d*) *Elemento simétrico. Matriz opuesta.*—Dada una matriz cualquiera $A \in M^k_{(m \times n)}$ a la que corresponde la aplicación lineal $f \in L(K^n, K^m)$ definimos el elemento simétrico de A para la ley +, llamada *matriz opuesta* y representada por $(-A)$ a la matriz de la aplicación opuesta $(-f) \in L(K^n, K^m)$; la aplicación opuesta de f será:

$$(-f)(v_i) = -f(v_i) = \sum_{j=1}^{m} (-\alpha_{ji})\, u_j$$

Luego:

$$-A = [-f] = \begin{bmatrix} (-\alpha_{11}) & \ldots\ldots & (-\alpha_{1n}) \\ \vdots & & \vdots \\ (-\alpha_{m1}) & \ldots\ldots & (-\alpha_{mn}) \end{bmatrix}$$

Por tanto, podemos concluir que $(M^k_{(m \times n)}, +)$ es un grupo abeliano.

2) *Ley externa. Producto de una matriz por un escalar.*—A cada par de elementos, uno $A \in M^k_{(m \times n)}$ y otro $\alpha \in K$, se les asocia un $P \in M^k_{(m \times n)}$ llamado producto de α por A y que representaremos por $P = \alpha \cdot A$ definido como sigue:
A la matriz A corresponde, como hemos dicho antes, una $f \in L(K^n$ $K^m)$ definida por:

$$f(v_i) = \sum_{j=1}^{m} \alpha_{ji}\, u_j, \quad \forall i \quad 1 \leqslant i \leqslant n$$

Definimos entonces P como la matriz de la aplicación producto $\alpha \cdot f$.
Hallemos P, entonces:

$$(\alpha f)(v_i) = \alpha \cdot f(v_i) = \alpha \cdot \sum_{j=1}^{m} \alpha_{ji}\, u_j = \sum_{j=1}^{m} (\alpha \cdot \alpha_{ji}) \cdot u_j$$

Luego:

$$\mathbf{P} = [\alpha \cdot f] = \begin{bmatrix} (\alpha \cdot \alpha_{11}) & \ldots\ldots & (\alpha \cdot \alpha_{1n}) \\ \vdots & & \vdots \\ (\alpha \cdot \alpha_{m1}) & \ldots\ldots & (\alpha \cdot \alpha_{mn}) \end{bmatrix}$$

Podemos decir, pues, que "para multiplicar una matriz por un escalar se multiplica cada elemento de la matriz por dicho escalar".
Esta ley externa definida de este modo cumple los cuatro axiomas de un espacio vectorial, ya que en definitiva se ha reducido a la ley producto de los escalares aplicada $(m \times n)$ veces. Por tanto, $M^k_{(m \times n)}$ constituye un espacio vectorial sobre K que representamos:

$$[(M^k_{(m \times n)}, +), (K, +, \cdot), \cdot]$$

EJEMPLOS:

1) Dadas las matrices

$$A = \begin{bmatrix} 1 & 2 & 1 \\ -3 & 2 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad y \quad B = \begin{bmatrix} 0 & 1 & 1 \\ 2 & -1 & -1 \\ 1 & -2 & 2 \end{bmatrix}$$

con elementos de R, la suma de ambas es otra matriz C de orden (3 x 3) dada por:

$$C = A + B = \begin{bmatrix} 1+0 & 2+1 & 1+1 \\ -3+2 & 2-1 & 1-1 \\ 1+1 & 1-2 & 0+2 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 2 \\ -1 & 1 & 0 \\ 2 & -1 & 2 \end{bmatrix}$$

2) El producto de la matriz A por el escalar $5 \in R$ será, según hemos señalado :

$$P = 5 \cdot A = \begin{bmatrix} 5 \cdot 1 & 5 \cdot 2 & 5 \cdot 1 \\ 5 \cdot (-3) & 5 \cdot 2 & 5 \cdot 1 \\ 5 \cdot 1 & 5 \cdot 1 & 5 \cdot 0 \end{bmatrix} = \begin{bmatrix} 5 & 10 & 5 \\ -15 & 10 & 5 \\ 5 & 5 & 0 \end{bmatrix}$$

Producto de matrices.—Vamos a utilizar una vez más el teorema 1 y a definir el producto de matrices a partir del producto de aplicaciones lineales. Entonces, igual que no todas las aplicaciones lineales se pueden multiplicar, tampoco se puede multiplicar cualquier par de matrices. Por consiguiente, puesto que sí que sabemos cuándo existe el producto de dos aplicaciones lineales, vamos a invertir el procedimiento y partir en este caso de dos aplicaciones en vez de dos matrices como hacíamos en la ley aditiva.

Sean $f \in L(K^n, K^m)$ y $g \in L(K^m, K^r)$. Sean $B_n = \{e_1, ..., e_n\}$ $B_m = \{u_1, ..., u_m\}$, $B_r = \{w_1, ..., w_r\}$ las bases canónicas de K^n, K^m y K^r. Los homomorfismos f y g están definidos por:

$$f(e_i) = \sum_{j=1}^{m} \alpha_{ji} \cdot u_j \quad \forall i \quad 1 \leqslant i \leqslant n$$

$$g(u_j) = \sum_{k=1}^{r} \beta_{kj} \cdot w_k \quad \forall j \quad 1 \leqslant j \leqslant m$$

De acuerdo con su definición y por el teorema 1, a las aplicaciones f y g les corresponden unas matrices $A \in M^k_{(m \times n)}$ y $B \in M^k_{(r \times m)}$ respectivamente:

$$A = [f] = \begin{bmatrix} \alpha_{11} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots\cdots & \alpha_{mn} \end{bmatrix} \qquad B = [g] = \begin{bmatrix} \beta_{11} & \cdots\cdots & \beta_{1m} \\ \vdots & & \vdots \\ \beta_{r1} & \cdots\cdots & \beta_{rm} \end{bmatrix}$$

Definimos la matriz C producto de B por A, que representaremos $C = B \cdot A$ igual a la matriz de la aplicación producto $g \cdot f$. Hallemos C

$$\begin{tikzcd} k^n \arrow[rr, "g \circ f"] \arrow[dr, "f"'] & & k^r \\ & k^m \arrow[ur, "g"'] & \end{tikzcd}$$

La aplicación producto es:

$$(g \cdot f)(e_i) = g(f(e_i)) = g\left(\sum_{j=1}^{m} \alpha_{ji} u_j\right) \quad \forall i \quad 1 \leqslant i \leqslant n$$

Como g es lineal y sustituyendo $g(u_j)$ por su valor queda:

$$(g \cdot f)(e_i) = \sum_{j=1}^{m} \alpha_{ji} \cdot g(u_j) = \sum_{j=1}^{m} \alpha_{ji} \cdot \left(\sum_{k=1}^{r} \beta_{kj} w_k\right) \quad \forall i \quad 1 \leqslant i \leqslant n$$

permutando los dos sumatorios:

$$(g \cdot f)(e_i) = \sum_{k=1}^{r} \left(\sum_{j=1}^{m} \beta_{kj} \cdot \alpha_{ji}\right) \cdot w_k \quad \forall i \quad 1 \leqslant i \leqslant n$$

Tenemos, pues, ya los elementos de la matriz $C = [g \cdot f]$. Si representamos por θ los elementos de C, entonces

$$\theta_{ki} = \sum_{j=1}^{m} \beta_{kj} \cdot \alpha_{ji}$$

Hallemos por ejemplo el elemento θ_{11} situado en la primera fila y primera columna de C. Para él tenemos $k = 1$ e $i = 1$

$$\theta_{11} = \sum_{j=1}^{m} \beta_{1j} \cdot \alpha_{j1}$$

Para el θ_{12} situado en la primera fila y segunda columna de C será $k = 1, i = 2$:

$$\theta_{12} = \sum_{j=1}^{m} \beta_{1j} \cdot \alpha_{j2}$$

Luego la matriz producto $C = B \cdot A$ es:

$$C = [g \cdot f] = \begin{bmatrix} \left(\sum_{j=1}^{m} \beta_{1j} \cdot \alpha_{j1}\right) & \left(\sum_{j=1}^{m} \beta_{1j} \cdot \alpha_{j2}\right) & \cdots\cdots & \left(\sum_{j=1}^{m} \beta_{1j} \cdot \alpha_{jn}\right) \\ \vdots & & & \vdots \\ \left(\sum_{j=1}^{m} \beta_{rj} \cdot \alpha_{j1}\right) & \cdots\cdots & \cdots\cdots & \left(\sum_{j=1}^{m} \beta_{rj} \cdot \alpha_{jn}\right) \end{bmatrix}$$

Donde podemos ver que para poder multiplicar dos matrices B y A, el número de columnas de B ha de ser igual al número de filas de A; puesto que $C = B \cdot A$ se ha definido a partir de la aplicación producto $(g \cdot f)$ y para que exista ésta, el conjunto de llegada de f (espacio vectorial K^m de m dimensiones) ha de ser el conjunto de partida de g.

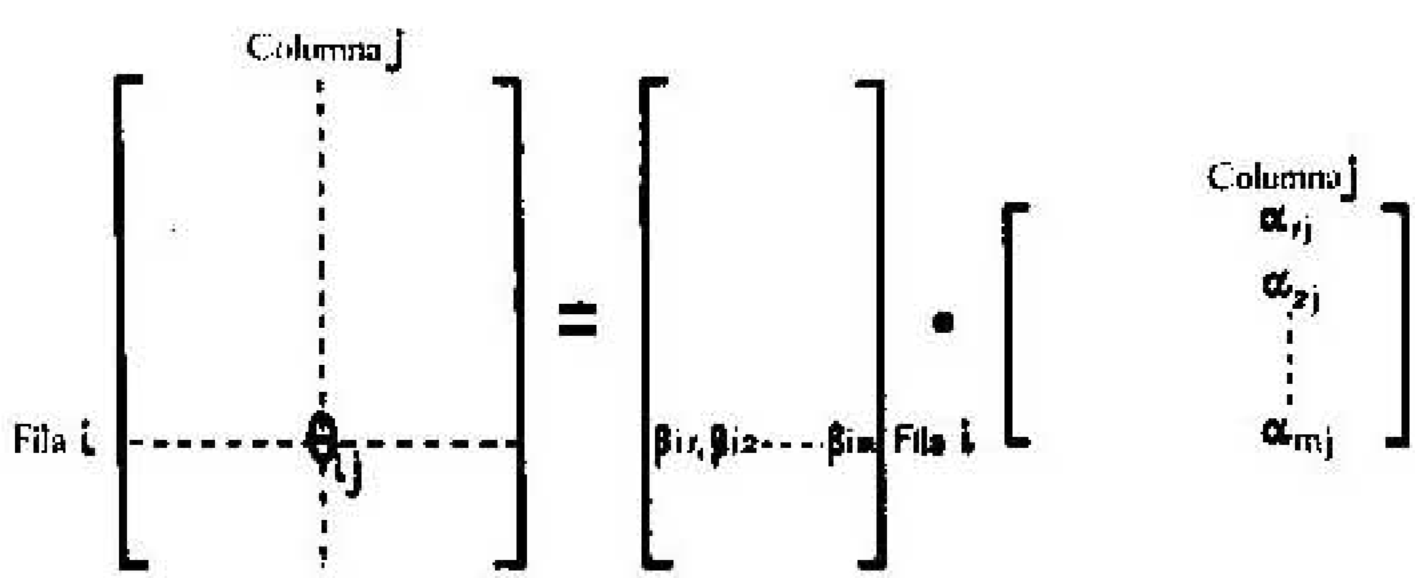
También podemos ver fácilmente el orden de la matriz producto C es $(r \times n)$. Tiene el mismo número de filas que B y el mismo número de columnas que A. Esquemáticamente, se puede representar lo que ocurre con las órdenes en el producto de matrices por:

$$(r \times m) \cdot (m \times n) = (r \times n)$$

Podemos deducir de aquí la regla práctica para multiplicar matrices. Por ejemplo, en el caso que ya hemos visto de la obtención de θ_{12}

$$\theta_{12} = \sum_{j=1}^{m} \beta_{1j} \cdot \alpha_{j2} = \beta_{11} \cdot \alpha_{12} + \beta_{12} \cdot \alpha_{22} + \beta_{13} \cdot \alpha_{32} +, \ldots, + \beta_{1m} \cdot \alpha_{m2}$$

Observando detenidamente esta suma y teniendo presentes las matrices B y A vemos que se han multiplicado término a término y se han sumado los escalares ($\beta_{11}, \beta_{12}, \ldots, \beta_{1m}$) por los ($\alpha_{12}, \alpha_{22}, \ldots, \alpha_{m2}$). Los primeros constituyen la primera fila de la matriz B (todos ellos tienen el primer subíndice, el de fila, igual a uno) y lo segundos forman la segunda columna de la matriz A (todos tienen el subíndice de columna igual a dos). Por consiguiente, si para hallar el θ_{12} hemos multiplicado término a término y sumado, los elementos de la primera fila de B con los de la segunda columna de A, podemos decir en general: "para hallar el elemento θ_{ij} de la matriz producto $C = B \cdot A$, se multiplican término a término y se suman los elementos de la fila *i* de B por los de la columna *j* de A". Gráficamente, esto lo podemos representar así:



$$(r \times n) \qquad (r \times m) \qquad (m \times n)$$

$$\mathbf{C} = \mathbf{B} \cdot \mathbf{A}$$

quedando:

$$\boxed{\theta_{ij} = \beta_{i1} \cdot \alpha_{1j} + \beta_{i2} \cdot \alpha_{2j} +, \ldots, + \beta_{im} \cdot \alpha_{mj}}$$

EJEMPLOS:

1) Sea la matriz $A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & -1 & -3 \\ 1 & 0 & -1 \end{bmatrix}$ y la $B = \begin{bmatrix} 2 & 2 & 0 \\ -1 & 3 & 1 \\ 1 & 1 & 3 \\ -1 & 1 & 2 \end{bmatrix}$

Hallemos la matriz producto de estos $C = B \cdot A$

En primer lugar sabemos que este producto se puede efectuar, pues el número de columnas de B es igual al número de filas de A igual a 3. Según la regla que hemos obtenido se tiene:

$$C = B \cdot A = \begin{bmatrix} (2 \cdot 1 + 2 \cdot 2 + 0 \cdot 1) & (2 \cdot 2 + 2 \cdot -1 + 0 \cdot 0) & (2 \cdot 1 + 2 \cdot -3 + 0 \cdot -1) \\ (-1 \cdot 1 + 3 \cdot 2 + 1 \cdot 1) & (-1 \cdot 2 + 3 \cdot -1 + 1 \cdot 0) & (-1 \cdot 1 + 3 \cdot -3 + 1 \cdot -1) \\ (1 \cdot 1 + 1 \cdot 2 + 3 \cdot 1) & (1 \cdot 2 + 1 \cdot -1 + 3 \cdot 0) & (1 \cdot 1 + 1 \cdot -3 + 3 \cdot -1) \\ (-1 \cdot 1 + 1 \cdot 2 + 2 \cdot 1) & (-1 \cdot 2 + 1 \cdot -1 + 2 \cdot 0) & (-1 \cdot 1 + 1 \cdot -3 + 2 \cdot -1) \end{bmatrix}$$

Operando:

$$C = \begin{bmatrix} 6 & 2 & -4 \\ 6 & -5 & -11 \\ 6 & 1 & -5 \\ 3 & -3 & -6 \end{bmatrix}$$

que es una matriz 4×3, como ya podíamos prever.

2) Hallemos el producto de la matriz fila $A = [1\ 2\ 1\ -3]$ por la matriz columna $B = \begin{Bmatrix} 1 \\ -1 \\ 2 \\ 1 \end{Bmatrix}$

Primero calcularemos $C_1 = A \cdot B$

$$C_1 = A \cdot B = [1\ \ 2\ \ 1\ \ -3] \cdot \begin{Bmatrix} 1 \\ -1 \\ 2 \\ 1 \end{Bmatrix} = [1 \cdot 1 + 2 \cdot -1 + 1 \cdot 2 + -3 \cdot 1] = [-2]$$

Conclusión: el producto de una matriz fila $1 \times n$ por una matriz columna $n \times 1$, es una matriz 1×1; es decir, un escalar.

En segundo lugar hallemos $C_2 = B \cdot A$

$$C_2 = B \cdot A = \left\{\begin{array}{r} 1 \\ -1 \\ 2 \\ 1 \end{array}\right\} \cdot [1 \cdot 2\ 1\ -3] = \begin{bmatrix} 1 & 2 & 1 & -3 \\ -1 & -2 & -1 & 3 \\ 2 & 4 & 2 & -6 \\ 1 & 2 & 1 & -3 \end{bmatrix}$$

El producto, pues, de una matriz columna $n \times 1$ por una matriz fila $1 \times n$ es una matriz $n \times n$.

Estos resultados nos hacen ver rápidamente que el producto de matrices no es conmutativo.

3) Sea la matriz $A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & -1 & -3 \\ 1 & 0 & -1 \\ 2 & 1 & 1 \end{bmatrix}$ y la

matriz columna $B = \left\{\begin{array}{r} -1 \\ 1 \\ 1 \end{array}\right\}$ vamos a hallar el producto de ambos.

El orden de la matriz producto será 4×1, pues $(4 \times 3) \cdot (3 \times 1) = (4 \times 1)$

$$C = A \cdot B = \begin{bmatrix} 1 & 2 & 1 \\ 2 & -1 & -3 \\ 1 & 0 & -1 \\ 2 & 1 & 1 \end{bmatrix} \left\{\begin{array}{r} -1 \\ 1 \\ 1 \end{array}\right\} = \begin{bmatrix} 1 \cdot -1 + 2 \cdot 1 + 1 \cdot 1 \\ 2 \cdot -1 + -1 \cdot 1 + -3 \cdot 1 \\ 1 \cdot -1 + 0 \cdot 1 + -1 \cdot 1 \\ 2 \cdot -1 + 1 \cdot 1 + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 2 \\ -6 \\ -2 \\ 0 \end{bmatrix}$$

Consecuencia.—Definido ya el producto entre matrices, podemos representar matricialmente la ecuación que define el homomorfismo $y = f(x)$ que indica que el elemento $y \in F$ es la imagen de $x \in E$ por medio de $f \in L(E, F)$. Esta ecuación, fijada unas bases B_E y B_F, la podremos expresar:

Sea la matriz asociada a y en estas bases, $\{y\}_{\varphi_F} = \left\{\begin{array}{c} \beta_1 \\ \vdots \\ \beta_m \end{array}\right\}$ siendo la matriz asociada a x: $\{x\}_{\Phi_E} = \begin{Bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{Bmatrix}$ Entonces, si la matriz de f es:

$$[f]_{\Phi_E\ \varphi_F} = \begin{bmatrix} \gamma_{11} & \cdots\cdots & \gamma_{1n} \\ \vdots & & \vdots \\ \gamma_{m1} & \cdots\cdots & \gamma_{mn} \end{bmatrix}$$

la ecuación del homomorfismo $y = f(x)$ queda:

$$\begin{Bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{Bmatrix} = \begin{bmatrix} \gamma_{11} & \cdots\cdots & \gamma_{1n} \\ \vdots & & \vdots \\ \gamma_{m1} & \cdots\cdots & \gamma_{mn} \end{bmatrix} \begin{Bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{Bmatrix}$$

En esta ecuación tenemos todos los elementos necesarios para estudiar el homomorfismo $f \in L(E, F)$. Por ejemplo, para hallar el núcleo, basta con tomar la matriz $\{y\}_{\varphi_F}$ igual a la matriz nula.
Por tanto, el núcleo queda determinado a partir de la ecuación: $x \in E \mid f(x) = 0$, o sea,

$$\begin{bmatrix} \gamma_{11} & \cdots\cdots & \gamma_{1n} \\ \vdots & & \vdots \\ \gamma_{m1} & \cdots\cdots & \gamma_{mn} \end{bmatrix} \begin{Bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{Bmatrix} = \begin{Bmatrix} 0 \\ \vdots \\ 0 \end{Bmatrix}$$

El subespacio imagen queda definido por las columnas de la matriz, que son las coordenadas de los transformados por f de los vectores de la base B_E en la base B_F.

Si $B_E = \{v_1, \ldots\ldots, v_n\}$ y $B_F = \{u_1, \ldots\ldots, u_n\}$

$$\begin{aligned} f(v_1) &= \gamma_{11}\, u_1 +, \ldots\ldots, + \gamma_{m1}\, u_m \\ f(v_2) &= \gamma_{12}\, u_1 +, \ldots\ldots, + \gamma_{m2}\, u_m \\ &\ \vdots \\ f(v_n) &= \gamma_{1n}\, u_1 +, \ldots\ldots, + \gamma_{mn}\, u_m \end{aligned}$$

Y la familia $\{f(v_1), \ldots, f(v_n)\}$ es, como sabemos, generadora del subespacio imagen.

9-2-2 ANILLO DE LAS MATRICES $n \times n$

A este tipo de matrices que poseen el mismo número de filas que de columnas se las llama *matrices cuadradas.* Veamos que estas matrices cuadradas forman un anillo.

1) *Grupo abeliano.*—En primer lugar constituyen un grupo abeliano para la ley de composición interna aditiva, suma de matrices, que hemos definido anteriormente. Tenemos, pues: $(M^k_{(n\times n)}, +)$.

2) *Ley producto.*—La ley producto definida anteriormente es ley de composición para el conjunto $M^k_{(n\times n)}$, ya que las condiciones que debían cumplir dos matrices A y B para que existiese su producto era que los elementos de ambos fueran del mismo cuerpo K y que el número de columnas de la primera fuese igual al número de filas de la segunda y esto se cumple. Por otra parte, el orden de la matriz producto será $(n \times n) \cdot (n \times n) = (n \times n)$. Luego el producto de dos matrices $M^k_{(n\times n)}$ es otra matriz $M^k_{(n\times n)}$. Lo que implica que la ley producto de matrices es interna en $M^k_{(n\times n)}$.
Veamos qué propiedades cumple esta ley en el conjunto $M^k_{(n\times n)}$.

2a) *Asociativa.*—Acabamos de probar que

$$\forall\ A,B \in M^k_{(n\times n)} \quad \exists^*\ D \in M^k_{(n\times n)} \ \mid\ D = A \cdot B$$

Ahora bien, A y B son dos matrices que representan dos aplicaciones, los homomorfismos

$$A \to (f : E_1 \to E_2)$$
$$B \to (g : E_2 \to E_3)$$

entre los espacios vectoriales E_1, E_2 y E_2, E_3, todos de dimensión n. En el capítulo 2 vimos que el producto de aplicaciones es asociativo, luego *por isomorfismo* el producto de matrices también lo será, es decir, dadas tres matrices $A, B, C \in M^k_{(n\times n)}$, podremos siempre decir que:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

2b) *Distributiva.*—Sean A, B, C tres matrices $n \times n$:

$$A = [\alpha_{ij}], \quad B = [\beta_{ij}], \quad C = [\gamma_{ij}]$$

Vamos a demostrar que:

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

En efecto: llamemos $T = A \cdot (B + C)$, siendo $T = [\tau_{ij}]$ $P = A \cdot B$, con $P = [\pi_{ij}]$ y $M = A \cdot C$, tal que $M = [\mu_{ij}]$ todas ellas, T, P y M, de orden $n \times n$.
Por definición de producto:

$$\tau_{ij} = \sum_{k=1}^{n} \alpha_{ik} \, (\beta_{kj} + \gamma_{kj})$$

teniendo en cuenta que los escalares cumplen la distributiva:

$$\tau_{ij} = \sum_{k=1}^{n} \alpha_{ik} \, \beta_{kj} + \sum_{k=1}^{n} \alpha_{ik} \, \gamma_{kj}$$

pero por definición también de producto:

$$\sum_{k=1}^{n} \alpha_{ik} \, \beta_{kj} = \pi_{ij} \quad \text{y} \quad \sum_{k=1}^{n} \alpha_{ik} \, \gamma_{kj} = \mu_{ij}$$

luego:

$$\tau_{ij} = \pi_{ij} + \mu_{ij}$$

y por definición de suma de matrices:

$$T = P + M$$

es decir, sustituyendo:

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

como queríamos demostrar.

2c) *Elemento unidad.*—Para esta ley producto existe un elemento neutro que es la llamada matriz unidad de orden $n \times n$, I_n. La definimos del siguiente modo: "la matriz unidad es la matriz de la aplicación idéntica $I : K^n \to K^n$. Es decir, aquella que dada una base $B_E = \{e_1, ..., e_n\}$, la transforma en sí misma:

$$\text{In}\,(e_i) = e_i \quad \forall i \quad 1 \leqslant i \leqslant n.$$

o sea:

$$I_n(e_1) = 1 \cdot e_1 + 0 \cdot e_2 + 0 \cdot e_3 +, ..., + 0 \cdot e_n = e_1$$
$$I_n(e_2) = 0 \cdot e_1 + 1 \cdot e_2 + 0 \cdot e_3 +, ..., + 0 \cdot e_n = e_2$$
$$\vdots$$
$$I_n(e_n) = 0 \cdot e_1 + 0 \cdot e_2 + 0 \cdot e_3 +, ..., + 1 \cdot e_n = e_n$$

Luego la matriz unidad es:

$$I_n = \begin{bmatrix} 1 & 0 & 0 & 0 \dots 0 \\ 0 & 1 & 0 & 0 \dots 0 \\ 0 & 0 & 1 & 0 \dots 0 \\ 0 & 0 & 0 & 1 \dots 0 \\ \vdots & \vdots & \vdots & \vdots \quad \vdots \\ 0 & 0 & 0 & 0 \dots 1 \end{bmatrix}$$

en ella son todos los elementos iguales a cero, excepto los de la diagonal, que son iguales a 1.
De todo lo que llevamos dicho concluimos, pues, que el conjunto de matrices $(n \times n)$ de elementos de K, $M^k_{(n \times n)}$ es un anillo unitario.
Existe entonces un isomorfismo entre el anillo de los endomorfismos de K^n, $L(K^n, K^n)$ y el anillo de las matrices $M^k_{(n \times n)}$.

9-2-3 MATRICES INVERSIBLES

Decimos que una matriz $A \in M^k_{(n \times n)}$ es inversible cuando posee elemento simétrico para la ley producto de matrices. Es decir, cuando existe otra matriz de $M^k_{(n \times n)}$ que representamos por A^{-1} tal que:

$$A \cdot A^{-1} = A^{-1} \cdot A = I_n$$

Si una matriz A es inversible, en virtud del isomorfismo existente entre los anillos $M^k_{(n \times n)}$ y $L(K^n, K^n)$, el endomorfismo que le corresponde, $f \in L(K^n, K^n)$ tendrá también un endomorfismo recíproco $f^{-1} \in L(K^n, K^n)$ tal que $[f^{-1}] = A^{-1}$ y esto es tanto como decir que f será una aplicación biyectiva. Inversamente, si una aplicación lineal $f \in L(K^n, K^n)$ es biyectiva poseerá en $L(K^n, K^n)$

un endomorfismo recíproco f^{-1}, y las matrices que corresponden a ellos $[f]$ y $[f^{-1}]$ respectivamente en virtud del isomorfismo cumplirán:

$$[f] \cdot [f^{-1}] = [f^{-1}] \cdot [f] = I_n$$

luego $[f]$ será inversible, y su matriz inversa será $[f^{-1}]$

$$[f]^{-1} = [f^{-1}]$$

Si llamamos M_n^k al conjunto de matrices inversibles de $M_{(n\times n)}^k$ podemos afirmar a la vista de lo que llevamos dicho que $(M_n^k, \cdot)$ es un grupo llamado *grupo lineal* o grupo de las matrices inversibles, que es isomorfo al grupo lineal de los automorfismos de K^n

---

EJEMPLO:

1) Sea la matriz $A = \begin{bmatrix} 1 & -1 \\ 2 & 1 \end{bmatrix}$, $A \in M_{(2\times 2)}^R$. Hallemos su matriz inversa. Sea $A^{-1} = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$

Por ser inversa: $A \cdot A^{-1} = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Luego, efectuando el producto de matrices:

$$\begin{bmatrix} 1 & -1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} \alpha_{11} - \alpha_{21} & \alpha_{12} - \alpha_{22} \\ 2\alpha_{11} + \alpha_{21} & 2\alpha_{12} + \alpha_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

e igualando término a término los dos miembros de la igualdad:

$$\left.\begin{aligned} \alpha_{11} - \alpha_{21} &= 1 \\ \alpha_{12} - \alpha_{22} &= 0 \\ 2\alpha_{11} + \alpha_{21} &= 0 \\ 2\alpha_{12} + \alpha_{22} &= 1 \end{aligned}\right\}$$

luego resolviendo el sistema:

$$\alpha_{11} = \frac{1}{3}, \quad \alpha_{12} = \frac{1}{3} \quad \alpha_{22} = \frac{1}{3} \quad \alpha_{21} = -\frac{2}{3}$$

La matriz inversa de A es, pues:

$$A^{-1} = \begin{bmatrix} 1/3 & 1/3 \\ -2/3 & 1/3 \end{bmatrix}$$

2) Sea ahora la matriz $B = \begin{bmatrix} 2 & -3 \\ 6 & -9 \end{bmatrix}$, $B \in M^{R}_{(2\times2)}$. Hallemos la matriz inversa B^{-1}.

$$\text{Sea } B^{-1} = \begin{bmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{bmatrix}$$

$$\begin{bmatrix} 2 & -3 \\ 6 & -9 \end{bmatrix} \cdot \begin{bmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

efectuando el producto e igualando, queda:

$$\left.\begin{array}{ll} (1) & 2\beta_{11} - 3\beta_{21} = 1 \\ (2) & 6\beta_{11} - 9\beta_{21} = 0 \\ (3) & 2\beta_{12} - 3\beta_{22} = 0 \\ (4) & 6\beta_{12} - 9\beta_{22} = 1 \end{array}\right\}$$

que al intentarlo resolver da:

$$\text{de (2)} \quad \beta_{11} = \frac{3}{2}\beta_{21}$$

$$\text{de (3)} \quad \beta_{12} = \frac{3}{2}\beta_{22}$$

y sustituyendo en (1) y (4):

$$\text{en (1)} \quad 2 \cdot \frac{3}{2}\beta_{21} - 3\beta_{21} = 1 \Rightarrow 3\beta_{21} - 3\beta_{21} = 1 \Rightarrow 0 \cdot \beta_{21} = 1$$

$$\text{en (4)} \quad 6 \cdot \frac{3}{2}\beta_{22} - 9\beta_{22} = 1 \Rightarrow 9\beta_{22} - 9\beta_{22} = 1 \Rightarrow 0 \cdot \beta_{22} = 1$$

lo cual indica que no hay soluciones posibles para los B. Luego el sistema que teníamos propuesto no tiene solución, y por consiguiente no existe matriz inversa B^{-1}. Entonces B es *no inversible.*

A esta matríz B, corresponde un homomorfismo $g \in L(R^2, R^2)$, que recordando la definición de matriz de una aplicación lineal cumple:

$$g(e_1) = (2, 6)$$
$$g(e_2) = (-3, -9)$$

siendo $\{e_1, e_2\}$ la base económica de R^2 y (2, 6) y (−3, −9) dos columnas de la matriz B.
Según lo que hemos visto, la familia $\{g(e_1), g(e_2)\}$ engendra el subespacio imagen, Im *(g)*. Hallemos su dimensión:

$$\alpha \cdot (2, 6) + \beta(-3, -9) = (0, 0)$$
$$(2\alpha - 3\beta, 6\alpha - 9\beta) = (0, 0)$$

de donde:

$$\left.\begin{aligned} 2\alpha - 3\beta = 0 \\ 6\alpha - 9\beta = 0 \end{aligned}\right\}$$

estas dos ecuaciones son ambas la misma, y de ellas deducimos $\alpha = \frac{3}{2} g$. Es decir, los vectores $g(e_1)$ y $g(e_2)$ son linealmente dependientes y $(2, 6) = -\frac{3}{2}(-3, -9)$

o lo que es lo mismo:

$$g(e_1) = -\frac{3}{2} g(e_2)$$

luego dm Im $(g) = 1$, o sea, Im $(g) \neq R^2$, por consiguiente g no es sobre y no es biyectiva como habíamos asegurado y pretendido al intentar calcular B^{-1}.

9-3 MATRIZ TRASPUESTA

Dada una matriz $A \in M^k_{(m \times n)}$ llamamos matriz traspuesta de ella a una matriz ${}^tA \in M^k_{(n \times m)}$ obtenida cambiando en A las filas por columnas.

Si A es:

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots\cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots\cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots\cdots & \alpha_{mn} \end{bmatrix}$$

la traspuesta de ella ${}^tA$ es:

$$ {}^tA = \begin{bmatrix} \alpha_{11} & \alpha_{21} & \cdots\cdots & \alpha_{m1} \\ \alpha_{12} & \alpha_{22} & \cdots\cdots & \alpha_{m2} \\ \vdots & \vdots & & \vdots \\ \alpha_{1n} & \alpha_{2n} & \cdots\cdots & \alpha_{mn} \end{bmatrix} $$

Si la matriz A tiene un orden $(m \times n)$, la traspuesta ${}^tA$ tiene un orden $(n \times m)$.

Consecuencias: a) "La traspuesta de una suma de dos matrices es igual a la suma de las traspuestas".

$$ {}^t(A + B) = {}^tA + {}^tB $$

En efecto, sean $A = [\alpha_{ij}]$, $B = [\beta_{ij}]$ de orden $m \times n$ y llamemos $C = A + B$ tal que $C = [\theta_{ij}]$ que será también de orden $m \times n$ y por definición de suma:

$$ \theta_{ij} = \alpha_{ij} + \beta_{ij} \quad \forall ij, \quad 1 \leqslant i \leqslant n, \quad 1 \leqslant j \leqslant m $$

Por definición de matriz traspuesta, el elemento de ${}^t\theta_{ji}$ que está en la fila j y la columna i es precisamente θ_{ij}

$$ {}^t\theta_{ji} = \theta_{ij} $$

pero también

$$ {}^t\alpha_{ji} = \alpha_{ij} \text{ y } {}^t\beta_{ji} = \beta_{ij} $$

luego sustituyendo queda

$$ {}^t\theta_{ji} = {}^t\alpha_{ji} + {}^t\beta_{ji} $$

o sea:

$$ {}^tC = {}^tA + {}^tB \Rightarrow {}^t(A + B) = {}^tA + {}^tB $$

b) Dado un escalar cualquiera del cuerpo $\alpha \in K$ y una matriz $A \in M^k_{(m \times n)}$

$$ {}^t(\alpha \cdot A) = \alpha \cdot {}^tA $$

En efecto, por definición de producto por un escalar siendo $A = [\alpha_{ij}]$,

$$\alpha \cdot [\alpha_{ij}] = [\alpha \cdot \alpha_{ij}]$$

y transponiendo queda:

$$^t[\alpha \cdot \alpha_{ij}] = [\alpha \cdot \alpha_{ji}]$$

y de nuevo por definición de producto queda:

$$^t[\alpha \cdot \alpha_{ij}] = \alpha \cdot [\alpha_{ji}]$$

pero

$$[\alpha_{ji}] = {}^t[\alpha_{ij}]$$

luego

$$^t[\alpha \cdot \alpha_{ij}] = \alpha \cdot {}^t[\alpha_{ij}]$$

pero

$$^t[\alpha \cdot \alpha_{ij}] = {}^t[\alpha \cdot A] \quad \text{y} \quad {}^t[\alpha_{ij}] = {}^tA$$

$$^t(\alpha \cdot A) = \alpha \cdot {}^tA$$

como queríamos demostrar.

c) Dadas dos matrices A y B de órdenes *(m* × *n)* y *(n* × *r)* respectivamente, se cumple:

$$^t(A \cdot B) = {}^tB \cdot {}^tA$$

En efecto: llamemos $C = A \cdot B$ de elementos $C = [\theta_{ij}]$ y orden *(m* × *r)*, y sean $A = [\alpha_{ij}]$ y $B = [\beta_{ij}]$

Teniendo en cuenta la definición de matriz traspuesta y el producto

de matrices ${}^t\theta_{ij} = \theta_{ji} = \sum_{k=1}^{n} \alpha_{jk}\, \beta_{ki} = \sum_{k=1}^{n} \beta_{ki} \cdot \alpha_{jk}$

pero, $\beta_{ki} = {}^t\beta_{ik}$ y $\alpha_{jk} = {}^t\alpha_{kj}$, y sustituyendo queda: ${}^t\theta_{ij} = \sum_{k=1}^{n} {}^t\beta_{ik} \cdot {}^t\alpha_{kj}$

pero, $\sum_{k=1}^{n} {}^t\beta_{ik} \cdot {}^t\alpha_{kj}$ no es más que el término *i,j* de la matriz producto ${}^tB \cdot {}^tA$, luego:

$${}^tC = {}^t(A \cdot B) = {}^tB \cdot {}^tA$$

como queríamos demostrar.

9-4 MATRIZ SIMETRICA

Decimos que una matriz A es simétrica si es igual a su traspuesta.

$${}^tA = A.$$

Esto significa que A y ${}^tA$ han de tener el mismo orden, luego para que una matriz sea simétrica ha de ser cuadrada y, además, si $A = [\alpha_{ij}]$ y ${}^tA = [\alpha_{ji}]$

$$\alpha_{ij} = \alpha_{ji} \quad \forall_{i,j}$$

Luego A será:

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots\cdots & \alpha_{1n} \\ \alpha_{12} & \alpha_{22} & \cdots\cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{1n}, & \alpha_{2n} & \cdots\cdots & \alpha_{nn} \end{bmatrix}$$

y en ella existe una simetría en sentido intuitivo respecto a la diagonal.

9-5 MATRIZ HEMISIMETRICA O ANTISIMETRICA

Una matriz B es antisimétrica si es igual a la opuesta de su traspuesta.

$$B = -{}^tB$$

También por esta razón una matriz antisimétrica ha de ser cuadrada y, además, si $B = [\beta_{ij}]$ y ${}^tB = [\beta_{ji}]$

Se cumplirá:

$$\beta_{ij} = -\beta_{ji} \quad \forall i,j \quad 1 \leqslant i,j \leqslant n$$

Como consecuencia, se puede observar que cuando se trate de los elementos de la diagonal, es decir, aquellos cuyas i y j coinciden β_{11}, β_{22}, ..., β_{nn}, se cumplirá: $\beta_{ii} = -\beta_{ii}$, lo que implica que

$$\beta_{ii} = 0 \quad \forall i \quad 1 \leqslant i \leqslant n$$

O sea, que la diagonal de una matriz hemisimétrica está formada por ceros.
Luego B será:

$$B = \begin{bmatrix} 0 & \beta_{12} & \beta_{13} & \cdots\cdots \beta_{1n} \\ (-\beta_{12}) & 0 & \beta_{23} & \cdots\cdots \beta_{2n} \\ (-\beta_{13}) & (-\beta_{23}) & 0 & \cdots\cdots \beta_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ (-\beta_{1n}) & (-\beta_{2n}) & (-\beta_{3n}) & \cdots\cdots \; 0 \end{bmatrix}$$

Teorema.—Toda matriz cuadrada M puede descomponerse en suma de una simétrica S y otra hemisimétrica H.
En efecto, sea:

$$M = S + H$$

tomando la traspuesta: ${}^tM = {}^tS + {}^tH$, pero como ${}^tS = S$ y ${}^tH = -H$ tenemos:

$$\left.\begin{aligned} M &= S + H \\ {}^tM &= S - H \end{aligned}\right\}$$

Despejando de estas ecuaciones H y S queda:

$$S = \frac{1}{2}(M + {}^tM)$$

$$H = \frac{1}{2}(M - {}^tM)$$

Existen, pues, dos matrices cuadradas, una simétrica S y otra hemisimétrica H que cumplen que M = S + H, que se pueden calcular aplicando la última expresión.

9-6 CAMBIO DE BASE

Hasta ahora hemos visto que fijada una base en un espacio vectorial todo vector posee asociada una matriz, fila o columna, y sólo una. Igualmente, fijadas las bases de dos espacios vectoriales, toda aplicación lineal entre ellos posee una matriz asociada y sólo una. Sin embargo, estas matrices asociadas dependen fundamentalmente de la base que se ha fijado y ocurre que un mismo vector y una misma aplicación lineal poseen varias matrices cuando se refieren a distintas bases de los espacios vectoriales en que están definidos. Por todo esto y a fin de que la representación matricial de los problemas lineales sea enteramente útil y práctica, nos conviene estudiar la relación existente entre la matriz de un vector o una aplicación lineal cuando se refieren a unas bases de los espacios vectoriales en que están definidos y la matriz que les corresponde cuando se refieren a otras bases distintas de esos mismos espacios. Este problema es el que denominaremos de "cambio de base".

9-6-1 CAMBIO DE BASE. MATRIZ DE UN VECTOR

Sea E un espacio vectorial de n dimensiones sobre K. Consideremos en E dos bases $B_E = \{u_1, ..., u_n\}$ y $B'_E = \{u'_1, ..., u'_n\}$ con unos isomorfismos asociados $\Phi_E \in L(K^n, E)$ y $\Phi'_E \in L(K^n, E)$, respectivamente. Representamos por $B_n = \{e_1, ..., e_n\}$ la base canónica de K^n. Todo vector $x \in E$ con la base B_E posee unas coordenadas $(\alpha_1, ..., \alpha_n)$. Es decir:

$$x = \alpha_1 \cdot u_1 + ... + \alpha_n \cdot u_n$$

O bien:

$$\Phi_E^{-1}(x) = (\alpha_1, ..., \alpha_n) \in K^n$$

Dada, pues, esta base, x posee asociada una matriz:

$$\{x\} = \begin{Bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{Bmatrix}$$

Si fijamos la otra base de E, la B'_E, por ejemplo, el vector x tendrá unas coordenadas $\alpha'_1, \ldots, \alpha'_n$. Es decir:

$$x = \alpha'_1 \cdot u'_1 + \ldots + \alpha'_n \cdot u'_n$$

y también:

$$\Phi_E'^{-1}(x) = (\alpha'_1, \ldots, \alpha'_n) \in K^n$$

con lo que la matriz asociada en esta base será:

$$\{x\}' = \begin{Bmatrix} \alpha'_2 \\ \vdots \\ \alpha'_n \end{Bmatrix}$$

encontremos la relación existente entre las dos matrices $\{x\}$ y $\{x\}'$. Para ello planteemos un esquema del proceso que vamos a seguir:

$$\begin{tikzcd} & E \arrow[dr, "\Phi_E'^{-1}"] & \\ k^n \arrow[ur, "\Phi_E"] \arrow[rr, "\Psi = \Phi_E'^{-1} \cdot \Phi_E"'] & & k^n \end{tikzcd}$$

Veamos cómo actúa este isomorfismo (producto de dos isomorfismos) $\Psi = \Phi_E'^{-1} \cdot \Phi_E$. Actúa de K^n en K^n, luego hallemos la imagen por Ψ de $(\alpha_1, \ldots, \alpha_n)$, coordenadas de x en la base B_E.

$$\Psi(\alpha_1, \ldots, \alpha_n) = \Phi_E'^{-1}\,[\Phi_E(\alpha_1, \ldots, \alpha_n)] = \Phi_E'^{-1}\,(x) = (\alpha'_1, \ldots, \alpha'_n)$$

luego la imagen por Ψ de las coordenadas de x en B_E son las coordenadas de x en B'_E. Escribamos la ecuación

$$\Psi(\alpha_1, \ldots, \alpha_n) = (\alpha'_1, \ldots, \alpha'_n)$$

en forma matricial (siempre podemos hacerlo como hemos visto en una consecuencia anteriormente, pues Ψ es un isomorfismo de K^n).

$$[\Psi] \cdot \begin{Bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{Bmatrix} = \begin{Bmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{Bmatrix}$$

O bien:

$$[\Psi]\,\{x\} = \{x\}'$$

Por consiguiente, resolver este problema de cambio de base es encontrar la matriz $[\Psi]$, llamada *matriz de cambio.*
Puesto que B_E y B'_E son dos bases de E, los vectores de una de ellas se pueden escribir como combinación lineal de los de la otra.
Sean:

$$u_i = \sum_{j=1}^{n} \gamma_{ji}\, u'_j \quad \forall i \quad 1 \leqslant i \leqslant n$$

entonces, para hallar $[\Psi]$ hemos de determinar las transformadas de la base canónica de K^n.

$$\Psi\,(e_i) = \Phi_E'^{-1}\,[\Phi_E\,(e_i)] = \Phi_E'^{-1}\,(u_i) = \Phi_E'^{-1}\,(\sum_{j=1}^{n} \gamma_{ji}\, u'_j)$$

como $\Phi_E'^{-1}$ es isomorfismo, se puede permutar con los escalares, y teniendo en cuenta el diagrama:

$$\Psi\,(e_i) = \sum_{j=1}^{n} \gamma_{ji} \cdot \Phi_E'^{-1}\,(u'_{ij}) = \sum_{j=1}^{n} \alpha_{ji} \cdot e_j$$

Colocando en columnas las transformadas de la base canónica B_n por Ψ tenemos la matriz buscada.

$$[\Psi] = \begin{bmatrix} \gamma_{11} & \gamma_{12} & \cdots\cdots & \gamma_{1n} \\ \gamma_{21} & \gamma_{22} & \cdots\cdots & \gamma_{2n} \\ \vdots & \vdots & & \vdots \\ \gamma_{n1} & \gamma_{n2} & \cdots\cdots & \gamma_{nn} \end{bmatrix}$$

y la ecuación de cambio de base será, pues:

$$\begin{bmatrix} \gamma_{11}, & \cdots\cdots, & \gamma_{1n} \\ \vdots & & \\ \gamma_{n1}, & \cdots\cdots, & \gamma_{nn} \end{bmatrix} \cdot \begin{Bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{Bmatrix} = \begin{Bmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{Bmatrix}$$

Analizando el significado inicial de estos γ_{ji} podemos enunciar la siguiente regla para hallar la matriz de cambio: "Para hallar la matriz de cambio $[\Psi]$ de una base B_E a otra B'_E se colocan en columna las coordenadas de los vectores de B_E expresados en la base B'_E".

Puesto que Ψ es un isomorfismo, existe el isomorfismo recíproco y la matriz inversa de $[\Psi]$. Luego:

$$[\Psi]^{-1}\,([\Psi]\cdot \}x\{) = [\Psi]^{-1}\,\}x\{'$$

en virtud de la asociativa:

$$([\Psi]^{-1}\,[\Psi])\cdot \}x\{ = [\Psi]^{-1}\,\}x\{'$$

pero $[\Psi]^{-1}\cdot[\Psi] = I_n$ luego

$$\}x\{ = [\Psi]^{-1}\,\}x\{' \qquad (18)$$

y por la misma razón, las columnas de la matriz $[\Psi]^{-1}$ serán las coordenadas de los vectores de B'_E expresados en la base B_E.

9-6-2 b) CAMBIO DE BASE. MATRIZ DE UNA APLICACION LINEAL

Sean dos espacios vectoriales E y F sobre el mismo cuerpo K de dimensiones n y m, respectivamente. Consideremos la aplicación lineal $f \in L(E, F)$.

1) Consideremos una base $B_E = \}u_1, \dots, u_n\{$ de E, y otra $B_F = \}v_1, \dots, v_m\{$ definidas por sus isomorfismos Φ_E y φ_F, respectivamente. Asociemos a $f \in L(E, F)$ su matriz en estas bases.

$$\begin{tikzcd} E \arrow[r, "f"] & F \arrow[d, "\varphi_F^{-1}"] \\ k^n \arrow[u, "\Phi_E"] \arrow[r, "\Omega = \varphi_F^{-1}\cdot f\cdot \Phi_E"'] & k^m \end{tikzcd}$$

Llamemos $\Omega = \varphi_F^{-1}\cdot f\cdot \Phi_E, \Omega \in L(K^n, K^m)$. Existe, pues, una matriz $[\Omega] \in M^k_{m\times n}$ que dijimos que era la matriz de f:

$$[f]_{\Phi_E \varphi_F} = [\Omega]$$

$$\begin{tikzcd} E \arrow[r, "f"] & F \arrow[d, "\varphi'^{-1}_F"] \\ k^n \arrow[u, "\Phi'_E"] \arrow[r, "\Pi = \varphi'^{-1}_F\cdot f\cdot \Phi'_E"'] & k^m \end{tikzcd}$$

2) Sean ahora otra base de E, $B'_E = \}u'_1, \dots, u'_n\{$ y otra base de F, $B'_F = \}v'_1, \dots, v'_m\{$ con sus isomorfismos asociados Φ'_E y φ'_F, respectivamente. Hallemos la matriz de $f \in L(E, F)$ en estas bases:

llamando a este homomorfismo resultante

$$\Pi = \varphi'^{-1}_F \cdot f \cdot \Phi'_E$$

Tenemos, por definición de una aplicación lineal:

$$[f]_{\Phi'_E \varphi'_F} = [\Pi]$$

Hallemos ahora la relación existente entre la matriz de f en las bases B_E, B_F y la matriz de f en las bases B'_E y B'_F. Para ello estudiemos la relación que existe entre Ω y Π.

Hemos visto:

$$\Omega = \varphi_F^{-1} \cdot f \cdot \Phi_E \Rightarrow f = \varphi_F \cdot \Omega \cdot \Phi_E^{-1}$$

$$\Pi = \varphi_E'^{-1} \cdot f \cdot \Phi'_E \Rightarrow f = \varphi'_F \cdot \Pi \cdot \Phi_E'^{-1}$$

Igualando éstas quedan:

$$\varphi_F \cdot \Omega \cdot \Phi_E^{-1} = \varphi'_F \cdot \Pi \cdot \Phi_E'^{-1}$$

Es decir:

$$\Omega = \varphi_F^{-1} \cdot \varphi'_F \cdot \Pi \cdot \Phi_E'^{-1} \cdot \Phi_E$$

Pero observando el diagrama 1, pág.238, vemos en el producto que tenemos la matriz de cambio del espacio E:

$$\Psi_E = \Phi_E'^{-1} \cdot \Phi_E$$

y la inversa de la matriz de cambio de F:

$$\Psi_F^{-1} = (\varphi_F'^{-1} \cdot \varphi_F)^{-1} = \varphi_F^{-1} \cdot \varphi'_F$$

luego queda finalmente:

$\Omega = \Psi_F^{-1} \cdot \Pi \cdot \Psi_E$

Matricialmente esto es:

$[\Omega] = [\Psi_F]^{-1} \cdot [\Pi] \cdot [\Psi_E]$

teniendo en cuenta que $[\Omega] = [f]_{\Phi_E \varphi_F}$ y $[\Pi] = [f]_{\Phi'_E \varphi'_F}$, queda:

$$[f]_{\Phi_E \varphi_F} = [\Psi_F]^{-1} \cdot [f]_{\Phi'_E \varphi'_F} \cdot [\Psi_E]$$

Como Ψ_E y Ψ_F son isomorfismos, también se podrá escribir:

$$[f]_{\Phi'_E \varphi'_F} = [\Psi_F] \cdot [f]_{\Phi_E \varphi_F} \cdot [\Psi_E]^{-1}$$

El problema, pues, radica en saber hallar en un espacio vectorial dado E, la matriz de cambio.

CONSECUENCIA.—En el caso de que se trate de encontrar cómo cambiar la matriz de un endomorfismo $f \in L(E, E)$ al cambiar de base en el espacio vectorial E, se tendrá que $\Psi_E = \Psi_F$, y las ecuaciones de cambio son:

$$[f]_{\Phi_E} = [\Psi_E]^{-1} \cdot [f]_{\Phi'_E} \cdot [\Psi_E]$$

$$[f]_{\Phi'_E} = [\Psi_E] \cdot [f]_{\Phi_E} \cdot [\Psi_E]^{-1}$$

EJEMPLOS: 1) Sea E un espacio vectorial de 4 dimensiones sobre R y sean $B_E = \{\vec{u}_1, u_2, u_3, u_4\}$ y $B'_E = \{u'_1, u'_2, u'_3, u'_4\}$ dos bases del mismo. Sean las coordenadas de los vectores de B_E en la base B'_E los siguientes:

$$\begin{aligned} u_1 &= 2u'_1 - u'_2 + u'_3 \\ u_2 &= u'_1 - u'_3 + u'_4 \\ u_3 &= u'_2 - u'_4 \\ u_4 &= u'_2 - 2u'_3 - 2u'_4 \end{aligned}$$

Hallemos las coordenadas en B'_E del vector $x \in E$, cuyas coordenadas en B_E son: (2, −1, 1, 1).

Según lo que hemos explicado anteriormente, el problema consiste en determinar la matriz de cambio Ψ_E de E. Para ello colocamos en columna las coordenadas de los vectores u_i en la base B'_E\

$$[\Psi_E] = \begin{bmatrix} 2 & 1 & 0 & 0 \\ -1 & 0 & 1 & 1 \\ 1 & -1 & 0 & -2 \\ 0 & 1 & -1 & -2 \end{bmatrix}$$

y ahora, operando:

$$\begin{pmatrix} \alpha_1' \\ \alpha_2' \\ \alpha_3' \\ \alpha_4' \end{pmatrix} = \begin{bmatrix} 2 & 1 & 0 & 0 \\ -1 & 0 & 1 & 1 \\ 1 & -1 & 0 & -2 \\ 0 & 1 & -1 & -2 \end{bmatrix} \begin{pmatrix} 2 \\ -1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 1 \\ -4 \end{pmatrix}$$

luego las coordenadas de x en B_E' son (3, 0, 1 —4).

2) Sean los espacios vectoriales E y F de dimensiones 3 y 2 respectivamente sobre R. Sea $B_E = (u_1, u_2, u_3,)$ una base de E y $B_F = \{v_1, v_2\}$ una base de F. Consideremos la aplicación lineal $f \in L(E, F)$ dada or:

$$\begin{aligned} f(u_1) &= 2v_1 - 4v_2 \\ f(u_2) &= 3v_1 - 6v_2 \\ f(u_3) &= v_1 - 2v_2 \end{aligned}$$

La matriz de esta aplicación lineal en estas bases es:

$$[f]_{\Phi_E, \varphi_F} = \begin{bmatrix} 2 & 3 & 1 \\ -4 & -6 & -2 \end{bmatrix}$$

Sean ahora $B_E' = \{u_1', u_2', u_3',\}$ y $B_F' = \{v_1', v_2'\}$ otras dos bases de E y F, respectivamente. Los vectores de B_E poseen unas coordenadas en B_E' dados por:

$$\begin{aligned} u_1 &= 2u_1' - u_2' + u_3' \\ u_2 &= u_1' - 2u_2' \\ u_3 &= u_2' \end{aligned} \qquad (1)$$

y los de B_F se expresan como combinación lineal de los B_F' del siguiente modo:

$$\begin{aligned} v_1 &= v_1' + 2v_2' \\ v_2 &= -v_1' + v_2' \end{aligned}$$

Hallemos la matriz de la aplicación lineal $f \in L(E, F)$ en las nuevas bases B_E' y B_F'. Para ello utilizaremos la ecuación que hemos visto anteriormente:

$$[f]_{\Phi_E' \varphi_F'} = [\Psi_F] \cdot [f]_{\Phi_E \varphi_F} \cdot [\Psi_E]^{-1}$$

Nos interesa, pues, conocer la matriz de cambio $[\Psi_F]$ de B_F a B_F'; y la inversa de la matriz de cambio $[\Psi_E]$ de B_E a B_E'.

La $[\Psi_F]$ se obtiene inmediatamente colocando en columna las coordenadas de los vectores de B_F en B'_F:

$$[\Psi_F] = \begin{bmatrix} 1 & -1 \\ 2 & 1 \end{bmatrix}$$

La $[\Psi_E]^{-1}$ es la matriz que corresponde al isomorfismo Ψ^{-1}. Si Ψ_E pasa de B_E a B'_E y, por tanto, las columnas de su matriz $[\Psi_E]$ son las coordenadas de los vectores de B_E en B'_E, Ψ_E^{-1} pasa de B'_E a B_E y las columnas de su matriz $[\Psi]^{-1}$ son las coordenadas de los vectores de B'_E en B_E.
Hallemos las coordenadas de los vectores B'_E en B_E a partir del sistema (1):

$$\begin{aligned} u'_1 &= u_2 + 2u_3 \\ u'_2 &= u_3 \\ u'_3 &= u_1 - 2u_2 - 3u_3 \end{aligned}$$

luego

$$[\Psi_E]^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -2 \\ 2 & 1 & -3 \end{bmatrix}$$

Entonces la matriz $[f]_{\Phi'_E, \varphi'_F}$ que buscamos aplicando será:

$$[f]_{\Phi'_E; \varphi'_F} = [\Psi_F] \cdot [f]_{\Phi_E\, \varphi_F} \cdot [\Psi_E]^{-1} = \begin{bmatrix} 1 & -1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 & 1 \\ -4 & -6 & -2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -2 \\ 2 & 1 & -3 \end{bmatrix}$$

Haciendo el segundo producto queda:

$$[f]_{\Phi'_E\, \varphi'_F} = \begin{bmatrix} 1 & -1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 5 & 1 & -7 \\ -10 & -2 & 14 \end{bmatrix}$$

y, finalmente:

$$[f]_{\Phi'_E, \varphi'_F} = \begin{bmatrix} 15 & 3 & -21 \\ 0 & 0 & 0 \end{bmatrix}$$

TEMA 10 FUNCIONES MULTILINEALES

10-1 FUNCIONES MULTILINEALES

Definición: Dado un espacio vectorial E sobre el cuerpo K, llamamos función r-lineal sobre E a una aplicación

$$f = E^r \to K$$

tal que $\forall\ (v_1, \ldots, v_r) \in E^r\ \exists^*\ k \in K \mid f(v_1, \ldots, v_r) = k$

que es lineal para cada uno de los r espacios vectoriales E que definen en $E^r = \underbrace{E \times E \times E \ldots, \times E}_{r}$. Es decir:

$$\forall\, i \quad 1 \leqslant i \leqslant r, \quad \forall\, \alpha, \beta \in K, \quad \forall\, v_1, v_2, \ldots, v_i, \ldots, v_r, u_i \in E$$

$$f(v_1, v_2, \ldots, v_{i-1}, (\alpha \cdot v_i + \beta \cdot u_i), v_{i+1}, \ldots, v_r) =$$

$$= \alpha \cdot f(v_1, v_2, \ldots, v_i, \ldots, v_r) + \beta \cdot f(v_1, v_2, \ldots, u_i, \ldots, v_r)$$

Caso particular: En particular, podemos tomar como espacio vectorial E el propio cuerpo K. En este caso

$$f: K^r \to K$$

$$\forall\ (\alpha_1, \ldots, \alpha_r) \in K^r \quad \exists^*\ k \in K \mid f(\alpha_1, \ldots, \alpha_r) = k$$

es una función r-lineal también, si cumple la condición que hemos ya enunciado de ser lineal en cada uno de los r espacios vectoriales K de K^r.

10-1-1 CONSECUENCIAS

Sea E un espacio vectorial de n dimensiones sobre K y sea $f: E^r \to K$ una función r-lineal.

a) $\forall (v_1, ..., v_r) \in E^r \ \forall \alpha_1, ..., \alpha_r \in K$

$$f(\alpha_1 \cdot v_1, ..., \alpha_r \cdot v_r) = \alpha_1 \cdot \alpha_2, ..., \alpha_r \cdot f(v_1, ..., v_r)$$

La demostración de este resultado es inmediata, procediendo por recurrencia.

Como f es r-lineal, se cumple:

$$f(\alpha_1 \cdot v_1, \alpha_2 \cdot v_2, ..., \alpha_r \cdot v_r) = \alpha_1 \cdot f(v_1, \alpha_2 \cdot v_2, ..., \alpha_r \cdot v_r)$$

también, ahora:

$$f(v_1, \alpha_2 \cdot v_2, ..., \alpha_r \cdot v_r) = \alpha_2 \cdot f(v_1, v_2, \alpha_3 \cdot v_3, ..., \alpha_r \cdot v_r)$$

por tanto, sustituyendo, queda:

$$f(\alpha_1 \cdot v_1, \alpha_2 \cdot v_2, ..., \alpha_r \cdot v_r) = \alpha_1 \cdot \alpha_2 \cdot f(v_1, v_2, \alpha_3 \cdot v_3, ..., \alpha_r \cdot v_r)$$

es decir, que se cumple, pues, para $i = 1$ y para $i = 2$. Supongamos que es cierto para $i = r - 1$, y vamos a demostrarlo para $i = r$.

En virtud de que es cierto para $i = r - 1$ se cumple:

$$f(\alpha_1 \cdot v_1, \alpha_2 \cdot v_2, ..., \alpha_{r-1} \cdot v_{r-1}, \alpha_r \cdot v_r) = \alpha_1 \cdot \alpha_2, ..., \alpha_{r-1} \cdot f(v_1, v_2, ..., v_{r-1}, \alpha_r \cdot v_r)$$

y como f es r-lineal

$$f(v_1, v_2, ..., v_{r-1}, \alpha_r \cdot v_r) = \alpha_r \cdot f(v_1, v_2, ..., v_{r-1}, v_r)$$

luego

$$f(\alpha_1 \cdot v_1, ..., \alpha_r \cdot v_r) = \alpha_1, ..., \alpha_r \cdot f(v_1, ..., v_r).$$

como queríamos demostrar.

b) Si los r vectores v_i, $1 \leqslant i \leqslant r$ son combinación lineal de p vectores $u_1, u_2, \ldots, u_p \in E$, se expresarán:

$$v_1 = \sum_{j_1=1}^{p} \alpha_{j_1 1}\, u_{j_1} = \alpha_{11}\, u_1 + \alpha_{21}\, u_2 + \alpha_{31}\, u_3 + \ldots + \alpha_{p1}\, u_p$$

$$v_2 = \sum_{j_2=1}^{p} \alpha_{j_2 2}\, u_{j_2} = \alpha_{12}\, u_1 + \alpha_{22}\, u_2 + \alpha_{32}\, u_3 + \ldots + \alpha_{p2}\, u_p$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$v_r = \sum_{j_r=1}^{p} \alpha_{j_r r}\, u_{j_r} = \alpha_{1r}\, u_1 + \alpha_{2r}\, u_2 + \alpha_{3r}\, u_r + \ldots + \alpha_{pr}\, u_p$$

entonces $f(v_1, \ldots, v_r)$ se expresará:

$$f(v_1, \ldots, v_r) = f\Big(\sum_{j_1=1}^{p} \alpha_{j_1 1}\, u_{j_1}, \ldots, \sum_{j_r=1}^{p} \alpha_{j_r r} \cdot u_{j_r} \Big) = \sum_{j_1=1}^{p} \ldots \sum_{j_r=1}^{p} \alpha_{j_1 1} \ldots \alpha_{j_r r}\; f(u_{j_1}, \ldots, u_{j_r})$$

que también podemos escribir así:

$$f(v_1, \ldots, v_r) = \sum_{j_1, \ldots, j_r=1}^{p} \alpha_{j_1 1}, \ldots, \alpha_{j_r r} \cdot f(u_{j_1}, \ldots, u_{j_r})$$

En efecto, vamos a demostrarlo también por recurrencia:

Para $i = 1$ $\quad v_1 = \sum_{j_1=1}^{p} \alpha_{j_1 1}\, u_{j_1}$

$$f\Big(\sum_{j_1=1}^{p} \alpha_{j_1 1} \cdot u_{j_1}, v_2, v_3, \ldots, v_r \Big) = \sum_{j_1=1}^{p} \alpha_{j_1 1} \cdot f(u_{j_1}, v_2, v_3, \ldots, v_r)$$

en virtud de que f es r-lineal.
Para $i = 2$

$$f\Big(\sum_{j_1=1}^{p} \alpha_{j_1 1}\, u_{j_1}, \sum_{j_2=1}^{p} \alpha_{j_2 2}\, u_{j_2}, v_3, v_4, \ldots, v_r \Big) = \sum_{j_1=1}^{p} \alpha_{j_1 1}\, f\Big(u_{j_1}, \sum_{j_2=1}^{p} \alpha_{j_2 2}\, u_{j_2}, v_3, \ldots, v_r\Big)$$

y del mismo modo que antes:

$$f\Big(u_{j_1}, \sum_{j_2=1}^{p} \alpha_{j_2 2}, u_{j_2}, v_3, \ldots, v_r\Big) = \sum_{j_2=1}^{p} \alpha_{j_2 2}\, f(u_{j_1}, u_{j_2}, v_3, \ldots, v_r)$$

sustituyendo este resultado en la expresión inicial para que $i = 2$, se obtiene finalmente:

$$f\left(\sum_{j_1=1}^{p} \alpha_{j_1 1} \quad u_{j_1}, \sum_{j_2=1}^{p} \alpha_{j_2 2} \quad u_{j_2}, v_3, \dots, v_r\right) = \sum_{j_1=1}^{p} \sum_{j_2=1}^{p} \alpha_{j_1 1} \alpha_{j_2 2} f(u_{j_1}, u_{j_2}, v_3, \dots, v_r)$$

Supongamos que se cumple para $i = r - 1$ y vamos a demostrarlo para $i = r$. Así, pues, por hipótesis:

$$f\left(\sum_{j_1=1}^{p} \alpha_{j_1 1} \; u_{j_1}, \sum_{j_2=1}^{p} \alpha_{j_2 2} \quad u_{j_2}, \dots, \sum_{j_{r-1}=1}^{p} \alpha_{j_{r-1} r-1} \; u_{jr-1}, \sum_{j_r=1}^{p} \alpha_{j_r r} \; u_{j_r}\right) =$$

$$= \sum_{j_1, j_2, \dots, j_{r-1}=1}^{p} \alpha_{j_1 1} \quad \alpha_{j_2 2}, \dots, \alpha_{j_{r-1} r-1} \; f\left(u_{j_1}, u_{j_2}, \dots, u_{jr-1}, \sum_{j_r=1}^{p} \alpha_{j_r r} \; u_{j_r}\right)$$

como f es r-lineal:

$$f\left(u_{j_1}, u_{j_2}, \dots, u_{jr-1}, \sum_{j_r=1}^{p} \alpha_{j_r r} \, u_{jr}\right) = \sum_{j_r=1}^{p} \alpha_{j_r r} \, f(u_{j_1}, \dots, u_{jr})$$

Sustituyendo este resultado en la expresión anterior queda, finalmente, lo que deseamos demostrar:

$$f\left(\sum_{j_1=1}^{p} \alpha_{j_1 1} \quad u_{j_1}, \dots, \sum_{j_r=1}^{p} \alpha_{j_r r} \quad u_{jr}\right) = \sum_{j_1, j_2, \dots, j_r = 1}^{p} \alpha_{j_1 1} \; \alpha_{j_2 2}, \dots, \alpha_{j_r r} \, f(u_{j_1}, \dots, u_{j_r})$$

10-1-2 EXPRESION EN UNA BASE

Supongamos que $B = \{e_1, \dots, e_n\}$ sea una base del espacio vectorial E. Entonces, cada vector $v_1, \dots, v_r$ se puede escribir como combinación lineal de la misma:

$$v_i = \sum_{j_i=1}^{n} \alpha_{j_i i} \, e_{j_i} \quad \forall i \quad 1 \leq i \leq r$$

donde los $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_n}$ son las n coordenadas del vector v_i en la base B.

De acuerdo con lo que hemos visto en la consecuencia *(b)* podemos escribir:

$$f(v_1, \dots, v_r) = \sum_{j_1, \dots, j_r = 1}^{n} \alpha_{j_1 1}, \dots, \alpha_{j_r r} \quad f(e_{j_1}, e_{j_2}, \dots, e_{j_r})$$

Así, pues, de acuerdo con esto, la imagen por medio de una aplicación r-lineal, $f: E^r \to K$ de cualquier conjunto ordenado de r vectores depende sólo de las imágenes que da esta f de todos los conjuntos ordenados de r vectores de una base cualquiera de E que podemos formar. Esto soluciona, en cierto modo, el problema de la *determinación unívoca de una aplicación r-lineal.* En general, para conocer unívocamente una aplicación es necesario conocer su grafo, es decir, cuál es la imagen de cada elemento del conjunto original. De acuerdo con esto, en el caso que nos ocupa, para conocer f deberíamos conocer cuál es la imagen de cada elemento de E^r, o sea, de cada conjunto ordenado de r vectores de E. Ahora bien, hemos visto que las imágenes de los conjuntos ordenados de r vectores de E dependen solamente de las imágenes de los conjuntos ordenados,de r vectores de una base de E,que se puedan formar. Por consiguiente, "una aplicación r-lineal f, queda unívocamente determinada cuando conocemos todos los escalares

$$f(e_{j_1}, \dots, e_{j_r}) \quad \forall j_i \quad 1 \leqslant j_i \leqslant n \quad \forall_i \quad 1 \leqslant i \leqslant r$$

El número de escalares que definen la aplicación r-lineal será igual, pues, al número de conjuntos de r vectores que se pueden formar con $\{e_1, \dots, e_n\}$ y éstos no son mas que las variaciones con repetición de n elementos tomados de r en r: $V'^r_n = n^r$. Necesitamos, por consiguiente, n^r escalares de K para definir $f: E^r \to K$.

EJEMPLO:

Sea el espacio vectorial $E = R^3$ sobre el cuerpo R. Vamos a definir una aplicación 2-lineal, tambien llamada bilineal, $f: (R^3 \times R^3) \to R$.
Según lo que hemos explicado en 10-1-2 tomemos una base de R; por ejemplo la canónica $B = \{e_1, e_2, e_3\}$. Para definir esta aplicación bilineal necesitamos $3^2 = 9$ escalares. Sean éstos, por ejemplo:

$$\begin{array}{lll} f(e_1, e_1) = 1 & f(e_1, e_2) = -1 & f(e_1, e_3) = 2 \\ f(e_2, e_1) = 0 & f(e_2, e_2) = 1 & f(e_2, e_3) = -1 \\ f(e_3, e_1) = 1 & f(e_3, e_2) = -2 & f(e_3, e_3) = 1 \end{array}$$

Tomemos un par de vectores de R^3 cualesquiera. Por ejemplo, $v_1 = (1, 2, -3)$ y $v_2 = (1, 0, -4)$. Hallemos la imagen por f del par $(v_1, v_2) \in R^3 \times R^3$:
Expresando v_1 y v_2 en función de B, las α_{j_i} serán:

$$\left.\begin{array}{l} v_1 = 1\,e_1 + 2\,e_2 - 3\,e_3 \\ v_2 = 1\,e_1 + 0 \cdot e_2 - 4 \cdot e_3 \end{array}\right\} \begin{array}{l} \alpha_{11} = 1; \alpha_{21} = 2; \alpha_{31} = -3 \\ \alpha_{12} = 1; \alpha_{22} = 0; \ \alpha_{32} = -4 \end{array}$$

Entonces, de acuerdo con lo establecido para la expresión de $f(v_1\ v_2)$ en una base:

$$f(v_1, v_2) = \sum_{j_1=1}^{3} \cdot \sum_{j_2=1}^{3} \alpha_{j_1 1}\ \alpha_{j_2 2}\ \cdot f(e_{j_1}, e_{j_2}) = \sum_{j_1=1;\ j_2=1}^{3} \alpha_{j_1 1}\ \alpha_{j_2 2}\ f(e_{j_1}, e_{j_2})$$

Desarrollando este sumatorio queda:

$$\begin{aligned} f(v_1, v_2) = {} & \alpha_{11}\ \alpha_{12}\ f(e_1\ e_1) + \alpha_{11}\ \alpha_{22}\ f(e_1\ e_2) + \alpha_{11}\ \alpha_{32}\ f(e_1\ e_3) + \\ & + \alpha_{21}\ \alpha_{12}\ f(e_2\ e_1) + \alpha_{21}\ \alpha_{22}\ f(e_2\ e_2) + \alpha_{21}\ \alpha_{32}\ f(e_2\ e_3) + \\ & + \alpha_{31}\ \alpha_{12}\ f(e_3\ e_1) + \alpha_{31}\ \alpha_{22}\ f(e_3\ e_2) + \alpha_{31}\ \alpha_{32}\ f(e_3\ e_3) \end{aligned}$$

y sustituyendo cada elemento que aparece por sus valores numéricos queda:

$$\begin{aligned} f(v_1, v_2) = {} & 1 \cdot 1 \cdot 1 + 1 \cdot 0 \cdot (-1) + 1 \cdot (-4) \cdot 2 + 2 \cdot 1 \cdot 0 + 2 \cdot 0 \cdot 1 + \\ & + 2 \cdot (-4) \cdot (-1) + (-3) \cdot 1 \cdot 1 + (-3) \cdot 0 \cdot (-2) + (-3) \cdot (-4) \cdot 1 = \\ = {} & 1 + 0 - 8 + 0 + 0 + 8 - 3 + 0 + 12 = 10 \end{aligned}$$

Ha quedado, pues, unívocamente definida la imagen de cualquier par de elementos (v_1, v_2) de $R^3 \times R^3$.

10-2 FUNCION r-LINEAL ALTERNADA

Decimos que una función r-lineal, $f: E^r \to K$, es alternada cuando cumple:

$$\text{Si } v_i = v_j \Rightarrow f(v_1, v_2, \ldots, v_i, \ldots, v_j, \ldots, v_r) = 0 \quad \forall\, v_1, v_2, \ldots, v_r \in E$$

Es decir, cuando la imagen de cualquier conjunto de r vectores en que se repite alguno de ellos es el 0 de K.

10-2-1 CONSECUENCIAS

Sea E un espacio vectorial de n dimensiones sobre K, y sea $f: E^r \to K$ una función r-lineal alternada. Entonces:

a) Si $(v_1, v_2, \ldots, v_i, \ldots, v_j, \ldots, v_r)$ es un conjunto cualquiera de r vectores de E, cuya imagen es

$$f(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_r) = \lambda$$

al cambiar dos vectores cualesquiera entre sí en este conjunto ordenado, la imagen es el opuesto de λ

$$f(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_r) = -\lambda$$

Vamos a demostrarlo. Por ser f alternada se cumple que:

$$f(v_1, \ldots (v_i + v_j), \ldots (v_i + v_j), \ldots, v_r) = 0$$

teniendo en cuenta que f es lineal queda:

$$f(v_1, \ldots, (v_i + v_j), \ldots (v_i + v_j), \ldots, v_r) = f(v_1, \ldots, v_i, \ldots, v_i, \ldots, v_r)$$
$$+ f(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_r) + f(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_r) + f(v_1, \ldots, v_j, \ldots, v_j, \ldots, v_r) = 0$$

Como f es alternada,

$$f(v_1, \ldots, v_i, \ldots, v_i, \ldots, v_r) = f(v_1, \ldots, v_j, \ldots, v_j, \ldots, v_r) = 0$$

luego queda, finalmente:

$$f(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_r) + f(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_r) = 0$$

Es decir:

$$f(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_r) = -f(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_r)$$

como queríamos demostrar.

b) Si $N = \{v_1, \ldots, v_r\}$ es una familia ligada de vectores de E, entonces,

$$f(v_1, \ldots, v_r) = 0$$

En efecto, si N es una familia ligada de vectores, habrá uno, al menos, que se podrá escribir como combinación lineal de los demás. Supongamos, por ejemplo, que v_1 sea combinación lineal:

$$v_1 = \sum_{i=2}^{r} \beta_i v_i$$

Entonces:

$$f(v_1, \ldots, v_r) = f\left(\sum_{i=2}^{r} \beta_i v_i, v_2, \ldots, v_r\right)$$

Como f es lineal:

$$f(v_1, \ldots, v_r) = \sum_{i=2}^{r} \beta_i f(v_i, v_2, \ldots, v_r)$$

y en este último sumatorio, como la i varía desde 2 hasta r, en cada sumando la $f(v_i, v_2, \ldots, v_r)$ será igual a cero, ya que siempre se repetirán dos de ellos, luego:

$$f(v_1, \ldots, v_r) = 0$$

c) Si la función r-lineal que hemos definido sobre E (n dimensional), es tal que r es estrictamente mayor que n, entonces

$$r > n \quad \forall (v_1, \ldots, v_r) \in \mathrm{E}^r \quad f(v_1, \ldots, v_r) = 0$$

En efecto, si r es mayor que la dimensión n del espacio vectorial E, cualquier familia con r vectores será una familia ligada por definición de dimensión y, por tanto, en virtud de *(b)*:

$$f(v_1, \ldots, v_r) = 0$$

En virtud, pues, de la consecuencia *(c)* que acabamos de ver, sólo se consideran funciones r-lineales alternadas sobre E de n dimensiones, que tengan $r \leqslant n$. Nosotros restringiremos, sin embargo, y desde ahora hasta el final del tema sólo consideraremos funciones r-lineales alternadas que verifiquen $r = n$; se llamarán, por consiguiente, funciones n-lineales alternadas.

10-2-2 EXPRESION EN UNA BASE

Sea E el espacio vectorial de n dimensiones definido sobre K que venimos considerando, y sea f una función n-lineal alternada definida sobre E.

$$f: \mathrm{E}^n \to \mathrm{K}$$

$$\forall\ (v_1, \ldots, v_n) \in \mathrm{E}^n, \quad f(v_1, \ldots, v_n) \in \mathrm{K}$$

Según hemos visto, dada una base $\mathrm{B} = \{e_1, \ldots, e_n\}$ de E, para tener unívocamente definida f nos hacen falta los n^n escalares $f(e_{j_1}, \ldots, e_{j_n})$, donde $j_1, \ldots, j_n \in \mathrm{N}$ toman todos los valores desde 1 a n.

Si las coordenadas de los vectores v_i $1 \leqslant i \leqslant n$, en B son:

$$v_i = \sum_{j_i=1}^{n} \alpha_{j_i i}\, e_{j_i}$$

según la expresión de f en la base B será:

$$f(v_1, \ldots, v_n) = \sum_{j_1, \ldots, j_n=1}^{n} \alpha_{j_1 1}, \ldots, \alpha_{j_n n}\, f(e_{j_1}, \ldots, e_{j_n})$$

sumatorio que, según lo que hemos dicho más arriba, posee n^n sumandos.

Vamos ahora a tener en cuenta el hecho de que la función f es alternada. Entonces, siempre que sean iguales dos o más elementos $j_1, \ldots, j_n$ en un sumando, esto significará que en $f(e_{j_1}, \ldots, e_{j_n})$ hay dos o más vectores iguales y, por consiguiente, la imagen de ese conjunto de vectores será el $0 \in \mathrm{K}$. Luego sólo serán distintos de cero aquellos sumandos cuyos subíndices $j_1, \ldots, j_n$ sean todos distintos. Por tanto, si los $e_{j_1}, \ldots, e_{j_n}$ han de ser distintos y sólo hay n vectores $\{e_1, \ldots, e_n\}$, esto equivale a agrupar estos n elementos de todas las maneras posibles de n en n. Es decir, formar las permutaciones de los n elementos. El número de permutaciones de n elementos es, como sabemos, $n!$ luego no son necesarios n^n escalares para definir unívocamente una función n-lineal alternada, sino que, de momento, hemos visto que $n!$ escalares serán suficientes, ya que los otros $n^n - n!$ son todos nulos.

Sigamos ahora para tratar de darle una expresión más sencilla.

Tenemos, pues, un conjunto de n índices $j_1, ..., j_n$ distintos con valores de 1 a n. Según lo que acabamos de decir, $j_1, ..., j_n$ no es más que el resultado de haber permutado entre sí los elementos $1, 2, 3, ..., n$. Llamemos σ a esta permutación. σ será una permutación del grupo simétrico S_n (grupo de las permutaciones de n elementos). En la notación de teoría de aplicaciones decimos:

$$\begin{aligned} j_1 &= \sigma(1) \\ j_2 &= \sigma(2) \\ &\vdots \\ j_n &= \sigma(n) \end{aligned}$$

Entonces $f(v_1, ..., v_n)$ quedará así:

$$f(v_1, ..., v_n) = \sum_{\sigma \in S_n} \alpha_{\sigma(1)1}\ \alpha_{\sigma(2)2},\ ...,\ \alpha_{\sigma(n)n} \cdot f(e_{\sigma(1)}, e_{\sigma(2)}, ..., e_{\sigma(n)})$$

Pero según vimos en el tema de permutaciones, toda permutación puede escribirse como un producto de trasposiciones. Puesto que la acción de una trasposición se concreta en cambiar dos elementos entre sí, esto significa que tras actuar una trasposición cambia solamente el signo de la imagen (consecuencia *a)*).
Si, por ejemplo, tenemos la trasposición $\tau_{12} \in S_n$ $(\tau_{12}(1) = 2,\ \tau_{12}(2) = 1,\ \tau_{12}(i) = i\ \forall_i\ 3 \leqslant i \leqslant n)$, tendremos:

$$f(e_{\tau_{12}(1)}, e_{\tau_{12}(2)}, ..., e_{\tau_{12}(n)}) = f(e_2, e_1, e_3, ..., e_n) = -f(e_1, e_2, ..., e_n)$$

Entonces, el actuar una permutación cualquiera sobre $12 \ldots n$ equivale a cambiar el signo de $f(e_1, e_2, ..., e_n)$ tantas veces como trasposiciones contiene σ. Llamando al número de trasposiciones de σ, $\operatorname{sgn}(\sigma)$ (signatura de σ), habrá que cambiar el signo de $f(e_1, ..., e_n)$ un número de veces igual a $\operatorname{sgn}(\sigma)$, y entonces:

$$f(e_{\sigma(1)}, ..., e_{\sigma(n)}) = (-1)^{\operatorname{sgn}(\sigma)} \cdot f(e_1, ..., e_n)$$

llamando a $(-1)^{\operatorname{sgn}(\sigma)}$ *paridad* de σ.
Par. $(\sigma) = (-1)^{\operatorname{sgn}(\sigma)}$, luego

$$f(e_{\sigma(1)}, ..., e_{\sigma(n)}) = \text{Par.}\ (\sigma) \cdot f(e_1, ..., e_n)$$

y la ecuación de $f(v_1, ..., v_n)$ queda finalmente:

$$f(v_1, ..., v_n) = \sum_{\sigma \in S_n} \alpha_{\sigma(1)1}, ..., \alpha_{\sigma(n)n} \cdot \text{Par.}(\sigma) \cdot f(e_1, ..., e_n)$$

Este sumatorio posee $n!$ sumandos correspondientes a los $n!$ permutaciones de S_n. En esta ecuación vemos que la imagen de cualquier conjunto de n vectores $(v_1, ..., v_n) \in E^n$ depende de las coordenadas de estos vectores en una base B dada y del escalar $f(e_1, ..., e_n)$ imagen del conjunto ordenado $(e_1, ..., e_n)$, que toma la base B. Por consiguiente, podemos concluir que "para definir de una forma única una función n-lineal alternada basta con dar un solo escalar".

Y a la inversa se puede demostrar el teorema siguiente:

Teorema 1: Dado el espacio vectorial E de n dimensiones sobre K y una base cualquiera de él, $B = \{e_1, ..., e_n\}$, para todo escalar $\delta \in K$ existe una y solo una función n-lineal alternada f tal que:

$$f(e_1, ..., e_n) = \delta$$

(Explicación del teorema en la pág. 255.)

EJEMPLO:

Vamos a definir una función trilineal alternada en el espacio vectorial R^3.
Para construir una $f: R^3 \to R$ alternada y trilineal, según hemos visto en teoría sólo necesitamos un escalar, $f(e_1, e_2, e_3) \in R$, siendo $\{e_1, e_2, e_3\}$ una base de R^3.
Tomemos por ejemplo la base canónica de R^3 $\{(1, 0, 0,), (0, 1, 0), (0, 0, 1)\}$ y sea el escalar que necesitamos $f(e_1, e_2, e_3) = 2$. Según lo que hemos dicho queda así unívocamente definida f. Calculemos $f(v_1, v_2, v_3)$, siendo

$$v_1 = (2, -1, -3) = 2 \cdot e_1 - 1 \cdot e_2 - 3\, e_3$$
$$v_2 = (1, -2, \ \ 1) = 1\, e_1 - 2\, e_2 + 1\, e_3$$
$$v_3 = (2, -2, -3) = 2\, e_1 - 2\, e_2 - 3\, e_3$$

y según vimos:

$$f(v_1, v_2, v_3) = \sum_{\sigma \in S_3} \alpha_{\sigma(1)1} \cdot \alpha_{\sigma(2)2} \cdot \alpha_{\sigma(3)3} \cdot \text{Par.}(\sigma) \cdot f(e_1, e_2, e_3)$$

El grupo simétrico S_3 tiene 6 permutaciones que ya estudiamos en su día en el tema correspondiente.

$$\begin{aligned}
\sigma_1\ (1,2,3) &= (1,2,3)\\
\sigma_2\ (1,2,3) &= (2,3,1)\\
\sigma_3\ (1,2,3) &= (3,1,2)\\
\sigma_4\ (1,2,3) &= (1,3,2)\\
\sigma_5\ (1,2,3) &= (2,1,3)\\
\sigma_6\ (1,2,3) &= (3,2,1)
\end{aligned}$$

y hallando sus paridades respectivas.

$\text{Par.}\ (\sigma_1) = (-1)^0 = 1$

$\text{Par.}\ (\sigma_2) = \text{Par.}\ (\tau_{13}) \cdot \text{Par.}\ (\tau_{12}) = (-1) \cdot (-1) = 1$

$\text{Par.}\ (\sigma_3) = \text{Par.}\ (\tau_{13}) \cdot \text{Par.}\ (\tau_{32}) = (-1) \cdot (-1) = 1$

$\text{Par.}\ (\sigma_4) = \text{Par.}\ (\tau_{23}) = -1$

$\text{Par.}\ (\sigma_5) = \text{Par.}\ (\tau_{12}) = -1$

$\text{Par.}\ (\sigma_6) = \text{Par.}\ (\tau_{13}) = -1$

luego:

$$\begin{aligned}
f(v_1\ v_2\ v_3) = [&\alpha_{11} \cdot \alpha_{22} \cdot \alpha_{33} \cdot \text{Par.}\ (\sigma_1) + \alpha_{21} \cdot \alpha_{32} \cdot \alpha_{13} \cdot \text{Par.}\ (\sigma_2) +\\
+\ &\alpha_{31} \cdot \alpha_{12} \cdot \alpha_{23} \cdot \text{Par.}\ (\sigma_3) + \alpha_{11} \cdot \alpha_{32} \cdot \alpha_{23} \cdot \text{Par.}\ (\sigma_4) +\\
+\ &\alpha_{21} \cdot \alpha_{12} \cdot \alpha_{33} \cdot \text{Par.}\ (\sigma_5) + \alpha_{31} \cdot \alpha_{22} \cdot \alpha_{13} \cdot \text{Par.}\ (\sigma_6)] \cdot f(e_1\ e_2\ e_3)
\end{aligned}$$

Con todo esto podemos hallar ya $f(v_1, v_2, v_3)$, sin más que observar que siempre α_{ij} es la coordenada j del vector i en la base B:

$$\begin{aligned}
\alpha_{11} &= 2 & \alpha_{12} &= -1 & \alpha_{13} &= -3\\
\alpha_{21} &= 1 & \alpha_{22} &= -2 & \alpha_{23} &= 1\\
\alpha_{31} &= 2 & \alpha_{32} &= -2 & \alpha_{33} &= -3
\end{aligned}$$

Colocando los valores numéricos y calculando da: $f(v_1, v_2, v_3) = 14$.

Nota: Damos a continuación la demostración del teorema 1 de la página 253.

Teorema.—Dado el espacio vectorial E de n dimensiones sobre el cuerpo K y una base cualquiera de él $B = \{e_1\ e_2\ ..., e_n\}$, para todo escalar $\delta \in K$ existe una y solo una función n-lineal alternada f, tal que:

$$f(e_1, e_2, ..., e_n) = \delta \qquad (1)$$

En efecto. La unicidad de la función n-lineal alternada definida por (1), cuando existe, es evidente, como ya se ha visto.
Veamos que siempre existe al menos una función n-lineal alternada que cumpla (1). Para ello definimos una aplicación de E^n en K del siguiente modo:

$$f : E^n \rightarrow K$$

$$(2) \quad \forall (v_1, v_2, ..., v_n) \in E^n$$

$$f(v_1, v_2, ..., v_n) = \sum_{\sigma \in S_n} \alpha_{\sigma(1),1} \cdot \alpha_{\sigma(2),2}, ..., \alpha_{\sigma(n),n} \cdot \text{Par}(\sigma) \cdot \delta$$

siendo $\alpha_{\sigma(1)1}$ la coordenada $\sigma(1)$-ésima del vector v_1 en B; $\alpha_{\sigma(2)2}$ la coordenada $\sigma(2)$-ésima del vector v_2 en B; y $\alpha_{\sigma(n)n}$ la coordenada $\sigma(n)$-ésima del vector v_n en B. Par (σ) la paridad de la permutación de S_n correspondiente y δ el escalar dado por la hipótesis del teorema (1).

Demostremos que f definida de este modo es lineal y alternada.

1) f es lineal.

Tomemos un vector $u \in E$ que expresado en la base B será: $u = \sum_{j=i}^{n} \beta_j e_j$.

$$(v_i + u) = \sum_{j=i}^{n} (\alpha_{ji} + \beta_j) e_j \qquad \forall i \qquad 1 \leqslant i \leqslant n$$

y hallemos $f(v_1, v_2, ..., (v_i + u), ..., v_n)$, según la definición que hemos dado de f.

$$f(v_1, v_2, ... (v_i + u), ..., v_n) =$$

$$= \sum_{\sigma\in S_n} \alpha_{\sigma(1)1} \cdot \alpha_{\sigma(2)2} \cdot \ldots \cdot (\alpha_{\sigma(i)i} + \beta_{\sigma(i)}) \cdot \ldots \cdot \alpha_{\sigma(n)n} \cdot \mathrm{Par}(\sigma) \cdot \delta =$$

$$= \sum_{\sigma\in S_n} \alpha_{\sigma(1)1} \ldots \alpha_{\sigma(i)i} \ldots \alpha_{\sigma(n)n} \cdot \mathrm{Par}(\sigma) \cdot \delta + \sum_{\sigma\in S_n} \alpha_{\sigma(1)1} \ldots \beta_{\sigma(i)} \ldots \alpha_{\sigma(n)n} \cdot \mathrm{Par}(\sigma) \cdot \delta$$

$$= f(v_1, v_2, \ldots, v_i, \ldots, v_n) + f(v_1, v_2, \ldots, u, \ldots, v_n) \quad \forall_i \quad 1 \leqslant i \leqslant n$$

Demostremos la otra condición de n-linealidad:

$$\forall\, \gamma \in K \qquad \gamma \cdot v_i = \sum_{j=1}^{n} (\gamma \cdot \alpha_{ji}) \cdot e_j \qquad \forall_i \qquad 1 \leqslant i \leqslant n$$

Entonces:

$$f(v_1, v_2, \ldots, (\gamma \cdot v_i), \ldots, v_n) = \sum_{\sigma\in S_n} \alpha_{\sigma(i)i} \ldots (\gamma \cdot \alpha_{\sigma(i)i}) \cdot \ldots \alpha_{\sigma(n)n} \cdot \mathrm{Par}(\sigma) \cdot \delta =$$
$$= \gamma \cdot \sum_{\sigma\in S_n} \alpha_{\sigma(1)1} \ldots \alpha_{\sigma(i)i} \ldots \alpha_{\sigma(n)n} \cdot \mathrm{Par}(\sigma) \cdot \delta = \gamma \cdot f(v_1, v_2, \ldots, v_i, \ldots, v_n)$$

2) *f es alternada.*

Consideremos una trasposición $\tau = (i,j)$, $\tau \in S_n$, donde tomamos $i < j$.
Se trata de demostrar que:

$$f(v_1, v_2, \ldots, v_i, \ldots, v_j, \ldots, v_n) = 0 \quad \text{si} \quad v_i = v_j$$

Para ello, llamemos $S'_n \subset S_n$ al conjunto de todas las permutaciones σ, $\sigma \in S_n$, tales que $\sigma(i) < \sigma(j)$, y llamemos $S''_n \subset S_n$ al conjunto de las $\sigma \in S_n$ que cumplen $\sigma(i) > \sigma(j)$. Es evidente de esta definición que:

$$S_n = S'_n \cup S''_n \qquad S'_n \cap S''_n = \phi \qquad (3)$$

Dada una $\sigma' \in S'_n$, formemos la permutación producto $(\sigma' \cdot \tau) \in S_n$, siendo $\tau = (i,j)$. Veamos si esta nueva permutación pertenece a S'_n o a S''_n.

$$\sigma''(i) = (\sigma' \cdot \tau)(i) = \sigma'(\tau(i)) = \sigma'(j)$$

$$\sigma''(j) = (\sigma' \cdot \tau)(j) = \sigma'(\tau(j)) = \sigma'(i)$$

$$\sigma''(k) = (\sigma' \cdot \tau)(k) = \sigma'(\tau(k)) = \sigma'(k) \quad \forall\, k \neq i,j;\ 1 \leqslant k \leqslant n$$

Como $\sigma'(i) < \sigma'(j)$ por ser $\sigma' \in S'_n$, entonces $\sigma''(i) > \sigma''(j)$, luego $\sigma'' \in S''_n$.
Por otra parte, para toda $\sigma' \in S'_n$ existe siempre una $\sigma'' = \sigma' \cdot \tau$, $\sigma'' \in S''_n$ y esta es única, puesto que S_n es un grupo.
Se puede por consiguiente establecer una aplicación biyectiva:

$$\varphi : S'_n \to S''_n$$

$$\forall\ \sigma' \in S'_n \quad \varphi(\sigma') = \sigma'' = \sigma' \cdot \tau$$

Por otra parte, y teniendo en cuenta (3), podemos reescribir (2) del siguiente modo:

$$f(v_1, v_2, \ldots, v_i, \ldots, v_j, \ldots, v_n) = \sum_{\sigma' \in S'_n} \alpha_{\sigma'(1)1} \ldots \alpha_{\sigma'(i)i} \ldots \alpha_{\sigma'(j)j} \ldots \alpha_{\sigma'(n)n} \cdot \text{Par}(\sigma') \cdot \delta +$$
$$+ \sum_{\sigma'' \in S''_n} \alpha_{\sigma''(1)1} \ldots \alpha_{\sigma''(i)i} \ldots \alpha_{\sigma''(j)j} \ldots \alpha_{\sigma''(n)n} \cdot \text{Par}(\sigma'') \cdot \delta \qquad (4)$$

Para probar que f es alternada, supongamos que $v_i = v_j$. Teniendo en cuenta la relación existente entre σ' y σ'':

$$\alpha_{\sigma'(i)i} \cdot \alpha_{\sigma'(j)j} = \alpha_{\sigma''(j)i} \cdot \alpha_{\sigma''(i)j} \qquad (5)$$

Ahora bien, $\alpha_{\sigma''(j)i}$ es la coordenada $\sigma''(j)$-ésima del vector v_i, y como por hipótesis $v_i = v_j$, ésta será igual a la misma coordenada $\sigma''(j)$-ésima del vector v_j:

$$\alpha_{\sigma''(j)i} = \alpha_{\sigma''(j)j}$$

Por la misma razón:

$$\alpha_{\sigma''(i)j} = \alpha_{\sigma''(i)i}$$

Entonces la ecuación (5) queda:

$$\alpha_{\sigma'(i)i} \cdot \alpha_{\sigma'(j)j} = \alpha_{\sigma''(i)i} \cdot \alpha_{\sigma''(j)j}$$

Como por otro lado sabemos que:

$$\alpha_{\sigma'(k)k} = \alpha_{\sigma''(k)k} \quad \forall\ k \neq i,j \quad 1 \leqslant k \leqslant n$$

queda:

$$\alpha_{\sigma'(1)1} \cdot \alpha_{\sigma'(2)2} \cdot \dots \alpha_{\sigma'(i)i} \dots \alpha_{\sigma'(j)j} \dots \alpha_{\sigma'(n)n} =$$

$$= \alpha_{\sigma''(1)1} \cdot \alpha_{\sigma''(2)2} \dots \alpha_{\sigma''(i)i} \dots \alpha_{\sigma''(j)j} \dots \alpha_{\sigma''(n)n}$$

Como: Par (σ'') = Par $(\sigma' \cdot \tau)$ = Par (σ') · Par $(\tau,)$ = – Par (σ'), de donde:

$$\alpha_{\sigma'(1)1} \dots \alpha_{\sigma'(i)i} \dots \alpha_{\sigma'(j)j} \dots \alpha_{\sigma'(n)n} \cdot \text{Par } (\sigma') \cdot \delta +$$

$$+ \ \alpha_{\sigma''(1)1} \dots \alpha_{\sigma''(i)i} \dots \alpha_{\sigma''(j)j} \dots \alpha_{\sigma''(n)n} \cdot \text{Par } (\sigma'') \cdot \delta = 0$$

Y esto sucede para cada par de sumandos, uno del primer sumatorio y otro del segundo en la ecuación (4), correspondientes a unos σ' y σ'', tales que:

$$\sigma'' = \sigma' \cdot \tau$$

Pero como hemos dicho que existe una aplicación biyectiva $\varphi\colon S'_n \to S''_n$, por cada σ' de S'_n, existe una y sólo una σ'' de S''_n, tal que $\sigma'' = \sigma' \cdot \tau$, y por cada σ'' de S''_n existe a su vez una y sólo una σ' de S'_n, tal que $\sigma'' = \sigma' \cdot \tau$. Luego cada sumando del primer sumatorio de (4) se anula con uno del segundo sumatorio y solamente con uno. Por consiguiente:

$$f(v_1\ v_2 \dots v_i \dots v_j \dots v_n) = 0$$

como deseábamos demostrar.

TEMA 11 | DETERMINANTES

11-1 DEFINICION

Dado un espacio vectorial E de n dimensiones sobre K, llamamos determinante de n vectores del mismo, $(v_1, \ldots, v_n)$, o función determinante de los mismos en una base $B = \{e_1, \ldots, e_n\}$ a la imagen de este conjunto de n vectores por la aplicación n-lineal alternada f definida en E por $f(e_1, \ldots, e_n) = 1$. Lo representaremos por:

$$\text{det.}\ (v_1, \ldots, v_n) = |(v_1, \ldots, v_n)|$$

EJEMPLO:

Para los tres vectores (v_1, v_2, v_3) del último ejemplo del tema 10 su función determinante en la base canónica se hallará tomando $f(e_1, e_2, e_3) = 1$ en vez de 2 como habíamos tomado arbitrariamente.
Como $f(e_1, e_2, e_3)$ aparece en todos los sumandos, basta con dividir el resultado que habíamos obtenido allí por 2, quedando:

$$|(v_1, v_2, v_3)| = \frac{14}{2} = 7$$

11-2 DETERMINANTE DE UNA MATRIZ *(n × n)*

Sea una matriz A de orden *(n × n)* de elementos del cuerpo K.

$$A = \begin{bmatrix} \alpha_{11} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots\cdots & \alpha_{nn} \end{bmatrix}$$

Las columnas de A son vectores de K^n, que podemos denominar $v_1, \ldots, v_n$

$$\begin{array}{l} v_1 = (\alpha_{11}, \alpha_{21}, \ldots\ldots, \alpha_{n1}) \\ \vdots \\ v_n = (\alpha_{1n}, \alpha_{2n}, \ldots\ldots, \alpha_{nn}) \end{array}$$

Puesto que las coordenadas de estos vectores en la base canónica de K^n, son los mismos escalares de K que los definen, podemos establecer una aplicación n-lineal alternada $f: K^n \to K$, $f(e_1, \ldots, e_n) = 1$.

Entonces *llamamos determinante de la matriz A y lo representaremos por det. (A) ó $|A|$ al determinante de los vectores columna de la matriz*

$$\det.(A) = |A| = |(v_1, \ldots, v_n)| = \sum_{\sigma \in S_n} \alpha_{\sigma(1)1}, \ldots, \alpha_{\sigma(n)n} \cdot \text{Par.}(\sigma)$$

EJEMPLOS:

1) Calculemos el determinante de la matriz

$$A = \begin{pmatrix} 2 & 1 & 2 \\ -1 & -2 & -2 \\ -3 & 1 & -3 \end{pmatrix} \quad \text{sus vectores columna son:} \quad \begin{array}{l} v_1 = (2, -1, -3) \\ v_2 = (1, -2, \ \ 1) \\ v_3 = (2, -2, -3) \end{array}$$

entonces: $|A| = |(v_1, v_2, v_3)|$

pero (v_1, v_2, v_3) son los vectores del ejemplo anterior, por tanto:

$$|A| = 7$$

2) Tomemos una matriz (2×2) de elementos de K, y vamos a tratar de obtener una regla práctica para calcular su determinante.

Sea

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$$

Según hemos definido, $|A|$ será:

$$|A| = \sum_{\sigma \in S_n} \alpha_{\sigma(1)1} \cdot \alpha_{\sigma(2)2} \cdot \text{Par. } (\sigma)$$

En S_2 sólo hay dos permutaciones; la idéntica $\sigma(1, 2) = (1, 2)$ y la trasposición τ_{12}, $\tau_{12}\ (1, 2) = (2, 1)$. Fácilmente vemos que:

$$\text{Par. } (\sigma) = +1 \quad \text{Par. } (\tau_{12}) = -1$$

luego:

$$|A| = \alpha_{11}\ \alpha_{22} - \alpha_{12} \cdot \alpha_{21}$$

que en la matriz, gráficamente, equivale a multiplicar los dos elementos unidos por la raya continua a restarle los dos unidos por la discontinua

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$$

3) Tomemos una matriz cualquiera (3×3) y hagamos lo mismo que en el ejemplo 2.

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix}$$

y según sabemos, el determinante de esta matriz será:

$$|A| = \alpha_{11} \cdot \alpha_{22} \cdot \alpha_{33} + \alpha_{12} \cdot \alpha_{23} \cdot \alpha_{31} + \alpha_{13} \cdot \alpha_{21} \cdot \alpha_{32}$$
$$- \alpha_{11} \cdot \alpha_{23} \cdot \alpha_{32} - \alpha_{12} \cdot \alpha_{21} \cdot \alpha_{33} - \alpha_{13} \cdot \alpha_{22} \cdot \alpha_{31}$$

$$\begin{array}{ccc} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{array} \qquad \qquad \begin{array}{ccc} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{array}$$

quedando como regla práctica: multiplicar entre sí los tres elementos unidos por la raya continua poniéndoles signo +, y a éstos restarles los tres productos obtenidos al multiplicar entre sí los que están unidos por la raya discontinua.

Teorema 1: Dada una matriz $A \in M^k_{(n \times n)}$ el determinante de la matriz traspuesta de A, ${}^tA$ es igual al determinante de A.

$$|{}^tA| = |A|$$

En efecto: sea $A = [\alpha_{ij}]$ y sea ${}^tA = [\theta_{ij}]$ la matriz traspuesta de A. Es decir:

$$\theta_{ij} = \alpha_{ji} \quad \forall_{i,j} \in \{1, ..., n\}$$

Según la definición dada de determinante de una matriz

$$|{}^tA| = \sum_{\sigma \in S_n} \theta_{\sigma(1)1}, ..., \theta_{\sigma(n)n} \cdot \text{Par. } (\sigma)$$

Puesto que S_n es un grupo, para cada $\sigma \in S_n$ existe $\sigma^{-1} \in S_n$ tal que si $\sigma(i) = x_i$ $\forall i$ $1 \leqslant i \leqslant n$, entonces $i = \sigma^{-1}(x_i)$ y podemos, pues, escribir:

$$\theta_{\sigma(1)1} \dots \theta_{\sigma(n)n} = \theta_{x_1 \sigma^{-1}(x_1)} \dots \theta_{x_n \sigma^{-1}(x_n)}$$

Como σ es una permutación, $x_1, ..., x_n$ son los elementos $1, 2, 3, ..., n$ escritos en un orden distinto. Podemos, pues, reordenar los factores del segundo miembro por el primer subíndice obteniendo:

$$\theta_{\sigma(1)1} \cdot \theta_{\sigma(2)2} \dots \theta_{\sigma(n)n} = \theta_{1\sigma^{-1}(1)} \cdot \theta_{2\sigma^{-1}(2)} \dots \theta_{n\sigma^{-1}(n)}$$

Por otro lado sabemos que $\sigma \cdot \sigma^{-1} = \sigma^{-1} \cdot \sigma = I$. Luego la paridad de σ^{-1} será tal que:

$$\text{Par. } (\sigma) \cdot \text{Par. } (\sigma^{-1}) = +1$$

Es decir: $\text{Par. } (\sigma) = \text{Par. } (\sigma^{-1})$

y podemos escribir:

$$|^tA| = \sum_{\sigma \in S_n} \theta_{1\sigma^{-1}(1)} \cdot \theta_{2\sigma^{-1}(2)}, \ldots, \theta_{n\sigma^{-1}(n)} \cdot \text{Par. } (\sigma^{-1})$$

Al recorrer σ todo S_n la σ^{-1} también lo recorre todo, y entonces podemos sustituir en el sumatorio σ por σ^{-1}.

$$|^tA| = \sum_{\sigma^{-1} \in S_n} \theta_{1\sigma^{-1}(1)} \cdot \theta_{2\sigma^{-1}(2)}, \ldots, \theta_{n\sigma^{-1}(n)} \cdot \text{Par. } (\sigma^{-1})$$

Podemos designar σ^{-1} con la letra γ, puesto que ahora sólo designa un índice que toma valores en un conjunto y quedará:

$$|^tA| = \sum_{\gamma \in S_n} \theta_{1\gamma(2)} \cdot \theta_{2\gamma(2)}, \ldots, \theta_{n\gamma(n)} \cdot \text{Par. } (\gamma)$$

Recordando ahora que por hipótesis $\theta_{ij} = \alpha_{ji}$

$$|^tA| = \sum_{\gamma \in S_n} \theta_{1\gamma(1)}, \ldots, \theta_{n\gamma(n)} \cdot \text{Par. } (\gamma) = \sum_{\gamma \in S_n} \alpha_{\gamma(1)1}, \ldots, \alpha_{\gamma(n)n} \cdot \text{Par. } (\gamma) = |A|$$

como queríamos demostrar.
De aquí podemos afirmar que "el determinante de una matriz A es igual al determinante de sus vectores fila o al de sus vectores columna".

11-3 PROPIEDADES DE LOS DETERMINANTES

Vamos a considerar algunas propiedades de los determinantes, que se desprenden rápidamente del hecho de que son funciones multilineales alternadas:

1) Sea la matriz

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots\ldots & (\alpha_{1i} + \beta_1) & \ldots\ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots\ldots & (\alpha_{2i} + \beta_2) & \ldots\ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \alpha_{n2} & \ldots\ldots & (\alpha_{ni} + \beta_n) & \ldots\ldots & \alpha_{nn} \end{bmatrix}$$

Veamos que se cumple que:

$$|A| = \left|\begin{bmatrix} \alpha_{11} & \cdots\cdots & \alpha_{1i} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots \\ \alpha_{n1} & \cdots\cdots & \alpha_{ni} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| + \left|\begin{bmatrix} \alpha_{11} & \cdots\cdots & \beta_{1} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots \\ \alpha_{n1} & \cdots\cdots & \beta_{n} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right|$$

En efecto, llamando $v_1 = (\alpha_{1i}, \ldots, \alpha_{ni})$ $\forall_i$ $1 \leqslant i \leqslant n$ y $u = (\beta_1, \ldots, \beta_n)$, esto se puede escribir así:

$$|(v_1, v_2, \ldots, (v_i + u), \ldots, v_n)|$$

y como la función determinante es lineal queda:

$$|(v_1, v_2, \ldots, (v_i + u), \ldots, v_n)| = |(v_1, v_2, \ldots, v_i, \ldots, v_n)| + |(v_1, v_2, \ldots, u, \ldots, v_n)|$$

como deseábamos establecer.

2)

$$\left|\begin{bmatrix} \alpha_{11} & \cdots\cdots & \beta \cdot \alpha_{1i} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots \\ \alpha_{n1} & \cdots\cdots & \beta \cdot \alpha_{ni} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| = \beta \cdot \left|\begin{bmatrix} \alpha_{11} & \cdots\cdots & \alpha_{1i} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots \\ \alpha_{n1} & \cdots\cdots & \alpha_{ni} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right|$$

En efecto, en la notación anterior será:

$$|(v_1, v_2, \ldots, \beta \cdot v_i, \ldots, v_n)|$$

y como la función determinante es lineal, queda:

$$|(v_1, v_2, \ldots, \beta \cdot v_i, \ldots, v_n)| = \beta \cdot |(v_1, v_2, \ldots, v_i, \ldots, v_n)|$$

con lo que podemos enunciar: "Si se multiplica una fila o columna de una matriz por en escalar, el determinante de la matriz que resulta es igual al de la matriz que teníamos multiplicado por dicho escalar".

3) Si

$$A = \begin{bmatrix} \alpha_{11} & \cdots\cdots & \alpha_{1i} & \cdots\cdots & \alpha_{1e} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \alpha_{n1} & \cdots\cdots & \alpha_{ni} & \cdots\cdots & \alpha_{ne} & \cdots\cdots & \alpha_{nn} \end{bmatrix}$$

y $(\alpha_{1i}, ..., \alpha_{ni}) = (\alpha_{1e}, ..., \alpha_{ne})$ para dos valores cualesquiera de i y e pertenecientes a $\{1, 2, ..., n\}$ entonces:

$$|A| = 0$$

En efecto, ya que esto significa:

$$|(v_1, ..., v_i, ..., v_e, ..., v_n)| \text{ con}$$

$v_i = v_e$ y por ser la función determinante alternada:

$$|(v_1, ..., v_i, ..., v_e, ..., v_n)| = 0 \quad \text{si } v_i = v_e$$

que podemos enunciar así: "Si una matriz tiene dos filas o columnas iguales, su determinante es igual a cero".

4) "Si permutamos entre sí dos filas o columnas de una matriz, el determinante de la matriz que resulta es el opuesto".

En efecto, ya que por ver alternada la función determinante:

$$|(v_1, ..., v_i, ... v_e, ..., v_n)| = -|(v_1, ..., v_e, ..., v_i, ..., v_n)|$$

5) "Si a una fila o columna de una matriz se le suma otra multiplicada por un escalar, el determinante de la matriz que resulta es el mismo".

$$|(v_1, ..., v_i, ..., (v_j + \beta \cdot v_i), ..., v_n)| = |(v_1, ..., v_i, ..., v_j, ..., v_n)|$$

En efecto, por ser lineal:

$$|(v_1, ..., v_i, ..., (v_j + \beta \cdot v_i), ..., v_n)| = |(v_1, ..., v_i, ..., v_j, ..., v_n)| + \beta \cdot |(v_1, ..., v_j, ..., v_j, ..., v_n)|$$

y en virtud de la propiedad 3.ª

$$\beta \cdot |(v_1, ..., v_i, ..., v_i, ..., v_n)| = 0$$

Teorema 4.—Si A y B son dos matrices de $M^k_{(n \times n)}$, el determinante de la matriz producto $(A \cdot B)$ es igual al producto de los determinantes de A y B.

$$|A \cdot B| = |A| \cdot |B|$$

En efecto, sea $A = [\alpha_{ij}]$ y $B = [\beta_{ij}]$, o también, llamando:

$$v_i = (\alpha_{1i}, \dots, \alpha_{ni})$$
$$u_i = (\beta_{1i}, \dots, \beta_{ni})$$

$$\forall i \quad 1 \leqslant i \leqslant n \quad A = [v_1, \dots, v_n] \quad y \quad B = [u_1, \dots, u_n]$$

Teniendo en cuenta la definición del producto de matrices, tendremos:

$$A \cdot B = [A \cdot u_1, \dots, A \cdot u_n]$$

ya que por ejemplo la columna i de la matriz $A \cdot B$ será

$$\left(\sum_{e=1}^{n} \alpha_{1e}\, \beta_{ei}, \dots, \sum_{e=1}^{n} \alpha_{ne}\, \beta_{ei}\right)$$

pero esto no son más que las coordenadas de $(A \cdot u_i)$ como queríamos comprobar.
Vamos ahora a fijar la matriz A y definir con ello una aplicación

$$\theta : K^n \to K$$

tal que

$$\forall\, (u_1, \dots, u_n) \in K^n, \theta\, (u_1, \dots, u_n) = |\, (A \cdot u_1, \dots, A \cdot u_n)\, | = |\, A \cdot B\, |$$

Por estar θ definida a partir de la función determinante de los n vectores $(A \cdot u_1, \dots, A \cdot u_n)$ es n-lineal y alternada y por consiguiente para que quedase unívocamente definida bastaría conocer el escalar $\theta\, (e_1, \dots, e_n)$ siendo $\{e_1, \dots, e_n\}$ la base canónica de K^n.

Por definición:

$$\theta\, (e_1, \dots, e_n) = |\, (A\, e_1, \dots, A\, e_n)\, | = |\, A \cdot I_n\, | = |\, A\, |$$

(ya que la matriz que tiene por columnas los vectores de la base canónica de K^n es la matriz unidad).
Entonces θ está perfectamente definida, y por ello tendremos:

$$|\, A \cdot B\, | = \theta\, (u_1, \dots, u_n) = \sum_{\sigma \in S_n} \beta_{\sigma(1)1}, \dots, \beta_{\sigma(n)n} \cdot \text{Par}\, (\sigma) \cdot |\, A\, |$$

Pero este último sumatorio, excepto $|A|$, no es mas que el determinante de B, y por tanto:

$$|A \cdot B| = |A| \cdot |B|$$

11-4 DEFINICION DE MENOR Y ADJUNTO

Sea una matriz $A \in M^k_{(n \times n)}$. Llamamos "menor *(i,j)*" de A, donde $1 \leq i \leq n$, $1 \leq j \leq n$, al determinante de la matriz de orden $(n-1) \times (n-1)$ que resulta al suprimir la *i*-esima fila y la *j*-esima columna de A. Se llama "adjunto *(i,j)*" Δ_{ij} de A a $(-1)^{i+j}$ por el menor *(i,j)* de A.

Teorema 5.—Sea $A = [\alpha_{ij}]$, $A \in M^k_{(n \times n)}$. Veamos que se cumple que:

$$\left|\begin{bmatrix} 1 & \alpha_{12} & \alpha_{13} & \cdots\cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \alpha_{23} & \cdots\cdots & \alpha_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & \alpha_{n2} & \alpha_{n3} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| = \left|\begin{bmatrix} \alpha_{22} & \cdots\cdots & \alpha_{2n} \\ \vdots & & \vdots \\ \alpha_{n2} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| = \Delta_{11}$$

En efecto, sabemos que

$$|A| = \sum_{\sigma \in S_n} \alpha_{\sigma(1)1} \cdot \ldots, \alpha_{\sigma(n)n} \cdot \text{Par}(\sigma)$$

Sin embargo, lo que tenemos en el enunciado no es la matriz A, sino una matriz obtenida de A sustituyendo la primera columna por el vector e_1 (1, 0, 0, ..., 0). Luego $\alpha_{\sigma(1)1}$ es igual a 1 si $\sigma(1) = 1$ y es igual a cero si $\sigma(1) \neq 1$. Entonces tenemos por un lado que el sumatorio solo quedará extendido a aquellos $\sigma \in S_n$ tales que $\sigma(1) = 1$ y por otro que no es necesario escribir el factor $\alpha_\sigma(1)1$, puesto que para todos los $\sigma \in S_n$ a los cuales se extiende el sumatorio es $\alpha_{\sigma(1)1} = 1$. Y así el determinante de la matriz inicial será

$$\left|\begin{bmatrix} 1 & \alpha_{12} & \cdots\cdots & \alpha_{1n} \\ 0 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & \alpha_{n2} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| = \sum_{\substack{\sigma \in S_n \\ (\sigma(1) = 1)}} \alpha_{\sigma(2)2} \cdot \cdots\cdots \cdot \alpha_{\sigma(n)n} \cdot \text{Par}(\sigma)$$

Las permutaciones que aparecen en este sumatorio, sabemos que son aplicaciones biyectivas sobre el conjunto $\{1, 2, \ldots, n\}$ tales que $\sigma(1) = 1$. Para cada $\sigma \in S_n$, tal que $\sigma(1) = 1$, existe una permutación $\sigma' \in S_{n-1}$ tal que sea restricción de σ al conjunto $\{2, \ldots, n\}$. Es decir, $\sigma(i) = \sigma'(i) \, \forall i \in \{2, \ldots, n\}$. También es cierta la recíproca de esta afirmación, es decir, que para toda $\sigma' \in S_{n-1}$ existe una $\sigma \in S_n$, prolongación de σ', tal que $\sigma(1) = 1$. De acuerdo con esto:

$$\left|\begin{bmatrix} 1 & \alpha_{12} & \cdots\cdots & \alpha_{1n} \\ 0 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & \alpha_{n2} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| = \sum_{\sigma' \in S_{n-1}} \alpha_{\sigma'(2)2} \cdot \cdots\cdots \cdot \alpha_{\sigma'(n)n} \cdot \operatorname{Par}(\sigma')$$

y esto no es sino el desarrollo del determinante

$$\left|\begin{bmatrix} \alpha_{22} & \cdots\cdots & \alpha_{2n} \\ \vdots & & \vdots \\ \alpha_{n2} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| = \Delta_{11}$$

Luego si tenemos una matriz cuya primera columna es $(1, 0, \ldots, 0)$, el determinante de la misma es igual al de la matriz que resulta de suprimir en aquella la primera fila y la primera columna.

Corolario.—Sea como antes $A = [\alpha_{ij}]$, $A \in M^{k}_{(n \times n)}$. Veamos que se cumple:

$$\begin{array}{cc} & \begin{array}{c} \text{columna } j \\ \downarrow \end{array} \\ \text{fila } i \longrightarrow & \left|\begin{bmatrix} \alpha_{11} & \cdots\cdots & \alpha_{1(j-1)} & 0 & \alpha_{1(j+1)} & \cdots\cdots & \alpha_{1n} \\ \vdots & & & 0 & & & \\ \vdots & & & \vdots & & & \\ \alpha_{i1} & \cdots\cdots & \alpha_{i(j-1)} & 1 & \alpha_{i(j+1)} & \cdots\cdots & \alpha_{in} \\ \vdots & & & & & & \\ \alpha_{n1} & \cdots\cdots & \alpha_{n(j-1)} & 0 & \alpha_{n(j+1)} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| = \Delta_{ij} \end{array}$$

En efecto, teniendo en cuenta la propiedad que nos permite permutar columnas vamos a pasar la columna j hasta la primera, permutándola cada vez con la anterior. En total habremos de permutar las columnas de la matriz $(j-1)$ veces luego.

$$|(v_1,\dots,v_{j-1},e_j,v_{j+1},\dots,v_n)| = (-1)^{j-1}\left|\begin{bmatrix} 0 & \alpha_{11} & \cdots\cdots & \alpha_{1(j-1)} & \alpha_{1(j+1)} & \cdots\cdots & \alpha_{1n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & \alpha_{(i-1)1} & \cdots\cdots & \alpha_{(i-1)(j-1)} & \alpha_{(i-1)(j+1)} & \cdots\cdots & \alpha_{(i-1)n}\\ 1 & \alpha_{i1} & \cdots\cdots & \alpha_{i(j-1)} & \alpha_{i(j+1)} & \cdots\cdots & \alpha_{in}\\ 0 & \alpha_{(i+1)1} & \cdots\cdots & \alpha_{(i+1)(j-1)} & \alpha_{(i+1)(j+1)} & \cdots\cdots & \alpha_{(i+1)n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & \alpha_{n1} & \cdots\cdots & \alpha_{n(j-1)} & \alpha_{n(j-1)} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right|$$

Subamos ahora la fila i hasta la primera, con lo que aparecerá un factor $(-1)^{i-1}$, ya que permutaremos entre sí las filas de la matriz $(i-1)$ veces.

$$|(v_1,\dots,v_{j-1},e_j,v_{j+1},\dots,v_n)| = (-1)^{j-1}\cdot(-1)^{i-1}\cdot \begin{array}{c} \text{Falta la columna } j \\ \left|\begin{bmatrix} 1 & \alpha_{i1} & \cdots\cdots & \alpha_{i(j-1)} & \alpha_{i(j+1)} & \cdots\cdots & \alpha_{in}\\ 0 & \alpha_{11} & \cdots\cdots & \alpha_{1(j-1)} & \alpha_{1(j+1)} & \cdots\cdots & \alpha_{1n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & \alpha_{(i-1)1} & \cdots\cdots & \alpha_{(i-1)(j-1)} & \alpha_{(i-1)(j+1)} & \cdots\cdots & \alpha_{(i-1)n}\\ 0 & \alpha_{(i+1)1} & \cdots\cdots & \alpha_{(i+1)(j-1)} & \alpha_{(i+1)(j+1)} & \cdots\cdots & \alpha_{(i+1)n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & \alpha_{n1} & \cdots\cdots & \alpha_{n(j-1)} & \alpha_{n(j+1)} & \cdots\cdots & \alpha_{nn} \end{bmatrix}\right| \end{array} \begin{array}{l}\text{Falta la}\\ \text{fila } i\end{array}$$

y en virtud ahora del teorema 5:

$$|(v_1,\dots,e_j,\dots,v_n)| = (-1)^{i+j-2}\cdot[\text{menor } (i,j)] = $$
$$= (-1)^{i+j}[\text{menor } (i,j)] = \Delta_{ij}$$

Teorema 6.—Desarrollo de un determinante por los elementos de una fila o por los de una columna. Dada la matriz $A = [\alpha_{ij}]$ $A \in M^k_{(n\times n)}$ se tiene:

1) Fijado una j, $1 \leqslant j \leqslant n$ (desarrollo por los elementos de la columna j).

$$|A| = \alpha_{1j}\,\Delta_{1j} +,\dots,+\,\alpha_{nj}\cdot\Delta_{nj}$$

2) Fijado un i, $1 \leqslant i \leqslant n$ (desarrollo por los elementos de la fila i).

$$|A| = \alpha_{i1}\,\Delta_{i1} + \dots + \alpha_{in}\cdot\Delta_{in}$$

Demostremos la primera parte del teorema. Para ello consideremos un j fijo.

$$v_j = \sum_{i=1}^{n} \alpha_{ij}\cdot e_i$$

$$|(v_1, \ldots, v_j, \ldots, v_n)| = |(v_1, \ldots, \sum_{i=1}^{n} \alpha_{ij}\, e_i, \ldots, v_n)| = \sum_{i=1}^{n} \alpha_{ij}\, |(v_1, \ldots, e_i, \ldots, v_n)|$$

y veamos ahora que

columna j

$$|(v_1, \ldots, e_i, \ldots, v_n)| = \Delta_{ij}$$

En efecto, lo es por el colorario anterior.

Luego:

$$|(v_1, \ldots, v_n)| = \sum_{i=1}^{n} \alpha_{ij}\, \Delta_{ij} = \alpha_{1j}\, \Delta_{1j} +, \ldots, + \alpha_{nj}\, \Delta_{nj}$$

como queríamos demostrar.

Para demostrar 2) basta con tomar la matriz traspuesta ${}^tA$ de A, que sabemos tiene el mismo determinante que A. Entonces el determinante de ${}^tA$ (que es el de A) se puede desarrollar como acabamos de ver por los elementos de la columna i de ${}^tA$. Pero los elementos de la columna i de ${}^tA$ no son más que los de la fila i de A. Con lo cual queda probada la posibilidad de desarrollos de $|A|$ por los elementos de una fila i de A como:

$$|A| = \sum_{k=1}^{n} \alpha_{ik}\, \Delta_{ik}$$

EJEMPLO:

Vamos a hallar el determinante de la matriz

$$A = \begin{bmatrix} 1 & 2 & 1 & 1 \\ 2 & 2 & -1 & 0 \\ -1 & 2 & 1 & -1 \\ 1 & -1 & 3 & 0 \end{bmatrix}$$

desarrollándolo por los elementos de la tercera columna.

$$|A| = 1 \cdot \Delta_{13} + (-1)\, \Delta_{23} + 1 \cdot \Delta_{33} + 3 \cdot \Delta_{43}$$

$$\Delta_{13} = (-1)^{1+3} \cdot \left| \begin{bmatrix} 2 & 2 & 0 \\ -1 & 2 & -1 \\ 1 & -1 & 0 \end{bmatrix} \right| = -4$$

$$\Delta_{23} = (-1)^{2+3} \cdot \left| \begin{bmatrix} 1 & 2 & 1 \\ -1 & 2 & -1 \\ 1 & -1 & 0 \end{bmatrix} \right| = +4$$

$$\Delta_{33} = (-1)^{3+3} \cdot \left| \begin{bmatrix} 1 & 2 & 1 \\ 2 & 2 & 0 \\ 1 & -1 & 0 \end{bmatrix} \right| = -4$$

$$\Delta_{43} = (-1)^{4+3} \cdot \left| \begin{bmatrix} 1 & 2 & 1 \\ 2 & 2 & 0 \\ -1 & 2 & -1 \end{bmatrix} \right| = -8$$

$$|A| = 1 \cdot -4 + (-1) \cdot 4 + 1 \cdot (-4) + 3 \cdot (-8) = -36$$

11-5 MATRIZ ADJUNTA. DEFINICION

Sea $A = [\alpha_{ij}]$ una matriz *(n × n)*. Se llama matriz adjunta de A, a una matriz $\tilde{A} \in M^k_{(n \times n)}$ cuyo elemento *(i,j)*, $\tilde{\alpha}_{ij}$ es igual al adjunto Δ_{ji} de A.

$$\tilde{\alpha}_{ij} = \Delta_{ji}$$

Teorema 7.—Dada la matriz $A \in M^k_{(n \times n)}$ se cumple que:

$$A \cdot \tilde{A} = \tilde{A} \cdot A = |A| \cdot I_n$$

En efecto, llamemos $B = A \cdot \tilde{A}$ y $B = [\beta_{ij}]$

Demostremos que los elementos de la diagonal principal de B son todos iguales a $|A|$ y que los demás elementos de B son iguales a cero.

$$\beta_{ii} = \sum_{k=1}^{n} \alpha_{ik} \cdot \bar{\alpha}_{ki} = \sum_{k=1}^{n} \alpha_{ik} \cdot \Delta_{ik}$$

pero este último elemento es como sabemos el resultado de desarrollar el determinante de A por los elementos de la fila *i*. Luego:

$$\beta_{ii} = |A|$$

Veamos ahora β_{ij} con $i \neq j$

$$\beta_{ij} = \sum_{k=1}^{n} \alpha_{ik} \cdot \bar{\alpha}_{kj} = \sum_{k=1}^{n} \alpha_{ik} \cdot \Delta_{jk}$$

Para demostrar que esto es igual a cero tomemos una matriz $C = [\theta_{ij}]$ de orden $(n \times n)$, cuyos elementos sean iguales a los de A excepto los de la fila *j*, que serían iguales a la fila *i* de A.

es decir:

$$C = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots\cdots & \alpha_{1n} \\ \vdots & \vdots & & \vdots \\ \alpha_{i1} & \alpha_{i2} & \cdots\cdots & \alpha_{in} \\ \vdots & \vdots & & \vdots \\ \alpha_{i1} & \alpha_{i2} & \cdots\cdots & \alpha_{in} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots\cdots & \alpha_{nn} \end{bmatrix} \begin{array}{l} \\ \\ \rightarrow \text{fila } i \\ \\ \rightarrow \text{fila } j \\ \\ \\ \end{array}$$

El determinante de esta matriz C que tiene dos filas iguales, luego es igual a cero; por tanto, desarrollando $|C|$ por los elementos de la fila *j* queda:

$$0 = |C| = \sum_{k=1}^{n} \theta_{jk} \Delta_{jk}^{c}$$

pero los adjuntos Δ_{jk}^{c} de la matriz C son los mismos que los de A (como se ve fácilmente en la matriz) y con la definición de las θ_{jk} queda:

$$0 = \sum_{k=1}^{n} \theta_{jk} \Delta_{jk}^{c} = \sum_{k=1}^{n} \alpha_{ik} \Delta_{jk}$$

con lo que queda demostrado el teorema.

11-6 MATRIZ INVERSA

Teorema 8.—La matriz $A = [\alpha_{ij}]$ $A \in M^k_{(n \times n)}$ es inversible si y solo si $|A| \neq 0$, y en este caso su inversa A^{-1} es:

$$A^{-1} = |A|^{-1} \cdot \tilde{A} \quad \text{siendo} \quad |A^{-1}| = |A|^{-1}$$

En efecto, si A es inversible, existe A^{-1}, tal que $A \cdot A^{-1} = A^{-1} \cdot A = I_n$.

Teniendo en cuenta que el determinante de un producto de matrices es igual al producto de los determinantes, queda:

$$|A| \cdot |A^{-1}| = |A^{-1}| \cdot |A| = |I_n| = 1$$

como $|A|$ y $|A^{-1}|$ son elementos de un cuerpo y su producto no es cero, han de ser ambos distintos de cero

$$|A| \neq 0 \quad y \quad |A^{-1}| \neq 0$$

Supongamos ahora que $|A| \neq 0$. En virtud del teorema 7:

$$A \cdot \tilde{A} = \tilde{A} \cdot A = |A| \cdot I_n$$

multiplicando por el escalar $|A|^{-1}$ queda:

$$(A \cdot \tilde{A}) \cdot |A|^{-1} = (\tilde{A} \cdot A) \cdot |A|^{-1} = I_n$$

y como los escalares conmutan con las matrices

$$A \cdot (\tilde{A} \cdot |A|^{-1}) = (\tilde{A} \cdot |A|^{-1}) \cdot A = I_n$$

luego la matriz $(\tilde{A} \cdot |A|^{-1})$ es la matriz inversa de A como queríamos demostrar

$$A^{-1} = \tilde{A} \cdot |A|^{-1}$$

hallando el determinante de A^{-1} en esta expresión queda:

$$|A^{-1}| = |\tilde{A}| \cdot |A|^{-1}$$

pero el determinante de $\tilde{A}$ es la unidad, ya que tomando los determinantes en la ecuación $A \cdot \tilde{A} = |A| \cdot I_n$ queda

$$|A| \cdot |\tilde{A}| = |A| \cdot 1$$

luego $|\tilde{A}| = 1$
y finalmente resulta

$$|A^{-1}| = |A|^{-1}$$

A partir de este teorema, podemos enunciar desde el punto de vista práctico los siguientes pasos para calcular la inversa de una matriz A:

1.° Hallamos la matriz traspuesta.

2.° Sustituimos en la ${}^tA$ hallada, cada elemento por su adjunto correspondiente, con los que obtenemos la matriz adjunta.

3.° Dividimos cada elemento de la matriz adjunta por el determinante de A.

EJEMPLO:

Calculemos la inversa de la matriz

$$A = \begin{bmatrix} 1 & -1 & -3 \\ 3 & 2 & 2 \\ 2 & -1 & 2 \end{bmatrix}$$

1)

$${}^tA = \begin{bmatrix} 1 & 3 & 2 \\ -1 & 2 & -1 \\ -3 & 2 & 2 \end{bmatrix}$$

2) Calculando los adjuntos

$$\tilde{A} = \begin{bmatrix} 6 & 5 & 4 \\ -2 & 8 & -11 \\ -7 & -1 & 5 \end{bmatrix}$$

3)

$$|A| = 29$$

luego:

$$A^{-1} = \begin{bmatrix} 6/29 & 5/29 & 4/29 \\ -2/29 & 8/29 & -11/29 \\ -7/29 & -1/29 & 5/29 \end{bmatrix}$$

11-7 RANGO DE UNA MATRIZ

11-7-1 RANGO DE UNA FAMILIA DE VECTORES

Dado un espacio vectorial E definido sobre el cuerpo K, llamamos rango de una familia $F = \{v_1, \ldots, v_p\}$ de vectores de E a la dimensión del subespacio $\mathcal{E}\{v_1, \ldots, v_p\}$ engendrado por esta familia.

$$\text{rango}\ (F) = \dim \mathcal{E}\{v_1, \ldots, v_p\}$$

Puesto que de toda familia de generadores puede extraerse una base, la dimensión de $\mathcal{E}\{v_1, \ldots, v_p\}$ y por tanto el rango de F será el número de vectores de esa base. Por ello podemos concluir: "Rango de una familia F de vectores es el número de ellos, linealmente independientes, que posee".

11-7-2 RANGO DE UNA MATRIZ

Dada una matriz $A = [\alpha_{ij}]$ de elementos de K de orden $(m \times n)$, llamamos rango de A al rango de la familia de sus vectores columna. Es decir, sea:

$$A = \begin{bmatrix} \alpha_{11} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots\cdots & \alpha_{mn} \end{bmatrix}$$

y

$$F = \{v_1, \ldots, v_n\}$$

con

$$v_i = (\alpha_{1\,i}, \ldots, \alpha_{m\,i}) \in K^m \quad 1 \leqslant i \leqslant n$$

Entonces decimos

$$\text{rango } A = \text{rango } (F)$$

Teorema 9.—En toda matriz A, el rango de la familia de sus vectores fila F_f es igual al rango de la familia F_c de sus vectores columna.
Sea:

$$A = \begin{bmatrix} \alpha_{1\,1} & \cdots\cdots & \alpha_{1\,n} \\ \vdots & & \vdots \\ \alpha_{m\,1} & \cdots\cdots & \alpha_{m\,n} \end{bmatrix}$$

y llamemos a los vectores columna $F_c = \{v_1, \ldots, v_n\}$ con

$$v_i = (\alpha_{1\,i}, \ldots, \alpha_{m\,i})$$

$$v_i \in K^m \quad \forall i \quad 1 \leqslant i \leqslant n$$

sea también $F_f = \{u_1, \ldots, u_m\}$ la familia de vectores fila, con:

$$u_j = (\alpha_{j1}, \ldots, \alpha_{jn})$$

$$u_j \in K^n \quad \forall j \quad 1 \leqslant j \leqslant n$$

Supongamos que rango $A = r$ y por consiguiente que rango $(F_c) = r$, y vamos a demostrar que también es rango $(F_f) = r$.
En efecto, si rango $(F_c) = r$, esto quiere decir que habrá r vectores linealmente independientes en F_c y que los otros n-r se podrán escribir como combinación lineal de éstos. Supongamos, para simplificar la escritura, que los r vectores linealmente independientes sean los $\{v_1, v_2, \ldots, v_r\}$
Entonces:

$$v_{r+k} = \sum_{e=1}^{r} \beta_{ke} \cdot v_e \quad \forall k \quad 1 \leqslant k \leqslant n\text{-}r$$

de esto se deduce que cada coordenada s, $1 \leqslant s \leqslant m$ de todos los vectores v_{r+k} será combinación lineal de las coordenadas s de todos los vectores v_e $(1 \leqslant e \leqslant r)$
luego:

$$\alpha_{(r+k)\,s} = \sum_{e=1}^{r} \beta_{ke} \cdot \alpha_{es}$$

Sea ahora por otra parte $B_n = \{e_1, ..., e_n\}$ la base canónica de K^n. Podemos escribir, pues:

$$u_s = \sum_{t=1}^{n} \alpha_{ts} \cdot e_t = \sum_{e=1}^{r} \alpha_{es} \cdot e_e + \sum_{k=1}^{n-r} \alpha_{(r+k)s} \cdot e_{r+k}$$

sustituyendo aquí el resultado que hemos obtenido para $\alpha_{(r+k)s}$

$$u_s = \sum_{e=1}^{r} \alpha_{es} \cdot e_e + \sum_{k=1}^{n-r} \left[\sum_{e=1}^{r} \beta_{ke} \cdot \alpha_{es} \right] e_{r+k}$$

permutando los sumatorios en k y l y reuniendo todo en uno:

$$u_s = \sum_{e=1}^{r} \left[e_e + \sum_{k=1}^{n-r} \beta_{ke} \cdot e_{r+k} \right] \cdot \alpha_{es}$$

con lo que resulta que todos los vectores pueden escribirse como combinación lineal de r vectores linealmente independientes $[e_e + \sum_{k=1}^{n-r} \beta_{ke} \cdot e_{r+k}]$. Por tanto, en F_f hay solo r vectores linealmente independientes, y queda demostrado como queríamos que

$$\text{rango } (F_c) = \text{rango } (F_f) = \text{rango } A$$

11-8 MATRIZ REGULAR Y SINGULAR

Decimos que una matriz A es regular si todos sus vectores fila y todos sus vectores columna son linealmente independientes. Cuando una matriz no es regular, la llamaremos singular.

Se comprende fácilmente que una matriz A para ser regular necesariamente ha de ser cuadrada, ya que en virtud del teorema 9 el número de vectores fila linealmente independientes es igual al número de vectores columna libres, y como para que sea regular han de ser independientes todos, resulta, pues, que el número de filas ha de ser igual al de columnas. Sin embargo, si una matriz es cuadrada no necesariamente es regular, como se vé fácilmente a partir de la definición.

Teorema 10.—La condición necesaria y suficiente para que una matriz A sea regular es que su determinante sea distinto de cero.
En efecto, si A es regular, entonces ha de ser cuadrada. Supongamos que $A \in M^k_{(n\times n)}$, entonces en virtud del isomorfismo existente entre $M^k_{(n\times n)}$ y $L(K^n, K^n)$ existe una aplicación lineal $f \in L(K^n, K^n)$ cuya matriz es A. Como los vectores columna de A constituyen una familia de generadores del subespacio imagen y por ser regular son todos libres, resulta que

$$\dim f\,(K^n) = n$$

y esto significa que la aplicación f es sobre.
También se deduce que:

$$\dim \operatorname{Ker}(f) = n - \dim f\,(K^n) = n - n = 0$$

luego f es inyectiva y por consiguiente biyectiva. Entonces, si f es biyectiva, su matriz A es inversible y por lo tanto $|A| \neq 0$.
Si inversamente es $|A| \neq 0$, entonces por definición de determinante han de ser todos sus vectores columnas y todos sus vectores fila libres, luego A es regular.

11-9 SUBMATRIZ

Dada una matriz $A = [\alpha_{ij}]$, $A \in M^k_{(n\times n)}$ se llama submatriz a toda matriz cuyas filas son partes de las filas de A y cuyas columnas son partes de las columnas de A. Si

$$A = \begin{bmatrix} \alpha_{11} & \cdots\cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots\cdots & \alpha_{mn} \end{bmatrix}$$

una submatriz M de A será:

$$M = \begin{bmatrix} \alpha_{i_1 j_1} & \alpha_{i_1 j_2} & \cdots\cdots & \alpha_{i_1 j_s} \\ \alpha_{i_2 j_1} & \alpha_{i_2 j_2} & \cdots\cdots & \alpha_{i_2 j_s} \\ \vdots & \vdots & & \vdots \\ \alpha_{i_t j_1} & \alpha_{i_t j_2} & \cdots\cdots & \alpha_{i_t j_s} \end{bmatrix} \qquad \begin{matrix} 1 \leqslant i_1, i_2, \ldots, i_t \leqslant m \\ \\ \\ 1 \leqslant j_1, j_2, \ldots, j_s \leqslant n \end{matrix}$$

Vemos rápidamente que en la primera columna de M, por ejemplo, todos los elementos que aparecen son de la misma columna j_1 de A, pero pertenecientes a distintas filas $i_1, \ldots, i_t$. Igualmente, en la segunda fila de M, por ejemplo, todos los elementos que aparecen son de la misma fila i_2 de A, pero de distintas columnas $j_1, \ldots, j_s$ de A.
Nosotros, en lo que sigue, utilizaremos principalmente las submatrices cuadradas de A. Es decir, aquellos en que $s = t$.

Teorema 11.—El rango de una matriz A es igual al número de filas (o de columnas) de las submatrices regulares de mayor orden de A.
Sea $A = [\alpha_{ij}]$ una matriz de orden $(n \times n)$ de elementos de K.
Supongamos que el número de filas de las submatrices regulares de mayor orden sea r; entonces el orden de estas submatrices será $r \times r$ y su rango será r por ser regulares. Sea M una de estas submatrices regulares de A, de orden $(r \times r)$.
Tratemos de demostrar, pues, que rango $A = r$. En efecto, por ser M una submatriz de A, se cumple que:

$$\text{rango } A \geqslant \text{rango } M = r$$

Demostremos ahora que no pueden existir en A $(r + 1)$ filas (o columnas) linealmente independientes. En efecto, si así fuese, tomando los $r + 1$ primeros escalares, de estos $r + 1$ filas formaríamos una submatriz M' de A de orden $(r + 1) \times (r + 1)$, y por tener sus $(r + 1)$ filas linealmente independientes sus $(r + 1)$ columnas también lo serán y M' será regular. Pero esto significa que hemos encontrado una submatriz regular M' de A con $r + 1$ filas, lo cual va contra la hipótesis del teorema de que el número máximo de filas de las submatrices regulares de A era r. Por consiguiente queda demostrado que en A no pueden existir $r + 1$ filas (o columnas) linealmente independientes. Esto significa por tanto que

$$\text{rango } A < r + 1$$

luego, se deduce lo que deseábamos demostrar:

$$\text{rango } A = r$$

Cálculo del rango de una matriz.—Como hemos visto en el teorema 11, para hallar el rango de una matriz A basta con encontrar las submatrices regulares de mayor orden de A. Ahora bien, hemos visto en el teorema 10 que la condición necesaria y suficiente para que una matriz sea regular es que su determinante sea distinto de cero. Por lo tanto, para determinar el rango de A de un modo práctico, comenzaremos por escribir todas las submatrices cuadradas de mayor orden que se pueden extraer de A y hallaremos su determinante; si hay alguna que tenga determinante no nulo, el rango de la matriz será el número de filas (o columnas) de esa submatriz. Si por el contrario todos tuviesen determinante igual a cero, hallaríamos el determinante de todas las submatrices cuadradas de un orden inferior en una unidad a las anteriores y volveríamos a razonar igual; si existe alguna cuyo determinante sea distinto de cero, el rango de la matriz es igual a su número de filas o columnas. Si no existe ninguna, continuamos el proceso rebajando cada vez en una unidad el orden de las submatrices cuadradas que vamos tomando para calcular su determinante.

EJEMPLO:

Vamos a hallar por ejemplo el rango de la matriz

$$A = \begin{bmatrix} 1 & -1 & 2 & -1 \\ 2 & -2 & 1 & 3 \\ 1 & -1 & -4 & 9 \end{bmatrix}$$

En primer lugar, como hemos señalado, vamos a calcular el determinante de las submatrices de orden (3×3) que son los mayores que podemos formar siendo cuadrados.

$$\left\| \begin{bmatrix} 1 & -1 & 2 \\ 2 & -2 & 1 \\ 1 & -1 & -4 \end{bmatrix} \right\| = 0 \qquad \left\| \begin{bmatrix} 1 & 2 & -1 \\ 2 & 1 & 3 \\ 1 & -4 & 9 \end{bmatrix} \right\| = 0$$

$$\left\|\begin{bmatrix} 1 & -1 & -1 \\ 2 & -2 & 3 \\ 1 & -1 & 9 \end{bmatrix}\right\| = 0 \qquad \left\|\begin{bmatrix} -1 & 2 & -1 \\ -2 & 1 & 3 \\ -1 & -4 & 9 \end{bmatrix}\right\| = 0$$

luego no tiene rango 3.

Hallemos ahora los determinantes de las submatrices de orden 2 X 2

$$\left\|\begin{bmatrix} 1 & -1 \\ 2 & -2 \end{bmatrix}\right\| = 0$$

$$\left\|\begin{bmatrix} -1 & 2 \\ -2 & 1 \end{bmatrix}\right\| = -1 + 4 = 3 \neq 0$$

como ya hemos encontrado un determinante distinto de cero, ya no es necesario seguir. Concluimos, pues, que el rango de A es 2.

$$\text{rango } A = 2$$

TEMA 12 | SISTEMAS DE ECUACIONES LINEALES

TEMA 12 SISTEMAS DE ECUACIONES LINEALES

12-1 DEFINICION

Sea K un cuerpo. Llamamos "sistema de m ecuaciones lineales con n incógnitas" a:

$$\left.\begin{array}{l} \alpha_{11}\ x_1 + \alpha_{12}\ x_2 +, \ldots\ldots, + \alpha_{1n}\ x_n = \beta_1 \\ \alpha_{21}\ x_1 + \alpha_{22}\ x_2 +, \ldots\ldots, + \alpha_{2n}\ x_n = \beta_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}\ x_1 + \alpha_{m2}\ x_2 +, \ldots\ldots, + \alpha_{mn}\ x_n = \beta_m \end{array}\right\} \quad (1)$$

con

$$\alpha_{ij} \in \mathrm{K} \quad 1 \leqslant i \leqslant m \quad 1 \leqslant j \leqslant n$$

Los elementos α_{ij} se llaman "coeficientes". Los x_j son las "incógnitas y los β_i los "segundos miembros".
Se llama "solución" del sistema a todo conjunto de n escalares x_1, $x_2, \ldots, x_n$ de K que lo satisface. Nuestro problema fundamental será, pues, encontrar todas las posibles soluciones del sistema (todos los conjuntos $x_1, x_2, \ldots, x_n) \in \mathrm{K}^n$ que lo satisfacen).

12-2 REPRESENTACION MATRICIAL

Teniendo en cuenta la ley de multiplicación de matrices, podemos representar el sistema de ecuaciones (1) como:

$$A \cdot \{x\} = \{y\} \qquad (2)$$

siendo

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots\cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots\cdots & \alpha_{2n} \\ \vdots & & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots\cdots & \alpha_{mn} \end{bmatrix}$$

también llamada "matriz del sistema"
y

$$\{x\} = \begin{Bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{Bmatrix} \quad \text{e} \quad \{y\} = \begin{Bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{Bmatrix}$$

También utilizaremos a menudo la matriz:

$$B = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots\cdots & \alpha_{1n} & \beta_1 \\ \alpha_{21} & \alpha_{22} & \cdots\cdots & \alpha_{2n} & \beta_2 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots\cdots & \alpha_{mn} & \beta_m \end{bmatrix}$$

llamada "matriz orlada con los segundos miembros" o sencillamente "orlada".

12-3 ESTUDIO VECTORIAL

Dada la ecuación matricial $A \cdot \{x\} = \{y\}$ donde $A \in M^k_{(m \times n)}$ sabemos que existe una y solo una aplicación lineal $f \in L(K^n, K^m)$ cuya matriz en las bases canónicas de K^n y K^m es A. En este sentido, también es $\{x\}$ la matriz de un vector $x \in K^n$ y $\{y\}$ la de un vector $y \in K^m$. Con esto la ecuación matricial (2) se transforma en:

$$f(x) = y \qquad (3)$$

En esta nueva representación, resolver el sistema será encontrar el conjunto S de todos los vectores $x \in K^n$ que tienen a y por imagen por la aplicación f. En general, f no es una aplicación sobre, es decir, $I_m\ (f) \subset K^m$ y puede ocurrir por lo tanto que:

el vector $y = \begin{Bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{Bmatrix}$ pertenezca a Im (f)

o el vector y, no pertenezca a Im (f).

Veamos ambos casos:

1) Si $y \in$ Im (f), entonces el conjunto S de elementos que tienen a y por imagen no será vacío. Tomando un elemento $x_1 \in S$ tendremos:

$$f(x_1) = y \qquad (4)$$

Para cualquier otro elemento $x \in S$ se cumple también que:

$$f(x) = y \qquad (5)$$

Restando, pues, a la ecuación (5) la (4) queda:

$$f(x) - f(x_1) = 0$$

por ser f lineal tenemos:

$$f(x - x_1) = 0$$

lo cual significa que el elemento $x - x_1 \in K^n$, pertenece al núcleo de f:

$$x - x_1 \in \text{Ker}\ (f)$$

Como x era una solución cualquiera del sistema, si $v \in \text{Ker}\,(f)$ podemos decir que el conjunto S de soluciones se obtiene sumando a una solución x_1 del sistema cada uno de los vectores del núcleo

$$S = \{x_1 + v, \ \forall v \in \text{Ker}\,(f)\} \qquad (6)$$

Según indica (6), el sistema de ecuaciones puede tener una solución única (S tiene entonces un solo elemento) o muchas soluciones. Se observa fácilmente que la condición necesaria y suficiente para que el sistema tenga solución única es que el núcleo de f sea el vector nulo

$$\text{Ker}\,(f) = \{0\}$$

"lo que implica que f tenga que ser inyectiva".
Cuando el sistema posee una solución única se llama *"determinado"*, y cuando posee muchas soluciones (S tiene, pues, más de un elemento) se llama *"indeterminado"*.

2) Si $y \notin \text{Im}\,(f)$ entonces no hay ningún $x \in K^n$ tal que $f(x) = y$. Por consiguiente, el sistema no tendrá ninguna solución. Es decir:

$$S = \phi$$

Cuando el sistema no posee soluciones ($S = \phi$) se le llama *"incompatible"* y del mismo modo, cuando posee alguna solución ($S \neq \phi$) se le llama *"compatible"*.

12-4 DISCUSION DEL SISTEMA

Discutiremos el sistema al objeto de establecer sus posibles soluciones, utilizando para ello el rango de la matriz del sistema, así como el de la matriz ampliada.

Llamemos: rango (A) $= r$ rango (B) $= r'$

Existen dos casos posibles en principio:

1) $r \neq r'$. Esto significa que entre las n vectores columna de A hay solo r que son linealmente independientes. Entonces el subespacio imagen $\text{Im}\,(f)$ está engendrado por estos r vectores. Como $r \neq r'$ solo puede ser $r' > r$, ya que B posee las mismas columnas que

A más otra constituida por el vector y de los segundos miembros. Por ser $r' > r$ significa que y es linealmente independiente con los r vectores que engendran Im *(f)*, luego $y \notin$ Im *(f)*, y por consiguiente no existe solución para el sistema de ecuaciones. El sistema es, pues, en este caso *"incompatible"*.

$$(S = \phi)$$

2) $r = r'$. En este caso el vector columna y de la matriz B es combinación lineal de los r vectores linealmente independientes que engendran Im *(f)*, luego $y \in$ Im *(f)*, y por consiguiente el sistema posee un conjunto de soluciones $S \neq \phi$. El sistema es, pues, *"compatible"*.
En esta situación de $r = r'$ puede haber dos casos, según que el rango de la matriz sea igual al número de incógnitas o que sea distinto de él.

12-5 RESOLUCION DEL SISTEMA

Para estudiar la resolución de los sistemas en general, vamos a considerar las tres posibilidades según que el número de ecuaciones sea igual, mayor o menor que el número de incógnitas. Es obvio que los sistemas que vamos a resolver tienen solución, es decir, $r = r'$.

1) $m = n$. Podrá ocurrir que la solución sea única, o no.

1a) *Solución única.*—En este caso, según hemos visto, Ker *(f)* $= \{0\}$. Como dim Im *(f)* + dim Ker *(f)* $= n$, resulta dim Im *(f)* $=$ $= n =$ dim K^n. Por tanto, Im *(f)* $= K^n$, lo cual significa que f es *sobre.* Como f es ya inyectiva por ser Ker *(f)* $= \{0\}$, resulta, pues, que f es biyectiva. Esto significa que la matriz A es inversible, y entonces la solución única del sistema de ecuaciones se obtiene inmediatamente del siguiente modo:
El sistema matricialmente era:

$$A \cdot \{x\} = \{y\}$$

como A es inversible, queda:

$$\{x\} = A^{-1} \{y\}$$

o sea:

$$\begin{Bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{Bmatrix} = \begin{bmatrix} \frac{\Delta_{11}}{|A|} & \frac{\Delta_{21}}{|A|} & \cdots & \frac{\Delta_{n1}}{|A|} \\ \frac{\Delta_{12}}{|A|} & \frac{\Delta_{22}}{|A|} & \cdots & \frac{\Delta_{n2}}{|A|} \\ \vdots & \vdots & & \vdots \\ \frac{\Delta_{1n}}{|A|}, & \frac{\Delta_{2n}}{|A|} & \cdots & \frac{\Delta_{nn}}{|A|} \end{bmatrix} \begin{Bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{Bmatrix}$$

Efectuando este producto queda:

$$\begin{Bmatrix} x_1 \\ \vdots \\ x_n \end{Bmatrix} = \begin{Bmatrix} \sum_{i=1}^{n} \frac{\Delta_{i1}}{|A|} \cdot \beta_i \\ \vdots \\ \sum_{i=1}^{n} \frac{\Delta_{in}}{|A|} \cdot \beta_i \end{Bmatrix}$$

Luego cada uno de los escalares x_j de la solución $(x_1, x_2, ..., x_n)$ del sistema de ecuaciones se halla en este caso por:

$$x_j = \sum_{i=1}^{n} \frac{\Delta_{ij}}{|A|} \beta_i = \frac{\sum_{i=1}^{n} \Delta_{ij} \cdot \beta_i}{|A|}$$

Pero $\sum_{i=1}^{n} \Delta_{ij} \beta_i$ no es más que el desarrollo por los elementos de la columna j del determinante de la matriz

$$\begin{bmatrix} \alpha_{11} & \alpha_{12}, \cdots\cdots, \alpha_{1(j-1)} & \beta_1 & \alpha_{1(j+1)}, \cdots\cdots, \alpha_{1n} \\ \alpha_{21} & \alpha_{22}, \cdots\cdots, \alpha_{2(j-1)} & \beta_2 & \alpha_{2(j+1)}, \cdots\cdots, \alpha_{2n} \\ \vdots & & \vdots & \vdots \\ \alpha_{n1} & \alpha_{n2}, \cdots\cdots, \alpha_{n(j-1)} & \beta_n & \alpha_{n(j+1)}, \cdots\cdots, \alpha_{nn} \end{bmatrix}$$

obtenida reemplazando en A la columna j por el vector $\{y\}$.

Este tipo de sistemas que cumplen $r = r' = n = m$ se llaman "Sistemas de Cramer". Son siempre "determinados", como hemos visto por poseer una única solución.

1b) Existe un conjunto de soluciones S que posee más de un elemento. Entonces como $\text{Ker}\,(f) \neq \{0\}$, $\dim \text{Ker}\,(f) \neq 0$, y por tanto

$$\dim \text{Im}\,(f) = n - \dim \text{Ker}\,(f) < n$$

de donde $\text{Im}\,(f) \neq K^n$, luego f no es suprayectiva.
De esto se deduce también que $r = r' < n$. Es decir, que de las n filas de la matriz B, hay $n\text{-}r$ que son combinación lineal de los demás. Esto supone, puesto que estas filas son los coeficientes de otras tantas $n\text{-}r$ ecuaciones, que hay también $n\text{-}r$ ecuaciones que dependen de las otras r. Supongamos que estas $n\text{-}r$ ecuaciones sean las últimas del sistema.

$$\left.\begin{array}{l}
\alpha_{11} x_1 + \alpha_{12} x_2 + \ldots\ldots + \alpha_{1n} x_n = \beta_1 \\
\alpha_{21} x_1 + \alpha_{22} x_2 + \ldots\ldots + \alpha_{2n} x_n = \beta_2 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\alpha_{r1} x_1 + \alpha_{r2} x_2 + \ldots\ldots + \alpha_{rn} x_n = \beta_r \\
\text{n-r}\left\{\begin{array}{l}
\alpha_{(r+1)1} x_1 + \alpha_{(r+1)2} x_2 + \ldots\ldots + \alpha_{(r+1)n} x_n = \beta_{r+1} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\alpha_{n1} x_1 + \alpha_{n2} x_2 + \ldots\ldots + \alpha_{nn} x_n = \beta_n
\end{array}\right.
\end{array}\right\}$$

Podemos, pues, eliminar estas últimas quedando el sistema:

$$\left.\begin{array}{l}
\alpha_{11} x_1 + \alpha_{12} x_2 + \ldots\ldots + \alpha_{1n} x_n = \beta_1 \\
\alpha_{21} x_1 + \alpha_{22} x_2 + \ldots\ldots + \alpha_{2n} x_n = \beta_2 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\alpha_{r1} x_1 + \alpha_{r2} x_2 + \ldots\ldots + \alpha_{rn} x_n = \beta_r
\end{array}\right\}$$

Este nuevo sistema es equivalente al inicial, puesto que posee el mismo conjunto de soluciones que él, pero en éste, sin embargo, se verifica que el número de ecuaciones r es menor que el número de incógnitas n. Por ello su resolución la estudiaremos en el caso 2 en que el sistema original cumple $r = r'$ y $m < n$.

Un sistema de este tipo será, pues: compatible (por tener solución) e indeterminado (por tener varias soluciones).

2) $m < n$. El sistema será:

$$\left.\begin{array}{l} \alpha_{11}\ x_1 + \ldots\ldots + \alpha_{1n}\ x_n = \beta_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}\ x_1 + \ldots\ldots + \alpha_{mn}\ x_n = \beta_m \end{array}\right\}$$

y pueden ocurrir dos casos: que $r = r' = m < n$ y $r = r' < m < n$. En los dos casos el sistema es compatible indeterminado, ya que:

$$\dim \operatorname{Ker} (f) = n - r \neq 0$$

2a) Sea $r = r' = m < n$. Para resolver el sistema, tratemos de reducirlo a un sistema del tipo Cramer; es decir, un sistema en el que la matriz A sea regular (y por tanto, inversible). Para ello pasemos al segundo miembro $n - m$ términos $\alpha_{ij}\, x_j$ en cada una de las ecuaciones. Por ejemplo, los $n - m$ últimos términos $\alpha_{ij}\, x_j$. El sistema queda entonces:

$$\left.\begin{array}{l} \alpha_{11}\ x_1 + \ldots\ldots + \alpha_{1m}\ x_m = \beta_1 - \alpha_{1\,(m+1)}\, x_{m+1} - \ldots\ldots - \alpha_{1n}\ x_n \\ \alpha_{21}\ x_1 + \ldots\ldots + \alpha_{2m}\ x_m = \beta_2 - \alpha_{2\,(m+1)}\, x_{m+1} - \ldots\ldots - \alpha_{2n}\ x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{m1}\ x_1 + \ldots\ldots + \alpha_{mm}\ x_m = \beta_m - \alpha_{m\,(m+1)}\, x_{m+1} - \ldots\ldots - \alpha_{mn}\ x_n \end{array}\right\}$$

El sistema dispuesto así, considerando incógnitas $(x_1, \ldots, x_m)$ es ya un sistema de Cramer, pues en él el rango de la matriz del sistema, de la matriz ampliada, el número de ecuaciones y el número de incógnitas, coinciden. Por lo tanto su solución es inmediata:

$$x_j = \frac{\sum_{i=1}^{m} \Delta_{ij} \cdot (\beta_i - \sum_{k=m+1}^{n} \alpha_{ik}\, x_k)}{|A|} \qquad \forall j\ 1 \leqslant j \leqslant m$$

$$A = \begin{bmatrix} \alpha_{11} & \ldots\ldots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{m1} & \ldots\ldots & \alpha_{mm} \end{bmatrix}$$

y el numerador, el resultado de desarrollar por la columna j el determinante de la matriz que se obtiene de reemplazar la columna j de A por el vector columna:

$$\begin{pmatrix} \beta_1 - \sum_{k=m+1}^{n} \alpha_{1k} x_k \\ \vdots \\ \beta_2 - \sum_{k=m+1}^{n} \alpha_{2k} x_k \\ \vdots \\ \beta_m - \sum_{k=m+1}^{n} \alpha_{mk} x_k \end{pmatrix}$$

A este caso 2a se asimila el 1b.

2b) Si $r = r' < m < n$, entonces esto significa que hay $m - r$ filas de la matriz ampliada que dependen linealmente de los r primeras. Supongamos que sean éstas las $m - r$ últimas filas. Entonces podemos eliminar las $m - r$ últimas ecuaciones, quedando el sistema:

$$\left.\begin{array}{l} \alpha_{11} x_1 + \alpha_{12} x_2 + \ldots\ldots, + \alpha_{1n} x_n = \beta_1 \\ \vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \alpha_{r1} x_1 + \alpha_{r2} x_2 + \ldots\ldots, + \alpha_{rn} x_n = \beta_r \end{array}\right\}$$

y este nuevo sistema es equivalente al anterior, pues cumple $r = r' =$ n.° de ecuaciones$< n$, que es el caso 2a que ya hemos analizado.

3) $m > n$, puede ocurrir dos casos, que $r = r' = n < m$ y $r = r' < n < m$.
Si $r = r' = n < m$, dim ker $(f) = n - r = 0$ sistema compatible *determinado.*
Si $r = r' < n < m$, dim ker $(f) = n - r \neq 0 \Rightarrow$ sistema compatible *indeterminado.*.
Veamos la resolución en cada uno de estos dos casos:

3a) $r = r' = n < m$. En este caso existen en la matriz ampliada, $m - n$ filas que con combinación lineal de los n restantes. Si suponemos como hasta ahora que las $m - n$ últimas dependen de los n primeros podemos suprimirlas del sistema quedando:

$$
\begin{array}{l}
\alpha_{11} x_1 + \alpha_{12} x_2 + \ldots\ldots + \alpha_{1n} x_n = \beta_1 \\
\alpha_{21} x_1 + \alpha_{22} x_2 + \ldots\ldots + \alpha_{2n} x_n = \beta_2 \\
\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
\alpha_{n1} x_1 + \alpha_{n2} x_2 + \ldots\ldots + \alpha_{nn} x_n = \beta_n
\end{array}
$$

en este sistema se cumple que el rango de la matriz del mismo, es igual al de la matriz ampliada, e igual, a su vez, al número de incógnitas y al de ecuaciones. Por consiguiente, es un sistema de Cramer con solución única y cuya resolución ya hemos estudiado.

3b) $r = r' < n < m$. Vamos a tratar de reducirlo a un sistema de Cramer. Como $r < m$ significa que hay $m - r$ filas que dependen linealmente de las primeras. Eliminemos, pues, estos $m - r$ filas, con lo cual el sistema queda:

$$
\begin{array}{l}
\alpha_{11} x_1 + \alpha_{12} x_2 + \ldots\ldots + \alpha_{1n} x_n = \beta_1 \\
\alpha_{21} x_1 + \alpha_{22} x_2 + \ldots\ldots + \alpha_{2n} x_n = \beta_2 \\
\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
\alpha_{r1} x_1 + \alpha_{r2} x_2 + \ldots\ldots + \alpha_{rn} x_n = \beta_r
\end{array}
$$

tenemos, pues, ahora un sistema en el que se cumple que $r = r' =$ n.° de filas $<$ n.° de incógnitas. La resolución de este caso que ya la hemos estudiado en el aparatado 2a.

Podemos resumir todo lo que llevamos dicho en el siguiente cuadro:

<table>
<tr><td colspan="3">$r \neq r'$ Sistema incompatible</td></tr>
<tr><td rowspan="3">$r = r'$ Sistema compatible</td><td>$m = n$</td><td>$r = r' = m = n$ Determinado (Cramer)
$r = r' < m = n$ indeterminado</td></tr>
<tr><td>$m < n$</td><td>$r = r' = m$ indeterminado
$r = r' < m$ indeterminado</td></tr>
<tr><td>$m > n$</td><td>$r = r' = n$ determinado
$r = r' < n$ indeterminado</td></tr>
</table>

12-6 SISTEMAS HOMOGENEOS

Llamamos sistema homogeneo, a aquel en que todos los segundos miembros son nulos.

$$\begin{array}{l} \alpha_{11}\ x_1 + \alpha_{12}\ x_2 + \dots\dots + \alpha_{1n}\ x_n = 0 \\ \alpha_{21}\ x_1 + \alpha_{22}\ x_2 + \dots\dots + \alpha_{2n}\ x_n = 0 \\ \vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \alpha_{m1}\ x_1 + \alpha_{m2}\ x_2 + \dots\dots + \alpha_{mn}\ x_n = 0 \end{array}$$

Puesto que la matriz ampliada u orlada es la obtenida añadiendo a la matriz del sistema la columna de ceros de los segundos miembros, se deduce, pues, que $r = r'$ para este tipo de sistema. Podemos decir, pues, que el sistema homogéneo es siempre *"compatible"*.
Hallar las soluciones de este sistema, es hallar el núcleo de la aplicación lineal f: $K^n \to K^n$ cuya matriz correspondiente es:

$$A = \begin{bmatrix} \alpha_{11} & \dots\dots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \dots\dots & \alpha_{mn} \end{bmatrix}$$

Puede ocurrir que $r = r' = n$ con lo que dim Ker $(f) = n - n = 0$, y por ello Ker $(f) = \{0\}$ significando que el sistema es *"determinado"*, y su única solución será la solución trivial $x_1 = x_2 = \dots = x_n = 0$.
La otra alternativa es $r = r' < n$. En este caso dim Ker $(f) = n - r > 0$. Por tanto, Ker $(f) \neq \{0\}$ y el sistema es en este caso *"indeterminado"*. Para hallar las soluciones se pasan al segundo miembro $n - r$ sumandos $\alpha_{ij}\ x_j$ en cada ecuación, de modo que queden en el primer miembro sólo r incógnitas y el sistema se resuelve como hemos visto en el caso más general.

EJEMPLOS:

1) Vamos a intentar resolver el sistema

$$\left.\begin{array}{r} 2x - \ \ y = 3 \\ 3x + 2y = 0 \\ 2x + \ \ y = 1 \end{array}\right\}$$

cuyas matrices serán:

$$A = \begin{bmatrix} 2 & -1 \\ 3 & 2 \\ 2 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 2 & -1 & 3 \\ 3 & 2 & 0 \\ 2 & 1 & 1 \end{bmatrix}$$

de rangos:

$$r = 2 \quad \text{y} \quad r' = 3$$

es decir: $r \neq r'$

Luego el sistema es incompatible sin ninguna posible solución.

Los ejemplos siguientes serán siempre compatibles, es decir: $r = r'$.

2) Sea el sistema

$$\left.\begin{aligned} 4x + 2y - z &= 3 \\ 3x \qquad + 2z &= 0 \\ 2x + y - z &= 2 \end{aligned}\right\}$$

donde sus matrices respectivas son:

$$A = \begin{bmatrix} 4 & 2 & -1 \\ 3 & 0 & 2 \\ 3 & 1 & -1 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 4 & 2 & -1 & 3 \\ 3 & 0 & 2 & 0 \\ 2 & 1 & -1 & 2 \end{bmatrix}$$

de rangos $r = 3$ y $r' = 3$, pues el 1A1 = 7. Por otra parte, n.° de ecuaciones = n.° de incógnitas.

Luego:

$$\left.\begin{aligned} r = r' &\Rightarrow \text{compatible} \\ r = r' = m &= n = 3 \end{aligned}\right\} \Rightarrow \text{determinado (sistema de Cramer)}$$

Es decir, se resuelve directamente

$$x = \frac{\begin{vmatrix} 3 & 2 & -1 \\ 0 & 0 & 2 \\ 2 & 1 & -1 \end{vmatrix}}{\begin{vmatrix} 4 & 2 & -1 \\ 3 & 0 & 2 \\ 3 & 1 & -1 \end{vmatrix}} = \frac{2}{7}$$

$$y = \frac{\begin{vmatrix} 4 & 3 & -1 \\ 3 & 0 & 2 \\ 2 & 2 & -1 \end{vmatrix}}{7} = \frac{-1}{7}$$

$$z = \frac{\begin{vmatrix} 4 & 2 & 3 \\ 3 & 0 & 0 \\ 2 & 1 & 2 \end{vmatrix}}{7} = \frac{-3}{7}$$

El conjunto S de soluciones tiene un único elemento $S = \left\{ \frac{2}{7}, \frac{-1}{7}, \frac{-3}{7} \right\}$

3) Sea el sistema:

$$\left.\begin{aligned} 2x - 3y + 2z &= 1 \\ 3x + y - z &= 2 \\ 5x - 2y + z &= 3 \end{aligned}\right\}$$

En este sistema:

$$A = \begin{bmatrix} 2 & -3 & 2 \\ 3 & 1 & -1 \\ 5 & -2 & 1 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 2 & -3 & 2 & 1 \\ 3 & 1 & -1 & 2 \\ 5 & -2 & 1 & 3 \end{bmatrix}$$

$$r = \text{rango } A = 2 \qquad r' = \text{rango } B = 2$$

Es, pues: $r = r' < m = n$

Estamos, pues, en el caso que hemos estudiado como (1a). Hay entonces $m - r$ filas de la matriz B que dependen de las r primeras.

$$m - r = 3 - 2 = 1$$

Vemos inmediatamente que la 3.ª fila es suma de las dos primeras. Suprimiéndola, queda:

$$\left.\begin{aligned} 2x - 3y + 2z &= 1 \\ 3x + y - z &= 2 \end{aligned}\right\}$$

Este es un sistema en el que:

$$A = \begin{bmatrix} 2 & -3 & 2 \\ 3 & 1 & -1 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 2 & -3 & 2 & 1 \\ 3 & 1 & -1 & 2 \end{bmatrix}$$

$$r = \text{rango } A = 2 \qquad r' = \text{rango } B = 2$$

$r = r' = m < n$, que es un sistema como los que hemos estudiado en (2a). Para resolverlo, basta con pasar una incógnita al segundo miembro.

$$\left.\begin{aligned} 2x - 3y &= 1 - 2z \\ 3x + \ \ y &= 2 + z \end{aligned}\right\}$$

y ahora esto es un sistema de Cramer. Resolviendo, pues, queda:

$$x = \frac{\begin{vmatrix} (1-2z) & -3 \\ (2+z) & 1 \end{vmatrix}}{\begin{vmatrix} 2 & -3 \\ 3 & 1 \end{vmatrix}} = \frac{7+z}{11} \qquad y = \frac{\begin{vmatrix} 2 & (1-2z) \\ 3 & (2+z) \end{vmatrix}}{\begin{vmatrix} 2 & -3 \\ 3 & 1 \end{vmatrix}} = \frac{1+8z}{11}$$

El conjunto de soluciones S será, pues:

$$S = \left\{ \left(\frac{7+z}{11}, \frac{1+8z}{11}, z \right) \ \forall z \in R \right\}$$

Consideremos ahora casos en que $m < n$.

4) Sea el sistema

$$\left.\begin{aligned} 2x + \ \ y + \ \ z &= 3 \\ x - 3y + 2z &= 0 \end{aligned}\right\}$$

cuyas matrices son:

$$A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & -3 & 2 \end{bmatrix} \qquad \text{y} \qquad B = \begin{bmatrix} 2 & 1 & 1 & 3 \\ 1 & -3 & 2 & 0 \end{bmatrix}$$

de rangos $r = 2$ y $r' = 2$, siendo $m = 2$ y $n = 3$, luego:

$$\left.\begin{aligned} &r = r' = 2 \Rightarrow \text{compatible} \\ &r = r' = m = 2 < n = 3 \end{aligned}\right\} \Rightarrow \text{indeterminado}$$

Como se ha visto en (2*a*), basta con pasar al segundo miembro una de las incógnitas y el sistema es ahora de Cramer (1*a*):

$$\left.\begin{aligned} 2x + z &= 3 - y \\ x + 2z &= 3y \end{aligned}\right\}$$

con lo que en función de y las soluciones serán:

$$x = \frac{\begin{vmatrix} 3-y & 1 \\ 3y & 2 \end{vmatrix}}{\begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix}} = \frac{6-5y}{3} \qquad z = \frac{\begin{vmatrix} 2 & 3-y \\ 1 & 3y \end{vmatrix}}{3} = \frac{-3+7y}{3}$$

El conjunto de soluciones S será:

$$S = \left\{ \left(\frac{6-5y}{3},\ y,\ \frac{-3+7y}{3} \right) \quad \forall y \in R \right\}$$

5) Sea el sistema de 2 ecuaciones con incógnitas $m = 2$, $n = 3$.

$$\left. \begin{array}{r} 2x - 3y + z = 1 \\ -4x + 6y - 2z = -2 \end{array} \right\}$$

cuyas matrices son

$$A = \begin{bmatrix} 2 & -3 & 1 \\ -4 & 6 & -2 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 2 & -3 & 1 & 1 \\ -4 & 6 & -2 & -2 \end{bmatrix}$$

en las que se observa que la segunda fila es el producto de la primera por -2 luego:

$$r = 1 \quad \text{y} \quad r' = 1$$

Es decir:

$$\left. \begin{array}{l} r = r' = 1 \Rightarrow \text{compatible} \\ r = r' = 1 < m = 2 < n = 3 \end{array} \right\} \Rightarrow \text{indeterminado}$$

Este es el caso (2b) que hemos estudiado. Para resolverlo suprimimos la segunda ecuación que es combinación lineal de la primera y resolvemos como en el caso (2a):

$$2x - 3y + z = 1 \}$$

y la solución se expresará en función de dos de los parámetros: $x = \dfrac{3y - z + 1}{2}$

El conjunto de soluciones de este sistema S será:

$$S = \left\{ \left(\frac{3y - z + 1}{2},\ y, z \right) \quad \forall y, z \in R \right\}$$

Consideremos ahora casos en que $m > n$ (número de ecuaciones > número de incógnitas).

6) Sea el sistema

$$\left.\begin{aligned} 2x + y &= 1 \\ 3x - 2y &= 0 \\ 5x - y &= 1 \end{aligned}\right\}$$

Cuyas matrices son:

$$A = \begin{bmatrix} 2 & 1 \\ 3 & -2 \\ 5 & -1 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 2 & 1 & 1 \\ 3 & -2 & 0 \\ 5 & -1 & 1 \end{bmatrix}$$

de rangos $r = 2$ que se observa evidentemente y $r' = 2$, pues, $|B| = 0$, y tiene menores de rango 2 distinto de cero.

Luego:

$$\left.\begin{aligned} &r = r' = 2 \Rightarrow \text{compatible} \\ &r = r' = n = 2 < m = 3 \end{aligned}\right\} \Rightarrow \text{determinado}$$

Según hemos estudiado en el caso (3*a*), suprimiremos la tercera ecuación, que es suma de las dos primeras, quedando:

$$\left.\begin{aligned} 2x + y &= 1 \\ 3x - 2y &= 0 \end{aligned}\right\}$$

que es un sistema de Cramer de soluciones

$$x = \frac{\begin{vmatrix} 1 & 1 \\ 0 & -2 \end{vmatrix}}{\begin{vmatrix} 2 & 1 \\ 3 & -2 \end{vmatrix}} = \frac{-2}{-7} \qquad\qquad y = \frac{\begin{vmatrix} 2 & 1 \\ 3 & 0 \end{vmatrix}}{-7} = \frac{-3}{-7}$$

El sistema tiene solución única:

$$S = \left\{ \left(\frac{2}{7}, \frac{3}{7} \right) \right\}$$

7) Sea el sistema de tres ecuaciones $(m = 3)$ y dos incógnitas $(n = 2)$

$$\left.\begin{aligned} x - 2y &= 1 \\ 2x - 4y &= 2 \\ 3x - 6y &= 3 \end{aligned}\right\}$$

Cuyas matrices son:

$$A = \begin{bmatrix} 1 & -2 \\ 2 & -4 \\ 3 & -6 \end{bmatrix} \qquad \text{y} \qquad B = \begin{bmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 3 & -6 & 3 \end{bmatrix}$$

y al establecer sus rangos, éstos resultan:

$$r = 1 \qquad \text{y} \qquad r' = 1$$

Luego:

$$\left.\begin{aligned} &r = r' = 1 \Rightarrow \text{compatible} \\ &r = r' = 1 < n = 2 < m = 3 \end{aligned}\right\} \Rightarrow \text{indeterminado}$$

Para resolverlo suprimiremos las dos últimas ecuaciones, quedando el sistema reducido a:

$$x - 2y = 1 \}$$

y la solución en función de y será:

$$x = 1 + 2y$$

El conjunto S de soluciones será:

$$S = \{ (1 + 2y, y) \quad \forall y \in R \}$$

8) Sea el sistema homogéneo:

$$\left.\begin{aligned} 2x - 3y - z &= 0 \\ x - 4y + z &= 0 \\ -3x + 6y - 2z &= 0 \end{aligned}\right\}$$

En él:

$$A = \begin{bmatrix} 2 & -3 & -1 \\ 1 & -4 & 1 \\ -3 & 6 & -2 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 2 & -3 & -1 & 0 \\ 1 & -4 & 1 & 0 \\ -3 & 6 & -2 & 0 \end{bmatrix}$$

$$r = \text{rango } A = 3 \qquad r' = \text{rango } B = 3$$

Se cumple, pues, que:

$$r = r' = m = n$$

es, pues, un sistema compatible y determinado (solución única). Como: $x = 0$, $y = 0$, $z = 0$ es una solución, es pues la única (solución trivial) y

$$S = \left\{ (0,0,0) \right\}$$

9) Consideremos el sistema homogéneo:

$$\left.\begin{aligned} 4x - 5y - 6z &= 0 \\ 6x + 6y - 4z &= 0 \\ -2x - 36y - 12z &= 0 \end{aligned}\right\}$$

En él:

$$A = \begin{bmatrix} 4 & -5 & -6 \\ 6 & 6 & -4 \\ -24 & -36 & -12 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 4 & -5 & -6 & 0 \\ 6 & 6 & -4 & 0 \\ -24 & -36 & -12 & 0 \end{bmatrix}$$

$$r = \text{rango } A = 2 \qquad r' = \text{rango } B = 2$$

Se tiene, pues, $r = r' < m = n$. Es, pues, un sistema compatible como el que se ha visto en el caso (1b). Hay en él $m - r = 3 - 2 = 1$ filas de B (o ecuaciones del sistema) que son combinación lineal de los $r = 2$ primeros.
Vemos inmediatamente que la tercera fila es igual a la primera multiplicada por 4 menos la segunda multiplicada por 3. Eliminándola, pues, queda:

$$\left.\begin{aligned} 4x - 5y - 6z &= 0 \\ 6x + 6y - 4z &= 0 \end{aligned}\right\}$$

Que es un sistema en el que:

$$A = \begin{bmatrix} 4 & -5 & -6 \\ 6 & 6 & -4 \end{bmatrix} \qquad B = \begin{bmatrix} 4 & -5 & -6 & 0 \\ 6 & 6 & -4 & 0 \end{bmatrix}$$

$$r = \text{rango } A = 2 \qquad r' = \text{rango } B = 2$$

$r = r' = m < n$. Es, pues, ahora un sistema como los que hemos estudiado en (2a). Pasando al segundo miembro $n - r = 1$ incógnitas, tendremos:

$$\left.\begin{array}{l} 4x - 5y = 6z \\ 6x + 6y = 4z \end{array}\right\}$$

que es ahora un sistema de Cramer. Resolviendo, queda:

$$x = \frac{\begin{vmatrix} 6z & -5 \\ 4z & 6 \end{vmatrix}}{\begin{vmatrix} 4 & -5 \\ 6 & 6 \end{vmatrix}} = \frac{36z + 20z}{24 + 30} = \frac{28z}{27}; \quad y = \frac{\begin{vmatrix} 4 & 6z \\ 6 & 4z \end{vmatrix}}{\begin{vmatrix} 4 & -5 \\ 6 & 6 \end{vmatrix}} = \frac{16z - 36z}{54} = \frac{10z}{27}$$

Con lo que el conjunto de soluciones del sistema que nos habíamos propuesto es:

$$S = \left\{ \left(\frac{28z}{27}, \frac{10z}{27}, z \right) \quad \forall z \in R \right\}$$

INDICE