ISSN 1853-709X

Fascículo 12

Cursos y seminarios de matemática

Serie A

Jean Dieudonné

Álgebra Lineal

Departamento de Matemática

Facultad de Ciencias Exactas y Naturales

Universidad de Buenos Aires

2011

Cursos y Seminarios de Matemática – Serie A

Fascículo 12

ISSN 1853-709X (Versión Electrónica)
ISSN 0524-9643 (Versión Impresa)

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria – Pabellón I
(1428) Ciudad de Buenos Aires
Argentina.
http://www.dm.uba.ar
e-mail. secre@dm.uba.ar
tel/fax: (+54-11)-4576-3335

FASCICULO 12

cursos y seminarios de matemática

Jean Dieudonné

ALGEBRA LINEAL

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES - DEPARTAMENTO DE MATEMATICA

1964

CURSOS
FASCICULO 12 | Y SEMINARIOS
DE MATEMATICA

Jean Dieudonne

ALGEBRA LINEAL

U N I V E R S I D A D D E B U E N O S A I R E S

FACULTAD DE CIENCIAS EXACTAS Y NATURALES - DEPARTAMENTO DE MATEMATICA

1964

Este fascículo consiste en la recopilación y redacción unificada de las exposiciones que se realizaron en el seminario que, con el mismo nombre, dirigió el Profesor Jean Dieudonné en el Centro Regional de Matemática para Américs Latina en los meses de agosto, setiembre y octubre del presente año. Dichas exposiciones fueron realizadas (aparte de las del propio Profesor Dieudonné) por los becarios del Centro Regional y corresponden, aproximadamente, a las siguientes partes del libro:

Primera exposición: a cargo de J. Dieudonné (§ 1 y § 2)

Segunda: Jean Dieudonné (§§ 3,5,6 y 7)

Tercera: Héctor Merklen (Uruguay) (§ 10)

Cuarta: José Luis Benza (Paraguay) (§ 11)

Quinta: Horacio Feliciángeli (Paraguay)(§ 4 y Ap.III)

Sexta: César Carranza (Perú) (§§ 9,12 y 13)

Séptima: Roberto Velázquez (Perú) (Ap. II)

Octava: Alonso Viteri (Ecuador)(§ 8) y Héctor Merklen (partes 1,2 y 3 del Ap. IV).

Novena: Jean Dieudonné (partes, 4,5 y 6 del Ap. IV)

Para la redacción del resto me he valido libremente del tratado de Bourbaki.

El Profesor Dieudonné, a quien se debe todo lo original que se encuentre en este fascículo, se impuso a sí mismo la ingrata tarea de supervisar y corregir la redacción definitiva. Además, debemos agradecer especialmente a los profesores de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires, Dres. Luis Santaló y Cora R. de Sadosky y al Profesor de la Universidad del Sur, Antonio Monteiro, por haber leído y criticado el manuscrico. Finalmente, nosotros, los becarios del Centro Regional, debemos nuestro agradecimiento al Dr. Alberto González Domínguez, Director del Centro y Jefe del Departamento de Matemática de la Facultad de Ciencias Exactas y Naturales y en general a las autoridades y personal de esta Facultad, por hacer posible la publicación de éste, nuestro trabajo.

Buenos Aires, noviembre, 1961. Héctor Merklen

CAPITULO 0

INTRODUCCION

Desde el punto de vista actual, la geometría elemental en dos o tres dimensiones se reduce al estudio de una forma cuadrática no degenerada sobre un espacio vectorial sobre el cuerpo $\mathbb{R}$ de los números reales. Como ejemplo ilustrativo basta pensar el plano euclídeo como conjunto de pares ordenados de números reales (vectores salientes del origen) (a,b) entre los cuales están definidas las operaciones de suma y producto por escalares:

$$(a,b) + (c,d) = (a+c\ ,\ b+d)$$

$$\lambda.(a,b) = (\lambda a, \lambda b) \qquad (\lambda \in \mathbb{R})$$

junto con una forma cuadrática positiva no degenerada:

$$|(a,b)|^2 = a^2 + b^2$$

que da el cuadrado de la longitud $|(a,b)|$ del vector (a,b) o el cuadrado de la distancia del punto (a,b) al origen.

Esta, la primera, aparición de la teoría de las formas cuadráticas en la matemática, y más concretamente en la geometría, data de las épocas griega y babilónica; y es prácticamente la única (en esas épocas) ya que, por ejemplo, la noción de ortogonalidad, que hoy se nos aparece como ligada estrechamente a la forma cuadrática básica, era introducida en la antigüedad por medio de la noción de ángulo recto (que descansaba a su vez en los conceptos poco claros de ángulos, rectas, etc.). El "puente" entre los dos tipos de concepciones lo constituye el teorema de Pitágoras.

Luego, el avance de la geometría analítica con Fermat y Descartes mostró la íntima relación entre las formas cuadráticas y la teoría de las cónicas (por ejemplo, Fermat ya sabe que una ecuación de segundo grado en el plano representa una cónica), y problemas de ésta y otras teorías impulsaron al estudio de las formas cuadráticas por sí mismas (por ejemplo, el problema de la reducción de la ecuación de una cónica a ejes principales condujo a la reducción de una forma cuadrática a suma de cuadrados y a la búsqueda de sus ejes respecto de una forma métrica). Modernamente se ha puesto en evidencia que las nociones de polaridad, elementos conjugados y tangentes en las cónicas o cuádricas son meros ejemplos de relaciones de ortogonalidad respecto de formas cuadráticas distintas de la forma métrica (cf. Cap. IV, § 11).

El siglo XVII ve comenzar la geometría proyectiva, y, sobre todo con Poncelet, se pasa luego a la geometría proyectiva compleja (de la cual algo se había esbozado antes con la aparición esporádica de "puntos imaginarios"). Así se comienzan a manifestar los primeros motivos que llevarían luego al estudio de formas cuadráticas sobre espacios vectoriales generales sobre cuerpos de base también generales.

Los últimos pasos en la evolución general de la geometría, dependieron esencialmente de la aparición de la noción moderna de aplicación puntual y de la noción de dualidad (que se refiere luego a la teoría de las formas bilineales); también dependieron del nuevo enfoque de las propiedades métricas y proyectivas, por una parte, y de las geometrías euclidenas y no euclidianas, por otra. Así se llegó al convencimiento de que toda la geometría clásica consiste en el estudio de propiedades o relaciones entre invariantes o covariantes de ciertos grupos (como por ejemplo el de las semejanzas): es la tesis de Klein en su célebre "programa de Erlangen".

Así en el último siglo los trabajos se encaminaron más bién hacia el estudio de los grupos lineales, ortogonales, simplécticos, etc. (los "grupos clásicos") que aparecían como los grupos característicos de las geometrías métrica, proyectiva, o de la geometría del "complejo lineal"; y, en relación con estos estudios, se desarrolló el estudio de las formas cuadráticas y bilineales asociadas a ellas (primero bajo la forma de "producto escalar" en el "cálculo vectorial") y también de las formas sesquilineales hermitianas, etc.

Además de la tendencia generalizadora que distingue la matemática moderna hay razones histórico-prácticas para los sucesivos abandonos de las restricciones al cuerpo de escalares y a la dimensión del espacio. Es bien conocido el caso del pasaje del cuerpo real, R , al cuerpo complejo, C . A fines del siglo XIX, Hilbert y sus émulos fueron llevados, debido a sus investigaciones en torno a los "fundamentos", a construir "geometrías" de tipo completamente nuevo tomando cuerpos más o menos patológicos, para dar ejemplos y contraejemplos apropiados en su estudio de las relaciones entre los diversos axiomas. También, desde Galois, se fueron introduciendo aplicaciones lineales con coeficientes y valores en cuerpos primos finitos, lo que llevó naturalmente al estudio de las formas sesquilineales y cuadráticas, y de los grupos clásicos, sobre estos cuerpos y sobre los cuerpos finitos en general. Y es de notar que los grupos clásicos así generalizados aparecieron como importantes en dominios variados de la matemática clásica y moderna (por ejemplo en el estudio de los períodos de las integrales abelianas).

-o-

En todo este libro, nos limitaremos al caso de cuerpos conmutativos (generalmente de característica distinta de 2) y a espacios vectoriales de dimensión finita. El libro (excepto parte del apéndice IV) está contenido (y en forma más general) en el

texto, y/o apéndices y/o ejercicios de BOURBAKI: "Eléments de Mathématique", Livre II: Algèbre, Chap. 1,2,3 y 9 (especialmente este último).

-o-

REQUISITOS

Como este libro está destinado especialmente a los profesores de enseñanza secundaria, suponemos que el lector tendrá cierta familiaridad con el lenguaje de la matemática moderna, y que conoce los conceptos y propiedades fundamentales del álgebra y, en particular, del álgebra lineal.(#)

Procederemos a describir estos conceptos y mencionar algunas de sus propiedades sin cuidarnos excesivamente del rigor ni de las demostraciones.

Es sabido que se denomina ley de composición (interna) entre elementos de un conjunto E a toda aplicación f que asigna a cada par (a,b) de un conjunto de pares $A \subset E \times E$ un elemento $f(a,b) \in E$. A es el dominio de definición de f; $f(a,b)$ se llama el compuesto de a y b por f. Si $A = E \times E$ uno dice que f está definida en todas partes o sobre todo E. Es cómodo remplazar la notación $f(a,b)$ por $a \top b$ (donde "$\top$" es un signo apropiado, usualmente "+" ó "·"). Las leyes que verifican la condición: $a \top (b \top c) = (a \top b) \top c$ $(a,b,c \in E)$ se denominan asociativas y es costumbre notarlas multiplicativamente; las que verifican: $a \top b = b \top a$ $(a,b \in E)$ se llaman conmutativas y suelen notarse aditivamente. Por lo general, las leyes de composición se consideran extendidas a las familias finitas de elementos en la forma usual: $a_1 \top a_2 \top \ldots \top a_n = (\ldots((a_1 \top a_2) \top a_3) \top \ldots) \top a_n)$, y valen para las leyes asociativas (resp. conmutativas) los teoremas generales de asociatividad (resp. conmutatividad). Por definición, un elemento $e \in E$ es un elemento neutro para la ley $\top$ si $a \top e = e \top a = a$ $(a \in E)$ (y cuando existe es necesariamente único). Se lo nota 0, 1, en notación aditiva, multiplicativa, respectivamente. Los elementos x, x' tales que $x \top x' = x' \top x = e$ se llaman simétricos; si $\top$ se nota multiplicativamente (resp. aditivamente) se denominan inversos (resp. opuestos).

Una ley de composición externa entre elementos de un conjunto Ω (dominio de operadores) y elementos de un conjunto E es, por definición, una aplicación f que a ciertos pares $(\alpha, a) \in \Omega \times E$ hace corresponder un elemento $f(\alpha, a) \in E$. Si f está definida en todo $\Omega \times E$ se dice que está definida en todas partes. En lugar de la notación $f(\alpha, a)$ se suelen usar las notaciones αa (ó $\alpha.a$) (multiplicativa a la izquierda) ó $a\alpha$ (ó $a.\alpha$) (multiplicativa a la derecha) ó a^{α} (exponencial).

(#) Para detalles, puede consultarse el libro de álgebra lineal de Cotlar-Sadosky.

Dotar a un conjunto E de una estructura algebraica es, por definición, definir en E una o varias leyes de composición internas o externas. Sean E , E' , dos conjuntos con estructuras algebraicas homólogas (por ejemplo dotados de leyes de composición homólogas que representaremos con la misma notación τ_i para E que para E') y f : E $\longrightarrow$ E' una aplicación de E en E' . Entonces, f es un homomorfismo respecto de esas estructuras si "respeta" cada una de las leyes de composición en el sentido siguiente: $f(a \tau_i b) = f(a) \tau_i f(b)$. Si hay leyes externas , un homomorfismo debe respetarlas en sentido análogo. Por ejemplo, si están definidas sendas leyes de composición externas sobre E y E' con el mismo dominio de operadores Ω , y se notan con "$\perp$" , el homomorfismo f debe verificar la condición: $f(\alpha \perp x) = \alpha \perp f(x)$. Si f es un homomorfismo inyectivo (es decir si es un homomorfismo biunívoco) se dice que es un isomorfismo de E en E' y si además es survectiva (es decir es una aplicación de E sobre E') se llama isomorfismo de E sobre E' o se dice que E y E' son isomorfos mediante f . Los homomorfismos de E en E se denominan endomorfismos de E , y los isomorfismos de E sobre E , automorfismos de E .

-o-

Por definición un grupo G es un conjunto G munido de una estructura algebraica de grupo, que es la que define en G una ley de composición interna asociativa , definida sobre G , con elemento neutro e , y tal que (notada multiplicativamente) cada elemento a de G tiene un inverso, a^{-1} (que es necesariamente único). Cuando la ley de grupo de G es conmutativa el grupo se llama conmutativo o abeliano y se nota por lo general aditivamente; en ese caso, el elemento neutro se designa con 0 y el opuesto de a con -a .

Si $H \subset G$ es estable para la ley de grupo (es decir si $a.b \in H$ cuando a y b están en H) y si $a \in H$ implica $a^{-1} \in H$, la restricción a H de la ley de G es una ley de grupo en H y se dice que H es un subgrupo de G . Para cada $x \in G$, la aplicación que a cada $a \in G$ hace corresponder xax^{-1} es un automorfismo de G que se llama automorfismo interior (asociado a x). Si el subgrupo H es estable para automorfismos interiores (es decir si $xhx^{-1} \in H$ para todo $h \in H$ y cualquiera sea $x \in G$) se dice que H es un subgrupo distinguido de G . G y $\{e\}$ son subgrupos distinguidos de G ; si no hay otros, el grupo se llama simple.

Si se define $x \sim y$ (x,y elementos de G) cuando $y \in xH = \{xh/h \in H\}$ (*) donde H es un subgrupo distinguido de G , "$\sim$" es una relación de equivalencia en G tal que: Si $\bar{x}$ representa la clase de equivalencia de x , y si G/H es el conjunto de estas clases, entonces la aplicación $\bar{x}.\bar{y} = \overline{xy}$ es una ley de grupo en

---

(*) Esta notación se interpreta así: Si P(x) es una propiedad que define conjunto, $\{x/P(x)\}$ es el conjunto de los x que tienen la propiedad P .

G/H . Este grupo se denomina grupo cociente de G sobre H . (Puede probarse que para que una relación de equivalencia "$\sim$" en G permita definir en esta forma un grupo G/H es necesario y suficiente que "$\sim$" sea de la forma $y \in xH$ donde H es un subgrupo distinguido distinguido de G).

Se llama centro de G al conjunto de los z tales que $zx = xz$ $(x \in G)$. Es un subgrupo distinguido de G .

Si f es un homomorfismo (de grupos) de un grupo G en un grupo G' (cuyos elementos neutros designamos, respectivamente, e , e') se demuestra que $H = f^{-1}(e') = \{a \in E/f(a) = e'\}$ es un subgrupo distinguido de G , que se llama núcleo de f . El grupo G/H es isomorfo al grupo $f(G) = \{a' \in G' \text{ / existe } a \in G \text{ tal que } f(a) = a'\}$, imágen de G por f . Más precisamente, ese isomorfismo está dado por la aplicación $\bar{f}$ que se define así: $\bar{f}(\bar{x}) = f(x)$.

Si G_1 , G_2 , son dos grupos, la ley de composición definida entre elementos de $G_1 \times G_2$ mediante: $(a,b) \longrightarrow (a_1.b_1 , a_2.b_2)$ (donde a representa el par (a_1,a_2) y b el par (b_1,b_2)) es una ley de grupo y el grupo $G_1 \times G_2$ así obtenido se llama grupo producto de G_1 por G_2 . Esta definición se extiende sin dificultades a cualquier producto cartesiano $\prod_{i \in I} \{G_i\}$, donde cada G_i es un grupo.

Se demuestra que cualquiera sea la parte A del grupo G existe un mínimo subgrupo que contiene a A y que se llama grupo engendrado por A . Este subgrupo está formado por los productos $x_1 x_2 \ldots x_n$ (n natural cualquiera) donde $x_i \in A$ ó $x_i^{-1} \in A$. Los grupos engendrados por un solo elemento se denominan monógenos y entre estos, los que constan de un número finito de elementos se llaman grupos cíclicos. Si H es el subgrupo engendrado por el elemento $a \in G$ y si H tiene p elementos se dice que a es un elemento de orden p de G . En general, si G es un grupo con un número finito p de elementos este número p se llama orden de G. Si a es un elemento de orden p de G , p es el mínimo número natural tal que $a^p = \underbrace{a.a \ldots a}_{p} = e$.

-o-

Se llama anillo, A , cualquier conjunto munido de dos leyes de composición (internas) definidas sobre A (que notaremos con "+" y ".") tales que la primera es una ley de grupo abeliano y la segunda una ley asociativa doblemente distributiva respecto de la primera. En otras palabras, A es un anillo si están definidas una "suma" y un "producto" que satisfacen los siguientes axiomas:

$a + (b+c) = (a+b) + c$.

$a + b = b + a$.

$\exists\ 0 \in A$ tal que $a+0 = 0+a = a$ $(a \in A)$.

Para cada $a \in A$, existe $-a$ A tal que $a+(-a) = 0$

$a(b.c) = (a.b)c$

$a.(b+c) = a.b + a.c$

$(a+b).c = a.c + b.c$

(Estas condiciones se suponen válidas para todo a, todo b, y todo c en A).- En general, si a la segunda ley (producto) se le exige alguna condición suplementaria, el anillo mismo se designa con el calificativo correspondiente. Por ejemplo, si el producto es conmutativo, el anillo se llama conmutativo, etc.

-o-

Se dice que un anillo K es un <u>cuerpo</u> si el conjunto de los elementos de K diferentes de 0 es un grupo respecto de la "multiplicación" de K. Este grupo se designa usualmente con la notación $K^* = K - \{0\}$. El elemento neutro de K^* suele notarse con el símbolo 1 y está caracterizado por la propiedad: $a.1 = 1.a = a$ (cualquiera sea a K). Además, por la misma definición, dado $a \in K$, existe $a^{-1} \in K$ tal que $a.a^{-1} = a^{-1}.a = 1$.

Se llama <u>característica</u> de un cuerpo K (si existe) al mínimo número de sumandos, m, tal que $m.x = \underbrace{x+x+\ldots+x}_{m} = 0$ <u>para todo</u> $x \in K$. Si $x \neq 0$ implica que $m.x \neq 0$ para todo $m \neq 0$ se dice que K es de característica 0.

-o-

<u>REFERENCIA A LOS PRINCIPALES CONCEPTOS Y TEOREMAS DEL ALGEBRA LINEAL</u>

I.- E S P A C I O S V E C T O R I A L E S

Sea A un anillo y E un conjunto munido de <u>una ley de grupo abeliano</u> (notada aditivamente) y <u>una ley externa</u> que tiene a A como dominio de operadores y que (notada multiplicativamente) satisface las siguientes condiciones:

$$\lambda(x+y) = \lambda x + \lambda y \qquad (\lambda+\mu)x = \lambda x + \mu x \qquad \lambda(\mu x) = (\lambda\mu)x$$

(cualesquiera sean λ, μ en A, y x,y en E). En esas condiciones se dice que E <u>es un módulo (a izquierda) con respecto a</u> A, o, más simplemente, que E es un <u>A-módulo</u>. Si A tiene <u>unidad</u> (es decir si la multiplicación tiene elemento neutro) y si la unidad, 1, es también elemento neutro de la ley externa de E: $1.x = x$ (x E), se dice que E es un <u>A-módulo unitario</u>. Los elementos de A suelen llamarse <u>escalares</u>, y la ley externa de E se denomina entonces "producto por escalares".

De acuerdo con la definición general, un <u>homomorfismo</u>, h, de un A-módulo E en un A-módulo E' es una aplicación de E en E' que verifica las condiciones:

$$h(x+y) = h(x) + h(y) \qquad h(\lambda x) = \lambda h(x) \qquad (x,y \in E,\ \lambda \in A)$$

y se le da el nombre especial de <u>aplicación lineal de</u> E <u>en</u> E'

Se llama <u>homotecia de razón</u> $\alpha \in A$ a la aplicación h_α del A-módulo E en sí misma definida por: $h_\alpha(x) = \alpha x$. Es claro que las homotecias "respetan" la suma de E (son homomorfismos respecto de la estructura de grupo abeliano de E) pero no necesariamente son aplicaciones lineales porque $h_\alpha(\beta x) = (\alpha\beta)x \neq (\beta\alpha)x =$

$= \beta h_\alpha(x)$. Para que todas las homotecias sean aplicaciones lineales es suficiente que A sea conmutativo.

-o-

Se dice que E es un espacio vectorial (a izquierda) sobre K si K es un cuerpo y E es un K-módulo unitario. En los espacios vectoriales sólo se consideran homotecias a las de razón $\alpha \neq 0$. Ellas son automorfismos respecto de la estructura de grupo abeliano de E , y si el cuerpo de escalares, K , es conmutativo, son automorfismos de la estructura de espacio vectorial de E .

En lo que sigue se usarán las notaciones: $M+N$, $H.N$ para representar los conjuntos:

$$M+N = \{x+y \;/\; x\in M \;,\; y\in N\} \qquad H.N = \{\lambda x \;/\; \lambda\in H \;,\; x\in N\} \quad \left(\begin{smallmatrix} M,N\subset E \\ H\subset K\end{smallmatrix}\right)$$

Si M y N son subespacios vectoriales, $M+N$ es el mínimo subespacio que los contiene.

Por definición, $M\subset E$ es un subespacio vectorial de E si $x,y \in M$ implica que también $\lambda x+\mu y \in M$ cualesquiera sean $\lambda,\mu \in K$. Si se define $x\sim y$ cuando $x = y+M$, se comprueba que "$\sim$" es una relación de equivalencia en E tal que si entre las clases de equivalencia, $\bar{x},\bar{y},\ldots$ se define: $\bar{x}+\bar{y} = \overline{x+y}$ y $\lambda\bar{x} = \overline{\lambda x}$ $(\lambda\in K)$, se tiene en el conjunto E/M de dichas clases de equivalencia una estructura de espacio vectorial (sobre K) que se llama cociente de la estructura del espacio vectorial de E por la del subespacio M . (Se puede demostrar que para que "$\sim$" sea una relación de equivalencia que permita definir un espacio vectorial cociente en esa forma, es necesario y suficiente que $x\sim y$ sean equivalente a $x = y+M$, donde M es un cierto subespacio vectorial de E .)

Si E_1 , E_2 , son dos espacios vectoriales sobre K , puede definirse en $E_1 \times E_2$ una estructura de espacio vectorial (sobre K) mediante las leyes:

$$(x_1,x_2)+(y_1,y_2) = (x_1+y_1 \;,\; x_2+y_2) \quad ; \quad \lambda(x_1,x_2) = (\lambda x_1 \;,\; \lambda x_2)$$

$(\lambda\in K \;,\; x_1,y_1\in E_1 \;,\; x_2,y_2\in E_2)$. El espacio vectorial $E_1 \times E_2$ que resulta se llama producto de E_1 por E_2 . Esta definición se extiende sin dificultades a cualquier producto cartesiano $\prod_{i\in I}\{E_i\}$, donde cada E_i es un espacio vectorial (sobre K) . El propio cuerpo K puede considerarse, respecto de sus operaciones de suma y producto, como un espacio vectorial sobre sí mismo. El espacio $\underbrace{K\times\ldots\times K}_{n}$ se representa con la notación K^n .

-o-

Consideremos una familia finita: $\{M_i\}$ $(1\leq i\leq n)$ de subespacios vectoriales de E . Supongamos que cada $x\in E$ admite una y sólo una expresión de la forma: $x = m_1+m_2+\ldots+m_n$ $(m_i\in M_i)$. En esas condiciones, se dice que E es suma directa de los subespacios $\{M_i\}$ y se escribe: $E = M_1 \oplus M_2 \oplus \ldots \oplus M_n$. En este ca

so, también es E isomorfo al espacio producto: $M_1 \times M_2 \times \dots \times M_n$ (mediante la aplicación que a $(m_1,\dots,m_n) \in M_1 x \dots x M_n$, hace corresponder $m_1+\dots+m_n \in E$.) .

Si $E = M \oplus N$, se dice que M y N son <u>suplementarios</u> (entre sí). Se demuestra que para que esto ocurra es necesario y suficiente que $E = M + N$, y que además $M \cap N = \{0\}$. En este caso, la aplicación que a cada $x \in M$ hace corresponder su clase $\bar{x}$ en el cociente E/N es un isomorfismo de M sobre E/N . Por lo tanto dos subespacios suplementarios de uno mismo son isomorfos entre sí. Todo subespacio M admite por lo menos un suplementario N en E .

Si $\{\lambda_i\}_{i \in I}$ es una familia de escalares tal que sólo un número finito de ellos $\{\lambda_i\}_{i \in J}$ (J , parte finita de I) son diferentes de 0 , convendremos en representar la suma $\sum_{i \in J} \lambda_i x_i$ (donde $\{x_i\}_{i \in I}$ es una familia de elementos de E con el mismo conjunto de índices) con la notación: $\sum_{i \in I} \lambda_i x_i$, y diremos que es una <u>combinación lineal</u> de elementos de E (más precisamente: una combinación lineal de los elementos $x_i \in E$). Las combinaciones lineales de $\{x_i\}_{i \in I}$ constituyen un subespacio de E que es el mínimo subespacio que contiene la familia $\{x_i\}$ y se llama <u>subespacio engendrado</u> por la parte $\{x_i\} \subset E$.

La familia $\{x_i\}_{i \in I}$ se llama <u>libre</u> (y sus elementos, <u>linealmente independientes</u>) si la relación $\sum_{i \in I} \lambda_i x_i = 0$ implica $\lambda_i = 0$ para todo $i \in I$. Las familias que no son libres se llaman <u>ligadas</u> y se dice que sus elementos son <u>linealmente dependientes.</u> Una <u>base</u> de E es, por definición, una familia libre que engendra E . Todo espacio vectorial admite una base $\{e_i\}_{i \in I}$ y dos bases diferentes tienen el mismo cardinal, que se llama <u>dimensión</u> de E y se nota $\dim(E)$. Si $\{e_i\}$ es una base de E , E es suma directa de la familia de subespacios Ke_i . En todo lo que sigue de este libro <u>sólo consideraremos espacios vectoriales de dimensión finita sobre cuerpos conmutativos</u>.

Si M es un subespacio de E , entonces $\dim(M) \leq \dim(E)$. El número natural $\dim(E) - \dim(M) = \operatorname{codim}(M)$ se denomina <u>codimensión</u> del subespacio M (en E). Si M y N son dos subespacios de E valen las fórmulas de Grassmann:

$$\dim(M+N) + \dim(M \cap N) = \dim(M) + \dim(N)$$

$$\operatorname{codim}(M+N) + \operatorname{codim}(M \cap N) = \operatorname{codim}(M) + \operatorname{codim}(N) \quad .$$

Los subespacios de dimensión 1 y 2 se llaman, respectivamente, <u>rectas</u> y <u>planos</u> ; los subespacios de codimensión 1 , se llaman <u>hiperplanos</u>. Todo subespacio de E es igual a la intersección de los hiperplanos que lo contiene.

-o-

Si u es una aplicación lineal del espacio vectorial E (sobre K) en el espacio vectorial F (sobre K), $u(E)$ es un subespacio de F y $N = u^{-1}(0) =$

$= \{x \in E \,/\, u(x) = 0\}$, <u>núcleo</u> de u , es un subespacio de E . El espacio $u(E)$ es isomorfo al espacio cociente E/N , y su dimensión se llama <u>rango</u> de u . En tonces: rango de u = dim $(u(E))$ = codimen $(u^{-1}(0))$.

Si $F = F_1 \oplus \dots \oplus F_n$, cada $y \in F$ se escribe de modo único en la forma $y = y_1 + \dots + y_n$ $(y_i \in F_i)$. Sea p_i la proyección de F en F_i , es decir la aplicación (lineal) que a cada y F hace corresponder su componente $y_i \in F_i$. Sea u_i la aplicación lineal que a cada $x \in E$ hace corresponder la componente de $u(x)$ en F_i , es decir: $u_i = p_i.u$. Entonces u determina perfectamente las aplicaciones u_i y además: $u(x) = \sum_i p_i(u(x)) = \sum_i u_i(x)$. Recíprocamente, si se dan n aplicaciones lineales $\{u_i\}$ donde $u_i : E \longrightarrow F_i$, y se define $u(x) = \sum_i u_i(x)$, resulta que u es una aplicación lineal de E en F y la "componente" $p_i.u$ de E en F_i es justamente u_i .

Si en lugar de suponer que F se descompone en suma directa suponemos $E = E_1 \oplus \dots \oplus E_m$, y si llamamos p_j a la proyección de E en E_j , entonces como $u(x) = u(\sum_j p_j(x)) = \sum_j u(p_j(x))$, si se pone u_j = restricción de u a E_j , se ve que u determina las u_j y vale la expresión $u(x) = \sum_j u_j(p_j(x))$. Recíprocamente si se dan m aplicaciones lineales $\{u_j\}$ donde $u_j : E_j \longrightarrow F$, y si se define $u(x) = \sum_j u_j(p_j(x))$, resulta que u es una aplicación lineal de E en F cuya restricción a E_j es u_j .

Si se supone simultaneamente que $E = E_1 \oplus \dots \oplus E_m$, $F = F_1 \oplus \dots \oplus F_n$ el primer razonamiento se aplica a las u_j que son aplicaciones lineales de E_j en la suma directa F . Si se pone $u_{ij} = p_i(u_j(x))$ $(x \in E_j)$ se tiene que $u(x) = \sum_j u_j(p_j(x)) = \sum_i \sum_j u_{ij}(p_j(x))$ $(x \in E)$.

En particular, sea $\{e_j\}_{1 \le j \le m}$ una base de E , y $\{f_i\}_{1 \le i \le n}$ una base de F . Entonces E es suma directa de las rectas Ke_j , y F es suma directa de las rectas Kf_i . Un elemento $x \in E$ (resp. $y \in F$) se escribe de modo único en la forma $x = \sum_j x^j e_j$ (resp. $y = \sum_i y^i f_i$) y los (x^j) (respec. (y^i)) se denominan <u>coordenadas</u> de x (resp. y) respecto de la base (e_j) (resp. (f_i)). Si $u : E \longrightarrow F$ es lineal, las u_{ij} de antes son aplicaciones lineales de E_j en F_i , que son espacios unidimensionales. Entonces u_{ij} está perfectamente determinada por los escalares a_{ij} tales que: $u_{ij}(e_j) = a_{ij} f_i$ y la fórmula de antes se escribe:

$$u(x) = \sum_j x^j u(e_j) = \sum_i \sum_j x^j u_{ij}(e_j) = \sum_i \sum_j a_{ij} x^j f_i$$

que nos dice que las coordenadas (y^i) del vector $y = u(x)$ son:

$$y^i = \sum_j a_{ij} x^j$$

Si se nota $\mathcal{L}(E,F)$ el conjunto de las aplicaciones lineales de E en F, se le puede dar una estructura de espacio vectorial sobre K mediante las definiciones:

$$(u+v)(x) = u(x) + v(x)$$
$$(\lambda u)(x) = \lambda u(x) \qquad (\lambda \in K \ , \ x \in E \ , \ u,v \in \mathcal{L}(E,F))$$

Si se hace corresponder a cada $u \in \mathcal{L}(E,F)$ la matriz $M(u) = (a_{ij})$ definida más arriba, que tiene n filas y m columnas, la correspondencia $u \longrightarrow M(u)$ es una biyección de $\mathcal{L}(E,F)$ sobre el espacio vectorial de las matrices de $n \times m$ y es también un isomorfismo entre sus estructuras de espacios vectoriales. Naturalmente, este isomorfismo depende esencialmente de las bases (e_j), (f_i). Si los vectores $x \in E$, de coordenadas (x^j), $y \in F$, de coordenadas (y^i) se representan por matrices columnas:

$$x = \begin{pmatrix} x^1 \\ x^2 \\ \vdots \\ x^m \end{pmatrix} \qquad y = \begin{pmatrix} y^1 \\ y^2 \\ \vdots \\ y^n \end{pmatrix}$$

la fórmula $y^i = \sum_j a_{ij}x^j$ adquiere la expresión compacta (en notación matricial) siguiente:

$$M(u).x = y$$

Si se nota con $\mathcal{L}(E)$ el espacio vectorial de las aplicaciones lineales de E en E (endomorfismos de E), vale todo lo anterior con la particularidad de que las matrices son cuadradas de orden m. Además, puede definirse en $\mathcal{L}(E)$ una operación de producto:

$$(uv)(x) = u(v(x))$$

que convierte a $\mathcal{L}(E)$ en un <u>anillo</u> (con unidad) y también en un <u>álgebra sobre</u> K (ver más adelante). Además la correspondencia entre endomorfismos y matrices es también un isomorfismo para las correspondientes estructuras de anillo y de álgebras : $M(uv) = M(u).M(v)$.

Se designa con $GL(E)$ (grupo general lineal o <u>grupo lineal</u>) a la parte de $\mathcal{L}(E)$ formada por los <u>automorfismos</u> de E, que es evidentemente un grupo respecto del producto de $\mathcal{L}(E)$. Este grupo es isomorfo al grupo $GL(m,K)$ de los automorfismos del espacio $K^m = \underbrace{K \times K \times \ldots \times K}_{m}$, y también isomorfo al grupo multiplicativo de las matrices inversibles de orden m (cf. Ap. IV). Su centro está formado por las homotecias de E.

(Para simplificar) llamamos <u>determinante</u> de un endomorfismo u de E al determinante de la matriz $M(u)$. (Se demuestra que si dos matrices representan el mismo endomorfismo respecto de bases diferentes tienen el mismo determinante, de modo que

la definición es formalmente correcta). La aplicación $u \longrightarrow \det(u)$ es un homomorfismo del grupo $GL(E)$ en el grupo multiplicativo $K^{\#}$ y el núcleo de este homomorfismo es entonces un subgrupo distinguido de $GL(E)$ que se designa $SL(E)$ (grupo especial lineal). El subgrupo especial lineal $SL(m,K)$ de $GL(m,K)$ está formado (a menos de isomorfismo) por las matrices de orden m de determinante igual a 1, que se llaman matrices unimodulares.

-o-

Se designa con $E^{\#}$ (dual de E) el espacio vectorial de las aplicaciones lineales de E en K, $\mathcal{L}(E,K)$, para lo cual se considera a K como espacio vectorial sobre sí mismo. Los elementos de $E^{\#}$ reciben el nombre especial de formas lineales de E.

Si, para cada $x \in E$, se define $\tilde{x}(x') = x'(x)$ $(x' \in E)$ se ve que $\tilde{x}$ es una forma lineal sobre E, y la aplicación $x \longrightarrow \tilde{x}$ de E en $(E^{\#})^{\#} = E^{\#\#}$ es una aplicación lineal que (con nuestras hipótesis) es también un isomorfismo entre E y $E^{\#\#}$. Es fácil concluir de esto que $E^{\#}$ también es isomorfo a E, y que, en particular, tiene la misma dimensión que E. (No obstante, no existe ningún isomorfismo canónico o natural de E sobre $E^{\#}$.)

Es usual representar el escalar $x'(x)$ $(x \in E,\ x' \in E)$ con la notación $\langle x,x' \rangle$. La aplicación $(x,x') \longrightarrow \langle x,x' \rangle$ del espacio producto $E \times E^{\#}$ en K goza de las propiedades siguientes:

$$\langle x+y\ ,\ x' \rangle = \langle x,x' \rangle + \langle y,x' \rangle \qquad \langle \lambda x,x' \rangle = \lambda \langle x,x' \rangle$$

$$\langle x\ ,\ x'+y' \rangle = \langle x,x' \rangle + \langle y,y' \rangle \qquad \langle x, \lambda x' \rangle = \lambda \langle x,x' \rangle$$

y por eso se llama forma bilineal canónica sobre E y $E^{\#}$ (cf. (1.1)).

Se dice que $x \in E$ y $x' \in E^{\#}$ son ortogonales cuando $\langle x,x' \rangle = 0$. Si M es una parte de E, y si M' es el conjunto de los $x' \in E^{\#}$ ortogonales a cada elemento de M (ortogonales a M) se cumple que M' es un subespcio de $E^{\#}$ que se denomina el subespacio ortogonal a M. Es claro que si $M \subset N$, entonces $M' \supset N'$. Si además M es un subespacio de E de dimensión p, M' es un subespacio de $E^{\#}$ de dimensión $n-p$ (de codimensión p) y $(M')' = M''$ es idéntico a M (cuando se identifica E con $E^{\#\#}$ mediante el isomorfismo canónico mencionado más arriba). Además, valen las fórmulas:

$$(M+N)' = M' \cap N' \qquad (M,N \text{ subespcios de } E \text{ o de } E'')$$

$$(M \cap N)' = M' + N'$$

Para todo hiperplano H de E existe una forma lineal $x'_H \in E^{\#}$ tal que $H = x'^{-1}_H(0)$ = núcleo de x'_H y dos formas lineales que tengan esa propiedad difieren en un factor escalar constante (el ortogonal a un hiperplano es una recta del espa -

cio dual). Recíprocamente, cualquiera sea $x' \in E^{\#}$ $(x' \neq 0)$ su núcleo $H = x'^{-1}(0)$ es un hiperplano de E. En este caso, la ecuación $x'(x) = 0$ se denomina ecuación del hiperplano H. Para definir una forma lineal que se anula en un hiperplano no basta dar su valor en un punto cualquiera que no esté en el hiperplano.

Sea (e_i) una base de E, y $x' \in E^{\#}$. Podemos escribir: $x'(x) = x'(\sum_i x^i e_i) = \sum_i x^i x'(e_i)$. Si se designa e_i' la forma lineal que a cada x E hace corresponder su i-ésima coordenada, x^i, $e_i'(x) = x^i$, tenemos que $x'(x) = \sum_i x'(e_i) e_i'(x) = \sum_i x'^i e_i'(x)$ (poniendo $x'^i = x'(e_i)$). De ahí se deduce que (e_i') es una base de E, que se llama base dual de (e_i). Además se ve que $x'(e_i) = x'^i$ es justamente la i-ésima coordenada de x' respecto de la base dual. Puede probarse que la base dual (e_i'') de (e_i') en $E^{\#\#}$ coincide con (e_i) cuando se identifica E con $E^{\#\#}$ mediante el isomorfismo canónico $x \longrightarrow \tilde{x}$.

-o-

Sean E, F dos espacios vectoriales (como siempre de dimensión finita) sobre K; sea $u \in \mathcal{L}(E,F)$, e $y' \in F^{\#}$. Entonces es claro que la aplicación $y'(u(x))$ de E en K es una forma lineal, x', sobre E. De ese modo, para cada $y' \in F^{\#}$ tenemos asignado un $x' \in E^{\#}$. Esta aplicación $y' \longrightarrow x'$ de $F^{\#}$ en $E^{\#}$, es también lineal, se denomina traspuesta de u y se representa con la notación ${}^t u$. De acuerdo con esta definición, ${}^t u$ está determinada por la ecuación:

$$\langle x , {}^t u(y') \rangle = \langle u(x) , y' \rangle$$

Si $M(u)$ es la matriz de u respecto de ciertas bases de E y F, la matriz traspuesta ${}^t M(u)$ (que se obtiene de $M(u)$ cambiando filas por columnas) es justamente la matriz de ${}^t u$ respecto de las bases duales en $F^{\#}$ y $E^{\#}$.

II.- A L G E B R A S .

Sea E un anillo y A un anillo conmutativo con unidad 1. Por definición, E es un álgebra sobre A si está definida además en E una ley de composición externa $(\alpha, x) \longrightarrow \alpha x$, con A como dominio de operadores (también llamado en este caso anillo de escalares) tal que $(\alpha x)y = x(\alpha y) = \alpha(xy)$ y tal que la suma del anillo E y esa ley externa definen en E una estructura de módulo unitario. El caso que nos interesará es cuando A es un cuerpo conmutativo, y entonces esa última estructura hace de E un espacio vectorial sobre K.

Limitémonos al caso en que el álgebra E (como espacio vectorial) es de dimensión finita n. Entonces la multiplicación de E está determinada cuando se conocen los productos de los elementos e_i de una base de E: $e_i e_j = \sum_k \lambda_{ijk} e_i$. En efecto: $(\sum_i x^i e_i)(\sum_j y^j e_j) = \sum_{i,j} (x^i y^j)(e_i e_j)$. Estos datos suelen disponerse en un cuadrado que se denomina tabla de multiplicación del álgebra E:

1^{er} factor \ 2^{o} factor	e_1	e_2	$\cdots$	e_j	$\cdots$	e_n
e_1	$\sum_k \lambda_{11k}\, e_k$	$\sum_k \lambda_{12k}\, e_k$		$\sum_k \lambda_{1jk}\, e_k$		
e_2						
$\vdots$						
e_i	$\cdots$	$\cdots$		$\sum_k \lambda_{ijk}\, e_k$	$\cdots$	$\cdots$
$\vdots$						
e_n						

Si A es un anillo conmutativo con unidad 1, se llama <u>extensión cuadrática</u> de A a toda álgebra E (sobre A) que admite una base formada por dos elementos $1,u$, uno de los cuales es la unidad de E. La aplicación $\alpha \longrightarrow \alpha.1$ que es biunívoca, permite identificar entonces a A con una parte de E, y entonces todo elemento de E se escribe de un único modo en la forma: $a + bu$ $(a,b \in A)$. El álgebra E es conmutativa y su tabla de multiplicación es de la forma:

1^{er} factor \ 2^{o} factor	1	u
1	1	u
u	u	$u^2 = \alpha u + \beta$

de modo que el álgebra E está perfectamente determinada por la relación $u^2 = \alpha u + \beta$.

Sea K un cuerpo conmutativo <u>de característica diferente de 2</u>. En ese caso, se puede sustituir el generador u de una extensión cuadrática E de K por un elemento v de E tal que $(1,v)$ siga siendo una base de E y tal que $v^2 = \delta \in K$. Entonces, <u>si</u> δ <u>no es un cuadrado en</u> K, <u>resulta que</u> E <u>es un cuerpo</u> (el inverso del elemento $a+bv$ está definido por

$$\frac{1}{a+bv} = \frac{a}{a^2 - \delta b^2} - \frac{b}{a^2 - \delta b^2} v \quad).$$

En cambio, si $\delta = \gamma^2 \neq 0$ $(\gamma \in K)$, tomando la base

$$e_1 = \tfrac{1}{2}\left(1 + \frac{1}{\gamma} v\right) \qquad e_2 = \tfrac{1}{2}\left(1 - \frac{1}{\gamma} v\right)$$

que verifica las relaciones: $e_1^2 = e_1$, $e_2^2 = e_2$, $e_1 e_2 = e_2 e_1 = 0$, resulta que

E es compuesto directa de los dos cuerpos Ke_1 , Ke_2 (isomorfos a K) en el sentido de que todo elemento de E se escribe de modo único en la forma $ae_1 + be_2$ y además: $(ae_1+be_2)(a'e_1+b'e_2) = aa'e_1 + bb'e_2$. El caso $\delta = 0$ no nos interesa aquí (cf.: Bourbaki, Alg., Ch. 2).

Si E es una extensión cuadrática del cuerpo K y se mantiene la notación de antes: $x = a + bv$, etc., se define el conjugado $\bar{x}$ de un elemento x E mediante la expresión: $\bar{x} = a - bv$. Esta aplicación tiene las siguientes propiedades: $x + \bar{x} = 2a \in K$; $x.\bar{x} = a^2 - \delta b^2 \in K$; $\bar{\bar{x}} = x$. El escalar $x\bar{x}$ se representa con $N(x)$ y se llama norma de x y tiene las propiedades inmediatas siguientes: $N(x) = N(\bar{x})$; $N(xy) = N(x)N(y)$.

-o-

Sea A un anillo conmutativo con unidad y E un álgebra sobre A que admite una base de 4 elementos uno de los cuales es la unidad de E : 1,u,v,w . Se identifica A con una parte de E mediante la inyección $\alpha \longrightarrow \alpha.1$. Si además la tabla de multiplicación de E es de la forma que se indica a continuación, se dice que E es el álgebra de cuaterniones de A relativa al par (α,β) y (1,u,v,w) se llama base canónica de la misma.

	2^o factor			
1^{er} factor	1	u	v	w
1	1	u	v	w
u	u	α	w	αv
v	v	-w	β	$-\beta u$
w	w	$-\alpha v$	βu	$-\alpha\beta$

$(\alpha, \beta \in A \ , \alpha\beta \neq 0)$

Dado $x = a + bu + cv + dw \in E$, se llama conjugado de x al elemento $\bar{x} = a - bu - cv - dw$. La aplicación $x \longrightarrow \bar{x}$ es una aplicación biunívoca, lineal e involutiva (es decir $\bar{\bar{x}} = x$) de E en sí mismo tal que $\overline{xy} = \bar{y}\,\bar{x}$, es decir es un isomorfismo respecto de la estructura de espacio vectorial de E , pero invierte el orden del producto. Tales aplicaciones se denominan antiautomorfismos de E . También valen las propiedades: $x + \bar{x} = 2a \in A$ y $x\bar{x} = \bar{x}x = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2 \in A$. Se usa la notación $N(x) = x\bar{x}$ = norma de x = norma de $\bar{x}$ y también aquí vale la propiedad: $N(xy) = N(x).N(y)$. Los elementos x de primera componente nula, es decir los de la forma $x = bu + cv + dw$, se denominan cuaterniones puros de E y (cuando A es un cuerpo) constituyen un hiperplano del espacio vectorial E que se nota con la letra P . Si $A = K$ es un cuerpo conmutativo de característica diferente de 2 , la condición necesaria y suficiente para que E sea un cuerpo (no necesariamente conmutativo) es que $x \neq 0$ implica $N(x) \neq 0$. En ese caso, el

inverso de x está definido por: $x^{-1} = \bar{x}/N(x)$. Esta situación se da, por ejemplo, cuando K es el cuerpo $\mathcal{R}$ de los números reales y α y β se eligen menores que 0 . El cuerpo de cuaterniones clásico se obtiene cuando $K = \mathcal{R}$ y $\alpha = \beta = -1$, y en ese caso es costumbre designar a la base canónica con la notación $(1,i,j,k)$.

III.- ESPACIOS AFINES

Sea E un conjunto sobre el cual opera un espacio vectorial T de dimensión finita n sobre un cuerpo conmutativo K (es decir, para cada $\vec{t} \in T$ existe una aplicación biunívoca de E sobre E que representaremos por $x \longrightarrow x+\vec{t}$) de tal modo que $(x+\vec{t})+\vec{u} = x+(\vec{t}+\vec{u})$ y tal que $x+\vec{0} = x$ para todo $x \in E$. Supongamos además que dado $x \in E$, para cada $y \in E$ existe un $\vec{t} \in T$ tal que $x+\vec{t} = y$ (es decir que T opera transitivamente sobre E , cf. Apéndice IV) y que $\vec{0}$ es el único elemento de T que deja fijo cada punto de E (es decir, T opera fielmente sobre E). En esas condiciones se dice que E es un espacio afín de dimensión $n = \dim(T)$ y los elementos de T se denominan traslaciones de E o vectores libres de E . Dados dos puntos $a,b \in E$, existe una y sólo una traslación $\vec{t} \in T$ tal que $a+\vec{t} = b$, y es común notar esta traslación con $b-a$. Si $a,b,a',b' \in E$, y si $b-a = b'-a'$, entonces también $b'-b = a'-a$ (regla del paralelogramo). Fijado $a \in E$, la aplicación que a cada $x \in E$ hace corresponder la traslación $x-a \in T$ es una correspondencia biunívoca de E sobre T . Cuando se hace esto, se acostumbra decir que se considera E como espacio vectorial tomando a como origen. Esto muestra que la teoría de los espacios afines puede sumergirse en la de los espacios vectoriales (cosa que casi siempre es necesario hacer en la práctica). De hecho, un espació afín "es" en realidad un espacio vectorial sin un origen privilegiado.

-o-

Si V es una parte de un espacio afín E tal que al tomar un punto de V como origen ésta se transforma en un subespacio del espacio vectorial obtenido, se dice que V es una variedad afín de E . Si E se considera como espacio vectorial tomando uno de sus puntos como origen fijo, las variedades afines son exactamente los conjuntos obtenidos al trasladar subespacios de E . Para que V sea una variedad afín es entonces necesario y suficiente que:

$$x_i \in V \quad , \quad \sum \lambda_i = 1 \quad \text{implique} \quad \sum \lambda_i x_i \in V \quad .$$

Por eso estas combinaciones lineales cuyos coeficientes suman 1 se suelen llamar combinaciones lineales afines. Si V' es la variedad afín que se obtiene trasladando (para alguna traslación de T) el subespacio D del espacio vectorial E , se dice que D es la dirección de V , y la dimensión de D se llama dimensión de V. Las variedades de dimensión 1 (resp. $n-1$) se llaman rectas afines (resp. hiperplanos afines), etc. Cuando se considera simultáneamente a E como espacio afín o

como espacio vectorial es conveniente distinguir los subespacios vectoriales de E de las otras variedades afines agregando a los primeros el calificativo "homogéneo" o "por el origen". Así, un hiperplano homogéneo (hiperplano por el origen) es todo subespacio vectorial de E de dimensión $n-1$, en tanto que un hiperplano es una variedad afín de dimensión $n-1$, etc.

Si E es un espacio afín, y si $\sum \lambda_i = 1$, el punto $x \in E$ tal que $x-a = \sum \lambda_i (x_i-a)$ $(a, x_i \in E)$ es independiente del punto elegido como origen y se representa con la notación $x = \sum \lambda_i x_i$ y se llama <u>baricentro</u> de la familia $\{x_i\}$.

Si E, F son espacios afines cuyo espacio de traslaciones es T, toda aplicación u de E en F tal que:

$$u\left(\sum \lambda_i x_i\right) = \sum \lambda_i u(x_i) \qquad \left(\sum \lambda_i = 1\right)$$

se denomina <u>aplicación afín</u> de E en F. Para cada aplicación afín u existe una y sólo una aplicación lineal v de T en T tal que $u(x+\vec{t}) = u(x) + v(\vec{t})$; la aplicación v se denomina la <u>aplicación lineal asociada a la aplicación afín</u> u. La imagen de una variedad afín de E por una aplicación afín de E en F es una variedad afín de F. Las aplicaciones afines biunívocas de E sobre E constituyen un grupo que se denomina <u>grupo afín</u> de E. La aplicación que a cada aplicación afín del grupo afín hace corresponder su aplicación lineal asociada es un homomofismo del grupo afín de E sobre el grupo $GL(T)$ cuyo núcleo está formado por las traslaciones de E, es decir es igual a T.

IV.- ESPACIOS PROYECTIVOS.

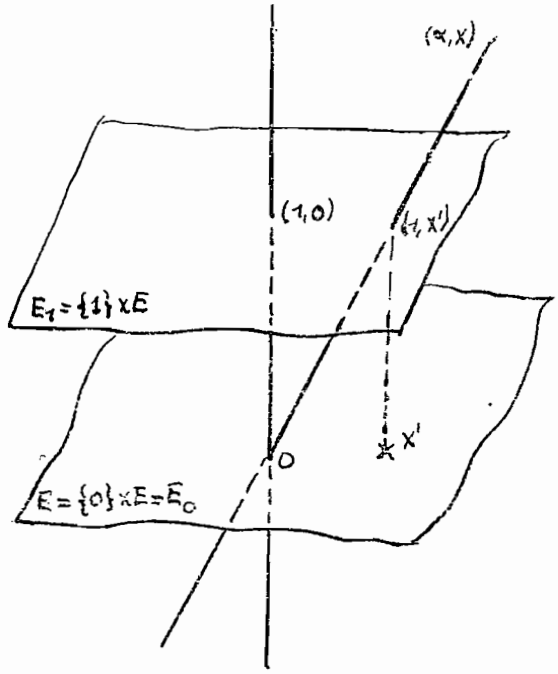
Sea, como siempre, E un espacio vectorial de dimensión finita n sobre un cuerpo conmutativo K. Se llama <u>espacio proyectivo</u>, $P(E)$, <u>deducido de</u> E el conjunto de las rectas de E privadas del origen (que coincide con el conjunto de las clases de equivalencia correspondientes a la relación $x \sim y \iff$ existe $\lambda \neq 0$ en K tal que $y = \lambda x$). El elemento de $P(E)$ que en esta forma corresponde a $x \in E$ se representará con $\bar{x}$ y se llamará <u>imagen canónica</u> de x en $P(E)$. Por definición, la dimensión de $P(E)$ es el número $\dim(E) - 1 = n-1$. El espacio proyectivo deducido de K^{n+1} se designa con la notación abreviada $P_n(K)$ ó $P(n,K)$. Los espacios proyectivos de dimensión 1 (resp. 2) se llaman <u>rectas</u> (resp. <u>planos</u>) <u>proyectivos</u>. Si para una cierta base (e_i) de E, (x^i) son las coordenadas de $x \in E$, se dice que (x^i) es un <u>sistema de coordenadas homogéneas del punto</u> $x \in P(E)$. Para que (x^i) y (x'^i) sean sistemas de coordenadas homogéneas de un mismo punto de $P(E)$ es necesario y suficiente que sean proporcionales, es decir que exista $\lambda \neq 0$ en K tal que $x^i = \lambda x'^i$ (para cada i).

Si F es un subespacio vectorial de E, la imagen canónica de F en $P(E)$,

$\bar{F}$ (es decir el conjunto de rectas privadas del origen que pasan por tres puntos distintos de 0 de F) se llama variedad lineal proyectiva asociada a F , y puede identificarse por un isomorfismo al espacio proyectivo P(F) deducido de F . Las variedades proyectivas asociadas a hiperplanos se denominan hiperplanos proyectivos de P(E) . Así, todas las propiedades de los subespacios vectoriales tienen una traducción en propiedades de las variedades proyectivas.

-o-

Sea E un espacio vectorial de dimensión n sobre el cuerpo conmutativo K . Entonces, el espacio proyectivo P(KxE) deducido del espacio vectorial KxE se denomina espacio proyectivo asociado a E . Su dimensión es igual a la de E . El conjunto $E_1 = \{1\} \times E$ es un hiperplano afín de KxE (trasladado del hiperplano homogéneo $E_0 = \{0\} \times E$) y se observa que si una recta de KxE no está contenida en E_0 , entonces contiene un punto (α, x) $(\alpha \in K \ , \ x \in E)$ con $\alpha \neq 0$, y por tanto también un punto de la forma $(1,x') \in E_1$. Así, la aplicación que a cada $x \in E$ hace corresponder la clase (recta privada de 0) de $(1,x)$ en P(KxE) es una aplicación biunívoca (llamada inyección canónica) de E en P(KxE) . La parte de P(KxE) que no es imagen de ningún elemento de E por esta aplicación es el hiperplano proyectivo $P(E_0)$ (es decir el conjunto de las rectas privadas de 0 que no cortan a E_1) y se llama hiperplano del infinito de P(KxE) , y, por abuso de lenguaje, también se lo llama hiperplano del infinito de E . E Puede identificarse a E_1 o también a su imagen (por la inyección canónica) en P(KxE) y haciendo ésto, los puntos de E se llaman puntos propios de P(KxE) , en tanto que los puntos que están en el hiperplano del infinito se llaman puntos impropios o puntos del infinito. Así, el espacio proyectivo asociado a un espacio vectorial E aparece como formado por los puntos de E más los puntos del infinito(*).

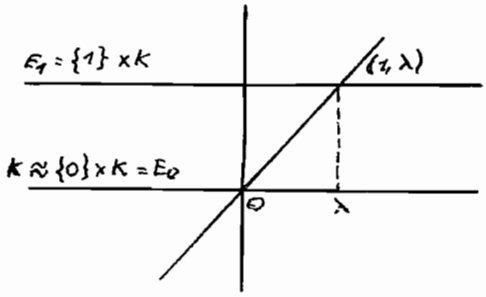


En particular, si E es de dimensión 1 , por ejemplo si $E = K$, el espacio $P_1(K) = P(KxK)$ se representa con $\tilde{K}$ y se suele llamar cuerpo proyectivo asociado

(*) Conviene notar que en esta representación a cada variedad afín V_1 de E_1 le corresponde la variedad proyectiva asociada al subespacio de KxE engendrado por V_1.

al cuerpo K .

Aquí, la inyección canónica de K en $\tilde{K}$ asigna a cada $\lambda \neq 0$ la recta que pasa por $(1,\lambda)$ privada del origen. En este caso, el hiperplano del infinito se reduce a un punto (pues debe tener dimensión 0) que se llama punto del infinito de K (y también de K) y suele representarse con la notación ∞ .



-o-

Sean E , F , dos espacios vectoriales (de dimensión finita) sobre K y sea f una aplicación lineal de E en F cuyo núcleo es $N = f^{-1}(0)$. Es claro que si r es una recta de E no contenida en N , f(r) es una recta de F y esto permite definir una aplicación $\bar{f}$ de P(E) en P(F) mediante $\bar{f}(\bar{x}) = \overline{f(x)}$ = (recta privada de 0 que pasa por f(x) en F) . Según hemos dicho, esa definición sólo tiene sentido si $x \in N$, así que $\bar{f}$ es una aplicación de P(E) - P(N) en P(F) , pero no obstante se la llama aplicación proyectiva de P(E) en P(F) de centro P(N) . Las aplicaciones proyectivas de P(E) sobre P(E) que además son biunívocas forman un grupo que se llama grupo proyectivo de P(E) y se representa con PGL(E) , y es isomorfo al grupo cociente de GL(E) por su centro (esto es: el subgrupo distinguido formado por las aplicaciones $z \in GL(E)$ tales que zu = uz para toda $u \in GL(E)$). Cuando $E = K^{n+1}$ se usa la notación $PGL_n(K)$ ó PGL(n,K) en lugar de $PGL(K^{n+1})$.

HIPOTESIS Y NOTACION

En todo este libro, salvo indicación expresa, sólo se consideran espacios vectoriales de dimensión finita sobre un cuerpo conmutativo. Los espacios vectoriales se notarán con las letras E , F , G , etc.; sus elementos, con x , y , etc.; el cuerpo de base con la letra K y sus elementos con α , λ , μ , etc.

CAPITULO I

FORMAS BILINEALES Y SESQUILINEALES
GENERALIDADES

1.- FORMAS BILINEALES Y APLICACIONES LINEALES ASOCIADAS

1.1.- DEFINICIONES

Se dice que una aplicación φ del espacio vectorial producto $E \times F$ en un espacio vectorial G es bilineal si verifica las condiciones:

$$(B)\quad \varphi(x_1+x_2,\, y) = \varphi(x_1,y) + \varphi(x_2,y) \qquad \varphi(x,\, y_1+y_2) = \varphi(x,y_1) + \varphi(x,y_2)$$

$$\varphi(\lambda x,\, y) = \lambda\varphi(x,y) \qquad \varphi(x,\, \lambda y) = \lambda\varphi(x,y)$$

$$(\forall\, \lambda \in K\ ;\ \forall\, x,\ \forall\, x_1,\ \forall\, x_2 \in E\ ;\ \forall\, y,\ \forall\, y_1,\ \forall\, y_2 \in F)$$

Si φ es bilineal de $E \times F$ en G, consideremos, para cada $y \in F$, la aplicación $d_\varphi(y) : E \longrightarrow G$ definida así: $d_\varphi(y) : x \longrightarrow \varphi(x,y)$ $(x \in E)$; es inmediato que cada $d_\varphi(y)$ es una aplicación lineal de E en G. Análogamente, para cada $x \in E$ la aplicación $s_\varphi(x)$ definida así: $s_\varphi(x) : y \longrightarrow \varphi(x,y)$ $(y \in F)$ es una aplicación lineal de F en G. En otras palabras, para cada $y \in F$, $d_\varphi(y) \in \mathcal{L}(E,G)$, y para cada $x \in E$, $s_\varphi(x) \in \mathcal{L}(F,G)$. Entonces, si se consideran $\mathcal{L}(E,G)$ y $\mathcal{L}(F,G)$ del modo usual como espacios vectoriales (sobre K) las condiciones (B) pueden volver a escribirse en la forma siguiente:

$$(B')\quad s_\varphi(x_1+x_2) = s_\varphi(x_1) + s_\varphi(x_2) \qquad s_\varphi(\lambda x) = \lambda s_\varphi(x)$$

$$d_\varphi(y_1+y_2) = d_\varphi(y_1) + d_\varphi(y_2) \qquad d_\varphi(\lambda y) = \lambda d_\varphi(y)$$

que expresan que $d_\varphi : y \longrightarrow d_\varphi(y)$ es una aplicación lineal del espacio vectorial F en el espacio vectorial $\mathcal{L}(E,G)$, y $s_\varphi : x \longrightarrow s_\varphi(x)$ es una aplicación lineal del espacio vectorial E en el espacio vectorial $\mathcal{L}(F,G)$. La aplicación d_φ (resp. s_φ) se llama aplicación lineal asociada a φ a la derecha (resp. a la izquierda).

Recíprocamente, es un sencillo ejercicio comprobar que si se da una aplicación lineal $d : y \longrightarrow d(y)$ de F en $\mathcal{L}(E,G)$ y si se define $\varphi(x,y) = [d(y)](x)$ entonces $\varphi(x,y)$ es una aplicación bilineal de $E \times F$ en G que tiene a d como aplicación lineal asociada a la derecha. También, si se da una aplicación lineal $s : x \longrightarrow s(x)$ de E en $\mathcal{L}(F,G)$ y se define $\varphi(x,y) = [s(x)](y)$, entonces φ es

una aplicación bilineal de ExF en G cuya aplicación bilineal asociada a la izquierda es s .

-o-

Nos interesará especialmente el caso en que $G = K$: las aplicaciones bilineales de ExF en el cuerpo de escalares K (considerado como espacio vectorial sobre sí mismo) se denominan formas bilineales sobre ExF . Cuando $F = E$, se tienen las formas bilineales sobre ExE que se llaman simplemente formas bilineales sobre E .

En este caso particular las aplicaciones lineales asociadas a ϕ tienen como espacios de llegada a $\mathcal{L}(E,K)$ y $\mathcal{L}(F,K)$ que no son otros que los duales E^* , F^* de E , F , respectivamente. Así, d_ϕ , por ejemplo, hace corresponder a cada $y \in F$ una forma lineal $d_\phi(y) \in E^*$ que, por definición, verifica la igualdad:

$$\phi(x,y) = \langle x , d_\phi(y) \rangle \qquad \text{(para cada } x \in E \text{)}$$

Análogamente, para cada $x \in E$, la forma lineal $s_\phi(x) \in F^*$ verifica la igualdad:

$$\phi(x,y) = \langle y , s_\phi(x) \rangle \qquad \text{(para cada } y \in F \text{)} .$$

1.2.- FORMAS BILINEALES NO DEGENERADAS

Se dice que una forma bilineal sobre ExF es degenerada a la izquierda si existe un elemento no nulo $x_0 \in E$ tal que

$$\phi(x_0,y) = 0 \qquad (\forall\ y \in F)$$

y degenerada a la derecha si existe un elemento no nulo $y_0 \in F$ tal que

$$\phi(x,y_0) = 0 \qquad (\forall\ x \in E)$$

Una forma bilineal simultáneamente degenerada a la izquierda y a la derecha se llama simplemente degenerada.

Recordemos que para que una aplicación lineal sea inyectiva es necesario y suficiente que su núcleo se reduzca a 0 . Ahora bien, si ϕ es degenerada a la derecha (resp. a la izquierda) la forma lineal $d_\phi(y_0)$ (resp. $s_\phi(x_0)$) es nula para cada $y_0 \neq 0$ (resp. $x_0 \neq 0$) que verifica la condición de arriba y por tanto d_ϕ (resp. s_ϕ) no es inyectiva. Recíprocamente (por la misma razón) si d_ϕ (resp. s_ϕ) no es inyectiva entonces ϕ es degenerada a la derecha (resp. a la izquierda). Así se ha probado que una forma bilineal es no degenerada si y sólo si sus dos aplicaciones lineales asociadas son inyectivas. (El teorema 1 de (1.4) amplía un poco este resultado).

1.3.- MATRIZ DE UNA FORMA BILINEAL

Sean (e_i) $(1 \leq i \leq n)$ y (f_j) $(1 \leq j \leq m)$ bases de E y F respectivamente, y sea ϕ una forma bilineal sobre ExF . Entonces las condiciones (B) dicen que ϕ está determinada por los valores $g_{ij} = \phi(e_i, f_j) \in K$ pues si $x \in E$, $y \in F$, estos vectores admiten expresiones únicas de la forma $x = \sum_i x^i e_i$, $y = \sum_j y^j f_j$, y entonces:

$$\phi(x,y) = \phi\Big(\sum_i x^i e_i \, , \sum_j y^j f_j\Big) = \sum_{ij} x^i y^j \phi(e_i, f_j)$$

$$\therefore \qquad \phi(x,y) = \sum_{ij} x^i y^j g_{ij}$$

La matriz (g_{ij}) se denomina matriz de ϕ respecto de las bases (e_i) (f_j) y si F = E y $\{e_i\}$ es idéntica a $\{e_j\}$, es decir si ϕ es una forma bilineal sobre E el determinante de (g_{ij}) se llama discriminante de ϕ y se nota con

$$D_\phi = \det(g_{ij}) = \det(\phi(e_i, e_j))$$

1.4.- ORTOGONALIDAD

Hemos visto que la noción de ortogonalidad aparece de modo natural cuando se considera un espacio vectorial E y su dual E^* , y también sabemos que E es isomorfo a E . Pero como no existe isomorfismo canónico entre E y E^* , no tenemos ningún medio natural de identificar E y E^* para definir una relación de ortogonalidad entre elementos de E . Para ello se necesita dar de alguna manera un isomorfismo particular entre E y E^* y a él quedará referida una tal relación de ortogonalidad. En este número veremos como puede servirnos a tal efecto el conocimiento de una forma bilineal no degenerada sobre E .

Sea ϕ una forma bilineal sobre ExF ; si x E , y F se dice que x e y son ortogonales con relación a ϕ si $\phi(x,y) = 0$. Si E_1 , F_1 , están contenidos, respectivamente, en E , F , se dice que son ortogonales con relación a ϕ si cada elemento de E_1 es ortogonal a cada elemento de F_1 .

El conjunto de los elementos de E ortogonales a F_1 se nota:

$$F_1^0 = \{x \in E \,/\, \phi(x,y) = 0 \text{ para cada } y \in F_1\}$$

y es en todos los casos un subespacio vectorial de E . En efecto, de las condiciones (B) se deduce que si $x_i \in F_1^0$ $(1 \leq i \leq p)$ entonces $\phi(\sum_i \lambda_i x_i \, , y) = \sum_i \lambda_i \phi(x_i, y) = 0$ para cada y F_1 , lo que significa que también $\sum_i \lambda_i x_i \in F_1^0$. El subespacio F_1^0 se llama el subespacio ortogonal a la parte F_1 de F (siempre con relación a ϕ). Análogamente, el conjunto E_1^0 de los elementos de F ortogo-

nales a E_1 es un subespacio de F que se llama el subespacio ortogonal a E_1 (#) .

Es evidente que si H , H' son subespacios de E (resp. de F) y si $H \subset H'$, entonces $H'^{o} \subset H^{o}$ y también $H \subset (H^{o})^{o} = H^{oo}$, pues por la definición todo $x \in H$ es ortogonal a cada y ortogonal a H , es decir a cada $y \in H^{o}$. A su vez esta relación da, como caso particular: $H^{o} \subset H^{ooo}$ (usando en ella H^{o} en lugar de H), y la primera propiedad que mostramos dice que si $H \subset H^{oo}$, entonces $H^{o} \supset H^{ooo}$. Entonces resulta en definitiva: $H^{o} = H^{ooo}$.

Además, con este lenguaje la definición de 1.2 se expresa así: φ es no degenerada a la izquierda si y sólo si $F^{o} = \{0\}$ y no degenerada a la derecha si y sólo si $E^{o} = \{0\}$.

Manteniendo la notación, podemos demostrar ahora que:

Lema 1 :

La dimensión de F/E^{o} es igual a la dimensión de E/F^{o} .

Demostración:

En primer lugar, observemos que si $x_0 \in F^{o}$, $y_0 \in E^{o}$, entonces $\varphi(x+x_0 , y+y_0) = \varphi(x,y)$ ($\forall\, x \in E$, $\forall\, y \in F$) , y eso muestra que sólo depende de las clases $\bar{x}$, $\bar{y}$ de x , y , en los espacios cocientes E/F^{o} , F/E^{o} , respectivamente. Entonces, si se define $\bar{\varphi}(\bar{x},\bar{y}) = \varphi(x,y)$ es claro que $\bar{\varphi}$ es una forma bilineal no degenerada sobre $(E/F^{o})\times(F/E^{o})$. (Esta aplicación $\bar{\varphi}$ tiene importancia en muchas cuestiones y se llama forma bilineal no degenerada asociada a φ).

Entonces, como sabemos, $d_{\bar{\varphi}}$ es una aplicación lineal inyectiva de F/E^{o} en el dual $(E/F^{o})^{\#}$ de E/F^{o} . Por lo tanto, la dimensión de F/E^{o} es menor o igual que la dimensión de $(E/F^{o})^{\#}$, la que a su vez es igual a la de E/F^{o} . Resulta así: $\dim (F/E^{o}) \leq \dim (E/F^{o})$, y razonando en la misma forma con $s_{\bar{\varphi}}$ resulta también $\dim (E/F^{o}) \leq \dim (F/E^{o})$ lo que prueba el lema.

Corolario 1 :

Si φ es además no degenerada, para cada subespacio M (de E ó de F) se verifica $\operatorname{codim} (M^{o}) = \dim (M)$, y $M = M^{oo}$.

Demostración:

Si φ es no degenerada $F^{o} = \{0\}$ y $E^{o} = \{0\}$. Si, por ejemplo, M es subespacio de E , la restricción de φ a $M\times F$ es una forma bilineal sobre $M\times F$ y por lo tanto $\dim (M/F^{o}) = \dim (M) = \dim (F/M^{o}) = \operatorname{codim} (M^{o})$. Aplicando este resulta-

(#) Más adelante (observación que sigue al corolario del teorema 1) se indica la relación entre esta noción de ortogonalidad y la del capítulo 0. Si se usa esto, la demostración precedente es superflua.

do a $M^0 = M^{000}$ que es el ortogonal de M^{00} se tiene que codim (M^0) = dim (M^{00}), lo que prueba que dim (M) = dim (M^{00}) y como $M \subset M^{00}$ eso implica que $M = M^{00}$, lq.q.d.

Corolario 2 :

Si φ es además no degenerada y M, N son subespacios (ambos de E o ambos de F) se tiene:

$$(M+N)^0 = M^0 \cap N^0$$

$$(M \cap N)^0 = M^0 + N^0$$

Demostración:

Es claro que el ortogonal a $M+N$ tiene que ser necesariamente ortogonal a M y a N, es decir: $(M+N)^0 \subset M^0 \cap N^0$, pero también todo elemento de M^0 N^0 es ortogonal a M y a N y por tanto a $M+N$, es decir también: $M^0 \cap N^0 \subset (M+N)^0$. Eso prueba la primera parte.

Para probar la segunda, llamemos G a M^0+N^0, de modo que por lo establecido hasta aquí: $G^0 = M^{00} \cap N^{00} = M \cap N$ (corolario 1). Además, como $M^0 \subset G$, también $G^0 \subset M^{00} = M$. Apliquemos entonces el lema a la restricción de φ a $M \times G$. Se tendrá: dim (M/G^0) = dim (G/M^0), que por lo ya dicho puede escribirse: dim $(M / M \cap N)$ = dim (G/M^0) = codim (M^0) - codim (G) = dim (M) - codim (G). Y como (corolario 1) dim $(M \cap N)$ = codim $(M \cap N)^0$ resulta que dim (G) = dim $(M \cap N)^0$. Finalmente, recordando que $(M \cap N)^0 = G^{00} = G$, esto implica que $G = (M \cap N)^0$ y, visto la definición de G, esto era lo que había que demostrar.

-o-

Este lema 1 permite formular la siguiente definición:

Sea φ una forma bilineal sobre $E \times F$; se llama rango de φ a la dimensión común de E/F^0 y F/E^0.

-o-

Lema 2 :

Las aplicaciones lineales asociadas a una forma bilineal tienen el mismo rango que ella.

Demostración:

Ya hemos visto qúe, por ejemplo, el núcleo de d_φ es E^0, y por lo tanto su rango es igual a dim (F/E^0) = rango de φ. Análoga demostración para s_φ.

-o-

Teorema 1 :

Si dim (E) = dim (F) las condiciones siguientes son equivalentes:

(a) La aplicación d_ϕ es inyectiva

(b) La aplicación d_ϕ es suryectiva (es decir sobre $E^\#$)

(c) La aplicación s_ϕ es inyectiva

(d) La aplicación s_ϕ es suryectiva

(e) La forma bilineal ϕ es no degenerada.

Demostración:

Por la hipótesis $\dim(E) = \dim(E^\#) = \dim(F) = \dim(F^\#)$. Como d_ϕ va de F en $E^\#$, si es inyectiva: $\dim(F) = \dim(d_\phi(F)) \leq \dim(E^\#) = \dim(F)$ prueba que $d_\phi(F) = E^\#$ y por lo tanto (a) implica (b) y, por lo mismo, (c) implica (d) . Ahora, si, por ejemplo, d_ϕ es suryectiva, como su núcleo es E^0 , se tiene que rango de $d_\phi = \dim(F/E^0) = \dim(E^\#) = \dim(F)$, y eso prueba que $E^0 = \{0\}$, es decir que d_ϕ es inyectiva. En esta forma se prueba que (b) implica (a) y que (d) implica (c) . Por otra parte, como (lema 2) d_ϕ y s_ϕ tienen el mismo rango, resulta por argumentos del mismo tipo que (a) es equivalente a (c) . Finalmente, como ya vimos que (a) es equivalente a la afirmación simultánea de (a) y (c) , y como éstas son equivalentes, se tiene que (e) es equivalente a (a) y equivalente a (c) , l.q.d.d.

Corolario:

Si ϕ es además no degenerada se tiene necesariamente $\dim(E) = \dim(F)$ y el teorema es aplicable. Por lo tanto:

(a) s_ϕ (resp. d_ϕ) es un isomorfismo de E sobre $F^\#$ (resp. de F sobre $E^\#$) y en particular para todo $y \in F$ existe un y sólo un $y' = d_\phi(y) \in E^\#$ tal que $\phi(x,y) = \langle x,y' \rangle$ $(\forall x \in E)$.

Además:

(b) Existen bases (e_i) (f_j) de E , F , respectivamente, tales que

$$g_{ij} = \phi(e_i,f_j) = \delta_{ij}$$

donde δ_{ij} es el símbolo de Kronecker, es decir $\delta_{ij} = 0$ si $i \neq j$ y $\delta_{ii} = 1$.

Demostración:

Si ϕ es no degenerada, $E^0 = \{0\}$, y $F^0 = \{0\}$, de modo que (lema 1) $\dim(E) = \dim(F)$. Ahora, por el teorema, d_ϕ es un isomorfismo de F sobre $E^\#$ (y análogamente s_ϕ). Entonces, si (e_i') es la base dual de una base (e_i) de E, la imagen $f_i = d_\phi^{-1}(e_i')$ es una base de F . Como además la base dual tiene la propiedad de que $\langle e_i, e_j' \rangle = \delta_{ij}$, se tiene:

$$\emptyset(e_i,f_j) = \langle e_i , d_\emptyset(f_j)\rangle = \langle e_i , e'_j\rangle = \delta_{ij} \quad ;$$

l.q.d.d.

-o-

OBSERVACION: El teorema anterior permite justificar lo que se adelantó al comienzo de este número pues según él, cuando $\emptyset$ es no degenerada, las dos aplicaciones $d_\emptyset$, $s_\emptyset$, son sendos isomorfismos entre los espacios correspondientes. Por otra parte, las igualdades:

$$\emptyset(x,y) = \langle x , d_\emptyset(y)\rangle = \langle y , s_\emptyset(x)\rangle$$

muestran que $x\in E$ e $y\in F$ son ortogonales con relación a $\emptyset$ si y sólo si $x\in E$ y la forma lineal $d_\emptyset(y)\in E^\#$; ó $y\in F$ y la forma lineal $s_\emptyset(x)\in F^\#$ son ortogonales en el sentido corriente del álgebra lineal. Así, la relación de ortogonalidad entre elementos de E (para el caso en que $\emptyset$ es una forma bilineal sobre E) aparece como un "transporte" a E de la relación natural de ortogonalidad entre E y $E^\#$ que se efectúa identificando $E^\#$ a E mediante el isomorfismo $d_\emptyset^{-1}$. (Conviene observar aquí que, siempre cuando $\emptyset$ es forma bilineal sobre E , la relación de ortogonalidad entre elementos de E aún no es satisfactoria desde el punto de fista de la geometría. En efecto, como $\emptyset(x,y) = 0$ no tien por qué ser equivalente a $\emptyset(y,x) = 0$; esta relación de ortogonalidad no sería simétrica.)

Si se analiza esta situación con más detenimiento se verá que las propiedades de ortogonalidad contenidas en los corolarios 1 y 2 del lema 1 son simples traducciones de las conocidas propiedades de ortogonalidad en el sentido natural del álgebra lineal.

-o-

1.5.- ADJUNTO DE UN ENDOMORFISMO

Mantenemos las hipótesis y notaciones de 1.4 , pero suponemos además que E = F y que $\emptyset$, forma bilineal sobre E , es no dezenerada.

Sea u un endomorfismo de E . Para cada $y\in E$ existe un único $y'\in E$ (cf. corolario del teorema) tal que: $\emptyset(u(x) , y) = (d_\emptyset(y'))(x)$. Pero esta igualdad se escribe, por la definición de $d_\emptyset$ en la forma:

$$\emptyset(u(x) , y) = \emptyset(x,y') \qquad (\forall\, x\in E)$$

Esto nos permite definir una aplicación $u^\# : E \longrightarrow E$ escribiendo: $u^\#(y) = y'$. Por otra parte, es inmediato verificar que $u^\#$ es lineal, es decir es un endomorfismo de E . Este endomorfismo $u^\#$ se denomina adjunto a la izquierda del endomor-

fismo u , y por su definición verifica la condición:

$$\phi(u(x) , y) = \phi(x , u^{\#}(y)) \qquad (\forall x \in E , y \in E)$$

Análogamente, se puede definir (luego de probar su existencia) el adjunto de u a la derecha (que seguiremos designando con $u^{\#}$) y que está determinado por la condición:

$$\phi(x , u(y)) = \phi(u^{\#}(x) , y) \qquad (\forall x \in E , y \in E)$$

Estas fórmulas muestran que si v es el adjunto a la derecha de u , entonces u es el adjunto a la izquierda de v (y recíprocamente).

§2.- FORMAS SESQUILINEALES

Veremos aquí que todos los resultados del §1 se extienden (con la misma demostración) a un tipo más general de aplicaciones denominadas sesquilineales.

2.1.- DEFINICION

Designaremos con J un automorfismo de K , es decir, por definición, una biyección de K sobre sí mismo que respeta la suma y el producto. Si se usa la notación exponencial, las propiedades formales de J son:

$$(\lambda+\mu)^J = \lambda^J + \mu^J \qquad (\lambda\mu)^J = \lambda^J \mu^J$$

Se dice que una aplicación ϕ de $E \times E$ en G es una aplicación sesquilineal para J (o respecto de J) si se verifican las condiciones:

(S) $$\phi(x_1+x_2 , y) = \phi(x_1,y) + \phi(x_2,y) \quad ; \quad \phi(\lambda x,y) = \lambda\phi(x,y)$$

$$\phi(x , y_1+y_2) = \phi(x,y_1) + \phi(x,y_2) \quad ; \quad \phi(x, \lambda y) = \lambda^J\phi(x,y)$$

$$(\forall x , \forall x_1 , \forall x_2 , \in E \; ; \quad \forall y , \forall y_1 , \forall y_2 , \in F \; ; \quad \lambda \in K)$$

Cuando $G = K$, se dice que ϕ es una forma sesquilineal (para J) sobre $E \times F$.(#)

Designemos con F^J el espacio vectorial definido en F reemplazando su multiplicación por escalares por esta otra:

$$(\lambda , y) \longrightarrow \lambda \text{ "escalar" } y = \lambda^{J'} y \qquad (\lambda \in K , y \in F)$$

donde J' designa el automorfismo inverso de J , J^{-1} . Entonces, las condiciones (S) expresan que ϕ (sesquilineal para J de $E \times F$ en G) es una aplicación

(#) Esta situación se presenta naturalmente y con frecuencia en el caso complejo (cf. 2.6)

bilineal de ExF^J en G . En efecto, las tres primeras condiciones de (S) son idénticas a las tres primeras de (B) , y en cuanto a la última, se tiene:

$$\phi(x, \lambda\text{"escalar"}y) = \phi(x, \lambda^{J'}y) = (\lambda^{J'})^J \phi(x,y) = \lambda\, \phi(x,y)$$

que es la última condición de (B) escrita para el espacio F^J en lugar de F .

En particular, eso vale cuando ϕ es una forma sesquilineal sobre ExF . Definamos en este caso la aplicación $\phi' : FxE \longrightarrow K$ mediante: $\phi'(y,x) = \phi(x,y)^{J'}$, que es una forma sesquilineal sobre FxE . Entonces ella también se identificará a una aplicación bilineal ϕ' de $FxE^{J'}$. Sea d_ϕ , $d_{\phi'}$, las aplicaciones lineales asociadas (a la derecha) a la forma bilineal ϕ sobre ExF^J y a la forma bilineal ϕ' sobre $FxE^{J'}$, respectivamente. Por definición, se dice que d_ϕ es la aplicación lineal asociada a la forma sesquilineal ϕ sobre ExF , a la derecha, y $d_{\phi'}$, se llama la aplicación lineal asociada a la forma sesquilineal ϕ , a la izquierda, y se representa con s_ϕ . Entonces, usando las fórmulas que caracterizan a d_ϕ y $d_{\phi'}$ (cf. 1.1) se deduce que d_ϕ y s_ϕ así definidas verifican las condiciones:

$$\phi(x,y) = \langle x , d_\phi(y) \rangle = \langle y , s_\phi(x) \rangle^J \qquad (\forall x \in E , y \in F)$$

2.2.- FORMAS SESQUILINEALES NO DEGENERADAS

Sea ϕ una forma sesquilineal (para J) sobre ExF . Se dice que ϕ es no degenerada, o degenerada a la izquierda, o degenerada a la derecha, si la forma bilineal correspondiente sobre ExF^J es, respectivamente, no degenerada, o degenerada a la izquierda, o degenerada a la derecha.

-o-

2.3.- MATRIZ DE UNA FORMA SESQUILINEAL

Se extiende al caso de formas sesquilineales lo dicho en 1.3 : la matriz de ϕ respecto de las bases (e_i) , (f_j) de E , F , es por definición:

$$(g_{ij}) = (\phi(e_i, f_j))$$

y cuando $E = F$ (forma sesquilineal sobre E) se define el discriminante de ϕ con relación a la base (e_i)) mediante:

$$D_\phi = \det (\phi(e_i, e_j))$$

-o-

2.4.- ORTOGONALIDAD

Se extiende a ϕ sesquilineal sobre $E \times F$ lo dicho en 1.4 sobre elementos y partes de E y F ortogonales con relación a ϕ. Con la misma notación de allí y con el mismo razonamiento se prueba que si $F_1 \subset F$, entonces F_1^o es un subespacio de E llamado el subespacio ortogonal a F_1. En la misma forma resultan las otras propiedades:

$$H \subset H_1 \iff H_1^o \subset H^o$$

$$H^o = H^{ooo}$$

$$\dim (F/E^o) = \dim (E/F^o)$$

(En la demostración del lema 1 se requieren ligeros cambios de notación que provienen de que si ϕ es sesquilineal, d_ϕ es lineal de F^J en $E^\#$, s_ϕ es lineal de E^J en $F^\#$, y no lineales de F en $E^\#$ y de E en $F^\#$, respectivamente, como sucede cuando ϕ es bilineal).

Se extiende también la noción de rango al caso de ϕ sesquilineal mediante:

$$\text{rango de } \phi = \dim (E/F^o) = \dim (F/E^o)$$

y valen (con las mismas demostraciones) los hechos siguientes:

d_ϕ y s_ϕ tiene el mismo rango que ϕ (#).

Si $\dim (E) = \dim (F)$, es equivalente decir que d_ϕ es inyectiva, o que es suryectiva, o que s_ϕ es inyectiva o que es suryectiva, o que ϕ es no degenerada (extensión a este caso del teorema 1).

Si ϕ es no degenerada, necesariamente $\dim (E) = \dim (F)$ y existen bases (e_i), (f_j) de E, F, respectivamente, tales que $g_{ij} = \phi(e_i, f_j) = \delta_{ij}$.

$\operatorname{codim} (M^o) = \dim (M)$ (M = subespacio de E ó de F, ϕ no degenerada)

$M = M^{oo}$

$(M+N)^o = M^o \cap N^o$ (M, N, subespacios de E ó de F, ϕ no degenerada)

$(M \cap N)^o = M^o + N^o$

2.- ADJUNTO DE UN ENDOMORFISMO

Igual que en 1.5 se prueba que si ϕ es una forma sesquilineal (para J) sobre E, no degenerada, y si u es un endomorfismo de E, entonces existe un único endomorfismo $u^\#$ (adjunto de u a la izquierda con respecto a ϕ) tal que:

(#) Y son aplicaciones semilineales (ver def. en 13.1)

$$\phi(u(x) , y) = \phi(x , u^{\#}(y)) \quad .$$

La linealidad de $u^{\#}$ resulta inmediatamente del siguiente cálculo:

$$\phi(x , u^{\#}(y_1+y_2)) = \phi(u(x) , y_1+y_2) = \phi(u(x) , y_1) + \phi(u(x) , y_2) = \phi(x , u^{\#}(y_1)) + \phi(x , u^{\#}(y_2)) \quad .$$

$$\phi(x , u^{\#}(\lambda y)) = \bar{\phi}(u(x) , \lambda y) = \lambda^{J}\phi(u(x) , y) = \lambda^{J}\phi(x , u^{\#}(y)) = \phi(x , u^{\#}(y))$$

$$(\forall x , \forall y , \forall y_1 , \forall y_2 \in E)$$

(Análogamente, para el adjunto a la derecha).

Si u_1 , u_2 son dos endomorfismos de E , valen además las propiedades:

$(u_1 + u_2)^{\#} = u_1^{\#} + u_2^{\#}$

$1^{\#} = 1$ (1 = aplicación idéntica de E)

$(\lambda u_1)^{\#} = \lambda^{J'} u_1^{\#}$ ($\lambda \in K$, $J' = J^{-1}$)

$(u_1 . u_2)^{\#} = u_2^{\#} . u_1^{\#}$

y además, si u es un automorfismo, vale: $(u^{-1})^{\#} = (u^{\#})^{-1}$.

Todas estas propiedades son de demostración directa. Veamos por ejemplo la tercera y la cuarta. La tercera resulta de que:

$$\phi(\lambda u(x) , y) = \lambda \phi(u(x) , y) = (\lambda^{J'})^{J} \phi(u(x) , y) = (\lambda^{J'})^{J} \phi(x , u^{\#}(y)) = \phi(x , \lambda^{J'} u^{\#}(y)) \quad .$$

y la cuarta de que:

$$\phi(u_1 \cdot u_2(x) , y) = \phi(u_2(x) , u_1^{\#}(y)) = \phi(x , u_2^{\#}(u_1^{\#}(y))) \quad .$$

2.6.- EL CASO $K = \mathbb{C}$

Cuando K es el cuerpo de los complejos, $\mathbb{C}$, existe un automorfismo (involutivo) natural: $J : \lambda \longrightarrow \bar{\lambda}$, que lleva cada complejo en su complejo conjugado. Cuando E y F son espacios vectoriales sobre $\mathbb{C}$, si se habla de formas sesquilineales sin indicar el automorfismo J , debe sobreentenderse que se trata de este automorfismo natural. Para este caso, las condiciones (S) se escriben:

$\phi(x_1+x_2 , y) = \phi(x_1,y) + \phi(x_2,y)$

$\phi(x , y_1+y_2) = \phi(x,y_1) + \phi(x,y_2)$

$\phi(\lambda x , y) = \lambda \phi(x,y)$

$\phi(x, \lambda y) = \bar{\lambda} \phi(x,y)$

y las propiedades del operador "adjunto": $u \longrightarrow u^{\#}$ son:

$$(u_1+u_2)^{\#} = u_1^{\#} + u_2^{\#}$$

$$1^{\#} = 1$$

$$(\lambda u_1)^{\#} = \bar{\lambda} u_1^{\#}$$

$$(u_1 . u_2)^{\#} = u_2^{\#} . u_1^{\#}$$

$$(u^{-1})^{\#} = (u^{\#})^{-1} \quad .$$

OBSERVACION: La teoría de las formas sesquilineales comprende la de las formas bilineales, que se obtienen cuando J es la identidad. De ahí que, por ejemplo las propiedades del operador "adjunto" indicadas en 2.5 valen también si $\emptyset$ es una forma bilineal (tomando J igual a la identidad) .

CAPITULO II

FORMAS HERMITIANAS Y ANTIHERMITIANAS
PROPIEDADES DE ORTOGONALIDAD

3.- ORTOGONALIDAD: RELACION SIMETRICA

3.1.- INTRODUCCION

Volvamos a la situación de los números 1.4 y 2.4 : K es un cuerpo conmutativo, E un espacio vectorial de dimensión finita, n , sobre K , y ϕ es una forma sesquilineal (respecto de un automorfismo J de K) o bilineal (caso particular en que J es la identidad) sobre E .

Probemos la siguiente definición: si x e y son vectores de E , se dice que x es ortogonal a y (respecto de ϕ) si y sólo si $\phi(x,y) = 0$. Es esencialmente la misma definición de 1.4 ó 2.4 adaptada a este caso pues allí el hecho de que se consideraban dos espacios distintos, E , F , permitía decir simplemente "... x e y son ortogonales si.. " , en lugar de "... x es ortogonal a y si... ...".) Ya hemos observado de que si x es ortogonal a y no necesariamente y es ortogonal a x : nuestra relación de ortogonalidad no tiene por qué ser simétrica. Sin embargo, desde el punto de vista de la geometría interesa definir una relación de ortogonalidad simétrica, lo cual puede lograrse imponiendo ciertas restricciones a la forma. Hay dos soluciones evidentes del problema: Poniendo la condición simplificadora de que J es la identidad (es decir ϕ es bilineal) puede exigirse además:

$$(\sigma) \qquad \phi(x,y) = \phi(y,x) \qquad (\forall x , \forall y \in E)$$

o bien

$$(\alpha) \qquad \phi(x,y) = -\phi(y,x) \qquad (\forall x , \forall y \in E)$$

Las formas bilineales que satisfacen (σ) se denominan simétricas, y las que satisfacen (α) , antisimétricas. (En partes importantes de este libro se supondrá que el cuerpo K es de característica diferente de 2 , y en ese caso, como se verá más adelante, una forma bilineal es antisimétrica si y sólo si es alternada)

Daremos a continuación, una solución aparentemente mucho más general de nuestro problema de ortogonalidad simétrica, es decir el problema de definir una forma sesquilineal tal que la relación de ortogonalidad correspondiente sea simétrica. Así

se llega a la consideración de las formas ε-hermitianas.

-o-

3.2.- FORMAS ε-HERMITIANAS

En todo lo que resta de este capítulo, salvo indicación expresa, se mantienen las hipótesis y notaciones del capítulo 1, con la excepción de que el automorfismo J se supone además involutivo (es decir $(\lambda^J)^J = \lambda$ para todo $\lambda \in K$). Para poner de manifiesto esta restricción, modificaremos la notación escribiendo $\lambda \longrightarrow \bar{\lambda}$ en lugar de $\lambda \longrightarrow \lambda^J$.

Sea $\varepsilon \in K$ Si ϕ es una forma sesquilineal (para J) sobre E, decimos que ϕ es ε-hermitiana, si además cumple la condición:

(h) $$\phi(x,y) = \varepsilon \overline{\phi(y,x)} \qquad (\forall x, \forall y \in E)$$

Nótese que si ϕ no es idénticamente nula se tiene $\varepsilon\bar{\varepsilon} = 1$ pues:

$$\phi(x,y) = \varepsilon \overline{\phi(y,x)} = \varepsilon \overline{\varepsilon \overline{\phi(x,y)}} = \varepsilon\bar{\varepsilon}\,\phi(x,y)$$

En los casos particulares en que $\varepsilon = 1$, ó $\varepsilon = -1$, ϕ se llama simplemente hermitiana o antihermitiana, respectivamente. Las formas bilineales simétricas son las formas sesquilineales hermitianas respecto de la identidad, y las formas bilineales antisimétricas son las formas antihermitianas respecto de la identidad. Conviene notar (porque será usado) que en el caso de formas hermitianas la relación de "adjunto" tiene la propiedad (inmediata): $u^{\#\#} = u$.

-o-

Vamos a mostrar ahora que las formas -hermitianas también proporcionan soluciones al problema de ortogonalidad simétrica. Pero esto es inmediato porque

$$\phi(x,y) = 0 \iff \overline{\phi(y,x)} = 0 \quad \text{y} \quad \overline{\phi(y,x)} = 0 \iff \phi(y,x) = 0$$

-o-

3.3.- REFERENCIA A SOLUCIONES GENERALES DEL PROBLEMA DE ORTOGONALIDAD SIMETRICA.

Daremos sin demostración algunas propiedades interesantes de las formas sesquilineales, ϕ , que definen una relación de ortogonalidad simétrica en E . De modo que ahora suponemos por una vez que J es un automorfismo cualquiera de K (no necesariamente involutivo), y haremos la restricción adicional de que el rango de ϕ es mayor o igual que 2 (de otro modo se está manifiestamente en casos excepcionales). ¿Qué se puede decir de ϕ si sólo se le impone la condición de ortogonalidad simétrica:

$$\phi(x,y) = 0 \iff \phi(y,x) = 0 \quad ?$$

En primer lugar, se puede comprobar que existe $\lambda \in K$ tal que: $\emptyset(x,y) = \lambda(\emptyset(x,y))^J$.

Observemos luego que, cualquiera sea $\alpha \in K$, la forma $\emptyset'(x,y) = \alpha\,\emptyset(x,y)$ es también sesquilineal para J . En efecto:

$$\emptyset'(\lambda x\ ,\ y) = \alpha\,\emptyset(\lambda x\ ,\ y) = \lambda\alpha\,\emptyset(x,y) = \lambda\,\emptyset'(x,y)$$

$$\emptyset'(x\ ,\ \lambda y) = \alpha\,\emptyset(x\ ,\ \lambda y) = \lambda^J\alpha\,\emptyset(x,y) = \lambda^J\,\emptyset'(x,y)$$

(Además, la relación $\varepsilon(\emptyset'(y,x))^J = \varepsilon.\alpha^J(\emptyset(y,x))^J$ nos dice que si J es involutivo, si $\emptyset$ es ε-hermitiana y si $\alpha = \alpha^J$, entonces $\emptyset' = \alpha\emptyset$ también es ε-hermitiana para J .)

Observado esto, se puede demostrar que la existencia de la forma $\emptyset$ a ortogonalidad simétrica implica que J es involutivo, y que existe $\alpha \in K$ tal que $\emptyset' = \alpha\emptyset$ es, o bien hermitiana, o bien antisimétrica.

En resumen, decimos que se puede demostrar que <u>toda forma sesquilineal a ortogonalidad simétrica puede reducirse a una forma hermitiana o a una forma antisimétrica.</u> De ahí que el estudio prácticamente se enfoca sobre éstas que tienen además otras propiedades importantes por otras razones.

-o-

3.4.- <u>MATRICES DE LAS FORMAS ε-HERMITIANAS</u>

Si $\emptyset$ es una forma ε-hermitiana (para J) sobre E , se cumple en particular que:

$$g_{ij} = \emptyset(e_i,e_j) = \varepsilon\,\overline{\emptyset(e_j,e_i)} = \varepsilon\,\overline{g_{ji}}$$

Recíprocamente, si se da una matriz (g_{ij}) con esa propiedad y se define $\emptyset(x,y) = \emptyset(\sum_i x^i e_i\ ,\ \sum_j y^j e_j) = \sum_{ij} x^i\,\bar{y}^j\,\emptyset(e_i,e_j) = \sum_{ij} x^i\,\bar{y}^j\,g_{ij}$ se comprueba fácilmente que $\emptyset$ es una forma ε-hermitiana (para J).

Las matrices (g_{ij}) que verifican la condición:

$$g_{ij} = \overline{g_{ji}}$$

y que como acabamos de ver caracterizan a las formas -hermitianas para J , se llaman también <u>matrices ε-hermitianas para</u> J . Los casos particulares son los siguientes:

$g_{ij} = \overline{g_{ji}}$ (matriz hermitiana)

$g_{ij} = -\overline{g_{ji}}$ (matriz antihermitiana)

$g_{ij} = g_{ji}$ (matriz simétrica)

$$g_{ij} = -g_{ji} \qquad \text{(matriz antisimétrica)}$$

-o-

4.- VECTORES Y SUBESPACIOS ISOTROPOS

Además de las hipótesis y notaciones generales indicadas al comienzo del §3 , supondremos aquí que φ es ξ-hermitiana y no degenerada. En este caso $F^{oo} = F$ para todo subespacio F .

4.1.- DEFINICIONES

Se dice que un vector $x \in E$ es isótropo (con relación a φ) cuando

(i) $$\varphi(x,x) = 0$$

Si F es un subespacio de E , se dice que F es un subespacio isótropo si existe $x \neq 0$, $x \in F$, tal que sea ortogonal a F , es decir $\varphi(x,y) = 0$ para todo $y \in F$. En otras palabras, F es isótropo si y sólo si $F \cap F^o \neq \{0\}$. Según vimos (cf.1.4) φ es no degenerada si y sólo si $E^o \neq \{0\}$, es decir que φ es no degenerada si y sólo si E es no isótropo. Por la misma razón, un subespacio F es isótropo si y sólo si la restricción de φ a F es degenerada. (Aquí hemos usado libremente del hecho observado en §3 de que la relación de ortogonalidad definida por φ es simétrica; eso implica, por ejemplo, que φ es degenerada si y sólo si es degenerada a la izquierda o si y sólo si es degenerada a la derecha, etc...)

Un subespacio F es totalmente isótropo cuando todo vector x F es ortogonal a F . Otras definiciones equivalentes son las siguientes: F es totalmente isótropo si y sólo si la restricción de φ a F es idénticamente nula. F es totalmente isótropo si y sólo si $F \subset F^o$.

Observemos que si dos (resp. n) subespacios F_1 , F_2 son totalmente isótropos y ortogonales (resp. ortogonales dos a dos) entonces $G = F_1 + F_2$ (resp. su suma) es totalmente isótropo, y recíprocamente. En efecto, si $x_1 \in F_1$, $x_2 \in F_2$, se tiene por la hipótesis:

$$\varphi(x_1,x_1) = 0 \qquad \varphi(x_1,x_2) = 0 \qquad \varphi(x_2,x_1) = 0 \qquad \varphi(x_2,x_2) = 0 \ .$$

Si $x,y \in G$, admiten expresiones de la forma $x = x_1 + x_2$, $y = y_1 + y_2$ (donde $x_1,y_1 \in F_1$; $x_2,y_2 \in F_2$) y por lo tanto:

$$\varphi(x,y) = \varphi(x_1,y_1) + \varphi(x_1,y_2) + \varphi(x_2,y_1) + \varphi(x_2,y_2) = 0$$

lo que demuestra que G es totalmente isótropo.

Teorema 1 :

Las siguientes proposiciones son equivalentes:

(a) F es un subespacio no isótropo de E

(b) F^0 es no isótropo

(c) $E = F \oplus F^0$

Demostración:

En primer lugar (b) implica (a) porque si F^0 es no isótropo, como $F \cap F^0 \subset F^0 \cap F^{00}$, y como $F^0 \cap F^{00} = \{0\}$, también $F \cap F^0 = \{0\}$ y F es no isótropo. Dado que $E = F \oplus F^0$ implica en particular $F \cap F^0 = \{0\}$ se sigue que (c) implica simultáneamente (a) y (b) . Finalmente, (a) implica (c) pues si F es no isótropo, $F \cap F^0 = \{0\}$ y además $\dim F^0 = \operatorname{codim} F$, de donde $F + F^0 = E$.

-o-

4.3.- HIPOTESIS

En todo lo que sigue de este parágrafo, es necesario suponer que ϕ y K son tales que se verifica la siguiente condición:

(T) Dado $x \in E$, existe $\alpha \in K$ tal que:

$$\phi(x,x) = \alpha + \varepsilon \bar{\alpha} \quad .$$

Esta suposición no es demasiado restrictiva desde el punto de vista práctico. Por ejemplo si el cuerpo K es de característica distinta de 2 (de modo que existe el inverso de 2 , $\frac{1}{2}$) y si ϕ es hermitiana ($\varepsilon = 1$) se puede escribir: $\phi(x,x) = \frac{1}{2}\phi(x,x) + \frac{1}{2}\overline{\phi(x,x)}$ y la condición (T) se satisface con $\alpha = \frac{1}{2}\phi(x,x)$. Es claro que la condición (T) se verifica trivialmente cuando ϕ es alternada (ver definición al comienzo del capítulo 5).

-o-

4.4.- Lema 1 :

Sea F un subespacio totalmente isótropo, $F \neq \{0\}$. Entonces para cada $x \notin F^0$ y para cada $\alpha \in K$, existe $y \in F$ tal que:

$$\phi(x+y\ ,\ x+y) = \alpha + \varepsilon \bar{\alpha}$$

Demostración:

Según la condición (T) , existe $\beta \in K$ tal que $\phi(x,x) = \beta + \varepsilon \bar{\beta}$. Ahora, si $y \in F$,

$$\phi(x+y\ ,\ x+y) = \beta + \varepsilon \bar{\beta} + \phi(x,y) + \overline{\phi(x,y)} + 0$$

($\phi(y,y) = 0$ porque $y \in F$ y F es totalmente isótropo). Se puede escribir también

así:

$$\phi(x+y\ ,\ x+y) \;=\; (\phi(x,y) + \beta\ ) + \varepsilon\,\overline{(\phi(x,y) + \beta\ )}$$

y esto reduce el problema a encontrar un y F tal que $\phi(x,y) + \beta = \alpha$, cosa siempre posible porque ϕ no puede ser constante ya que en tal caso sería idémticamente nula en contra de la hipótesis de que es no degenerada. En efecto, si $\phi(x,y_0) \neq 0$, por ejemplo $\phi(x,y_0) = \lambda$, se tiene $\phi(x,\mu y_0) = \alpha - \beta$ poniendo $\mu = \overline{(\frac{\alpha - \beta}{\lambda})}$ y entonces $y_0 = y \in F$ resuelve el problema.

-o-

4.5.- Teorema 2 :

Sea F un subespacio totalmente isótropo de dimensión r :

(a) Si F' es un subespacio totalmente isótropo de dimensión r y $F' \cap F^0 = \{0\}$ (es decir F' no contiene vectores no nulos ortogonales a F), entonces $F + F'$ es no isótropo y si (f_i) es una base de F , existe una base (f'_i) de F' tal que $\phi(f_i,f'_j) = \delta_{ij}$ (δ_{ij} = símbolo de Kronecker).

(b) Si G es un subespacio totalmente isótropo de dimensión menor o igual que r tal que $G \cap F^0 = \{0\}$, entonces existe un subespacio totalmente isótropo F' de dimensión r que contiene a G y también verifica $F' \cap F^0 = \{0\}$.

Demostración de (a) :

Llamemos ϕ' a la restricción de ϕ a $F \times F'$. Si $f' \in F'$, la relación " $\phi(f,f') = 0$ para todo $f \in F$ " implica $f' = 0$ (porque se supone que F' no tiene vectores no nulos ortogonales a F). Eso significa que $f' \longrightarrow d_{\phi'}(f')$ es inyectiva, y por tanto (teorema 1 del §1) ϕ' es no degenerada. Entonces (por definición) $F + F'$ es no isótropo.

Demostración de (b) :

Razonaremos por recurrencia sobre la dimensión s de G (que por hipótesis cumple $s \leq r$). Es claro que basta probar el enunciado siguiente: Si $s < r$ existe un subespacio $G' \subset G$ tal que G' es totalmente isótropo, $\dim(G') = s+1$ y $G' \cap F^0 = \{0\}$.

Sea ϕ' la restricción de ϕ a $F \times G$. Sabemos que si una forma sesquilineal sobre $F \times G$ es no degenerada, entonces $\dim(F) = \dim(G)$, de modo que podemos asegurar que ϕ' es degenerada. Pero como por hipótesis $G \cap F^0 = \{0\}$, tiene que ser $F \cap G^0 \neq \{0\}$ (de otro modo ϕ' sería no degenerada). Entonces $G^0 \cap F \subset G + F^0$ pues siendo $G^0 \cap F$ totalmente isótropo, se tiene: $G^0 \cap F \subset (G^0 \cap F)^0 = G^{00} + F^0$

Demostraremos en primer lugar, por el absurdo, que G^0 no está contenido en $G + F^0$. En efecto, si $G^0 \subset G + F^0$, entonces $G^{00} = G \supset G^0 \cap F^{00} = G^0 \cap F$. En-

tonces $G^o \cap F$ estaría contenido tanto en F como en G y se tendría: $G^o \cap F \subset$ $\subset G \cap F \subset G \cap F^o = \{0\}$, en contra de que, como vimos, $G^o \cap F \neq \{0\}$.

Sea entonces $x \in G^o$ tal que $x \notin G+F^o$ y sea $y \in G^o \cap F$. Entonces $x+y \in G^o$ pero $x+y \notin G+F^o$. Ahora, como $x \notin G+F^o = (G^o \cap F)^o$, por el lemà 1 si se da un $\alpha \in K$ siempre existe un $y \in G^o \cap F$ tal que $\emptyset(x+y , x+y) = \alpha + \varepsilon \bar{\alpha}$, y tomando $\alpha = 0$, deducimos que existe $y \in G^o \cap F$ tal que $\emptyset(x+y , x+y) = 0$. En resumen, $x' = x + y$ es un vector isótropo tal que $x' \in G^o$ pero $x' \notin G+F^o$.

Siendo, por eso, la recta Kx' ortogonal al subespacio totalmente isótropo G , el subespacio $G' = G + Kx' \supset G$ es también totalmente isótropo (cf. 4.1), y como x' no puede pertenecer a G porque ya no pertenece a $G+F^o \supset G$, G' tiene dimensión $s+1$.

Solo resta por probar que también $G' \cap F^o = \{0\}$. Para ello supongamos que G' tiene un punto $z = g + \lambda x'$ $(g \in G , \lambda \in K)$ tal que z F^o . Observamos en primer término que tiene que ser $\lambda = 0$ porque si no, como $z \in F^o \subset G+F^o$, y $g \in G \subset G+F^o$ resultaría $x' = \frac{z - g}{\lambda} \in G+F^o$, en contra de la elección de x' . Entonces, siendo $\lambda = 0$, se tiene que $z = g \in G$, y como $z \in F^o$, también $z \in G \cap F^o = \{0\}$, es decir $z = 0$, l.q.d.d.

Corolario :

Si F es totalmente isótropo, existe un subespacio totalmente isótropo F' de la misma dimensión tal que $F \cap F' = \{0\}$ y tal que $F + F'$ no es isótropo.

Demostración:

Basta aplicar la parte (b) del teorema con $G = \{0\}$ y luego la parte (a) .

-o-

4.6.- SUBESPACIOS TOTALMENTE ISOTROPOS MAXIMALES

De acuerdo con la terminología usual, se dice que F es un subespacio totalmente isótropo maximal si:

(1) F es totalmente isótropo;

(2) F no está propiamente contenido en ningún subespacio totalmente isótropo, es decir, " $G \supset F$ y G = tot. isótropo " implica $G = F$.

Observemos que si F es totalmente isótropo maximal y si x es isótropo y $x \in F^o$ entonces $x \in F$. Si no fuera así, $F + Kx$ sería un subespacio totalmente isótropo distinto de F que contendría a F .

Teorema 3 :

Sean F_1 , F_2 , dos subespacios totalmente isótropos maximales y $F = F_1 \; F_2$. Sean S_1 , S_2 , subespacios suplementarios de F en F_1 , F_2 , respectivamente (es decir: $F_1 = S_1 \oplus F$, $F_2 = S_2 \oplus F$) y $S = S_1 + S_2$. Entonces existen dos subespacios G , H (de H) tales que:

(a) $G + F$, S , H , son no isótropos y ortogonales dos a dos;

(b) $E = F \oplus S \oplus G \oplus H$;

(c) H no contiene vectores isótropos (diferentes de 0) ;

(d) G es totalmente isótropo;

(e) $\dim (F_1) = \dim (F_2)$; $\dim (G) = \dim (F)$; $\dim (S_1) = \dim (S_2)$; $\operatorname{codim} (H) = 2 \cdot \dim (F_1)$.

Demostración:

Procederemos por pasos:

(1) S_1 y S_2 son totalmente isótropos, porque están contenidos en subespacios totalmente isótropos.

(2) Si y S_1 es ortogonal a S_2 , es decir si $y \in S_1 \cap S_2^o$, entonces $y \in F_1^o$, es decir y es ortogonal a F_1 . Luego, con mayor razón, y es ortogonal a F , y por lo tanto también y es ortogonal a F_2 , pero siendo $y \in S_1$, es isótropo (cf. 1), y como F_2 es totalmente isótropo maximal, se sigue que $y \in F_2$ (cf. observación al comienzo de este número). Eso a su vez implica: $y \in S_1 \cap F_2 = S_1 \cap F_1 \cap F_2 = S_1 \cap F = \{0\}$. En resumen, hemos demostrado que la relación $y \in S_1 \cap S_2^o$ implica $y = 0$, o sea $S_1 \cap S_2^o = \{0\}$. Del mismo modo se demuestra que también $S_2 \cap S_1^o = \{0\}$.

(3) Las dos últimas conclusiones de (2) implican que:

$\dim (S_1) \leq \operatorname{codim} (S_2^o) = \dim (S_2)$ y $\dim (S_2) \leq \operatorname{codim} (S_1^o) = \dim (S_1)$; o sea $\dim (S_1) = \dim (S_2)$. Esto prueba la primera y la tercera partes de (e).

(4) Usando los resultados de (3) y (2) , podemos aplicar a S_1 y S_2 la parte (a) del teorema 2, que nos dice entonces que $S_1 + S_2 = S$ no es isótropo. Esto prueba la segunda parte de (a) .

(5) Ahora, (4) junto con el corolario del teorema 1 , nos dicen que S^o es no isótropo, y además: $S^o = (S_1 + S_2)^o = S_1^o \cap S_2^o \supset F_1^o \cap F_2^o \supset F_1 \cap F_2 = F$, es decir: $S^o \supset F$.

(6) Razonemos ahora en el espacio no isótropo S^o y apliquemos el teorema 2: existe un subespacio de S^o , G , totalmente isótropo tal que $\dim (G) = \dim (E)$, $G \cap F^o = \{0\}$ y $G + F$ es no isótropo. Esto prueba (d) , la primera parte de (a) , y la segunda parte de (e) .

(7) Sea H el ortogonal al subespacio no isótropo $G + F$ de S^o en el espacio S^o. Sabemos que H es también no isótropo y eso prueba la tercera parte de (a) . Como $G + F \subset S^o$, $G + F$ es ortogonal a S , y también H es ortogonal a

S por la misma razón; y por definición, H es ortogonal a $G + F$. Eso prueba lo que faltaba de (a) .

Además, por (6) , la suma de G y F es directa y entonces usando lo que sabemos, la definición de H y el corolario del teorema 1, resulta que S^o es suma directa de G , F y H . Y de ahí resulta finalmente que E es suma directa de G , F , H y S , lo que prueba (b) .

(8) Demostraremos ahora (c) . Para ello observemos que, como H es ortogonal a $G + F$ y está contenido en S^o , es ortogonal a F y a S_1 y por otra parte, $H \cap F_1 = \{0\}$. Así, $H \subset F_1^o = (S_1 + F)^o$ y entonces, por la observación que precede al teorema, H no puede contener vectores isótropos no nulos pues éstos estarían también en F_1 .

(9) Falta solamente la última parte de (e) , que es ya trivial en virtud de lo establecido. En efecto:

$$\text{codim}(H) = \dim(F) + \dim(S) + \dim(G) = 2.\dim(F) + \dim(S) =$$

$$= 2.\dim(F) + 2.\dim(S_1) = 2.\dim(F_1) \quad (\text{porque } S = S_1 \oplus S_2) ,$$

y así queda el teorema completamente demostrado.

Corolario :

Dos subespacios totalmente isótropos maximales tienen la misma dimensión. Si F es un subespacio totalmente isótropo maximal existe un subespacio F' totalmente isótropo maximal tal que $F + F'$ es no isótropo.

Demostración:

Basta aplicar a F el corolario del teorema 2 para la existencia de F' totalmente isótropo tal que $F' \cap F = \{0\}$ y tal que $F + F'$ no sea isótropo. La primera parte del corolario se sigue de (e) del teorema y ella implica que F' también es totalmente isótropo maximal.

-o-

4.7.- INDICE DE UNA FORMA ε-HERMITIANA, BASES DE VECTORES ISOTROPOS, FORMAS NEUTRAS.

El corolario del teorema 3 permite definir: se llama índice, ν , de ϕ , a la dimensión común a los subespacios totalmente isótropos maximales. El mismo corolario asegura que $2\nu < n$.

-o-

Lema 2 :

Si el índice de ϕ es $\nu \geq 1$, y si $a \neq 0$ es un vector isótropo existe una base de E de la forma $\{a , e_2 , \dots , e_n\}$ formada por vectores isótropos.

Demostración :

Sea $v_1,\dots,v_n = a$ una base de E . Seguramente, existe un i tal que $\phi(a,v_i) \neq 0$ $(i \neq n)$ pues de otro modo sería a ortogonal a E , en contradicción con que ϕ se supone no degenerada. Entonces se puede volver a ordenar los vectores (v_i) de modo que

$$\phi(a,v_i) \neq 0 \qquad (1 \leq i < r)$$
$$\phi(a,v_i) = 0 \qquad (r \leq i < n)$$

Definimos ahora los vectores:

$$t_i = v_i \quad (\text{para } 1 \leq i < r) \qquad y \qquad t_i = v_i + v_1 \quad (\text{para } r \leq i \leq n)$$

Veamos que los t_i son linealmente independientes, es decir que constituyen una nueva base de E . En efecto, si:

$$\sum_{i=1}^{n} \lambda_i t_i = 0 \implies \sum_{i=1}^{r-1} \lambda_i v_i + \sum_{r}^{n} \lambda_i (v_i+v_1) = 0 \implies$$

$$\implies \sum_{i=1}^{n} (\lambda_i)v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n = 0$$

y como (v_i) es una familia libre:

$$\sum_{i=1}^{n} \lambda_i = 0 \quad , \quad \lambda_2 = 0 \quad , \dots , \quad \lambda_n = 0 \implies \lambda_i = 0 \quad (1 \leq i \leq n)$$

l.q.d.d.

Por otra parte, si $1 \leq i < r$, $\phi(a,t_i) = \phi(a,v_i \neq 0$, y si $r \leq i \leq n$, también: $\phi(a,t_i) = \phi(a,v_i+v_1) = \phi(a,v_i) + \phi(a,v_1) = 0 + \phi(a,v_1) \neq 0$. Esto prueba que <u>existe una base de</u> E <u>formada por</u> a <u>y vectores no ortogonales a</u> a . Modifiquemos el orden suponiendo que a , t_2 , ... , t_n es una base formada por a y vectores no ortogonales a a .

Sea $F_i = Ka + Kt_i$ $(2 \leq i \leq n)$. Decimos que <u>existe</u> $e_i \in F_i$, <u>isótropo</u>. Para ello, podemos suponer $\phi(t_i,t_i) \neq 0$ porque si no basta poner $e_i = t_i$. Como Ka es totalmente isótropo y t_i no pertenece a $(Ka)^0$, el lema 1 nos dice que dado $\alpha \in K$ existe un $y \in Ka$ tal que $\phi(t_i+y\ ,\ t_i+y) = \alpha + \xi\bar{\alpha}$. Haciendo $\alpha = 0$, tenemos en particular que existe $\lambda_i \in K$ tal que $\phi(\lambda_i a+t_i\ ,\ \lambda_i a+t_i) = 0$, y entonces basta poner $e_i = \lambda_i a + t_i$.

Ahora, la demostración del lema estará completa si mostramos que $a, e_2, \dots, e_n$ es una base de E , es decir que dicha familia es libre. Para ello, supongamos que $\mu_1 a + \sum_{i=1}^{n} \mu_i e_i = 0$. Eso implica:

$$\mu_1 a + \sum_{i=1}^{n} \mu_i \lambda_i a + \sum_{i=1}^{n} \mu_i t_i = (\mu_1 + \sum_{i=1}^{n} \mu_i \lambda_i)a + \sum_{i=1}^{n} \mu_i t_i = 0$$

y como $a, t_2, \ldots, t_n$ son linealmente independientes, se tiene:

$$\mu_1 + \sum_{i=2}^{n} \mu_i \lambda_i = 0$$

$$\mu_2 = 0$$

$$\mu_3 = 0$$

$$\vdots$$

$$\mu_n = 0$$

que implica $\mu_i = 0$ $(1 \leq i \leq n)$, l.q.d.d.

-o-

Se dice que la forma ε-hermitiana no degenerada ϕ es neutra si E es suma directa de dos subespacios totalmente isótropos (respecto de ϕ). El corolario del teorema 3 asegura que éstos son entonces totalmente isótropos maximales (y por tanto de la misma dimensión), de modo que para que E admita una forma neutra es necesario que sea de dimensión par. También resulta que si dim (E) = n = 2k y si E admite una forma neutra, entonces ésta es de índice $\frac{n}{2} = k$. Del teorema 2 se sigue que si ϕ es neutra E admite una base de la forma $e_1, \ldots, e_{n/2}, f_1, \ldots, f_{n/2}$ tal que $\phi(e_i, f_j) = \delta_{ij}$. Además resulta de ahí que dos formas neutras ϕ , ϕ' sobre espacios de la misma dimensión, E , E' , son equivalentes (es decir, existe un isomorfismo $u : E \longrightarrow E'$ tal que: $\phi'(u(x) , u(y)) = \phi(x,y)$) .

-o-

Supongamos que E es suma directa de dos subespacios E_1 , E_2 , y sean ϕ_1 , ϕ_2 formas ε-hermitianas sobre E_1 , E_2 , respectivamente. Si x e y son vectores de E , se descomponen de manera única en la forma: $x = x_1 + x_2$, $y = y_1 + y_2$ $(x_1, y_1 \in E_1 \; ; \; x_2, y_2 \in E_2)$. Entonces se puede definir: $\phi(x,y) = \phi_1(x_1, y_1) + \phi_2(x_2, y_2)$ y es inmediato verificar que ϕ es también una forma ε-hermitiana sobre E que se llama suma directa de ϕ_1 y ϕ_2 . (Esta noción se generaliza a suma directa de una familia de aplicaciones sesquilineales: $\phi_i : E_i \times F_i \longrightarrow G$ poniendo $\phi(x,y) = \sum_i (x_i, y_i)$ para x (resp. y) en la suma directa de los E_i (respectivamente de los F_i)). Es claro que con esta definición, E_1 y E_2 son ortogonales con respecto a ϕ y ϕ_1 , ϕ_2 son las restricciones de ϕ a E_1 , E_2 , respectivamente. Recíprocamente, si E_1 y E_2 son subespacios ortogonales y suplementarios respecto de una forma -hermitiana ϕ , entonces ϕ es suma directa de sus restricciones a E_1 y E_2 .

Podemos demostrar ahora que: la suma directa de dos formas neutras es una forma neutra. En efecto, si $E = E_1 \oplus E_2$, $E_1 = E_1' \oplus E_1''$, $E_2 = E_2' \oplus E_2''$ y si ϕ_1 es

una forma neutra sobre E_1 para la cual E_1' y E_1'' son totalmente isótropos, y ϕ_2 una forma neutra sobre E_2 para la cual E_2' y E_2'' son totalmente isótropos, entonces su suma directa, ϕ , es una forma neutra. Pues es claro que $E = E_1' \oplus E_1'' \oplus E_1' \oplus E_2''$ y si se pone $F_1 = E_1' \oplus E_2'$, $F_2 = E_1'' \oplus E_2''$, es $E = F_1 \oplus F_2$ y éstos son totalmente isótropos para ϕ (porque, por ejemplo, E_1' , E_2' son totalmente isótropos para ϕ_1 , ϕ_2 y entonces también para ϕ , y por la definición de ϕ , también son ortogonales para ϕ).

-o-

Una última consecuencia del teorema 3 es la siguiente: <u>la forma ϕ -hermitiana ϕ es suma directa de una forma neutra y una forma de índice 0</u> . En efecto (con la notación del teorema 3) sabemos que E es suma directa de H^0 y H , donde $H^0 = F_1 \oplus F_2$, de modo que la restricción de ϕ a H^0 es una forma neutra (porque F_1 y F_2 son totalmente isótropos), y la restricción de ϕ a H es una forma de índice 0 (porque H no contiene vectores isótropos distintos de 0), y de ahí la proposición.

-o-

CAPITULO III

FORMAS HERMITIANAS Y FORMAS CUADRATICAS

5.- FORMAS CUADRATICAS

Como en capítulos anteriores, en este parágrafo, K designa un cuerpo conmutativo y E un espacio vectorial de dimensión finita, n, sobre K.

-o-

En la "geometría analítica plana" es $K = \mathbb{R}$ y $E = \mathbb{R}^2$, y está definido el "producto escalar" de dos vectores $x = (x^1, x^2)$, $y = (y^1, y^2)$ mediante la expresión: $(x|y) = x^1y^1 + x^2y^2$. Es un sencillo ejercicio verificar que $(\ |\ )$ es una forma bilineal simétrica sobre $\mathbb{R}^2$. Así, las formas bilineales simétricas aparecen como generalizaciones de la noción de producto escalar en el caso clásico. Además, en la geometría analítica plana se define la longitud o el módulo de un vector mediante $|x| = \sqrt{(x^1)^2 + (x^2)^2}$ (suponemos que no puede haber confusión entre los índices superiores y los exponentes), y la norma de un vector mediante: $N(x) = (x^1)^2 + (x^2)^2 = |x|^2 = (x|x)$. Es frecuente pensar el plano como espacio afín, en cuyo caso, la longitud de x se interpreta como la distancia del punto $x = (x^1, x^2)$ al origen $(0,0)$.

Así como las formas bilineales simétricas generalizan la noción de producto escalar, las formas cuadráticas generalizan la noción de norma de un vector en el caso clásico (= cuadrado de la longitud = cuadrado de la distancia al origen). Antes de definirlas, notemos todavía que la función $N(x)$ de E en los escalares tiene las siguientes propiedades:

$$N(\lambda x) = (\lambda x|\lambda x) = \lambda^2(x|x) = \lambda^2 N(x) \qquad (\lambda \in \mathbb{R}\ ,\ x \in \mathbb{R}^2)$$

$$N(x+y) = (x+y|x+y) = (x|x) + 2(x|y) + (y|y) = N(x) + N(y) + 2(x|y)\ ,$$

o sea que $N(x+y) - N(x) - N(y)$ es una forma bilineal simétrica.

-o-

Sea Q una aplicación del espacio vectorial E en el cuerpo de escalares, K. Se dice que Q es una forma cuadrática si:

(Q) $\quad Q(\lambda x) = \lambda^2 Q(x) \qquad (\forall\ \lambda \in K\ ,\ \forall\ x \in E)$

$\varphi(x,y) = Q(x+y) - Q(x) - Q(y) = Q(y+x) - Q(y) - Q(x) = \varphi(y,x) \qquad (\forall\ x, \forall\ y \in E)$

es una forma bilineal simétrica sobre E, que se llama forma bilineal simétrica asociada a la forma cuadrática Q.

Usando las condiciones (Q), tenemos que:

$Q(2x) = 4.Q(x)$

$\emptyset(x,x) = Q(x+x) - Q(x) - Q(x) = 4\,Q(x) - 2\,Q(x) = 2\,Q(x)$

es decir:

$$\emptyset(x,x) = 2.Q(x)$$

que nos dice que si el cuerpo K es de característica 2 la forma bilineal asociada a Q es alternada (cf. capítulo 5).

Es evidente (por las condiciones (Q)) que si $F(x,y)$ es cualquier forma bilineal sobre E, entonces $Q(x) = F(x,x)$ es una forma cuadrática cuya forma bilineal (simétrica) asociada es $\emptyset(x,y) = F(x,y) + F(y,x)$.

Esta estrecha relación entre formas bilineales y formas cuadráticas permite aplicar a los espacios provistos de una forma cuadrática la teoría de las formas bilineales (o sesquilineales, o -hermitianas). Así, por ejemplo, se habla de formas cuadráticas no degeneradas (por definición, Q es no degenerada si y sólo si su forma bilineal asociada lo es), o de ortogonalidad con relación a una forma cuadrática (x es ortogonal a y respecto de Q, si y sólo si lo es respecto de la forma bilineal asociada), o de índice de una forma cuadrática (por definición, si K es de característica distinta de 2, el índice de Q es el de su forma bilineal asociada), etc.

Por eso, el estudio de una forma cuadrática (en lo que a este libro respecta) es enteramente equivalente al de ciertas formas bilineales. Por ejemplo, si K es de característica 2, la teoría de las formas cuadráticas coincide con la teoría de las formas alternadas, que se desarrollará sumariamente en el capítulo 5. Por eso, en este capítulo nos ocuparemos del caso en que la característica de K es diferente de 2 .

En todo lo que sigue de este capítulo, supondremos que K es de característica diferente de 2 . En tal caso puede definirse $f(x,y) = \frac{1}{2}\,\emptyset(x,y)$, de modo que f es una forma bilineal simétrica tal que $Q(x) = f(x,x)$. Recíprocamente, cualquiera sea la forma bilineal simétrica $f(x,y)$, la forma cuadrática $Q(x) = f(x,x)$ tiene como forma bilineal asociada a $\emptyset(x,y) = f(x,y) + f(y,x) = 2.f(x,y)$. De modo que en este caso hay correspondencia total entre las formas cuadráticas y las formas bilineales simétricas, y es usual tomar como forma bilineal asociada a Q no la $\emptyset$ de antes sino la f de ahora, lo cual no modifica en nada la situación.

-o-

Sea (e_i) una base de E , y K de característica diferente de 2 . Si $x = \sum_i x^i e_i$, se tiene:

$$Q(x) = f(x,x) = f\Big(\sum_i x^i e_i\ ,\ \sum_j x^j e_j\Big) = \sum_{i,j} x^i x^j\ f(e_i,e_j) =$$

$$= \sum_i (x^i)^2 . Q(e_i) + \sum_{i\neq j} x^i x^j .\ f(e_i,e_j)\ .$$

-o-

§6.- GRUPO UNITARIO Y GRUPO ORTOGONAL. SIMETRIAS. SEMEJANZAS

6.1.- DEFINICIONES

Sea $\emptyset$ una forma hermitiana sobre un espacio vectorial E de dimensión finita n sobre un cuerpo conmutativo, K .

Los automorfismos, u , de E tales que $\emptyset(u(x)\ ,\ u(x)) = \emptyset(x,y)$ se denominan automorfismos (o transformaciones) unitarios. Forman evidentemente un grupo que se designa con $\Psi(\emptyset)$, ó $\Psi_n(\emptyset)$ y se llama grupo unitario relativo a $\emptyset$. Cuando J es la identidad, los automorfismos u tales que $Q(u(x)) = Q(x)$ (donde Q es la forma cuadrática definida por $\emptyset$) se llaman automorfismos ortogonales y forman un grupo denominado grupo ortogonal (suponemos en este caso, además, que K es de característica diferente de 2). El grupo ortogonal se designa con $\emptyset(Q)$ ó $\emptyset_n(Q)$ y evidentemente coincide con $\Psi(\emptyset)$.

En este libro sólo estudiaremos el grupo ortogonal en los casos más sencillos.

Por eso, en todo lo que sigue de este parágrafo supondremos que $\emptyset$ es una forma bilineal simétrica no degenerada asociada a una forma cuadrática Q y que K es de característica diferente de 2 .

6.2.- Teorema 1 :

La aplicación $u \longrightarrow \det u$ es un homomorfismo del grupo ortogonal sobre el subgrupo multiplicativo $\{1,-1\}$ de K .

Demostración:

Ya sabemos que $u \longrightarrow \det u$ es un homomorfismo de $GL(E)$ en K , de modo que sólo hay que probar la última parte, es decir que una transformación ortogonal tiene determinante 1 ó -1 (y que las hay de los dos tipos). Para ello, fijamos una base de E y designamos con $(g_{ij}) = G$ la matriz de $\emptyset$, y con $(u_{ij}) = M(u)$ la matriz de un automorfismo ortogonal u . Si demostramos que

$$G = {}^tUGU$$

resultará:

$$\det(G) = \det(U) \cdot \det(G) \cdot \det(U)$$

que, como $\det(G) \neq 0$ porque ϕ es no degenerada, implica $(\det(U))^2 = 1$ lo que demuestra el teorema (pues las simetrías (cf. 8.5) tienen determinante -1 y las rotaciones, o la identidad, determinante 1).

Para probar la relación indicada arriba basta hacer el cálculo:

$$g_{ij} = \phi(e_i, e_j) = \phi\Big(\sum_k u_{ik} e_k \,,\, \sum_l u_{jl} e_l\Big) = \sum_{k,l} u_{ik}\, u_{jl}\, \phi(e_k, e_l) =$$

$$= \sum_{k,l} u_{ik}\, g_{kl}\, u_{jl} \qquad \text{equivale a} \quad G = {}^tUGU \qquad (\#)$$

6.3.- ROTACIONES

Según el teorema 1, las transformaciones ortogonales de determinante igual a 1 , constituyen el núcleo de un homomorfismo y por lo tanto forman un subgrupo distinguido de $\varphi(Q)$ que se llama grupo de las rotaciones y se representa con $\varphi^+(Q)$.

6.4.- Lema 1 :

Sea u un automorfismo de E , y $u^\#$ el automorfismo adjunto. Entonces:

(a) $u \in \varphi(Q)$ si y sólo si $u^\# = u^{-1}$ (y por tanto también $u^\# \in \varphi(Q)$)

(b) Si $u \in \varphi(Q)$ y si E_1 es un subespacio y $E_2 = E_1^\circ$, entonces si $u(E_1) \subset E$ se tiene: $u(E_1) = u^\#(E_1) = E_1$ y $u(E_2) = u^\#(E_2) = E_2$.

Demostración:

La relación $\phi(x,y) = \phi(u(x) , u(y))$ es equivalente, por definición de adjunto, a $\phi(u^\# u(x) - x , y) = 0$ (para todo y E) de donde como ϕ es no generada, $u^\# u(x) = x$ para todo x , y esto prueba (a) .

Luego, siendo u un automorfismo, $\dim(u(E_1)) = \dim(E_1)$, de modo que si $u(E_1) \subset E_1$, también $u(E_1) = E_1$; si además $u \in \varphi(Q)$, usando (a) resulta que también $U^\#(E_1) = E_1$. Sea ahora $x \in E_2$, $y \in E_1$; entonces la relación $\phi(x,y) = 0$ implica $\phi(x, u^\#(y)) = 0$ porque $u^\#(y) \in E_1$, y de ahí: $\phi(u(x),y) = 0$ $(\forall\, y \in E)$, es decir $u(x) \in E_2$. Entonces, como para E_1 , se sigue $u(E_2) = u^\#(E_2) = E_2$.

Corolario 1 :

Sea E_1 no isótropo y sea $\varphi_{E_1}(Q)$ el subgrupo de $\varphi(Q)$ formado por los auto

(#) También resulta fácilmente del Ap. IV, teorema 1 .

morfismos ortogonales, u , tales que $u(E_1) = E_1$, y sean $\varphi(Q_1)$, $\varphi(Q_2)$, los grupos ortogonales relativos a las restricciones Q_1 , Q_2 , de Q a E_1 , E_2 , respectivamente. Entonces $\varphi_{E_1}(Q)$ es isomorfo al grupo producto $\varphi(Q_1) \times \varphi(Q_2)$.

Demostración:

Sea $u \in \varphi_{E_1}(Q)$. Por el lema, si u_1 , u_2 son las restricciones de u a E_1, E_2 , respectivamente, se tiene que $u_1 \in \varphi(Q_1)$, y $u_2 \in \varphi(Q_2)$. Entonces es de verificación trivial que la aplicación $u \longrightarrow (u_1, u_2)$ es una biyección de $\varphi_{E_1}(Q)$ sobre $\varphi(Q_1) \times \varphi(Q_2)$ que respeta las leyes de estos grupos, es decir un isomorfismo. En efecto, en este caso $E = E_1 \oplus E_2$ y cada aplicación lineal $u : E \longrightarrow E$ está determinada por sus restricciones u_1 , u_2 . Si u , $v \in \varphi_{E_1}(Q)$, $uv \in \varphi_{E_1}(Q)$ y sus restricciones son u , v y $u_2 v_2$, respectivamente.

Corolario 2 :

El subgrupo de $\varphi(Q)$ formado por los u tales que $u(x) = x$ para cada x en E_1 , es isomorfo a $\varphi(Q_2)$.

En efecto, es sabido que el subgrupo $\{\text{identidad de } E_1\} \times \varphi(Q_2)$ es isomorfo a $\varphi(Q_2)$ y por eso este corolario se sigue del corolario 1 .

-o-

OBSERVACION : El grupo ortogonal de un espacio de dimensión 1 (o también el grupo ortogonal correspondiente a la restricción de Q a un subespacio no isótropo de dimensión 1) está formado por las aplicaciones $x \longrightarrow x$ (identidad) y $x \longrightarrow -x$ (simetría respecto del origen) que se notan, respectivamente, 1 y -1 . En efecto, toda aplicación lineal de una recta en sí misma es de la forma $x \longrightarrow x$ y si pertenece al grupo ortogonal, la relación $\phi(\lambda x, \lambda x) = \phi(x,x)$ implica $\lambda = \pm 1$.

Entonces, según el corolario 2, hay sólo dos aplicaciones ortogonales que dejan fijos todos los puntos de un hiperplano no isótropo. Una de ellas es la identidad, y la otra está determinada por:

$$s(x) = x \qquad (x \text{ en el hiperplano})$$

$$s(x) = -x \qquad (x \text{ en la recta ortogonal al hiperplano}).$$

Se vé que ambas aplicaciones son involutivas (es decir, por ejemplo, que $s^2 = 1$). Como vamos a ver, s es la simetría respecto del hiperplano considerado.

-o-

6.5.- PROYECTORES ORTOGONALES. SIMETRIAS

En general, si p es un endomorfismo de un espacio vectorial E , se dice que p es un proyector si $p^2 = p$, es decir si para todo x : $p(p(x)) = p(x)$. Tam-

bién se dice que $p(E)$ es el subespacio sobre el cual proyecta p . Por otra parte, un endomorfismo u se denomina involutivo si $u^2 = 1$ (lo que implica que es un automorfismo igual a su propio inverso) .

Lema 2 :

Para que el endomorfismo u sea involutivo es necesario y suficiente que el endomorfismo $p^- = \frac{1}{2}(1-u)$ sea un proyector. En tal caso también $p^+ = \frac{1}{2}(1+u)$ es un proyector y es claro que $u = p^+ - p^-$.

(b) Si u es involutivo, los subespacios $V^+ = p^+(E)$ y $V^- = p^-(E)$ son suplementarios. V^+ es el conjunto de los vectores tales que $u(x) = x$ (vectores invariantes para u) y V^- el de los vectores tales que $u(x) = -x$.

Demostración:

Si $u^2 = 1$, se tiene:

$$(\tfrac{1}{2}(1-u))^2 = (\tfrac{1}{2}.1)^2 - \tfrac{1}{2}\,u + (\tfrac{1}{2}\,u)^2 = \tfrac{1}{4}.1 + \tfrac{1}{4}.1 - \tfrac{1}{4}.u = \tfrac{1}{2}(1-u) \ ,$$

es decir $(p^-)^2 = p^-$. Deshaciendo en sentido contrario el razonamiento, se ve que si p^- es un proyector, entonces $u^2 = 1$. Y un cálculo como el de arriba muestra que también $(p^+)^2 = p^+$.

(b) Es claro que $E = V^+ + V^-$ así que para probar que la suma es directa basta ver que $V^+ \cap V^- = \{0\}$. Para ello, comencemos observando que si $z \in V^+$, $p^+(z) = \frac{1}{2}(1+u)(z) = z$ y si $z \in V^-$, $p^-(z) = \frac{1}{2}(1-u)(z) = z$. De ahí se deduce que en el primer caso es $u(z) = \frac{1}{2}(u+1)(z) = z$ y en el segundo: $u(z) = \frac{1}{2}(u-1)(z) = -z$. Si z estuviera en los dos espacios a la vez, eso implicaría $z = -z$ y z sería 0 . Finalmente, $u(x) = x$ implica $x = \frac{1}{2}\,x + \frac{1}{2}\,u(x)$ V^+ y, análogamente, $u(x) = -x$ implica x V^- .

OBSERVACION: Recíprocamente, si se da la descomposición $E = V^+ \oplus V^-$ existe una y sólo una involución u que tiene a V^+ y V^- como subespacios propios en el sentido anterior. Basta definir la aplicación lineal u mediante $u(x) = x$ $(x \in V^+)$ y $u(x) = -x$ $(x \in V^-)$ y notar que es involutiva. La unicidad es consecuencia directa de lo que precede.

-o-

Lema 3 :

Con la notación del lema anterior: si u es involutivo, las tres condiciones siguientes son equivalentes:

(a) $u \in \varphi(Q)$

(b) Los subespacios $U^+ = p^+(E)$, $U^- = p^-(E)$ son ortogonales (lo cual implica que además son no isótropos).

(c) $u = u^{\#}$ (es decir u es hermitiano, cf. § 9) .

Las transformaciones involutivas u que verifican una (y por tanto las tres) de estas condiciones se llaman simetrías. En particular, se tiene: una transformación ortogonal u es una simetría si y sólo si existe un subespacio no isótropo M tal que $u(x) = x$ en M y $u(x) = -x$ en M^0 .

Demostración:

Si $x \in U^+$ y $y \in U^-$, se tiene: $\phi(x,y) = \phi(u(x) , -u(y)) = -\phi(x,y) \Longrightarrow \phi(x,y) = 0$, es decir: (a) implica (b) .

Supongamos ahora que U^+ y U^- son ortogonales y sea x,y dos vectores de U^+, o dos vectores de U^- , o un vector de U^+ y otro de U^- . En el primero o segundo caso lo observado arriba prueba que se tiene $\phi(x,y) = \phi(u(x) , u(y))$ ó $\phi(x,y) = \phi(-u(x) , -u(y)) = \phi(u(x) , u(y))$ respectivamente; en el tercer caso se tiene o bien $\phi(x,y) = \phi(u(x) , -u(x)) = 0$ o bien $= \phi(-u(x) , u(y)) = 0$, según cuál de los dos vectores es el que está en U^+ . En todos los casos esto prueba que $u \in \varphi(Q)$, de modo que también (b) implica (a) .

Finalmente, $u \in \varphi(Q)$ es equivalente a $u^{\#} = u^{-1}$, de modo que si $u^2 = 1$, $u \in \varphi(Q)$ es equivalente a $u = u^{\#}$, o sea (a) equivale a (c) .

La última parte se demuestra así: Si u es una simetría, basta poner $M = U^+$, y recíprocamente, si M es un subespacio no isótropo, la aplicación ortogonal definida por: $u(x) = x$ en M y $u(x) = -x$ en M^0 (corolario 1 del lema 1) verifica $u^2 = 1$ y es por consiguiente una simetría.

Este teorema establece una correspondencia biunívoca entre las simetrías y los subespacios no isótropos. Para ponerla de manifiesto se acostumbra a decir que u es la simetría respecto de M . Como nos interesarán especialmente las simetrías respecto de hiperplanos, en lo sucesivo si se dice simetría sin otro calificativo deberá sobreentenderse que se trata de una simetría respecto de un hiperplano (no isótropo).

-o-

Lema 4 :

Si $w \in \varphi(Q)$, y si s es la simetría respecto de M , entonces su conjugada wsw^{-1} es la simetría respecto de w(M) .

Demostración:

En primer lugar, notemos que $(wsw^{-1})^2 = wsw^{-1} wsw^{-1} = 1$ (porque $s^2 = 1$) , de modo que wsw^{-1} es una simetría. Entonces:

$wsw^{-1}(x) = wsw^{-1}(y) = ws(y) = w(y) = x$ ($x = w(y)$, y M)

$wsw^{-1}(x) = wsw^{-1}(y) = ws(y) = w(-y) = -x$ ($x = w(y)$, y M^0)

prueban que el subespacio de la simetría wsw^{-1} es justamente w(M) .

Terminemos este número mostrando la fórmula que da las simetrías respecto de hiperplanos. Sea s la simetría respecto del hiperplano H y sea $a \in H^0$, $a \neq 0$; cada $x \in E$ se escribe de modo único en la forma $x = x_H + \lambda a$ $(x_H \in H)$, de modo que: $s(x) = x_H - \lambda a = x - 2\lambda a$. Y podemos calcular λ en la forma siguiente:

$$\varphi(x,a) = \varphi(x_H + \lambda a , a) = \varphi(x_H,a) + \lambda \varphi(a,a) = \lambda \varphi(a,a)$$

de modo que se obtiene finalmente la expresión:

$$s(x) = x - 2 \frac{\varphi(x,a)}{\varphi(a,a)} \cdot a$$

-o-

6.6.- SEMEJANZAS

Un automorfismo u de E se denomina semejanza de multiplicador $\alpha \in K$ $(\alpha \neq 0)$ si: $\varphi(u(x) , u(y)) = \alpha \varphi(x,y)$ $(\forall x, \forall y \in E)$.

Es claro que las semejanzas forman un grupo, notado $S(Q)$, ya que la fórmula que las define permite verificar que si u es una semejanza de multiplicador α , y si v una semejanza de multiplicador β , entonces uv es una semejanza de multiplicador $\alpha\beta$. Esto mismo indica además que la aplicación $u \longrightarrow$ multipl.(u) es un homomorfismo de $S(Q)$ en el grupo multiplicativo K^* . El núcleo de este homomorfismo (semejanzas de multiplicador igual a 1) es precisamente el grupo ortogonal, que es entonces un subgrupo distinguido del grupo de las semejanzas.

También (obviamente) el grupo H de las homotesias (de razón no nula) es un subgrupo distinguido de $S(Q)$, y más precisamente el multiplicador de la homotecia de razón λ es λ^2 .

Sea v la homotecia de razón β , y u una transformación ortogonal. Entonces $\varphi(vu(x) , vu(y)) = \beta^2 \varphi(x,y)$, de modo que vu es una semejanza cuyo multiplicador es un cuadrado. Recíprocamente, si w es una semejanza de multiplicador β^2 , sea v la homotecia de razón β . Entonces: $\varphi(wv^{-1}(x) , wx^{-1}(y)) = \frac{1}{\beta^2} \varphi(w(x) , w(y)) = \frac{\beta^2}{\beta^2} \varphi(x,y) = \varphi(x,y)$ es decir que $wv^{-1} = u$ es una transformación ortogonal y por consiguiente también es w el producto uv de una transformación ortogonal y por consiguiente también es w el producto uv de una transformación ortogonal por una homotecia.

-o-

Si u es la semejanza de multiplicador α , como

$$\varphi(x, \alpha y) = \alpha \varphi(x,y) = \varphi(u(x) , u(y)) = \varphi(x , u^{\#}u(y))$$

y como φ es no degenerada, resulta que $u^{\#}u$ es la homotecia de razón α = = multipl. (u) . Como el determinante de esta homotecia es α^n $(n = \dim (E)$,

deducimos:

$$(\det u)^2 = \alpha^n = (\text{multip. } u)^n \qquad (\#)$$

lo que nos induce a analizar por separado los dos casos siguientes:

Si n es impar: $n = 2q+1$, llamemos h a la homotecia de razón $\alpha^{-q}.\det(u)$. Decimos que $h^{-1}u$ es una transformación ortogonal, es decir que en este caso toda semejanza es el producto de una homotecia por una transformación ortogonal. En efecto, h^{-1} es la homotecia de razón $\alpha^q(\det u)^{-1}$, y de multiplicador: $\alpha^{2q}(\det u)^{-2}$, de modo que el multiplicador de $h^{-1}u$ es: $\alpha = \alpha^{2q}(\det u)^{-2} = (\det u)^2.(\det u)^{-2} = 1$.

Si n es par: $n = 2q$, la relación de arriba prueba que

$$\det u = \pm \alpha^q$$

y eso permite clasificar las semejanzas en dos tipos: las semejanzas tales que $\det u = (\text{mult. } u)^{n/2}$ se llaman directas y las otras, inversas. Es claro que las semejanzas directas forman grupo, que es un subgrupo distinguido de $S(Q)$ y que contiene el grupo de las rotaciones $S^+(Q)$. Lo notaremos con $S^+(Q)$.

-o-

§7.- PROPIEDADES PARTICULARES DE LAS FORMAS HERMITIANAS

En este parágrafo mantenemos también en general las hipótesis y notaciones precedentes pero supondremos, para simplificar, que K es de característica diferente de 2 . ϕ designa una forma hermitiana no nula (pero no necesariamente no degenerada) para un automorfismo J . Como ya hemos observado, cuando J es la identidad, ϕ es bilineal simétrica, y por tanto toda la teoría es aplicable a la forma cuadrática definida por ϕ : $Q(x) = \phi(x,x)$ (o bien $Q(x) = 2\,\phi(x,x)$) .

(#) Aquí se usa $\det(u) = \det(u^\#)$, relación que se prueba así: Si R es la matriz de ϕ , vale la fórmula: $\phi(x,y) = {}^t xRy$. (Debido al escaso uso que haremos de esta fórmula nos pareció preferible excluirla de los capítulos I ó II para simplificar la expresión. Para el que conoce un poco de cálculo matricial, su demostración es inmediata). Entonces, si M , M' son las matrices de u , $u^\#$, se tiene : ${}^t x$, ${}^t MRy = {}^t xRM'y$, de donde: $M' = R^{-1}\,{}^t MR$, que implica: $\det(u) = \det(u^\#)$.

7.1.- Teorema 1 :

E admite una base ortogonal (para ϕ), es decir, por definición, una base (e_i) tal que $\phi(e_i,e_j) = 0$, $(i \neq j)$.

Demostración :

En primer lugar, debemos observar que existen en E vectores no isótropos. De otro modo se tendría que, para todo x y para todo y en E : $\phi(x,y) = -\overline{\phi(x,y)}$ (que se deduce de $\phi(x+y , x+y) = 0$) y tomando x e y de modo que $\phi(x,y) = 1$ resulta $1 = -1$ (porque $\phi(\lambda x,y) = -\overline{\phi(\lambda x,y)}$ implica $\bar{\lambda} = -\lambda$ para todo $\lambda \in K$) y K sería de característa 2 , contra lo supuesto.

Razonemos por recurrencia: suponemos que si la dimensión del espacio es menor que n , existe base ortogonal. Entonces, sea x , no isótropo, es decir $\phi(x,x) \neq 0$. Sabemos que si H es el hiperplano (#) ortogonal a Kx , entonces $E = H \oplus Kx$, y por la hipótesis de recurrencia, H admite una base ortogonal $\{e_2,\ldots,e_n\}$. Luego, $\{x,e_2,\ldots,e_n\}$ es una base ortogonal de E . Como el teorema es obvio si $n = 0$ o si $n = 1$, vale para todo n .

-o-

7.2.- REFERENCIA A LOS CASOS CLASICOS

En lo que sigue nos referiremos en diversas oportunidades a los dos casos clásicos siguientes:

(1) K es el cuerpo $\mathbb{R}$ de los números reales y J es la identidad, de modo que ϕ es bilineal simétrica y puede considerarse como asociada a una forma cuadrática.

(2) K es el cuerpo $\mathbb{C}$ de los números complejos y J es el automorfismo que lleva cada complejo en su conjugado.

Para abreviar la exposición en lo que sigue (y siempre que no de lugar a confusiones) cuando se haga referencia a una forma hermitiana sobre $\mathbb{R}$ o sobre $\mathbb{C}$ deberá sobreentenderse que se hacen, respectivamente, las hipótesis de (1) ó (2) . A veces diremos simplemente: "cuando $K = \mathbb{R}$ " , o " en el caso real" , etc.

En cualquiera de los dos casos, para todo $x \in E$ se verifica que $\phi(x,x)$ es real (pues en el segundo caso se tiene: $\phi(x,x) = \overline{\phi(x,x)}$).

En cualquiera de los dos casos, diremos que ϕ es positiva (resp. negativa) si $\phi(x,x) \geq 0$ para todo $x \in E$ (resp. ≤ 0 para todo $x \in E$). Para ello es necesario y suficiente que si (e_i) es una base ortogonal de E se verifique $\phi(e_i,e_i) \geq 0$

(#) El subespacio H ortogonal a x es de dimensión mayor o igual que n-1 , pero como no contiene a x porque éste no es isótropo, debe ser de dimensión exactamente n-1 ; de ahí que digamos el hiperplano H .

(respec. $\phi(e_i,e_i) \leq 0$). Si ϕ es positiva y no degenerada veremos que tiene que verificarse $\phi(e_i,e_i) > 0$ y por lo tanto E no contiene vectores isótropos (diferentes de 0), y $\phi(x,x)$ (ó $Q(x)$ cuando Q está definida) es un cuadredo para todo $x \in E$.

Corolario del teorema 1 :

Si $K = \mathcal{R}$ ó $K = C$ y si ϕ es positiva no degenerada, entonces existe una base ortonormal, es decir, por definición, una base (e_i) tal que: $\phi(e_i,e_j) = 0$ $(i \neq j)$.

Demostración:

El teorema 1 dice que existe una base (e'_i) ortogonal. Como ϕ es positiva no degenerada podemos escribir:

$$\phi(e'_i,e'_i) = \rho_i^2 \neq 0$$
$$\phi(e'_i,e'_j) = 0 \quad (i \neq j)$$

(cf. §7, corolario del teorema 1).

y entonces, definiendo $e_i = \frac{1}{\rho_i} e'_i$, se ve que (e_i) es la base ortonormal requerida (#) .

-o-

7.3.- MATRICES

Si E admite una base (e_i) ortogonal para la forma hermitiana ϕ , la matriz $(g_{ij}) = (\phi(e_i,e_j))$ de ϕ es de la forma:

$$\begin{pmatrix} g_{11} & 0 & 0 & \dots & 0 \\ 0 & g_{22} & 0 & \dots & 0 \\ 0 & 0 & g_{33} & \dots & 0 \\ \vdots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & g_{nn} \end{pmatrix}$$

donde, eventualmente, algunos de los g_{ii} puede ser nulos (cosa que sucede si y sólo si ϕ es degenerada). La fórmula que define a ϕ es evidentemente:
$\phi(\sum_i x^i e_i , \sum_j y^j e_j) = \sum_i x^i \bar{y}^i g_{ii}$ (en el caso real es un "polinomio homogéneo de segundo grado en dos variables").

Si E admite una base ortonormal para ϕ , la matriz de ϕ es:

(#) En el caso general, se puede afirmar la existencia de base ortonormal si, por ejemplo, ϕ es no degenerada y para cada $x \in E$ existe un $\rho \in K$ tal que $\phi(x,x) = \rho\bar{\rho}$. La demostración es trivial.

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & \dots & & \dots & 1 \end{pmatrix}$$

y la fórmula que define a ϕ es: $\phi(\sum_i x^i e_i , \sum_j y^j e_j) = \sum_i x^i y^{-i}$ (en el caso real ésta generaliza la expresión ordinaria del producto escalar).

-o-

§8.- LEY DE INERCIA

En este parágrafo supondremos además que $K = \mathbb{R}$ ó $K = \mathbb{C}$ y que ϕ es positiva .

8.1.- Teorema 1 :

Para todo x y para todo y en E vale la desigualdad de Schwartz:

$$\phi(x,y)\ \overline{\phi(x,y)} \leq \phi(x,x).\phi(y,y) \ .$$

Demostración :

Supongamos primero que $x = \lambda y$; entonces:

$$\phi(x,y)\ \overline{\phi(x,y)} = \phi(x,\lambda x)\ \overline{\phi(x,\lambda x)} = \bar{\lambda}\lambda\phi(x,x)\phi(x,x) = \phi(x,x)\phi(\lambda x,\lambda x)$$

lo que prueba el teorema en la forma: $\phi(x,y)\ \overline{\phi(x,y)} = \phi(x,x)\phi(y,y)$. En el caso general se puede razonar así:

$$0 \leq \phi(x+\lambda y\ ,\ x+\lambda y) = \phi(x,x) + \lambda\phi(y,x) + \bar{\lambda}\phi(x,y) + \lambda\bar{\lambda}\phi(y,y)$$

(para todo escalar λ). En particular, escribiendo $\lambda = \alpha\phi(x,y)$ $(\alpha \in \mathbb{R})$ se tiene que para todo α real:

$$\alpha^2\phi(x,y)\ \overline{\phi(x,y)}\ \phi(y,y) + 2\alpha\phi(x,y)\ \overline{\phi(x,y)} + \phi(x,x) \geq 0$$

Pero este es un polinomio de segundo grado en α con coeficientes reales. Sabemos que para que tenga signo constante el discriminante tiene que ser menor o igual que 0 , es decir:

$$\left[\phi(x,y)\ \overline{\phi(x,y)}\right]^2 \leq \phi(x,y)\ \overline{\phi(x,y)}\ \phi(x,x)\ \phi(y,y)$$

Entonces, si $\phi(x,y) \neq 0$, dividiendo por $\phi(x,y)\ \overline{\phi(x,y)} = |\phi(x,y)|^2$, se tiene la desigualdad de Schwartz. Cuando $\phi(x,y) = 0$, esta desigualdad es evidente.

Corolario :

Para que ϕ sea no degenerada es necesario y suficiente que $\phi(x,x) \neq 0$ para cada x diferente de 0 en E .

Demostración :

Si existe $x \neq 0$ tal que $\phi(x,x) = 0$, el teorema 1 dice que para todo y : $0 \leq \phi(x,y)\,\overline{\phi(x,y)} \leq 0$, o sea que x es ortogonal a todo E y ϕ es degenerada . En cambio, si $\phi(x,x) \neq 0$ para todo x diferente de 0 , no hay vectores isótropos no nulos y ϕ no puede ser degenerada.

-o-

8.2.- LEY DE INERCIA

Sea ϕ una forma hermitiana sobre E (no necesariamente positiva, pero suponiendo aún que $K = \mathbb{R}$ ó $K = \mathbb{C}$), entonces:

(a) Existen dos subespacios E^+ y E^- tales que $E = E^+ \oplus E^- \oplus E^0$, la restricción de ϕ a E^+ es positiva no degenerada y la restricción de ϕ a E^- es negativa no degenerada.

(b) Existe una base ortogonal (e_i) de E tal que

$$\phi\Big(\sum_i x^i e_i \,,\, \sum_j y^j e_j\Big) = \sum_{i=1}^{s} x^i \bar{y}^i - \sum_{i=s+1}^{s+t} x^i \bar{y}^i$$

(c) Si $\dim(E^+) = s$ y $\dim(E^-) = t$, estas dimensiones son las mismas para cada par de subespacios E^+ , E^- que verifiquen (a) . s es la máxima dimensión de los subespacios en los cuales ϕ es positiva no degenerada y t es la máxima dimensión de los subespacios en los cuales ϕ es negativa no degenerada.

(d) El rango de ϕ es $s+t$.

(e) Si ϕ es no degenerada, su índice, ν , es el menor de los números s y t. El par $(s;t)$ se denomina signatura de ϕ .

Demostración:

Procederemos por pasos:

(1) Sea (e'_i) una base ortogonal de E y ordenemos sus elementos de modo que

$$\phi(e'_i,e'_i) > 0 \quad (1 \leq i \leq s) \;;\; \phi(e'_i,e'_i) \leq 0 \quad (s+1 \leq i \leq s+t) \;;$$

$$\phi(e'_i,e'_i) = 0 \quad (s+t+1 \leq i \leq n) \;.$$

Entonces, usando el corolario del teorema 1, resulta que vale (a) si se llama E^+ (resp. E^-) al subespacio engendrado por $\{e'_1,\ldots,e'_s\}$ (resp. $\{e'_{s+1},\ldots,e'_{s+t}\}$, y se ve que E^0 es el subespacio engendrado por $\{e'_{s+t+1},\ldots,e'_n\}$.

(2) Para probar (b) , observamos que:

$$\phi(e_i', e_i') = \rho_i^2 \in \mathbb{R} \quad , \quad \phi(e_i', e_i') = -\rho_i^2 \in \mathbb{R} \quad , \quad \phi(e_i', e_i') = 0$$

según que sea $1 \leq i \leq s$, $s+1 \leq i \leq s+t$, ó $s+t+1 \leq i \leq n$, respectivamente. Entonces si se pone $e_i = e_i'/\rho_i$, (e_i) sigue siendo una base ortogonal pero ahora se tiene: $\phi(e_i, e_i) = 1$, ó -1 , ó 0 , según que $1 \leq i \leq s$, ó $s+1 \leq i \leq s+t$, ó $s+t+1 \leq i \leq n$, y vale (b) .

(3) Sea P (resp. N) un subespacio de E tal que la restricción a P (resp. a N) de ϕ es positiva y no degenerada (resp. negativa y no degenerada) . Si se prueba que $\dim(P) \leq \dim(E^+) = s$ (resp. $\dim(N) \leq \dim(E^0) = t$) se tiene la última parte de (c) , y ésta implica la primera parte porque si hay otra descomposición del tipo (a) : $E = E'^+ \oplus E'^- \oplus E^0$ resulta, por una parte, $\dim(E'^+) \leq \dim(E^+)$, e intercambiando las letras: $\dim(E^+) \leq \dim(E'^+)$, y análogamente para E^- .

Observando esto, razonemos, por ejemplo, para P , Por la definición de E^+, $P \cap (E^- \oplus E^0) = \{0\}$ lo que prueba que la suma de P , E^- y E^0 es directa. Entonces $\dim(P) + \dim(E^-) + \dim(E^0) \leq n$, de donde, escribiendo la relación análoga que se deduce de (a) , se concluye $\dim(P) \leq \dim(E^+) = s$. Así, (c) está demostrada .

(4) Por definición, el rango de ϕ es la dimensión de E/E^0 , que es igual a la de un suplementario de E^0 , es decir, por ejemplo a $\dim(E^+) + \dim(E^-) = s+t$. Esto prueba (d) .

(5) Demostremos, finalmente, (e) . Designemos por el momento con q al menor de los números s y t (que en este caso verifican $s+t = n$ porque siendo ϕ no degenerada es $E^0 = 0$). Definimos: F = subespacio engendrado por $\{e_1+e_{s+1}, \ldots, e_q+e_{s+q}\}$; F' = subespacio engendrado por $\{e_1-e_{s+1}, \ldots, e_q-e_{s+q}\}$. En primer lugar, veamos que F y F' son totalmente isótropos. Por ejemplo , si $x = \sum_i \lambda_i (e_i+e_{s+i})$ y si $y = \sum_i \mu_i (e_i+e_{s+i})$ (elementos arbitrarios de F) se tiene:

$$\phi(x,y) = \sum_{ij} \lambda_i \bar{\mu}_j \, \phi(e_i+e_{s+i} \, , \, e_j+e_{s+j}) =$$

$$= \sum_{ij} \lambda_i \bar{\mu}_j \, (\phi(e_i, e_j) + \phi(e_{s+i}, e_j) + \phi(e_i, e_{s+j}) + \phi(e_{s+i}, e_{s+j})) = 0$$

(debido a las propiedades de la base (e_i) ; si todos los índices son distintos de a pares, el paréntesis es nulo porque la base es ortogonal; en cambio si $i = j$, el paréntesis es $1+0+0-1$ y nuevamente se anula).

En segundo lugar, notamos que $F + F'$ está engendrado por los vectores $\{e_1, \ldots, e_q, e_{s+1}, \ldots, e_{s+q}\}$, y eso nos permite concluir que $F + F'$ es no isótropo. Entonces, si H es su subespacio ortogonal, sabemos que H es no isótropo y $E = (F \, F') \oplus H$. Ahora, recurriendo a los e_i que engendran H se ve en seguida que o bien ϕ restringida a H es positiva no degenera-

da o bien esta restricción es negativa no degenerada. En ambos casos se concluye que H no contiene vectores isótropos.

Por otra parte, como F es totalmente isótropo, $F \subset F^0$, y de ahí:

$$F \subset F + F' \implies (F+F')^0 = H \supset F^0 \implies F + H \subset F^0$$

Pero como $\dim (F+H) = \text{codim}\,(F') = \text{codim}\,(F) = \dim (F^0)$, se tiene necesariamente que $F + H$ es igual a F^0.

El resto de la demostración se resume así: demostraremos que si z es un vector isótropo perteneciente a F^0, entonces necesariamente z pertenece a F. Eso probará que F es un subespacio totalmente isótropo maximal y por lo tanto $\nu = \dim (F) = q$.

Como $F^0 = F \oplus H$, un tal z se escribe de modo único en la forma $z = z_F + z_H$ $(z_F \in F \ , \ z_H \in H)$. Entonces, usando que F es totalmente isótropo, que H es ortogonal a F y que z se supone isótropo, se tiene:

$$0 = \phi(z,z) = \phi(z_F, z_F) + \phi(z_F, z_H) + \phi(z_H, z_F) + \phi(z_H, z_H)$$

vale decir: $\phi(z_H, z_H) = 0$. Y como H no contiene vectores isótropos diferentes de 0, resulta $z_H = 0$, es decir $z = z_F \in F$, l.q.q.d. (#)

-o-

OBSERVACION: Según 7.3, la forma ϕ puede escribirse (por ejemplo en el caso real) como un polinomio homogéneo de segundo grado de la forma:

$$\phi(x,y) = \sum_{ij} x^i y^j g_{ij}$$

La ley de inercia dice que puede hacerse un "cambio de base" de modo que Q se reduzca a una suma algebraica de cuadrados:

$$\phi(x,y) = \sum_{i=1}^{s} x^i y^i - \sum_{i=s+1}^{t} x^i y^i$$

$$Q(x) = \phi(x,x) = \sum_{i=1}^{s} (x^i)^2 - \sum_{i=s+1}^{s+t} (x^i)^2$$

y la signatura (s,t) indica la cantidad de cuadrados, s, afectados del signo $+$ y la cantidad de cuadrados, t, afectados del signo $-$. Además, el teorema dice que estas "cantidades" son independientes del método seguido para la "reducción" de la forma ϕ

-o-

(#) Aquí se prueba un hecho completamente general de la teoría de subespacios totalmente isótropos: Si $E = F \oplus F' \oplus H$ con F y F' totalmente isótropos, $F+F'$ no isótropo y ortogonal a H y H sin ningún vector isótropo no nulo, entonces F y F' son totalmente isótropos maximales.

§9.- REDUCCION DE ENDOMORFISMOS NORMALES Y HERMITIANOS

En todo este parágrafo supondremos que estamos en uno de los casos clásicos: $K = \mathbb{R}$, ó $K = \mathbb{C}$, y que ϕ es una forma hermitiana positiva y no degenerada sobre E (cf. 6.12). Por primera vez estudiamos en este parágrafo relaciones de otra forma sesquilineal con respecto a la forma fundamental ϕ ("forma métrica") o (cosa que en ciertos casos es equivalente) relaciones de un endomorfismo de E con ϕ .

9.1.- ENDOMORFISMOS NORMALES. REDUCCION

Teorema 1 :

Sea S un conjunto de endomorfismos de E tal que si $u \in S$, entonces también $u^* \in S$ (abreviadamente: S es estable para la aplicación $u \longrightarrow u^*$):

(a) *Si V es un subespacio de E estable para S (es decir, si $u(V) \subset V$ para cada $u \in S$) entonces V^0 es estable para S .*

(b) *E se descompone en suma directa: $E = E_1 \oplus \dots \oplus E_p$ de subespacios ortogonales dos a dos y estables minimales para S .*

(esto último significa lo siguiente: en primer lugar, $u(E_i) \subset E_i$ para cada $u \in S$, y en segundo lugar, si F es un subespacio no nulo contenido en un E_i y si $u(F) \subset F$ para cada u S , entonces $F = E_i$).

Demostración de (a) :

Por la hipótesis, si $x \in V^0$ y $y \in V$, se tiene:

$$\phi(y, u(x)) = \phi(u^*(y), x) = 0 \quad (\forall y \in V) \text{ que implica } u(x) \in V^0 .$$

Demostración de (b) :

Razonamos por recurrencia sobre $n = \dim(E)$, observando en primer lugar que la proposición es trivial si $n = 0$ o si $n = 1$ (en tal caso el propio E es minimal y estable para S). Suponemos entonces que si F es un espacio de dimensión menor que n munido de una forma como ϕ , entonces F se descompone en suma directa de subespacios F_i estables minimales para una familia de endomorfismos como S y ortogonales dos a dos. Sea entonces n' la menor de las dimensiones de los subespacios no nulos de E estables para S , y sea V un subespacio estable para S y de dimensión n' . Entonces, claro, V es estable minimal, pero por (a) , también V^0 es estable para S y su dimensión es menor que n . Entonces V^0 y la restricción de ϕ a V^0 proporcionan una situación en la cual es aplicable la hipótesis de recurrencia: V^0 se descompone en suma directa de subespacios ortogonales dos a dos y estables minimales para S . De aquí resulta que también $E = V \oplus V^0$ tiene esa propiedad.

-o-

Se dice que un endomorfismo es normal si conmuta con su adjunto, es decir: $u(u^{\#}(x)) = u^{\#}(u(x))$ para cada $x \in E$. Antes de enunciar el teorema particular de reducción de endomorfismos normales, recordemos algunas definiciones. Si u es un endomorfismo de E , un $x \in E$, $x \neq 0$, se llama vector propio de u si existe un escalar λ tal que $u(x) = \lambda x$ (es decir, si y sólo si u deja invariante la recta de x , o si y sólo si esta recta es estable para u). En tal caso, dicho escalar λ se llama valor propio de u .

Teorema 2 :

Supongamos $K = C$ y sea u un endomorfismo normal de E . Entonces E se descompone en suma directa de subespacios E_i ortogonales dos a dos y de dimensión 1 tales que cualquier elemento no nulo de cualquier E_i es un vector propio de u, y existe en E una base ortonormal formada por autovectores de u .

Demostración:

Aplicaremos el teorema 1 al álgebra S engendrada por u , $u^{\#}$ y 1 (es decir la mínima álgebra de endomorfismo que contiene estos tres). Como por hipótesis $u^{\#}u = uu^{\#}$, S es conmutativa y está formada por los polinomios construídos con las tres "variables" u , $u^{\#}$, 1 , es decir por los endomorfismos de la forma: $\sum_{\substack{h,k \\ u \longrightarrow u^{\#}}} \lambda_{hk}\, u^h\, (u^{\#})^k$. Como $(u^h(u^{\#})^k)^{\#} = u^k(u^{\#})^h$, es estable para la aplicación $u \longrightarrow u^{\#}$.

Entonces, el teorema 1 dice que $E = E_1 \oplus \ldots \oplus E_p$ donde los E_i son ortogonales dos a dos y estables minimales para S . Decimos que una vez que se demuestre que cada E_i contiene un vector propio x_i para u : $u(x_i) = \lambda_i x_i$, el teorema puede considerarse demostrado.

En primer lugar: $u(\mu x_i) = \mu u(x_i) = \mu \lambda_i x_i$ prueba que cada recta Kx_i es estable para u . Si mostramos ahora que los autovectores de u también son autovectores de $u^{\#}$, esas rectas serán estables para $u^{\#}$ (y lógicamente también para 1) y por tanto para S , lo que implicará: $E_i = Kx_i$: los E_i serán unidimensionales. Con más precisión que lo afirmado, demostremos que, en general, si $u(x) = \lambda x$, entonces $u^{\#}(x) = \bar{\lambda} x$ (con la única hipótesis de que u es normal). Por una parte, tenemos: $\varphi(u(x) , x) = \lambda \varphi(x,x) = \varphi(x, \bar{\lambda} x) = \varphi(x , u^{\#}(x))$, es decir que $t = u^{\#}(x) - \bar{\lambda} x$ es un vector ortogonal a x . Pero además:

$$\varphi(u^{\#}(x) , u^{\#}(x)) = \varphi(t + \bar{\lambda} x , t + \bar{\lambda} x) = \bar{\lambda} \lambda \varphi(x,x) + \varphi(t,t) =$$

$$= \varphi(\lambda x, \lambda x) + \varphi(t,t) = \varphi(u(x) , u(x)) + \varphi(t,t) =$$

$$= \varphi(u^{\#}u(x) , x) + \varphi(t,t) = \varphi(uu^{\#}(x,x) + \varphi(t,t) =$$

$$= \varphi(u^{\#}(x) , u^{\#}(x)) + \varphi(t,t)$$

lo que nos dice que $\emptyset(t,t) = 0$, y siendo $\emptyset$ positiva no degenerada, esto implica $t = 0$ (cf. 7 , corolario del teorema 1). Por la definición de t , es entonces $u^{\#}(x) = \bar{\lambda} x$, l.q.q.d.

Entonces, puede considerarse demostrado que cada E_i es de dimensión 1 , de modo que tomando un vector en cada E_i se tiene una base ortogonal formada por autovectores de u (y de $u^{\#}$) . Y ya sabemos que a partir de ella (siendo $\emptyset$ positiva y no degenerada) siempre se puede construir una base ortonormal formada por vectores proporcionales a los dados.

Así hemos reducido el teorema a demostrar solamente que cada subespacio estable minimal E_i contiene un autovector de u . Para ello, comencemos observando que siendo E_i estable para u y para $u^{\#}$, las restricciones de éstos a E_i son endomorfismos de E_i , y, obviamente, endomorfismo normales de E_i . Entonces lo que queremos resulta en la forma siguiente: sea dada en E_i una base cualquiera y sean (x^j) las coordenadas de un punto x E_i , y (a_{kl}) la matriz del endomorfismo u_i (restricción de u) a E_i . La ecuación $u(x) = \lambda x$ se escribe entonces así:

$$\sum_1 a_{kl} x^l = \lambda x^k \qquad (k = 1,2,\ldots,m)$$

(suponiendo que m es la dimensión de E_i), de modo que equivale al sistema lineal homogéneo:

$$\begin{aligned}
&(a_{11}-\lambda)x^1_1 + \ldots + \ldots + \ldots + a_{1m}x^m_m = 0\\
&a_{21}x_1 + (a_{22}-\lambda)x^2 + \ldots + a_{2m}x^m = 0\\
&\vdots\\
&a_{m1}x^1 + \ldots + \ldots + (a_{mm}-\lambda)x^m
\end{aligned}$$

cuyo determinante es:

$$\Delta(\lambda) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & \cdots & a_{mm} \end{pmatrix}$$

Como $\Delta(\lambda) = 0$ es una ecuación algebraica de grado m en λ con coeficientes complejos, existe por lo menos un valor complejo de λ tal que $\Delta(\lambda) = 0$, y sabemos que el sistema homogéneo correspondiente a ese valor tiene una solución idénticamente nula que proporciona las coordenadas del autovector buscado.

-o-

9.2.- ENDOMORFISMOS HERMITIANOS

Se dice que un endomorfismo u de E es hermitiano si $u^{\#} = u$. En consecuencia, todo endomorfismo hermitiano es normal.

Teorema 3 a :

Sea $K = \mathbb{C}$, y u un endomorfismo hermitiano de E . Entonces todos sus autovectores pertenecen a $\mathbb{R}$, y existe una base de E formada por autovectores de E formada por autovectores de u , que es una base ortonormal.

Demostración :

Ya que u es normal, vale el teorema 2, y por tanto sólo hay que probar que si $u(x) = \lambda x$ para un cierto $x \in E$, $x \neq 0$, entonces λ es real. Pero esto es inmediato porque hemos visto que si x es autovector de u , también lo es de $u^{\#}$, y que vale más precisamente: $u^{\#}(x) = \bar{\lambda} x$, entonces si u es hermitiano resulta $\lambda = \bar{\lambda}$, l.q.q.d.

-0-

Teorema 3 b :

Sea $K = \mathbb{R}$, y u un endomorfismo hermitiano de E . Entonces existe una base ortonormal de E formada por autovectores de u .

Demostración:

Usaremos el teorema 3 a, para lo cual hemos de "sumergir" E , φ , u , en un caso en que dicho teorema sea aplicable.

Sea $E_c = E \times E$ (por ahora sólo como conjunto) y demos a E_c una estructura de espacio vectorial sobre $\mathbb{C}$ mediante las definiciones:

si $z_1 = (x_1, y_1)$ y $z_2 = (x_2, y_2)$, entonces $z_1 + z_2 = (x_1 + x_2 , y_1 + y_2)$

si $\lambda = \alpha + i\beta$, (α, β reales) y $z = (x,y)$: $\lambda z = (\lambda x - \beta y , \beta x + \lambda y)$

Es un simple ejercicio de cálculo verificar que esta suma $z_1 + z_2$ y este producto por escalares z , tienen todas las propiedades requeridas para hacer de E_c un espacio vectorial sobre $\mathbb{C}$

En particular, si $\alpha \in \mathbb{R}$, se tiene $\alpha z = \alpha (x,y) = (\alpha x, \alpha y) = \alpha(x,0) + \alpha(0,y)$ y si $\beta \in \mathbb{R}$, se tiene: $i\beta z = i\beta(x,y) = (-\beta y, \beta x) = -\beta(y,0) + \beta(0,x)$. De aquí resulta que si se identifica E a una parte de E_c mediante la inyección : $x \longrightarrow (x,0)$, el elemento (x,y) de E_c puede escribirse en la forma: $(x,y) = (x,0) + (0,y) = (x,0) - i.i(0,y) = (x,0) + i.(y,0) = x + iy$.

Si se define φ_c en E_c mediante:

$$\varphi_c(x+iy , x'+iy') = \varphi(x,x') + i\varphi(y,x') - i\varphi(x,y') + \varphi(y,y')$$

y se recuerda que ϕ (por estar en el caso real) es bilineal simétrica, y que $\bar{i} = -i$, se comprueba en seguida que ϕ_c es sesquilineal (para $\lambda \longrightarrow \bar{\lambda}$) y que $\phi_c(x+iy\ ,\ x'+iy') = \overline{\phi_c(x'+iy'\ ,\ x+iy)}$, es decir que ϕ_c es una forma hermitiana sobre E_c. Además, (haciendo y e y' iguales a 0 en la definición) $\phi_c(x,y) = \phi(x,y)$, de modo que ϕ_c extiende a ϕ. Finalmente:

$$\phi_c(x+iy\ ,\ x+iy) = \phi(x,x) - i\,\phi(y,x) - o\,\phi(x,y) + \phi(y,y) =$$

$$= \phi(x,x) + \phi(y,y) \geq 0$$

prueba que ϕ_c es positiva, y si $z = (x,y) \neq 0$ (lo que exige que o x ó y ó ambos sean no nulos) es $\phi_c(z,z) > 0$, de modo que ϕ_c es positiva y no degenerada.

Ahora extendemos u a E_c mediante la definición: $u_c(x+iy) = u(x) + i\,u(xy)$ y resulta (mediante cálculo trivial) que u_c es un endomorfismo hermitiano de E_c. (Se puede probar en la misma forma que si v es cualquier endomorfismo de E y si se define $v_c(x+iy) = v(x) + i\,v(y)$, entonces $(v_c)^{\#} = (v^{\#})_c$, es decir que $(v_c)^{\#}(x+iy) = v^{\#}(x) + i\,v^{\#}(y)$.)

Entonces el teorema 3 a dice que E_c admite una base ortonormal (para ϕ_c), $z_j = x_j + i\,y_j$ $(1 \leq j \leq n)$ [#] formada por autovectores de u_c:

$$u_c(z_j) = \lambda_j x_j + i\,\lambda_j y_j \qquad (\lambda_j \in \mathbb{R})$$

es decir: $u(x_j) + i\,u(y_j) = \lambda_j x_j + i\,\lambda_j y_j$, que implica:

$$u(x_j) = \lambda_j\, x_j$$

$$u(y_j) = \lambda_j\, y_j$$

Ahora bien, como u es hermitiano, el teorema 1 es aplicable al espacio E y a la familia S que consta del sólo elemento u. E se descompone en suma directa de subespacios E_i ortogonales dos a dos y estables minimales para u. Entonces, el razonamiento precedente es aplicable a cada E_i (extendiendo E_i a $E_{i,c}$, etc) y por lo tanto se concluye como allí que cada E_i admite un autovector para u. Ya sabemos que eso implica que E_i (por ser estable minimal para u) es de dimensión 1 y que si $x_i \in E_i$, (x_i) es una base ortogonal de autovectores de u que se lleva inmédiatamente a una base ortonormal formada por autovectores de u. El teorema está demostrado [##].

-o-

[#] No hemos probado, porque es inmediato, que E_c es de dimensión n sobre $\mathbb{C}$, si E es de dimensión n sobre $\mathbb{R}$. Por ejemplo, una base de E_c es $(e_i, 0)$ si e_i es una base de E.

[##] Este razonamiento, aplicado al caso en que u es normal (no necesariamente hermitiano) permite demostrar que los subespacios estables minimales para u y $u^{\#}$ (en el caso real) son de dimensión 1 ó 2.

9.3.- CASO DE AUTOMORFISMOS ORTOGONALES, O UNITARIOS

Si u es un automorfismo unitario, como $u^{\#} = u^{-1}$, también es normal y vale el teorema 2 (cf. la nota (##) que es aplicable a este caso). En particular, dicho teorema vale también para automorfismos ortogonales en el caso real (que son, en ese caso, los automorfismos unitarios para la forma bilineal simétrica asociada a la forma cuadrática dada).

-o-

9.4.- ENDOMORFISMOS HERMITIANOS Y FORMAS HERMITIANAS

Para cada endomorfismo hermitiano u , consideremos la aplicación Ψ_u de $E \times E$ en K definida así:

$$\Psi_u(x,y) = \varphi(u(x) , y)$$

Decimos que Ψ_u es una forma hermitiana sobre E . En efecto:

$$\Psi_u(x+x' , y) = \varphi(u(x+x') , y) = \varphi(u(x) , y) + \varphi(u(x') , y) =$$

$$= \Psi_u(x,y) + \Psi_u(x',y) \quad , \text{ etc.}$$

y: $\Psi_u(x,y) = \varphi(u(x) ,y) = \varphi(x , u(y)) = \overline{\varphi(u(y) , x)} = \overline{\Psi_u(y,x)}$.

Reciprocamente, si Ψ es una forma hermitiana sobre E , como φ se supone no degenerada, el corolario del teorema 1, §1 , dice que si se fija $y \in E$, para cada $x \in E$, existe un único elemento $u(x) \in E$ tal que $\Psi(x,y) = \varphi(u(x) , y)$, y luego es inmediato comprobar que $u : x \longrightarrow u(x)$ es una aplicación lineal de E en E que es un endomorfismo hermitiano pues:

$$\varphi(u(x) , y) = \Psi(x,y) = \overline{\Psi(y,x)} = \overline{\varphi(u(y) , x)} = \varphi(x , u(y))$$

$$\text{es decir} \quad u = u^{\#} .$$

Además, la aplicación $u \longrightarrow \Psi_u$ es claramente biunívoca, de modo que es una biyección del conjunto de los endomorfismos hermitianos de E sobre el conjunto de las formas hermitianas sobre E . Esto permite traducir cualquier propiedad de los endomorfismos hermitianos en una propiedad de las formas hermitianas. Por ejemplo:

Teorema 4 :

(Reducción de una forma hermitiana respecto de una forma hermitiana φ , positiva y no degenerada). Si Ψ es una forma hermitiana sobre E (siempre en los casos $K = \mathbb{R}$, o $K = \mathbb{C}$), existe una base (e_i) de E que es ortonormal respecto de Ψ .

Demostración:

Sea u el endomorfismo hermitiano asociado a Ψ según la observación precedente

te: $\Psi(x,y) = \phi(u(x), y)$. Sabemos que existe una base ortonormal (para ϕ), (e_i), cuyos elementos son autovectores de u : $u(e_i) = \lambda_i e_i$ $(\lambda_i \in R)$. Entonces $\Psi(e_i,e_j) = \phi(u(e_i), e_j) = \lambda_i \phi(e_i,e_j) = 0$ (si $i \neq j$), l.q.q.d.

-o-

OBSERVACION: Según vimos en 6.3 el teorema afirma que si está dada en E una forma positiva no degenerada ϕ, para cada forma hermitiana Ψ existe una base (e_i) tal que

$$\phi(x,y) = \sum_i x^i y^{-i} \qquad \phi(x,x) = \sum_i |x^i|^2$$

$$(x,y) = \sum_i a_{ii} x^i y^{-i} \qquad (x,x) = \sum_i a_{ii} |x^i|^2 \qquad (K = C)$$

y fórmulas similares cuando $K = R$. En otras palabras, la matriz de Ψ con respecto a esa base es una matriz diagonal de la forma:

$$\begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ \vdots & & \\ 0 & 0 & \ldots a_{nn} \end{pmatrix}$$

en la cual algunos a_{ii} pueden ser nulos si Ψ es degenerada. Nótese que los a_{ii} son <u>invariantes</u> por ser autovalores del endomorfismo hermitiano correspondiente. Además (por la misma razón) si <u>todos</u> los a_{ii} son diferentes, ellos determinan la base (e_i) unívocamente (demuéstrese!). Como veremos en el capítulo siguiente, este teorema encierra el <u>teorema de reducción de la ecuación de una cuádrica a ejes principales</u>.

-o-

CAPITULO IV

APLICACIONES GEOMETRICAS

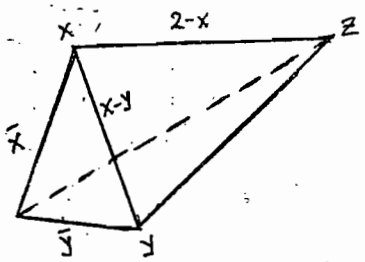
En este capítulo supondremos, para simplificar, que E es un espacio vectorial de dimensión finita sobre el cuerpo real, $\mathbb{R}$. Con $\varphi(x|y)$ designaremos una forma bilineal simétrica positiva y no degenerada sobre E, y con Q la forma cuadrática $Q(x) = (x|x)$. El número $(x|y)$ puede considerarse como el producto escalar de los vectores x e y, y $Q(x)$ como el cuadrado de la distancia del punto x al origen: $Q(x) = d(x,0)^2 = d(0,x)^2$; el número $\sqrt{Q(x)}$ se notará también con $|x|$ y se llamará longitud del vector x.

Para algunas cuestiones, es útil considerar a E como espacio afín (tomando como espacio de las traslaciones de E al propio espacio $E = T$). Por una única vez notemos con x, $\vec{x}$, a un mismo elemento según se considere como punto del espacio afín E o como traslación perteneciente al espacio vectorial $T = E$. Así, la traslación $\vec{t}$ aplicada al punto x da el punto $x+t$, de modo que con la notación de la introducción escribiremos: $x + \vec{t} = x+t$, etc., y siempre la diferencia $x-y$ de dos puntos de E representa una traslación de T (más precisamente, la traslación $\overrightarrow{x-y}$ que aplicada a y da x). De modo que, por ejemplo, si x e y son dos puntos de una recta afín, la dirección de esta recta está definida por el vector $x-y$, etc.

Cuando está dada en el espacio vectorial $T = E$ una forma $(x|y)$ con las propiedades de arriba, se dice que se ha definido una métrica (euclídea) en E, y el espacio afín E provisto de dicha forma se denomina espacio euclídeo. La distancia entre dos puntos x e y de un espacio euclídeo se define mediante: $d(x,y) = |\overrightarrow{x-y}| = \sqrt{(\vec{x}-\vec{y} \mid \vec{x}-\vec{y})}$. Por ejemplo, si x, y, z son tres puntos del espacio euclídeo E, para que los vectores $\overrightarrow{y-x}$ y $\overrightarrow{z-x}$ sean ortogonales es necesario y suficiente que $0 = (\overrightarrow{y-x}|\overrightarrow{z-x}) = (\vec{y}|\vec{z}) - (\vec{x}|\vec{z}) - (\vec{y}|\vec{x}) + (\vec{x}|\vec{x})$, condición que se verifica si y sólo si $(\overrightarrow{y-x}|\overrightarrow{y-x}) + (\overrightarrow{z-x}|\overrightarrow{z-x}) = (\vec{y}|\vec{y}) + (\vec{z}|\vec{z}) - 2.(\vec{y}|\vec{z})$, es decir que $\overrightarrow{y-x}$ y $\overrightarrow{z-x}$ son ortogonales si y sólo si

$$d^2(x,y) + d^2(y,z) = d^2(y,z)$$

Este es el teorema de Pitágoras.



Sea v una aplicación afín del espacio euclídeo E, y sea u la aplicación li

neal asociada (cf. Cap. 0). Se dice que v es un movimiento de E si y sólo si u es una transformación ortogonal para la forma Q definida por $(\ |\ )$ en el espacio vectorial $T = E$. Análogamente, v es una semejanza de E si u es una semejanza de $T = E$.

De manera similar, se extienden a los subespacios euclídeos todas las nociones más importantes de espacios vectoriales.

A modo de ejemplos digamos los siguientes: Si x e y son dos puntos distintos determinan una recta afín, que notaremos con R_{xy} (es la variedad afín engendrada por x e y) que está definida por la fórmula:

$$R_{xy} = \left\{ z \in E \ / \ z = x + \lambda(y-x) = (1-\lambda)x + \lambda y \right\}$$

o también:

$$R_{xy} = \left\{ z \in E \ / \ z = \lambda x + \mu y \quad , \text{ con } \lambda + \mu = 1 \right\}$$

Si x, y, z son tres puntos que no están en una misma recta afín, los vectores $\vec{a} = \overrightarrow{y-x}$ y $\vec{b} = \overrightarrow{z-x}$ son independientes. Entonces, x, y, z determinan un plano afín (la variedad afín engendrada por ellos) que está definido por:

$$P_{xyz} = \left\{ t \in E \ / \ t = x + \lambda\vec{a} + \mu\vec{b} = (1-\lambda-\mu)x - \lambda y - \mu z \right\}$$

o también:

$$P_{xyz} = \left\{ t \in E \ / \ t = \lambda x + \mu y + \nu z \quad , \text{ con } \lambda + \mu + \nu = 1 \right\}$$

-o-

También será usada la noción de espacio proyectivo asociado al espacio euclídeo E (que es el $P(\mathbb{R} \times E)$) en donde E puede identificarse con el hiperplano proyectivo definido por las rectas de $\mathbb{R} \times E$ que pasan por los puntos de la forma $(1,x)$. Para abreviar, nos referiremos a esta situación diciendo solamente: "considerando a E como parte del espacio proyectivo asociado...", etc.

-o-

10.- ANGULOS

En este parágrafo mantenemos las hipótesis y notaciones indicadas al comienzo del capítulo, pero supondremos $n = \dim(E) = 2$. No obstante, seguiremos usando la notación K en lugar de $\mathbb{R}$ porque la mayor parte de lo que digamos aquí vale para cuerpos conmutativos cualesquiera de característica diferente de 2 (si K es cualquier cuerpo conmutativo de característica diferente de 2, no tiene sentido decir que $(\ |\ )$ es positiva, pero debe seguirse suponiendo que es no degenerada).

Con (e_1,e_2) se designa una base ortonormal de E, pero para permitir la generalidad llamaremos $\alpha_1 = (e_1|e_1)$, $\alpha_2 = (e_2|e_2)$ y $\delta = -\alpha_2/\alpha_1$ (en el caso general, la base sólo se supone ortogonal, con lo que e_1 y e_2 son no isótropos y sólo puede asegurarse que α_1, α_2 son diferentes de 0; en el caso real con la suposición indicada se tiene que $\alpha_1 = \alpha_2 = 1$, y $\delta = -1$). Se notará con G la matriz de $(\ |\ )$ respecto de esta base:

$$G = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \qquad \text{y con} \quad M(u) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

la matriz del endomorfismo u tal que: $u(x) = u(x^1e_1+x^2e_2) = (ax^1+bx^2)e_1 + (cx^1+dx^2)e_2$.

Como vimos en 6.6 hay sólo dos tipos de semejanzas: las semejanzas directas, w, caracterizadas por la condición: multipl (w) = det (w) y las semejanzas inversas, que cumplen en cambio: multipl (w) = − det (w) (recordar que suponemos que la dimensión es 2).

En cuanto a las simetrías, prácticamente las hay de un sólo tipo, es decir las simetrías respecto de rectas (hiperplanos porque la dimensión es 2). Por ejemplo, la simetría respecto de la recta Ke_1 (puesto que lleva el vector de coordenadas (1,0) en (1,0) y el vector (0,1) en el opuesto (0,-1) tiene como matriz:

$$M(s_1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

En cuanto a la simetría respecto del origen: $x \longrightarrow -x$, es obvio que su matriz es:

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

de modo que también es una rotación (y por supuesto también es la homotesia de razón -1).

-o-

10.1.- PROPIEDADES DE LAS SEMEJANZAS DIRECTAS EN EL PLANO

Para realizar el estudio general de las semejanzas del plano, podemos limitarnos al subgrupo $S^+(Q)$ de las semejanzas directas. En efecto, si w es una semejanza inversa y s_1 la simetría respecto de Ke_1, es claro que ws_1 es una semejanza directa (con el mismo multiplicador que w) y, recíprocamente, si w es una semejanza directa, ws_1 es una semejanza inversa con el mismo multiplicador que w. (Es obvio que esta propiedad no es privativa de s_1: dejamos al lector la sencilla tarea de encontrar relaciones generales entre semejanzas directas e inversas.)

-o-

Sea Ψ una forma bilineal alternada y no degenerada sobre E (es decir, una forma bilineal tal que $\Psi(x,x) = 0$ para cada $x \in E$, lo que implica $\Psi(x,y) = -\Psi(y,x)$ para todo x y para todo y en E, cf. capítulo 5). Por el corolario del teorema 1, § 1, por ser Ψ no degenerada, fijado $y \in E$, para cada $x \in E$ existe un único elemento $w(x) \in E$ tal que $(x|y) = \Psi(w(x), y)$, y esa relación permite deducir que $w : x \longrightarrow w(x)$ es un endomorfismo de E.

Antes de proseguir, debemos llamar la atención sobre la siguiente propiedad de las formas alternadas en dimensión 2: cualquiera sea el endomorfismo u de E se cumple que: $\Psi(u(x), u(y)) = \det(u).\Psi(x,y)$ $(\forall x, \forall y) \in E)$. En efecto, si la matriz de u es $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ sabemos que $u(x) = u(x^1e_1+x^2e_2) = (ax^1+bx^2)e_1 + (cx^1+dx^2)e_2$, y entonces, usando las propiedades de Ψ tenemos:

$$\Psi(u(x), u(y)) = (ax^1+bx^2)(cy^1+dy^2) - (ay^1+by^2)(cx^1+dx^2)\,\Psi(e_1,e_2) =$$

$$= (ad-bc)(x^1y^2-x^2y^1)\,\Psi(e_1,e_2) = \det(u)\,\Psi(x,y)$$

Entonces volviendo a lo de antes, si u es una semejanza directa podemos escribir:

$$\det(u)\,(x|y) = (u(x)|u(y)) = \Psi(wu(x), u(y)) = \Psi(uu^{-1}wu(x), u(y)) =$$

$$= \det(u)\,\Psi(u^{-1}wu(x), y)$$

y como, por la definición de w, $\det(u)(x|y) = \det(u).\Psi(w(x),y)$, esas relaciones y el hecho de que Ψ es no degenerada implican

$$w = u^{-1}wu \quad \text{es decir:} \quad wu = uw$$

Como Ψ todavía está indeterminada, tomemos en particular la forma alternada cuya matriz es: $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, y calculemos la matriz del endomorfismo w correspondiente: $M(w) = (a_{ij})$. Introduciendo coordenadas, la relación $(x|y) = \Psi(w(x), y)$ se escribe:

$$(x^1e_1+x^2e_2 \mid y^1e_1+y^2e_2) = x^1y^1\alpha_1 + x^2y^2\alpha_2 =$$

$$= ((a_{11}x^1+a_{12}x^2)e_1 + (a_{21}x^1+a_{22}x^2)e_2,\ y^1e_1+y^2e_2),$$

es decir, usando la matriz de :

$$x^1y^1\alpha_1 + x^2y^2\alpha_2 = (a_{11}x^1+a_{12}x^2)y^2 - (a_{21}x^1+a_{22}x^2)y^1$$

Entonces, desarrollando el polinomio de la izquierda y teniendo en cuenta que los polinomios de ambos miembros deben ser idénticos (porque la relación inicial vale para todo x y para todo y en E) se deduce en seguida: $a_{11} = a_{22} = 0$, $a_{12} = \alpha_2$, $a_{21} = -\alpha_1$, es decir que:

$$M(w) = \begin{pmatrix} 0 & \alpha_2 \\ -\alpha_1 & 0 \end{pmatrix}$$

de donde, la relación ya establecida $wu = uw$ es equivalente a :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & \alpha_2 \\ -\alpha_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha_2 \\ -\alpha_1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

que implica, efectuando las operaciones e identificando los elementos correspondientes: $c\alpha_2 = -\alpha_1 b$, $-\alpha_1 a = -\alpha_1 d$, $d\alpha_2 = a\alpha_2$, $-\alpha_1 b = c\alpha_2$, es decir : $a = d$, $b = \delta c$.

Así se ha probado que <u>si</u> u <u>es una semejanza directa</u>, <u>su matriz es necesariamente de la forma</u>

$$M(u) = \begin{pmatrix} a & \delta b \\ b & a \end{pmatrix} \qquad (a^2 - \delta b^2 \neq 0)$$

(lo último debido a que u es un automorfismo y por lo tanto su determinante es diferente de 0) .

Se ve, por otra parte, inmediatamente que la suma y el producto de matrices de la forma

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \qquad .$$

es otra matriz de esa forma (aunque eventualmente podría tener determinante nulo), y lo mismo ocurre cuando se multiplica por un escalar. Esto significa que <u>dichas matrices forman un álgebra</u>, A , que es subálgebra de $\mathcal{L}(E)$, que es un álgebra conmutativa pues como K es conmutativo basta calcular para ver que:

$$\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}\begin{pmatrix} a' & \delta b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} a' & \delta b' \\ b' & a' \end{pmatrix}\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$$

Ahora bien, si se designa con v el elemento de A : $v = \frac{1}{-\alpha_1}.w$ (cuya matriz es $\left(\begin{smallmatrix} 0 & \delta \\ 1 & 0 \end{smallmatrix}\right)$) y si se representa con 1 a la identidad de E , se ve que: para cada $u \in A$ vale una expresión de la forma:

$$u = a.1 + b.v \quad (v^2 = \delta.1) \qquad \text{(siendo } M(u) = \begin{pmatrix} a & \delta b \\ b & a \end{pmatrix} \text{)} \quad .$$

Entonces, como tanto 1 como v son semejanzas directas, esto prueba que A <u>es la subálgebra de</u> $\mathcal{L}(E)$ <u>engendrada por las semejanzas directas</u>. Además, esa misma expresión demuestra que A es una <u>extensión cuadrática de</u> K generada por v y la unidad de A . Aplicando entonces a A la teoría general (ver la parte correspon-

diente de la introducción) tenemos los resultados siguientes:

Si δ es un cuadrado, es decir si $\delta = \gamma^2$ $(\gamma \in K)$, A es compuesto directo de dos cuerpos isomorfos a K . (Es útil observar aquí que este caso se presenta si y sólo si E contiene vectores isótropos pues la ecuación

$$(x^1 e_1 + x^2 e_2 \mid x^1 e_1 + x^2 e_2) = 0 \quad \text{es equivalente a} \quad \delta = \left(\frac{x^1}{x^2}\right)^2$$

Esto dice además que si hay rectas isótropos éstas son necesariamente dos, y que todos los vectores isótropos están dados por la expresión $\lambda e_1 \pm \frac{1}{\gamma} \lambda e_2$ (variando λ) .)

En cambio, si δ no es un cuadrado en K , A es un cuerpo, Este es el caso que nos interesa porque como hemos supuesto $K = \mathcal{R}$ y (|) positiva no degenerada, sabemos que no hay en E vectores isótropos. Más precisamente, sabemos que con nuestras hipótesis es $\delta = -1$, que no puede ser un cuadrado de un número real.Eso mismo implica que en nuestro caso A es igual al conjunto de las semejanzas directas porque el determinante de una aplicación perteneciente a A es de la forma $a^2 - \delta b^2$, es decir es, con nuestras hipótesis, igual a $a^2+b^2 > 0$ (exceptuándose, por supuesto, la aplicación nula).

Usaremos la notación general de las extensiones cuadráticas:

$$\text{si} \quad u = a + bv \quad , \quad \bar{u} = a - bv \quad y \quad N(u) = u\bar{u} = a^2 - \delta b^2 = \det(u)$$

Realicemos una última observación, dado $x \in E$ no isótropo (lo que permite tomarlo como primer vector de una base ortogonal) la igualdad:

$$\begin{pmatrix} y^1 & \delta y^2 \\ y^2 & y^1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} y^1 \\ y^2 \end{pmatrix}$$

prueba que para cada $y \in E$ existe un elemento u de A (que en el caso real que nos interesa será una semejanza directa) tal que $u(e_1) = y$. En general entonces para cada x no isótropo y para cada $y \in E$ existe una única aplicación $u \in A$ tal que $u(x) = y$.

En resumen, hemos demostrado lo siguiente:

Teorema fundamental:

La subálgebra A de $\mathcal{L}(E)$ engendrada por $S^+(Q)$ es una extensión cuadrática de K . Si E no tiene vectores isótropos, A es un cuerpo; en caso contrario , es compuesto directo de dos cuerpos isomorfos a K . $u \in A$ si y sólo si su matriz es de la forma:

$$M(u) = \begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$$

y $u \in S^+(Q)$ si y sólo si además es $a^2 - \delta b^2 \neq 0$. Si E se considera como A-módulo respecto del producto por escalares: $u.x = u(x)$ $(u \in A)$ entonces el A-módulo E es engendrado por cualquier elemento $x \in E$ no isótropo, es decir el conjunto $\{u.x\} = \{u(x)\}$ es igual a E . Si además se introducen las hipótesis de un principio ($K = \mathbb{R}$, $(x|y)$ positiva y no degenerada) A es un cuerpo que coincide con $S^+(Q)$ si se le priva de la aplicación nula , (de hecho, como se verá, A es isomorfo a C).

Consecuencias:

(1) Para que un elemento u de A , $u = a + bv$ sea una homotesia es necesario y suficiente que sea $b = 0$ pero $a \neq 0$

(2) Los elementos de A con $a = 0$ pero $b \neq 0$ (es decir los $u = bv$) transforman cada vector $x = x^1 e_1 + x^2 e_2$ en un vector ortogonal a x , es decir: $(x \mid bv(x)) = 0$ $(\forall x \in E)$. En efecto, recordando cuál es la matriz que define a v , tenemos que: $v(x) = \delta x^2 e_1 + x^1 e_2$, y entonces: $(v(x) \mid x) = (\delta x^2 e_1 + x^1 e_2 \mid x^1 e_1 + x^2 e_2) = \delta x^2 x^1 \alpha_1 + x^1 x^2 \alpha_2 = 0$ en virtud de la definición de δ .

Recíprocamente, si un endomorfismo $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tiene la propiedad de transformar cada x en un vector ortogonal a x , entonces u es de la forma $u = cv$. En efecto, la relación $(x \mid u(x)) = 0$ se escribe, pasando a coordenadas: $(ax^1 + bx^2)x^1 \alpha_1 + (cx^1 + dx^2)x^2 \alpha_2 = 0$ (para todo par de valores x^1, x^2). Entonces haciendo primero $x^1 = 0$, $x^2 = 1$ y luego $x^2 = 0$, $x^1 = 1$, se deduce $a = d = 0$, y esto a su vez implica que la relación supuesta es de la forma: $x^1 x^2 (b\alpha_1 + c\alpha_2) = 0$, lo que lleva a $b/c = -\alpha_2/\alpha_1 = \delta$, es decir que:

$$u = \begin{pmatrix} 0 & \delta c \\ c & 0 \end{pmatrix} = cv \quad , \qquad \text{l.q.d.d.}$$

(3) Si u es una semejanza directa, para que u^2 sea una homotecia es necesario y suficiente que o bien u sea una homotecia, o bien u sea un automorfismo que transforma cada vector de E en un vector ortogonal a él (es decir: $u = a + bv$ $(a^2 - \delta b^2 \neq 0)$ es tal que u^2 es una homotecia si y sólo a ó b son nulos, pero no ambos). En efecto: $u^2 = (a^2 + \delta b^2) + 2abv$ es una homotecia si y sólo si $ab = 0$, es decir si y sólo si ó a ó b son nulos (pero no ambos).

(4) Si u es un endomorfismo de A , se verifica mediante cálculo directo que $(u(x) \mid y) = (x \mid \bar{u}(y))$, $(\forall x, \forall y \in E)$, lo que significa que todos los elementos de A verifican la condición: $u^{\#} = \bar{u}$.

(5) Ya hemos visto que u es una semejanza inversa si y sólo si es de la forma we_1 , donde $w \in S^+(Q)$ y s_1 es la simetría respecto de Ke_1 . Como ahora conocemos la forma de las matrices de las semejanzas directas, y como conocemos la matriz de s_1 , podemos escribir la condición necesaria y suficiente

para que u sea una semejanza inversa diciendo que su matriz debe ser de la forma:

$$\begin{pmatrix} a & -\delta b \\ b & -a \end{pmatrix} \qquad (a^2 - \delta b^2 \neq 0)$$

(6) El grupo S^+ es conmutativo (porque $S^+ \subset A$). Si x e y son no isótropos existe un $u \in S^+$ tal que $u(x) = y$. En efecto, según el teorema el conjunto de los $u(x)$ es igual a E (al dejar x fijo y hacer variar u en A), de modo que existe un u en A tal que $u(x) = y$, y este u es único. Si $x = \lambda y$, u es la homotecia de razón λ, y por tanto es una semejanza directa; si x e y son linealmente independientes, podemos considerar(del mismo modo) la única aplicación de A, u', tal que $u'(y) = x$, de modo que se tiene: $u'u(x) = x$, $uu'(y) = y$, lo cual implica que $uu' = u'u = 1$, es decir que u es inversible y por consiguiente también u pertenece a S^+.

Esto prueba, en particular, que dadas dos rectas no isótropas, R y R', existe una semejanza directa u tal que $u(R) = R'$, y es claro que toda semejanza de la forma au ($a \in K$) tiene la misma propiedad (si $a \neq 0$). Entonces es inmediato que si se consideran las clases de semejanzas directas que sólo difieren en el producto por una homotecia, es decir los elementos de S^+/H (H = grupo de las homotecias), entonces dadas R y R' como antes, siempre existe un único elemento de S^+/H tal que cualquiera de sus semejanzas lleva R sobre R'. De hecho el grupo S^+/H puede considerarse operando sobre las rectas de E y escribiremos $\psi(R) = R'$ (para $\psi \in S^+/H$) cuando cualquier semejanza u de la clase ψ verifica $u(R) = R'$.

(7) ϕ^+ es un grupo conmutativo (porque está contenido en S^+). Si x e y son vectores no isótropos de la misma longitud, existe una rotación u y una sola tal que $u(x) = y$. En efecto, sabemos que hay una única semejanza directa tal que $u(x) = y$, y entonces la relación supuesta: $(x|x) = (y|y)$ dice que u tiene multiplicador 1, es decir u es una rotación.

Utilicemos ahora nuestras hipótesis restrictivas: $K \neq \mathbb{R}$, y $(x|y)$ es positiva y no degenerada. En este caso, dadas dos semirrectas no isótropas R y R', existe una rotación única, u, tal que $u(R) = R'$. En efecto, como $(x|x)$ es un cuadrado para todo x, siempre se pueden encontrar (mediante multiplicación por escalares apropiados) dos vectores x, y de R, R', respectivamente, que tengan la misma longitud, por ejemplo tales que: $(x|x) = (y|y) = 1$. Entonces la rotación u tal que $u(x) = y$ lleva R sobre R'. La unicidad resulta de que por el teorema hay una única aplicación de A que lleva x en y.

(8) Como el grupo ortogonal es un subgrupo (distinguido) del de las semejanzas,

si s es una transformación ortogonal de determinante igual a -1, s es una semejanza inversa. Por lo tanto debe verificar:

$$s = \begin{pmatrix} a & -\delta b \\ b & -a \end{pmatrix} \qquad -a^2 + \delta b^2 = -1$$

y esas condiciones implican (haciendo el cálculo) que $s^2 = 1$, es decir que s es una simetría. De otro modo: para que s sea una simetría, es necesario y suficiente que $\det(s) = -1$ (siempre que se suponga que s es una transformación ortogonal). Así, en el plano, se da el caso excepcional de que sólo hay dos tipos de transformacinnes ortogonales: las de determinante 1 son las rotaciones, las de determinante -1 son las simetrías (respecto de rectas) (cf. Ap. IV, Cor. 1 del teorema 4). Si σ es una simetría respecto de una recta no isótropa R, es cómodo decir que R es el <u>eje</u> de la simetría s. Evidentemente, cualquiera sea $x \in E$, el eje de s es la recta determinada por el vector $\frac{s(x)+x}{2}$ (cf.: 8.5).

Si x e y son vectores no isótropos de la misma longitud, hay una simetría única, s, tal que $s(x) = y$ (y, por supuesto, también: $s(y) = x$). Si tal simetría existe, es única y tiene como eje la recta determinada por $\frac{x+y}{2}$ porque $s(\frac{x+y}{2}) = \frac{s(x) + s(y)}{2}$ tiene que ser igual a $\frac{s(x) + s(y)}{2} = \frac{y+x}{2}$. Y efectivamente (verificación directa) la simetría cuyo eje pasa por $\frac{x+y}{2}$ tiene esa propiedad. (En el lenguaje clásico esto se expresaba diciendo que las diagonales de un rombo son ejes de simetría del mismo, o que la bisectriz de un triángulo isósceles es eje de simetría del triángulo.) El razonamiento anterior no es aplicable si $x = -y$, pero en este caso se comprueba directamente que la simetría cuyo eje es la recta ortogonal a la de x e y resuelve la cuestión.

Veamos ahora cómo se comporta una simetría con relación a los vectores isótropos (si existen). En virtud de lo que ya sabemos sobre las matrices de las simetrías y las coordenadas de los vectores isótropos, basta considerar:

$$\begin{pmatrix} a & -\delta b \\ b & -a \end{pmatrix} \begin{pmatrix} \lambda \\ \pm\frac{\lambda}{\gamma} \end{pmatrix} = \begin{pmatrix} a\lambda \mp b\gamma \\ \pm\frac{1}{\gamma}(a\lambda \mp b\gamma) \end{pmatrix} = \begin{pmatrix} a\lambda \mp b\gamma \\ \mp\frac{1}{\gamma}(a\lambda \mp a\lambda) \end{pmatrix}$$

lo que prueba que s lleva una de las rectas isótropas sobre la otra.

(9) Sea ahora $u = a+bv$ $(a^2 - \delta b^2 = 1)$ una rotación, y s una simetría. Entonces sus^{-1} (rotación conjugada de u) es justamente la rotación inversa: $sus^{-1} = u^{-1}$. Para demostrarlo, podemos (cambiando la base de E si es necesario) suponer que s es la simetría s_1 respecto de Ke_1, y entonces $M(s_1) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ implica que:

$$M(sus^{-1}) = \begin{pmatrix} a & -\delta b \\ -b & a \end{pmatrix} \quad \text{de donde:} \quad M(sus^{-1}u) = \begin{pmatrix} a & -\delta b \\ -b & a \end{pmatrix}\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

-o-

IO.2.- TRIGONOMETRIA PLANA

Como veremos luego, los ángulos de semirrectas se corresponden de modo natural con las rotaciones, en tanto que los ángulos de rectas se corresponden con las clases de semejanzas directas proporcionales de S^+/H . Si no se introduce en el plano una orientación, no es posible definir unívocamente las funciones trigonométricas que dependen de la base elegida en el álgebra A . No obstante, nos limitaremos a este caso (por simplicidad) construyendo una trigonometría que depende esencialmente de nuestro generador v de A . (Para el estudio de la trigonometría propiamente dicha, enviamos al lector al apéndice I).

Fijamos de una vez para siempre el elemento $v \in A$, $v^2 = \delta \in H$ (H = grupo de las homotecias, que se identifica con $K^{\#}$ en la extensión cuadrática A) que junto con la identidad 1 genera el álgebra A .

Hecho esto, a cada aplicación u S^+ se la puede escribir de modo único en la forma $u = a+bv$. Como los escalares a y b dependen de u , usaremos la notación: $u = c(u) + s(u) \cdot v$. Como veremos luego, $c(u)$ y $s(u)$ son, respectivamente, proporcionales al coseno y al seno de uno de los ángulos que forman dos semirrectas R , R' tales que $u(R) = R'$. Sea $\varphi \in S^+/H$. Entonces es claro que si u , $u' \in \varphi$, se verifica que $c(u)$, $s(u)$, son proporcionales a $c(u')$, $s(u')$. Conviene para lo que sigue considerar A como espacio vectorial de dimensión 2 con base $(1,v)$ y considerar el espacio proyectivo deducido, $P(A)$, que es isomorfo a $\tilde{K}$. Las rectas del espacio A son justamente las clases de S^+/H (semejanzas proporcionales) y por tanto éstas están también en isomorfismo con $\tilde{K}$. Este isomorfismo es justamente el que hace corresponder a cada $\varphi \in S^+/H$ las clases de pares proporcionales $\{\lambda s(u), \lambda c(u)\}$ (coordenadas homogéneas de φ) . Es cómodo representar estos elementos de K mediante $t(u) = \frac{s(u)}{c(u)}$ (siendo $u \in \varphi$) entendiéndose que cuando $c(u) = 0$, $t(\varphi)$ es el punto del infinito $t(\varphi) = \infty \in \tilde{K}$. La función $t(\varphi)$ es entonces una biyección de S^+/H sobre K que se denomina función tangente. Se dice que $t(\varphi)$ es la tangente de .

De acuerdo con la definición, si $t(\varphi) \neq \infty$ un elemento de φ es la semejanza $1 + t(\varphi)\, v$. Si $t(\varphi') \neq \infty$ también $1 + t(\varphi')\, v \in \varphi'$. Calculemos la semejanza producto:

$$1 + t(\varphi)v \quad 1 + t(\varphi')v = 1 + \delta\, t(\varphi)\, t(\varphi') + (t(\varphi)+t(\varphi'))\, v$$

Si notamos el grupo S^+/H aditivamente (cosa que se justifica porque es conmutativo) esa relación nos permite afirmar que la tangente de $+$ ' es :

$$t(\varphi+\varphi') = \frac{t(\varphi) + t(\varphi')}{1 + \delta\, t(\varphi)\, t(\varphi')} \qquad (\#)$$

que es un auténtico "cociente" si $1 + \delta\, t(\varphi)\, t(\varphi') \neq 0$.

Sean θ , θ' dos rotaciones. Razonando en la misma forma anterior, si se nota el grupo conmutativo $\phi^+(Q)$ aditivamente se tiene:

$$\begin{aligned} c(\theta+\theta') &= c(\theta)\,c(\theta') + \delta s(\theta)s(\theta') \\ s(\theta+\theta') &= s(\theta)\,c(\theta') + c(\theta)\,s(\theta') \end{aligned} \qquad (\#\#)$$

y la condición de que $\det(\theta) = 1$ se escribe:

$$c(\theta)^2 - \delta s(\theta)^2 = 1 \qquad (\#\#\#)$$

Usando que si $u = a + bv$ entonces su matriz es

$$M(u) = \begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$$

se tiene que

$$M(\theta) = \begin{pmatrix} c(\theta) & \delta s(\theta) \\ s(\theta) & c(\theta) \end{pmatrix} \qquad (\#\#\#\#)$$

En el caso que nos interesa, $K = \mathbb{R}$ y $(\ |\ )$ es positiva no degenerada, y si (e_1, e_2) es ortonormal, en las fórmulas anteriores hay que poner -1 en lugar de δ.

-o-

Antes de pasar a la definición de los ángulos, es conveniente que mencionemos las dos relaciones fundamentales que ligan los grupos S^+/H y ϕ^+ .

La primera es el homomorfismo canónico, i , de ϕ^+ en S^+/H . Esto significa lo siguiente: como $\phi^+ \subset S^+$, a cada rotación θ le corresponde la clase (única) de semejanzas de S^+/H a la cual θ pertenece, esa clase es $i(\theta)$, y es claro que $i : \theta \longrightarrow i(\theta)$ (pensada como aplicación de S^+ en S^+/H) es el homomorfismo natural que existe entre un grupo y su cociente por un subgrupo distinguido. (Si se piensa como antes a A como espacio vectorial de base $(1,v)$ provisto de la forma cuadrática $N(u) = a^2 - \delta b^2$ que en el caso real que nos interesa es positiva y no degenerada, S^+/H es el conjunto de las rectas de A , y el grupo de las rotaciones está formado por los puntos del "círculo unitario": $a^2 - \delta b^2 = 1$; si θ es un punto de este círculo, la clase de semejanzas que determina en S^+/H está representada por la recta que pasa por θ , de modo que i puede interpretarse como la aplicación que a cada punto del círculo unitario hace corresponder la recta que pasa por él). Las únicas rotaciones que son también homotecias son las aplicaciones 1 y -1, es decir $\phi^+ \cap H = \{1,-1\}$ y por consiguiente, el núcleo del homomorfismo i de ϕ^+ en S^+/H es precisamente el subgrupo distinguido $\{1,-1\}$ de ϕ^+ . Por las propiedades generales del cociente, sabemos que $\phi^+/\{1,-1\}$ es isomorfo a la imagen $i(\phi^+)$ S^+ (con la imagen de antes, esto significa que el conjunto de las rectas de A que cortan el círculo unitario está en correspondencia biunívoca que los pares de pun

tos del círculo unitario (rotaciones) situados en semirrectas opuestas, ya que si es una rotación, su clase en el cociente $\phi^+/\{1,-1\}$ es el conjunto $\{\theta,-\theta\}$).

(Usando aquí otra vez la notación multiplicativa para evitar confusiones con la notación de un principio) demostremos que la aplicación $u \longrightarrow \frac{u}{\bar{u}} = \frac{u^2}{N(u)}$ es un endomorfismo de S^+ . En efecto, basta ver que: $\overline{uv} = \bar{u}.\bar{v}$. El núcleo de este endomorfismo es, por definición, el conjunto de las semejanzas directas u tales que $\frac{u}{\bar{u}} = \frac{u^2}{N(u)} = 1$, es decir las semejanzas u tales que $u = \bar{u}$, que, por la definición de conjugado en una extensión cuadrática, resulta ser justamente el conjunto de las homotecias, H . Entonces la aplicación que a cada $\varphi \in S^+/H$ hace corresponder la aplicación $u/\bar{u}$ (donde u es cualquier semejanza directa perteneciente a la clase φ) es un isomorfismo entre el grupo S^+/H y el subgrupo imagen en S^+ , isomorfismo que representaremos con d . Decimos que, más precisamente, d <u>es un isomorfismo de</u> S^+/H <u>sobre</u> ϕ^+ . Para demostrar esto hay que probar dos cosas: que cada aplicación de la forma $u/\bar{u}$ es una rotación y que si θ es una rotación siempre existe una $u \in S^+$ tal que $\theta = u/\bar{u}$. Lo primero es inmediato si recordamos que las rotaciones son los elementos de A de norma igual a 1 :

$$N\left(\frac{u}{\bar{u}}\right) = N\left(\frac{u^2}{N(u)}\right) = \left(\frac{1}{N(u)}\right)^2 . N(u^2) = \frac{N(u)^2}{N(u)^2} = 1$$

Para probar lo segundo, distinguiremos dos casos: supongamos primero que la aplicación $1+\theta$ de A es inversible (insistimos en que aquí la suma es la suma del espacio vectorial A). Entonces, si ponemos $u = 1 + \theta$, tenemos: $\theta\,\bar{u} = \theta(\overline{1+\theta}) = \theta + \theta\bar{\theta} = \theta + 1 = u$, lo que prueba que $\theta = u/\bar{u}$. En cambio, veamos qué ocurre si $1+\theta$ no es inversible, es decir si $N(1+\theta) = 0$ ó $(1+\theta)(1+\bar{\theta}) = 0$. Si introducimos "coordenadas": $\theta = a + bv$, esa relación implica $2(1+a) = 0$, y usando que $a^2 - b^2 = 1$, se deduce que tiene que ser $a = -1$, y $b = 0$, o sea que la única rotación θ tal que $1+\theta$ no es inversible, es $\theta = -1$. Pero entonces, como nuestro generador v cumple que $v/\bar{v} = -1$, resulta que también en este caso se puede expresar a θ en la forma pedida: $\theta = -1 = v/\bar{v}$, y la afirmación está demostrada.

-o-

Puesto que i es una aplicación de ϕ^+ en S^+/H , y como d es una aplicación de S^+/H sobre ϕ^+ , el homomorfismo producto: $d \cdot i$ es un endomorfismo de ϕ^+ , en tanto que el otro producto: $i \cdot d$ es un endomorfismo de S^+/H . Si volvemos ahora a notar aditivamente estos grupos, podemos mostrar, con más precisión, que valen las fórmulas:

$$i.d(\varphi) = \varphi + \varphi = 2\varphi \qquad (\varphi \in S^+/H)$$

$$d.i(\theta) = \theta + \theta = 2\theta \qquad (\theta \in \phi^+)$$

Ya vimos en la consecuencia (4) del teorema fundamental de 10.1 que en general se

cumple $\theta = \theta^*$, de modo que si $\theta \in \phi^+(Q)$, siendo su adjunto igual a su inverso , concluímos que $\bar{\theta} = \theta^{-1}$ (hecho que ya fué usado en el razonamiento anterior), de manera que en la notación aditiva de ϕ^+ debemos escribir: $\bar{\theta} = -\theta$. Por definición, $i(\theta)$ es la clase de semejanzas que contiene a θ , y entonces para determinar la rotación $d(i(\theta))$ hay que tomar un elemento de esta clase, por ejemplo el propio θ y escribir $\theta/\bar{\theta}$, que, en notación aditiva, es igual a $\theta - (-\theta) = \theta + \theta = 2\theta$. Esto prueba la segunda fórmula. En segundo lugar, si $\varphi \in S^+/H$, sea $u \in \varphi$; entonces por definición, $d(\varphi)$ es, $\frac{u^2}{N(u)}$ y la clase de semejanzas $i(d(\varphi))$ que corresponde a esta aplicación es la misma que la que corresponde a u^2 que es justamente la clase $\varphi + \varphi = 2\varphi$, l.q.q.d.

-o-

Veamos qué consecuencias tienen aquellas relaciones desde el punto de vista de la trigonometría. Sea $\varphi \in S^+/H$, tal que $t(\varphi) = t \neq \infty$. Sabemos que una semejanza de la clase φ es precisamente $1 + t(\varphi)v = 1 + tv$, y la rotación $d(\varphi)$ es entonces: $(1+tv)^2/N(1+tv)$. Como $N(1+tv) = 1 - \delta t^2$, si se calculan las coordenadas de la rotación $d(\varphi)$ respecto de la base $(1,v)$ se tiene:

$$s(s(\varphi)) = \frac{2t}{1-\delta t^2} \qquad c(d(\varphi)) = \frac{1+\delta t^2}{1-\delta t^2}$$

Si aplicamos esa fórmula al caso en que θ es una rotación tal que la tangente de la clase $i(\theta)$, t , no es infinita, y recordando que $d(i\theta) = 2\theta$, tenemos:

$$s(2\theta) = \frac{2t}{1-\delta t^2} \qquad c(2\theta) = \frac{1+\delta t^2}{1-\delta t^2}$$

Análogamente, para cada clase $\varphi \in S^+/H$ cuya tangente, t , no sea infinita y además verifique: $1 + \delta t^2 \neq 0$, vale la expresión:

$$t(2\varphi) = \frac{2t}{1+\delta t^2}$$

En efecto, para cada $\varphi \in S^+/H$, $d(\varphi)$ es una rotación, θ , tal que la clase de semejanzas $i(2\theta)$ de 2θ es 2φ , entonces basta aplicar la fórmula precedente y la definición de la función tangente.

-o-

10.3.- ANGULOS (EN EL PLANO)

Recién en este número haremos efectivas nuestras hipótesis de que K es el cuerpo $\mathbb{R}$ de los números reales, $(\ |\ )$ una forma positiva no degenerada sobre E , (e_1, e_2) una base ortonormal, etc., con lo cual usaremos los resultados anteriores aplicados a este caso ($\delta = -1$, etc.) .

-o-

Consideremos los pares ordenados de rectas: (R_1,R_2) del espacio E, y definamos la relación $(R_1,R_2) \sim (R'_1,R'_2)$ cuando y sólo cuando existe una semejanza directa u tal que $u(R_1) = R'_1$ y $u(R_2) = R'_2$. Es claro que esta relación es una relación de equivalencia: por definición, la clase de equivalencia (para $\sim$) del par (R_1,R_2) se llama el ángulo que forma la recta R_1 con la recta R_2, y se representa con $(\widehat{R_1,R_2})$.

Se tiene la propiedad fundamental siguiente: si $(\widehat{R_1,R_2}) = (\widehat{R'_1,R'_2})$ entonces también $(\widehat{R_1,R'_1}) = (\widehat{R_2,R'_2})$. En efecto, la hipótesis significa que hay una semejanza directa u tal que $u(R_1) = R'_1$ y $u(R_2) = R'_2$, y la tesis es que existe una semejanza directa u' tal que $u'(R_1) = R'_1$ y $u'(R_2) = R'_2$. Eso se demuestra así: según la consecuencia (6) del teorema fundamental de 10.1, existe u' tal que $u'(R_1) = R'_1$, y S^+ es conmutativo, de modo que: $u'(R_2) = u'u(R_1) = uu'(R_1) = u(R'_1) = R'_2$, l.q.q.d. Resulta de ello que la condición necesaria y suficiente para que $(\widehat{R_1,R_2}) = (\widehat{R'_1,R'_2})$ es que exista una semejanza directa que superponga por una parte R_1 con R_2, y por otra, R'_1 con R'_2 (y en ese caso tal semejanza superpone en la misma forma los lados de cualquier ángulo igual a ellos). Entonces, si se hace corresponder a cada ángulo $(\widehat{R_1,R_2})$ la clase de S^+/H formada por las semejanzas directas tales que llevan R_1 sobre R_2, esta correspondencia es evidentemente una biyección entre el conjunto de los ángulos de rectas, que llamaremos $\mathcal{A}_0$, y el conjunto de las clases de semejanzas, S^+/H. Usaremos la notación $\hat{\varphi}$ para designar el ángulo que así queda asociado a la clase $\varphi \in S^+/H$, y que se llamará el ángulo de las semejanzas de φ. Esa biyección nos permite "transportar" al conjunto $\mathcal{A}_0$ la estructura de grupo abeliano de S^+/H (un ángulo es la suma de otros dos cuando su semejanza es la suma de las que corresponden a éstos, etc.). Así $\mathcal{A}_0$ es un grupo (grupo de los ángulos de rectas) isomorfo al grupo S^+/H, y valen evidentemente las fórmulas:

$$(\widehat{R,R'}) = (\widehat{R,R''}) + (\widehat{R'',R'}) \qquad \text{(fórmula de Chasles)}$$

(cualesquiera sean las tres rectas R, R', R'') y, en particular:

$$(\widehat{R,R}) = 0$$
$$(\widehat{R,R'}) = -(\widehat{R',R})$$

Según la consecuencia (2) del teorema fundamental, todos los pares de rectas ortogonales definen un ángulo (que por lo anterior es igual a su opuesto, es decir es un elemento de $\mathcal{A}_0$ de orden 2) que se llama ángulo recto. Otro modo de ver que el ángulo recto es de orden dos, consiste en observar que una de las semejanzas de ángulo recto es precisamente la v, cuyo cuadrado es una homotecia, y por tanto v^2 define el ángulo nulo. Eso dice justamente que el ángulo definido por v cumple: "recto" + "recto" = 0.

-o-

Todo lo que acabamos de hacer para rectas puede repetirse para semirrectas en la forma siguiente:

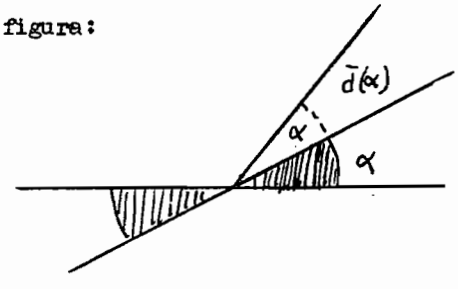
Si R_1, R_2, R'_1, R'_2 son semirrectas, definiemos $(R_1,R_2) \sim (R'_1,R'_2)$ cuando y sólo cuando existe una rotación θ tal que $\theta(R_1) = R'_1$, $\theta(R_2) = R'_2$. Esta es una relación de equivalencia y la clase del par (R_1,R_2) se llama el ángulo que forma la semirrecta R_1 con la semirrecta R_2 y se lo representa con la notación $(\widehat{R_1,R_2})$. Igual que antes se demuestra (usando (7) en lugar de (6)) que para que $(\widehat{R_1,R_2}) = (\widehat{R'_1,R'_2})$ es necesario y suficiente que $(\widehat{R_1,R'_1}) = (\widehat{R_2,R'_2})$ y también necesario y suficiente que exista una rotación θ (que debe ser única por (7)) tal que superponga los lados de los ángulos iguales, es decir: $\theta(R_1) = R_2$ y $\theta(R'_1) = R'_2$ (y entonces θ superpone también los lados de los otros ángulos iguales a ellos). Si a cada rotación θ se le hace corresponder el ángulo $\hat{\theta}$ que forma una semirrecta R_1 con la semirrecta R_2 tales que $\theta(R_1) = R_2$, se ve que esta correspondencia es una biyección del grupo ϕ^+ sobre el conjunto $\mathcal{A}_1$ de los ángulos de semirrectas. Esta correspondencia biunívoca permite "transportar" a $\mathcal{A}_1$ la estructura de grupo abeliano de ϕ^+, de modo que tenemos también un grupo de los ángulos de semirrectas isomorfo al grupo de rotaciones, para el cual valen las relaciones:

$$(\widehat{R,R'}) = (\widehat{R,R''}) + (\widehat{R'',R'}) \qquad \text{(Chassles)}$$
$$(\widehat{R,R}) = 0$$
$$(\widehat{R,R'}) = -(\widehat{R',R})$$

La rotación -1 que lleva cada semirrecta sobre la semirrecta opuesta es involutiva, es decir $(-1)^2 = 1$ = identidad = elemento neutro del grupo de rotaciones, y por tanto el ángulo que ella define, llamado ángulo llano (ángulo que forma una semirrecta con su opuesta) es un elemento de orden 2 del grupo $\mathcal{A}_1$, es decir verifica la relación: "llano" + "llano" = 0 .

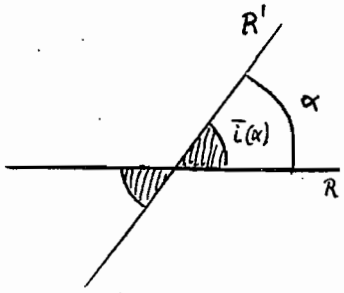
-o-

Llamemos con $\bar{d}$ al isomorfismo de $\mathcal{A}_o$ sobre $\mathcal{A}_1$ que se obtiene transportando de modo natural el isomorfismo d de S^+/H sobre ϕ^+ (es decir la imagen por $\bar{d}$ del ángulo de dos rectas que se superponen por $\varphi \in S^+/H$ es, por definición, el ángulo de dos semirrectas que se superponen por $d(\varphi) \in \phi^+$); y llamemos $\bar{i}$ el homomorfismo de $\mathcal{A}_1$ en $\mathcal{A}_o$ que se obtiene transportando de modo natural el homomorfismo i de ϕ^+ en S^+/H. Razonando sobre las aplicaciones (es decir recordando la definición de d) se ve que $\bar{d}$ opera como indica la figura:



En cuanto al homomorfismo $\bar{i}$, razonemos así: Si θ es la rotación que lleva la semirrecta R sobre la semirrecta R', todas las semejanzas proporcionales a θ es decir las de la clase $i(\varphi)$ llevan la rec-

ta que contiene a R sobre la recta que contiene a R' . Eso se expresa diciendo que si α es el ángulo de la semirrecta R con la semirrecta R' , entonces $\bar{i}(\alpha)$ es el ángulo de la recta R con la recta R' . Sabemos que con las hipótesis que hemos realizado, si se dan dos rectas y en cada una de ellas se elige una semirrecta siempre hay una rotación (única) que lleva la semirrecta de la primera recta sobre la semirrecta de la segunda. Se deduce de aquí que el ángulo de las rectas dadas proviene del ángulo de las semirrectas elegidas mediante el homomorfismo $\bar{i}$. Esto prueba que (en nuestro caso real) el homomorfismo $\bar{i}$ es suryectivo. Como ejercicio sencillo (que puede ser útil) instamos al lector a demostrar que en este caso el grupo ϕ^+ es isomorfo al grupo cociente S^+/H^+ (donde H^+ es el subgrupo de las homotecias de razón positiva).



-o-

Usando las propiedades de los homomorfismos d e i , se deduce que:

$$\bar{d}\,(\bar{i}(\alpha)) = 2\alpha \qquad \bar{i}\,(\bar{d}(\alpha)) = 2\alpha$$

y ambas aplicaciones compuestas son suryectivas. Esto prueba, en particular, que siempre existe la mitad de un ángulo de rectas o de semirrectas (cosa que puede demostrarse también sin utilizar las hipótesis tan restrictivas de $K = \mathbb{R}$, etc.).

Los isomorfismos que a una clase de semejanzas de S^+/H hacen corresponder un ángulo de rectas y que a una rotación hace corresponder un ángulo de semirrectas, permiten trasladar a los ángulos las funciones t( ) , s( ) , c( ) , que se llaman tangente, seno y coseno, respectivamente y se notan comunmente con tg , sen , cos , respectivamente. También se extiende la función tangente a ángulos de semirrectas mediante: $tg(\hat{\theta}) = \text{sen}\,(\hat{\theta}) \,/\, \cos\,(\hat{\theta})$, y se definen las funciones nuevas: $\cot\,(\hat{\theta}) = 1/tg\,(\hat{\theta})$, $\cot\,(\varphi) = 1/tg\,(\hat{\varphi})$, con valores en el cuerpo proyectivo $\tilde{\mathbb{R}}$ (funciones cotangente) . Entonces las fórmulas deducidas antes (poniendo ahora $\delta = 1$) se escriben así:

$$tg\,(\hat{\varphi} + \hat{\varphi}') = \frac{tg\,(\hat{\varphi}) + tg\,(\hat{\varphi}')}{1 - tg\,(\hat{\varphi})\,tg(\hat{\varphi}')}$$

$$tg\,(2\hat{\varphi}) = \frac{2 \cdot tg\,(\hat{\varphi})}{1 - tg\,(\hat{\varphi})^2}$$

$$\cos\,(\hat{\theta} + \hat{\theta}') = \cos\,(\hat{\theta})\cos\,(\hat{\theta}') - \text{sen}\,(\hat{\theta})\,\text{sen}\,(\hat{\theta}')$$

$$\text{sen}\,(\hat{\theta} + \hat{\theta}') = \text{sen}\,(\hat{\theta})\cos\,(\hat{\theta}') + \cos\,(\hat{\theta})\,\text{sen}\,(\hat{\theta}')$$

$$\text{sen}^2\,(\hat{\theta}) + \cos^2\,(\hat{\theta}) = 1$$

$$\cos(2\hat{\theta}) = \cos^2(\hat{\theta}) - \operatorname{sen}^2(\hat{\theta}) = \frac{1 - tg^2(\hat{\theta})}{1 + tg^2(\theta)}$$

$$\operatorname{sen}(2\hat{\theta}) = 2 \cdot \operatorname{sen}(\hat{\theta}) \cdot \cos(\hat{\theta}) = \frac{2 \cdot tg(\hat{\theta})}{1 + tg^2(\hat{\theta})}$$

$$1 + tg^2(\hat{\theta}) = \frac{1}{\cos^2(\hat{\theta})}$$

$$1 + \cot^2(\hat{\theta}) = \frac{1}{\operatorname{sen}^2(\hat{\theta})}$$

-o-

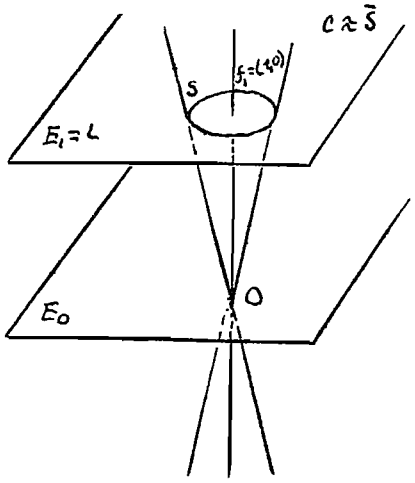
OBSERVACION IMPORTANTE: Hacemos notar que hasta aquí (es decir luego de haber hecho la teoría de ángulos y la trigonometría, que serán completadas en el apéndice I) no ha sido necesario introducir ninguna noción de medida de ángulos. Simplemente resulta que los ángulos de rectas son asimilables a las aplicaciones de S^+/H y los de demirrectas a las de ϕ^+ , de modo que los grupos de ángulos de rectas o semirrectas son isomorfos a los grupos S^+/H y ϕ^+ , y por tanto pueden tener propiedades muy diferentes de las propiedades del grupo aditivo de K . De hecho hay un ángulo de rectas privilegiado, el recto, y un ángulo privilegiado de semirrectas, el llano, que tienen la propiedad de que sumados consigo mismos dan 0 . Si K es, como siempre se ha supuesto, de característica diferente de 2 , ningún elemento del grupo aditivo de K (salvo el 0) puede tener esa propiedad. Además, y es importante, no tiene ningún sentido geométrico el considerar los "ángulos descritos" por semirrectas que dan "una o más" vueltas alrededor de su origen. La rotación que superpone una semi - rrecta consigo misma es única y es la rotación nula. El ángulo que forma una semi - rrecta consigo mismo es único y es el ángulo 0 . Es absurdo "dotar" a una semirrecta que "da vueltas" de memoria para que se pueda saber cuántas vueltas ha dado para describir un ángulo y distinguir así (para dos semirrectas superpuestas) los ángulos 0 , 2π , 4π , etc. Estos ángulos (y otros análogos) no existen.

Lo que sí existe es un homomorfismo entre el grupo aditivo de K y el grupo aditivo de los ángulos (de semirrectas, por ejemplos) que en el caso clásico es el conocido $\alpha \longrightarrow e^{i\alpha}$, pero esta es una cuestión totalmente extraña a la geometría: un tal homomorfismo puede muy bien no existir si no se imponen ciertas restricciones al cuerpo K . Decimos esto sin pretender disminuir la importancia del homomorfismo $\alpha \longrightarrow e^{i\alpha}$ de $\mathcal{R}$ sobre el grupo de rotaciones, que da nada menos que los caracteres del grupo localmente compacto y conmutativo $\mathcal{R}$, de importancia fundamental en el Análisis Moderno.

§11.- CUADRICAS Y ESFERAS

11.1.- CUADRICAS PROYECTIVAS Y AFINES

Sea $\dim(E) \geq 3$, y sea C una forma cuadrática sobre E y $\emptyset$ su forma bilineal simétrica asociada. El conjunto $\mathcal{C} = \{x \in E \,/\, C(x) = 0\}$ (#) se llama cono isótropo de ecuación $C(x) = 0$ (nótese que si $x \in \mathcal{C}$, entonces la recta $\mathbb{R}x \subset \mathcal{C}$, y de ahí la denominación de cono: el vértice del cono es el punto 0). Sabemos que las rectas (privadas de 0) de E pueden asimilarse a puntos de un espacio proyectivo de dimensión $n-1$: $P(E) = P$. La imagen canónica del cono $\mathcal{C}$ en el espacio P (es decir el conjunto de las rectas privadas de 0 de $\mathcal{C}$) se denomina cuádrica proyectiva $\bar{S}$, de ecuación homogénea $C(x) = 0$ (##) (esto porque las coordenadas de un punto x de E son coordenadas homogéneas del punto proyectivo correspondiente $\bar{x}$ en P , y la ecuación $C(x) = 0$ es, por ejemplo si la base es ortogonal, un polinomio homogéneo de segundo grado en esas coordenadas).



Si se saca a P su hiperplano del infinito, los puntos restantes pueden identificarse al hiperplano E_1 (ver figura), hiperplano afín de E que se obtiene trasladando el hiperplano E_0 al punto p (y esto puede hacerse de infinitos modos), y esta identificación consiste en asociar a cada punto propio de P (que es una recta de E) su intersección con E_1 . Entonces al cono $\mathcal{C}$ le corresponde su intersección con E_1 (= conjunto de puntos propios de la cuádrica proyectiva $\bar{S}$). Esto nos permite definir las cuádricas afines en la forma siguiente:

Si L es un espacio afín de dimensión $n-1 \geq 2$, elijamos uno de sus puntos como origen con lo que L se convierte en un espacio E_0 (vectorial) de dimensión $n-1$, y sea $E = \mathbb{R} \times E_0$ y P el espacio proyectivo deducido de E , $P = P(E)$, es decir el espacio proyectivo asociado al espacio vectorial E_0 . Ya hemos dicho varias veces que L puede identificarse al hiperplano afín $E_1 = \{1\} \times E_0$ de E , que a su vez puede pensarse como el conjunto de los puntos propios de P . Entonces, se llama cuádrica afín, S , a todo conjunto no vacío de L tal que $S = \bar{S} \cap E_1 = \bar{S} \cap L$, donde $\bar{S}$ designa una cuádrica proyectiva de P . En otras palabras, una cuádrica afín es el conjunto de los puntos propios de una cuádrica proyectiva del espacio pro-

---

(#) Esperamos que el lector no habrá de confundir el cono $\mathcal{C}$ con el cuerpo de los complejos $\mathbb{C}$.

(##) Cuando C es de índice 0 , puede ser $\mathcal{C} = \{0\}$ y $\bar{S}$ ser vacío.

yectivo asociado. Cuando la dimensión de E es 3 (es decir cuando la dimensión de P ó de L es 2) las cuádricas proyectivas reciben el nombre particular de cónicas proyectivas, y las cuádricas afines, el nombre de cónicas afines.

-o-

Si la forma cuadrática C que define una cuádrica proyectiva es no degenerada, dicha cuádrica también se llama no degenerada. Si S es una cuádrica afín, se puede demostrar que sólo pueden darse dos posibilidades que se excluyen mutuamente: o bien existe una única cuádrica proyectiva no degenerada $\bar{S}$ tal que $S = \bar{S} \cap L$, o bien no existe ninguna. En el primer caso, se dice que la cuádrica afín S es no degenerada.

-o-

Sean $\bar{V}_1$, $\bar{V}_2$ dos variedades lineales proyectivas de P y sean V_1 , V_2 , los subespacios de E cuyas rectas (privadas de O) definen los puntos de los primeros. Diremos que $\bar{V}_1$ y $\bar{V}_2$ son variedades conjugadas respecto de la cuádrica proyectiva $\bar{S}$ si y sólo si los subespacios V_1 , V_2 son ortogonales respecto de la forma cuadrática C que define a $\bar{S}$. (Por ejemplo, los puntos proyectivos $\bar{x}$, $\bar{y}$ son conjugados si las rectas $\mathcal{R}x$, $\mathcal{R}y$, son ortogonales en E respecto de C , es decir, en este caso, si y sólo si $\phi(x,y) = 0$).

Sea $\bar{V}$ una variedad proyectiva, y V el subespacio correspondiente en E ; sea V^o el ortogonal (para C) de V , y $\bar{V}^o$ la variedad proyectiva definida por V^o . En estas condiciones, diremos que $\bar{V}^o$ es la polar de $\bar{V}$ respecto de la cuádrica $\bar{S}$ (es claro que la polaridad es una relación simétrica). Si $\bar{S}$ es no degenerada, y si V es un hiperplano, V^o es una recta, de modo que la polar $\bar{V}^o$ de $\bar{V}$ es en este caso un punto de P : se dice que $\bar{V}^o$ es el polo del hiperplano proyectivo $\bar{V}$ respecto de la cuádrica no degenerada $\bar{S}$. Cuando V es un subespacio isótropo de E (respecto de la forma C) $\bar{V}$ y $\bar{V}^o$ tienen por lo menos un punto en común con la cuádrica $\bar{S}$; en este caso, se dice que $\bar{V}$ (y $\bar{V}^o$ también) es tangente a la cuádrica $\bar{S}$.

-o-

Sea ahora S una cuádrica afín no degenerada y $\bar{S}$ la cuádrica proyectiva no degenerada (única) tal que $S = \bar{S} \cap L$. Si W_1 , W_2 son dos variedades afines de L , se dice que son conjugadas respecto de S si las variedades proyectivas correspondientes, $\bar{V}_1$, $\bar{V}_2$ (iguales a W_1 , W_2 más sus puntos impropios, es decir tales que $\bar{V}_1 \cap L = W_1$, etc.) son conjugadas respecto de $\bar{S}$. La polar de una variedad afín W es, por definición, la variedad afín $W^o = \bar{V}^o \cap L$ correspondiente a la polar $\bar{V}^o$ de la variedad proyectiva $\bar{V}$ asociada a W (es decir que cumple: $\bar{V} \cap L = W$) . En forma totalmente similar se extienden a los espacios afines las nociones de polo de una variedad afín, o de variedades afines tangentes, respecto de una cuádrica S .

-o-

El polo del hiperplano del infinito de P se denomina <u>centro</u> de la cuádrica proyectiva $\bar{S}$ (y de la cuádrica afín asociada: $S = \bar{S} \cap L$). Usando las propiedades de las bases ortogonales (con respecto a la forma C) se puede probar que tomando el centro de $\bar{S}$ (resp. S) como origen de L y eligiendo una base ortogonal (para C) del espacio vectorial así obtenido, la ecuación de $\bar{S}$ es de la forma:

$$-(x^1)^2 + a_2(x^2)^2 + \ldots + a_n(x^n)^2 = 0$$

y la ecuación de S es de la forma:

$$a_2(x^2)^2 + a_3(x^3)^2 + \ldots + a_n(x^n)^2 = 1 \qquad (\#)$$

(esto siempre que el hiperplano del infinito no sea tangente a la cuádrica, es decir cuando el centro es un punto propio y por tanto es un punto de L).

Cuando el hiperplano del infinito es tangente a la cuádrica, el centro es un punto impropio y es usual decir que $\bar{S}$ (ó S) es una cuádrica <u>sin</u> centro. En este caso, se puede demostrar que existe un origen de L y una base ortogonal (para C) tales que la ecuación de S , por ejemplo, es de la forma:

$$a_2(x^2)^2 + \ldots + a_{n-1}(x^{n-1})^2 + x^n = 0 \qquad (\#\#)$$

Si $n = 3$, las cónicas sin centro se llaman parábolas y su ecuación (llamando x e y a las coordenadas de un punto de L) es de la forma $ax^2 + y = 0$ ó puede reducirse a esta forma. Las cónicas con centro que no cortan el hiperplano del infinito (recta del infinito en este caso) se llaman elipses, y sus ecuaciones pueden llevarse a la forma $x^2 + y^2 = 1$; las restantes (que cortan la recta impropia en dos puntos) se llaman hipérbolas, y sus ecuaciones pueden llevarse a una de las formas: $x^2 - y^2 = 1$, $y^2 - x^2 = 1$.

-o-

Antes de pasar al estudio de las esferas (afines) necesitamos un nuevo concepto.

Se dice que un subespacio M de E es <u>débilmente ortogonal</u> a otro N si se da una cualquiera de las relaciones siguientes: $M \subset N^o$ ó $M \supset N^o$ (estas relaciones son equivalentes, respectivamente, a $N \subset M^o$ y $N \supset M^o$, de modo que si M es débilmente ortogonal a N , entonces también N es débilmente ortogonal a M : <u>la relación</u>

(#) Recordar la expresión general de una forma cuadrática respecto de una base ortogonal (e_i) . Para obtener esta ecuación para S basta elegir uno de los e_i siguiendo la resta que corresponde al centro. Por la ley de inercia es posible lograr que los a_i sean iguales a 1 ó a -1 .

(##) Para deducir esta ecuación hacemos las siguientes sugestiones. La resta del centro es ahora isótropa (respecto de C). Tomarla como la de e_n , elegir un vector isótropo e_1 tal que $c(e_1, e_n) = 1$ y tomar una base ortogonal del subespacio ortogonal al plano de e_0 y e_n . Esta da los $e_2, \ldots, e_{n-1}$.

es simétrica). En la misma forma se ve que M es débilmente ortogonal a N si y sólo si M^o es débilmente ortogonal a N^o .

Si V_1 , V_2 , son dos variedades afines de un espacio afín, se dice que son perpendiculares si sus direcciones (es decir los subespacios vectoriales obtenidos al trasladarlas al origen) son débilmente ortogonales. Para designar esta relación escribimos $V_1 \perp V_2$. Por ejemplo, para que dos rectas afines sean perpendiculares, es necesario y suficiente que al trasladarlas al origen una de ellas contenga el hiperplano ortogonal a la otra. En el caso de dimensión 2 , dos rectas son perpendiculares si y sólo si son ortogonales.

-o-

10.2.- ESFERAS

Sea L un espacio afín de dimensión $n-1$, E_o el espacio vectorial obtenido al tomar un punto de L como origen, $E = \mathcal{R} \times E_o$, $P = P(E)$ el espacio proyectivo asociado a $L = E_o$. Como hemos hecho varias veces, identificamos L con $E_1 = \{1\} \times E_o$. Siendo E el producto de la recta $\mathcal{R}$ y el hiperplano E_o , notamos los puntos de E en la forma: $x = (\lambda, x_o)$ donde λ es la componente de x en $\mathcal{R}$, y x_o la componente de x en E_o . Es inmediato verificar que la función:

$$\phi(x,y) = (x_o|y_o) - \rho^2 \lambda\mu \qquad \begin{matrix} x = (\lambda, x_o) \\ y = (\mu, y_o) \end{matrix}$$

donde $(\ |\ )$ es una forma bilineal simétrica positiva y no degenerada, es una forma bilineal simétrica de índice 1 sobre E . La forma cuadrática definida por ϕ es:

$$C(x) = \phi(x,x) = (x_o|x_o) - \rho^2 \lambda^2$$

y el cono isótropo $\mathcal{C}$ correspondiente es:

$$\mathcal{C} = \{ x \in E \ / \ (x_o|x_o) = \rho^2 \}$$

Es claro que no existe ningún punto proyectivo $\mathcal{R}x \in P$ tal que $(\lambda x_o | \lambda x_o) = \lambda^2 \rho^2$ cuando $\lambda = 0$, de modo que la cuádrica proyectiva no degenerada definida por $\mathcal{C}$ no tiene puntos impropios y por tanto puede identificarse con la cuádrica afín (intersección de $\mathcal{C}$ con $L = E_1$):

$$S = \{ x_o \in L \ / \ (x_o|x_o) = \rho^2 \}$$

Las cuádricas afines de este tipo se denominan esferas (#). Más precisamente, se dice que S es la esfera de L de centro en el origen y radio ρ . En la misma forma, usando la forma bilineal simétrica $\phi_{c_o}(x,y) = (x_o - c_o \mid x_o - c_o) - \rho^2 \lambda\mu$ que

(#) Notar que en el caso $n = 2$, éstos son las elipses de 11.1 .

se obtiene cambiando el origen a c_o , se llega a la cuádrica:

$$S_{c_o} = \{x_o \in L \,/\, (x_o - c_o \mid x_o - c_o) = \rho^2\}$$

que es el conjunto obtenido trasladando S mediante la traslación $c_o - O$ de L y se llama <u>esfera de centro</u> c_o <u>y radio</u> ρ .

Una vez aclaradas las ideas fundamentales, podemos razonar siempre dentro del espacio afín L ya que en cualquier caso el razonamiento completo puede consistir, a lo sumo, en los siguientes pasos: pasaje de L al espacio vectorial E o al espacio proyectivo P . razonamiento en E ó P , respectivamente, y "regreso" a L , y confiamos en que el lector esté suficientemente familiarizado con estos pasajes como para que ellos puedan suprimirse en lo que sigue. Por eso, a partir de aquí, modificaremos la notación (para simplificar) suprimiento el subíndice "o" en las letras que designan puntos de L . Entonces, la ecuación de la esfera S_c de centro c y radio es:

$$(x-c \mid x-c) = d^2(x,c) = \rho^2 \qquad (x, c \in L \ , \ \rho \in \mathbb{R})$$

donde, como dijimos al comienzo del capítulo, $d(x,y)$ es la distancia del espacio euclídeo L definido por la forma métrica (|) .

-o-

Aplicando la teoría general de 11.1 vemos que si V_1 , V_2 son dos variedades afines de L , ellas serán <u>conjugadas</u> respecto de la esfera S_c si y sólo si:

$$(x-c \mid y-c) = \rho^2 \qquad (\forall x \in V_1 \ , \ \forall y \in V_2)$$

Si V es una viariedad afín de L , su polar, V^o , está definida así:

$$V^o = \{x \in L \,/\, (x-c \mid y-c) = \rho^2 \ , \text{ para todo } y \ V\}$$

y la variedad V será <u>tangente</u> a S_c si y sólo si la intersección $V \cap V^o$ es no vacía, en cuyo caso los puntos de esta intersección también pertenecen a la esfera S_c. En particular, un hiperplano H será tangente a S_c si y sólo si su polo H^o pertenece a S_c . Por lo tanto las condiciones de tangencia se pueden escribir así:

V es tangente a S_c si y sólo si existe x V tal que

$$(x-c \mid y-c) = \rho^2 \quad \text{para todo } y \in V$$

Es obvio que cada punto de S_c es conjugado de sí mismo (autoconjugado), de modo que si $p \in S_c$, la polar de p es:

conjunto de los y de L tales que: $(p-c \mid y-c) = \rho^2$.

Así, notamos en primer lugar, que ésta es una ecuación lineal en L , es decir una ecuación de la forma $f(y) = k$ (donde f es una forma lineal no nula sobre

$L = E_o$), y eso comprueba que la polar de un punto es un hiperplano. Es más, ese hiperplano pasa por p porque p mismo verifica la ecuación: $(p-c \mid p-c) = \rho^2$ dado que $p \in S_c$, de modo que ese <u>hiperplano es el hiperplano tangente a</u> S_c <u>que pasa por</u> p . Veamos ahora que p es el único punto que tienen en común la esfera y el hiperplano. En efecto, en el espacio vectorial E , p corresponde a un vector x isótropo para Ø , la cual, como vimos, tiene índice 1 . El hiperplano en cuestión corresponde aquí al hiperplano ortogonal a x , H . Si hubiera en H otro vector, y isótropo y no colineal con x , el plano de x e y sería totalmente isótropo y el índice de Ø sería ≥ 2 . Luego, en H , los vectores isótropos (para Ø) son los de la recta de x . Esto lleva a que, en L , p sea el único punto común a S y el hiperplano tangente.

-o-

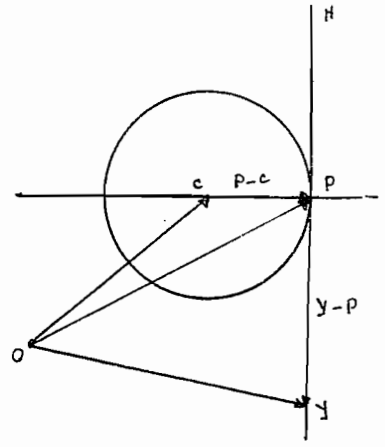
Sea z un punto de la recta R_{pc} (determinada por $p \in S_c$ y c), recta formada por los puntos $c + \lambda(p-c)$ y que tiene la dirección del vector p-c . Si y es un punto del hiperplano tangente en p a S_c , tenemos:

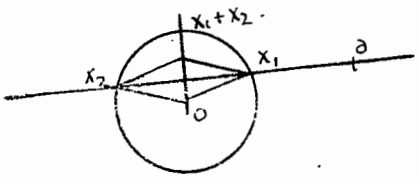
$$(z-c \mid y-p) = (p-c \mid y-p) = (p-c \quad y-c-(p-c)) = \lambda\,[(p-c \mid y-c)-(p-c \mid p-c)] =$$

$$= \lambda\,(\rho^2 - \rho^2) = 0$$

lo que prueba que <u>el hiperplano tangente en</u> p <u>a</u> S_c <u>es perpendicular a la recta (llamada diametral) que pasa por el punto de tangencia y por el centro de la esfera (recta diametral que pasa por</u> p) .

-o-





Razonemos ahora (para simplificar la escritura) sobre esferas S con centro en el origen de L (esto no constituye pérdida de generalidad porque las propiedades que vamos a estudiar se conservan en las traslaciones de L). Consideremos las rectas que pasan por un punto a de L y <u>cortan</u> a S (es fácil probar que en general cortan a S en 2 puntos , y nunca en más de dos, porque las "soluciones" del problema de intersección deben satisfacen (en coordenadas) un sistema de segundo grado)(#). Sea R una recta que pasa por a y corta a S en x_1, x_2. Como estos puntos están en la esfera (que tiene centro en el origen) se verifica $(x_1|x_1) = (x_2|x_2)$, y por tanto $(x_1+x_2 \mid x_1-x_2) = 0$, lo que prueba que la recta diametral que pasa por x_1+x_2 es perpendicu-

(#) Si $a+\overline{\xi}t$ es un punto de una recta que pasa por a y $a+\overline{\xi}t \in S$, se debe cumplir: $(a+\overline{\xi}t \mid a+\overline{\xi}t) - \rho^2 = 0$ que es una ecuación de segundo grado.

lar a la recta R (este hecho corresponde al teorema clásico que dice que las diagonales de un rombo son perpendiculares). Entonces podemos efectuar el siguiente razonamiento:

$$(x_1-a|x_2-a) = (a|a) + (x_1|x_2-a) - (a|x_2) = d^2(a,0) - \rho^2 + (x_2|x_2)-(a|x_2)+(x_1|x_2-a)=$$

$$= d^2(a,0) - \rho^2 + (x_2-a|x_1+x_2) = d^2(a,0) - \rho^2 \ .$$

Esto significa que el número $(x_1-a|x_1-a)$ es independiente de la recta R elegida (con tal de que corte a S en dos puntos). Se lo llama potencia de a con relación a S . Si S_c es la esfera de centro c y radio ρ , y si $a \in L$, resulta trivialmente por traslación que la potencia de a con relación a S_c está dada por:

$$(x_1-a \mid x_2-a) = d^2(a,c) - \rho^2$$

(basta reemplazar x_1 , x_2 , a , 0 , por x_1+c , x_2+c , a+c , c en la fórmula anterior).

-o-

Sean ahora S_1 , S_2 , las esferas de centros c_1 , c_2 y radios ρ_1 , ρ_2 respectivamente (además suponemos que los centros son distintos), y consideremos el conjunto:

$$H = \left\{ x \in L \ / \ (x-c_1 \mid x-c_1) - \rho_1^2 = (x-c_2|x-c_2) - \rho_2^2 \right\}$$

que no es otro que el conjunto de los puntos de L que tienen la misma potencia respecto de las esferas.

Veamos cómo transformar las condiciones que determinan a H en una ecuación lineal, lo que probará que H es un hiperplano:

Por la definición se tiene:

$$x \in H \iff -2\,(x|c_1) + 2\,(x|c_2) = \rho_1^2 - \rho_2^2 + (c_2|c_2) - (c_1|c_1)$$

$$\iff (x|c_2-c_1) = \tfrac{1}{2}(\rho_1^2 - \rho_2^2 - |c_1|^2 + |c_2|^2$$

que es evidentemente una ecuación de la forma $(x|c) = k$, es decir una ecuación lineal. Así se ha demostrado que el conjunto H de los puntos de L que tienen igual potencia respecto de S_1 y S_2 es un hiperplano de L , que se llama hiperplano radical de S_1 y S_2 . Es claro que si un punto pertenece a las dos esferas, entonces tiene potencia nula respecto de ambas, y por tanto está en H : el hiperplano radical de dos esferas que se cortan contiene su intersección.

Puesto que la ecuación de H es de la forma $(x|c_1-c_2) = k$, si x' y x" son dos puntos de H , se cumple $(x'-x"|c_1-c_2) = 0$, lo que prueba que el vector x'-x" es ortogonal al vector c_1-c_2 , o también que el hiperplano radical, H , de S_1, S_2,

es perpendicular a la recta de los centros, $R_{c_1c_2}$

-o-

Manteniendo la notación anterior, decimos que las siguientes condiciones son equivalentes:

(a) Existe un punto t común a S_1 y S_2 tal que los hiperplanos H_1, H_2, tangentes, respectivamente, a S_1, S_2, en t, son perpendiculares.

(b) La potencia de c_1 con relación a S_2 es ρ_2^2.

(b') La potencia de c_2 con relación a S_1 es ρ_1^2.

(c) El hiperplano H (radical) es la polar de c_1 respecto de S_2.

(c') El hiperplano H (radical) es la polar de c_2 respecto de S_1.

Como vimos al final del número anterior, $H_1 \perp H_2$ si y sólo si la recta ortogonal a H_1 es perpendicular a la recta ortogonal a H_2, lo que ocurre si y sólo si $(t-c_1|t-c_2) = 0$. De modo que (a) es una condición equivalente a que exista en S_1 S_2 un punto t tal que $(t-c_1|t-c_2) = 0$. Por otra parte es inmediato (escribiendo las ecuaciones correspondientes) que (b) es equivalente a (b') y que (c) es equivalente a (c'). Demostremos que (a) implica (b') $\Longleftrightarrow$ (b):

$$(c_1-c_2|c_1-c_2) = (c_1-t-(c_2-t)|c_1-t-(c_2-t)) =$$

$$= (c_1-t|c_1-t) + (c_2-t|c_2-t) + (c_1-t|t-c_2) + (t-c_2|c_1-t) =$$

$$= (c_1-t|c_1-t) + (c_2-t|c_2-t) = \rho_1^2 + \rho_2^2 ,$$

es decir:

$$(c_1-c_2|c_1-c_2) - \rho_2^2 = \rho_1^2$$

$$(c_2-c_1|c_2-c_1) - \rho_1^2 = \rho_2^2$$

Ahora, para ver que (b) $\Longleftrightarrow$ (b') implica (c) $\Longleftrightarrow$ (c') tenemos que probar que una cualquiera de las igualdades equivalentes de arriba implica que si $x \in H$ = hiperplano radical, entonces pertenece a la polar de c_2 respecto de S_1 (y recíprocamente) y también a la polar de c_1 respecto de S_2 (y recíprocamente). Pero esto es **inmediato** porque usando esas relaciones se tiene:

$$2(x|c_2-c_1) = \rho_1^2 - \rho_2^2 - (c_1|c_1) + (c_2|c_2)$$

(que es la ecuación de H) equivale sucesivamente a:

$$2(x|c_2-c_1) = \rho_1^2 + \rho_1^2 - (c_2-c_1|c_2-c_1) - (c_1|c_1) + (c_2|c_2) \Longleftrightarrow$$

$$2(x|c_2-c_1) = 2\rho_1^2 + 2(c_1|c_2-c_1) \Longleftrightarrow (x-c_1|c_2-c_1) = \rho_1^2$$

y análogamente: $\Longleftrightarrow (x-c_2|c_1-c_2) = \rho_2^2$ (que son las ecuaciones de las polares en cuestión).

Por medio de cálculos similares se prueba que (c) $\Longleftrightarrow$ (c') implica (a) , de modo que las cinco condiciones son equivalentes.

Por definición, cuando S_1 , S_2 (de centros distintos) verifican una (y por tanto todas) de las condiciones anteriores, se dice que S_1 y S_2 son dos esferas ortogonales.

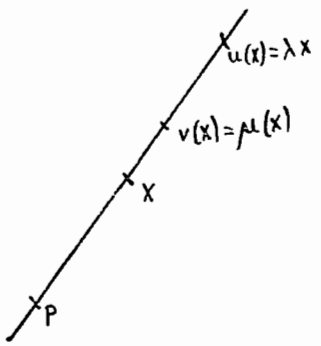
Dejamos a cargo del lector la tarea de deducir otras propiedades conocidas de la geometría clásica de dos o tres dimensiones dentro de esta teoria más general. Por ejemplo, demostrar que si S_1 y S_2 son ortogonales, si x es un punto de L cuyas potencias respecto de S_1 y S_2 son w_1 , w_2 , respectivamente, entonces vale la relación:

$$w_1 + w_2 = 2.(x-c_1|x-c_2)$$

-o-

11.3.- LA INVERSION

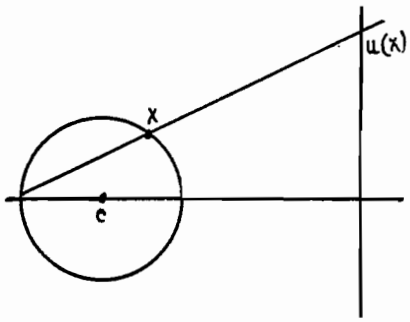
Consideremos un punto p L y un número real, α diferente de 0 . Si x es un punto de L diferente de p , existe en la recta de p y x , R_{px} un punto (único), u(x) , tal que x-c|u(x)-c) = (porque en L no hay rectas isótropas). Esto permite definir una aplicación puntual: $x \longrightarrow u(x)$ del conjunto $L - \{p\}$ sobre si mismo, que deja invariantes las rectas (privadas de p) que pasan por p (si bien en general no deja invariantes los puntos de dichas rectas). Además, como la forma métrica (|) es simétrica, la definición dice que si y es la imagen de x según esta permutación (cf. Apéndice IV) de $L-\{p\}$, entonces también x es la imagen de y para la misma permutación u . En otras palabras, para todo x diferente de p se cumple: u(u(x)) = x : la aplicación u es una permutación involutiva de $L- \{p\}$. Por definición, estas permutaciones se denominan inversiones, y más precisamente, se dice que u es la inversión de polo p y potencia α .



Si u , v son inversiones de polo p y potencias α , β respectivamente, tomemos p como origen de L (p = 0) y sea $x \neq 0$. Como u(x) está en la recta que une x con el origen (recta homogénea de x) , existe un escalar λ tal que $u(x) = \lambda x$, y, análogamente, $v(x) = \mu x$. Entonces, como por definición de inversión $(\mu x|u(\mu x)) = \beta$, y por lo mismo: $(x|u(x)) = \lambda(x|x) = \alpha$, y $(x|v(x)) = \mu(x|x) = \beta$, se tiene $\mu\lambda^{-1} = \beta\alpha^{-1}$ (porque $(x|x) \neq 0$) . Entonces $v(x) = (\beta\alpha^{-1})u(x)$ y siendo u(x) arbitrario en $L- \{p\}$, se sigue que uv^{-1} es la homotecia (restringida a $L- \{p\}$) de razón α/β .

-o-

Consideremos ahora la esfera S de centro c que pasa por el origen 0 (es decir cuyo radio cumple: $(c|c) = \rho^2$), y sea u la homotecia de polo 0 y potencia α . (Una situación equivalente se tiene si se considera cualquier esfera y una inversión cuyo polo pertenezca a la esfera). Si $x \in S$, $x \neq 0$, $u(x)$ es de la forma λx . Calculemos λ . Por definición de u , $(x|u(x)) = \lambda(x|x) = \alpha$ y por definición de S : $(x-c|x-c) = \rho^2$. Desarrollando esta expresión y usando la relación anterior tenemos: $\alpha = 2.\lambda.(x|c)$ de donde deducimos luego:



$$(c|u(x)) = \frac{\alpha\,(c|x)}{2\,(c|x)} = \frac{\alpha}{2}$$

Esto significa que la imagen de $S - \{0\}$ por la inversión u está contenida en el hiperplano cuya ecuación es $(c|z) = \frac{\alpha}{2}$ $(z \in L)$. Pero de hecho podemos ver que dicha imagen es <u>todo</u> este hiperplano, es decir: si z L verifica: $(c|z) = \frac{\alpha}{2}$, entonces existe en S un punto x diferente de 0 tal que $u(x) = z$; Puesto que H no contiene al origen, porque α es diferente de 0 , tiene sentido considerar el punto $u(z) = \lambda z$. Entonces, la relación $(z|u(z)) = \alpha$, implica $\lambda = \frac{\alpha}{(z|z)}$, de donde, usando la ecuación del hiperplano podemos calcular:

$$(u(z)-c|u(z)-c) = (u(z)|u(z)) - 2(c|u(z)) + (c|c) =$$

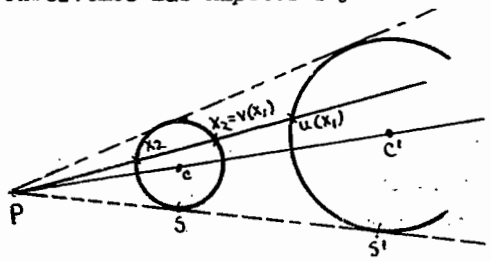
$$= \frac{\alpha^2}{(z|z)}\,2(z|z) - \frac{2\alpha}{(z|z)}\,(c|z) + \rho^2 = \frac{\alpha^2}{(z|z)} - \frac{\alpha^2}{(z|z)} + \rho^2 = \rho^2$$

y esto prueba que $u(z) \in S$, de manera que si se escribe $x = u(z)$, este punto responde a la cuestión: $u(x) = z$ (porque u es involutiva).

<u>Una inversión de polo</u> p <u>transforma toda esfera que pasa por</u> p (<u>privada de</u> p) <u>en un hiperplano ortogonal a la recta que une</u> p <u>con el centro de la esfera; y todo hiperplano que no pasa por</u> p <u>en una esfera que pasa por</u> p <u>y cuyo centro está sobre la recta perpendicular al hiperplano y que contiene a</u> p . (La condición de ortogonalidad aquí indicada resulta usando la ecuación del hiperplano, la cual muestra que si z' , z" están en la imagen de S , entonces $(z'-z"|c) = 0$; la aserción sobre la imagen de un hiperplano que no pasa por p es consecuencia obvia de la primera en virtud de que las inversiones son involutivas).

-o-

Conservemos las hipótesis y notaciones del razonamiento anterior pero suponiendo ahora que S no contiene el polo $p = 0$, y usemos la letra w para designar la potencia de p respecto de S : (en la figura) $w = (x_1|x_2) \neq 0$. Entonces, si v es la inversión de polo p y potencia w,

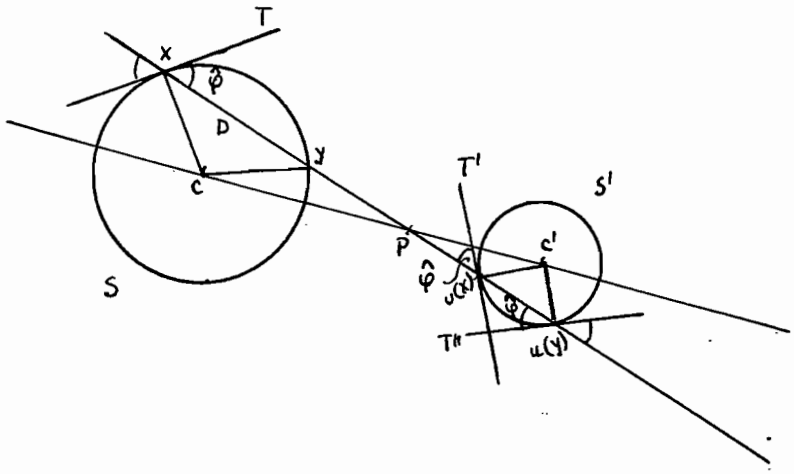


es claro que $v(x_1) = x_2$ (y $v(x_2) = x_1$) , y por lo tanto, v <u>transforma</u> S <u>en sí misma</u>. Ahora bien, ya hemos visto que la aplicación compuesta uv^{-1} es la homotecia de razón α/w , lo que prueba que $u(S) = uv^{-1}(S)$, imagen de S por u , es igual a la imagen de S por una homotecia, y por tanto es una esfera cuyo centro es $c' = \frac{\alpha}{w} .c$, y cuyo radio es $\rho' = \frac{\alpha}{w} .\rho$ (que las homotecias transforman esferas en esferas en la forma indicada, es un hecho simple de demostración inmediata que dejamos a cargo del lector).

<u>Una inversión de polo</u> p <u>transforma toda esfera que no pasa por</u> p <u>en otra esfera que no pasa por</u> p <u>cuyo centro es la imagen del centro de la esfera dada por una homotecia de centro</u> p <u>y de razón igual al cociente de la potencia de la inversión por la potencia de</u> p <u>respecto de la esfera dada</u>.

—o—

Supongamos ahora que, o bien la dimensión de L es 2 , o bien razonamos en un plano de L que pasa por el polo, p (= 0) de la inversión u . En este caso, las esferas de L (resp. las intersecciones de las esferas de L con el plano P) son esferas de un espacio afín de dimensión 2 y se denominan <u>circunferencias</u>. Supongamos, como antes, que tenemos una circunferencia S , que la inversión u transforma en una circunferencia S' , y que p no pertenece a S (por tanto tampoco pertenece a S'). Razonaremos con la ayuda de la figura. Sea D la recta que pasa por el vector x (es decir por el punto x y por el origen p), T la tangente en x a S , T" la tangente en u(y) a S' , siendo u(y) el punto correspondiente de x en la homotecia del razonamiento anterior que lleva S sobre S' . Como T forma ángulo recto con la recta R_{xc} , debe transformarse por esa homotecia en una recta que pase por u(y) y forme ángulo recto con $R_{c'u(y)}$. Como, por otra parte, dicha homotecia lleva D sobre D , el ángulo de D con T tiene que ser igual al ángulo de D con T" , donde T" que es la perpendicular a $R_{c'u(y)}$ en u(y) , tiene que



(#) Conviene notar el la figura al pie de la página anterior, que por un razonamiento anterior (pág.), las direcciones de las rectas cx_1, cx_2 son simétricas respecto del hiperplano ortogonal a la dirección de la recta px_1x_2 .

ser la imagen de T por la homotecia mencionada. Entonces podemos escribir:

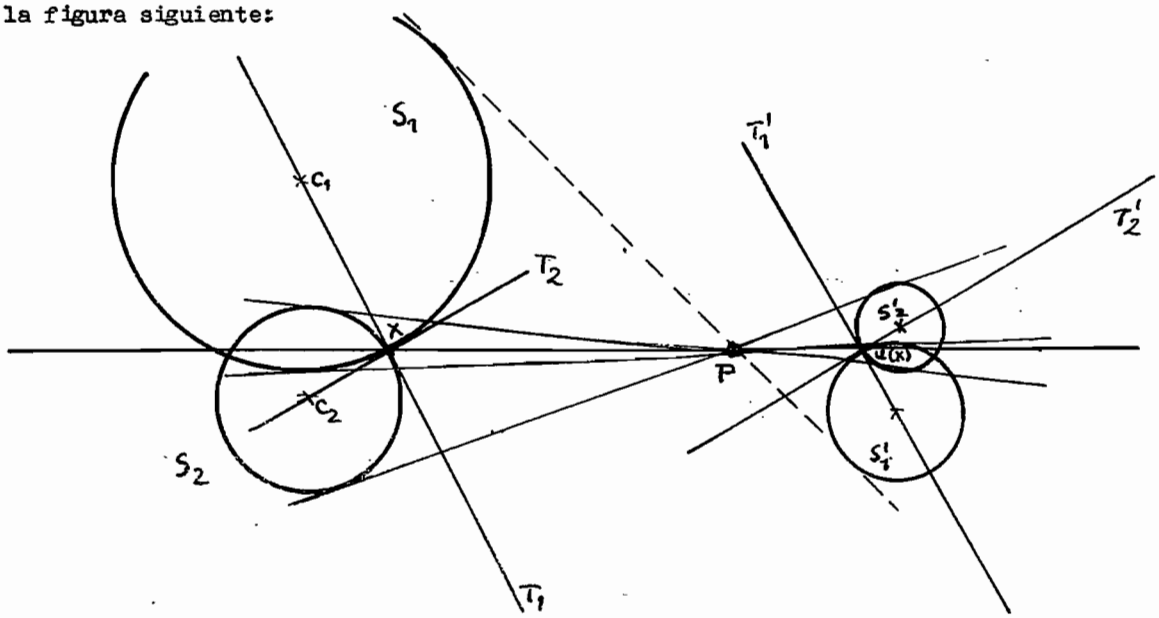
$$(\hat{D,T}) = (\hat{D,T^*}) = (\hat{T',D})$$

donde T' es la tangente en $u(x)$. En efecto, es fácil ver usando las propiedades que vimos en el §10 que una simetría (en el plano) invierte los ángulos de rectas, es decir, si la simetría s lleva una recta R en R' , y una recta R_1 en R_1' , entonces el ángulo $(\hat{R,R_1})$ es igual al opuesto de $(\hat{R',R_1'})$, es decir igual al $(\hat{R_1',R_1})$. Entonces basta aplicar este hecho a la simetría que lleva $u(y)$ sobre $u(x)$ y cuyo eje pasa por c' .

En resumen, la inversión u es tal que el ángulo que forma la recta determinada por x y $u(x)$ con la tangente en x a S , es igual al opuesto del ángulo que forma aquella recta con la tangente en $u(x)$ a S' .

-o-

Sean ahora S_1 , S_2 , dos esferas ortogonales (que no pasan por p) y S_1' , S_2' , sus imágenes respecto de la inversión u . Razonemos ahora en el plano determinado por los centros c_1 , c_2 de S_1 , S_2 (que necesariamente contiene los centros c_1' , c_2' de S_1' , S_2') y por el origen $p = 0$. Sea x un punto común a las circunferencias correspondientes (es decir las intersecciones de S_1 , S_2 con aquel plano) . Como los hiperplanos tangentes en x a las dos esferas son perpendiculares, y el que contiene al radio R_{xc_1} es perpendicular al que contiene al radio R_{xc_2} , etc., resulta que las rectas Rxc_1 y R_{xc2} son perpendiculares entre sí. Si las llamamos , respectivamente, T_1 , y T_2 , resulta que T_1 es la tangente a la circunferencia S_2 en el punto x , en tanto que T_2 es la tangente a la circunferencia S_1 en x. Esto prueba, entre otras cosas, que las circunferencias de intersección también son ortogonales. Llamemos D a la recta que pasa por x y por p , y razonemos sobre la figura siguiente:



Como acabamos de ver, el ángulo $(D,\hat{T}_2)$ es igual al ángulo $(T_2',\hat{D})$, y el ángulo $(D,\hat{T}_1)$ igual al ángulo $(T_1',\hat{D})$, donde T_1' , T_2' son, respectivamente, las tangentes en $u(x)$ a S_2' y S_1' . Entonces, el ángulo $(T_1',\hat{T}_2)$, que es recto y es la suma de los dos primeros, es igual al ángulo $(T_1',\hat{T}_2')$ (#). Esto prueba, en primer lugar, que también las circunferencias S_1' , S_2' son ortogonales, pero también prueba que las esferas de S_1' , S_2' son ortogonales, pues sus respectivos hiperplanos tangentes en $u(x)$ contienen sendas rectas ortogonales (en el plano considerado).

Dos esferas ortogonales que no contienen el polo de una inversión son transformadas por ésta en dos esferas ortogonales.

-o-

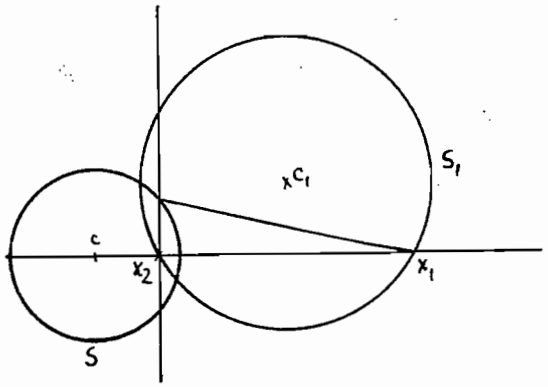
Otro razonamiento igualmente simple permite demostrar también que:

Si S_1 contiene el polo p y S_2 no lo contiene, entonces S_1' es un hiperplano que pasa por el centro de la esfera S_2' (y se dice que un tal hiperplano es ortogonal a la esfera); si las dos esferas contienen el punto p , los hiperplanos S_1', S_2' son perpendiculares entre sí .

-o-

Terminemos este número con las propiedades de la inversión respecto de una esfera:

Sea u la inversión de polo $c = 0$, y de potencia $\alpha = \rho^2 > 0$, y sea S la esfera de centro c y radio ρ . Si los puntos x_1 , x_2 , determinan una recta que pasa por c , las propiedades siguientes son equivalentes:



(a) $u(x_1) = x_2$ y $u(x_2) = x_1$

(b) x_1 , x_2 , son conjugados respecto de S (es decir, cada uno está contenido en la polar del otro, o también, en fórmulas, $(x_1|x_2) = \rho^2$)

(c) Si S_1 es una esfera cualquiera que pasa por los puntos x_1 , x_2 , entonces S es ortogonal a S_1 .

En efecto: si $u(x_1) = x_2$, $(x_1|u(x_1)) = (x_1|x_2) = \alpha = \rho^2$, de modo que (a) implica (b) . También (b) es equivalente a (c) porque si x_1 , x_2 están en una misma esfera (por ejemplo de centro c_1) se verifica que la potencia de c (centro de S) respecto de esa esfera es, por definición, igual a $(x_1|x_2) = \rho^2$, que es una de las condiciones necesarias y suficientes para que S y S_1 sean ortogonales . Finalmente, es claro también que (b) implica (a) , porque si x_2 está en la rec-

(#) También se puede razonar así: Como ya vimos (pág.), las direcciones de las rectas T_1 , T_2 , son simétricas de las direcciones de las rectas T_1' , T_2' , con relación a un mismo hiperplano (el ortogonal a la dirección de la recta por $u(x)$). Entonces, como T_1 , T_2 son ortogonales, T_1' , T_2' también lo son (cf. nota al pié de la pág.).

ta que pasa por x_1 y por el polo de la inversión, c y si además se verifica $(x_1|x_2) = \rho^2 = \alpha$, entonces $(x_1|x_2) = (x_1|u(x_1))$, lo que prueba que $x_2 = u(x_1)$.

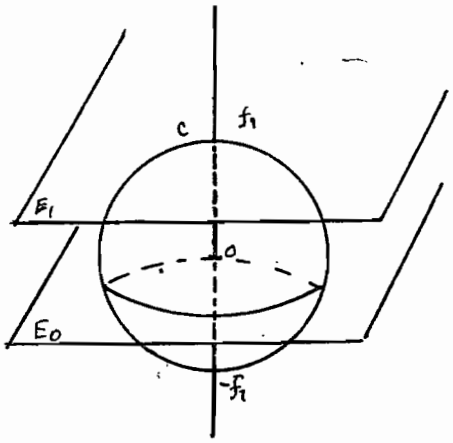
Cuando se cumple una (y por tanto todas) de estas tres propiedades, se dice que u es la inversión respecto de la esfera S . Nótese, en particular, que u deja fijo cada uno de los puntos de S .

-o-

11.4.- EL GRUPO CONFORME

Volvamos a la situación del comienzo de este parágrafo, sin modificar la notación. Llamemos f_1 al punto (1,0) de E .Consideremos en E la forma bilineal positiva y no degenerada:

$$\phi(x+\lambda f_1|y+\mu f_1) = (x|y) + \lambda\mu$$



donde x , y son puntos de $L = E_0$) y sea C la esfera de centro en el origen y de radio 1 (con relación a la forma métrica ϕ). Notemos con s la inversión de E de polo $-f_1$ y potencia 2 . Decimos que la imagen de $L = E_0$ (hiperplano de E) es justamente la esfera C (privada del polo $-f_1$). Para ello, en vista de lo que ya sabemos de las inversiones, basta observar que la relación: $\phi(0-(-f_1), f_1-(-f_1)) = 2$, prueba que s transforma 0 en f_1 . Esta inversión s se denomina proyección estereográfica de L sobre C de polo $-f_1$ (y también $s^{-1} = s$ se llama la proyección estereográfica de C sobre L de polo $-f_1$).

Si u es una inversión de $E_0 = L$ de polo c , la aplicación $u' = sus^{-1}$ lleva la esfera C (privada de $-f_1$ y de s(c)) sobre la esfera C privada de los mismos puntos y por tanto puede prolongarse u' a toda la esfera C definiendo que $u'(-f_1) = s(c)$, $u'(c) = -f_1$. Hecho esto, es claro que u' es una permutación involutiva (ver el apéndice IV) de la esfera C sobre sí misma, que se llama inversión en C deducida de la inversión u en L .

Análogamente, si v es una simetría (afín) de L respecto de un hiperplano, la aplicación svs^{-1} lleva el conjunto C privado de $-f_1$ sobre el conjunto C privado de $-f_1$. Si la designamos con v' , ésta aplicación puede prolongarse a una permutación involutiva de C sobre C mediante: $v'(-f_1) = -f_1$. Hecho esto, la permutación v' de C se denomina la simetría de C deducida de la simetría v de L .

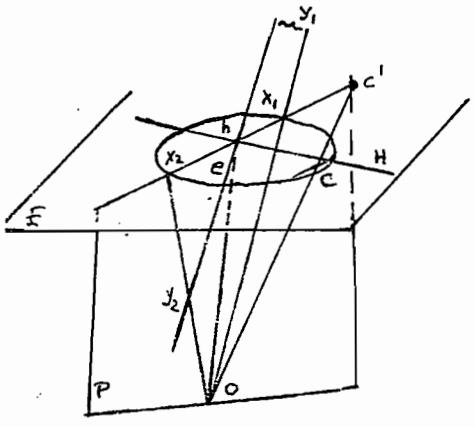
El subgrupo Γ del grupo simétrico (C) (ver apéndice IV) engendrado por las inversiones y las simetrías de C se denomina grupo conforme de C (y también, por abuso de lenguaje, grupo conforme de L) .

Las propiedades más importantes del grupo conforme, que no demostraremos, son las siguientes:

(1) . está engendrado por las simetrías v' y por las inversiones u' asociadas a inversiones u de potencia positiva. (Para demostrarlo, hay que probar primero que en L toda traslación es producto de simetrías respecto de hiperplanos, y usar que el producto de dos inversiones es una homotecia, que una inversión de potencia $\alpha < 0$ es producto de la de potencia $-\alpha > 0$ y la simetría $x \longrightarrow -x$ y que ésta es el producto de las simetrías respecto de los n hiperplanos de coordenadas.)

(2) Si u' es la inversión asociada a u y la potencia de u es positiva, entonces u' es la restricción a C de una inversión de E , respecto de una esfera ortogonal a C , o si no es la restricción a C de una simetría respecto de un hiperplano homogéneo de E . Hay propiedades análogas para una simetría v'. (Para la demostración, notar que u es la inversión respecto de una cierta esfera S_0 de E_0 y es también la restricción a E_0 de la inversión de E , v_1 con respecto a la esfera S del mismo centro y el mismo radio en E . Si se pone $S' = s(S)$ es claro que S' es ortogonal a C puesto que S es ortogonal a E_0 ; si toda esfera que pasa por x_1 , x_2 es ortogonal a S , toda esfera que pasa por $s(x_1)$, $s(x_2)$ es ortogonal a $s(S) = S'$. Por lo tanto la inversión de esfera s' es $v' = svs^{-1}$ (porque $s(x_2) = s(v(x_1)) = v'(s(x_1))$. Se sigue que su restricción a C es sus^{-1} , es decir u' . (En la última parte se usa la característica de la inversión con respecto a una esfera dada en pag.).)

(3) Consideremos el espacio $F = \mathbb{R} \times E$, y en él la forma cuadrática definida por $Q_2(\lambda, x) = \lambda^2 - \phi(x,x)$ (donde ahora x designa un punto de E y no de E_0). Entonces, el grupo conforme Γ de C (ó de L) es isomorfo al grupo cociente $\phi(Q_2 | \mathcal{Z}(Q_2))$ donde $\mathcal{Z}(Q_2)$ es el centro de $\phi(Q_2)$. (Identificar C con la intersección del cono isótropo Σ : $Q_2(\lambda, x) = 0$ y el hiperplano $\lambda = 1$ identificado con E y designar con e el vector de F centro de C . Con las notaciones de 2 , sea c' el centro de S' , H el hiperplano polar de c' con relación a C . La relación $(h|c') = 1$ en E se transforma en $\phi_2(h, c') = 0$ en F por definición de Q_2 . Entonces en el plano P definido por las rectas Ox_1 , Ox_2 , las rectas



Oh , Oc' son ortogonales respecto de la restricción $\phi_{2,P}$ de ϕ_2 a P , y Ox_1 , Ox_2 son las rectas isótropas de ese plano. Entonces, ellas se transforman una en la otra por la simetría con respecto a Oh en ese plano. De otro modo: si se traza por h una parálela a Oc' , los puntos y_1 , y_2 en que corta a Ox_1 , Ox_2 son simétricos con relación a h . Entonces, Oy_1, Oy_2 son transformadas una en la otra por la simetría w relativa al hiperplano $\bar{H}$ que pasa por O y H (respecto de ϕ_2 y en F !). En otras palabras, la restricción de esta simetría al cono isótropo determina completamente u' . El recíproco se deduce fácilmente (usando el lema 2, 4.7), y es claro que -w también determina a u' . Usando ahora el teorema 1 del Ap. IV, se obtiene la isomorfía del grupo conforme con el cociente de $O(Q_2)$ por su centro.)

(4) Identificando E como es usual con una parte del espacio proyectivo asociado P(F) , el conjunto de los puntos de P(F) que o bien no son puntos de E (puntos impropios), o bien son puntos de E pero $\phi(x,x)$ 1 , se pueden poner en correspondencia biunívoca con las esferas e hiperplanos de L , de modo que a dos puntos distintos del primer conjunto y conjugados respecto de C correspondan dos esferas ortogonales de L . (Manteniendo las notaciones: si S" es una esfera ortogonal a S' , su centro c" tiene que estar sobre H pues ella es a la vez ortogonal a S' y a C y entonces su centro debe tener la misma potencia respecto de estas dos esferas y por lo tanto estar sobre su hiperplano radical. Se pasa ahora a las esferas de E con centro en E_o , considerando s(S') y s(S") y es claro que decir que dos tales esferas de E son ortogonales es equivalente a decir que sus intersecciones con E_o son dos esferas de E_o ortogonales. Con esto todo está prácticamente demostrado.)

(5) La geometría asociada al grupo $\phi_2(Q)/\ _2$ es la geometría no euclidiana hiperbólica.

-o-

CAPITULO V

GRUPOS SIMPLECTICOS Y FORMAS ALTERNADAS

§12.- FORMAS ALTERNADAS. BASE SIMPLECTICA. GRUPO SIMPLECTICO

12.1.- FORMAS ALTERNADAS

Sea K un cuerpo conmutativo (no se excluye que K sea de característica 2) y E un espacio vectorial de dimensión n sobre K .

Una forma bilineal Ψ , sobre E , se llama alternada si $\Psi(x,x) = 0$ para cada x en E . En particular, se verifica: $\Psi(x+y,x+y) = \Psi(x,x) + \Psi(x,y) + \Psi(y,x) + \Psi(y,y) = \Psi(x,y) + \Psi(y,x) = 0$, de modo que toda forma alternada es antisimétrica. En cambio, si Ψ es antisimétrica se tiene, por definición $\Psi(x,x) = -\Psi(x,x)$, lo que implica $2\Psi(x,x) = 0$ para cada x en E , y si K es de característica diferente de 2 , Ψ es alternada. Por lo tanto, en ese caso, una forma es alternada si y sólo si es antisimétrica.

La primera observación dice también que toda forma alternada es -1-hermitiana respecto del automorfismo idéntico de K , de modo que valen para las formas alternadas todas las propiedades de las formas $-$-hermitianas.

-o-

12.2.- Teorema 1 :

Existe una base (e_i) de E , y un entero par, $2r$ 0 tales que

$$\Psi(x,y) = \Psi\Big(\sum_i x^i e_i \,,\, \sum_j y^j e_j\Big) = \sum_{j=1}^{r} (x^{2j-1} y^{2j} - x^{2j} y^{2j-1})$$

donde Ψ es una forma alternada dada previamente. Tal base se llama simpléctica (para Ψ). El rango de Ψ es siempre un número par, y más precisamente, es igual a $2r$.

Demostración:

Este teorema es consecuencia del último resultado de 4.7 . En efecto, en un suplementario de E^0 , Ψ es no degenerada y aquí se tiene necesariamente $H = 0$ porque todo vector es isótropo (notación de 4.7) . No obstante razonaremos así:

En primer lugar, podemos suponer $\Psi \neq 0$ pues si $\Psi = 0$ el teorema es trivial. Además, podemos limitarnos al caso en que es no degenerada, demostrando que entonces necesariamente $n = 2r$ y el resto del teorema (esto equivale a razonar en un suple -

mentario de E^o , aprovechando que en E^o ψ es idénticamente nula). Razonaremos por recurrencia sobre la dimensión n , de E .

La suposición de que ψ es no nula implica que n vale por menos 2 , pues si se verifica $\psi(x,y) \neq 0$ para un par de vectores x e y de E , éstos son necesariamente linealmente independientes.

Si $n = 2$, y ψ no degenerada, existen e_1' , e_2' (linealmente independientes) tales que $\psi(e_1',e_2') \neq 0$ (por la observación precedente). Si se escribe $e_1 = \frac{1}{\psi(e_1',e_2')} e_1'$, y $e_2 = e_2'$, (e_1,e_2) es una base que es la base simpléctica buscada (con $r = 1 = n/2$). En efecto, esa elección implica que $\psi(e_1,e_2) = 1$, y $\psi(e_2,e_1) = -1$, de modo que

$$\psi(x^1e_1+x^2e_2 \, , \, y^1e_1+y^2e_2) = x^1y^2 - x^2y^1$$

Supongamos entonces que si se tiene una forma alternada no degenerada sobre un espacio vectorial de dimensión menor que n , entonces necesariamente esta dimensión es par ($= 2r'$) y valen las restantes afirmaciones del teorema. Sea ψ una forma alternada no degenerada sobre E de dimensión n . Como ψ es no nula, existen (igual razonamiento que antes) dos vectores e_1 , e_2 , linealmente independientes, tales que $\psi(e_1,e_2) = 1$. Sea P el plano engendrado por ellos; decimos que P es no isótropo. En efecto, si existieran λ_o , μ_o (no los dos nulos) tales que para todo λ y para todo μ se verificara $\psi(\lambda_o e_1+\mu_o e_2 \, , \, \lambda e_1+\mu e_2) = 0$ resultaría $\lambda_o\mu - \lambda\mu_o = 0$ $(\forall\lambda \, , \forall\mu \in K)$, lo que es absurdo. Entonces E es suma directa de P y P^o (cf. teor. 1 del §4), y ψ es no degenerada en P^o , que tiene dimensión $n-2 < n$. Por la hipótesis de recurrencia, P^o es de dimensión par y admite una base simpléctica $e_3,e_4,\ldots,e_{2r}$. Entonces resulta por simple cálculo que $e_1,e_2,e_3,\ldots,e_{2r}$ es una base simpléctica para todo E .

-o-

Corolario:

Si A es una matriz alternada (es decir matriz de una forma alternada) existe una matriz inversible B tal que:

$$t_{BAB} = \begin{pmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} & 0 & 0 & \cdots & & & & & 0 \\ 0 & \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} & 0 & \cdots & & & & & 0 \\ 0 & 0 & \ddots & & & & & & \vdots \\ \vdots & & & \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} & & & & & 0 \\ & & & & 0 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 0 & & \\ 0 & \cdots & & & & & & \ddots & 0 \end{pmatrix}$$

$2r$

Demostración:

En efecto, si Ψ es la forma alternada definida por A y si B es la matriz que relaciona la base dada con una base simpléctica, ${}^tBAB$ es la matriz de Ψ respecto de la base simpléctica, que es de esa forma (#) .

-o-

12.3.- GRUPO SIMPLECTICO.

Los automorfismos de E tales que dejan invariante una forma alternada Ψ : $\Psi(u(x),u(y)) = \Psi(x,y)$ o sea las transformaciones unitarias(para Ψ) se llaman, en este caso especial, transformaciones simplécticas (para Ψ). Forman un grupo (que no es otro que el grupo unitario de Ψ) que se llama grupo simpléctico de Ψ y que se designa con la notación $Sp(\Psi)$. Las matrices de las transformaciones simplécticas se llaman matrices simplécticas y se puede demostrar que todas ellas tienen determinante igual a 1 . (cf.: Bourbaki, Alg. Ch.9, §5, Prop. 3) .

-o-

13.- REDUCCION DE UNA FORMA ALTERNADA RESPECTO DE UNA FORMA HERMITIANA POSITIVA.

Suponemos en este parágrafo que estamos en el caso $K = \mathbb{R}$ ó $K = \mathbb{C}$ (cf.: §.2); $\emptyset$ designa una forma hermitiana positiva y no degenerada sobre E ; Ψ designa una forma alternada sobre E .

13.1.- APLICACIONES SEMILINEALES

Una aplicación u de E en E se llama semilineal si cumple las condiciones:

$$\begin{aligned} u(x+y) &= u(x) + y(y) \\ u(\lambda x) &= \bar{\lambda}\, u(x) \end{aligned} \qquad (\forall x, \forall y \in E, \forall \lambda \in K)$$

Como $\emptyset$ es no degenerada, para cada $x \in E$ existe un único elemento $u^{\#}(x)$ de E tal que $\emptyset(x,u(y)) = \overline{\emptyset(u^{\#}(x),y)}$ $(\forall y \in E)$ (cf. corolario del teor. 1, §1). Entonces la aplicación $u^{\#} : x \longrightarrow u^{\#}(x)$ es una aplicación semilineal de E en E pues:

$$\emptyset(x_1+x_2 , u(y)) = \emptyset(x_1 , u(y)) + \emptyset(x_2 , y(y)) = \overline{\emptyset(u^{\#}(x_1),y)} + \overline{\emptyset(u^{\#}(x_2),y)}$$

$$\emptyset(\lambda x,u(y)) = \lambda\, \emptyset(x , u(y)) = \overline{\bar{\lambda}\, \emptyset(u^{\#}(x) , y)} = \overline{\emptyset(\bar{\lambda}\, u^{\#}(x) , y)}$$

(#) No hemos demostrado en los cap. I ó II la fórmula ${}^tBAB$ para un cambio de base debido a que sólo sería usada aquí. Para la demostración ver cualquier texto de álgebra lineal, por ejemplo Bourbaki.

Por definición, $u^{\#}$ se denomina la adjunta de la aplicación semilineal u (respecto de la forma hermitiana ϕ).

-o-

Nuevamente, debido a que ϕ es no degenerada, si φ es una forma bilineal sobre E , para cada $x \in E$ existe un único elemento $u(x)$ en E tal que $\varphi(x,y) = \overline{\phi(u(x),y)}$ $(\forall y \in E)$ (cf. corolario del teor. 1, §1) , y es inmediato verificar (en forma parecida a la del razonamiento anterior) que la aplicación $u : x \longrightarrow u(x)$ es semilineal de E en E .

Recíprocamente, si u es una aplicación semilineal de E en E , la forma φ definida por $\varphi(x,y) = \overline{\phi(u(x),y)}$ es bilineal. La demostración es del mismo tipo ; a modo de ejemplo mostremos que:

$$\varphi(x_1+x_2 , y) = \overline{\phi(u(x_1+x_2) , y)} = \overline{\phi(u(x_1),y)} + \overline{\phi(u(x_2),y)} = \varphi(x_1,y)+\varphi(x_2,y)$$

$$\varphi(\lambda x,y) = \overline{\phi(u(\lambda x),y)} = \overline{\phi(\lambda u(x),y)} = \overline{\bar{\lambda}\phi(u(x),y)} = \overline{\lambda \phi(u(x),y)} = \lambda\varphi(x,y) .$$

Esto muestra que de esa manera se pueden poner, mediante ϕ , en correspondencia biunívoca los conjuntos de las formas bilineales sobre E y de las aplicaciones semilineales de E en E . Observemos, finalmente que en esta correspondencia ψ es alternada si y sólo si su aplicación semilineal asociada u , verifica $u^{\#} = -u$ (es decir $u^{\#}(x) = -u(x)$, $\forall x \in E$).

En efecto, si ψ es alternada se tiene:

$$\phi(u^{\#}(x),y) = \phi(x,u(y)) = \phi(u(y),x) = \psi(y,x) = -\psi(x,y) =$$

$$= -\phi(u(x),y) = \phi(-u(x),y) \quad (\forall y \in E) \text{ implica: } u^{\#}(x) = -u(x)$$

(recíprocamente, de modo similar).

-o-

13.2.- REDUCCION DE FORMAS ALTERNADAS. INVARIANTES

Teorema 1 :

Sea S una familia de aplicaciones semilineales de E en E estable para "#" es decir: $u \in S$ implica $u^{\#} \in S$. Entonces:

(a) Si V es un subespacio de E estable para S (e.i.: $u(V) \subset V$, $u \in S$) entonces el ortogonal (respecto de ϕ) V^{o} es estable para S .

(b) E se descompone en suma directa $E = E_1 \oplus \ldots \oplus E_p$ de subespacios ortogonales dos a dos y estables minimales para S , en el sentido de que si un subespacio no nulo F está contenido en un E_i y es estable para S , entonces $F = E_i$ (cf.: teorema 1 del §9).

Demostración:

(a) Si $x \in V^{o}$, $u \in S$, se tiene $\phi(y,u(x)) = \overline{\phi(u^{\#}(y),x)} = 0$ para cada $y \in V$,

lo que implica que $u(x) \in V^0$ y V^0 es estable para S .

(b) (la misma demostración de (b) del teorema 1 del §9).

Corolario:

Si u es semilineal y $u^{\#} = -u$, E se descompone en suma directa de subespacios ortogonales dos a dos y estables minimales para u . (Basta aplicar el teorema a la familia S formada por u y $-u$, observando que un subespacio es estable para u si y sólo si lo es para $-u$.)

Teorema 2 :

Si Ψ es una forma alternada sobre E , existe una base (e_i) , ortonormal para φ , tal que respecto de ella la matriz de Ψ es de la forma:

$$\begin{pmatrix}
0 & \alpha_1 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
-\alpha_1 & 0 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 0 & 0 & \alpha_2 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 0 & -\alpha_2 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & & & & & & & & & & & \\
0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & \alpha_p & 0 & & 0 & 0 \\
0 & 0 & 0 & \cdots & \cdots & \cdots & -\alpha_p & 0 & 0 & & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\
\vdots & & & & & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0
\end{pmatrix}$$

donde los α_i son números reales no negativos (sólo si $K = \mathbb{C}$).

Demostración :

Sea u la aplicación semilineal asociada a Ψ : $\Psi(x,y) = \overline{\varphi(u(x),y)}$. Sabemos que $u^{\#} = -u$, y u^2 es evidentemente lineal y además: $(u^2)^{\#} = u^{\#}u^{\#} = (-u)(-u) = u^2$, de manera que u^2 es un endomorfismo hermitiano de E . Sabemos que entonces se puede asociar a u^2 , mediante la φ , una forma hermitiana φ_u , de la cual nos interesa observar que es negativa (cf. : 9.4). En efecto:

$$\varphi_u(x,x) = \varphi(u^2(x),x) = \overline{\varphi(x,u^2(x))} = \overline{\varphi(u^{\#}(x),u(x))} =$$

$$= \overline{-\varphi(u(x),u(x))} \leq 0 \quad \text{porque } \varphi \text{ es positiva .}$$

Por el teorema 1, E se descompone en suma directa de subespacios estables minimales respecto de u. Sea V uno de ellos. Como u^2 es hermitiano, (y como V es también estable para u^2), sabemos que V contiene autovectores $x \neq 0$ de u^2: $u^2(x) = ax$ (cf.: §9). Por la observación anterior, $\phi(u^2(x),x) = a\,\phi(x,x) \leq 0$, de manera que $a \leq 0$ (porque $\phi(x,x) > 0$). Definamos entonces los vectores siguientes:

$$y = \sqrt{-a}.x + u(x) \in V$$

$$z = \sqrt{-a}.x - u(x) \in V$$

con lo cual $u(y) = -\sqrt{-a}.z$, y $u(z) = \sqrt{-a}.y$. Esto prueba que el subespacio de V engendrado por y y por z es estable para u, y por tanto es igual a V (de modo que V tiene a lo sumo dimensión 2).

Hay que distinguir dos casos: si $y = 0$ (lo cual es equivalente a $z = 0$), las expresiones de y y de z prueban que $a = 0$, es decir que $u(x) = u^{\#}(x) = 0$, y la recta Kx es estable para u, o sea $V = Kx$. Entonces, la restricción de ψ a V es una forma alternada sobre V que es de dimensión 1, y por consiguiente esa restricción es nula.

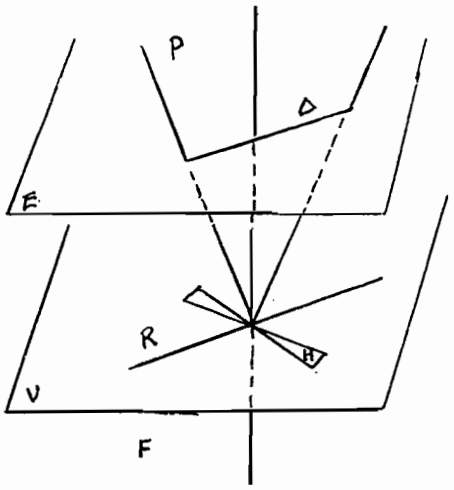
Si $y \neq 0$, también $z \neq 0$, y como $\psi(y,z) = -\sqrt{-a}\,\overline{\phi(z,z)} \neq 0$, estos vectores son linealmente independientes y V es de dimensión 2. Por otra parte, usando las relaciones ya establecidas se deduce fácilmente que $\phi(y,z) = -a\,\phi(x,x) - \phi(u(x),u(x)) = 0$, así que y y z son ortogonales (para ϕ). Sabemos que en tal caso es posible multiplicar estos vectores por escalares reales apropiados de modo de tener una base y',z', ortonormal (para ϕ) de V. Además, ψ es una forma alternada sobre V cuya matriz respecto de esa base es de la forma $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$ (con $b = \psi(y',z')$, $b \in \mathcal{R}$). Finalmente, si x_1, x_2 pertenecen a diferentes subespacios estables minimales, V_1, V_2, para u, como estos espacios son ortogonales para ϕ, se tiene $\psi(x_1,x_2) = \phi(u(x_1),x_2) = 0$. Entonces, hemos probado que E se descompone en suma directa de subespacios $V_1,\ldots,V_p$ estables minimales para u, de dimensiones 1 ó 2 que admiten bases ortonormales (para ϕ) respecto de las cuales la restricción de ψ tiene matriz (0) o matriz $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$, respectivamente, y además los V_i son ortogonales dos a dos respecto de la forma ψ y también respecto de la forma ϕ. Entonces es claro que la reunión de las bases antes mencionadas proporciona una base ortonormal (para ϕ) de E respecto de la cual la matriz de ψ es de la forma indicada en el teorema.

-o-

13.3.- REFERENCIA A LOS COMPLEJOS LINEALES

Sea V un espacio vectorial de dimensión impar: $2r+1$ sobre el cuerpo $\mathcal{R}$, y consideremos en el espacio vectorial $F = \quad xV$ una forma alternada, ψ, no degene

rada (nótese que para que tal forma exista es necesario que la dimensión de F sea par, de ahí que se supuso que la de V es impar). Se llama <u>complejo lineal proyectivo</u> asociado a Ψ al conjunto C_0 de las rectas proyectivas del espacio proyectivo $P(F)$ (es decir las variedades proyectivas de dimensión 1 de $P(F)$) que se obtienen como imágenes canónicas de los planos totalmente isótropos (respecto de la forma Ψ) de F .



Sea R la recta ortogonal a V en F (respecto de Ψ) que(por ser Ψ alternada) está contenida en V . Supongamos que en V está dada una forma ϕ bilineal simétrica positiva y no degenerada, y sea H el hiperplano de V ortogonal a la recta R respecto de ϕ . En F , el subespacio H es no isótropo (respecto de Ψ) y por tanto su ortogonal (para Ψ) es un plano P , no isótropo, tal que $F = P \oplus H$, y obviamente $R \subset P$.

Sea E el espacio afín $\{1\} \times V \subset F$. Entonces el conjunto C de las intersecciones de la forma $\Pi \cap E$ (donde Π es un plano de F totalmente isótropo para Ψ y no contenido en V) se denomina <u>complejo lineal afín</u> asociado a Ψ . (En cierto sentido, C es igual a C_0 menos sus elementos impropios). La recta $\Delta = P \cap E$ se llama <u>eje</u> del complejo lineal C respecto de la estructura de espacio euclídeo definida en E por ϕ

Esto muestra que la teoría clásica de los complejos lineales está incluída en la teoría general de las formas alternadas.

El caso más interesante se tiene cuando la dimensión de F es 4 . (cf.: Bourbaki, Alg., ch.9, §10. Ex.16) .

-o-

A P E N D I C E S

Suponemos que quien lea estos apéndices está suficientemente familiarizado con los conceptos y razonamientos del texto. Los temas que aquí se tratan (especialmente en los apéndices III y IV) presentan más dificultades que los del texto, por lo menos para el que se inicia en estas cuestiones. Debemos hacer la advertencia de que en algunos casos se utilizan conceptos de álgebra lineal sin dar sus definiciones (que no aparecen tampoco en el texto). Además, las demostraciones son bastante más concisas que las del texto. A todo aquél que desee información adicional sobre los conceptos fundamentales, remitimos a los capítulos del tratado de Bourbaki citados en la introducción.

-o-

I.- ANGULOS EN EL PLANO ORIENTADO

Aquí se completa el parágrafo 10 manteniendo su notación: E es un espacio vectorial de dimensión 2 sobre el cuerpo $\mathbb{R}$; $(x|y)$ es una forma bilineal simétrica positiva y no degenerada; (e_1, e_2) es una base ortonormal de E . Además, supondremos que el plano E está orientado, lo que significa lo siguiente:

Se sabe que al ser $\dim(E) = 2$, $E \wedge E$ es unidimensional, de modo que fijado un bivector $x \wedge y \neq 0$, existe una única semirrecta de $E \wedge E$ que lo contiene y que se llamará positiva; sus bivectores también se llaman positivos, y los de la semirrecta opuesta, negativos. Una vez que se hace esto, se dice que E es un plano orientado, o que se ha dado una orientación en E .

-o-

I.1.- TRIGONOMETRIA EN EL PLANO ORIENTADO

Como ya hemos dicho, en un plano orientado la trigonometría puede desarrollarse sin ambigüedades, como deduciremos del siguiente lema. Este prueba el hecho intuitivo de que las semejanzas directas no cambian la orientación del plano.

Lema 1 :

Dada $u \in S^+$, todos los bivectores de la forma $x \wedge u(x)$ pertenecen a una misma semirrecta de $E \wedge E$ (al variar x en E).

Demostración:

El caso en que u es una homotecia es trivial porque si es así se verifica $x \wedge u(x) = 0$ para todo x . Si u no es una homotecia, $x \wedge u(x)$ no es nulo si

$x \neq 0$. Sea y otro vector cualquiera y mostremos que $y \wedge u(y)$ es un múltiplo positivo de $x \wedge u(x)$ (que es lo que hay que demostrar). Como no hay en E vectores isótropos, existe una semejanza directa w tal que $w(x) = y$, y entonces: $y \wedge u(y) = w(x) \wedge uw(x) = w(x) \wedge wu(x) = (\det(w))(x \wedge u(x))$, con lo que queda demostrado ya que como $(x|y)$ es positiva, el determinante de w es positivo.

-o-

Si A es el álgebra de endomorfismos engendrada por las semejanzas directas, sabemos que existen en A generadores v tales que $v^2 = \delta = -1 \in \mathbb{R}$. De hecho, existen dos y sólo dos de tales aplicaciones que difieren en su signo, y por el lema precedente, hay una sola tal que para cada $x \in E$, $x\, v(x)$ es un bivector positivo. Este hecho nos permite determinar sin ambigüedades el generador v de A que hemos utilizado en el parágrafo 10 para construir la trigonometría, por eso es claro que en el plano orientado la trigonometría puede desarrollarse sin ambigüedades.

-o-

Además de las fórmulas que ya conocemos, valen en este caso otros dos resultados frecuentemente usados en la geometría elemental. Para ello, convengamos en definir el ángulo del vector x con el vector y , que designamos con $(\hat{x,y})$, como igual al ángulo de la semirrecta que contiene a x con la semirrecta que contiene a y . Hecho esto, afirmamos que valen las fórmulas:

$$\cos(\hat{x,y}) = \frac{(x|y)}{|x|.|y|} \qquad \text{e . } \operatorname{sen}(\hat{x,y}) = \frac{(x \wedge y)}{|x|.|y|}$$

donde e designa el único bivector positivo tal que la extensión $(\ |\ )_{(2)}$ de $(\ |\ )$ a $E \wedge E$ cumple: $(e|e)_{(2)} = 1$.

Para demostrar la primera fórmula, designemos, para abreviar, con x' , y' a $x/|x|$ e $y/|y|$, respectivamente. Sabemos que existe una única rotación, θ , tal que $\theta(x') = y'$, la cual está determinada por: $\theta = \cos(\hat{x,y}) + \operatorname{sen}(\hat{x,y})\, .\, v$. Entonces, usando la expresión de y' en función de x' que se deduce de $\theta(x') = y'$ tenemos:

$$(x'|y') = (x' \mid \cos(\hat{x,y})x') = \cos(\hat{x,y})$$

que es otra manera de escribir la primera fórmula.

Para demostrar la segunda, comencemos recordando que, por definición:

$$(x_1 \wedge x_2 \ ,\ y_1 \wedge y_2)_{(2)} = \begin{vmatrix} (x_1|y_1) & (x_1|y_2) \\ (x_2|y_1) & (x_2|y_2) \end{vmatrix}$$

Entonces, procediendo como antes, tenemos:

$$(x' \wedge y') = x' \wedge (\cos(\hat{x,y})x' + \operatorname{sen}(\hat{x,y})v(x')) = \operatorname{sen}(\hat{x,y})\, .\, x' \wedge v(x')$$

y recordando que v gira los vectores un ángulo recto, un cálculo directo muestra que:

$$(x' \wedge v(x') \ , \ x' \wedge v(x'))_{(2)} = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

de modo que la fórmula anterior es la que queríamos demostrar con $e = x' \wedge v(x') > 0$.

-o-

I.2.- SECTORES ANGULARES

Sean D_0 , D_1 , D_2 , tres semirrectas de E , y x_0 , x_1 , x_2 , vectores no nulos que les pertenecen, y considérense los bivectores $x_0 \wedge x_1$, $x_1 \wedge x_2$, $x_2 \wedge x_0$. Si dos de tales bivectores (por lo menos) son (estrictamente) positivos, diremos que la terna D_0 , D_1 , D_2 , es directa. (Esta noción es evidentemente independiente de cuáles son los vectores no nulos que se eligen en las semirrectas). Nótese que si D_0 , D_1 , D_2 es directa, entonces D_1 , D_2 , D_0 y D_2 , D_0 , D_1 son directas, en tanto que D_1 , D_0 , D_2 ; D_0 , D_2 , D_1 y D_2 , D_1 , D_0 no son directas.

Vamos a mostrar ahora que el hecho de tener una orientación en el plano E permite definir un orden total en el conjunto de las semirrectas distintas de una semirrecta prefijada de antemano. Sea D_0 una semirrecta fijada de una vez para siempre, y sobreentendamos que todas las semirrectas consideradas son diferentes de D_0 .

Diremos que $D_1 \leqslant D_2$ (léase: "D_1 precede a D_2") si: o bien $D_1 = D_2$, o bien la terna D_0 , D_1 , D_2 es directa. Es claro entonces que para toda semirrecta D se verifica $D \ D$; y como las ternas D_0 , D_1 , D_2 y D_0 , D_2 , D_1 no pueden ser simultáneamente directas, si $D_1 \leqslant D_2$ y $D_2 \leqslant D_1$ entonces necesariamente $D_1 = D_2$. Además, es claro que o bien $D_1 \leqslant D_2$ o bien $D_2 \leqslant D_1$, cualesquiera sean las semirrectas D_1 y D_2 . Por lo tanto, nuestra relación es un orden total si y sólo si se demuestra que es una relación transitiva, cosa que, por otra parte, no es trivial como las anteriores.

Sea e un bivector positivo que tomaremos como base de E E , y si x_0, x_1, x_2, x_3 son vectores no nulos de D_0, D_1, D_2, D_3 , escribiremos:

$$x_i \ x_j = a_{ij} \ e \qquad (i,j = 0,1,2,3)$$

Siempre puede suponerse que $e = x_0 \wedge y$, donde (x_0, y) es una base de E . Entonces, si se pasa a coordenadas:

$$x_0 = 1.x_0 + 0.y \quad , \quad x_1 = \alpha_1 x_0 + \alpha_2 y \quad , \quad x_2 = \beta_1 x_0 + \beta_2 y \quad , \quad x_3 = \gamma_1 x_0 + \gamma_2 y$$

y se calcula en función de estas coordenadas los valores a_{01} , a_{23} , a_{02} , a_{31} , a_{03}, a_{12} y luego el valor de $a_{01}a_{23} + a_{02}a_{31} + a_{03}a_{12}$ se comprueba que:

$$a_{01}a_{23} + a_{02}a_{31} + a_{03}a_{12} = 0 \qquad (\#)$$

Hecho esto, pasemos a demostrar que "$\lesssim$" es transitiva, para lo cual supondremos que $D_1 \lesssim D_2$ y $D_2 \lesssim D_3$, y demostraremos que $D_1 \lesssim D_3$. Es claro que podemos limitarnos al caso en que ninguno de los signos " " es el signo "=", de modo que el teorema puede sustituirse por este otro: si las ternas $D_0\, D_1\, D_2$ y $D_0\, D_2\, D_3$ son directas, entonces también $D_0\, D_2\, D_3$ es directa. Distinguiremos dos casos:

(1) Sea $a_{01} < 0$. Tenemos que probar que entonces a_{13} t a_{30} son positivos. Como $D_0\, D_1\, D_2$ es directa, $a_{12} > 0$ y $a_{20} > 0$, y entonces $a_{02} < 0$. Ahora, como $D_0\, D_2\, D_3$ es directa, eso implica que $a_{23} > 0$ y $a_{30} > 0$. Entonces, de los signos establecidos resulta que (#) tiene negativos su primer y tercer términos, y como además a_{02} es negativo, a_{13} 0, l.q.q.d.

(2) Sea $a_{01} > 0$. Si además fuera $a_{30} > 0$, $D_0\, D_1\, D_3$ sería directa y el teorema estaría demostrado. Si, en cambio, $a_{30} < 0$, como $D_0\, D_2\, D_3$ es directa, resulta que $a_{02} > 0$ y $a_{23} > 0$. Entonces $a_{20} < 0$ y como $D_0\, D_1\, D_2$ es directa, tiene que ser $a_{12} > 0$. Entonces, usando estos signos en la relación (#), se deduce que $a_{31} < 0$, es decir $a_{13} > 0$ lo cual junto con la suposición inicial prueba que $D_0\, D_1\, D_3$ es directa, l.q.q.d.

-o-

Dadas dos semirrectas D_1, D_2 (distintas) llamamos sector angular (abierto) de origen D_1 y extremo D_2 al conjunto de las semirrectas D tales que la terna $D_1\, D\, D_2$ es directa. Si se agregan a este conjunto las semirrectas D_1, D_2, el conjunto obtenido se denomina sector angular cerrado de origen D_1 y extremo D_2. Usando la relación de orden que hemos definido entre semirrectas, podemos afirmar que el sector de origen D_1 y extremo D_2 coincide con el conjunto de las D tales que $D_1 < D < D_2$ para la relación de orden definida por cualquier semirrecta D_0 tal que $D_0\, D_1\, D_2$ sea directa. (Demostración a cargo del lector).

-o-

Teorema 1 :

Con la notación de antes, el conjunto totalmente ordenado de las semirrectas distintas de D_0 es isomorfo al cuerpo totalmente ordenado

Demostración :

Todo consiste en definir una función f de $\mathcal{R}$ en el conjunto de las semirrectas diferentes de D_0 de modo que sea suryectiva y estrictamente creciente. Para ello, elegimos una base de E formada por un vector x_0 de la semirrecta opuesta a D_0 y otro vector y tal que x_0 y sea positivo. Para cada número real t, definimos $f(t)$ igual a la semirrecta que pasa por el punto $(1-t^2)x_0 + 2ty$. Es claro que $f(t)$ nunca puede coincidir con D_0, de modo que f va efectivamente en el conjun-

to de las semirrectas distintas de D_o

Veamos que f es estrictamente creciente, es decir que la relación t t' implica que la terna D_o , $f(t)$, $f(t')$ es directa. Para ello, usemos los vectores de cada semirrecta que fueron usados arriba al definir la función f , expresando los bivectores correspondientes mediante el escalar que multiplica al bivector positivo x_o y . Vemos que D_o , $f(t)$, $f(t')$ es directa si y sólo si dos de los números

$$-2t \quad , \quad (1-t^2).2t - (1-t'^2).24 \quad , \quad 2t'$$

son positivos. Ahora bien, si t y t' tienen signo distinto, la hipótesis dice que $-2t$ y $2t'$ son positivos. Luego, notando que el segundo número es igual a $(t'-t)(1+tt').2$, si t y t' son del mismo signo, este segundo número es positivo. Si se da el caso $t'>0$, el tercer número es también positivo; si, en cambio, $t'<0$, es el primero el otro que es positivo, l.q.q.d.

Para terminar, debemos mostrar que f es suryectiva, es decir que si D es una semirrecta diferente de D_o , existe un número real t tal que $f(t) = D$. Sabemos que si D es diferente de D_o , existe un único ángulo φ tal que $2\varphi = (-D_o\hat{}, D)$, donde $-D_o$ designa la semirrecta opuesta de D_o . Además, como el ángulo $(-D_o\hat{}, D)$ no es el llano porque $D \neq D_o$, resulta que φ no es el ángulo recto, y por consiguiente su tangente, t , no es infinita. Entonces, una de las semejanzas asociadas a 2φ lleva el punto x_o sobre el punto $(1-t^2)x_o + 2ty$, lo que prueba que $D = f(t)$.

Así, el teorema está completamente demostrado.

-o-

II.- ALGEBRAS DE CLIFFORD, CUATERNIONES Y GRUPO ORTOGONAL

Por razones de simplicidad, supondremos aquí que K es un cuerpo conmutativo de característica distinta de 2 , y E es un espacio vectorial de dimensión finita, n, (particularmente $n = 2$ ó $n = 3$); ϕ designa una forma bilineal simétrica no degenerada sobre E , y Q la forma cuadrática asociada.

II.1.- ALGEBRA DE CLIFFORD

Supongamos que existe un álgebra con unidad, 1 , sobre el cuerpo K tal que el espacio vectorial E puede "sumergirse" en ella, es decir existe una inyección de E en el álgebra que permite identificar E con una parte del álgebra, y supongamos además que vale la condición:

$$x.x = \phi(x,x) \, . \, 1 \qquad (\forall x \in E) \qquad (C)$$

(es decir, pensando el elemento x como perteneciente al álgebra, su cuadrado es igual al múltiplo de la unidad según el escalar $\phi(x,x)$), y que E engendra el álgebra total. Una tal álgebra, que notaremos con $C(\phi)$, y que, bajo ciertas condiciones se puede demostrar que existe y es única salvo isomorfismo, se llama el álgebra de Clifford de E provisto de ϕ (#) .

De la condición (C) se pueden deducir inmediatamente estas otras propiedades:

(1) Para todo x y para todo y en $E \subset C(\phi)$ vale:

$$x.y + y.x = 2\,\phi(x,y).1$$

(para demostrarlo, usar que $(x+y).(x+y) = \phi(x+y\ ,\ x+y)\ .\ 1$, desarrollar ambos miembros y simplificar).

(2) Para que dos vectores x e y de E sean ortogonales (para ϕ) es necesario y suficiente que:

$$x.y = -y.x$$

(consecuencia trivial de (1)).

(3) Para que $x \in E$ tenga inverso x^{-1} en el álgebra $C(\phi)$ es necesario y suficiente que x no se isótropo, y en tal caso:

$$x^{-1} = \frac{x}{\phi(x,x)}$$

(también consecuencia trivial de (C)).

-o-

Sabemos que si H es un hiperplano no isótropo de E y a es un vector no nulo ortogonal a H , la simetría s_a respecto de H está definida por:

$$s_a(x) = x - 2\,\frac{\phi(x,a)}{\phi(a,a)}\ .\ a \qquad \text{(cf.: 6.5 al final)}$$

Consideremos entonces el elemento $a.x.a^{-1} \in C(\phi)$ (imagen de x por el automorfismo interior definido por el elemento inversible a). Usando (3) tenemos:

$$a.x.a^{-1} = \frac{a.x.a}{\phi(a,a)} = a.x.\frac{a}{\phi(a,a)} = (2\,\phi(x,a).1 - x.a)\,\frac{a}{\phi(a,a)} =$$

$$= 2\,\frac{\phi(x,a)}{\phi(a,a)}\ .\ a - x\ .\ \frac{a.a}{\phi(a,a)} = -x + 2\,\frac{(x,a)}{\phi(a,a)}\ .\ a = -s_a(x)$$

Así que (excepto por un signo) la simetría respecto del hiperplano ortogonal a a es la restricción a E del automorfismo interior del álgebra de Clifford definido por a : $x \longrightarrow a.x.a^{-1}$.

(#) Para la definición general, existencia y desarrollo de la teoría en forma más precisa, ver Bourbaki , Alg. Ch.9, §9 .

Es bien conocido, y lo demostraremos en el apéndice IV, que toda transformación ortogonal de E , u es de la forma:

$$u = s_{a_1} \cdot s_{a_2} \cdots s_{a_k}$$

donde s_{a_i} es la simetría respecto del hiperplano ortogonal al vector no isótropo a_i.

Entonces, usando el resultado anterior y razonando por inducción completa, se deduce que si se piensa E contenido en $C(\emptyset)$, la transformación u está definida por:

$$u(x) = (-1)^k a_1 a_2 \ldots a_k x a_k^{-1} \ldots a_2^{-1} a_1^{-1}$$

es decir que para cada u $\phi(Q)$ existe un elemento $b = a_1 \ldots a_k \in C(\emptyset)$ tal que u es (salvo el signo) la restricción a E del automorfismo interior definido por b : $u(x) = \pm\, b.x.b^{-1}$. Recíprocamente, si b es un elemento inversible de $C(\emptyset)$ cuyo automorfismo interior deja E invariante (es decir: $bxb^{-1} \in E$ para cada $x \in E$), entonces la restricción a E de este automorfismo es una transformación ortogonal.

En efecto, si $bxb^{-1} \in E$ podemos escribir:

$$\emptyset(bxb^{-1}\,,\, bxb^{-1})\, 1 = bxb^{-1}\, bxb^{-1} = bxxb^{-1} = b.\emptyset(x,x).1.b^{-1} = \emptyset(x,x).1$$

lo que implica: $\emptyset(bxb^{-1}, bxb^{-1}) = \emptyset(x,x)$ para cada $x \in E$.

-o-

Sea $e_1, e_2, \ldots, e_n$ una base ortogonal de E , y pongamos $\alpha_i = \emptyset(e_i, e_i)$. Por definición, el álgebra de Clifford, $C(\emptyset)$, está engendrada por los elementos $1, e_1, \ldots, e_n$, y estará perfectamente determinada una vez que se de la tabla de multiplicación correspondiente. En todo lo que sigue, identificaremos también K a una parte de $C(\emptyset)$ mediante la inyección: $\lambda \longrightarrow \lambda.1$, donde 1 es la unidad de $C(\emptyset)$. Entonces, es claro que la condición (C) equivale a éstas:

$$e_i.e_i = \alpha_i \in K \qquad e_i.e_j = -e_j.e_i \qquad (j \neq i)$$

De aquí resulta que, si bien $C(\emptyset)$ no es conmutativa, es posible reordenar los factores e_i de un producto cualquiera siempre que se anteponga (según corresponda) un signo + o un signo - . Por ejemplo:

$$e_1e_2e_5e_7e_3 = e_1e_2e_5(-e_3e_7) = -e_1e_2(e_3e_5)e_7 = e_1(-e_3e_2)e_5e_7 = -e_1e_3e_2e_5e_7 =$$

$$= e_3e_1e_2e_5e_7$$

Eso cuando los factores son distintos, y si hay dos iguales se tiene resultados como éste:

$$e_2e_1e_4e_3e_1 = -e_2e_1e_4e_1e_3 = e_2e_1e_1e_4e_3 = \alpha_1 e_2e_4e_3$$

Por consiguiente, todo elemento de $C(\emptyset)$ es o bien un escalar, o bien el producto de un escalar por un elemento de la forma: $e_i e_j \ldots e_p$ $(i < j < \ldots < p)$. Por otra parte, se puede demostrar que $1, e_1, \ldots, e_n$ y los productos de dos o más elementos que son de esa forma son linealmente independientes, de modo que constituyen una base de $C(\emptyset)$. Pero se ve (haciendo corresponder 1 a la parte vacía) que esos elementos están en correspondencia biunívoca con el conjunto de partes del conjunto $\{e_1, \ldots, e_n\}$, y por lo tanto son en total 2^n . Esto demuestra que el álgebra de Clifford (si existe) de un espacio de dimensión n tiene dimensión 2^n .

-o-

II.2.- CASO $n = 2$

Suponemos aquí que E es de dimensión 2 . Si aplicamos el razonamiento precedente a una base ortogonal (e_1, e_2) llamando $e_3 = e_1 e_2$ al cuarto generador del álgebra de Clifford, se ve que ésta está definida por la tabla de multiplicación siguiente:

		2^o f.		
1^o f.	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	α_1	e_3	$\alpha_1 e_2$
e_2	$+e_2$	$-e_3$	α_2	$-\alpha_2 e_1$
e_3	e_3	$-\alpha_1 e_2$	$\alpha_2 e_1$	$-\alpha_1 \alpha_2$

que es justamente la del álgebra de cuaterniones generada por $u = e_1$, $v = e_2$ y $w = e_3$, relativa al par $(\alpha, \beta) = (\alpha_1, \beta_2)$.

En general (para cualquier álgebra de Clifford) la relación $bxb^{-1} = b'xb'^{-1}$ $(x \in E)$ es equivalente a $cx = xc$ (con $c = b'^{-1}b$) , de modo que para que b y b' definan una misma transformación ortogonal de E es necesario que c conmute con todos los x de E . Para esto, si escribimos c en la forma $\lambda_0 + \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3$, se tiene que cumplir en particular:

$$(\lambda_0 + \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3)\, e_1 = \lambda_0 e_1 + \lambda_1 a_1 - \lambda_2 e_3 - \alpha_1 \lambda_3 e_2 =$$

$$= \lambda_0 e_1 + \lambda_1 a_1 + \lambda_2 e_3 + \alpha_1 \lambda_3 e_2 = e_1(\lambda_0 + \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3)$$

y relaciones análogas con e_2 , e_3 en lugar de e_1 . De ellas resulta inmediatamente que $\lambda_1 = \lambda_2 = \lambda_3 = 0$, es decir que c es un escalar: $c = {}_0.1$. Esto prueba dos cosas: los elementos de $C(\emptyset)$ que definen una misma transformación ortogonal son proporcionales, y, el centro de $C(\emptyset)$ está formado por los escalares : $c = \lambda.1$.(#) .

(#) Este resultado vale en general para todo n .

En el caso general (dim (E) = n) tienen importancia fundamental los subespacios vectoriales de $C(\emptyset)$ definidos así:

$C^+(\emptyset)$ = (subespacio engendrado por los productos de la forma $e_{i_1}e_{i_2}\dots e_{i_{2k-1}}$ con un número par de factores)

$C^-(\emptyset)$ = (subespacio engendrado por 1 y los productos de la forma $e_{i_1}\dots e_{i_{2k}}$ con un número impar de factores)

Es claro que $C = C^+ \oplus C^-$, $C^-.C^- \subset C^+$, $C^+.C^+ \subset C^+$, $C^+C^- \subset C^-$ y $C^-C^+ \subset C^-$. Veamos la importancia de estos subespacios en nuestro caso de dimensión 2 . Sabemos que las transformaciones ortogonales son restricciones a E de ciertos automorfismos interiores de $C(\emptyset)$. Más precisamente, las simetrías, son los automorfismos: $x \longrightarrow -axa^{-1}$ que corresponden a un vector $a \in E$, no isótropo. Veremos en el apéndice IV (cf. Ap. IV, teor. 2), que toda rotación de E es un producto de dos simetrías, de modo que toda rotación es de la forma: $x \longrightarrow (a_1a_2)x(a_1a_2)^{-1}$. Ahora bien, todo elemento de E se escribe en la forma: $a = \lambda_1 e_1 + \lambda_2 e_2$, de modo que los 'a que definen simetrías pertenecen necesariamente a C^- . Y el producto de dos elementos de E es de la forma: $a_1a_2 = \lambda_0 + \lambda_3 a_3$ (para demostrarlo basta multiplicar) , de modo que los elementos de $C(\emptyset)$ que definen rotaciones de E pertenecen necesariamente a C^+ .

-o-

Sabemos que si $x \neq 0$ implica $N(x) \neq 0$, el álgebra de cuaterniones $C(\emptyset)$ es un cuerpo. Evidentemente, esa condición no se satisface si E admite vectores isótropos, de modo que conviene ver cómo es el álgebra de Clifford en este caso.

Si E admite vectores isótropos, sabemos que necesariamente tiene dos (y sólo dos) rectas isótropas distintas, y que se puede elegir una base de E , f_1 , f_2 , formada por vectores isótropos y tal que $\emptyset(f_1,f_2) = \emptyset(f_2,f_1) = 1$. Entonces en el álgebra de Clifford se verifican las relaciones: $f_1f_1 = f_2f_2 = 0$, y $f_1f_2+f_2f_1 = 1$. Entonces, si tomamos como cuarto generador a $f_3 = f_1f_2$, se construye fácilmente la siguiente tabla de multiplicación que define a $C(\emptyset)$:

		2^o f.		
1^o factor	1	f_1	f_2	f_3
1	1	f_1	f_2	f_3
f_1	f_1	0	f_3	0
f_2	f_2	$1-f_3$	0	f_2
f_3	f_3	f_1	0	f_3

Consideremos ahora el álgebra de matrices $M_2(K)$ cuadradas de orden 2 , que sabemos es un espacio vectorial de dimensión 4 sobre K (igual dimensión que $C(\emptyset)$) que tiene como base canónica la formada por las unidades matriciales: $E_{11} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$,

$E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ y $E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Entonces, usando la definición del producto de matrices, se ve en seguida que si se identifica: $f_1 = E_{21}$, $f_2 = E_{12}$, $f_3 = E_{22}$ y $1 = E_{11}+E_{22} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, la tabla de multiplicación del álgebra de Clifford coincide con la tabla de multiplicación de $M_2(K)$. Esto prueba que si el índice de $\emptyset$ es 1 , el álgebra de Clifford de E es isomorfa a $M_2(K)$ y por tanto también isomorfa al álgebra de los endomorfismos de E , (E) .

-o-

II.3.- CASO $n = 3$

Sea como siempre (e_1, e_2, e_3) una base ortogonal de E , que ahora suponemos de dimensión 3 . Como sabemos, el álgebra de Clifford, $C(\emptyset)$, tiene en este caso dimensión S , pero en cambio la subálgebra $C^+(\emptyset)$ tiene como base a 1 , $i_1 = e_2e_3$, $i_2 = e_3e_1$ y $i_3 = -\alpha_3 e_1e_2$ (luego veremos el por qué de elegir así los elementos de la base) y por consiguiente tiene dimensión 4 (como ocurría con la $C(\emptyset)$ del caso de dimensión 2). La tabla de multiplicación de C^+ se determina por el mismo procedimiento que ya hemos utilizado en otros casos y se tiene:

$$i_1^2 = e_2e_3e_2e_3 = -e_2e_3e_3e_2 = -\alpha_3\alpha_2 = \beta_1$$

$$i_2^2 = e_3e_1e_3e_1 = -e_3e_1e_1e_3 = -\alpha_1\alpha_3 = \beta_2$$

$$i_3^2 = \alpha_3^2 e_1e_2e_1e_2 = -\alpha_3^3\alpha_1 e_2e_2 = -\alpha_3^2\alpha_1\alpha_2 = -\beta_1\beta_2$$

y análogamente, $i_1i_2 = i_3$, $i_2i_3 = -\beta_2 i_1$, $i_3i_1 = -\beta_1 i_2$. Esto prueba que C^+ es el álgebra de cuaternios con base $(1, i_1, i_2, i_3)$ relativa al par (β_1, β_2) .

-o-

Designemos con I el subespacio de C^+ (hiperplano) de los cuaternios puros, es decir los $z \in C^+$ tales que $z = -\bar{z}$ (o también los cuaternios que tienen la parte escalar nula), y con j el elemento $e_1e_2e_3$ de $C(\emptyset)$ (el "octavo" elemento de la base). Entonces decimos que la aplicación $x \longrightarrow x.j$ es una biyección de E en P . En efecto, basta observar que:

$$e_1.j = e_1e_1e_2e_3 = \alpha_1 i_1 \quad , \quad e_2.j = \alpha_2 i_2 \quad , \quad e_3.j = -i_3$$

lo que prueba que la base de E se corresponde con la base de P y como la aplicación es lineal, es una biyección.

Ya vimos que para que un elemento $b \in C(\emptyset)$ defina una transformación ortogonal es necesario que sea inversible. Recíprocamente, podemos demostrar ahora que si $b \in C^+$ y si b es inversible, entonces $bxb^{-1} \in E$ para cada $x \in E$, o sea b define una transformación ortogonal. En otras palabras: para que un elemento de C^+ defina una transformación ortogonal es necesario y suficiente que sea inversible. La demostración resulta de que $bxb^{-1} = b(xj)b^{-1}j^{-1} = bpb^{-1}j^{-1} = p'j^{-1} \in E$, porque P es invariante

respecto de automorfismos interiores, es decir que siendo $p = xj$ un cuaternio puro, entonces también $p' = bpb^{-1}$ es un cuaternio puro, de modo que $p'j^{-1}$ es un elemento de E.

Ya vimos que si dos elementos de $C(\emptyset)$ definen la misma transformación ortogonal, entonces son proporcionales; ahora como (Ap. IV) toda rotación es producto de un número par de simetrías, proviene de un elemento de C^+, y, análogamente las transformaciones ortogonales de determinante -1 provienen de elementos de C^-, se sigue fácilmente que si $(C^+)^\#$ es el grupo multiplicativo de los elementos inversibles de C^+, entonces $\phi^+(Q)$ es isomorfo a $(C^+)^\#/K^\#$. Si suponemos además que el índice de $\emptyset$ es 1, sabemos que C^+ es isomorfa a $M_2(K) \approx \mathcal{L}(E)$, de modo que $(C^+)^\#$ es isomorfa al grupo $GL(2,K)$. Esto prueba que si el índice de $\emptyset$ es 1, el grupo de las rotaciones en tres dimensiones $\phi^+(3,K) \approx (C^+)^\#/K$ es isomorfo al grupo proyectivo $PGL(2,I) \approx GL(2,K)/(\text{centro de } GL(2,K))$ (porque el centro de $GL(2,K)$ está formado por matrices diagonales y es entonces isomorfo a K).

-o-

III.- TEOREMA DE WITT

En este apéndice se completa el §4, de modo que se hacen las mismas hipótesis generales que allí, y también se usa la misma notación. Además, se supondrá que $\emptyset$ cumple la hipótesis de (4.3)).

III.1.- ENDOMORFISMOS METRICOS

De acuerdo con lo convenido, $\emptyset$ es una forma ξ-hermitiana sobre un espacio vectorial E de dimensión finita, n, sobre el cuerpo conmutativo K. Sea $\emptyset'$ una forma ξ-hermitiana sobre otro espacio vectorial E' de dimensión n' sobre K. Entonces, toda aplicación lineal u de E en E' se denomina homomorfismo métrico (respecto de $\emptyset$, $\emptyset'$) si para cada x y para cada y en E se verifica: $\emptyset'(u(x), u(y)) = \emptyset(x,y)$. (Esta definición no necesita que las formas sean no degeneradas, ni tampoco que sean ξ-hermitianas, pudiendo extenderse sin cambios a formas sesquilineales cualesquiera).

Teorema 1 :

Si $\dim(E) = \dim(E')$ y $\emptyset$ y $\emptyset'$ son no degeneradas, entonces todo homomorfismo métrico $u : E \longrightarrow E'$ es un isomorfismo (métrico)

Demostración:

Si $u(x) = 0$, para cada y E se tiene $\emptyset(x,y) = \emptyset'(0,u(y)) = 0$ y por lo tanto

eso implica $x = 0$, es decir que el núcleo de u es $\{0\}$ y por lo tanto es inyectiva. Eso demuestra el teorema porque los espacios son de la misma dimensión.

-o-

III.2.- TEOREMA DE WITT

Si $\dim(E) = \dim(E')$, si φ , φ' son ε-hermitianas no degeneradas que cumplen la condición (T) de (4.3) y si existe un isomorfismo métrico de E sobre E' , entonces todo isomorfismo métrico (es decir homomorfismo métrico inyectivo) de un subespacio F de E en E' puede prolongarse en un isomorfismo métrico de E sobre E'. (La demostración que sigue puede aplicarse aún en el caso más general en que K no es conmutativo e incluso si su característica es igual a 2).

Demostración:

Comencemos realizando la observación de que si E y E' son isomorfos, podemos limitarnos al caso $E = E'$, $\varphi = \varphi'$, es decir a probar que si u es un homomorfismo métrico inyectivo de un subespacio F de E en E , entonces u puede prolongarse a todo E , manteniendo su carácter inyectivo.(#)

Procederemos por pasos:

(1) Si F_1 , F_2 son subespacios de E con intersección reducida a $\{0\}$, si u_1, u_2 son homomorfismos métricos de F_1 , F_2 en E , respectivamente, y si $\varphi(u_1(x_1),u_2(x_2)) = \varphi(x_1,x_2)$ $(\forall x_1 \in F_1$, $\forall x_2 \in F_2)$, entonces el homomorfismo u : $x = x_1+x_2 \longrightarrow u_1(x_1) + u_2(x_2)$ es un homomorfismo métrico de $F_1 \oplus F_2$ en E que prolonga u_1 y u_2 . La afirmación es prácticamente inmediata porque:

$$\varphi(x_1+x_2 \, , \, y_1+y_2) = \varphi(x_1,y_1) + \varphi(x_1,y_2) + \overline{\varphi(y_1,x_2)} + \varphi(x_2,y_2)$$

y

$$\varphi(u_1(x_1)+u_2(x_2) \, , \, u_1(y_1)+u_2(y_2)) =$$

$$= \varphi(u_1(x_1) \, , \, u_1(y_1)) + \varphi(u_1(x_1) \, , \, u_2(y_2)) + \varepsilon\,\overline{\varphi(u_1(y_1),u_2(x_2))} + \varphi(u_2(x_2),u_2(y_2)) =$$

$$= \varphi(x_1,y_1) + \varphi(x_1,y_2) + \varepsilon\,\overline{\varphi(y_1,x_2)} + \varphi(x_2,y_2) \, .$$

Además, si u_1 y u_2 son inyectivos y también $u_1(F_1) \cap u_2(F_2) = \{0\}$, entonces u es inyectiva. En efecto, la última hipótesis significa que la suma de $u_1(F_1)$ y $u_2(F_2)$ es directa, de modo que la suposición $u(x) = u_1(x_1) + u_2(x_2) = 0$ implica simultáneamente $u_1(x_1) = 0$ y $u_2(x_2) = 0$ de modo que si ambos homomorfismos son inyectivos, es $x_1 = 0$ y $x_2 = 0$ y también $x = 0$. Esto dice que el núcleo de u es $\{0\}$, de

(#) Puede descartarse el caso en que $u(x) = x$ en F pues entonces la prolongación es evidente.

modo que u es inyectivo.

(2) Estudiemos ahora el caso particular en que u es un homomorfismo inyectivo de F en E tal que deja fijos todos los puntos de un hiperplano U de F (#). En este caso el teorema de Witt puede demostrarse con cierta facilidad:

Por la hipótesis, todo supelementario de U en F es una recta, de donde se sigue que el conjunto de los elementos de la forma $\{u(x) - x\}$ $(x \in F)$ es una recta que llamaremos D. Observemos entonces que si pudiera hallarse un subespacio F' ortogonal a D que tenga intersección nula con F y tal que además $F' \cap u(F) = \{0\}$, lo dicho en (1) nos permitiría extender u a $F+F'$. En efecto, comencemos observando que, por la definición de U y de D : $\varphi(u(x),y) - \varphi(x,y) = \varphi(u(x)-x\ ,\ y) = 0$ para cada y en F', de modo que si F' se elige como se indicó arriba puede aplicarse (1) con F en lugar de F_1, F' en lugar de F_2, u en lugar de u_1 y la identidad de F' en lugar de u_2. Pero podemos decir más: no sólo u puede extenderse a $F+F'$ sino que esto puede hacerse de modo que la extensión de u deje fijos cada uno de los puntos de F', y por tanto se sigue cumpliendo para la extensión que $D = \{u(x)-x \ /\ x \in F+F'\}$. Y por último debemos notar que se tiene la propiedad siguiente:

$$\text{si } x,y \in F : \quad \varphi(u(x)\ ,\ u(y)) = \varphi(u(x)\ ,\ u(y)) - \varphi(u(x),y) = \tag{\#}$$

$$= \varphi(x,y) - \varphi(u(x),y) = \varphi(x-u(x)\ ,\ y)$$

que nos dice que si x U (o sea $u(x) = x$) entonces $\varphi(x,u(y)-y) = 0$ para cada $y \in F$. En otras palabras: U está contenido en el ortogonal a D en F, y por tanto, con mayor razón, $U \subset D^0$.

(2a) Observado esto, supongamos que además F no está contenido en D^0. Tomemos entonces un x de F que no sea ortogonal a D. Para cada $y \in F$, la fórmula (#) nos dice que $\varphi(y-u(y),x) \neq 0$ implica $\varphi(u(x),u(y)-y) \neq 0$ y por lo tanto tampoco $u(F)$ está contenido en D^0. Eso implica que $F \cap D^0 = u(F) \cap D^0 = U$, y por tanto, si se elige F' de modo que sea un suplementario de U en D^0, F' verifica las condiciones indicadas al comienzo de (2), de modo que sabemos que u puede extenderse en un homomorfismo inyectivo de $F+F'$ en E. Pero $F+F'$, por lo que hemos dicho, contiene a D^0 y es distinto de D^0, y D^0 es un hiperplano de E. Esto significa que necesariamente $F+F' = E$, es decir que u puede extenderse a un homomorfismo inyectivo de E en E, y por lo tanto el teorema de Witt está demostrado en este caso.

(2b) Supongamos ahora que F está contenido en D^0. Usando la fórmula (#), vemos que si x e y son puntos de F, la relación $\varphi(u(y)-y,x) = 0$ implica $\varphi(u(y),u(x)-x) = 0$, que nos dice que también $u(F)$ está contenido en D^0. Entonces, como D es igual a $\{u(x)-x\}$ $(x \in F)$, también $D \subset D^0$, así que D es una

(#) Se descarta, como siempre, el caso $u(x) = x$ en todo x de F.

recta isótropa. Para encontrar ahora un subespacio F' en las condiciones indicadas al comienzo de (2), busquemos un suplementario (en D^0) de F y $u(F)$. La existencia de un tal suplementario es obvia si $F = u(F)$. Si $F \neq u(F)$ razonamos así: Sea x un elemento de F que no pertenece a U, y sea y un elemento de $u(F)$ que tampoco pertenece a U. Por la definición de U, sabemos entonces que $F = U+Kx$, $u(F) = U + Ky$, y es claro que $x+y$ no puede pertenecer a F porque y no pertenece a U (si $x+y \in F$, $y = x+y - x \in F$ $u(F) = U$), y análogamente, $x+y$ tampoco puede pertenecer a $u(F)$. Esto significa que $K(x+y)$ es una recta que es a la vez suplementaria de F y de $u(F)$ en el subespacio $F+u(F)$. Entonces, tomando un sumplementario G de $F+u(F)$ en D^0, el subespacio $F' = G + K(x+y)$ es simultáneamente suplementario de F y de $u(F)$ en D^0.

Es claro que F' verifica las condiciones indicadas al comienzo de (2), de modo que u puede extenderse a $F+F' = u(F) + F' = D^0$. Además, si v es la prolongación de u como homomorfismo métrico inyectivo de D^0 en E, tenemos que $v(x_F, x'_{F'}) = v(x_F)+ + x'_F$ (porque como ya vimos, la prolongación de u dejaba fijos los puntos de F'). Esto significa que $v(D^0) = D^0$ (teorema 1).

Así, hemos conseguido reducir la demostración del teorema de Witt a este caso: tenemos un automorfismo métrico, v, de un hiperplano (que antes era D^0, pero que ahora notamos con F) de E y queremos prolongarlo a un automorfismo métrico de E. (Por construcción, v deja fijos los puntos de un hiperplano V de D^0).

Para resolver este problema, vamos a basarnos en lo dicho al comienzo de (2). Comencemos demostrando que si $z \in E$, existe $z' \in E$ tal que $\phi(u(x),z') = \phi(x,z)$ para todo x en F. En efecto, la aplicación que a cada $x \in F$ hace corresponder el escalar $\phi(u^{-1}(x),z)$ es una forma lineal sobre F que es restricción a F de una forma lineal sobre E. Y sabemos que todas las formas lineales sobre E pueden escribirse como aplicaciones del tipo: $x \longrightarrow \phi(x,z')$ (cf.: Cor. del teor. 1, 1), l.q.q.d. Pero podemos hacer más: si se supone que z no pertenece a F puede elegirse z'' tal que: $z'' \notin F$, $\phi(u(x),z'') = \phi(x,z)$ para todo $x \in F$ y $\phi(z'',z'') = \phi(z,z)$. Decimos que eso puede lograrse con $z'' = x' + u(y) - y$ siempre que se elija apropiadamente y en F. En primer lugar, como $y \in F = D^0$, ya vimos que $u(y) - y \in D$, y entonces $\phi(u(x),u(y)-y) = 0$, de modo que también $\phi(u(x),z'') = \phi(x,z)$. Además, como $z' \in F = D^0$, podemos aplicar a D el lema 1 de 4.4 que nos dice que se puede sumar a z' un elemento de D de modo de tener un z'' tal que $\phi(z'',z'') = \phi(z,z)$, y como todos los elementos de D son de la forma $u(y)-y$, con y en $F = D^0$, la afirmación queda demostrada.

Entonces podemos tomar $F' = Kz$ y prolongar v a todo E mediante lo dicho en (1), poniendo, en F', $v'(z) = z''$, etc. Esto prueba también el teorema de Witt en este caso.

(3) Para demostrar el teorema de Witt en el caso general, usaremos lo demostrado en (2), (2a) y (2b) para razonar por recurrencia sobre $r = \dim(F)$. Observemos que el teorema es obvio si $r = 0$ pues basta tomar, por ejemplo, u igual a la identidad de E.

Sea U un hiperplano de F, y u_o la restricción de u a U. Entonces, por la hipótesis de recurrencia, existe un automorfismo métrico de E, v_o, que prolonga a u_o. Entonces, $v_o^{-1}u$ es un homomorfismo métrico inyectivo de F en E que deja fijos cada uno de los puntos de U y estamos dentro del caso especial demostrado en (2). Sabemos que existe un automorfismo métrico de E, v_1, que prolonga a $v_o^{-1}u$ y se sigue, obviamente, que el automorfismo métrico de E $v_o v_1$ prolonga u. El teorema está demostrado.

-o-

III.3.- APLICACION

Sean V, W, V_1, W_1, subespacios totalmente isótropos de E, todos de la misma dimensión, y tales que los subespacios $V+W$ y V_1+W_1 son no isótropos. Entonces, existe un automorfismo métrico de E tal que $u(V) = V_1$, $u(W) = W_1$. Este teorema es importante porque permite garantizar la existencia de transformaciones ortogonales que superponen ciertos elementos isótropos, cosa que de otro modo no puede lograrse en general (pero que puede ser bastante fácil cuando los elementos son no isótropos). En el apéndice IV haremos uso frecuente de esta propiedad y diremos solamente como justificación: "existe, por el teorema de Witt, una transformación ortogonal tal que..." etc.

Para demostrar aquella afirmación, recordemos que existen bases (e_i), (f_j) de V, W, respectivamente, tales que $\phi(e_i,f_j) = \delta_{ij}$. Ahora, si $e' \in V_1$, sabemos que $e' \notin W_1^o$, de modo que (lema 1 de 4.4) se puede sumar a e' un elemento f' de W_1 de tal modo que

$$\phi(e'+f', e'+f') = \phi(e',f') + \varepsilon\overline{\phi(e',f')} = \delta_{ij} + \varepsilon\overline{\delta_{ij}}$$

de donde se deduce fácilmente que existen bases (e_i'), (f_j') de V_1, W_1, respectivamente, tales que $\phi(e_i',f_j') = \phi(e_i,f_j)$ y, obviamente, tales que $\phi(e_i',e_j') = \phi(e_i,e_j) = \phi(f_i',f_j') = \phi(f_i,f_j) = 0$. Entonces, si se define $u(e_i) = e_i'$, y $u(f_j) = f_j'$, resulta que u es un homomorfismo métrico inyectivo de $V+W$ sobre V_1+W_1 tal que $u(V) = V_1$ y $u(W) = W_1$, y luego, prolongando a todo E mediante el teorema de Witt, la propiedad queda demostrada.

-o-

IV.- ESTRUCTURA DEL GRUPO ORTOGONAL Y DEL GRUPO PROYECTIVO ORTOGONAL

Aquí se hace un estudio más o menos profundo del grupo ortogonal definido en el §6. Se mantienen las hipótesis y notaciones de ese parágrafo: E es un espacio vectorial de dimensión n sobre un cuerpo conmutativo, K , de característica distinta de 2 ; ϕ , una forma bilineal simétrica no degenerada sobre E ; Q , la forma cuadrática asociada a ϕ . Como los cuerpos finitos de 2 y 3 elementos, $\mathcal{F}_2$, $\mathcal{F}_3$ constituyen casos excepcionales, supondremos que K tiene por lo menos cinco elementos.

IV.1.- GENERADORES DEL GRUPO ORTOGONAL

Lema 1 :

Sea a E , u una transformación ortogonal; si u(a) - a no es isótropo, la simetría s respecto del hiperplano H ortogonal a u(a) - a verifica su(a) = a ; si u(a) - a es isótropo pero a no es isótropo, entonces u(a) + a no es isótropo y si s' es la simetría del hiperplano ortogonal a u(a) + a , se tiene a'u(a) = = -a .

Demostración:

Todo se reduce a aplicar la fórmula de la simetría respecto de un hiperplano. La simetría respecto de H es de la forma $s(x) = x - 2\frac{\phi(x,u(a)-a)}{\phi(u(a)-a,u(a)-a)}.(u(a)-a)$ (cf.: 6.7, al final). Se ve que si se hace x = u(a) , el coeficiente de (u(a)-a) se hace igual a 1 de modo que: s(u(a)) = u(a) - (u(a)-a) = a . Si $\phi(a,a) \neq 0$ y $\phi(u(a)-a,u(a)-a) = 0$, no puede ser $\phi(u(a)+a,u(a)+a) = 0$ porque las dos últimas relaciones implicarían $\phi(u(a),u(a)) + \phi(a,a) = 2\,\phi(a,a) = 0$, lo que contradice la primera relación. Hecho esto, la última parte del lema se prueba igual que la primera.

-o-

Teorema 1 :

Toda $u \in \phi(Q)$ es un producto de simetrías respecto de hiperplanos: las simetrías engendran el grupo ortogonal.

Demostración:

Razonemos por recurrencia sobre n = dim (E) , usando el hecho de que el teorema se verifica trivialmente si n = 0 y si n = 1 . Fijemos un vector a , no isótropo, y sea H su hiperplano ortogonal.

Si se da el caso u(a) = a , también u(H) = H y u (restringida a H) es una transformación ortogonal de H que tiene dimensión n-1 . Por la hipótesis inductiva, en H , u es un producto de simetrías s_i respecto de hiperplanos de H (subespacios de E de codimensión 2). Pero estas simetrías se extienden trivialmente a simetrías respecto de hiperplanos de E , s_i , definiendo $s_i(a) = a$, y es claro

que u es también el producto de las s_i en todo E .

Si sucede que $u(a) = -a$, y si s es la simetría respecto de H , es claro que $su(a) = a$. Por lo anterior, su es producto de simetrías s_i , de donde u es el producto de s por las s_i (recordar que las simetrías son involutivas).

En el caso general, vimos en el lema 1 que, como a es no isótropo, o bien $u(a)-a$ o bien $u(a)+a$ son no isótropos. El lema 1 dice que en el primer caso hay una simetría, s , tal que $su(a) = a$, y en el segundo, una simetría s' tal que $s'u(a) = -a$, y entonces el teorema es cierto por los razonamientos precedentes.

-o-

Según el corolario de lema 1 de 6.4 , las rotaciones que dejan fijos los puntos de un subespacio de codimensión 2 se corresponden biunívocamente con ciertas transformaciones ortogonales del plano ortogonal (cuando los subespacios son no-isótropos). Pero si u es una tal rotación, su matriz consta de dos bloques diagonales correspondientes a uno de esos subespacios, y como uno de los bloques es la matriz identidad y el determinante total es 1 , el determinante del otro bloque también es 1 . Se sigue que dichas rotaciones se corresponden biunivocamente con las rotaciones de aquél plano. Por eso, las rotaciones que dejan fijos los puntos de un subespacio no isótropo de codimensión 2, se llaman <u>rotaciones planas</u>. Entre ellas, son importantes las simetrías (que en francés reciben el nombre particular de "renversements"), es decir las transformaciones ortogonales involutivas que dejan fijos los puntos de un subespacio no isótropo de codimensión 2 .

<u>Teorema 2</u> :

<u>Toda rotación</u>, u , <u>es un producto de rotaciones planas involutivas</u> (es decir simetrías respecto de subespacios de codimensión 2), <u>siempre que</u> $n \geq 3$.

<u>Demostración</u>:

La demostración es prácticamente la misma del teorema 1. Razonaremos por recurrencia "descendente" a partir de n , y luego probaremos que el teorema vale si $n = 3$. Así que, por hipótesis inductiva, el teorema vale en espacios de dimensión menor que n .

Fijado $a \in E$, no isótropo, sea H su hiperplano ortogonal. Si $u(a) = a$, también $u(H) = H$ y u es una rotación en H , de modo que se descompone en producto de simetrías s'_i respecto de subespacios de H de codimensión 2 (en H). Prolongando estas simetrías a s_i mediante la definición $s_i(a) = a$, u resulta ser el producto de las s_i en todo E y el teorema es cierto en este caso.

Sea ahora $u(a) = -a$. Si s es cualquier simetría respecto de un subespacio de codimensión 2 que esté contenido en H , $s(-a) = a$, de modo que su está en el caso anterior.

En el caso general, como a no es isótropo, o bien u(a)-a ó bien u(a)+a son no isótropos. Razonemos sólo con la primera suposición. Es claro que el hiperplano ortogonal a u(a)-a contiene a u(a)+a y (por el lema 3 de más adelante) este hiperplano contiene un plano no isótropo en el cual está u(a)+a . Si s es la simetría (= rotación plana involutiva) respecto del ortogonal a este plano, se tiene: su(a)-s(a) = = u(a) - a y su(a)+s(a) = -u(a)-a , de donde se sigue su(a) = -a , lo que nos lleva a un caso ya estudiado. Análogo razonamiento cuando u(a)+a es no isótropo.

Sea ahora n = 3 . Ya sabemos que u es producto de simetrías respecto de planos (= hiperplanos en este caso) y como ellas tienen determinante -1 , debe ser producto de un número par de tales simetrías. Entonces basta demostrar que si s,t son simetrías respecto de planos, entonces el producto st es también un producto de simetrías respecto de rectas. Sean U , V , los hiperplanos de s y t . Como st deja fija la recta $U \cap V$, si ésta no es isótropo, st es una rotación plano (en el plano ortogonal a $U \cap V$). La restricción de st a su plano se descompone fácilmente en producto de dos simetrías del plano respecto de rectas (por ejemplo st en el plano lleva la semirrecta R sobre la R' , puede tomarse como primera simetría la de eje R , y como segunda la que tiene por eje la bisectriz del ángulo de R con R'). Luego, basta prolongar estas simetrías a todo E de modo que coincidan con la transformación $x \longrightarrow -x$ en la recta $U \cap V$ para tener st descompuesto en el producto de dos rotaciones planas involutivas. Si $U \cap V$ es isótropa, se considera un tercer plano W tal que $U \cap W$ y $W \cap V$ son rectas no isótropas. Si w es la simetría respecto de W , el razonamiento anterior dice que sw y wt son, cada una, producto de dos rotaciones planas involutivas, y por lo tanto st = swwt es producto de cuatro rotaciones planas involutivas, l.q.d.d.

(Se puede demostrar también este teorema sin usar el lema 3 así: se toma un vector a no isótropo. Siempre hay un "renversement" que transforma a en -a . Uno de los vectores u(a)-a y u(a)+a es no isótropo. En el segundo caso, hay un plano no isótropo P , ortogonal a u(a)+a que contiene a u(a)-a y un "renversement" que tiene a P como subespacio V^- (notación de 6.5) que cambia u(a)+a en u(a)+a y u(a)-a en u-u(a) y que por lo tanto lleva a en u(a) . Si u(a)-a es el nó isótropo, hay, en la misma forma, un "renversement" que transforma a en -u(a) y otro que transforma -u(a) en u(a) . De modo que siempre que $n \geq 3$ podemos limitar la demostración al caso u(a) = a , que ya fué hecha. Cuando n = 3 , también vale la reducción al caso que n deja invariante un vector no isótropo, b , de modo que su restricción al plano , ortogonal a b , es una rotación. Esta se expresa como producto de dos simetrías (ver el razonamiento anterior) s_1 , s_2 de Q . Luego se prolongan s_1 , s_2 a "renversements" poniendo $s_1'(b) = -b$ y $s_2'(b) = -b$ y todavía se tiene $u = s_1' s_2'$) .

-o-

Lema 2:

Sea $u \in \phi(Q)$, si $u(x)-x$ es isotropo para todo x no isótropo, entonces $u(x)-x$ es isótropo para todo x .

Demostración:

Sea x un vector isótropo e y uno no isótropo. La ecuación de segundo grado : $\emptyset(x+\lambda y , x+\lambda y) = 0$ no se verifica por lo menos para tres valores de λ (porque no puede tener más de dos soluciones y suponemos que K tiene por lo menos 5 elementos). Eso significa que hay por lo menos tres vectores no isótropos de esa forma en E . Para ellos, es decir para esos valores de λ , se tiene por la hipótesis: $\emptyset(w(x)+\lambda w(y) , w(x)+\lambda w(y)) = 0$ (donde hemos llamado w a $u-1$ para simplificar la notación). Así, tenemos una ecuación de segundo grado que se verifica para tres valores distintos de la variable λ . Eso implica que se verifica idénticamente, y entonces haciendo $\lambda = 0$ se tiene la tesis del lema: $\emptyset(w(x)|w(x)) = 0$.

-o-

Teorema 3 :

Si $n = 2$ y si $u \in \phi(Q)$ no deja ningún vector no nulo fijo (es decir el rango de $w = u-1$ es 2), entonces u es producto de dos simetrías (respecto de rectas = hiperplanos).

Demostración:

Como $w(E) = E$ y E tiene vectores no isótropos porque $\emptyset$ es no degenerada, no sucede que $u(x)-x$ es isótropo para todo x , de modo que por el lema 2, existe un a no isótropo tal que $u(a)-a$ es no isótropo. Sabemos que si s es la simetría respecto de la recta ortogonal a $u(a)-a$, entonces $su(a) = a$, lo que nos dice que su deja fija una recta no isótropo y por tanto su es una simetría t . De ahí se sigue que $u = st$.

-o-

Se puede demostrar más generalmente que:

Teorema 4 :

Con la notación de antes, si $w(E)$ no es totalmente isótropo u es un producto de r simetrías (r = rango de w) pero no de menos simetrías; si $w(E)$ es totalmente isótropo, u es producto de $r+2$ simetrías pero no de menos simetrías. (Se razona por inducción a partir del teorema 3, pero la demostración es demasiado fatigosa y ella en sí carece de interés para nosotros).

Corolario 1 :

Si $u \in \phi(Q)$, entonces u es producto de un número de simetrías no mayor que $n =$ = dimensión del espacio.

Demostración:

Si $w(E)$ no es totalmente isótropo, lo dice el teorema. Si $w(E)$ es totalmente isótropo y $n>2$, $r+2\leq n$ (si, por ejemplo $n=3$, r es a lo sumo 1 por ser la dimensión de un subespacio totalmente isótropo menor o igual que la mitad de la dimensión del espacio) y nuevamente basta usar el teorema. Si $n=2$ ya sabemos que u es o una rotación ó una simetría, y que las primeras son producto de dos de las segundas. Si $n=1$, trivial.

Corolario 2 :

Si n es impar y $u\in\Phi(Q)$, $\det(u)=1$, u deja fijo un vector no nulo. Si n es par y $\det(u)=-1$, u deja fijo un vector no nulo.

Demostración:

En el primer caso, u es producto de un número par y por tanto menor que n (corolario 1), de simetrías. Los hiperplanos de estas simetrías tienen intersección de dimensión por lo menos 1 y esta intersección tiene todos sus puntos invariantes para u. Análogo razonamiento para el otro caso.

-o-

Los planos no isótropos, $P\subset E$, que contienen rectas isótropas (necesariamente son 2) se llaman hiperbólicos. Las transformaciones ortogonales (resp. rotaciones) que dejan fijos los puntos de un subespacio ortogonal a un plano hiperbólico se llaman transformaciones ortogonales hiperbólicas (respec. rotaciones hiperbólicas).

Teorema 5 :

Si Q es de índice $\nu\geq 1$, $\Phi(Q)$ está engendrado por las transformaciones hiperbólicas.

Demostración:

Si $n=2$, ν es necesariamente igual a 1 y la afirmación es trivial porque todas las transformaciones ortogonales son hiperbólicas. Esto nos permite razonar por recurrencia suponiendo que para los espacios de dimensión menor que n el teorema es cierto.

El teorema 1 nos autoriza a razonar solamente para una simetría, s , respecto de un hiperplano. Sea a no isótropo, H el hiperplano ortogonal, s la simetría respecto de H . Existe un vector isótropo b no ortogonal a a . Entonces, el plano P de a y b es hiperbólico y s deja fijos los puntos de P^o . Luego s es hiperbólica, l.q.q.d.

-o-

IV.2.- EL GRUPO DE CONMUTADORES

Designaremos con $\Omega(Q)$ el grupo de conmutadores de $\Phi(Q)$, es decir el subgrupo engendrado por los elementos de la forma $uvu^{-1}v^{-1}$, y con $\Gamma(Q)$ el grupo de cuadra

dos es decir el subgrupo engendrado por los elementos de la forma u^2 . Es claro que para todo grupo vale $\Omega(Q) \subset \Gamma'(Q)$ porque todo conmutador es producto de cuadrados: $uvu^{-1}v^{-1} = u^2(u^{-1}v)^2(v^{-1})^2$.

Teorema 6 :

$\Omega(Q) = \Gamma'(Q)$.

Demostración:

Según lo que acabamos de ver, basta demostrar que todo elemento de la forma u^2 es producto de conmutadores. Razonaremos por recurrencia sobre el número de simetrías cuyo producto es u usando el hecho de que la proposición es obvia cuando este número es 1 ó 2. Suponemos entonces que si v es producto de $p-1$ simetrías entonces v^2 es producto de conmutadores. Sea $u = sv$ (s = simetría) una transformación producto de p simetrías. Entonces la proposición queda demostrada por la igualdad:
$u^2 = (svs^{-1}v^{-1})v^2$.

-o-

Teorema 7 :

$\Omega(Q)$ es engendrado por los elementos $(st)^2$, donde s y t son simetrías (respecto de hiperplanos).

Demostración:

El claro que los $stst$ son conmutadores, de modo que engendran un subgrupo G contenido en $\Omega(Q)$. Probemos primero que los conmutadores del tipo $sus^{-1}u^{-1}$ (s = simetria) pertenecen a G . Razonamos por inducción a partir del número de simetrías que componen la transformación ortogonal u : suponemos que si v es producto de $p-1$ simetrías, entonces $svs^{-1}v^{-1} \in G$. Entonces, tenemos:

$$tut^{-1}u^{-1} = tsts.s.tvt^{-1}v^{-1}.s^{-1} \in G \quad (\text{si } t \text{ es simetría})$$

porque $tsts \in G$, $tvt^{-1}v^{-1} \in G$ por la hipótesis inductiva y $s.tvt^{-1}v^{-1}.s^{-1}$, transformado de G por un automorfismo interior definido por una simetría también pertenece a G (en efecto: ya vimos (lema 4 de 6.5) que si $w \in \phi(Q)$ y s es una simetría, entonces wsw^{-1} es otra simetría, y de ahí se sigue que G es invariante para automorfismos interiores).

Ahora podemos probar por recurrencia que todo cuadrado u^2 de una transformación ortogonal pertenece a G . En efecto:

$$u^2 = svsv = (svs^{-1}v^{-1})v^2 = \ldots$$

y entonces el teorema 6 completa la demostración de que $\Omega(Q) \subset G$.

Teorema 8 :

Si $n \geq 3$, el grupo $\Omega^+(Q)$ de conmutadores de $\phi^+(Q)$ es igual al subgrupo $\Omega(Q)$

de $\phi(Q)$

Demostración:

Las mismas demostraciones de antes (usando simetrías respecto de subespacios de codimensión 2, es decir rotaciones planas involutivas, en lugar de simetrías respecto de hiperplanos) prueban que también $\Omega^+(Q)$ es igual al grupo de cuadrados $\Gamma^+(Q)$ de $\phi^+(Q)$. Por otra parte, si s y t son simetrías, $st \in \phi^+(Q)$, de modo que por el teorema anterior: $\Omega(Q) \in \Omega^+(Q)$. Como recíprocamente es obvio que $\Omega^+(Q) \subset \subset \Omega(Q)$, el teorema está demostrado.

-o-

Corolario:

El cociente $\phi^+(Q)/\Omega(Q)$ es un grupo conmutativo cuyos elementos son todos de orden 2 .

Demostración:

En efecto, cualquiera sea $u \in \phi^+(Q)$, para todo v_1 y para todo v_2 en $\Omega(Q)$, se tiene: $uv_1uv_2 = (uv_1uv_1)v_1^{-1}v_2 \in \Omega(Q)$, lo que prueba que la clase de u , $u.\Omega(Q)$, multiplicada por sí misma, de el elemento neutro del cociente, que es la clase $\Omega(Q)$

-o-

Teorema 9 :

Si K es un cuerpo ordenado pitagórico (cf. Bourbaki, Alg., Ch.VI, 2, Ex.8), o sea si toda suma de cuadrados es un cuadrado, si $\emptyset$ es positiva y si E admite base ortonormal, entonces $\Omega(Q) = \phi^+(Q)$. Esto ocurre, por ejemplo, si K es el cuerpo $\mathcal{R}$.

Demostración:

Basta probar que toda rotación plana es el cuadrado de una rotación plana. Si en un plano u es una rotación que lleva x sobre y (x e y en el "círculo" unitario) las hipótesis hechas implican que la bisectriz del ángulo de Ox con Oy corta al círculo unitario en un punto z . La única rotación v tal que $v(x) = z$ verifica $v^2 = u$, l.q.q.d.

-o-

IV.3.- CENTRO DEL GRUPO ORTOGONAL

Lema 3 :

Toda recta isótropa de E es intersección de dos planos no isótropos (si $n \geq 3$) .

Demostración:

Sea x un vector isótropo. Existe un y ortogonal a x pero no colinal a x , y un z no isótropo ni ortogonal a x . Entonces x y z definen un plano no isótropo, P , y los vectores x e y+z definen otro plano no isótropo P' que es dis

tinto de P . Por lo tanto, P y P' se cortan según la recta isótropa que contiene a x (#).

Teorema 10:

Las únicas aplicaciones lineales biyectivas que conmutan con todos los elementos de $\phi(Q)$ son las homotesias de E .

Demostración:

Cuando $n = \dim(E) = 1$, el teorema es obvio.

Supongamos que $n \geq 3$ y sea v una biyección lineal que permuta con las transformaciones ortogonales. Si H es un hiperplano no isótropo, sea s la simetría respecto de H , y sea $x \in H$. Entonces: $v(x) = vs(x) = s(v(x))$ nos dice que $v(x)$ queda fijo para s , de modo que $v(x) \in H$. Esto prueba que v deja fijo H y análogamente se demuestra que deja invariante la recta ortogonal a H . Así, v deja invariantes todas las rectas no isótropas y por tanto, también los planos no isótropos . Entonces, por el lema 3, v deja invariantes todas las rectas de E . Esto basta para asegurar en general que v es una homotecia pues: si a y b son no colineales:

$$\begin{aligned} v(a) &= \lambda_a a \\ v(b) &= \lambda_b b \\ v(a+b) &= \lambda_{a+b}(a+b) \end{aligned}$$

implican

$$\lambda_a = \lambda_b = \lambda_{a+b}$$

Cuando $n = 2$, se razona así: sea e_1 , e_2 una base ortogonal de E . Si Q es de índice 0 no hay vectores isótropos y entonces, el razonamiento precedente prueba que si v conmuta con las transformaciones ortogonales deja invariantes todas las rectas de E y por tanto es una homotecia. Si no, Q es de índice 1 y por el mismo motivo, v deja invariantes las rectas no isótropas. Entonces observamos que existe un $\alpha \neq 0$ tal que $e_1 + \alpha e_2$ es no isótropo, de modo que por lo que acabamos de decir, existe $\lambda \in K$ tal que $v(e_1+\alpha e_2) = (e_1+\alpha e_2)$ y entonces v es la homotecia de razón λ . l.q.q.d.

-o-

Teorema 11 :

El centro de $\phi(Q)$ está formado por las dos aplicaciones siguientes: $1 : x \longrightarrow x$, $-1 : x \longrightarrow -x$.

En efecto, si v es una transformación ortogonal que conmuta con todas las trans -

(#) La existencia de z resulta por ejemplo del corolario del teor. 2, §4. Entonces, y puede elegirse en el ortogonal al plano no isótropo que pasa por x y z .

formaciones ortogonales, por una parte v es una homotecia, y por otra debe verificar : $\phi(v(x),v(x)) = \phi(x,x)$, de modo que si la razón de la homotecia es λ , se tiene $\lambda^2 = \pm 1$. Recíprocamente, es obvio que estas dos aplicaciones son ortogonales y conmutan con todas las transformaciones ortogonales, l.q.q.d.

-o-

Corolario:

Si $n \geq 3$, el centro de $\phi^+(Q)$ es igual al centro de $\phi(Q)$.

Demostración:

Si v está en el centro del grupo de rotaciones, resulta, como en el teorema 10, que deja invariantes los planos no isótropos (porque debe conmutar con las rotaciones planas) y esto implica que deja invariantes todas las rectas y por tanto que es una homotecia. El resto es trivial.

La restricción $n > 2$ es efectiva porque si $n = 2$, el grupo de rotaciones es conmutativo y en general difiere del grupo $\{1,-1\}$.

-o-

IV.4.- SIMPLICIDAD DEL GRUPO DE ROTACIONES $\phi_3^+(\mathcal{R}) = S\phi(3,\mathcal{R})$.

La notación $\phi_3^+(\mathcal{R})$ o la $S\phi^+(3,\mathcal{R})$ se usa para designar el grupo de rotación en el caso particular en que $K = \mathcal{R}$, $E = \mathcal{R}^3$, y ϕ está definida por la matriz unidad respecto de la base canónica formada por los vectores $i = (1,0,0)$, $j = (0,1,0)$ y $k = (0,0,1)$. Supongamos que estamos en este caso.

Un grupo se llama simple si no contiene subgrupos distinguidos no triviales (es decir diferentes del subgrupo formado por el único elemento 1 , y del grupo total).

Teorema 12 :

$\phi_3^+(\mathcal{R})$ es simple.

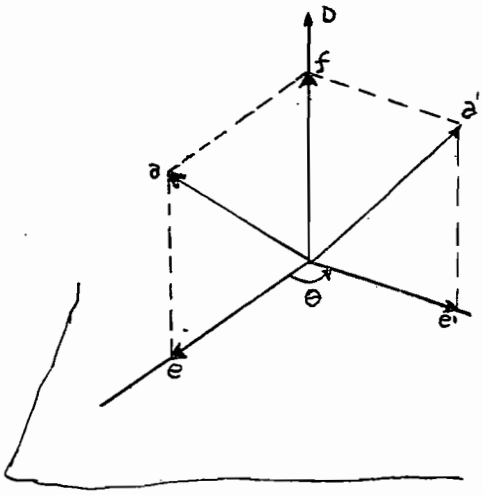
Demostración:

Como los subgrupos distinguidos son los estables para automorfismos interiores, basta probar que si s es una rotación diferente de la identidad, el subgrupo engendrado por los transformados de s por automorfismos interiores es todo el grupo de rotaciones. En otras palabras, basta demostrar que toda rotación es un producto de rotaciones de una de las formas: usu^{-1} ó $us^{-1}u^{-1}$, donde u $\phi_3^+(\mathcal{R})$. Distinguiremos tres casos:

(a) s es involutiva: $s^2 = 1$. En este caso la proposición es corolario del teorema 2. En efecto: en el caso $\phi_3^+(\mathcal{R})$ se cumple además que dos "reversements" cualesquiera son conjugados pues dadas dos rectas cualesquiera existe siempre una rotación que transforma una en la otra (teor. de Witt).

Como n es impar, s deja una recta fija (corolario 2 del teorema 4), D , y está perfectamente determinada por la rotación del plano P ortogonal a D obtenida como restricción de s (recordar que estamos en el caso clásico: no hay vectores isótropos). Si $\hat{\theta}$ es el ángulo de esta rotación, podemos suponer que es distinto del llano porque si no estaríamos en el caso (a) . Entonces caben dos posibilidades:

(b) $\cos(\hat{\theta}) > 0$. Puede tomarse D como tercer eje de coordenadas. Sea e P un vector de longitud 1 , y sea e' su transformado: e' = s(e) . Tomemos en D un vector f de longitud 1 . Decimos que existe un escalar $\lambda \in \mathbb{R}$ tal que si a = $= e+\lambda f$, a' = s(a) = $e'+\lambda f$, entonces a y a' son ortogonales. En efecto, un tal λ verifica esa condición si: $\phi(a,s(a)) = \phi(e+\lambda f \mid e'+\lambda f) = \lambda^2 + \cos\hat{\theta} = 0$, y entonces es claro que siempre existe un tal λ real porque hemos supuesto $\cos\hat{\theta} < 0$. Designemos con t la simetría respecto de la recta $\mathbb{R}a$, de modo que sts^{-1} es la simetría respecto de $\mathbb{R}a'$. Eso significa que $tsts^{-1}$ por ser el producto de dos simetrías de ejes ortogonales es la simetría respecto de la recta ortogonal al plano de a y a' . Así, por un lado $tsts^{-1}$ (que es obviamente una rotación) es involutiva, y además está en el subgrupo distinguido engendrado por s porque $tsts^{-1} = (tst^{-1})s^{-1}$, de modo que por (a), este grupo es también igual a $\phi_3^+(\mathbb{R})$ en este caso.



(c) $\cos(\hat{\theta}) > 0$. Entonces, decimos que existe un entero positivo k tal que $\cos(k\hat{\theta}) \leq 0$. Supongamos en efecto, que se hubiera demostrado que $\cos h\theta > 0$, $\cos(h+1)\theta \leq \cos(h\theta)$ para $0 < h < k$. De ahí resultaría $\operatorname{sen}(h+1)\theta \geq \operatorname{sen}(h\theta)$ (por la relación $\cos^2\theta + \operatorname{sen}^2\theta = 1$) y $\operatorname{sen}(h\theta) \geq 0$ (por recurrencia sobre h). Entonces se tiene: $\cos(k+1)\theta = \cos k\theta \cos\theta - \operatorname{sen} k\theta \operatorname{sen}\theta \leq \cos k\theta - \operatorname{sen}^2\theta$, y la recurrencia puede continuarse, lo que prueba que no puede ser $\cos k\theta \geq 0$ para todo k. Por lo tanto, tenemos en el subgrupo distinguido engendrado por s un elemento, s^k cuyo ángulo, $k\hat{\theta}$, tiene coseno negativo o nulo. Entonces, por (a) o por (b), también en este caso dicho subgrupo distinguido es todo $\phi_3^+(\mathbb{R})$.

Debemos hacer notar (cosa que se ve en la demostración) que este teorema está intimamente relacionado con propiedades especiales del cuerpo real.

-o-

IV.5.- SIMPLICIDAD DEL GRUPO PSL(n,K) $(n \geq 2)$.

Antes de entrar en el tema, recordemos algunas definiciones.

Si E es un conjunto cualquiera, las biyecciones de E sobre E se denominan permutaciones de E y constituyen evidentemente un grupo que se llama grupo simétrico de E y se nota $\mathfrak{S}(E)$. Si dos conjuntos tienen el mismo cardinal, sus grupos simétricos son isomorfos. Los subgrupos de $\mathfrak{S}(E)$ se llaman grupos de transformaciones ó grupo de permutaciones de E .

Sea Γ un grupo de permutaciones de E . Si dados dos partes de E de k elementos: $a_1,\dots,a_k$,y $b_1,\dots,b_k$ siempre existe una permutación f de Γ tal que $f(a_i) = b_i$, entonces Γ se llama k veces transitivo. Cuando $k = 1$, el grupo se llama simplemente transitivo, o se dice que Γ opera transitivamente sobre E . La relación " x es equivalente a y si y sólo si existe un elemento $f\in\Gamma$ tal que $f(x) = y$ " es una relación de equivalencia en E . La clase que contiene el elemento x E se llama órbita de x para Γ y es el conjunto de las imágenes de x por elementos de Γ . E se descompone en partes disjuntas dos a dos cada una de las cuales es una órbita (la órbita de cualquiera de los elementos que contiene). Si Γ es transitivo, E es la órbita de cualquiera de sus puntos.

En lo que sigue introduciremos otros conceptos relacionados con los grupos de permutaciones a medida que sean necesarios.

-o-

Ya hemos dicho que con $GL(n,K)$ se nota el grupo general lineal (conjunto de automorfismos) de K^n , con $SL(n,K)$ el grupo de los automorfismos unimodulares. $PGL(n,K)$ es el grupo proyectivo correspondiente (que es isomorfo al cociente de $GL(n,K)$ por su centro $K^{\#}$) y $PSL(n,K)$ es la imagen de $SL(n,K)$ en $PGL(n,K)$ por la aplicación canónica de $GL(n,K)$ en $PGL(n,K)$.

Lema 4 :

El grupo $PSL(n,K)$ es dos veces transitivo (recordar que $n \geqslant 2$) .

Demostración:

El enunciado es equivalente a probar que si se dan dos pares, a,b , a',b' , de vectores linealmente independientes (es decir $\lambda a \neq \mu b$, $\lambda a' \neq \mu b'$), que es lo mismo que dar dos pares de rectas de E , entonces existe una aplicación u de $GL(n,K)$ que lleva a sobre a' y b sobre b' . Pero la existencia de una tal u es inmediata si se piensan dos bases de E , una conteniendo a,b , la otra conteniendo a',b' .

-o-

Si $\Gamma \subset \mathfrak{S}(E)$ es un grupo transitivo de permutaciones de un conjunto E , se dice que Γ es imprimitivo si existe una partición no trivial de E compatible con el grupo. Es decir, si E se descompone en una familia $\{A_i\}$ de partes disjuntas dos a dos, distintas de E , tales que una tenga por lo menos 2 elementos y tales que cualquiera sea $f\in\Gamma$, $f(A_i) \subset A_j$ (j igual o distinto de i).

Los grupos transitivos que no son imprimitivos se llaman primitivos.

Lema 5 :

Si Γ es k veces transitivo y $k \geq 2$, entonces es primitivo.

Demostración:

Sean A_1, A_2 , dos partes de E de una partición compatible con el grupo. Tomemos a y b en A_1 , a' en A_1 y b' en A_2 . Por la hipótesis, existe $f \in \Gamma$, tal que $f(a) = a'$, $f(b) = b'$, y esto contradice la definición de A_1 y A_2 . Por tanto, no existen particiones compatibles con el grupo y Γ es primitivo.

-o-

Lema 6 :

Todo subgrupo distinguido distinto de $\{e\}$ de un grupo primitivo es transitivo.

Demostración:

Sea Γ un grupo primitivo, y N un subgrupo distinguido de Γ . Sea U la órbita del punto x E para el grupo N , y sean $s \in \Gamma$, $t \in N$. Entonces: $st(x) = (sts^{-1})s(x)$ prueba que el conjunto: $sU = \{x \in E \,/\, \exists\, y : x = s(y) , y \in U\}$ es también una órbita de N . Entonces, si N no fuera transitivo, existirían más de una órbita para N que constituirían una partición de E compatible con el grupo Γ, en contra de que Γ es primitivo.

-o-

Sea Γ un grupo de permutaciones de E . Para cada $x \in E$, el subconjunto de Γ , $S_x = \{x \in \Gamma \,/\, s(x) = x\}$ es un subgrupo de Γ que se llama estabilizador de x.

Lema 7 :

Si N es un subgrupo transitivo de Γ , se verifica $\Gamma = N.S_x$ cualquiera sea el punto x en E .

Demostración:

En efecto, si s es cualquier elemento de Γ , s(x) es un punto de E , y como N es transitivo, existe un t en N tal que t(x) es s(x) , es decir: $t^{-1}s(x) = x$. Estro prueba que $t^{-1}s$ está en S_x , de modo que s es el producto de $t \in N$ por un elemento de S_x , l.q.q.d.

-o-

Lema 8 de Iwasawa:

Sea Γ un grupo primitivo de permutaciones de E . Si se verifican las condiciones:

- Γ es igual a su propio grupo de conmutadores Γ' .
- Para cada $x \in E$, S_x tiene un subgrupo abeliano, H_x , que es distinguido en S_x y los subgrupos de la forma sH_xs^{-1} $(s \in \Gamma)$ engendran Γ ,

entonces Γ es un grupo simple.

Demostración:

Tomemos un subgrupo distinguido, N, de Γ, distinto del $\{1\}$, y demostremos que necesariamente $N = \Gamma$. Si $x \in E$, como N es transitivo por el lam 6, se verifica que $\Gamma = N.S_s$. Además, la segunda condición nos dice que cada elemento s de Γ puede escribirse como un producto de la forma: $s = \prod_i s_i h_i s_i^{-1}$, donde los s_i están en Γ, y los h_i en H_x. La primera observación dice que s_i también es un producto de la forma $t_i u_i$, con $t_i \in N$ y $u_i \in S_x$. Entonces, como H_x es distinguido en S_x, tenemos:

$$s_i h_i s_i^{-1} = t_i h_i' t_i^{-1} \quad (\text{con } h_i' = u_i h_i u_i^{-1} \in H_x) \qquad (\#)$$

Observemos ahora que, siendo N distinguido, todo producto de la forma $tht'h'$, con t y t' en N, puede escribirse así:

$$tht'h' = t''hh' \quad (\text{donde } t'' = tht'h^{-1} \text{ y por tanto } t'' \in N)$$

Quiere decir que, si bien N no es conmutativo, los productos de ese tipo pueden transformarse de modo de tener un factor de N al principio y luego los factores restantes en el mismo orden en que estaban inicialmente. Podemos aplicar esta propiedad a los factores cuyo producto es s, que por (#) son de la forma indicada. Esto prueba que todo tal s puede escribirse como un elemento de N multiplicado por un elemento de H_x, es decir $\Gamma = N.H_x$. Pero ahora, aplicando esta propiedad podemos ver enseguida que N contiene todo conmutador de Γ. En efecto, si $\Gamma = N.H_x$, un conmutador cualquiera de Γ es de la forma $(th)(t'h')(th)^{-1}(t'h')^{-1}$, con los elementos t,t' en N, y los h,h' en H_x. Pero por lo ya vimos un tal producto siempre se puede escribir en la forma: $t'''.h.h'.h^{-1}.h'^{-1} = t''' \in N$, porque H_x es abeliano. Entonces, N contiene el grupo de conmutadores de Γ, que por hipótesis es igual a Γ, de modo que $N = \Gamma$, l.q.q.d.

-o-

Si E es un espacio vectorial sobre un cuerpo K, se llama transvección de hiperplano H a todo automorfismo de E que deja fijos los vectores de H y por pasaje al cociente se convierte en la identidad de E/H. Se sabe que si t es una tal transvección y f una forma lineal no nula que se anula en H, entonces existe un vector a en H tal que, para todo x en E vale la fórmula: $t(x) = x+f(x).a$. Recíprocamente, todo automorfismo de ese tipo es una transvección respecto de un hiperplano que pasa por a y en el cual se anula f

Sea (e_i) una base de E y consideremos una transvección cuyo hiperplano sea el engendrado por los e_k $(k \neq i)$. Fijemos un índice $j \neq i$, y supongamos que la transvección es de la forma: $t(x) = x+f(x)e_j$. Entonces, es obvio que t está determinada cuando se da $t(e_i) = e_i+e_j$, ya que por hipótesis $t(e_k) = e_k$ si $k \neq i$.

Como t es conocida cuando se dan los índices i,j y el escalar λ, la representaremos con la notación $B_{ij}(\lambda)$, y por lo dicho es claro que su matriz es

$$B_{ij}(\lambda) = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & \dots & 1 \end{pmatrix} = I + \lambda E_{ij}$$

(una matriz igual a la de la identidad pero que en la fila j y en la columna i tiene el elemento λ en lugar del 0, o sea es igual a la identidad I más la unidad matricial E_{ij} multiplicada por λ). Reciprocamente, es claro que todas las matrices de la forma $B_{ij}(\lambda)$, $\lambda \neq 0$ definen una transvección. Pero hay más: <u>las</u> $B_{ij}(\lambda)$ <u>son transvecciones pertenecientes al grupo</u> $SL(E) = SL(n,K)$. (Obvio).(')

Investiguemos cómo operan estas matrices mediante multiplicación. Si $A = (a_{ij})$ es una matriz de orden n cualquiera, los elementos de la matriz $A.B_{ij}(\lambda)$ son los mismos que los de A, excepto los de la columna i: el a_{ki} debe sustituirse por $a_{ki} + \lambda a_{kj}$, o sea, <u>se sustituye la columna</u> i <u>por la columna</u> i <u>sumada con la</u> j <u>multiplicada por</u> λ. Análogamente, la matriz $B_{ij}(\lambda)A$ se obtiene de la matriz A <u>sustituyendo la fila</u> i <u>por la fila</u> i <u>más la fila</u> j <u>multiplicada por</u> λ.

Hechas estas observaciones, cuando $n \geq 2$, es un sencillo ejercicio deducir que si A es una matriz de determinante igual a uno, se puede lograr por medio de varias multiplicaciones a la derecha y a la izquierda por matrices de la forma $B_{ij}(\lambda)$ (variando i, j y $\lambda \neq 0$) que A se convierta en la matriz identidad. Se sigue que A es un producto de matrices de la forma $B_{ij}^{-1}(\lambda)$, y como éstas están en $SL(n,K)$, hemos demostrado el siguiente:

<u>Lema 9</u> :

<u>El grupo</u> $SL(n,K)$ <u>está engendrado por transvecciones.</u>

-o-

(')Obsérvese que, inversamente, si se da una transvección t, existe una base (e_i) para la cual ella tiene la forma $B_{12}(1)$ (basta tomar $n-1$ de los e_i en el hiperplano de t, etc.) y por lo tanto <u>dos transvecciones cualesquiera son conjugadas en</u> $GL(n)$.

Lema 10:

El grupo $SL(n,E)$ es igual a su propio grupo de conmutadores.

Demostración:

Hay que probar que toda transformación unimodular está en el grupo de conmutadores, o, por el lema 9, que toda transvección $B_{ij}(\lambda)$ es un producto de conmutadores de $SL(n,K)$. Para ello, basta razonar para una transvección particular porque dos de ellas son conjugadas respecto de un automorfismo interior de $GL(n)$, y $SL(n)$ es distinguido en $GL(n)$; por tanto, si una es un producto de conmutadores la otra también. Tomemos entonces la trasvección $B_{21}(\lambda)$ que es:

$$\begin{pmatrix} 1 & \lambda & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

de modo que podemos limitarnos a los bloques de las dos primeras filas y las dos primeras columnas. Consideremos las matrices:

$$A = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Ellas pertenecen a $SL(n,K)$ y un cálculo directo muestra que su conmutador es:

$$A\,B\,A^{-1}\,B^{-1} = \begin{pmatrix} 1 & \mu^2-1 \\ 0 & 1 \end{pmatrix}$$

que nos dice que $B_{ij}(\lambda) = ABA^{-1}B^{-1}$ si se toma $\lambda = \mu^2-1$ y μ de modo que $\mu^2 \neq 1$. Esto demuestra el lema. (Nótese que aquí se usa que el cuerpo tiene más de tres elementos).

-o-

Teorema 13 :

El grupo $PSL(n,K)$ es simple.

Demostración:

Sea z un punto del espacio proyectivo $P_n(K)$, y a un punto de K^{n+1} cuya imágen canónica en $P_n(K)$ sea justamente z (podemos pensar, si se quiere, a z como una recta privada del origen y a a como un punto de esa recta). Los lemas 4 y 5 dicen que $PSL(n,K)$ es primitivo, y el lema 10, que es igual a su grupo de conmutadores. Entonces, bastará encontrar subgrupos H_z que cumplan las condiciones del lema de Iwasawa para que este lema pruebe que $PSL(n,K)$ es simple. Para ello, consideremos las transvecciones del vector a : $x \longrightarrow x + f(x)\,a$, donde f es una forma lineal tal que $f(a) \neq 0$,

que forman un grupo abeliano y designemos con H_z a la imagen canónica de este grupo en $PSL(n,K)$. Entonces por su definición y por lo demostrado antes, resulta que H_z es un subgrupo distinguido del grupo S_z tal que los grupos $tH_zt^{-1} = H_{t(z)}$ engendran $PSL(n,K)$ (esto último porque $SL(n,K)$ es engendrado por transvecciones y porque por el lema 4, cualquier punto de P_n puede obtenerse como imagen $t(z)$ de z por un $t \in PSL(n,K)$) . Entonces, por el lema de Iwasawa, el teorema queda demostrado.

-o-

IV.6.- SIMPLICIDAD DEL GRUPO $P\Omega_n(Q)$.

Aquí se hacen las hipótesis de que Q es una forma cuadrática de índice $\nu \geq 1$ sobre $E \approx K^n$, que $n \geq 3$ y se excluye el caso en que simultáneamente $n = 4$ y $\nu = 2$.

Comencemos con algunas propiedades del grupo de conmutadores del grupo ortogonal , $\Omega(Q)$, que nos serán necesarias.

Lema 11 :

Sea P un plano hiperbólico, Toda transformación ortogonal (resp. toda rotación) , u , se puede escribir en la forma $u = sv$, donde s es una transformación (resp. rotación) hiperbólica de plano P y $v \in \Omega(Q)$.

Demostración:

Si u es hiperbólica de plano P' , como por el teorema de Witt existe una transformación ortogonal t tal que $t(P) = P'$, se sigue que u es de la forma $u = tst^{-1} = s(s^{-1}tst^{-1})$ y el lema está demostrado en ese caso.

En el caso general, si u es una transformación ortogonal, por el teorema 5 u es producto de p transformaciones hiperbólicas y podemos razonar por recurrencia(') . En tonces, $u = tu'$ donde u' es producto de $p-1$ transformaciones hiperbólicas, y t es hiperbólica. Por la hipotesis de recurrencia, u' se puede escribir $u' = s'v'$ (con s' hiperbólica de plano P y $v' \in \Omega$) , y por lo que vimos antes, $t = sv$ (s hiperbólica de plano P , $v \in \Omega$). De ahí se sigue que también u es de esa forma porque: $ss'(s'^{-1}vs'v^{-1})vv'$.

-o-

Lema 12 :

Si los planos P,P' son hiperbólicos, existe $v \in \Omega(Q)$ tal que $v(P) = P'$.

Demostración:

Sabemos (teorema de Witt) que existe una transformación ortogonal, u , tal que $u(P) = P'$, y por el lema precedente, u es de la forma sv , con $v \in \Omega$ y s

(') Si $u = sv$ con s hiperbólica y $v \in \Omega$. Si u es una rotación, como v lo es también, s es una rotación.

hiperbólica de plano P' . Esto implica que también $v(P) = P'$ y el lema está demostrado.

Lema 13 :

Sea R una recta no ortogonal a R' , y R_1 una no ortogonal a R_1' , y además , R, R', R_1, R_1' , isótropas. Entonces existe una transformación $v \in \Omega$ tal que $v(R) = R_1$, $v(R') = R_1'$.

Demostración :

Los planos P, P_1 definidos por R, R' y R_1, R_1' , respectivamente, son hiperbólicos. El lema precedente dice que existe una $w \in \Omega$ tal que $w(P) = P'$ y como w es una transformación ortogonal, lleva necesariamente R y R' sobre R_1 y R_1' , pero no sabemos si lleva justamente R sobre R_1 y R' sobre R_1' . De todos modos, basta encontrar otro elemento de Ω que lleve $w(R)$ sobre R_1 y $w(R')$ sobre R_1' . Así, el problema se reduce a encontrar una aplicación de Ω tal que lleve cada recta isótropa de un plano hiperbólico sobre la otra. Sea a un vector no isótropo ortogonal a P . Existe en P un vector (necesariamente no isótropo) b , tal que $Q(b) \neq Q(a)$ (porque hay en P vectores x tales que $Q(x)$ toma cualquier valor deseado (')). Como sabemos, existe entonces una transformación ortogonal t que lleva a sobre b : $t(a) = b$. Ahora, por la elección de a , si s es la simetría de hiperplano ortogonal a a , se tiene que $s(R) = R$ y $s(R') = R'$. Si $s' = tst^{-1}$, sabemos que s' es la simetría de hiperplano ortogonal a $b = t(a)$, de modo que $s'(R) = R'$, y $s'(R') = R$. Entonces basta tomar $v = s's = tst^{-1} \in \Omega$ para tener: $v(R) = R'$, $v(R') = R$, l.q.d.d.

-o-

Lema 14 :

Si a, b, b' son tres vectores isótropos distintos tales que a es ortogonal a b y a b' , existe $v \in \Omega$ tal que $v(a) = a$, $v(b) = b'$.

Demostración:

Supongamos primero que b no es ortogonal a b' . Entonces, usando el teorema de (4.5) podemos encontrar un vector a' no ortogonal a a , isótropo, y ortogonal a b y a b' . Entonces, el subespacio F de E ortogonal a a y a' es no isótropo y de dimensiones mayor o igual que 3 (porque se excluye el caso $n = 4$ y $\nu = 2$). Si aplicamos a F el lema precedente, concluímos que existe v' en el grupo de conmutadores del grupo ortogonal de la restricción de Q a F tal que $v'(b) = b'$. Ahora, si se extiende v' a todo E mediante una aplicación v que deje invariantes las rectas ortogonales a F , se tiene una v en Ω que satisface las condiciones del lema .

(') En efecto, si en P se toma una base formada por vectores isótropos,

$$a(x^1 e_1 + x^2 e_2) = 2x^1 x^2 \, \varphi(e_1, e_2) \quad .$$

Supongamos ahora que b es ortogonal a b'. Nuevamente, consideramos a' isótropo y no ortogonal a a, y el subespacio F de antes, no isótropo, ortogonal a a y a' y de dimensión mayor o igual que 3. Sean, respectivamente, b_1, b_1', vectores de las rectas $F \cap (Ka+Kb)$ y $F \cap (Ka+Kb')$, respectivamente (e isótropos porque los planos $Ka+Kb$ y $Ka+Kb'$ son evidentemente totalmente isótropos). Sea c un vector de F, isótropo, y no ortogonal a b_1. Es claro que c tampoco es ortogonal a b pero es ortogonal a a. Entonces, el razonamiento anterior puede usarse ahora y mediante él deducimos que existe v_1 en Ω tal que $v_1(a) = a$, $v_1(b) = b_1$, de modo que sólo falta encontrar otra aplicación v_2 en Ω tal que $v_2(a) = a$ y $v_2(b_1) = b_1'$. Pero esto es inmediato porque por el lema precedente, existe v_2' con esa propiedad, donde v_2' pertenece al grupo de conmutadores del grupo ortogonal de la restricción de Q a F, y luego basta prolongar como antes v_2' a todo E de modo que deje invariantes las rectas ortogonales.

Se dice que un grupo de permutaciones <u>opera fielmente</u> sobre el conjunto en cuestión cuando la única transformación del grupo que deja fijos todos los puntos del conjunto es la identidad.

-o-

<u>Lema 15</u> :

<u>Sea C el conjunto de las rectas isótropas de E. El grupo proyectivo $P\Omega(Q)$ opera fielmente sobre C.</u>

<u>Demostración</u> :

Considerando las rectas de E como puntos de P_n, es claro que toda transformación de $P\Omega$ hace corresponder a una recta otra recta, de modo que $P\Omega$ es un grupo de permutaciones sobre las rectas de E. Por otra parte, es obvio que cualquier recta isótropa debe transformarse en una recta isótropa por cualquier transformación proyectiva ortogonal.

En nuestro caso entonces, todo se reduce a demostrar que si u es una transformación ortogonal que deja invariante cada recta isótropa de E, entonces u es una homotecia. Pero esto prácticamente ya fué demostrado antes pues si u deja fijas las rectas isótropas, deja fijos los planos hiperbólicos, y toda recta no isótropa es intersección de dos planos hiperbólicos. Se sigue que u deja fijas todas las rectas de E y por tanto es una homotecia. (Para probar que si x no es isótropo hay dos planos hiperbólicos que se cortan en la recta de x se razona más o menos como en el lema 3 : se toma y isótropo y no ortogonal a x, y z no isótropo, ortogonal a x pero no ortogonal a y ; el plano de y y z es no isótropo y por tanto contiene y' isótropo y no ortogonal a x ; entonces los planes de x e y, y de x e y' resuelven el problema; para demostrar la existencia de vectores como los anteriores se usa que K tiene más de tres elementos, es decir por lo menos cinco elementos.)

-o-

Lema 16 :

El grupo $P\Omega(Q)$, considerado como grupo de permutaciones del conjunto C de las rectas isótropas de E , es primitivo.

Demostración:

Supongamos, por el absurdo, que C admite una partición compatible con P , y sea M una de las partes de esta partición con dos elementos R , R' distintos, como mínimo. Si probamos que esto implica que M es todo C , tendremos una contradicción que demostrará el lema. Si R es ortogonal a R' , M contiene todas las rectas ortogonales a R ó a R' (lema 14). Además existe (por el teorema de (4.5)) R" ortogonal a R pero no ortogonal a R' , y por tanto $R'' \in M$. Entonces, reemplazando R por R" si fuera necesario, podemos suponer que R y R' no son ortogonales. Sea R_1 una recta de C no ortogonal a R . El lema 14 dice que hay una transformación de $P\Omega$ que lleva R , R' sobre R , R_1 , de modo que también $R_1 \in M$. Razonamdo en la misma forma con R' , tenemos que M contiene todas las rectas isótropas no ortogonales a R y todas las no ortogonales a R' . Si el indice ν de Q es igual a uno, estas son todas las rectas isótropas y C = M . Si $\nu \geq 2$ existe (por el teorema de (4.5)) una recta isótropa R_1 , no ortogonal a R y ortogonal a R' . Por lo que acabamos de ver, $R_1 \in M$ y por el lema 14 existe una transformación de $P\Omega$ que deja fija R' y lleva R_1 sobre cualquier recta isótropa prefijada distinta de R' y ortogonal a R'. Eso significa que M contiene también todas las rectas isótropas ortogonales a R' (y , por lo mismo, todas las ortogonales a R). Esto completa la demostración.

-o-

Como lo indica su título, esta última parte del apéndice tiene como objetivo la demostración de que el grupo $P\Omega$ es simple. Para ello nos basaremos en el lema de Iwasawa, y por tanto necesitamos probar todavía unas cuantas cosas. Por ejemplo, debemos construir los H_x con las propiedades del lema de Iwasawa y demostrar que $P\Omega$ es igual a su grupo de conmutadores. En todo esto pensamos el grupo $P\Omega$ como grupo de permutaciones del conjunto C de las rectas isótropas de E .

Lema 17:

Si a (no nulo) es un vector isótropo y L es el hiperplano ortogonal, la transvección de L definida por $t_a : z \longrightarrow z + \emptyset(z,y)a$ (y fijo en L) se extiende de una sola manera en una transformación ortogonal $\rho_{(a,y)}$ de todo E . (Recordar que: $a \in L$) .

Demostración:

Como $Q(a) = 0$ y como z es ortogonal a a , es inmediato que $Q(z) = (z+((z,y)a)$, de modo que t_a puede extenderse a todo E por el teorema de Witt. Así, lo único que hay que probar es que esta extensión, que notamos $\rho_{(a,y)}$, es única.

Sea b un vector isótropo no ortogonal a a , y P el plano hiperbólico definido

por a y b . Si u , u' son dos extensiones de t_a , coinciden en el subespacio F ortogonal de P . Entonces, la transformación ortogonal $u'u^{-1}$ deja fijos los puntos de F y por consiguiente deja invariante el plano P . Pero en el plano P , $u'u^{-1}$ es una transformación ortogonal que deja fijo un vector isótropo (el a) y entonces las propiedades vistas en (10.1) aseguran que $u'u^{-1}$ es la identidad en P . Por lo tanto, u' es igual a u en todo E .

-o-

Lema 18 :

Con la notación de antes, valen las fórmulas:

$$\rho_{(a,y)} \cdot \rho_{(a,y')} = \rho_{(a,y+y')} \qquad (y,y' \in L)$$

$$\rho_{(a,\lambda y)} = \rho_{(\lambda a,y)} \qquad (\lambda \neq 0)$$

$$v \cdot \rho_{(a,y)} v^{-1} = \rho_{(v(a),v(y))} \qquad \text{para cada } v \text{ en } \Phi(Q) ,$$

y además la relación $\rho_{(a,y)} = 1$ es equivalente a la relación $y = Ka$.

Demostración:

Por el lema precedente (unicidad), basta probar las relaciones en L (o en v(L) la tercera), lo cual es inmediato a partir de la fórmula que define t_a .

-o-

Lo que hemos demostrado nos permite la observación siguiente. Con la notación de antes, el conjunto de las aplicaciones ortogonales de la forma $\rho_{(a,y)}$ (a isótropo , $y \in L$) es un subgrupo abeliano de $\Phi(Q)$, que no cambia si se sustituye a por λa ($\lambda \neq 0$) , es decir un subgrupo que sólo depende del punto $Ka \in C$. Entonces, si representamos con x la recta Ka , y con H_x la imagen de aquél grupo en $P\Phi(Q)$, se tiene que H_x es un subgrupo conmutativo de $P\Phi(Q)$ tal que para cada $v \in P\Phi(Q)$, $vH_xv^{-1} = H_{v(x)}$. En particular entonces, H_x es un subgrupo distinguido del estabilizador de x en $P\Phi(Q)$.

-o-

Lema 19:

El grupo de permutaciones $P\Omega$ es engendrado por los H_x (x variando en C) .

Demostración:

Comencemos demostrando que cualquiera sea x , H_x está contenido en $P\Omega$ y no sólo en $P\Phi$, como habíamos visto. Para demostrarlo, alcanza con ver que las aplicaciones $\rho_{(a,y)}$ que corresponden a los y de una base ortogonal de F (notación del lema 17) están en el grupo de conmutadores $\Omega(Q)$ (donde a es, como siempre, un vector isotropo cuya recta es x). Eso mismo equivale a su vez a demostrar que para cada $y \in L$ y no isótropo, $\rho_{(a,y)} \in \Omega$. Pero si recordamos la fórmula que define las t_a , vemos que cuando y no es isótropo, t_a es el producto de las simetrias s y s' res-

pecto de los hiperplanos ortogonales a y y a $y' = y+Q(y)a$, respectivamente (observar que $Q(y) = Q(y')$). Ahora bien, por el teorema de Witt, hay una transformación ortogonal, u , tal que $u(y) = y'$, lo que significa que s' es igual a usu^{-1} (Cf.: lema 4 de (8.5)). Por lo tanto, en el hiperplano L , $\rho_{(a,y)}$ coincide con $susu^{-1} \in \Omega$, y entonces por la unicidad de la extensión (lema 17) esa igualdad sigue siendo válida en todo E , de modo que $\rho_{(a,y)} \in \Omega$, l.q.d.d.

Ahora hay que demostrar que los $\{\rho_{(a,y)}\}$ engendran el grupo de conmutadores, Ω . Ya vimos (teorema 7) que $\Omega = Ha(Q)$ está engendrado por los conmutadores de la forma $susu^{-1}$, donde s es una simetría respecto de un hiperplano. Sea z ortogonal al hiperplano de s . Si el plano P definido por z y $u(z)$ es isótropo, y si a es el (único) vector isótropo que contiene, entonces $susu^{-1}$ pertenece al grupo H_a cuya imágen canónica es H_x (esto se sigue del cálculo anterior usando que $Q(u(z)) = Q(z)$ porque $u \in \phi(Q)$) . Esto prueba que en el caso considerado, los conmutadores de $\phi(Q)$ son transformaciones engendradas por los $\rho_{(a,y)}$.

Si, en cambio, el plano P es no isótropo, decimos que existe un subespacio V de E , no isótropo, de dimensión 3, que contiene P y un vector isótropo c . Eso es obvio si P es hiperbólico porque se puede tomar c en P . Como todos los vectores isótropos no pueden pertencer a un mismo hiperplano (cf.: lema 2 de (4.7)), si P no es hiperbólico, existe un vector isótropo c que no pertenece ni a P ni a P^o . Entonces el subespacio $V = P+Kc$ tiene dimensión 3 y contiene a P y a c . Falta probar que V es no isótropo. En primer lugar, notamos que V no puede contener ningún plano totalmente isótropo pues de otro modo éste cortaría a P en una recta isótropa (y hemos supuesto que P no es hiperbólico). Entonces, si V fuera isótropo, $V \subset V^o$ sería un subespacio totalmente isótropo no nulo que, por lo anterior, necesariamente es igual a la recta Kc , y eso contradice la elección de c , l.q.d.d.

Ahora, apliquemos a la restricción de Q a V lo dicho en el apéndice II: el grupo ortogonal ϕ_V de la restricción de Q a V es isomorfo al grupo $PGL(2,K)$ (Cf.: final del apéndice II), y por lo tanto, su grupo de conmutadores Ω_V es isomorfo al grupo $PSL(2,K)$. Esto y el teorema 13 prueban que el grupo Ω_V es un grupo simple. Ahora bien, en general, si un grupo es simple y H es un subgrupo cualquiera, los elementos de la forma uhu^{-1} ($h \in H$, u en el grupo) engendran todo el grupo. Por lo tanto, aplicando las propiedades ya establecidas, se sigue que en V, el conmutador $susu^{-1}$ es (en el caso que nos ocupa) producto de restricciones a V de transformaciones de la forma $\rho_{(a,y)}$ (con a e y en V). Pero entonces, éstas $\rho_{(a,y)}$ dejan fijos los vectores ortogonales a V y por tanto $susu^{-1}$ es también igual a su producto en todo el espacio E .

Por lo tanto, los generadores de Ω , $susu^{-1}$ son siempre productos de transformaciones de la forma $\rho_{(a,y)}$, de modo que Ω es engendrado por ellas. Esto demuestra el lema.

Lema 20 :

El grupo de conmutadores de $P\Omega$ es igual a $P\Omega$.

Demostración:

Por el lema precedente, basta demostrar que cada elemento de cada H_x pertenece al grupo de conmutadores de $P\Omega$. Por las hipótesis hechas a K , existe un λ no nulo cuyo cuadrado es distinto de uno. Sean a y b dos vectores isótropos tales que $\Phi(a,b) = 1$ y P el plano hiperbólico definido por ellos. Sea v la rotación de plano P tal que $v(a) = \lambda a$ y $v(b) = \lambda^{-1}b$ (usar las fórmulas del parágrafo 10). Sabemos que $v^2 \in \Omega$. Si y es ortogonal a a se tiene:

$$v^2 . \rho_{(a,y)} v^{-2} \rho^{-1}_{(a,y)} = \rho_{(a,(\lambda^2-1)y)} \qquad \text{(lema 18)}$$

de modo que cada elemento de H_a es un conmutador de elementos de Ω , por lo que hemos dicho en general sobre las transvecciones. De aquí, pasando a $P\Omega$ se deduce la tesis del lema.

-o-

Teorema 14 :

El grupo $P\Omega$ es simple .

Demostración:

En efecto, los lemas anteriores dicen que para P (como grupo de permutaciones en C) valen todas las condiciones del lema de Iwasawa .

-o-

I N D I C E