UNA NUEVA CLASIFICACION DE AUTOMORFISMOS EN UN ESPACIO VECTORIAL

por

JOSÉ MARÍA MONTESINOS AMILIBIA

En este trabajo (*) abordamos la clasificación de automorfismos de un espacio vectorial de dimensión finita sobre un cuerpo conmutativo. La clasificación clásica establece que dos automorfismos, u y u', son equivalentes si existe un tercero, v, tal que $u' = vu\, v^{-1}$. Pero entonces u y u' pueden interpretarse como iguales, a menos de un cambio de base. Así esta clasificación es excesivamente fina. Nuestro propósito es establecer una nueva clasificación menos fina que la anterior —tendrá un número finito de clases—, pero que aísle las propiedades geométricas de los automorfismos. Estas propiedades están representadas clasicamente por las variedades invariantes: en efecto, si construimos el espacio proyectivo y la proyectividad a partir del espacio vectorial y del automorfismo, lo que pretendemos es obtener la clasificación clásica de las proyectividades en homologías, etc.

Nuestro nuevo criterio de clasificación establecerá, pues —hablando sin rigor—, que dos automorfismos serán equivalentes cuando tengan el mismo número de variedades invariantes de la misma dimensión y las relaciones de dependencia lineal entre ellas sean las mismas.

Daremos algunas formulaciones más usuales de esta clasificación, y luego abordaremos el problema más útil: caracterizarla en términos matriciales.

También en este trabajo obtendremos algunos resultados adyacentes, como, por ejemplo, el cálculo efectivo del anulador de cada vector x, en el módulo sobre $\mathbb{K}[x]$ obtenido del par (E, u). El cálculo del anulador permite obtener las variedades invariantes.

Las demostraciones serán sintéticas. Las notaciones y definiciones serán esencialmente las usadas por N. Bourbaki, cap. VII. *Algébre*.

En la introducción reuniremos los resultados que se usarán más tarde. En la sección segunda definiremos equivalencia de automorfismos y daremos algunas definiciones equivalentes más útiles. También veremos su relación con la definición usual mencionada más arriba.

En la sección tercera se enunciará el teorema principal del trabajo,

(*) La definición 2.1, y la idea central del trabajo, se deben al Profesor don Francisco Botella, a quien agradezco su continuo interés por el mismo.

que no se demostrara hasta la sección quinta. La sección cuarta se dedica a algunos resultados previos, como el cálculo del anulador de un vector y obtención de un isomorfismo usado en la demostración del teorema. En la sección sexta demostraremos una versión matricial del teorema, que proporciona una caracterización de equivalencia de automorfismos en términos de matrices.

El resultado final se demuestra para cuerpos algebráicamente cerrados. En un trabajo posterior generalizaremos estos resultados a otros cuerpos.

I. Introducción.

Daremos los resultados mas importantes que luego usaremos. Muchos de ellos pueden hallarse en N. Bourbaki, caps. II y VII, *Algebre*; otros resultados son consecuencia de aquéllos. Sólo las consecuencias irán seguidas de prueba. Seguiremos las notaciones y definiciones de la obra citada.

1.1. E designa un espacio vectorial de dimensión finita n sobre un cuerpo conmutativo $\mathbb{K}$; u es un automorfismo de E.E_u, es el módulo asociado al par (E, u). La mínima variedad invariante que contiene a $x \in E$ se representa por L_x, está engendrada por $\{ u^i x \}_{\in \mathbb{N}}$, es un submódulo monógeno de E_u; y, por tanto,

$$L_x \approx \frac{\mathbb{K}[x]}{(q)},$$

donde (q) = anul x = anul L_x.

El anul $E_u = (q[x])$ se llama polinomio minimal de E_u. Entonces $q = q_1^{\alpha_1} \ldots q_r^{\alpha_r}$ es la descomposición de q en factores irreducibles. Representamos por $M(q_i)$ a ker $q_i^{\alpha_i}(u)$, entonces $M(q_i)$ es el subespacio invariante formado de los vectores $x \in E$, tales que existe $k \in N$ y $q_i^k(u)x = 0$. Se tiene la descomposición $E = M(q_1) \oplus \ldots \oplus M(q_r)$, y se designa con el nombre de primera descomposición canónica. Además anul $M(q_i) = (q_i^{\alpha_i})$.

Como los q_i son primos dos a dos, sea $x = x_1 + \ldots + x_r$, las componentes de $x \in E$, en la primera descomposición canónica; entonces

$$\text{anul } x = \prod_{i=1}^{r} \text{anul } x_i$$

1.2. Una variedad invariante se dice reducible o irreducible si lo es el submódulo correspondiente en E_u, es decir, si es o no suma directa de dos variedades invariantes no triviales. Entonces L es irreducible sí y sólo sí

$$L \approx \frac{\mathbb{K}[x]}{(p^n)}$$

donde p es un polinomio irreducible, es decir, sii L es monógena y su anulador es p^n, o todavía sii $L = L_x$ y anul $x = (p^n)$, y entonces usaremos la notación $L_x(p, n)$ para indicar que x genera a la variedad en E_u, y que anul $x = (p^n)$, con p irreducible.

Entonces E es suma directa de variedades $L_x(p, n)$. Para todo polinomio unitario irreducible $p \in |K[x]$, y para todo entero $n \geqslant 1$ el número $m(p, n)$ de subespacios $L_x(p, n)$ está determinado de manera única por el par (E, u). Además $m(p, n) > 0$ sólo si p es un divisor irreducible del polinomio minimal $q(X)$. A una descomposición de este tipo se le llamará tercera descomposición canónica de E relativa a u.

Se tiene claramente que $M(q_i)$ es suma directa de las variedades de una tercera descomposición, que sean del tipo $L_x(q_i, n)$, donde anul $x = (q_i^n)$.

II. Equivalencia de automorfismos en términos de variedades invariantes.

2.1. *Definicion.*—E es un espacio vectorial de dimensión n sobre un cuerpo conmutativo |K; u y u', dos automorfismos de E, entonces se dice que u y u' son equivalentes, sii existe un automorfismo H de E, tal que se cumple: «para toda variedad L invariante por u, y toda variedad L′ invariante por u', se tiene

a) $L = H^{-1}u' H(L)$.
b) $L' = H\ u\ H^{-1}(L')$.

Sólo hace falta demostrar que es transitiva, es decir, si además u' y u'' son equivalentes, entonces existe un automorfismo K, de modo que para toda variedad L″ invariante por u'' es:

c) $L' = K^{-1}u'' K(L')$.
d) $L'' = K\ u'\ K^{-1}(L'')$.

Entonces de *a)* y *d)* se deduce que $HL = u'\ HL$ y $K^{-1}L'' = u\ K^{-1}L''$, es decir, HL y $K^{-1}L''$ son invariantes por u'.

De *b)* y *c)* se obtiene entonces:

$$HL = K^{-1}u''K\ HL$$

$$K^{-1}L'' = HuH^{-1}\ K^{-1}L''$$

o bien

$$L = (KH)^{-1}u''\ (KH)L$$

$$L'' = (KH)\ u\ (KH)^{-1}L''$$

es decir, u y u'' son equivalentes, pues KH es un automorfismo de E.

Ahora es fácil comprobar que esta clasificación es menos fina que la siguiente: u y u' equivalentes si existe H tal que $u = H^{-1}u'H$. Es estrictamente menos fina: en efecto, veremos en 6.3. que nuestra clasificación tiene un número finito de clases.

En la proposición siguiente, que da una formulación más útil de la anterior definición, usaremos la notación L_x y L_x' para indicar variedades invariantes por u y u', respectivamente.

2.2. *Proposición.* Las tres proposiciones siguientes son equivalentes:

a) u es equivalente a u'.

b) Existe un automorfismo H, tal que para todo $x \in E$:

$$L_x = H^{-1}u' \, H(L_x)$$

$$L'_X = HuH^{-1} \, (L'_x)$$

c) Existe un automorfismo H, tal que para todo $x \in E$:

$$HL_x = L'_{Hx}$$

Dem. Que *a)* implica *b)* se deduce de ser L_x y L'_x invariantes por u y u', respectivamente.

Vamos a ver que *b)* implica *a)*. Si L y L′ son invariantes por u y u', entonces es claro que

$$L = \sum_{x \in L} L_x \quad \text{y} \quad L' = \sum_{x \in L'} L'_x.$$

Vamos a probar que $L = H^{-1}u' \, HL$, la segunda relación se demuestra de modo análogo.

Como por hipótesis

$$L = \sum_{x \in L} H^{-1}u' \, HL_x$$

basta probar que

$$\sum_{x \in L} H^{-1}u' \, HL_x = H^{-1}u' \, H(\sum_{x \in L} L_x),$$

pero esto es trivial.

Veamos que *b)* implica *c)*. Por hipótesis $HL_x = u'HL_x$, entonces $u'H_x \in HL_x$, una inducción fácil prueba que $u'^i Hx \in HL_x$; como $\{u'^i Hx\}_{i \in N}$, es un sistema de generadores de L'_{Hx}, se tiene que

$$L'_{Hx} \subset HL_x$$

También por hipótesis $H^{-1}L'_y = uH^{-1} \, L'_y$, un razonamiento análogo al anterior nos lleva a $L_{H^{-1}y} \subset H^{-1}L'_y$, $\forall \, y \in E$: para $y = Hx$ se obtiene $HL_x \subset L'_{Hx}$.

Sólo queda ver que *c)* implica *b)*. Como $HL_x = L'_{Hx}$ también $u'L'_{Hx} = u'HL_x$, como L'_{Hx} es invariante por u', se tiene $u'HL_x = HL_x$ y por tanto $L_x = H^{-1}u' \, HL_x$. La segunda relación se prueba de modo análogo. c.q.d.

La importancia del criterio *c)* estriba en que sólo se manejan variedades invariantes mínimas.

III. El Teorema principal.

Si E y E′ son dos espacios vectoriales de dimensión finita n, sobre un cuerpo conmutativo $\mathbb{K}$; distinguiremos con ′ los conceptos referentes al par (E′, u'). Entonces, por ejemplo $q(X) = q_1^{\alpha_1} \ldots q_r^{\alpha_r}$ y $q'(X) =$

$= q'^{\alpha'_1}_1 \ldots q'^{\alpha'_s}_s$, son los polinomios minimales de u y u'. $M(q_i)$ y $M(q'_i)$ tienen significados analogos, y de un modo semejante se interpretan $L_x(p, n)$, $L'_x(p', n)$ y $m(p, n)$ y $m(p', n)$. Representamos por $Q = \{q_1, \ldots, q_r\}$; analogamente Q'.

3.1. *Definición.* u y u' se llaman analogos si existe una biyección λ: $Q \longrightarrow Q'$, tal que para todo $q_i \in Q$.

a) Grado q_i = grado $\lambda(q_i)$.

b) $m(q_i, n) = m(\lambda\,[q_i], n)$ para todo $n \in N$.

Como $m(q_i, n)$ y $m(\lambda[q_i], n)$ están determinados de manera única por los pares (E, u) y (E', u'), entonces la definición anterior no depende de las terceras descomposiciones canónicas elegidas. Representamos $\lambda(q_i)$ por q'_i , $i = 1, \ldots, r$.

La proposición siguiente agrupa algunas consecuencias de la definición.

3.2. *Proposición.* Sean u y u' dos automorfismos analogos; $q(X) = q_1^{\alpha_1} \ldots q_r^{\alpha_r}$ y $q'(X) = q'^{\alpha'_1}_1 \ldots q'^{\alpha'_s}_s$ son las descomposiciones de sus polinomios minimales en factores irreducibles entonces $r = s$.

Además las dimensiones de $M(q_i)$ y $M(q'_i)$ y las de $L_x(q_i, n)$ y $L'_y(q'_i, n)$ son iguales.

Dem.-Que $r = s$ es trivial. Como

$$L_x(q_i, n) \approx \frac{\mathbb{K}[x]}{(q_i^n)},$$

entonces su dimensión es (grado $q_i)n$, como grado q_i = grado q'_i, entonces las dimensiones de $L_x(q_i, n)$ y $L'_y(q_i', n)$ son iguales. Como $M(q_i)$ y $M(q'_i)$ son suma directa de las variedades de la forma $L_x(q_i, n)$ y $L'_y(q'_i, n)$, respectivamente, también tienen la misma dimensión. c.q.d.

Ahora estableceremos el enunciado del teorema más importante. Este teorema es una versión sintética del que aparece en la sección VI, que es el más útil en las aplicaciones.

3.3. *Teorema.* Si E es un espacio vectorial de dimensión finita n sobre un cuerpo $\mathbb{K}$ conmutativo, tal que contiene las raíces de los polinomios minimales de dos automorfismos u y u', entonces u y u' son equivalentes sí y sólo sí son análogos.

3.4. *Corolario.* Si el cuerpo $\mathbb{K}$ es algebráicamente cerrado, entonces dos automorfismos u y u' son equivalentes si son análogos. En un trabajo posterior intentaremos generalizar estos resultados a cuerpos más generales.

El objeto de la sección siguiente es la preparación de la demostración del teorema.

IV. Anulador de $x \in E_u$.

Nuestro propósito es determinar de modo efectivo el anulador de un vector de E en E_u.

4.1. *Proposición.*—Sea $L_x(p, n)$ una variedad irreducible. Entonces:

a) Existe una cadena, que consta de exactamente n-miembros, $L_x(p, n) \supset L_{px}(p, n - 1) \supset \ldots \supset L_{p^m x}(p, n - m) \supset \ldots \supset L_{p^{n-1}x}(p, 1)$ de variedades irreducibles, donde $L_{p^m x}(p, n - m)$ esta generada por $p^m x$ en E_u y anul $p^m x = (p^{n-m})$.

b) Si $z \in L_{p^m x}(p, n\text{-}m)$, pero z no pertenece al siguiente miembro de la cadena, entonces anul $z = (p^{n-m})$.

c) La cadena está unívocamente determinada por $L_x(p, n)$; y una variedad invariante contenida en $L_x(p, n)$ debe coincidir necesariamente con uno de los miembros de la cadena.

Dem.—Una inducción trivial demuestra que anul $p^m x = (p^{-mn})$, usando que anul $x = (p^n)$. Por tanto la variedad monógena generada por $p^m x$ es irreducible, pues el anulador de un generador es potencia de un polinomio irreducible p.

Para completar *a)*, sólo queda ver que $L_{p^m x}(p, n - m) \supset L_{p^{m+1}x}(p, n - m - 1)$, para $m = 0, \ldots, n - 2$. Como $p^m x \in L_{p^m x}(p, n - m)$ invariante, entonces $p(p^m x) = p^{m+1}x \in L_{p^m x}(p, n - m)$ y así $L_{p^{m+1}x}(p, n - m - 1) \subset L_{p^m x}(p, n - m)$. Para ver que hay exactamente n miembros, basta observar que dos variedades sucesivas de la cadena son distintas, porque $p^m x \in L_{p^m x}$ y $p^m x \notin L_{p^{m+1}x}$, pues anul $p^m x = (p^{n-m})$.

Veamos *b)*. Si $y \in L_x(p, n)$, $y \neq 0$, entonces anul $y \supset$ anul $L_x(p, n) =$ anul $x = (p^n)$. Así, anul y es del tipo (p^k) con $k \neq 0$, pues p es irreducible, $y \neq 0$. Voy a ver que si $z \in L_{p^m x}(p, n - m)$ y z no pertenece a la variedad siguiente de la cadena, entonces $k = n - m$.

z será del tipo $z = qp^m x$, $q \in K[x]$, por ser $L_{p^m x}$ monógena. Además, p no divide a q, en otro caso $z = q' p^{m+1}x$ y $z \in L_{p^{m+1}x}$. Esto implica que $q \notin$ anul y para $y \in L_x(p, n)$, $y \neq 0$. Claramente se ve que $p^{n-m}z = 0$. Pero si $p^h z = 0$ con $h < n - m$, entonces $p^h q p^m x = q(p^{h+m}x) = 0$, como $p^{h+m}x \in L_x(p, n)$, se tiene que $p^{h+m}x = 0$ con $h + m < n$, esto contradice que anul $x = (p^n)$. Así $k = n - m$.

Veamos *c)*. Para ver que la cadena está determinada por $L_x(p, n)$, hay que ver que sus miembros pueden describirse independientemente de x. Pero $L_{p^m x}(p, n - m)$ está constituído, debido a *b)*, por los vectores de $L_x(p, n)$, tales que su anulador es (p^h) con $h \leqslant n - m$; esta descripción no depende de x.

Supóngase ahora que $L \subset L_x(p, n)$ es invariante, debe pues, ser monógena generada por $y \in L_x(p, n)$, anul $y = (p^h)$, entonces $y \in L_{p^{n-h}}(p, h)$ y entonces $L \subset L_{p^{n-h}}(p, h)$; esto implica que son iguales, ya que tienen la misma dimensión: (grado $p)h$. c.q.d.

Como se dijo en la introducción, basta hallar anul x, con $x \in M(q_i)$, para tener el anulador de cada vector de E. Como $M(q_i)$ es suma directa de variedades irreducibles del tipo $L_x(q_i, n)$, si $x_1, \ldots, x_s$ son las componentes de y perteneciente a $M(q_i)$, anul $y = \underset{i=1,\ldots,s}{\text{m.c.m.}}$ (anul x_i). Así pues, el problema se reduce a hallar anul y con $y \in L_x(p, n)$, que es una variedad irreducible, completamente resuelto mediante la proposición anterior.

Supongamos que el grado de p es s, entonces la cadena definida en 4.1. está formada por variedades que decrecen en su dimensión de s en s. Sean $x_1, \ldots, x_s$, s vectores de $L_x(p, n)$ que no pertenecen a $L_{px}(p, n-1)$, linealmente independientes y tales que, si E_s es la variedad generada por $\{x_1 \ldots, x_s\}$, sea $L_x(p, n) = L_{px}(p, n-1) \oplus E_s$.

Por la proposición 4.1., anul $x_\iota = (p^n)$, $\iota = 1, \ldots, s$. Además si $y \neq 0$ $y \in E_s$, entonces anul $y = (p^n)$.

Sean los $n.s$ elementos de $L_x(p, n)$ $\{p^m x_j\} m = 0, \ldots, n-1; j = 1, \ldots, s$.

4.2. *Proposición.*— $\{p^m x_j\}$ $m = 0, \ldots, n-1$; $j = 1, \ldots, s$ es una base de $L_x(p, n.)$.

Dem.— Obsérvese que $\{p^{n-1}x_j\}$ $j = 1, \ldots, s$, es base de $L_{p^{n-1}x}(p, 1)$, ya que si

$$\sum_{j=1}^{s} \lambda j\, p^{n-1}xj = 0$$

entonces es,

$$p^{n-1}\left(\sum_{j=1}^{s}\lambda j x_j\right) = 0$$

pero

$$\sum_{j=1}^{s} \lambda j\, xj \in Es$$

y su anulador es (p^n) a menos que

$$\sum_{j=1}^{s} \lambda j\, x_j = 0$$

y en tal caso $\lambda j = 0$, $j = 1, \ldots, s$ por ser los x_j linealmente independientes.

Supuesto que $\{p^m x_j\}$ $m = k, k+1, \ldots, n-1$; $j = 1, \ldots, s$ es base de $L_{p^k x}(p, n-k)$, voy a probar que $\{p^m x_j\}$ $m = k-1, k, \ldots, n-1$; $j = 1, \ldots, s$ es base de $L_{p^{k-1}x}(p, n-k+1)$. En efecto: $\{p^{k-1}x_j\}$ $j = 1, \ldots, s$ son linealmente independientes (argumento igual que antes). Además no pertenecen a $L_{p^k x}(p, n-k)$, pues su anulador es (p^{n-k+1}). Sea

$$z = \sum_{j=1}^{s} \lambda j\, p^{k-1}x_j$$

entonces si $z \neq 0$ anul $z = (p^{n-k+1})$, supongamos que no: sería $p^t z = 0$ con $t < n-k+1$, en ese caso

$$p^{t+k-1}\left(\sum_{j=1}^{s} \lambda j\, x_j\right) = 0$$

y entonces

$$\text{anul}\left(\sum_{j=1}^{s} \lambda j\, xj\right)$$

no es (p^n), pues

$$t + k - 1 < n \text{ y por tanto } \sum_{j=1}^{s} \lambda j \, x_j = 0.$$

Contradicción con $z \neq 0$. Por tanto la variedad generada por $\{p^{k-1}x_j\}$ $j = 1, \ldots, s$ y la $L_{p^k x}(p, n - k)$ son factores directos de $L_{p^{k-1}x}(p, n - k + 1)$. Es decir, $L_{p^m x}(p, n - m) = L_{p^{m+1}x}(p, n - m - 1) \oplus \oplus \{ p^m x_1, \ldots, p^m x_s \}$, $m = 0, \ldots, n - 1$. c.q.d.

Sean ahora E y E′ espacios vectoriales sobre K, u y u' dos automorfismos de E y E′, respectivamente, análogos. Los divisores irreducibles de los polinomios minimales de u y u' correspondientes mediante la biyección de 3.1, son q_i, q'_i como ya dijimos.

Si $x \in E$, entonces anul $x \supset (q(X))$, por tanto anul $x = (q_1^{\beta_1} \ldots q_r^{\beta_r})$ con $\beta_i \leqslant \alpha_i$ del mismo modo $y \in E'$, anul $y = (q'^{\gamma_1}_1 \ldots q'^{\gamma_r}_r)$, con $\gamma_i \leqslant \beta'_i$.

Sea H la familia de isomorfismos v: E $\longrightarrow$ E′, tales que si anul $x = (q_1^{\beta_1} \ldots q_r^{\beta_r})$, entonces anul $vx = (q'^{\beta_1}_1 \ldots q'^{\beta_r}_r)$.

Sea $m(q_i, n)$ el número de variedades del tipo $L_x(q_i, n)$ de una tercera descomposición de E relativa a u. Del mismo modo sea $m(q'_i, n)$ el número de variedades del tipo $L_y(q'_i, n)$ de una tercera descomposición de E′ relativa a u'. Como u y u' análogos, entonces $m(q_i, n) = m(q'_i, n)$.

Así, pues, sea λ una biyección entre el conjunto de variedades del tipo $L_x(q_i, n)$ y conjunto de variedades del tipo $L_y(q'_i, n)$. Supogamos que $L_x(q_i, n)$ y $L_{x'}(q'_i, n)$ son correspondientes en esta biyección.

Para definir un isomorfismo entre E y E′ bastará que definamos un isomorfismo entre $L_x(q_i, n)$ y $L_{x'}(q'_i, n)$.

Entonces, si $\{q_i^m x_j\}$ $m = 0, \ldots, n - 1$; $j = 1, \ldots, s$ y $\{ q'^m_i x'_j \}$ $m = 0, \ldots, n - 1$; $j = 1, \ldots, s$ son las bases de $L_x(q_i, n)$ y $L_{x'}(q'_i, n)$, respectivamente, definidas en 4.2; me bastará con definir $H(q_i^m x_j) = q'^m_i x'_j$ $m = 0, \ldots, n - 1$; $j = 1, \ldots, s$. Así H es un isomorfismo que transforma $L_{q_i^h x}(q_i, n - h)$ en $L_{q'^h_i x'}(q'_i, n - h)$ por la proposición 4.2.

También $H(M(q_i)) = M(q'_i)$, $i = 1, \ldots, r$. En efecto, si $x \in M(q_i)$ entonces, como anul $x = (q_i^{\beta_i})$, debe ser $Hx \in M(q'_i)$ para que anul $Hx = (q'^{\beta_i}_i)$.

Obsérvese que las elecciones de H dependen de la elección de dos descomposiciones canónicas para E y E′; de la biyección λ, y por fin de elección de los $\{ x_i \}$ y $\{ x'_i \}$ $i = 1, \ldots, s$. Utilizaremos la notación V para la familia de isomorfismos H así definidos. Entonces:

4.3. *Proposición.*—$V \subset H$.

Dem.—Sea $H \in V$ anul $y = (q_1^{\beta_1} \ldots q_r^{\beta_r})$; hay que probar que anul $Hy = (q'^{\beta_1}_1 \ldots q'^{\beta_r}_r)$. Basta probarlo para $y \in M(q_i)$, en efecto, si $y \in$ E y $\{ y_1 \ldots , y_t \}$ son sus componentes en las variedades $M(q_i)$, se tiene

$$\text{anul } y = \prod_{j=1}^{t} \text{anul } y_j,$$

y como $H(M(q_i)) = M(q'_i)$, entonces

$$\text{anul } Hy = \prod_{j=1}^{t} \text{anul } Hy_j.$$

Si ahora $y \in M(q_i)$, sean $\{y_1, \ldots , y_m\}$ sus componentes en variedades del tipo $L_x(q_i, n)$; entonces basta probar la proposición para $y \in L_x(q_i, n)$.

Sea $y \in L_x(q_i, n)$ y anul $y = (q_i^{n-m})$, entonces $y \in L_{q_i^m x}(q_i, n - m)$, pero no pertenece a la siguiente variedad de la cadena, esto implica que $Hy \in L_{q'_i{}^m x}(q'_i, n - m)$, pero no pertenece a la siguiente variedad de la cadena, por tanto anul $Hy = (q'_i{}^{n-m})$. c.q.d.

V. Demostración del teorema 3.3.

El teorema será una consecuencia de una sucesión de lemas y proposiciones más generales.

5.1. *Proposición.*—E, E′ son espacios vectoriales de dimensión finita n sobre un cuerpo conmutativo $\mathbb{K}$; u y u' dos automorfismos análogos de E y E′, respectivamente; $H : E \longrightarrow E'$ un isomorfismo de H, tal que $HL_x(p, n) = L_{Hx}$ para toda variedad irreducible $L_x(p, n)$; entonces L_{Hx} es irreducible y además $HL_y = L_{Hy}$, para todo $y \in E$.

Dem.—Que L_{Hx} es irreducible se deduce inmediatamente de la propiedad para $L_x(p, n)$.

Sea $y \in E$, y sea anul $y = (q_1{}^{\beta_1} \ldots q_r{}^{\beta_r}) =$ anul L_y, como L_y es invariante, entonces

$$L_y = \bigoplus_{i=1}^{r} [L_y \cap M(q_i)].$$

Pero $L_y \cap M(q_i)$ es monógena por ser submódulo de un módulo monógeno, además anul $L_y \cap M(q_i) = (q_i^{n_i})$ con q_i irreducible; por tanto, $L_y \cap M(q_i)$ es una variedad irreducible, así es del tipo $L_{z_i}(q_i, n_i)$.

De esto se deduce que

$$HL_y = \bigoplus_{i=1}^{r} HL_{z_i}(q_i, n_i) = \bigoplus_{i=1}^{r} L_{Hz_i}.$$

Pero anul $z_i = (q_i^{n_i})$, como $H \in H$, entonces anul $Hz_i = (q'_i{}^{n_i})$, por tanto

$$L_{Hz_i} \approx \frac{\mathbb{K}[x]}{(q'_i{}^{n_i})}$$

y se deduce que

$$\mathrm{HL}_y \approx \frac{\mathrm{K}\,[x]}{(q'_1{}^{n_1} \dots q'_r{}^{n_r})}$$

pues los q'_i son primos entre sí; así HL_y es monógena y contiene a H_y, por tanto, contiene a $\mathrm{L}_{\mathrm{H}y}$; como HL_y y $\mathrm{L}_{\mathrm{H}y}$ tienen la misma dimensión — dim $\mathrm{HL}z_i\,(q_i, n_i)$ = (*grado* q_i) n_i = (grado q'_i) n_i = dim $\mathrm{L}_{\mathrm{H}zi}(q'_i, n_i)$ — se deduce $\mathrm{HL}_y = \mathrm{L}_{\mathrm{H}y}$. c.q.d.

5.2. *Lema*.—L_x es irreducible sii $x \in \mathrm{M}(q_i)$ para algún $i = 1, \dots, r$. Esto implica que $\mathrm{L}_x \subset \mathrm{M}(q_i)$.

Dem.—Si $x \notin \mathrm{M}(q_i)$, $i = 1, \dots, r$, entonces anul $x = (q_1{}^{\beta^1} \dots q_r{}^{\beta^r})$ con $\beta_i \neq 0$ $\beta_j \neq 0$, $i \neq j$; y así L_x no puede ser irreducible.

Si $x \in \mathrm{M}(q_i)$, para algún i, entonces anul $x = (q_i{}^{\beta i})$, $\beta_i \leqslant \alpha_i$, q_i irreducible, y por tanto L_x es irreducible. c.q.d.

5.3. *Proposición*.—E y E′ espacios vectoriales de dimensión finita n sobre **K** conmutativo, u y u' analogos y $\mathrm{H} \in H$ tal que $\mathrm{HL}_x = \mathrm{L}'_{\mathrm{H}x}$, para todo $x \in \mathrm{M}(q_i)$, $i = 1, \dots, r$, entonces $\mathrm{HL}_x = \mathrm{L}'_{\mathrm{H}x}$ para $\forall\, x \in \mathrm{E}$.

Dem.—Se deduce de la proposición 5.1 y del lema 5.2., que asegura que hay coincidencia entre variedades monógenas engendradas por $x \in \mathrm{M}(q_i)$ y variedades irreducibles en E.

5.4. *Lema*.—Sea $\mathrm{H} \in V$, si $x \in \mathrm{M}(q_i)$, entonces es $\mathrm{H}(q_i x) = q'_i \mathrm{H}x$ $i = 1, \dots, r$.

Dem.—La demostración es por inducción en n, siendo anul $x = (q_i{}^n)$. Para $n = 0$ es trivial.

Ahora suponemos que es cierto hasta $n - 1$. Sea x tal que anul $x = (q_i{}^n)$, como $\mathrm{M}(q_i)$ es suma directa de variedades del tipo $\mathrm{L}_y(q_i, m)$ procedentes de una tercera descomposición de E, sean $\{y_1, \dots, y_t\}$ las componentes de x en esa suma directa. Bastará probar que $\mathrm{H}q_i y_j = q'_i \mathrm{H}y_j$, $j = 1, \dots, t$. Sea $y_j \in \mathrm{L}_z(q_i, m)$ y anul $y_j = (q_i{}^{m-c})$, entonces $y_j \in \mathrm{L}q_i^c z(q_i, m - c)$ y no pertenece al siguiente miembro de la cadena. En caso de ser $m - c < n$, por hipótesis de inducción debe de ser $\mathrm{H}q_i y_j = q'_i \mathrm{H}y_j$.

Si $m - c = n$, como por la proposición 4.2., $\mathrm{L}q_i^c z(q_i, m - c) = \mathrm{L}q_i^{c+1} z(q_i, m - t - 1) \oplus \{q_i{}^c x_1, \dots, q_i{}^c x_s\}$, entonces $y_j = a + \lambda_1\, q_i{}^c x_1 + \dots + \lambda_s\, q_i{}^c x_s$, con $a \in \mathrm{L}q_i{}^{c+1}z$. Pero anul $a = (q_i{}^h)$ con $h \leqslant m - c - 1 = n - 1$, entonces $\mathrm{H}q_i a = q'_i \mathrm{H}a$.

Como $\mathrm{H} \in V$ por la definición en 4.3., cumple $\mathrm{H}q_i{}^{c+1}x_j = q'_i{}^{c+1}\mathrm{H}x_j$. por tanto $\mathrm{H}q_i(q_i{}^c x_j) = q'_i{}^{c+1}\mathrm{H}x_j = q'_i(q'_i{}^c \mathrm{H}x_j) = q'_i \mathrm{H}q_i{}^c x_j$. Por tanto $\mathrm{H}q_i y_j = \mathrm{H}q_i a + \lambda_1\, \mathrm{H}q_i(q_i{}^c x_1) + \dots + \lambda_s\, \mathrm{H}q_i(q_i{}^c x_s) = q'_i \mathrm{H}y_j$ c.q.d.

5.5. *Proposición*.—E y E′ espacios vectoriales de dimensión finita n sobre **K** conmutativo, que contiene las raíces de los polinomios minimales de u y u' isomorfismos análogos de E y E′, respectivamente. Entonces existe H tal que $\mathrm{HL}_x = \mathrm{L}_{\mathrm{H}x}$ para todo $x \in \mathrm{M}(q_i)$, y para $i = 1, \dots, r$; H isomorfismo de E sobre E′.

Dem.—Como q_i es de primer grado, una base de $\mathrm{L}_x(q_i, n)$ como la definida en 4.2., es, por ejemplo, la $\{x, q_i x, \dots, q_i{}^{n-1}x\}$. Sea $\mathrm{H} \in V$,

definido por $H(q_i^m x) = q'_i{}^m y$, para $m = 0, \ldots, n - 1$; donde $\{y, \ldots$
$\ldots, q'_i{}^{n-1} y\}$ es la base correspondiente para $L_y(q'_i, n)$.

Vamos a probar que H así definido cumple las condiciones del teorema. Sea $x \in M(q_i)$, anul $x = (q_i^n)$; vamos a probar por inducción en n que $HL_x = L_{Hx}$.

Para $n = 0$ es trivial.

Supongámoslo cierto hasta $n - 1$. Lo probaremos para $x \in M(q_i)$, tal que anul $x = (q_i^n)$. La dimensión de L_x es entonces $n = n$ (grado q_i).

Sea la variedad $Lq_i x$ contenida en L_x, como anul $q_i x = (q_i^{n-1})$ y $x \notin Lq_i x$, se tiene $L_x = Lq_i x \oplus \{x\}$, ya que la dimensión de $Lq_i x$ es $n - 1$.

Entonces $HL_x = HLq_i x \oplus \{H\, x\} = L_H q_i x \oplus \{H\, x\}$ por hipótesis de inducción. Por el lema 5.4 $Hq_i x = q'_i Hx$, entonces se tiene $HL_x =$ $= Lq'_i H_x \oplus \{Hx\}$. Pero L_{Hx} tal que anul $Hx = (q'_i{}^n)$, pues H pertenece a H, por tanto $q_i' Hx$ tiene de anulador a $(q'_i{}^{n-1})$ y como $Hx \notin Lq'_i H_x$, entonces se tiene $HL_x = Lq'_i H_x \oplus \{Hx\} = L_{Hx}$. c.q.d.

5.6. *Proposición.*—Sea E un espacio vectorial de dimensión finita n sobre un cuerpo K conmutativo, u y u' dos automorfismos de E, tales que u sea equivalente a u', entonces u y u' son análogos.

Dem.—Sea J una tercera descomposición canónica de E relativa a u. Sea H un automorfismo de E tal que $HL_x = L'_{Hx}$, para todo $x \in E$, que existe por hipótesis. Si $L_x(q_i, n)$ es una variedad de J, entonces $HL_x(q_i, n)$ es una variedad irreducible de $E_{u'}$, como indicábamos en 5.1.

Por tanto la imagen de J mediante H es una descomposición de E en suma directa de variedades irreducibles de $E_{u'}$.

Representamos esta suma directa por HJ, por lo tanto HJ es una tercera descomposición canónica de E relativa a u'.

Vamos ahora a definir una aplicación λ entre $\{q_1, \ldots, q_r\}$ y $\{q'_1, \ldots$
$\ldots, q'_s\}$ divisores irreducibles de los polinomios minimales de u y u', respectivamente. Sea $L_x(q_i, n)$ y consideremos $HL_x(q_i, n)$ que es irreducible, y como $HL_x = L_{Hx}$, entonces $HL_x(q_i, n) = L'_{Hx}(q'_j, m)$. Entonces $n = m$; en efecto, si n distinto de m, sea en $L_x(q_i, n)$ la cadena de exactamente n miembros definida en 4.1, entonces la imagen por H de esa cadena, está formada de una cadena con exactamente n miembros comenzando en $L'_{Hx}(q'_j, m)$, formada de variedades irreducibles, esto contradice 4.1., *c)*.

Como H es isomorfismo, las dimensiones de HL_x y de L'_{Hx} coinciden; como $n = m$, esto implica que grado q_i = grado q'_j.

Definimos $\lambda(q_i) = q'_j$, entonces grado q_i = grado $\lambda(q_i)$.

λ es aplicación. Sea otra $L_y(q_i, r)$, y considero $HL_y(q_i, r)$ entonces $HL_y(q_i, r) = L_{Hy}(q'_k, r)$; queremos ver que $j = k$.

Supongamos que $n \leqslant r$, entonces anul $(x + y)$ = m.c.m. (anul x, anul y) $= (q_i^n)$, por tanto si $z = x + y$, la variedad L_z es irreducible, y por tanto también la $HL_z = L'_{Hz}$, entonces anul $H_z = (q'_s{}^h)$; pero por otra parte anul Hz = m.c.m. (anul Hx, anul Hy) = m.c.m. $(q'_j{}^n, q'_k{}^r) = (q'_s{}^h)$, así $j = k = s$.

Queda probado también que para cada variedad de J, $L_x(q_i, n)$ hay al menos una en HJ, la $HL_x(q_i, n)$, del tipo $L_y(\lambda(q_i), n)$; por tanto $m(q_i, n) \leqslant m(\lambda(q_i), n)$.

λ es inyectiva. Sean $L_x(q_i, n)$ y $L_y(q_j, m)$ tales que $HL_x(q_i, n) = L_{Hx}(\lambda(q_i), n)$ y $HL_y(q_j, m) = L_{Hy}(\lambda(q_j), m)$ y $\lambda(q_i) = \lambda(q_j)$. Entonces, si $z = x + y$, el anulador de Hz es m.c.m. (anul Hx, anul Hy) $=$ m.c.m. $(\lambda(q_i)^n, \lambda(q_i)^m) = (\lambda(q_i)^{\text{máx}(m,n)})$. Así L'_{Hz} es irreducible, esto implica que $H^{-1}L'_{Hz} = Lz$ es irreducible, pero anul $z =$ m.c.m. (q_i^n, q_j^m), por tanto $i = j$.

λ es sobre. Toda variedad de HJ es del tipo $HL_x(q_i, n)$. Sea $M(q'_i)$, y $L'_y(q'_i, m)$ una variedad de HJ contenida en $M(q'_i)$, que es suma directa de tales variedades. Entonces $L'_y(q'_i, m) = HL_x(q_j, m)$, por tanto $q'_i = \lambda(q_j)$. Las variedades de HJ del tipo $L_y(\lambda(q_i), n)$ son exactamente las imágenes de las variedades de J del tipo $L_x(q_i, n)$.

Por tanto, se tiene que $m(q_i, n) = m(\lambda(qi), n)$. Así u y u' son análogas. c-q.d.

Ahora el teorema 3.3. se deduce de 5.3., 5.4., 5.5.

El corolario 3.4. es evidente.

VI. Caracterización matricial de equivalencia de automorfismos

Establecemos en esta sección una versión matricial de automorfismos análogos, definiendo lo que se entiende por matrices canónicas análogas. Entonces dos automorfismos serán equivalentes, si sus matrices canónicas son análogas.

Si el cuerpo es algebráicamente cerrado y u es un automorfismo, entonces el polinomio minimal de u se descompone así: $q = (X - \alpha_1)^{s_1} \ldots (X - \alpha_r)^{s_r}$. Si tomamos una tercera descomposición de E relativa a u, una base de la variedad irreducible $L_{xi}((X - \alpha_i), m_i)$, perteneciente a la descomposición, era $\{(X - \alpha_i)^k x\}$, $k = 0, \ldots, m_i - 1$, y era la usada para definir el isomorfismo H, del teorema 3.3.

Está claro que $X(X - \alpha_i)^k = \alpha_i (X - \alpha_i)^k + (X - \alpha_i)^{k+1}$. Por lo tanto, la matriz de la restricción de u a $L_{xi}((X - \alpha_i), m_i)$ en función de esa base, es la matriz de orden m_i:

$$U_{m_i,\alpha_i} = \begin{pmatrix} \alpha_i & 0 & 0 & \ldots & 0 & 0 \\ 1 & \alpha_i & 0 & \ldots & 0 & 0 \\ 0 & 1 & \alpha_i & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \alpha_i & 0 \\ 0 & 0 & 0 & \ldots & 1 & \alpha_i \end{pmatrix}$$

llamada matriz de Jordán de orden m_i, relativa a α_i. Nótese que m_i es la dimensión de $L_{xi}((X - \alpha_i), m_i)$.

Así pues, respecto a la base que servía para definir H, la matriz del automorfismo u está formada de cajas en diagonal que son matrices de Jordán:

$$U = \begin{pmatrix} U_{m_1,\alpha_1} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & U_{m_k,\alpha_k} \end{pmatrix}$$

a esta matriz se le llama tercera forma canónica de u. El número de cajas iguales a la caja U_{m_i,α_i} está claro que es $m((X - \alpha_i), m_i)$.

6.1. *Definición.*—Dadas dos matrices diagonales en cajas, donde las cajas son matrices de Jordán,

$$U = \begin{pmatrix} U_{m_1,\, \alpha_1} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & U_{mi,\, \alpha r} \end{pmatrix} ; U^s =$$

$$= \begin{pmatrix} U_{m'_1,\, \alpha'_1} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & U_{m's,\, \alpha's} \end{pmatrix}$$

Sean $\{\alpha_1, \dots, \alpha_r\}$ las α distintas que intervienen en U; del mismo modo sean $\{\alpha'_1, \dots, \alpha'_s\}$ las α' distintas que intervienen en U'.

Entonces U y U' se dicen análogas si se puede establecer una biyección λ: $\{\alpha_1, \dots, \alpha_r\} \longrightarrow \{\alpha'_1, \dots, \alpha'_s\}$ de tal modo que el número de cajas de U de orden m_j relativas a α_i, sea el mismo que el número de cajas de U' de orden m_j relativas a $\lambda(\alpha_i)$, $\forall\ m_j \in \mathbb{N}$.

Si ahora u y u' son análogos, existe $\bar{\lambda} : \{(X - \alpha_1), \dots (X - \alpha_r)\} \longrightarrow$ $\longrightarrow \{(X - \alpha'_1), \dots, (X - \alpha'_s)\}$ biyección, de tal modo que $m((X - \alpha_i), m_i) = m(\bar{\lambda}(X - \alpha_i), m_i)$. Entonces $\bar{\lambda}$ define λ: $\{\alpha_1, \dots, \alpha_r\} \longrightarrow$ $\longrightarrow \{\alpha'_1, \dots, \alpha'_s\}$ biyectiva, así $\bar{\lambda}(X - \alpha_i) = (X - \lambda(\alpha_i))$. Además $\{\alpha_1, \dots, \alpha_r\}$ y $\{\alpha'_1, \dots, \alpha'_s\}$ son los α y α' distintos que intervienen en las terceras formas canónicas U *y* U' de u y u', respectivamente.

Como $m((X - \alpha_i), m_j) = m(\lambda(X - \alpha_i), m_j)$ se deduce que el número de cajas de Jordán de U' de orden m_j correspondientes a αi, coincide con el número de cajas de Jordán de U' de orden m_j, correspondientes a $\lambda(\alpha_i)$. Así U y U' son análogas. El recíproco es igualmente evidente.

6.2. *Teorema.*—E es un espacio vectorial sobre un cuerpo conmutativo **K** que contienen las raíces de los polinomios minimales de u y u'.

Si U y U′ son las terceras formas canónicas de u y u', entonces u es equivalente a u' si U y U′ son análogas.

Obsérvese que el número de clases de analogía entre matrices diagonales en cajas de Jordán es finito. Esto implica el corolario.

6.3. *Corolario.*—E espacio vectorial de dimensión finita sobre un cuerpo algebráicamente cerrado y conmutativo $\mathbb{K}$. El número de clases de equivalencia de automorfismos es finito.