ANELLO DEGLI ENDOMORFISMI

Sia V uno spazio vettoriale non banale su un campo K. Denotiamo con $\mathrm{End}_K(V)$ l'insieme degli endomorfismi di V. Su tale insieme consideriamo una somma (come l'usuale somma di applicazioni) e un prodotto (come la composizione di applicazioni). Queste sono operazioni binarie ben definite. Proviamo che rispetto ad esse $\mathrm{End}_K(V)$ è un anello unitario. Notoriamente, è un gruppo abeliano rispetto alla somma (questa struttura è, in realtà, parte della sua struttura di spazio vettoriale su K). L'elemento zero è l'endomorfismo nullo. La proprietà associativa del prodotto è anch'essa ben nota dalla teoria delle applicazioni. L'elemento neutro del prodotto è l'automorfismo identico. Resta da verificare la proprietà distributiva del prodotto rispetto alla somma. La prova si scinde in due parti. Consideriamo prima la distributività a destra. Siano $f, g, h \in \mathrm{End}_K(V)$. Si ha allora, per ogni $x \in V$, in virtù della definizione di somma di endomorfismi,

$$((g+h)\circ f)(x) = (g+h)(f(x)) = g(f(x)) + h(f(x)) = (g\circ f)(x) + (h\circ f)(x) = (g\circ f + h\circ f)(x).$$

Ciò prova che $(g+h)\circ f = g\circ f + h\circ f$, come volevasi. Passiamo ora alla distributività a sinistra. Per ogni $x \in V$ si ha:

$$(f\circ(g+h))(x) = f((g+h)(x)) = f(g(x)+h(x)) = f(g(x)) + f(h(x)) = (f\circ g)(x) + (f\circ h)(x) = (f\circ g + f\circ h)(x),$$

e ciò prova che $f\circ(g+h) = f\circ g + f\circ h$. Si noti come nell'uguaglianza $=$ centrale sia intervenuta la proprietà di f come omomorfismo di gruppi (in quanto omomorfismo di spazi vettoriali).

L'anello $\mathrm{End}_K(V)$ **è commutativo se e solo se** $\dim_K V = 1$**.** Lo dimostriamo di seguito.
Se $\dim_K V = 1$, sia v_1 l'elemento di una base di V. Siano $f, g \in \mathrm{End}_K(V)$. Sia inoltre $x \in V$. Esiste allora $\lambda \in K$ tale che $x = \lambda v_1$. Siano $\alpha, \beta \in K$ tali che $f(v_1) = \alpha v_1$, $g(v_1) = \beta v_1$. Si ha quindi, stante la linearità di f e g,

$$f\circ g(x) = f(g(x)) = f(g(\lambda v_1)) = f(\lambda g(v_1)) = \lambda f(\beta v_1) = \lambda\beta f(v_1) = \lambda\beta\alpha v_1.$$

Un calcolo del tutto analogo permette di concludere che

$$g\circ f(x) = \lambda\alpha\beta v_1.$$

Ciò prova che $f\circ g = g\circ f$ (si ricordi che il prodotto di K è commutativo, e quindi $\alpha\beta = \beta\alpha$).

Supponiamo ora che sia $\dim_K V > 1$. Esistono allora due elementi di V linearmente indipendenti, siano essi v_1 e v_2. È allora possibile definire due endomorfismi f e g in modo tale che si abbia

$f(v_1) = v_2$,
$g(v_2) = v_1$, $g(v_1) = 0$

Si ha dunque

$$f \circ g(v_1) = f(g(v_1)) = f(0) = 0,$$

mentre

$$g \circ f(v_1) = g(f(v_1)) = g(v_2) = v_1.$$

Ciò prova che $f \circ g \neq g \circ f$. Quindi l'anello $\text{End}_K(V)$ non è commutativo.

Esaminiamo ora le proprietà di invertibilità. Ricordiamo che gli elementi invertibili a destra sono gli endomorfismi surgettivi, quelli invertibili a sinistra gli endomorfismi iniettivi.
Se $\dim_K V$ è finita, allora un endomorfismo è iniettivo se e solo se è surgettivo, quindi le nozioni di invertibilità a destra e a sinistra sono coincidenti, e quindi equivalenti all'invertibilità.
Supponiamo allora che $\dim_K V$ sia infinita. In tal caso è possibile determinare elementi invertibili a destra e non a sinistra, oppure a sinistra e non a destra, e confutare l'unicità dell'inverso destro e dell'inverso sinistro.
Considerata una base di V, data dalla famiglia $\{v_i\}_{i\in I}$, ove I è un insieme infinito, siano $\varphi : I \to I$ un'applicazione non iniettiva, ma surgettiva, e $\psi : I \to I$ un'applicazione iniettiva, ma non surgettiva. Allora, ponendo, per ogni $i \in I$, $f(v_i) = v_{\varphi(i)}$ e $g(v_i) = v_{\psi(i)}$, si determinano univocamente un endomorfismo f invertibile a destra, ma non a sinistra, ed un endomorfismo g invertibile a sinistra, ma non a destra.
Inoltre, ogni endomorfismo invertibile solo a destra è dotato di almeno due inversi destri, ogni endomorfismo invertibile solo a sinistra ha almeno due inversi sinistri.
<u>Sia $f \in End_K(V)$ non iniettivo, ma surgettivo</u>. Esiste allora un elemento non nullo $v \in V$ per il quale esistono due distinti elementi $w, w' \in V$ tali che $f(w) = f(w') = v$ (si ricordi che la controimmagine di un qualsiasi elemento di V, qualora non vuota, è uno sottospazio affine di V avente la stessa dimensione di $\text{Ker} f$.) Sia B una base di V a cui appartiene v. Allora per ogni $x \in B \setminus \{v\}$ esiste $y_x \in V$ tale che $f(y_x) = x$. Definiamo un endomorfismo g ponendo $g(x) = y_x$ per ogni $x \in B \setminus \{v\}$, e $g(v) = w$. Allora, per ogni $x \in B \setminus \{v\}$ si ha $f \circ g(x) = f(g(x)) = f(y_x) = x$, e $f \circ g(v) = f(w) = v$, quindi $f \circ g = \text{id}_V$, ossia g è un

inverso destro di f. Tale è però anche l'endomorfismo g' definito come la variante di g ottenuta modificando l'immagine di v, e ponendo $g'(v) = w'$. Nel caso in cui K sia infinito, infinite sono le scelte di w' e quindi infiniti gli inversi destri di f.
Sia ora $f \in \text{End}_K(V)$ iniettivo, ma non surgettivo. Sia B una base di V. La sua immagine secondo f è una base B' di $\text{Im}f$ (che è un sottospazio proprio di V). Sia B'' un suo completamento ad una base di V. Per ogni $y \in B'$ esiste un unico $x_y \in B$ tale che $f(x_y) = y$. Definiamo un endomorfismo g ponendo, per ogni $y \in B'$, $g(y) = x_y$, ed assegnando in un modo qualsiasi le immagini degli elementi di B''. Allora si ha $g \circ f(x_y) = x_y$, ossia $g \circ f$ manda ogni elemento di B in sé stesso, e dunque $g \circ f = \text{id}_V$. Poiché B'' è non vuota, esistono più modi di definire g, visto che l'immagine di ogni elemento di B'' potrà essere assegnata almeno in due modi: ponendola uguale all'elemento stesso, oppure a 0. Nuovamente, se K è infinito, esistono infiniti modi di definire g, e quindi infiniti inversi sinistri per f.

Veniamo ora ai divisori dello zero. Un endomorfismo f è divisore dello zero se e solo se esiste un endomorfismo g non nullo tale che

$f \circ g = 0$ oppure $g \circ f = 0$

ove con 0 abbiamo indicato l'endomorfismo nullo. Queste due condizioni si traducono, rispettivamente in
1) $\text{Im}g \subset \text{Ker}f$
2) $\text{Im}f \subset \text{Ker}g$

La 1) è verificata da qualche endomorfismo non nullo g se e solo se $\text{Ker } f$ **non è ridotto al solo zero (ossia f non è iniettivo)**. In tal caso, basterà definire un endomorfismo g che invii ogni elemento di una base di V nello stesso elemento non nullo di $\text{Ker } f$.
La 2) è verificata da qualche endomorfismo non nullo g se e solo se $\text{Im } f$ **non è l'intero spazio V** (**ossia f non è surgettivo**). In tal caso basterà definire g in modo che ogni elemento di una base di $\text{Im } f$ sia inviato in 0, e gli elementi che completano tale base ad una base di V siano inviati nello stesso elemento non nullo di V.

In conclusione: **i divisori dello zero di $\text{End}_K(V)$ sono tutti e soli quelli non nulli che non sono bigettivi. In altri termini: in $\text{End}_K(V)$ un elemento non nullo è regolare se e solo se è invertibile.**

APPENDICE - ANELLI DI MATRICI
Quanto osservato a proposito di $\text{End}_K(V)$ quando $\dim_K V = n < \infty$ si trasferisce, secondo

le modalità ben note dall'algebra lineare, a $M_n(K)$, insieme delle matrici quadrate di ordine n a coefficienti in K. Questo, rispetto alla somma termine a termine ed al prodotto righe per colonne, è un anello unitario, avente come elemento uno la matrice identità e come elemento zero la matrice nulla, inoltre è commutativo se e solo se $n = 1$. Un elemento X di questo anello è invertibile a destra se e solo se è invertibile a sinistra, ed in tal caso il suo inverso è la sua cosiddetta *matrice inversa* X^{-1}. La matrice X è invertibile se e solo se $\det X$ è diverso da zero. Infine, l'invertibilità equivale alla regolarità.

Più in generale, dato un anello commutativo unitario (non banale) A, l'insieme $M_n(A)$ delle matrici quadrate di ordine n a coefficienti in A è a sua volta un anello unitario. Se $n = 1$, allora è anche commutativo, in quanto è isomorfo ad A, mediante l'assegnazione $a \mapsto (a)$. Se, invece, $n > 1$, allora l'anello non è commutativo. Infatti non commuta il prodotto delle matrici $X = (x_{ij})$ e $Y = (y_{ij})$ così definite:

$x_{21} = 1,\ x_{ij} = 0$ per $(i, j) \neq (2, 1)$
$y_{12} = 1,\ y_{ij} = 0$ per $(i, j) \neq (1, 2)$

Basta osservare che, da un lato, il coefficiente di indice $(1, 1)$ di XY è $0,$ dato che la prima riga di X è nulla, mentre il coefficiente di indice (1,1) di YX è $y_{12}x_{21} = 1$, unico prodotto non nullo nella moltiplicazione della prima di riga di Y per la prima colonna di X.
Infine, si prova che X **è un elemento regolare di** $M_n(A)$ **se e solo se** $\det X$ **è un elemento regolare di** A**.**